IBM Spectrum Protect Knowledge Center Version 8.1.2

Inhaltsverzeichnis

Dokumentation für IBM Spectrum Protect

IBM Spectrum Protect stellt automatisierte, zentral geplante, maßnahmenverwaltete Sicherungs-, Archivierungs- und Speicherverwaltungsfunktionen für Dateiserver, Workstations, virtuelle Maschinen und Anwendungen bereit. Verwenden Sie die IBM Spectrum Protect-Dokumentation, die Sie beim Definieren, Konfigurieren und Verwalten Ihrer Datenschutzlösungen unterstützt.

Einführung

Installation und Upgrade für Server durchführen
Operations Center installieren und Operations Center-Upgrade durchführen
Clients für Sichern/Archivieren installieren
Datenschutzlösungen auswählen und implementieren
Neuerungen für den Server
Neuerungen für Clients
Videos mit den Neuerungen
PDF-Dateien

Allgemeine Tasks

Tägliche Überwachungstasks
Clients hinzufügen
Clientdaten auf einen anderen Server replizieren
Server, Clients und Operations Center verwalten
Speicher konfigurieren
Clients für Sichern/Archivieren konfigurieren
Daten sichern
Serverbefehle, -optionen und -dienstprogramme

Fehlerbehebung und Unterstützung

Fehler beheben
Leistung optimieren
Neueste Fixpacks für IBM Spectrum Protect-Clients und -Server
IBM Software Support

Weitere Informationen

Hinweise für Benutzer des IBM® Knowledge Center
Produktsuites und zugehörige Produkte
Homepage der Produktfamilie
Wiki für IBM Spectrum Protect-Produkte
IBM Spectrum Protect Developer Center
IBM Redbooks-Veröffentlichungen
IBM Systems Training
Behindertengerechte Bedienung
Rechtliche Hinweise zum Produkt

Funktionen zur behindertengerechten Bedienung für die IBM Spectrum Protect-Produktfamilie

Funktionen zur behindertengerechten Bedienung helfen Benutzern mit Behinderungen, wie eingeschränkter Beweglichkeit oder Sehfähigkeit, damit sie informationstechnologische Inhalte erfolgreich verwenden können.

Übersicht

Die IBM Spectrum Protect-Produktfamilie umfasst die folgenden bedeutenden Funktionen zur behindertengerechten Bedienung:

- Bedienung ausschließlich über die Tastatur
- Operationen, die ein Sprachausgabeprogramm verwenden

Die IBM Spectrum Protect-Produktfamilie verwendet den neuesten W3C-Standard WAI-ARIA 1.0, um die Einhaltung von US Section 508 und der Web Content Accessibility Guidelines (WCAG) 2.0 sicherzustellen. Um die Funktionen zur behindertengerechten Bedienung zu nutzen, verwenden

Sie das neueste Release Ihres Sprachausgabeprogramms in Verbindung mit dem neuesten Web-Browser, der von diesem Produkt unterstützt wird.

Die Produktdokumentation im IBM Knowledge Center ist für die behindertengerechte Bedienung aktiviert. Eine Beschreibung der Funktionen zur behindertengerechten Bedienung im IBM Knowledge Center finden Sie im Abschnitt 'Accessibility' der IBM Knowledge Center-Hilfe .

Navigation mithilfe der Tastatur

Dieses Produkt verwendet Standardnavigationstasten.

Schnittstelleninformationen

In den Benutzerschnittstellen gibt es keine Inhalte, die 2 - 55 Mal in der Sekunde blinken.

Die Webbenutzerschnittstellen basieren auf Cascading Style Sheets, um Inhalte ordnungsgemäß wiederzugeben und um positive Erfahrungen zu ermöglichen. Die Anwendung bietet eine funktional entsprechende Möglichkeit für Benutzer mit eingeschränktem Sehvermögen, um die Systemanzeigeeinstellungen des Benutzers einschließlich des Modus für kontraststarke Anzeige zu verwenden. Sie können die Schriftgröße über die Einstellungen für die Einheit oder für den Web-Browser steuern.

Die Webbenutzerschnittstellen beinhalten WAI-ARIA-Navigationsmarkierungen, mit deren Hilfe Sie schnell zu Funktionsbereichen in der Anwendung navigieren können.

Software anderer Anbieter

Die IBM Spectrum Protect-Produktfamilie enthält bestimmte Software anderer Anbieter, die nicht der IBM Lizenzvereinbarung unterliegt. IBM gibt keine Erklärung zu den Funktionen zur behindertengerechten Bedienung dieser Produkte ab. Wenden Sie sich an den Softwareanbieter, um Informationen zur behindertengerechten Bedienung der Produkte zu erhalten.

Zugehörige Informationen zur behindertengerechten Bedienung

Neben dem standardmäßigen IBM Help-Desk und den Support-Websites bietet IBM einen TTY-Telefonservice für gehörlose oder hörgeschädigte Kunden für den Zugriff auf Vertriebs- und Support-Services:

TTY-Service
800-IBM-3383 (800-426-3383)
(innerhalb von Nordamerika)

Weitere Informationen zum Engagement von IBM im Bereich der behindertengerechten Bedienung finden Sie in IBM Accessibility.

Produktsuites und zugehörige Produkte

IBM Spectrum Protect-Suites und zugehörige Speicherprodukte verbessern und erweitern die Features des IBM Spectrum Protect-Basisprodukts.

Produktsuites und Lizenzoptionen

Die Produkte IBM Spectrum Protect und IBM Spectrum Protect Extended Edition stellen die Kernkomponenten für automatisierte und zentrale Sicherungs- und Zurückschreibungsoperationen bereit. Die Serverkomponente und die Clientkomponente für Sichern/Archivieren stellen Basisfunktionen wie z. B. Sicherungs- und Zurückschreibungsoperationen sowie Archivierungs- und Abrufoperationen für Dateien, Verzeichnisse und Plattenimages zur Verfügung.

Die Produktdokumentation enthält Informationen sowohl für IBM Spectrum Protect als auch für IBM Spectrum Protect Extended Edition.

Produktsuites, die IBM Spectrum Protect mit zugehörigen Produkten kombinieren, bieten unter Umständen eine einfachere Möglichkeit, um IBM Spectrum Protect-Software zu kaufen und zu verwalten. Die Suites umfassen Produkte, die einen Bereich von Datenschutz- und Wiederherstellungsanforderungen mit vereinfachter Lizenzierung erfüllen können. Weitere Informationen zu IBM Spectrum Protect-Produktsuites.

Zugehörige Produkte

Sie können IBM Spectrum Protect mit Funktionen und Features erweitern, die in zugehörigen Produkten verfügbar sind.

Produkt	Wichtige Vorteile	Links
IBM Spectrum Copy Data Management	Katalogisiert NetApp- und VMware-Momentaufnahmen, um die rollenabhängige Verwaltung und Wiederherstellung von Sicherungsdaten zu erleichtern.	• Weitere Informationen und Kauf • Produktdokumentation

Produkt	Wichtige Vorteile	Links
IBM Spectrum Protect High Speed Data Transfer	Verwenden Sie dieses Produkt für die Aktivierung der FASP-Technologie (FASP = Fast Adaptive Secure Protocol), um die Datenübertragung in einer Umgebung zu verbessern, in der WAN-Leistungsprobleme erkannt werden.	• Weitere Informationen und Kauf • Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann
IBM Spectrum Protect for Data Retention	Stellt beim Archivieren von Geschäftsaufzeichnungen, Dateien oder Daten einen langfristigen Aufbewahrungsschutz zur Verfügung. Die Archivierung von Daten zur Einhaltung gesetzlicher Bestimmungen erfordert zusätzliche Sicherheitseinrichtungen oder zusätzlichen Schutz, der als Aufbewahrungsschutz für Daten bezeichnet wird. Mit diesen Sicherheitseinrichtungen kann sichergestellt werden, dass Daten entweder versehentlich oder mutwillig nicht frühzeitig gelöscht werden. Um die gesetzlichen Bestimmungen einzuhalten, stellt IBM Spectrum Protect for Data Retention einen zusätzlichen Schutz für Daten bereit, die von IBM Spectrum Protect archiviert werden.	• Weitere Informationen und Kauf • Produktdokumentation Tipp: Dokumentation für dieses Produkt ist in der IBM Spectrum Protect-Dokumentation enthalten.
IBM Spectrum Protect Snapshot	Schützt Daten mit integrierten, anwendungsgesteuerten Momentaufnahmesicherungs- und -zurückschreibungsfunktionen. Daten, die von IBM® DB2-, SAP-, Oracle-, Microsoft Exchange- und Microsoft SQL Server-Anwendungen gespeichert werden, können mit IBM Spectrum Protect Snapshot-Software geschützt werden. Mit der Software können Sie Momentaufnahmen auf Datenträgerebene für Dateisysteme und kundenspezifische Anwendungen erstellen und verwalten. Sie können auswählen, ob IBM Spectrum Protect Snapshot in IBM Spectrum Protect integriert werden soll.	• Weitere Informationen und Kauf • Produktdokumentation
IBM Spectrum Protect for Databases	Schützt Oracle-Daten und Microsoft SQL-Daten durch automatische Tasks, Dienstprogramme und Schnittstellen. Diese Software erstellt konsistente und zentrale Onlinesicherungen, um Ausfallzeiten zu vermeiden, kritische Unternehmensdaten zu schützen und Betriebskosten zu minimieren. Tipp: Unterstützung für Onlinesicherungen von IBM DB2- und IBM Informix-Datenbanken ist mit IBM Spectrum Protect-Servern eingeschlossen. Sie müssen nicht IBM Spectrum Protect for Databases installieren, um diese Datenbanken zu sichern. Weitere Informationen finden Sie in der Dokumentation für die Produkte DB2 und Informix.	• Weitere Informationen und Kauf • Produktdokumentation
IBM Spectrum Protect for Enterprise Resource Planning	Stellt Schutz bereit, der für SAP-Systemdaten angepasst ist.	• Weitere Informationen und Kauf • Produktdokumentation
IBM Spectrum Protect for Mail	Automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass Microsoft Exchange-Server oder IBM Domino-Server heruntergefahren werden.	• Weitere Informationen und Kauf • Produktdokumentation

Produkt	Wichtige Vorteile	Links
IBM Spectrum Protect for Space Management	Ein Produkt für die hierarchische Speicherverwaltung, mit dem Speicherkosten für Informationen reduziert werden, auf die selten zugegriffen wird, ohne dass sich die Art und Weise ändert, wie Benutzer und Anwendungen mit ihren Daten interagieren. Verwenden Sie dieses Produkt auf AIX- und Linux-Betriebssystemen.	• Weitere Informationen und Kauf • Produktdokumentation
IBM Spectrum Protect HSM for Windows	Ein Produkt für die hierarchische Speicherverwaltung, mit dem Speicherkosten für Informationen reduziert werden, auf die selten zugegriffen wird, ohne dass sich die Art und Weise ändert, wie Benutzer und Anwendungen mit ihren Daten interagieren. Verwenden Sie dieses Produkt auf Windows-Betriebssystemen.	• Weitere Informationen und Kauf • Produktdokumentation
IBM Spectrum Protect for SAN	Arbeitet mit Servern und Client-Computern, um Daten über ein Speicherbereichsnetz (SAN) anstelle eines LAN zu übertragen. Das Produkt ist ein Speicheragent, der LAN-unabhängige Sicherungs- und Zurückschreibungsoperationen ermöglicht.	• Weitere Informationen und Kauf • Produktdokumentation Version der Produktdokumentation: Die Dokumentation für IBM Spectrum Protect for SAN Version 7.1 ist für die Verwendung mit der IBM Spectrum Protect-Produktfamilie Version 8.1 anwendbar.
IBM Spectrum Protect for Virtual Environments	Stellt Schutz bereit, der für virtuelle VMware- und Hyper-V-Umgebungen angepasst ist.	• Weitere Informationen und Kauf • Produktdokumentation
IBM Tivoli Storage Manager for z/OS Media	Verwaltet z/OS-Platten- und -Bandressourcen für IBM Spectrum Protect-Server, die auf AIX- oder Linux on System z-Systemen ausgeführt werden.	• Produktdokumentation

PDF-Dateien

Sie können vorgefertigte PDF-Dateien aus dem IBM® Knowledge Center oder von einer FTP-Download-Site herunterladen.

Vorgefertigte PDF-Dateien

In den folgenden Abschnitten sind die vorgefertigten PDF-Dateien aufgeführt, die für dieses Release verfügbar sind:

- Datenschutzlösungen
- Server
- Clients für Sichern/Archivieren
- API

Paket der PDF-Dateien

Laden Sie ein Paket, das alle PDF-Dateien für dieses Release enthält, von der folgenden FTP-Site herunter:

ftp://public.dhe.ibm.com/software/products/ISP/current/

Aktualisierungen in diesem Release

Lesen Sie die Informationen zu den neuen Funktionen und funktionalen Erweiterungen, die in den Produkten verfügbar sind, um die potenziellen Vorteile für Ihre Speicherverwaltungsoperationen erkennen zu können. Die Releaseinformationen enthalten Links, auf die Sie zugreifen können, um wichtige Informationen abzurufen, bevor Sie Produkte und Komponenten installieren oder aktualisieren.

Komponente	Zusammenfassung der Aktualisierungen	Releaseinformationen für Version 8.1
Serverkomponenten	Aktualisierungen	Releaseinformationen
Client für Sichern/Archivieren	Aktualisierungen	Releaseinformationen

Komponente	Zusammenfassung der Aktualisierungen	Releaseinformationen für Version 8.1
Anwendungsprogrammierschnittstelle (API)	Aktualisierungen	Releaseinformationen

IBM Spectrum Protect-Konzepte

IBM Spectrum Protect stellt eine umfassende Datenschutzumgebung bereit.

- Übersicht über IBM Spectrum Protect
  IBM Spectrum Protect stellt zentralen automatisierten Datenschutz bereit, mit dessen Hilfe die Wahrscheinlichkeit eines Datenverlusts verringert und die Erfüllung von Anforderungen hinsichtlich Datenschutz und Verfügbarkeit gewährleistet werden kann.
- Konzepte der Datenspeicherung in IBM Spectrum Protect
  IBM Spectrum Protect stellt Funktionen zum Speichern von Daten in Einheitenspeicher und externem Speicher bereit.
- Datenschutzstrategien bei IBM Spectrum Protect
  IBM Spectrum Protect stellt Möglichkeiten zur Implementierung verschiedener Datenschutzstrategien bereit.

Übersicht über IBM Spectrum Protect

IBM Spectrum Protect stellt zentralen automatisierten Datenschutz bereit, mit dessen Hilfe die Wahrscheinlichkeit eines Datenverlusts verringert und die Erfüllung von Anforderungen hinsichtlich Datenschutz und Verfügbarkeit gewährleistet werden kann.

- Datenschutzkomponenten
  Die Datenschutzlösungen, die von IBM Spectrum Protect bereitgestellt werden, umfassen einen Server, Clientsysteme und -anwendungen sowie Speichermedien. IBM Spectrum Protect stellt Managementschnittstellen für die Überwachung und das Zurückmelden des Datenschutzstatus bereit.
- Datenschutzservices
  IBM Spectrum Protect stellt Datenschutzservices zum Speichern und Wiederherstellen von Daten für verschiedene Clienttypen bereit. Die Datenschutzservices werden über Maßnahmen implementiert, die auf dem Server definiert sind. Die Datenschutzservices können mithilfe der Clientzeitplanung automatisiert werden.
- Prozesse zur Verwaltung des Datenschutzes mit IBM Spectrum Protect
  Der IBM Spectrum Protect-Serverbestand übernimmt eine wichtige Rolle in den Prozessen für den Datenschutz. Sie definieren Maßnahmen, die der Server zum Verwalten des Datenspeichers verwendet.
- Benutzerschnittstellen für die IBM Spectrum Protect-Umgebung
  Für Überwachungs- und Konfigurationstasks stellt IBM Spectrum Protect verschiedene Schnittstellen, einschließlich des Operations Center, einer Befehlszeilenschnittstelle und einer SQL-Verwaltungsschnittstelle, bereit.

Datenschutzkomponenten

Die Datenschutzlösungen, die von IBM Spectrum Protect bereitgestellt werden, umfassen einen Server, Clientsysteme und -anwendungen sowie Speichermedien. IBM Spectrum Protect stellt Managementschnittstellen für die Überwachung und das Zurückmelden des Datenschutzstatus bereit.

Server

Clientsysteme senden Daten zur Speicherung als Sicherungen oder archivierte Daten an den Server. Der Server umfasst einen *Bestand*, der ein Repository der Informationen zu Clientdaten ist.

Der Bestand umfasst die folgenden Komponenten:

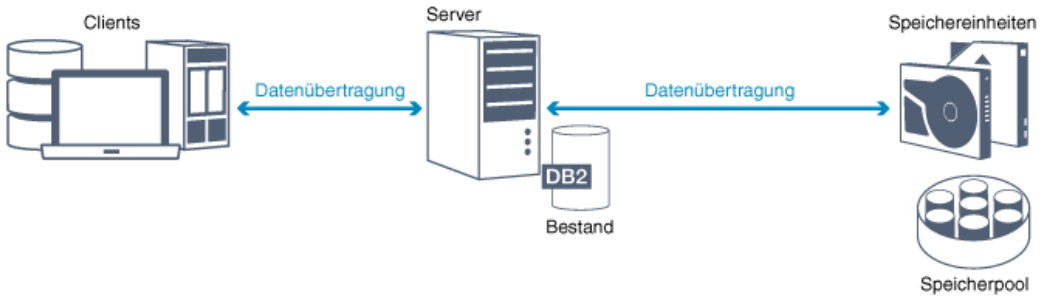
Datenbank
: Informationen zu jeder Datei, jedem logischen Datenträger oder jeder Datenbank, die bzw. den der Server sichert, archiviert oder umlagert, werden in der Serverdatenbank gespeichert. Die Serverdatenbank enthält auch Informationen zu der Maßnahme und den Zeitplänen für Datenschutzservices.

Wiederherstellungsprotokoll
: Aufzeichnungen von Datenbanktransaktionen werden in diesem Protokoll aufbewahrt. Die Datenbank verwendet das Wiederherstellungsprotokoll, um Datenkonsistenz in der Datenbank zu gewährleisten.

Clientsysteme und -anwendungen

Clients sind Anwendungen, virtuelle Maschinen und Systeme, die geschützt werden müssen. Die Clients senden Daten an den Server (siehe Abbildung 1).

Abbildung 1. Komponenten in der Datenschutzlösung



Client-Software
: Damit IBM Spectrum Protect Clientdaten schützen kann, muss auf dem Clientsystem die entsprechende Software installiert sein und der Client muss beim Server registriert sein.

Clientknoten
: Ein *Clientknoten* ist äquivalent zu einem Computer, einer virtuellen Maschine oder einer Anwendung, wie beispielsweise ein Client für Sichern/Archivieren, der auf einer Workstation für Dateisystemsicherungen installiert ist. Jeder Clientknoten muss beim Server registriert sein. Auf einem einzelnen Computer können mehrere Knoten registriert sein.

Speichermedien

Der Server speichert Clientdaten auf Speichermedien. Die folgenden Typen von Medien werden verwendet:

Speichereinheiten

: Der Server kann Daten auf Festplattenlaufwerke, Plattenarrays und -subsysteme, Standalone-Bandlaufwerke, Bandarchive und andere Typen von Speicher mit wahlfreiem und sequenziellem Zugriff schreiben. Speichereinheiten können direkt mit dem Server verbunden werden oder über ein lokales Netz (LAN) oder ein Speicherbereichsnetz (SAN).

Speicherpools

: Speichereinheiten, die mit dem Server verbunden sind, werden in *Speicherpools* gruppiert. Jeder Speicherpool stellt eine Gruppe von Speichereinheiten desselben Datenträgertyps dar, wie beispielsweise Platten- oder Bandlaufwerke. IBM Spectrum Protect speichert alle Clientdaten in Speicherpools. Sie können Speicherpools in einer *Hierarchie* anordnen, sodass Datenspeicher aus Plattenspeicher in kostengünstigeren Speicher, wie beispielsweise Bandeinheiten, übertragen werden kann.

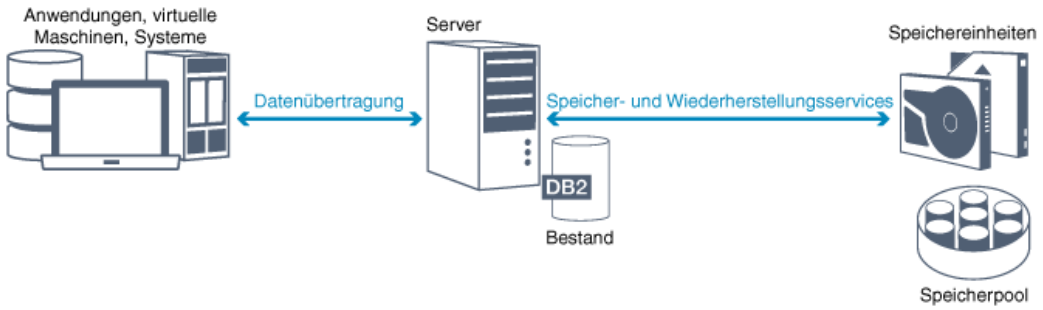
Datenschutzservices

IBM Spectrum Protect stellt Datenschutzservices zum Speichern und Wiederherstellen von Daten für verschiedene Clienttypen bereit. Die Datenschutzservices werden über Maßnahmen implementiert, die auf dem Server definiert sind. Die Datenschutzservices können mithilfe der Clientzeitplanung automatisiert werden.

Typen von Datenschutzservices

IBM Spectrum Protect stellt Services zum Speichern und Wiederherstellen von Clientdaten bereit (siehe Abbildung 1).

Abbildung 1. Datenschutzservices



IBM Spectrum Protect stellt die folgenden Typen von Datenschutzservices bereit:

Sicherungs- und Zurückschreibungsservices

: Sie führen einen Sicherungsprozess aus, um eine Kopie eines *Datenobjekts* zu erstellen, das für die Wiederherstellung verwendet werden kann, wenn das ursprüngliche Datenobjekt verloren geht. Ein Datenobjekt kann eine Datei, ein Verzeichnis oder ein benutzerdefiniertes Datenobjekt, wie beispielsweise eine Datenbank, sein.

Um die Nutzung von Systemressourcen während der Sicherungsoperation zu minimieren, verwendet IBM Spectrum Protect die *progressive Teilsicherung*. Bei dieser Sicherungsmethode wird eine erste Gesamtsicherung aller Datenobjekte erstellt und in nachfolgenden Sicherungsoperationen werden nur geänderte Daten in den Speicher versetzt. Verglichen mit Teil- und Differenzsicherungen, bei denen regelmäßige Gesamtsicherungen erforderlich sind, bietet die progressive Teilsicherung die folgenden Vorteile:

- Die Datenredundanz wird reduziert.
- Es wird weniger Netzbandbreite verwendet.
- Es ist weniger Speicherbereich im Speicherpool erforderlich.

Um die Speicherkapazitätsanforderungen und Netzbandbreitennutzung weiter zu reduzieren, schließt IBM Spectrum Protect die *Datendeduplizierung* für Datensicherungen ein. Beim Datendeduplizierungsverfahren werden doppelte Datenbereiche aus Sicherungen entfernt.

Sie führen einen Zurückschreibungsprozess aus, um ein Objekt aus einem Speicherpool auf den Client zu kopieren. Sie können eine einzelne Datei, alle Dateien in einem Verzeichnis oder alle Daten auf einem Computer zurückschreiben.

Archivierungs- und Abrufservices

Der Archivierungsservice dient zum Aufbewahren von Daten für die Langzeitspeicherung, wie beispielsweise für die Einhaltung gesetzlicher Bestimmungen. Vom Archivierungsservice werden die folgenden Funktionen bereitgestellt:

- Beim Archivieren von Daten können Sie angeben, wie lange die Daten gespeichert werden müssen.
- Sie können das Kopieren von Dateien und Verzeichnissen für die Langzeitspeicherung auf Datenträgern anfordern. Beispielsweise können Sie diese Daten auf einer Bandeinheit speichern, wodurch die Speicherkosten gesenkt werden können.
- Sie können angeben, dass die ursprünglichen Dateien nach der Archivierung vom Client gelöscht werden.

Vom Abrufservice werden die folgenden Funktionen bereitgestellt:

- Beim Abrufen von Daten werden die Daten aus einem Speicherpool auf einen Clientknoten kopiert.
- Die Abrufoperation hat keine Auswirkungen auf die Archivierungskopie im Speicherpool.

Umlagerungs- und Rückrufservices

Umlagerungs- und Rückrufservices dienen zur Verwaltung von Speicherbereich auf Clientsystemen. Ziel der Speicherbereichsverwaltung ist es, die verfügbare Datenträgerkapazität für neue Daten zu maximieren und die Zeit für den Zugriff auf Daten zu minimieren. Sie können Daten in Serverspeicher umlagern, damit immer genügend freier Speicherbereich in einem lokalen Dateisystem vorhanden ist. Zum Speichern umgelagerter Daten bestehen die folgenden Möglichkeiten:

- In Plattenspeicher für die Langzeitspeicherung
- In einem *virtuellen Bandarchiv* (VTL = Virtual Tape Library) für den schnellen Rückruf von Dateien

Sie können Dateien bei Bedarf automatisch oder selektiv auf den Clientknoten zurückrufen.

Typen von Clientdaten, die geschützt werden können

Sie können Daten für die folgenden Clienttypen mit IBM Spectrum Protect schützen:

Anwendungsclients

IBM Spectrum Protect kann Daten für bestimmte Produkte oder Anwendungen schützen. Diese Clients werden als *Anwendungsclients* bezeichnet. Um die *strukturierten Daten* für diese Clients, das heißt die Daten in Datenbankfeldern, zu schützen, müssen Sie Komponenten sichern, die für die Anwendung spezifisch sind. Mit IBM Spectrum Protect können die folgenden Anwendungen geschützt werden:

- IBM Spectrum Protect for Enterprise Resource Planning-Clients:
  - Data Protection for SAP HANA
  - Data Protection for SAP for DB2
  - Data Protection for SAP for Oracle
- IBM Spectrum Protect for Databases-Clients:
  - Data Protection for Microsoft SQL Server
  - Data Protection for Oracle
- IBM Spectrum Protect for Mail-Clients:
  - Data Protection for IBM® Domino
  - Data Protection for Microsoft Exchange Server

Virtuelle Maschinen

Virtuelle Maschinen, die unter Verwendung von Anwendungsclient-Software gesichert werden, die auf der virtuellen Maschine installiert ist. In der IBM Spectrum Protect-Umgebung kann eine virtuelle Maschine mithilfe von IBM Spectrum Protect for Virtual Environments geschützt werden.

Systemclients

Die folgenden IBM Spectrum Protect-Clients werden als *Systemclients* bezeichnet:

- Alle Clients, die Daten in Dateien und Verzeichnissen sichern, das heißt *unstrukturierte Daten*, wie Clients für Sichern/Archivieren und API-Clients, die auf Workstations installiert sind.
- Ein Server in einer Konfiguration für virtuelle Datenträger für die Kommunikation zwischen Servern.

- Eine virtuelle Maschine, die unter Verwendung der Software von Clients für Sichern/Archivieren gesichert wird, die auf der virtuellen Maschine installiert ist.

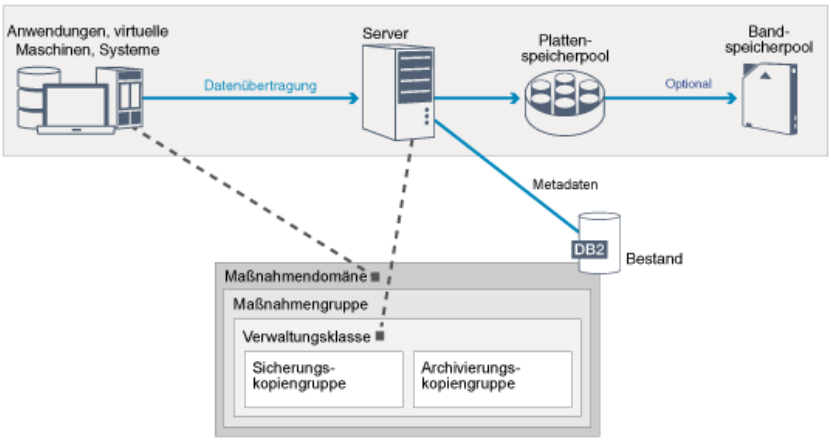
Prozesse zur Verwaltung des Datenschutzes mit IBM Spectrum Protect

Der IBM Spectrum Protect-Serverbestand übernimmt eine wichtige Rolle in den Prozessen für den Datenschutz. Sie definieren Maßnahmen, die der Server zum Verwalten des Datenspeichers verwendet.

Datenverwaltungsprozess

Abbildung 1 zeigt den IBM Spectrum Protect-Datenverwaltungsprozess.

Abbildung 1. Datenverwaltungsprozess



IBM Spectrum Protect verwendet Maßnahmen, um zu steuern, wie der Server Datenobjekte auf verschiedenen Typen von Speichereinheiten und -medien speichert und verwaltet. Sie ordnen einen Client einer Maßnahmendomäne zu, die eine einzelne aktive Maßnahmengruppe enthält. Wenn ein Client eine Datei sichert, archiviert oder umlagert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Die Verwaltungsklasse und die Sicherungs- und Archivierungskopiengruppen geben an, wo Dateien gespeichert werden und wie sie verwaltet werden. Wenn Sie Serverspeicher in einer Hierarchie konfigurieren, können Sie Dateien in andere Speicherpools umlagern.

Bestandskomponenten

Die folgenden Bestandskomponenten sind Schlüsselkomponenten für den Betrieb des Servers:

Serverdatenbank
: Die Serverdatenbank enthält Informationen zu Clientdaten und Serveroperationen. In der Datenbank werden Informationen zu Clientdaten gespeichert, die als *Metadaten* bezeichnet werden. Informationen zu Clientdaten umfassen den Dateinamen, die Dateigröße, den Dateieigner, die Verwaltungsklasse, die Kopiengruppe sowie die Position der Datei im Serverspeicher. Die Datenbank umfasst die folgenden Informationen, die für den Betrieb des Servers erforderlich sind:

  - Definitionen von Clientknoten und Administratoren
  - Maßnahmen und Zeitpläne
  - Servereinstellungen
  - Aufzeichnungen von Serveroperationen wie Aktivitätenprotokolle und Ereignissätze
  - Zwischenergebnisse für Verwaltungsabfragen

Wiederherstellungsprotokoll
: Der Server zeichnet Datenbanktransaktionen im Wiederherstellungsprotokoll auf. Mithilfe des Wiederherstellungsprotokolls kann sichergestellt werden, dass ein Fehler nicht zu einem inkonsistenten Zustand der Datenbank führt. Das Wiederherstellungsprotokoll wird außerdem dazu verwendet, die Konsistenz über Startoperationen des Servers hinweg zu gewährleisten. Das Wiederherstellungsprotokoll umfasst die folgenden Protokolle:

  Aktive Protokolldatei
  : Mit diesem Protokoll werden aktuelle Transaktionen auf dem Server aufgezeichnet. Diese Informationen sind erforderlich, um den Server und die Datenbank nach einem Katastrophenfall zu starten.

  Protokollspiegel (optional)
  : Der Spiegel der aktiven Protokolldatei ist eine Kopie der aktiven Protokolldatei, die verwendet werden kann, wenn die aktiven Protokolldateien nicht gelesen werden können. Alle Änderungen, die an der aktiven Protokolldatei vorgenommen werden, werden auch in einen Protokollspiegel geschrieben. Sie können nur einen einzigen Spiegel der aktiven Protokolldatei konfigurieren.

  Archivprotokoll
  : Das Archivprotokoll enthält Kopien von geschlossenen Protokolldateien, die in der aktiven Protokolldatei enthalten waren. Das Archivprotokoll wird in Datenbanksicherungen eingeschlossen und für die Wiederherstellung der Serverdatenbank verwendet.

Archivprotokolldateien, die in eine Datenbanksicherung eingeschlossen werden, werden automatisch bereinigt, nachdem ein vollständiger Datenbankzyklus abgeschlossen ist. Im Archivprotokoll muss genügend Speicherbereich verfügbar sein, um die Protokolldateien für Datenbanksicherungen speichern zu können.

Archivübernahmeprotokoll (optional)
: Das Archivübernahmeprotokoll, das auch als sekundäres Archivprotokoll bezeichnet wird, ist das Verzeichnis, in dem der Server Archivprotokolldateien speichert, wenn das Archivprotokollverzeichnis voll ist.

Auf Maßnahmen basierende Datenverwaltung

In der IBM Spectrum Protect-Umgebung enthält eine *Maßnahme* für die Verwaltung des Datenschutzes Regeln, die festlegen, wie Clientdaten gespeichert und verwaltet werden. Der Hauptzweck einer Maßnahme ist die Implementierung der folgenden Datenverwaltungsziele:

- Steuerung, in welchem Speicherpool Clientdaten anfänglich gespeichert werden
- Definition von Aufbewahrungskriterien, die steuern, wie viele Kopien von Objekten gespeichert werden
- Definition der Aufbewahrungsdauer der Objektkopien

Die auf Maßnahmen basierende Datenverwaltung ermöglicht es Ihnen, den Fokus statt auf die Verwaltung von Speichereinheiten und -medien auf Geschäftsanforderungen für den Schutz von Daten zu richten. Administratoren definieren Maßnahmen und ordnen Clientknoten einer *Maßnahmendomäne* zu.

Abhängig von Ihren Geschäftsanforderungen können eine oder mehrere Maßnahmen vorhanden sein. Beispielsweise können in einem Unternehmen verschiedene Abteilungen mit unterschiedlichen Typen von Daten angepasste Speicherverwaltungspläne haben. Maßnahmen können aktualisiert werden und die Aktualisierungen können auf bereits verwaltete Daten angewendet werden.

Wenn Sie IBM Spectrum Protect installieren, ist bereits eine Standardmaßnahme mit dem Namen STANDARD definiert. Die Maßnahme STANDARD stellt grundlegenden Sicherungsschutz für Benutzerworkstations bereit. Um unterschiedliche Service-Levels für unterschiedliche Clients bereitzustellen, können Sie die Standardmaßnahme ergänzen oder eine neue Maßnahme erstellen.

Sie erstellen Maßnahmen, indem Sie die folgenden Maßnahmenkomponenten definieren:

Maßnahmendomäne
: Die Maßnahmendomäne ist die primäre Organisationsmethode zur Gruppierung von Clientknoten, die allgemeine Regeln für die Datenverwaltung gemeinsam nutzen. Obwohl ein Clientknoten für mehr als einen Server definiert werden kann, kann der Clientknoten nur für eine einzige Maßnahmendomäne auf jedem Server definiert werden.

Maßnahmengruppe
: Eine *Maßnahmengruppe* umfasst eine Reihe von Maßnahmen, die in einer Gruppe zusammengefasst sind, sodass die Maßnahme für die Clientknoten in der Domäne nach Bedarf aktiviert oder inaktiviert werden kann. Ein Administrator verwendet eine Maßnahmengruppe, um unterschiedliche Verwaltungsklassen auf der Basis von Geschäfts- und Benutzeranforderungen zu implementieren. Eine Maßnahmendomäne kann mehrere Maßnahmengruppen enthalten, in der Domäne kann jedoch jeweils nur eine einzige Maßnahmengruppe aktiv sein. Jede Maßnahmengruppe enthält eine Standardverwaltungsklasse und eine beliebige Anzahl weiterer Verwaltungsklassen.

Verwaltungsklasse
: Eine *Verwaltungsklasse* ist ein Maßnahmenobjekt, das Sie an eine beliebige Kategorie von Daten binden können, um anzugeben, wie der Server die Daten verwaltet. Es können eine oder mehrere Verwaltungsklassen vorhanden sein. Eine der Verwaltungsklassen wird als Standardverwaltungsklasse festgelegt, die von Clients verwendet wird, es sei denn, für den Client ist eine bestimmte Verwaltungsklasse festgelegt, die den Standardwert überschreibt.

  Die Verwaltungsklasse kann eine Sicherungskopiengruppe, eine Archivierungskopiengruppe und Speicherverwaltungsattribute enthalten. Eine Kopiengruppe legt fest, wie der Server Sicherungsversionen oder archivierte Kopien der Datei verwaltet. Die Speicherverwaltungsattribute legen fest, ob die Datei für die Umlagerung in Serverspeicher vom Client für das Speicherplatzmanagement auswählbar ist, und unter welchen Bedingungen die Datei umgelagert wird.

Kopiengruppe
: Eine *Kopiengruppe* ist eine Gruppe von Attributen in einer Verwaltungsklasse, die die Folgendes steuert:

  - Wo der Server Versionen von gesicherten Dateien oder Archivierungskopien speichert
  - Wie lange der Server Versionen von gesicherten Dateien oder Archivierungskopien aufbewahrt
  - Wie viele Versionen von Sicherungskopien aufbewahrt werden
  - Welche Methode zum Generieren der Versionen von gesicherten Dateien oder Archivierungskopien verwendet werden soll

Sicherheitsmanagement

IBM Spectrum Protect umfasst Sicherheitsfunktionen für die Registrierung von Administratoren und Benutzern. Nachdem Administratoren registriert wurden, muss ihnen Berechtigung erteilt werden, indem ihnen eine oder mehrere Berechtigungsklassen für Verwaltungsaufgaben zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Serverfunktion ausführen. Administratoren mit Maßnahmen-, Speicher-, Bediener- oder Knotenberechtigung können Untergruppen von Serverfunktionen ausführen. Der Zugriff auf den Server kann mithilfe jeder der folgenden Methoden, die jeweils über ein Kennwort gesteuert werden, erfolgen:

- Administratorzugriff zum Verwalten des Servers
- Clientzugriff auf Knoten zum Speichern und Abrufen von Daten

Außerdem stehen Funktionen zur Verfügung, die dazu beitragen können, die Sicherheit zu gewährleisten, wenn Clients eine Verbindung zum Server herstellen. Abhängig von Geschäftsanforderungen können Sie als Administrator eine der folgenden Clientregistrierungsmethoden auswählen:

Offene Registrierung
: Wenn der Client zum ersten Mal die Verbindung zum Server herstellt, wird der Benutzer zur Eingabe eines Knotennamens, eines Kennworts und der Kontaktinformationen aufgefordert. Bei der offenen Registrierung werden dem Benutzer die folgenden Standardeinstellungen zur Verfügung gestellt:

  - Der Clientknoten ist der Maßnahmendomäne STANDARD zugeordnet.
  - Der Benutzer kann definieren, ob Dateien komprimiert werden, um das über Netze gesendete Datenvolumen und den von den Daten im Speicher belegten Speicherbereich zu reduzieren.
  - Der Benutzer kann archivierte Kopien von Dateien aus Serverspeicher löschen, aber keine Sicherungsversionen von Dateien.

Geschlossene Registrierung
: Die geschlossene Registrierung ist die Standardmethode für die Registrierung des Clients beim Server. Bei diesem Typ von Registrierung werden alle Clients von einem Administrator registriert. Der Administrator kann die folgenden Einstellungen implementieren:

  - Zuordnung des Knotens zu einer beliebigen Maßnahmendomäne
  - Festlegung, ob der Benutzer die Komprimierung verwenden kann oder nicht oder ob der Benutzer die Wahl hat
  - Steuerung, ob der Benutzer gesicherte Dateien oder archivierte Dateien löschen kann

Sie können weiteren Schutz für Ihre Daten und Kennwörter hinzufügen, indem Sie Secure Sockets Layer (SSL) verwenden. SSL ist die Standardtechnologie, mit der verschlüsselte Sitzungen für Server und Clients erstellt werden; SSL stellt einen sicheren Kanal für die Kommunikation über offene Kommunikationspfade zur Verfügung. Bei SSL wird die Identität des Servers mithilfe digitaler Zertifikate geprüft. Wenn die Authentifizierung mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) erfolgt, werden Kennwörter zwischen dem Server und dem LDAP-Server durch TLS (Transport Layer Security) geschützt. Das TLS-Protokoll ist der Nachfolger des SSL-Protokolls. Bei der Kommunikation zwischen einem Server und einem Client wird mithilfe von TLS sichergestellt, dass Nachrichten nicht von Dritten abgefangen werden können.

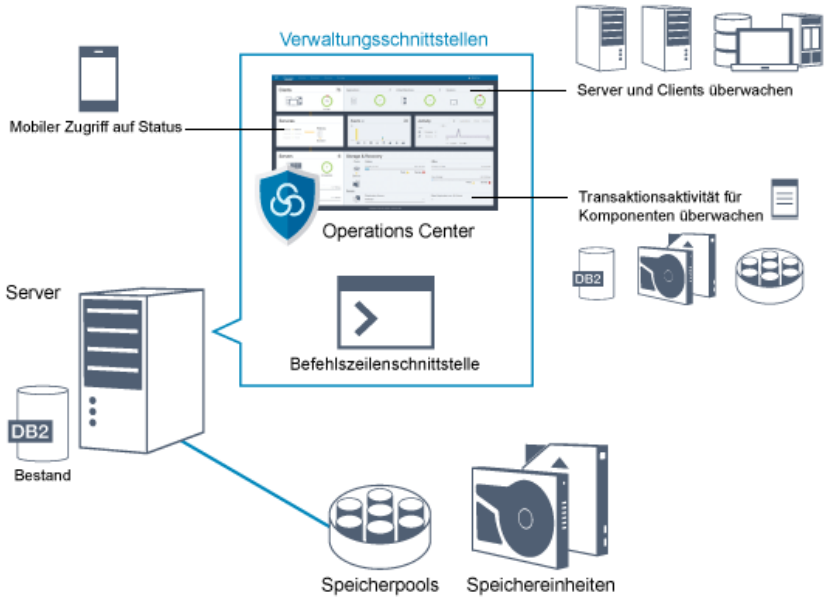
Benutzerschnittstellen für die IBM Spectrum Protect-Umgebung

Für Überwachungs- und Konfigurationstasks stellt IBM Spectrum Protect verschiedene Schnittstellen, einschließlich des Operations Center, einer Befehlszeilenschnittstelle und einer SQL-Verwaltungsschnittstelle, bereit.

Schnittstellen für die Datenspeicherverwaltung

Das Operations Center ist die primäre Schnittstelle für Administratoren zur Überwachung und Verwaltung von Servern. Ein Hauptvorteil des Operations Center ist die Möglichkeit, mehrere Server überwachen zu können (siehe Abbildung 1). Sie können IBM Spectrum Protect auch über eine Befehlszeilenverwaltungsschnittstelle überwachen und verwalten.

Abbildung 1. Benutzerschnittstellen für die Datenspeicherverwaltung



Für die Interaktion mit IBM Spectrum Protect können Sie die folgenden Schnittstellen verwenden:

Operations Center
: Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie Überwachungstasks und bestimmte Verwaltungstasks ausführen, wie beispielsweise:

- Überwachung mehrerer Server und Clients
- Überwachung der Transaktionsaktivität für bestimmte Komponenten im Datenpfad, wie beispielsweise die Serverdatenbank, das Wiederherstellungsprotokoll, Speichereinheiten und Speicherpools

Befehlszeilenschnittstelle
: Mithilfe einer Befehlszeilenschnittstelle können Sie Verwaltungstasks für Server ausführen. Der Zugriff auf die Befehlszeilenschnittstelle kann entweder über den IBM Spectrum Protect-Verwaltungsclient oder das Operations Center erfolgen.

Zugriff auf Informationen in der Serverdatenbank mithilfe von SQL-Anweisungen
: Mithilfe von SQL-Anweisungen SELECT können Sie die Serverdatenbank abfragen und die Ergebnisse anzeigen. SQL-Tools anderer Anbieter sind verfügbar, um Administratoren bei der Datenbankverwaltung zu unterstützen.

Schnittstellen für die Verwaltung der Clientaktivität

IBM Spectrum Protect stellt die folgenden Typen von Schnittstellen zur Verwaltung der Clientaktivität bereit:

- Anwendungsprogrammierschnittstelle (API)
- Grafische Benutzerschnittstellen für Clients
- Browserschnittstelle für den Client für Sichern/Archivieren
- Befehlszeilenschnittstellen für Clients

Konzepte der Datenspeicherung in IBM Spectrum Protect

IBM Spectrum Protect stellt Funktionen zum Speichern von Daten in Einheitenspeicher und externem Speicher bereit.

Um dem Server Speichereinheiten zur Verfügung zu stellen, müssen Sie die Speichereinheiten anschließen und Speicherpools Einheitenklassen, Speicherarchiven und Laufwerken zuordnen.

- Typen von Speichereinheiten
  Zur Erreichung bestimmter Datenschutzziele können verschiedene Speichereinheiten in IBM Spectrum Protect verwendet werden.
- Datenspeicherung in Speicherpools
  Logische Speicherpools sind die Hauptkomponenten im IBM Spectrum Protect-Modell der Datenspeicherung. Die Verwendung von Speichereinheiten kann optimiert werden, indem die Merkmale von Speicherpools und Datenträgern bearbeitet werden.
- Datenübertragung über Netze in Speicher
  Die IBM Spectrum Protect-Umgebung bietet verschiedene Möglichkeiten, um Daten über verschiedene Typen von Netzen und Konfigurationen sicher in Speicher zu versetzen.

Typen von Speichereinheiten

Zur Erreichung bestimmter Datenschutzziele können verschiedene Speichereinheiten in IBM Spectrum Protect verwendet werden.

Speichereinheiten und Speicherobjekte

Der IBM Spectrum Protect-Server kann mit einer Kombination aus manuellen und automatisierten Speichereinheiten verbunden werden. IBM Spectrum Protect kann mit den folgenden Typen von Speichereinheiten verbunden werden:

- Platteneinheiten, die direkt angeschlossen, an ein SAN angeschlossen oder an ein Netz angeschlossen sind
- Physische Bandeinheiten, die manuell oder automatisch betrieben werden
- Virtuelle Bandeinheiten
- Cloudobjektspeicher

IBM Spectrum Protect stellt physische Speichereinheiten und Datenträger durch Speicherobjekte dar, die Sie in der Serverdatenbank definieren. Speicherobjekte klassifizieren verfügbare Speicherressourcen und handhaben die Umlagerung von einem Speicherpool in einen anderen. In Tabelle 1 sind die Speicherobjekte in der Serverspeicherumgebung beschrieben.

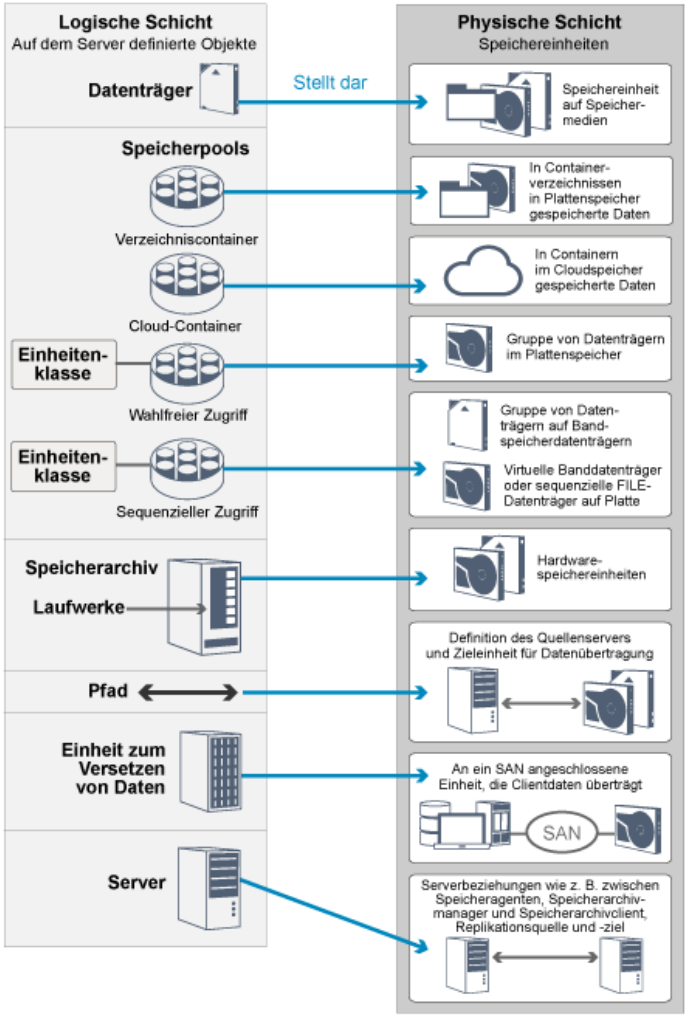
Tabelle 1. Speicherobjekte und Darstellungen

Speicherobjekt	**Durch das Objekt dargestellte Ressource**
Datenträger	Eine diskrete Speichereinheit auf Platte, Band oder anderen Speichermedien. Jeder Datenträger ist einem einzelnen Speicherpool zugeordnet.

Speicherobjekt	Durch das Objekt dargestellte Ressource
Speicherpool	Eine Gruppe von Speicherdatenträgern oder Containern, die als Ziel zum Speichern von Clientdaten dient. IBM Spectrum Protect verwendet die folgenden Typen von Speicherpools: • Verzeichniscontainerspeicherpools • Cloud-Containerspeicherpools • Speicherpools mit sequenziellem Zugriff, die einer Einheitenklasse zugeordnet sind • Speicherpools mit wahlfreiem Zugriff, die einer Einheitenklasse zugeordnet sind
Container	Eine Datenspeicherposition, beispielsweise eine Datei, ein Verzeichnis oder eine Einheit.
Containerspeicherpool	Ein primärer Speicherpool, der von einem Server zum Speichern von Daten verwendet wird. Daten werden in Containern in Dateisystemverzeichnissen oder in Cloudspeicher gespeichert. Daten werden, falls erforderlich, dedupliziert, während der Server Daten in den Speicherpool schreibt.
Einheitenklasse	Der Typ der Speichereinheit, der die Datenträger verwenden kann, die in einem Speicherpool mit sequenziellem Zugriff oder einem Speicherpool mit wahlfreiem Zugriff definiert sind. Jede Einheitenklasse für Typen austauschbarer Datenträger ist einem einzelnen Speicherarchiv zugeordnet.
Speicherarchiv	Eine Speichereinheit. Beispielsweise kann ein Speicherarchiv ein Standalone-Laufwerk, eine Gruppe von Standalone-Laufwerken, eine automatisierte Einheit mit mehreren Laufwerken oder eine Gruppe von Laufwerken darstellen, die durch einen Datenträgermanager gesteuert wird.
Laufwerk	Ein Objekt einer Bandarchiveinheit, die die Funktionalität zum Lesen und Schreiben von Daten von bzw. auf Bandarchivdatenträger bereitstellt. Jedes Laufwerk ist einem einzelnen Speicherarchiv zugeordnet.
Pfad	Die Angabe der Datenquelle und der Zielposition der Einheit. Bevor eine Speichereinheit verwendet werden kann, muss ein Pfad zwischen der Einheit und dem Quellenserver, der Daten versetzt, definiert werden.
Einheit zum Versetzen von Daten	Eine an ein SAN angeschlossene Einheit, die zur Übertragung von Clientdaten verwendet wird. Eine Einheit zum Versetzen von Daten wird nur bei einer Datenübertragung verwendet, bei der der Server nicht vorhanden ist, wie beispielsweise in einer NDMP-Umgebung. Einheiten zum Versetzen von Daten übertragen Daten zwischen Speichereinheiten, ohne viele Server-, Client- oder Netzressourcen zu verwenden.
Server	Ein Server, der von einem anderen IBM Spectrum Protect-Server verwaltet wird.

Der Administrator definiert die Speicherobjekte in der logischen Schicht des Servers (siehe Abbildung 1).

Abbildung 1. Speicherobjekte



Platteneinheiten

Sie können Clientdaten auf Platteneinheiten mit den folgenden Datenträgertypen speichern:

- Verzeichnisse in Verzeichniscontainerspeicherpools
- Datenträger mit wahlfreiem Zugriff des Einheitentyps DISK
- Datenträger mit sequenziellem Zugriff des Einheitentyps FILE

IBM Spectrum Protect stellt die folgenden Funktionen bereit, wenn Sie Verzeichniscontainerspeicherpools für die Datenspeicherung verwenden:

- Datendeduplizierungs- und Plattencachingverfahren können angewendet werden, um die Datenspeichernutzung zu maximieren.
- Daten können sehr viel schneller von Platte als aus Bandspeicher abgerufen werden.

Physische Bandeinheiten

In einem physischen Bandarchiv wird die Speicherkapazität als Gesamtzahl Datenträger in dem Speicherarchiv definiert. Physische Bandeinheiten können für die folgenden Aktivitäten verwendet werden:

- Speichern von Clientdaten, die von Clientknoten gesichert, archiviert oder umgelagert werden.
- Speichern von Datenbanksicherungen
- Exportieren von Daten auf einen anderen Server oder in Speicher an einem anderen Standort

Das Versetzen von Daten auf Band bietet die folgenden Vorteile:

- Daten für Clients können auf einer Platteneinheit verbleiben, während die Daten gleichzeitig auf Band versetzt werden.
- Die Leistung von Bandlaufwerken kann verbessert werden, indem Daten mittels Streaming von Platte auf Band umgelagert werden.
- Die Nutzungszeiten für Bandlaufwerke können verlängert werden, um die Effizienz der Bandlaufwerke zu verbessern.
- Daten auf Band können in Vaults an anderen Standorten versetzt werden.
- Der Stromverbrauch kann eingeschränkt werden, da Bandeinheiten nach dem Schreiben von Daten auf Band keinen Strom mehr verbrauchen.
- Verschlüsselung, die von der Bandlaufwerkhardware bereitgestellt wird, kann angewendet werden, um die Daten auf Band zu schützen.

Verglichen mit entsprechendem Plattenspeicher und virtuellem Bandspeicher sind die Einheitenkosten zum Speichern von Daten bei physischen Bandeinheiten tendenziell sehr viel geringer.

Virtuelle Bandarchive

Ein virtuelles Bandarchiv (VTL) verwendet keine physischen Banddatenträger. Wenn Sie VTL-Speicher verwenden, werden die Zugriffsmechanismen von Bandhardware emuliert. In einem virtuellen Bandarchiv können Datenträger und Laufwerke definiert werden, um größere Flexibilität für die Speicherumgebung bereitzustellen. Die Speicherkapazität eines virtuellen Bandarchivs wird als insgesamt verfügbarer Plattenspeicherplatz definiert. Sie können die Anzahl und Größe der Datenträger auf der Platte erhöhen oder reduzieren.

Das Definieren eines virtuellen Bandarchivs für den IBM Spectrum Protect-Server kann zu einer Leistungsverbesserung führen, da der Server die Mountpunktverarbeitung für virtuelle Bandarchive anders als für reale Bandarchive handhabt. Obwohl die logischen Einschränkungen für Bandeinheiten weiterhin bestehen, gelten die physischen Einschränkungen für Bandhardware nicht für ein virtuelles Bandarchiv, das somit bessere Skalierbarkeit bietet. Sie können das virtuelle IBM Spectrum Protect-Bandarchiv verwenden, wenn die folgenden Bedingungen erfüllt sind:

- In dem virtuellen Bandarchiv wird nur ein einziger Typ und eine einzige Generation von Laufwerk und Datenträger emuliert.
- Jeder Server und jeder Speicheragent mit Zugriff auf das VTL hat Pfade, die für alle Laufwerke in dem Bandarchiv definiert sind.

Datenspeicherung in Speicherpools

Logische Speicherpools sind die Hauptkomponenten im IBM Spectrum Protect-Modell der Datenspeicherung. Die Verwendung von Speichereinheiten kann optimiert werden, indem die Merkmale von Speicherpools und Datenträgern bearbeitet werden.

Speicherpooltypen

Die Gruppe von Speicherpools, die Sie für den Server konfigurieren, wird als *Serverspeicher* bezeichnet. Im Serverspeicher können die folgenden Typen von Speicherpools definiert werden:

Primäre Speicherpools
: Eine benannte Gruppe von Datenträgern, die der Server zum Speichern von Sicherungsversionen von Dateien, Archivierungskopien von Dateien und Dateien, die aus Clientknoten umgelagert werden, verwendet.

Kopienspeicherpools
: Eine benannte Gruppe von Datenträgern, die Kopien von Dateien enthalten, die in primären Speicherpools gespeichert sind. Kopienspeicherpools werden nur zum Sichern der Daten verwendet, die in primären Speicherpools gespeichert sind. Ein Kopienspeicherpool kann nicht als Ziel für eine Sicherungskopiengruppe, eine Archivierungskopiengruppe oder eine Verwaltungsklasse für speicherverwaltete Dateien verwendet werden.

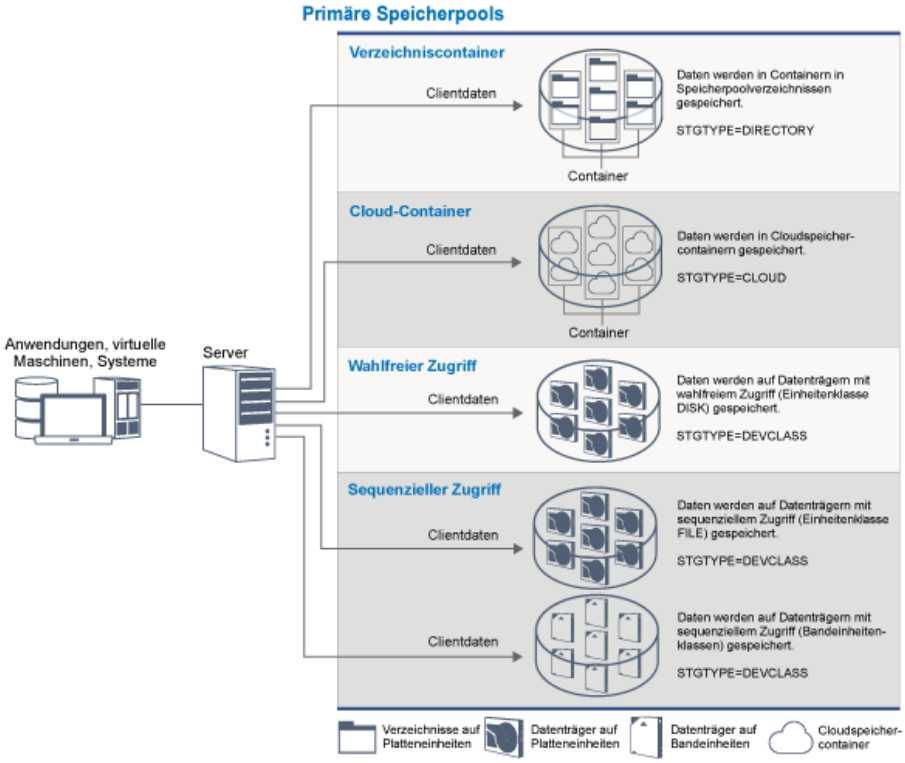
Containerkopienspeicherpools
: Eine benannte Gruppe von Datenträgern, die eine Kopie der Datenbereiche enthalten, die in Verzeichniscontainerspeicherpools gespeichert sind. Containerkopienspeicherpools werden nur zum Schützen der Daten verwendet, die in Verzeichniscontainerspeicherpools gespeichert sind.

Speicherpools für aktive Daten
: Eine benannte Gruppe von Speicherpooldatenträgern, die nur aktive Versionen von Clientsicherungsdaten enthalten.

Primäre Speicherpools

Wenn Sie Dateidaten zurückschreiben, abrufen, zurückrufen oder exportieren, wird die angeforderte Datei aus einem primären Speicherpool abgerufen. Abhängig vom Typ des primären Speicherpools können sich die Speicherpools vor Ort oder an einen anderen Standort befinden. Primäre Speicherpools können in einer Speicherhierarchie angeordnet werden, sodass Daten aus Plattenspeicher in kostengünstigeren Speicher, wie beispielsweise Bandeinheiten, übertragen werden können. Abbildung 1 zeigt das Konzept primärer Speicherpools.

Abbildung 1. Primäre Speicherpools



Sie können die folgenden Typen primärer Speicherpools definieren:

Verzeichniscontainerspeicherpools

Ein Speicherpool, den der Server zum Speichern von Daten in Containern in Speicherpoolverzeichnissen verwendet. Daten, die in einem Verzeichniscontainerspeicherpool gespeichert sind, können entweder die Inline-Datendeduplizierung, die clientseitige Datendeduplizierung, die Inline-Komprimierung oder die clientseitige Komprimierung verwenden. Bei der Inline-Datendeduplizierung und der Inline-Komprimierung erfolgt die Reduktion der Daten zu dem Zeitpunkt, zu dem sie gespeichert werden. Durch die Verwendung von Verzeichniscontainerspeicherpools entfällt die Notwendigkeit zur Datenträgerkonsolidierung, wodurch die Serverleistung verbessert und die Kosten der Speicherhardware reduziert werden. Daten in Verzeichniscontainerspeicherpools können auf der Ebene des Speicherpools geschützt und repariert werden.

Einschränkung: Folgende Funktionen können bei Verzeichniscontainerspeicherpools nicht verwendet werden:

- Umlagerung
- Konsolidierung
- Zusammenfassung
- Kollokation
- Gleichzeitiges Schreiben
- Speicherpoolsicherung
- Virtuelle Datenträger

Cloud-Containerspeicherpools

Ein Speicherpool, den ein Server zum Speichern von Daten in Cloudspeicher verwendet. Der Cloudspeicher kann sich vor Ort (on premises) oder außerhalb des Unternehmens (off premises) befinden. Bei Cloud-Containerspeicherpools, die von IBM Spectrum Protect bereitgestellt werden, können Daten in objektbasiertem Cloudspeicher gespeichert werden. Das Speichern von Daten in Cloud-Containerspeicherpools ermöglicht es Ihnen, die von Clouds gebotenen Vorteile der Kosten pro Einheit zusammen mit der vom Cloudspeicher bereitgestellten Skalierungsfunktionalität zu nutzen. IBM Spectrum Protect verwaltet die Berechtigungsnachweise, Sicherheit, Lese- und Schreib-E/As sowie den Lebenszyklus für Daten, die in der Cloud gespeichert werden. Wenn Cloud-Containerspeicherpools auf dem Server implementiert werden, können Daten direkt in die Cloud geschrieben werden, indem ein Cloud-Containerspeicherpool mit den Cloudberechtigungsnachweisen konfiguriert wird. Daten, die in einem Cloud-Containerspeicherpool gespeichert sind, können sowohl die Inline-Datendeduplizierung als auch die Inline-Komprimierung verwenden. Der Server schreibt deduplizierte und verschlüsselte Daten direkt in die Cloud. Sie können Daten direkt im Cloud-Containerspeicherpool sichern und aus ihm zurückschreiben oder direkt im Cloud-Containerspeicherpool archivieren und aus ihm abrufen.

Sie können die folgenden Typen von Cloud-Containerspeicherpools definieren:

On premises
: Sie können den On-Premises-Typ für Cloud-Containerspeicherpools verwenden, um Daten in einer privaten Cloud zu speichern, um mehr Sicherheit und maximale Kontrolle über Ihre Daten zu gewährleisten. Die Nachteile einer privaten Cloud sind höhere Kosten aufgrund der Hardwarevoraussetzungen und der Wartung vor Ort.

Off premises

Sie können den Off-Premises-Typ für Cloud-Containerspeicherpools verwenden, um Daten in einer öffentlichen Cloud zu speichern. Die Verwendung einer öffentlichen Cloud hat den Vorteil, dass die Kosten geringer sind als bei einer privaten Cloud, da beispielsweise die Wartung entfällt. Sie müssen jedoch diesen Vorteil und mögliche Leistungsprobleme aufgrund von Verbindungsgeschwindigkeiten und eingeschränkter Kontrolle über Ihre Daten gegeneinander abwägen.

Speicherpools, die Einheitenklassen zugeordnet sind

Sie können einen primären Speicherpool für die Verwendung der folgenden Typen von Speichereinheiten definieren:

Einheitenklasse DISK

In einem Speicherpool des Einheitentyps DISK werden Daten in Plattenblöcken mit wahlfreiem Zugriff gespeichert. Sie können Caching in DISK-Speicherpools verwenden, um die Clientzurückschreibungsleistung - mit einigen Einschränkungen bei der Serververarbeitung - zu verbessern. Die Speicherbereichszuordnung und -überwachung nach Blöcken verwendet mehr Datenbankspeicherbereich und erfordert eine höhere Verarbeitungsleistung als die Zuordnung und Überwachung nach Datenträger.

Einheitenklasse FILE

In einem Speicherpool des Einheitentyps FILE werden Dateien auf sequenziellen Datenträgern gespeichert, da hierbei die sequenzielle Leistung besser als bei der Speicherung in Plattenblöcken ist. Für den Server haben diese Dateien die Merkmale eines Banddatenträgers, sodass dieser Typ von Speicherpool für die Umlagerung auf Band besser geeignet ist. FILE-Datenträger sind für das *elektronische Vaulting* geeignet, bei dem ein Band nicht physisch an einen fernen Standort transportiert wird, sondern Daten elektronisch an einen fernen Standort übertragen werden. Im Allgemeinen wird dieser Typ von Speicherpool gegenüber DISK-Speicherpools bevorzugt.

Der Server verwendet die folgenden primären Standardspeicherpools mit wahlfreiem Zugriff:

ARCHIVEPOOL

In der Maßnahme STANDARD ist dieser Speicherpool das Ziel für Dateien, die von Clientknoten archiviert werden.

BACKUPPOOL

In der Maßnahme STANDARD ist dieser Speicherpool das Ziel für Dateien, die von Clientknoten gesichert werden.

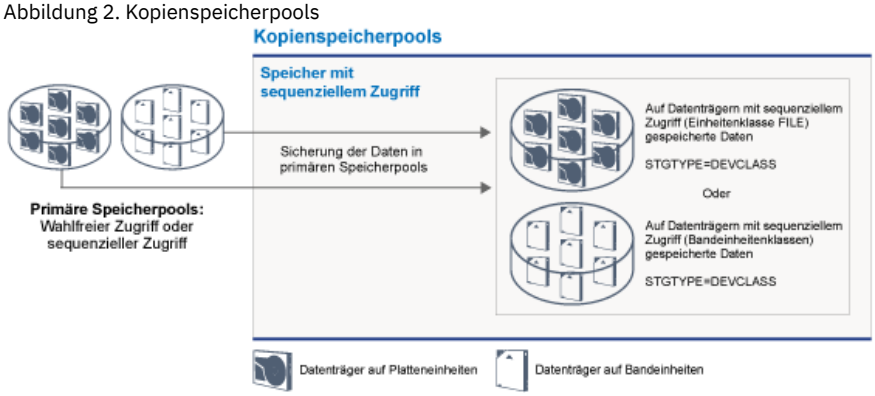
SPACEMGPOOL

Dieser Speicherpool ist für speicherverwaltete Dateien, die von IBM Spectrum Protect for Space Management-Clientknoten umgelagert werden.

Kopienspeicherpools

Kopienspeicherpools enthalten aktive und inaktive Versionen von Daten, die aus primären Speicherpools gesichert werden. Ein Verzeichniscontainerspeicherpool kann nicht als Kopienspeicherpool verwendet werden. Außerdem können Daten aus einem Verzeichniscontainerspeicherpool nicht in einen Kopienspeicherpool kopiert werden. Um Verzeichniscontainerspeicherpools zu schützen, kopieren Sie die Daten in einen Containerkopienspeicherpool. Abbildung 2 zeigt das Konzept von Kopienspeicherpools.

Abbildung 2. Kopienspeicherpools



Kopienspeicherpools dienen der Wiederherstellung nach einem Katastrophenfall oder nach Datenträgerfehlern. Wenn beispielsweise ein Client versucht, eine beschädigte Datei aus dem primären Speicherpool abzurufen, kann der Client die Daten aus dem Kopienspeicherpool zurückschreiben.

Die Datenträger in Kopienspeicherpools können ausgelagert und dennoch weiterhin vom Server verfolgt werden. Die Auslagerung dieser Datenträger ermöglicht die Wiederherstellung nach einem Katastrophenfall vor Ort. Ein Kopienspeicherpool kann nur Speicher mit sequenziellem Zugriff, wie beispielsweise eine Bandeinheitenklasse oder eine Einheitenklasse FILE, verwenden.

Containerkopienspeicherpools

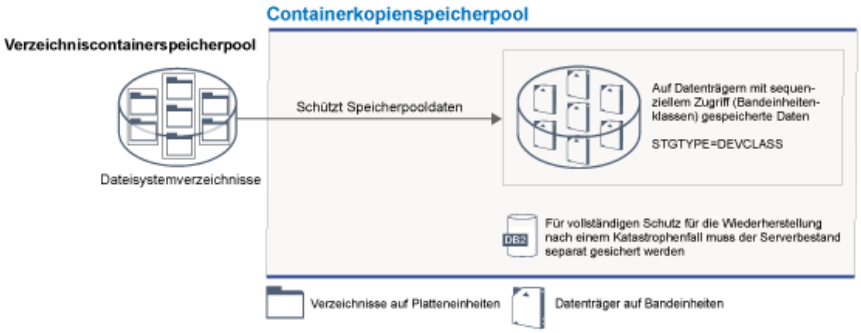
Ein Server kann einen Verzeichniscontainerspeicherpool schützen, indem er Kopien der Daten in einem Containerkopienspeicherpool speichert. Daten in Containerkopienspeicherpools werden auf Banddatenträgern gespeichert, die vor Ort oder an einem anderen Standort aufbewahrt werden können. Beschädigte Daten in Verzeichniscontainerspeicherpools können mithilfe dedupizierter Speicherbereiche in Containerkopienspeicherpools repariert werden. Containerkopienspeicherpools stellen eine Alternative zur Verwendung eines Replikationsservers zum Schützen von Daten in einem Verzeichniscontainerspeicherpool dar.

Einschränkung: Wenn alle Serverdaten verloren gehen, stellen Containerkopienspeicherpools alleine nicht dieselbe Schutzstufe wie die Replikation bereit:

- Bei der Replikation können Sie Clientdaten direkt vom Zielserver zurückschreiben, wenn der Quellenserver nicht verfügbar ist.
- Bei Containerkopienspeicherpools müssen Sie zunächst den Server aus einer Datenbanksicherung zurückschreiben und dann die Verzeichniscontainerspeicherpools mithilfe von Banddatenträgern reparieren.

Abbildung 3 zeigt das Konzept von Containerkopienspeicherpools.

Abbildung 3. Containerkopienspeicherpools



Abhängig von Ihrer Systemkonfiguration können Sie Zeitpläne für den Schutz erstellen, um gemäß Ihren Anforderungen die Daten im Verzeichniscontainerspeicherpool gleichzeitig in Containerkopienspeicherpools vor Ort oder an einem anderen Standort zu kopieren:

- Wenn die Replikation aktiviert ist, können Sie einen einzelnen Containerkopienpool an einem anderen Standort erstellen. Mithilfe der Kopie an dem anderen Standort kann zusätzlicher Schutz in einer replizierten Umgebung bereitgestellt werden.
- Wenn die Replikation nicht aktiviert ist, können Sie einen einzelnen Speicherpool vor Ort und einen einzelnen Speicherpool an einem anderen Standort erstellen.

Abhängig von den Ressourcen und Anforderungen Ihres Standorts bietet die Möglichkeit, Verzeichniscontainerspeicherpools auf Band zu kopieren, die folgenden Vorteile:

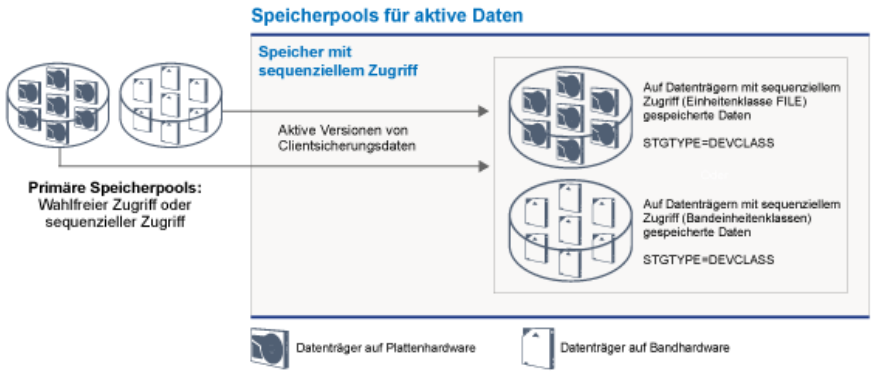
- Die Notwendigkeit, einen weiteren Server und weiteren Plattenspeicherplatz verwalten zu müssen, entfällt.
- Daten werden in Speicherpools kopiert, die auf dem Server definiert sind. Die Leistung ist nicht von der Netzverbindung zwischen Servern abhängig oder von ihr betroffen.
- Sie können gesetzliche Bestimmungen und Geschäftsanforderungen für Bandkopien an einem anderen Standort erfüllen.

Speicherpools für aktive Daten

Ein Pool für aktive Daten enthält nur aktive Versionen von Clientsicherungsdaten. In diesem Fall muss der Server keine Positionierung hinter inaktive Dateien ausführen, die nicht zurückgeschrieben werden müssen. Ein Verzeichniscontainerspeicherpool kann nicht als Speicherpool für aktive Daten verwendet werden. Pools für aktive Daten werden verwendet, um die Effizienz von Datenspeicher- und Zurückschreibungsoperationen zu verbessern; beispielsweise kann Sie dieser Typ von Speicherpool beim Erreichen der folgenden Ziele unterstützen:

- Erhöhen der Geschwindigkeit von Zurückschreibungsoperationen für Clientdaten
- Reduzieren der Anzahl Speicherdatenträger vor Ort oder an einem anderen Standort
- Reduzieren des Datenvolumens, das beim Kopieren oder Zurückschreiben von Dateien übertragen wird, die durch elektronisches Vaulting an einem fernen Standort geschützt werden.

Daten, die von Clients für die hierarchische Speicherverwaltung (HSM-Clients) umgelagert werden, und Archivierungsdaten sind in Pools für aktive Daten nicht zulässig. Während aktualisierte Versionen von Sicherungsdaten in Pools für aktive Daten gespeichert werden, werden ältere Versionen entfernt, da die verbleibenden Daten von einer großen Anzahl Datenträger mit sequenziellem Zugriff auf einer geringeren Anzahl neuer Datenträger mit sequenziellem Zugriff konsolidiert werden. Abbildung 4 zeigt das Konzepts von Speicherpools für aktive Daten.
Abbildung 4. Speicherpools für aktive Daten



Pools für aktive Daten können jeden Typ von Speicher mit sequenziellem Zugriff verwenden. Die Vorteile eines Pools für aktive Daten sind jedoch von dem Einheitentyp abhängig, der dem Pool zugeordnet ist. Beispielsweise sind Pools für aktive Daten, die einer Einheitenklasse FILE zugeordnet sind, aus den folgenden Gründen bestens für Clientschnellzurückschreibungsoperationen geeignet:

- FILE-Datenträger müssen nicht physisch bereitgestellt werden.
- Clientsitzungen, die Daten von FILE-Datenträgern in einen Pool für aktive Daten zurückschreiben, können gleichzeitig auf die Datenträger zugreifen, wodurch die Zurückschreibungsleistung verbessert wird.

Zugehörige Informationen:
Häufig gestellte Fragen (FAQs) zu Verzeichniscontainerspeicherpools
Häufig gestellte Fragen (FAQs) zu Cloud-Containerspeicherpools

Datenübertragung über Netze in Speicher

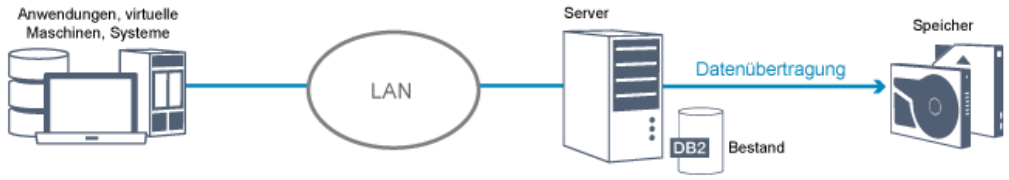
Die IBM Spectrum Protect-Umgebung bietet verschiedene Möglichkeiten, um Daten über verschiedene Typen von Netzen und Konfigurationen sicher in Speicher zu versetzen.

Netzkonfigurationen für Speichereinheiten

IBM Spectrum Protect stellt Methoden zur Konfiguration von Clients und Servern in einem lokalen Netz (LAN = Local Area Network), in einem Speicherbereichsnetz (SAN = Storage Area Network), für die LAN-unabhängige Datenversetzung und als Network-attached Storage (NAS) bereit.

Datensicherungsoperationen über ein LAN

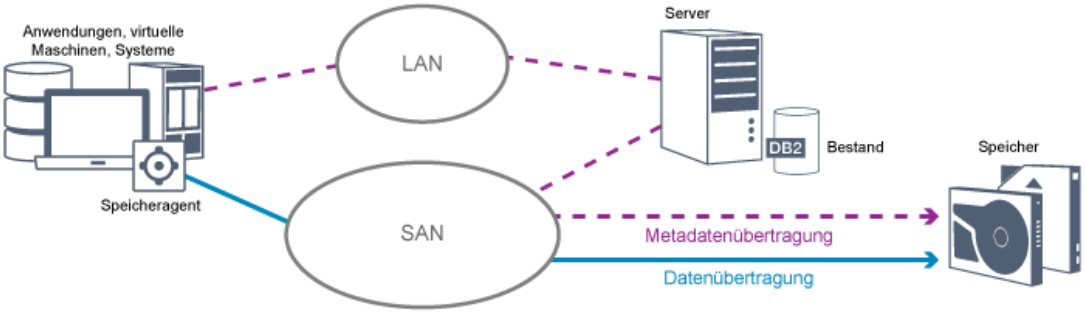
Abbildung 1 zeigt den Datenpfad für IBM Spectrum Protect-Sicherungsoperationen über ein LAN.
Abbildung 1. IBM Spectrum Protect-Sicherungsoperationen über ein LAN



In einer LAN-Konfiguration sind einem einzelnen IBM Spectrum Protect-Server ein oder mehrere Bandarchive zugeordnet. Bei diesem Typ von Konfiguration müssen Clientdaten, E-Mails, Terminalverbindung, Anwendungsprogramm und Einheitensteuerinformationen alle von demselben Netz gehandhabt werden. Einheitensteuerinformationen und Clientsicherungs- und -zurückschreibungsdaten fließen über das LAN.

Datensicherungsoperationen über ein SAN

Abbildung 2 zeigt den Datenpfad für IBM Spectrum Protect-Sicherungsoperationen über ein SAN.
Abbildung 2. IBM Spectrum Protect-Sicherungsoperationen über ein SAN



Ein Speicherbereichsnetz (SAN) ist ein dediziertes Speichernetz, das die Systemleistung verbessern kann. In einem SAN können Sie Speicher konsolidieren und die bei lokalen Netzen (LANs) und Weitverkehrsnetzen (WANs) bestehenden Einschränkungen in Bezug auf Entfernung, Skalierbarkeit und Bandbreite verringern. Die Verwendung von IBM Spectrum Protect in einem SAN ermöglicht Ihnen die Nutzung der Vorteile der folgenden Funktionen:

- Gemeinsame Nutzung von Speichereinheiten durch mehrere IBM Spectrum Protect-Server. Dies schließt keine Einheiten ein, die den Einheitentyp GENERICTAPE verwenden.
- Versetzen von Daten von einem Clientsystem direkt in Speichereinheiten ohne Verwendung des LAN. Die LAN-unabhängige Datenversetzung erfordert die Installation eines Speicheragenten auf dem Clientsystem. Der Speicheragent ist zusammen mit dem Produkt IBM Spectrum Protect for SAN verfügbar.

  Über den Speicheragenten kann der Client Daten direkt in einem Bandarchiv oder einem gemeinsam genutzten Dateisystem, wie beispielsweise GPFS, sichern und aus ihm zurückzuschreiben. Der IBM Spectrum Protect-Server verwaltet die Serverdatenbank und das Wiederherstellungsprotokoll und fungiert als Speicherarchivmanager, um Einheitenoperationen zu steuern. Der Speicheragent auf dem Client handhabt die Datenübertragung zu der Einheit auf dem SAN. Diese Implementierung gibt Bandbreite im LAN frei, die andernfalls für das Versetzen von Clientdaten verwendet würde.

- Gemeinsame Nutzung von Bandlaufwerken und Speicherarchiven, die vom IBM Spectrum Protect-Server unterstützt werden.
- Konsolidierung mehrerer Clients unter einem einzelnen Clientknotennamen in einem GPFS-Cluster (GPFS = General Parallel File System).

Network-attached Storage (NAS)

Bei NAS-Dateiservern handelt es sich um Server mit dediziertem Speicher, deren Betriebssysteme für Dateiservicefunktionen optimiert sind. . NAS-Dateiserver interagieren in der Regel mit IBM Spectrum Protect über standardisierte Netzprotokolle, wie beispielsweise Network Data Management Protocol (NDMP), oder als primärer Speicher für Speicherpools mit wahlfreiem oder sequenziellem Zugriff. IBM Spectrum Protect stellt die folgenden Basistypen von Konfigurationen bereit, die NDMP zum Sichern und Verwalten von NAS-Dateiservern verwenden:

- IBM Spectrum Protect sichert einen NAS-Dateiserver auf einer Speicherarchiveinheit, die direkt an den NAS-Dateiserver angeschlossen ist. Der NAS-Dateiserver, der remote an den IBM Spectrum Protect-Server angeschlossen sein kann, überträgt Sicherungsdaten direkt an ein Laufwerk in einem Bandarchiv, das über SCSI angeschlossen ist. Daten werden in NDMP-formatierten Speicherpools gespeichert; diese können auf Speichermedien gesichert werden, die zum Schutz vor einem Katastrophenfall vor Ort ausgelagert werden können.
- IBM Spectrum Protect sichert einen NAS-Dateiserver über das LAN in einer Speicherpoolhierarchie. Bei diesem Typ von Konfiguration können Sie NAS-Daten direkt auf Platte mit wahlfreiem Zugriff oder sequenziellem Zugriff speichern und die Daten dann auf Band umlagern. Sie können diesen Typ von Konfiguration auch für die Systemreplikation verwenden. Daten können auch auf Speichermedien gesichert werden, die ausgelagert werden können. Der Vorteil dieses Konfigurationstyps besteht darin, dass Ihnen alle Datenverwaltungsfunktionen, die für eine Speicherpoolhierarchie gelten, zur Verfügung stehen.
- Der IBM Spectrum Protect-Client liest die Daten mithilfe des NFS- oder CIFS-Protokolls aus dem NAS-System und sendet die Daten zum Speichern an den Server.

Speicherverwaltung

Die Verwaltung der Einheiten und Datenträger, die zum Speichern von Clientdaten verwendet werden, erfolgt über den IBM Spectrum Protect-Server. Der Server integriert die Speicherverwaltung in die Maßnahmen, die Sie für die Verwaltung von Clientdaten in den folgenden Bereichen definieren:

Typen von Einheiten für Serverspeicher

IBM Spectrum Protect ermöglicht Ihnen die Verwendung von direkt angeschlossenen Einheiten und NAS-Einheiten für Serverspeicher. IBM Spectrum Protect stellt physische Speichereinheiten und Datenträger durch vom Administrator definierte Speicherobjekte dar.

Datenumlagerung über die Speicherhierarchie

Bei primären Speicherpools, die keine Verzeichniscontainerspeicherpools sind, können Sie die Speicherpools in einer oder mehreren hierarchischen Strukturen zusammenfassen. Diese Speicherhierarchie bietet Flexibilität in vielerlei Hinsicht. Sie können beispielsweise eine Maßnahme definieren, um Daten für schnellere Sicherungsoperationen auf Platten zu sichern. Der IBM Spectrum Protect-Server kann dann automatisch Daten von Platte auf Band umlagern.

Entfernen verfallener Daten

Die von Ihnen definierte Maßnahme steuert, wann Clientdaten auf dem IBM Spectrum Protect-Server automatisch verfallen. Zum Entfernen von Daten, die für den Verfall auswählbar sind, markiert ein Serververfallsprozess die Daten als verfallen und löscht die Metadaten für die verfallenen Daten aus der Datenbank. Der von den verfallenen Daten belegte Speicherbereich ist dann wieder für neue Daten verfügbar. Sie können die Häufigkeit des Verfallsprozesses über eine Serveroption steuern.

Datenträgerwiederverwendung durch Konsolidierung

Da Daten aufgrund von Servermaßnahmen automatisch verfallen, nimmt der freie Speicherbereich auf den Datenträgern, auf denen die Daten gespeichert sind, ständig zu. Bei allen Speichermedien mit Ausnahme von Verzeichniscontainerspeicherpools und Plattenspeicherpools mit wahlfreiem Zugriff implementiert der IBM Spectrum Protect-Server die *Konsolidierung*, ein Prozess, bei dem Datenträger für die Wiederverwendung freigegeben werden, ohne dass die traditionelle Bandrotation angewendet wird. Bei der Konsolidierung wird ein Datenträger automatisch defragmentiert, indem nicht verfallene Daten auf anderen Datenträgern konsolidiert werden, wenn der freie Speicherbereich auf einem Datenträger einen definierten Stand erreicht. Der konsolidierte Datenträger kann dann vom Server erneut verwendet werden. Die Konsolidierung ermöglicht den automatischen Umlauf von Datenträgern im Speicherverwaltungsprozess und die Minimierung der Anzahl erforderlicher Datenträger.

Gesicherte Clientdaten konsolidieren

Durch das Gruppieren der Clientdaten, die gesichert werden, kann die Anzahl Datenträgermounts für eine Clientwiederherstellung auf ein Minimum reduziert werden. Der IBM Spectrum Protect-Server stellt die folgenden Methoden zum Gruppieren von Clientdateien in anderen Speichermedien als Verzeichniscontainerspeicherpools zur Verfügung:

Clientdaten kollokieren

Der IBM Spectrum Protect-Server kann Clientdaten *kollokieren*, das heißt, er kann Clientdaten auf einigen wenigen Datenträgern speichern, anstatt sie über viele Datenträger zu verteilen. Bei der Kollokation nach Client wird die Anzahl Datenträger, die zum Sichern und Zurückschreiben von Clientdaten erforderlich ist, auf ein Minimum reduziert. Bei der Datenkollokation kann sich die Anzahl Datenträgermounts erhöhen, da die Speicherung von Daten mehrerer Clients nicht auf demselben Datenträger erfolgt, sondern jeder Client möglicherweise über einen dedizierten Datenträger verfügt.

Sie können festlegen, dass der Server Clientdaten kollokiert, wenn die Daten anfänglich in Serverspeicher gestellt werden. In einer Speicherhierarchie können Sie die Daten kollokieren, wenn der Server die Daten aus dem ursprünglichen Speicherpool in den nächsten Speicherpool in der Speicherhierarchie umlagert. Sie können Daten nach Client, nach Dateibereich pro Client oder nach Clientgruppe kollokieren. Ihre Auswahl ist von der Größe der Dateibereiche, die gespeichert werden, und von Zurückschreibungsanforderungen abhängig.

Pools für aktive Daten verschiedenen Einheiten zuordnen

Pools für aktive Daten sind für die Schnellwiederherstellung von Clientdaten geeignet. Vorteile umfassen eine Reduzierung der Anzahl Speicherdatenträger vor Ort oder an einem anderen Standort oder eine Verringerung der Bandbreite, wenn Sie Dateien kopieren oder zurückschreiben, die durch elektronisches Vaulting an einem fernen Standort geschützt werden. Pools für aktive Daten, die austauschbare Datenträger verwenden, wie beispielsweise Bänder, bieten ähnliche Vorteile. Obwohl Bandeinheiten bereitgestellt werden müssen, muss der Server keine Positionierung hinter inaktive Dateien ausführen. Der Hauptvorteil bei der Verwendung austauschbarer Datenträger in Pools für aktive Daten liegt jedoch in der Reduzierung der Anzahl Datenträger, die für die Aufbewahrung vor Ort und an einem anderen Standort verwendet werden. Wenn Daten an einem fernen Standort gespeichert werden, können Sie das Datenvolumen, das übertragen werden muss, auf ein Minimum reduzieren, indem nur aktive Daten kopiert und zurückgeschrieben werden.

Sicherungsgruppe erstellen

Eine Sicherungsgruppe enthält alle aktiven gesicherten Dateien, die für den betreffenden Client im Serverspeicher vorhanden sind. Die Sicherungsgruppe ist portierbar und wird für den von Ihnen angegebenen Zeitraum aufbewahrt. Eine Sicherungsgruppe ist zusätzlich zu den Sicherungen vorhanden, die bereits gespeichert sind, und erfordert weitere Datenträger.

Daten für einen Clientknoten versetzen

Sie können Daten für einen Clientknoten konsolidieren, indem Sie die Daten innerhalb des Serverspeichers versetzen. Sie können eine Sicherungsgruppe auf verschiedene Datenträger versetzen, auf denen die Sicherungsgruppe für den von Ihnen angegebenen Zeitraum aufbewahrt wird. Durch die Konsolidierung von Daten kann die Effizienz während Clientzurückschreibungs- oder -abrufoperationen verbessert werden.

Datenschutzstrategien bei IBM Spectrum Protect

IBM Spectrum Protect stellt Möglichkeiten zur Implementierung verschiedener Datenschutzstrategien bereit.

In der Konfiguration von IBM Spectrum Protect können Sie angeben, ob Daten an Speichereinheiten am lokalen Standort oder an einem fernen Standort gesendet werden sollen. Um den Datenschutz zu maximieren, können Sie die Replikation auf einen fernen Server konfigurieren.

- Strategien zum Minimieren der Verwendung von Speicherbereich für Sicherungen
  Um die Größe des erforderlichen Speicherbereichs zu minimieren, sichert IBM Spectrum Protect Daten unter Verwendung der Datendeduplizierung und der progressiven Teilsicherung.
- Strategien zum Schutz vor Katastrophen
  IBM Spectrum Protect stellt Strategien bereit, um Daten in einem Katastrophenfall zu schützen. Diese Strategien umfassen Knotenreplikation an einen fernen Standort, Speicherpoolschutz, Datenbanksicherungen, Auslagerung von Sicherungsbändern und Einheitenreplikation auf einen Standby-Server.
- Strategien für die Wiederherstellung nach einem Katastrophenfall mithilfe von IBM Spectrum Protect
  IBM Spectrum Protect stellt verschiedene Möglichkeiten zur Wiederherstellung des Servers für den Fall bereit, dass die Datenbank oder Speicherpools fehlschlagen.

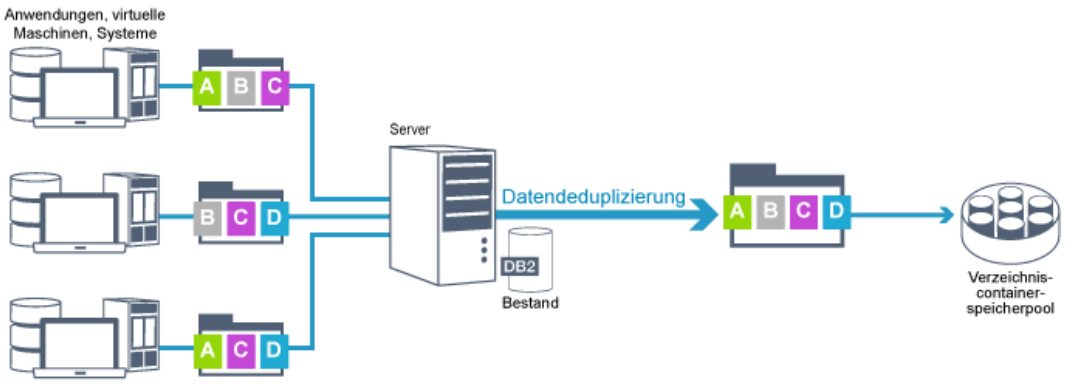
Strategien zum Minimieren der Verwendung von Speicherbereich für Sicherungen

Um die Größe des erforderlichen Speicherbereichs zu minimieren, sichert IBM Spectrum Protect Daten unter Verwendung der Datendeduplizierung und der progressiven Teilsicherung.

Datendeduplizierung

Wenn der IBM Spectrum Protect-Server Daten von einem Client empfängt, identifiziert der Server doppelte Datenbereiche und speichert eindeutige Instanzen der Datenbereiche in einem Verzeichniscontainerspeicherpool. Durch das Datendeduplizierungsverfahren wird die Speichernutzung verbessert und es ist keine dedizierte Datendeduplizierungsappliance erforderlich.

Abbildung 1. Datendeduplizierungsprozess



Wenn dasselbe Bytemuster mehrmals vorkommt, wird das Datenvolumen, das gespeichert oder übertragen werden muss, durch die Datendeduplizierung erheblich reduziert. Zusätzlich zu vollständigen Dateien kann IBM Spectrum Protect auch Teile von Dateien deduplizieren, die mit Teilen anderer Dateien identisch sind.

IBM Spectrum Protect stellt die folgenden Datendeduplizierungstypen bereit:

Serverseitige Datendeduplizierung
: Der Server identifiziert doppelte Datenbereiche und versetzt die Daten in einen Verzeichniscontainerspeicherpool. Der serverseitige Prozess verwendet die *Inline-Datendeduplizierung*, bei der Daten zu demselben Zeitpunkt dedupliziert werden, zu dem sie in einen Verzeichniscontainerspeicherpool geschrieben werden. Deduplizierte Daten können auch in anderen Typen von Speicherpools gespeichert werden. Die Inline-Datendeduplizierung auf dem Server bietet die folgenden Vorteile:

  - Die Notwendigkeit einer Konsolidierung entfällt.
  - Der Speicherbereich, der von den gespeicherten Daten belegt wird, wird reduziert.

Clientseitige Datendeduplizierung
: Mit dieser Methode wird die Verarbeitung während eines Sicherungsprozesses auf den Server und den Client verteilt. Der Client und der Server identifizieren und entfernen doppelte Daten, um Speicherbereich auf dem Server einzusparen. Bei der clientseitigen Datendeduplizierung werden nur komprimierte, deduplizierte Daten an den Server gesendet. Der Server speichert die Daten in dem vom Client zur Verfügung gestellten komprimierten Format. Die clientseitige Datendeduplizierung bietet die folgenden Vorteile:

  - Das Datenvolumen, das über das lokale Netz (LAN) gesendet wird, wird reduziert.
  - Die zusätzliche Verarbeitungsleistung und -zeit, die zum Entfernen doppelter Daten auf dem Server erforderlich sind, entfallen.
  - Die Datenbankleistung wird verbessert, da die clientseitige Datendeduplizierung ebenfalls inline erfolgt.

Sie können die clientseitige und serverseitige Datendeduplizierung in derselben Produktionsumgebung kombinieren. Die Möglichkeit, Daten entweder auf dem Client oder auf dem Server zu deduplizieren, bietet Flexibilität in Bezug auf Ressourcennutzung, Maßnahmenverwaltung und Datenschutz.

Komprimierung
: Verwenden Sie die Inline-Komprimierung, um die Größe des Speicherbereichs in Containerspeicherpools zu reduzieren. Daten werden beim Schreiben in den Containerspeicherpool komprimiert.
Einschränkung: Verschlüsselte Daten können vom IBM Spectrum Protect-Server nicht komprimiert werden.

Progressive Teilsicherung

Bei einer progressiven Teilsicherung überwacht der Server die Clientaktivität und sichert alle Dateien, die sich seit der ersten Gesamtsicherung geändert haben. Es werden vollständige Dateien gesichert, sodass der Server keine Basisversionen der Dateien referenzieren muss. Bei dieser Sicherungsmethode entfällt die Notwendigkeit, mehrere Gesamtsicherungen von Clientdaten erstellen zu müssen, wodurch Netzressourcen und Speicherbereich eingespart werden.

Strategien zum Schutz vor Katastrophen

IBM Spectrum Protect stellt Strategien bereit, um Daten in einem Katastrophenfall zu schützen. Diese Strategien umfassen Knotenreplikation an einen fernen Standort, Speicherpoolschutz, Datenbanksicherungen, Auslagerung von Sicherungsbändern und Einheitenreplikation auf einen Standby-Server.

Replikation an einen fernen Standort

Knotenreplikation ist der Prozess, bei dem Daten inkrementell von einem Server auf einen anderen Server kopiert werden. Der Server, von dem Clientdaten repliziert werden, wird als *Quellenreplikationsserver* bezeichnet. Der Server, auf den Clientdaten repliziert werden, wird als *Zielreplikationsserver* bezeichnet. Zum Schutz vor Katastrophen befindet sich der Zielreplikationsserver an einem fernen Standort. Ein Replikationsserver kann als Quellenserver und/oder Zielserver fungieren. Die Replikationsverarbeitung wird verwendet, um denselben Stand von Dateien auf dem Quellen- und dem Zielserver beizubehalten.

Die Knotenreplikation ermöglicht die sofortige Verfügbarkeit von Daten durch Übernahme. Auch wenn mithilfe der Knotenreplikation der größte Teil der Metadaten geschützt wird, bietet diese Methode keinen adäquaten Schutz vor einer Beschädigung der Datenbank. Sie können umfassenderen Schutz bereitstellen, indem Sie Speicherpools zum Speichern von Datensicherungen verwenden.

Vorteile

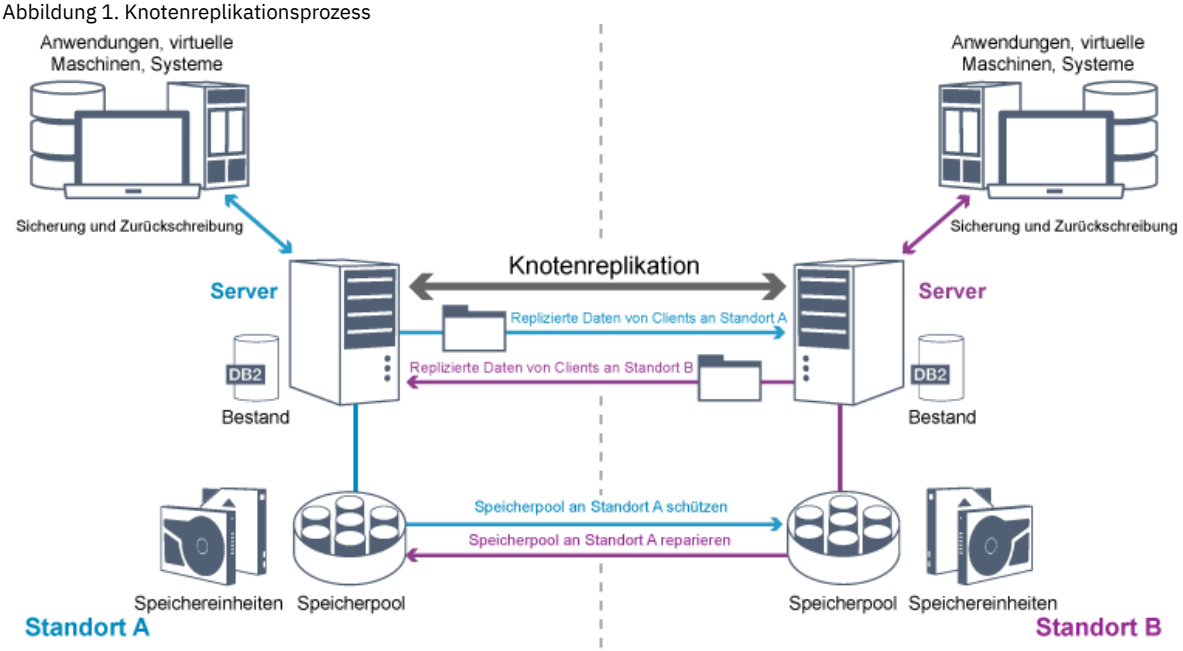
- Übernahme, sodass Daten sofort verfügbar sind, wenn ein Katastrophenfall eintritt
- Inkrementelle Replikation, die eine schnelle Datenübertragung zur Folge hat
- Elektronische Übertragung
- Schutz sowohl von Daten als auch von Metadaten

Nachteile

- Sowohl Daten als auch Metadaten müssen wiederhergestellt werden.
- Daten auf dem Quellenserver müssen erneut vom fernen Standort repliziert werden.

Abbildung 1 zeigt den Replikationsprozess an einen fernen Standort.

Abbildung 1. Knotenreplikationsprozess



Wenn Clientdaten repliziert werden, werden Daten, die nicht auf dem Zielserver vorhanden sind, auf den Zielserver kopiert. Wenn replizierte Daten den Aufbewahrungszeitraum überschreiten, entfernt der Zielserver die Daten automatisch vom Quellenserver. Um den Datenschutz zu maximieren, synchronisieren Sie den lokalen Server und den fernen Server; beispielsweise repliziert Standort B Daten von Standort A und Standort A repliziert Daten von Standort B. Im Rahmen der Replikationsverarbeitung werden Clientdaten, die vom Quellenserver gelöscht wurden, auch vom Zielserver gelöscht.

IBM Spectrum Protect stellt die folgenden Replikationsfunktionen bereit:

- Sie können Maßnahmen für den Zielserver auf folgende Art und Weise definieren:
  - Identische Maßnahmen auf dem Quellenserver und dem Zielserver
  - Unterschiedliche Maßnahmen auf dem Quellenserver und dem Zielserver, um unterschiedliche Geschäftsanforderungen zu erfüllen

  Wenn ein Katastrophenfall eintritt und der Quellenserver nicht verfügbar ist, können Clients Daten vom Zielserver wiederherstellen. Wenn eine Wiederherstellung des Quellenservers nicht möglich ist, können Sie Clients anweisen, Daten auf dem Zielserver zu speichern. Bei einem Ausfall kann für die Clients, die auf dem Quellenserver gesichert werden, automatisch eine Übernahme erfolgen, damit ihre Daten vom Zielserver zurückgeschrieben werden können.
- Mithilfe der Replikationsverarbeitung können Sie beschädigte Dateien aus Speicherpools wiederherstellen. Sie müssen die Clientdaten auf den Zielserver replizieren, bevor die Datei beschädigt wird. Nachfolgende Replikationsprozesse erkennen beschädigte Dateien auf dem Quellenserver und ersetzen sie durch unbeschädigte Dateien vom Zielserver.

Rolle der Replikation beim Schutz vor Katastrophen

Wenn ein Katastrophenfall eintritt, können Sie replizierte Daten vom fernen Standort wiederherstellen und denselben Stand von Dateien auf dem Quellenserver und dem Zielserver beibehalten. Die Replikation wird zum Erreichen der folgenden Ziele verwendet:

- Steuern des Netzdurchsatzes durch die Planung der Knotenreplikation für bestimmte Zeiten
- Wiederherstellen von Daten nach einem Verlust aller Daten am Standort
- Wiederherstellen beschädigter Dateien auf dem Quellenserver

Speicherpoolschutz

Stellen Sie im Rahmen einer Strategie zur Wiederherstellung nach einem Katastrophenfall sicher, dass eine Sicherungskopie der Daten in Speicherpools an einem fernen Standort verfügbar ist.

Vorteile

- Schnelle Wiederherstellung und Neuerstellung des Quellensystems

Nachteile

- Es werden nur Daten geschützt; Metadaten werden nicht geschützt.
- Für jeden Speicherpool müssen Sie das Speichermedium definieren.

Verschiedene Methoden können zum Schutz vor dem permanenten Verlust von Daten verwendet werden, die in Containerspeicherpools und in FILE- und DISK-Speicherpools gespeichert sind.

Verzeichniscontainerspeicherpools

Wenn nicht alle Daten in einem Clientknoten repliziert werden müssen, verwenden Sie Containerkopienspeicherpools, um einige Verzeichniscontainerspeicherpools zu schützen. Indem ein Verzeichniscontainerspeicherpool geschützt wird, werden keine Ressourcen verwendet, die vorhandene Daten und Metadaten replizieren, wodurch die Serverleistung verbessert wird.

Die bevorzugte Methode ist, den Verzeichniscontainerspeicherpool vor dem Replizieren des Clientknotens zu schützen. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch Speicherpoolschutz repliziert werden, übersprungen und die Replikationsverarbeitungszeit wird somit reduziert. Wenn die Daten in einem Verzeichniscontainerspeicherpool beschädigt werden, können Sie die Daten mithilfe einer Kopie in einem Containerkopienspeicherpool reparieren.

Containerkopienspeicherpools

Sie schützen Verzeichniscontainerspeicherpools, indem Sie die Daten im Verzeichniscontainerspeicherpool in Containerkopienspeicherpools kopieren. Verwenden Sie Containerkopienspeicherpools, um bis zu zwei Bandkopien eines Verzeichniscontainerspeicherpools zu erstellen. Die Bandkopien können vor Ort oder an einem anderen Standort aufbewahrt werden. Beschädigte Daten in Verzeichniscontainerspeicherpools können mithilfe von Containerkopienspeicherpools repariert werden. Containerkopienspeicherpools stellen eine Alternative zur Verwendung eines Replikationsservers zum Schützen von Daten in einem Verzeichniscontainerspeicherpool dar.

Speicherpools, die Einheitenklassen FILE und DISK zugeordnet sind

Für Speicherpools, die Einheitenklassen FILE und DISK zugeordnet sind, verwenden Sie die Knotenreplikation, um eine knotenkonsistente Kopie der Daten auf dem Zielserver beizubehalten. Die Datenkopie kann direkt vom Zielserver in die Speicherpools zurückgeschrieben werden.

Datenbanksicherungen

Sie verwenden Datenbanksicherungen, um Ihr System nach einer Beschädigung der Datenbank wiederherzustellen. Datenbanksicherungen müssen außerdem verwendet werden, um zu verhindern, dass bei DB2 der Speicherbereich für das Archivprotokoll knapp wird. Datenbanksicherungsoperationen sind nicht Teil der Knotenreplikation. Bei einer Datenbanksicherung kann es sich um eine Gesamt-, Teil- oder Momentaufnahmesicherung handeln. Um eine schnelle Wiederherstellung nach einem Katastrophenfall zu ermöglichen, muss eine Kopie der Datenbanksicherungen an einen anderen Standort gespeichert werden. Um die Datenbank zurückschreiben zu können, müssen Sie über die Sicherungsdatenträger für die Datenbank verfügen. Sie können die Datenbank mithilfe einer Operation für die Zurückschreibung nach Zeitpunkt oder einer Operation für die Zurückschreibung mit dem neuesten Stand aus Sicherungsdatenträgern zurückschreiben.

Zurückschreibung nach Zeitpunkt
Verwenden Sie Operationen für die Zurückschreibung nach Zeitpunkt bei der Wiederherstellung nach einem Katastrophenfall oder zum Entfernen der Auswirkungen von Fehlern, die Inkonsistenzen in der Datenbank zur Folge haben können. Zurückschreibungsoperationen für die Datenbank, bei denen Momentaufnahmesicherungen verwendet werden, sind eine Form der Operation für die Zurückschreibung nach Zeitpunkt. Die Operation für die Zurückschreibung nach Zeitpunkt umfasst die folgenden Aktionen:

- Das Verzeichnis für aktive Protokolldateien und das Archivprotokollverzeichnis, die in der Datei dsmserv.opt angegeben sind, werden entfernt und erneut erstellt.
- Das Datenbankimage wird von den Sicherungsdatenträgern in die Datenbankverzeichnisse, die in einer Datenbanksicherung aufgezeichnet wurden, oder in neue Verzeichnisse zurückgeschrieben.
- Archivprotokolle werden von den Sicherungsdatenträgern in das Überlaufverzeichnis zurückgeschrieben.
- Protokolldaten aus dem Überlaufverzeichnis werden bis zu einem angegebenen Zeitpunkt verwendet.

Zurückschreibung mit dem neuesten Stand
Wenn die Datenbank mit dem Stand wiederhergestellt werden soll, den sie zu dem Zeitpunkt hatte, zu dem sie verloren ging, stellen Sie die Datenbank mit dem neuesten Stand wieder her. Die Operation für die Zurückschreibung mit dem neuesten Stand umfasst die folgenden Aktionen:

- Ein Datenbankimage wird von den Sicherungsdatenträgern in die Datenbankverzeichnisse, die in einer Datenbanksicherung aufgezeichnet wurden, oder in neue Verzeichnisse zurückgeschrieben.
- Archivprotokolle werden von den Sicherungsdatenträgern in das Überlaufverzeichnis zurückgeschrieben.
- Protokolldaten aus dem Überlaufverzeichnis und Archivprotokolle aus dem Archivprotokollverzeichnis werden verwendet.

Im Rahmen der letzten Zurückschreibung werden das Verzeichnis für aktive Protokolldateien und das Archivprotokollverzeichnis nicht entfernt und erneut erstellt.

Alternativmethoden zum Schutz vor Katastrophen

Zusätzlich zu Replikation, Speicherpoolschutz und Datenbanksicherungen können Sie auch die folgenden Methoden zum Schutz von Daten und zur Implementierung der Wiederherstellung nach einem Katastrophenfall mit IBM Spectrum Protect verwenden:

Transport von Sicherungsbändern an einen fernen Standort

Daten werden zu geplanten Zeiten vom Quellenserver auf Band gesichert. Die Bänder werden an einen fernen Standort transportiert. Wenn ein Katastrophenfall eintritt, werden die Bänder an den Standort des Quellenservers zurücktransportiert und die Daten werden auf die Quellenclients zurückgeschrieben. Ausgelagerte Kopien der Daten auf Sicherungsband können Sie auch bei der Wiederherstellung nach Ransomware-Attacken unterstützen.

Replikation mit Appliances an mehreren Standorten auf einen Standby-Server

Bei der Konfiguration mit Appliances an mehreren Standorten wird die Quellen-Appliance auf einen fernen Server in einer SAN-Architektur repliziert. Wenn die Client-Hardware am ursprünglichen Standort beschädigt wird, kann bei dieser Konfiguration die Quelleneinheit vom Standby-Server am fernen Standort repliziert werden. Mit dieser Konfiguration werden plattenbasierte Sicherungs- und Zurückschreibungsoperationen bereitgestellt.

Vergleich der Konfigurationsstrategien für den Schutz

Beachten Sie die folgenden potenziellen Datenverlustszenarios:

- Datenbankdaten werden beschädigt: Schützen Sie sich mithilfe der Datenbanksicherung vor Ort vor dem Verlust von Daten in der Datenbank.
- Speicherpooldaten werden beschädigt: Schützen Sie sich mithilfe von Kopienspeicherpools vor Ort oder mithilfe der Knotenreplikation vor dem Verlust von Daten in Speicherpools.
- Störungsszenario, bei dem sowohl die Datenbank vor Ort als auch die Speicherpools vor Ort verloren gehen: Schützen Sie sich vor einer großen Katastrophe, indem Sie die Knotenreplikation und sowohl die Datenbanksicherung an einem anderen Standort als auch Speicherpoolsicherungskopien an einem anderen Standort verwenden.

Die folgenden potenziellen Konfigurationen betreffen die gängigsten Datenschutzszenarios:

Konfigurationen ausschließlich für den Schutz vor einer Beschädigung

- Implementieren Sie Datenbanksicherungsoperationen vor Ort mit einem optionalen Containerkopienspeicherpool vor Ort, um Daten in Verzeichniscontainerspeicherpools zu schützen.
- Implementieren Sie Datenbanksicherungsoperationen vor Ort und die Knotenreplikation vor Ort.

Konfigurationen für die Wiederherstellung nach einem Katastrophenfall und den Schutz vor einer Beschädigung

- Implementieren Sie Datenbanksicherungsoperationen an einen anderen Standort mit Containerkopienspeicherpools an einen anderen Standort, um Daten in Verzeichniscontainerspeicherpools zu schützen.
- Implementieren Sie Datenbanksicherungsoperationen vor Ort und die Knotenreplikation an einem anderen Standort mit einem optionalen Containerkopienspeicherpool vor Ort für die schnellere Wiederherstellung beschädigter Daten.

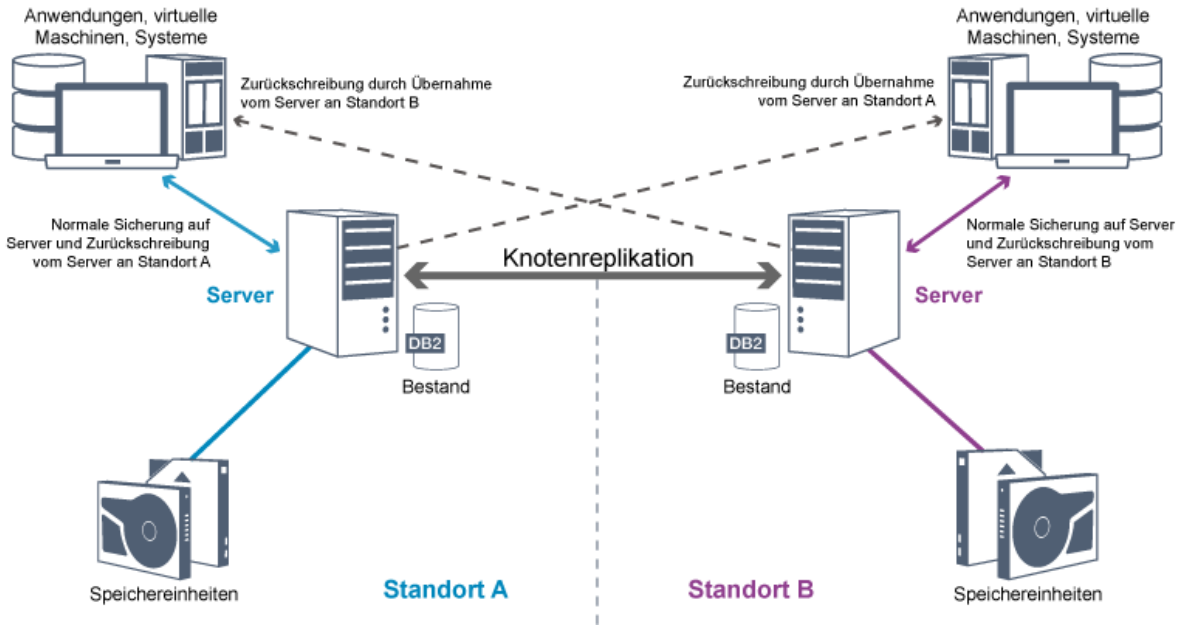
Strategien für die Wiederherstellung nach einem Katastrophenfall mithilfe von IBM Spectrum Protect

IBM Spectrum Protect stellt verschiedene Möglichkeiten zur Wiederherstellung des Servers für den Fall bereit, dass die Datenbank oder Speicherpools fehlschlagen.

Automatische Übernahme für die Wiederherstellung nach einem Katastrophenfall

Die *automatische Übernahme* ist eine Operation, mit zu einem Standby-System gewechselt wird, wenn eine Software-, Hardware- oder Netzunterbrechung auftritt. Die automatische Übernahme wird zusammen mit der Knotenreplikation zur Wiederherstellung von Daten nach einem Systemfehler verwendet. Abbildung 1 zeigt den automatischen Übernahmeprozess in IBM Spectrum Protect.

Abbildung 1. Automatischer Übernahmeprozess



Die automatische Übernahme für die Datenwiederherstellung erfolgt, wenn der Quellenreplikationsserver aufgrund einer Katastrophe oder eines Systemausfalls nicht verfügbar ist. Wenn der Client während des normalen Betriebs auf einen Quellenreplikationsserver zugreift, empfängt der Client Verbindungsinformationen für den Zielreplikationsserver. Der Clientknoten speichert die Übernahmeverbindungsinformationen in der Clientoptionsdatei.

Während Clientzurückschreibungsoperationen wechseln Clients automatisch vom Quellenreplikationsserver zum Zielreplikationsserver und wieder zurück; dieser Wechsel wird durch den Server ausgeführt. Für den Schutz durch Übernahme kann jeweils nur ein einziger Server pro Knoten verwendet werden. Wenn eine neue Clientoperation gestartet wird, versucht der Client, die Verbindung zum Quellenreplikationsserver herzustellen. Der Client nimmt die Operationen auf dem Quellenserver wieder auf, wenn der Quellenreplikationsserver verfügbar ist.

Um die automatische Übernahme für replizierte Clientknoten verwenden zu können, müssen der Quellenreplikationsserver, der Zielreplikationsserver und der Client Version 7.1 oder höher haben. Wenn einer der Server eine frühere Version hat, wird die automatische Übernahme inaktiviert und Sie müssen den Übernahmeprozess manuell ausführen.

Wiederherstellung von IBM Spectrum Protect-Komponenten

Die Serverdatenbank, das Wiederherstellungsprotokoll und die Speicherpools sind für den Betrieb von IBM Spectrum Protect kritisch und müssen geschützt werden. Wenn die Datenbank nicht verwendbar ist, ist der gesamte Server nicht verfügbar und die Wiederherstellung von Daten, die vom Server verwaltet werden, kann sich schwierig gestalten oder als unmöglich erweisen.

Sogar ohne die Datenbank könnten Datenfragmente oder vollständige Dateien von Speicherpooldatenträgern gelesen werden, die nicht verschlüsselt sind, und die Sicherheit kann beeinträchtigt werden. Aus diesem Grund müssen Sie die Datenbank immer sichern. Verschlüsseln Sie außerdem immer sensible Daten mithilfe des Clients oder der Speichereinheit, es sei denn, die Speichermedien sind physisch geschützt.

IBM Spectrum Protect stellt eine Reihe von Datenschutzmethoden bereit, die das Sichern von Speicherpools und der Datenbank umfassen. Sie können beispielsweise für die Ausführung der folgenden Operationen Zeitpläne definieren:

- Nach der ersten Gesamtsicherung Ihrer Speicherpools werden jede Nacht Speicherpoolteilsicherungen ausgeführt.
- Datenbankteilsicherungen werden jede Nacht ausgeführt.
- Datenbankgesamtsicherungen werden einmal pro Woche ausgeführt.

Bei bandbasierten Umgebungen können Sie Disaster Recovery Manager (DRM) zur Unterstützung bei der Ausführung vieler Tasks verwenden, die den Schutz und die Wiederherstellung von Daten betreffen. DRM ist in IBM Spectrum Protect Extended Edition verfügbar.

Vorbeugende Maßnahmen für die Wiederherstellung

Die Wiederherstellung basiert auf folgenden vorbeugenden Maßnahmen:

- Spiegeln, wodurch der Server eine Kopie der aktiven Protokolldatei beibehält
- Sichern der Datenbank
- Sichern der Speicherpools
- Prüfen der Speicherpools auf beschädigte Dateien und Wiederherstellen der beschädigten Dateien, falls erforderlich
- Sichern der Einheitenkonfigurationsdateien und Protokolldateien für Datenträger
- Prüfen der Daten in Speicherpools mithilfe der zyklischen Blockprüfung
- Speichern der Datei cert.kdb an einer sicheren Position, um zu gewährleisten, dass Secure Sockets Layer (SSL) sicher ist

Wenn Sie Bänder zum Speichern verwenden, können Sie auch einen Plan zur Wiederherstellung nach einem Katastrophenfall (der auch als Wiederherstellungsplan bezeichnet wird) erstellen, der Sie durch den Wiederherstellungsprozess mit DRM führt. Sie können den Wiederherstellungsplan zu Prüfzwecken verwenden, um die Wiederherstellbarkeit des Servers zu bestätigen. Die Methoden von DRM zur Wiederherstellung nach einem Katastrophenfall basieren auf den folgenden Maßnahmen:

- Erstellen einer Wiederherstellungsplandatei für den Server
- Sichern von Serverdaten auf Band
- Senden der Serversicherungsdaten an einen fernen Standort oder einen anderen Server
- Speichern von Clientsysteminformationen
- Definieren und Verfolgen der Speichermedien, die zum Speichern und Wiederherstellen von Clientdaten verwendet werden

IBM Spectrum Protect-Datenschutzlösungen

IBM Spectrum Protect-Server und -Clients stellen Datenschutzlösungen für die meisten allgemeinen Geschäfts- und Konformitätsanforderungen bereit.

- Datenschutzlösung für Ihre Umgebung auswählen
  Lesen Sie zur Unterstützung bei der Implementierung einer Datenschutzumgebung die Informationen zu Best-Practice-Konfigurationen von IBM Spectrum Protect und wählen Sie die beste Lösung für Ihre Geschäftsanforderungen aus.
- Plattenspeicherlösung für einen einzelnen Standort
  Diese Datenschutzlösung stellt kosteneffizienten Datenspeicher an einem einzelnen Standort mit minimaler Hardwarekonfiguration bereit.
- Plattenspeicherlösung für mehrere Standorte
  Diese Datenschutzlösung stellt Replikation an mehreren Standorten bereit, sodass jeder Server Daten für den jeweils anderen Standort schützt.
- Bandspeicherlösung
  Diese Datenschutzlösung stellt Speicher für Banddatenträger bereit, eine flexible und kosteneffiziente Option für die langfristige Aufbewahrung von Daten.
- Serverlösungsdokumentation in PDF-Dateien
  Vordefinierte PDF-Dateien für die IBM Spectrum Protect-Dokumentation sind zum Download verfügbar.

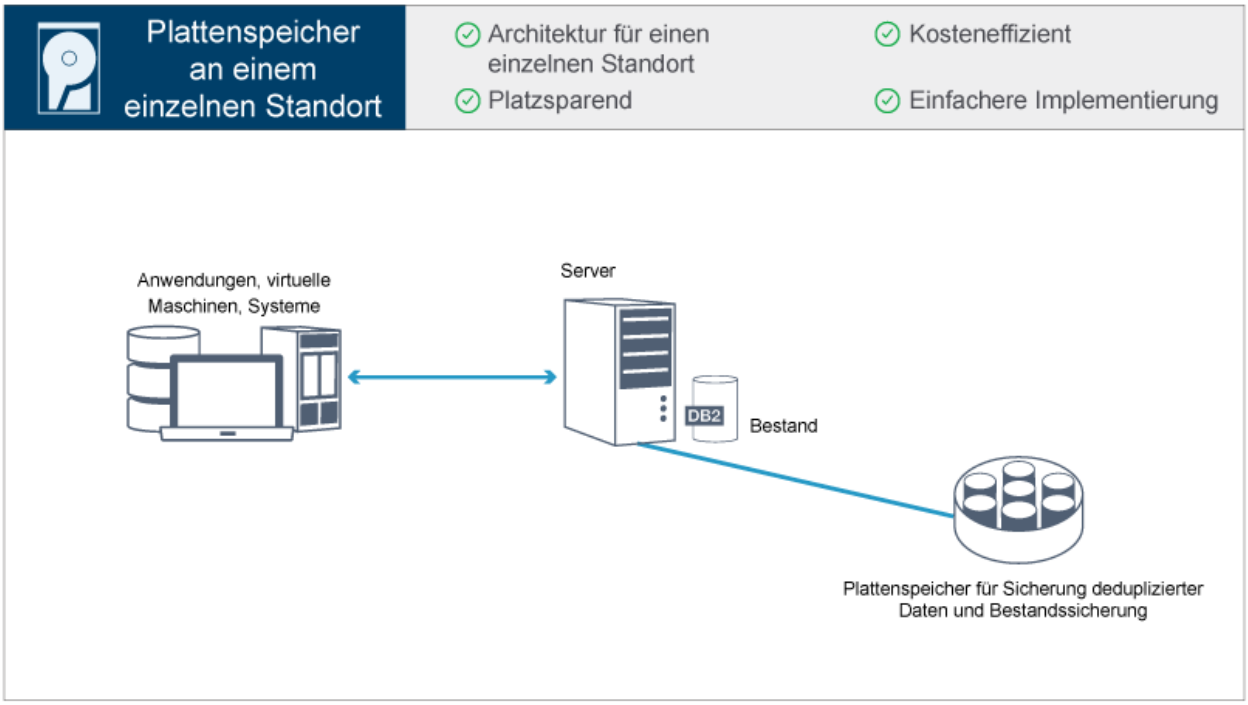
Datenschutzlösung für Ihre Umgebung auswählen

Lesen Sie zur Unterstützung bei der Implementierung einer Datenschutzumgebung die Informationen zu Best-Practice-Konfigurationen von IBM Spectrum Protect und wählen Sie die beste Lösung für Ihre Geschäftsanforderungen aus.

- Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort
  Diese plattenbasierte Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet Inline-Datendeduplizierung und stellt Schutz für Daten an einem einzelnen Standort bereit.
- Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte
  Diese plattenbasierte Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet Inline-Datendeduplizierung und Replikation an zwei Standorten.
- Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte
  Diese Implementierung einer IBM Spectrum Protect-Datenschutzlösung für mehrere Standorte verwendet appliance-basierte Datendeduplizierung und Replikation. Ein Standby-Server ist an einem zweiten Standort für die Wiederherstellung von Daten für den Fall konfiguriert, dass der primäre Server nicht verfügbar ist.
- Bandbasierte Implementierung einer Datenschutzlösung
  Diese Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet eine oder mehrere Bandspeichereinheiten zum Sichern von Daten. Die Bandsicherung stellt kostengünstige Skalierbarkeit bereit, die für die langfristige Aufbewahrung optimiert ist.
- Vergleich der Datenschutzlösungen
  Vergleichen Sie die Schlüsselfunktionen der einzelnen IBM Spectrum Protect-Lösungen, um die Konfiguration zu bestimmen, die Ihre Datenschutzanforderungen am besten erfüllt. Lesen Sie dann die verfügbare Dokumentation, um die Lösung zu implementieren.
- Roadmap für die Implementierung einer Datenschutzlösung
  Planen und implementieren Sie die geeignetste Datenschutzlösung für Ihre Geschäftsumgebung mit IBM Spectrum Protect.

Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort

Diese plattenbasierte Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet Inline-Datendeduplizierung und stellt Schutz für Daten an einem einzelnen Standort bereit.



Diese Datenschutzlösung bietet die folgenden Vorteile:

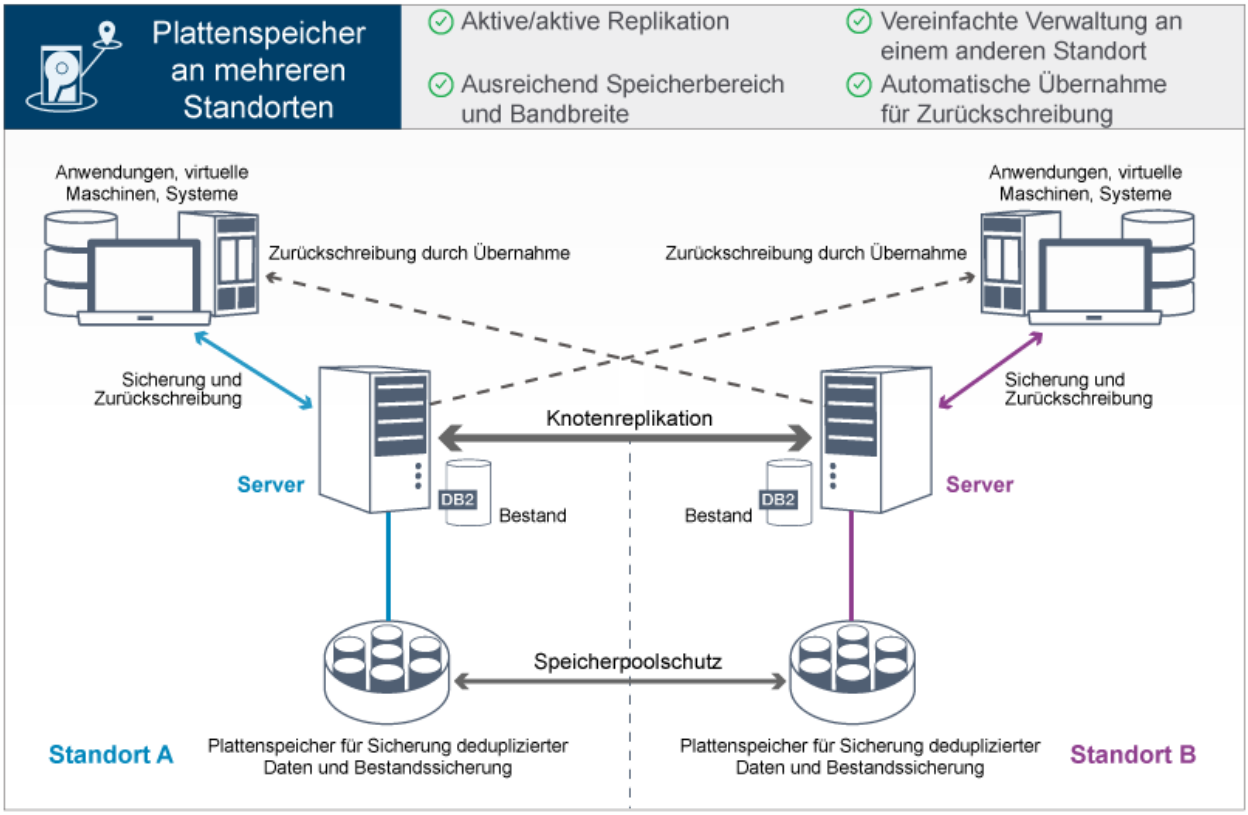
- Serversystem und Speicherhardware an einem einzigen Standort
- Kosteneffizient Nutzung des Speichers über die Datendeduplizierungsfunktion
- Platzsparende Lösung mit minimaler Hardwarekonfiguration
- Minimale Implementierung, die nur die Installation und Konfiguration für einen einzigen Server und unterstützende Speicherhardware erfordert

Bei dieser Lösung sendet der Client Daten an den IBM Spectrum Protect-Server, auf dem die Daten dedupliziert und in einem Verzeichniscontainerspeicherpool gespeichert werden, der in Plattenspeicher implementiert ist. Daten aus dem Bestand werden ebenfalls in Plattenspeicher gesichert. Diese Lösung ist für Einstiegsumgebungen geeignet, bei denen keine zweite Kopie der Daten erforderlich ist.

Zugehörige Verweise:
Vergleich der Datenschutzlösungen
Roadmap für die Implementierung einer Datenschutzlösung

Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte

Diese plattenbasierte Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet Inline-Datendeduplizierung und Replikation an zwei Standorten.



Diese Datenschutzlösung bietet die folgenden Vorteile:

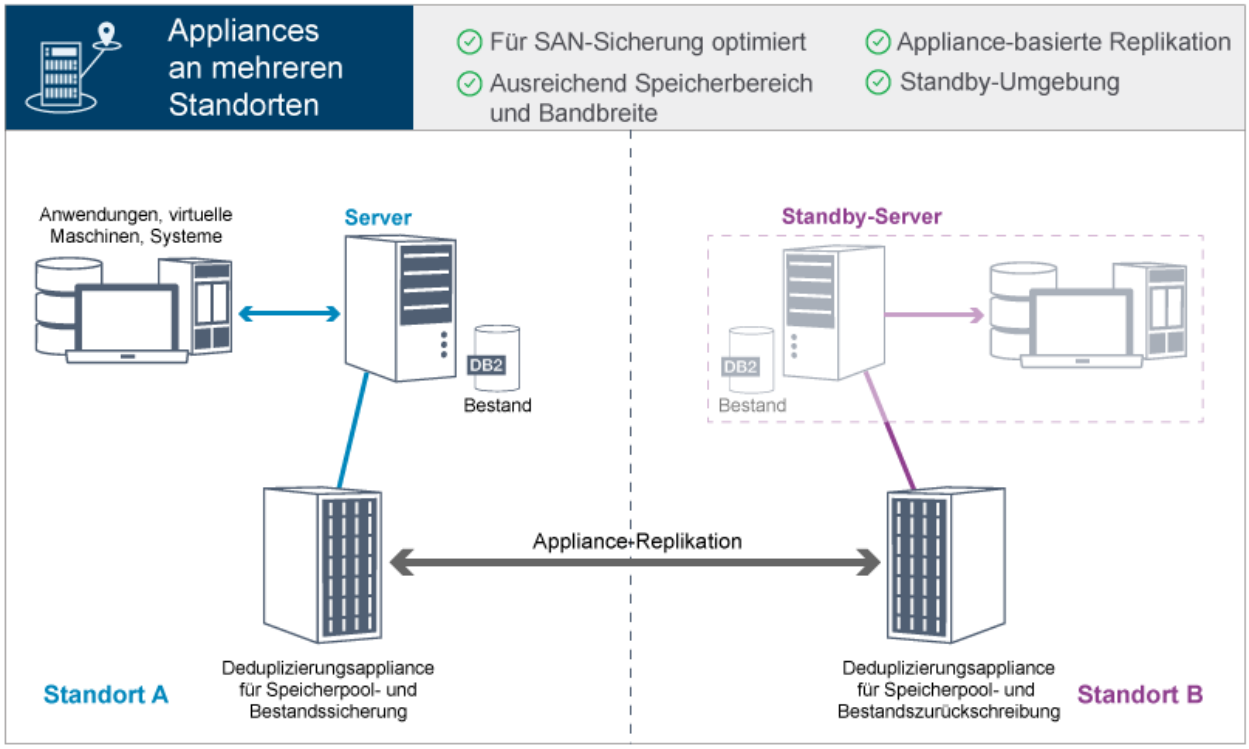
- Replikation kann an beiden Standorten konfiguriert werden, sodass jeder Server Daten für den jeweils anderen Standort schützt.
- Die Auslagerung von Daten für jeden Standort wird vereinfacht.
- Bandbreite wird effizient genutzt, da nur deduplizierte Daten zwischen den Standorten repliziert werden.
- Für Clients kann eine automatische Übernahme durch einen Zielreplikationsserver erfolgen, wenn der Quellenreplikationsserver nicht verfügbar ist.

Bei dieser Lösung senden Clients Daten an den Quellenserver, auf dem die Daten dedupliziert und in einem Verzeichniscontainerspeicherpool gespeichert werden, der in Plattenspeicher implementiert ist. Die Daten werden für jeden Standort in den Speicherpool auf dem Zielserver repliziert. Diese Lösung ist für Umgebungen geeignet, die Schutz vor Katastrophen erfordern. Wenn die gegenseitige Replikation konfiguriert ist, können Clients an beiden Standorten die Wiederherstellung durch Übernahme für unterbrechungsfreie Sicherungen und Datenwiederherstellung von dem am anderen Standort verfügbaren Server nutzen.

Zugehörige Verweise:
Vergleich der Datenschutzlösungen
Roadmap für die Implementierung einer Datenschutzlösung

Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte

Diese Implementierung einer IBM Spectrum Protect-Datenschutzlösung für mehrere Standorte verwendet appliance-basierte Datendeduplizierung und Replikation. Ein Standby-Server ist an einem zweiten Standort für die Wiederherstellung von Daten für den Fall konfiguriert, dass der primäre Server nicht verfügbar ist.



Diese Datenschutzlösung bietet die folgenden Vorteile:

- Die Leistung ist für Sicherungen in Hochgeschwindigkeits-SANs und für die Verwendung mit IBM Spectrum Protect for SAN optimiert, wenn Clients Daten direkt auf virtuelle Bandeinheiten sichern, die an ein Speicherbereichsnetz (SAN) angeschlossen sind.
- Durch die schnelle, appliance-basierte Replikation wird der Server von der Notwendigkeit befreit, Replikationsmetadaten in der Serverdatenbank verfolgen zu müssen.
- Bandbreite und Speicherbereich werden effizient genutzt, da nur deduplizierte Daten zwischen den Standorten repliziert werden.
- Eine Standby-Umgebung ist für die Wiederherstellung nach einem Katastrophenfall verfügbar, erfordert aber nicht so viele Ressourcen, wie für einen vollständig aktiven Standort benötigt werden.

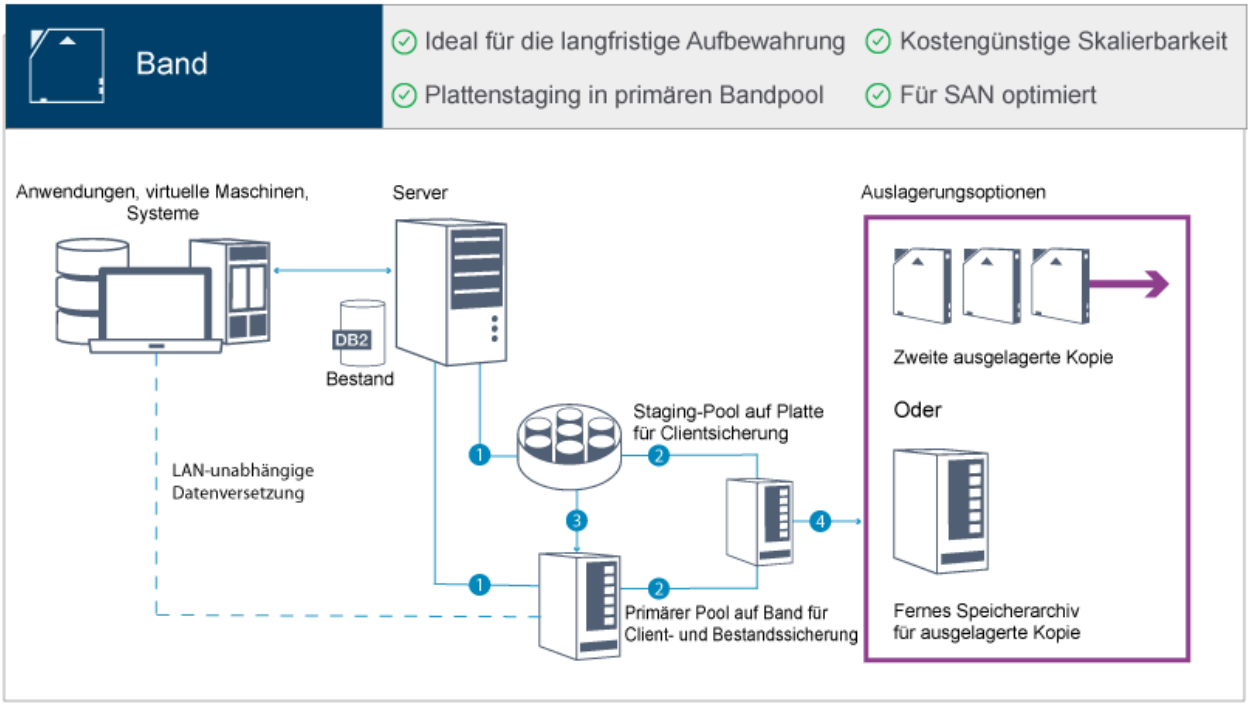
Bei dieser Datenschutzkonfiguration verwendet der Server Hardware-Appliances zum Deduplizieren und Replizieren von Daten. Die Appliance an Standort A dedupliziert Daten und repliziert die Daten anschließend zum Schutz vor Katastrophen auf die Appliance an Standort B. Bei einem Ausfall an Standort A können Sie den Standby-Server aktivieren, indem Sie die neueste Datenbanksicherung zurückschreiben und die replizierte Kopie der Daten aktivieren.

Weitere Informationen zum Konfigurieren virtueller Bandarchive finden Sie in Virtuelle Bandarchive konfigurieren.

Zugehörige Verweise:
Vergleich der Datenschutzlösungen
Roadmap für die Implementierung einer Datenschutzlösung

Bandbasierte Implementierung einer Datenschutzlösung

Diese Implementierung einer Datenschutzlösung mit IBM Spectrum Protect verwendet eine oder mehrere Bandspeichereinheiten zum Sichern von Daten. Die Bandsicherung stellt kostengünstige Skalierbarkeit bereit, die für die langfristige Aufbewahrung optimiert ist.



Diese Datenschutzlösung bietet die folgenden Vorteile:

- Die Leistung wird für Sicherungsoperationen in Hochgeschwindigkeits-SANs, die direkt auf Band erfolgen, für große Datentypen und für die langfristige Aufbewahrung von Daten optimiert.
- Die Datenverfügbarkeit wird optimiert, indem Kopien von Daten für die Wiederherstellung nach einem Katastrophenfall an anderen Standorten aufbewahrt werden.
- Kostengünstige Skalierbarkeit wird erzielt, indem die Notwendigkeit zusätzlicher Plattenhardware reduziert und Energiekosten gesenkt werden.

Zugehörige Konzepte:
Bandeinheitentreiber auswählen
Zugehörige Tasks:
Datensicherungsstrategien erstellen
Datenträgerbestand verwalten
Zugehörige Verweise:
Vergleich der Datenschutzlösungen
Bandeinheitentreiber installieren und konfigurieren

Vergleich der Datenschutzlösungen

Vergleichen Sie die Schlüsselfunktionen der einzelnen IBM Spectrum Protect-Lösungen, um die Konfiguration zu bestimmen, die Ihre Datenschutzanforderungen am besten erfüllt. Lesen Sie dann die verfügbare Dokumentation, um die Lösung zu implementieren.

	Plattenspeicher an einem einzelnen Standort	**Plattenspeicher an mehreren Standorten**	**Appliances an mehreren Standorten**	**Band**
				
Schwerpunkte				
Kosten	$	$$$	$$$$	$$
Schutzstufe	1 Datenkopie	2 oder mehr Datenkopien	2 oder mehr Datenkopien	2 oder mehr Datenkopien
Wiederherstellung nach einem Katastrophenfall	Keine	Aktiver Server	Standby-Server	Kopien an einem anderen Standort
Hauptvorteile				
Erstklassige Datenreduktion	✓	✓	✓	✓

	Plattenspeicher an einem einzelnen Standort	Plattenspeicher an mehreren Standorten	Appliances an mehreren Standorten	Band
				
Schnelle und effiziente plattenbasierte Sicherungs- und Zurückschreibungsoperationen	✓		✓	
Vereinfachte Verwaltung an einem anderen Standort		✓		
Datendeduplizierungsfunktion ohne Zusatzkosten	✓	✓		
Inklusive Replikationsverarbeitung ohne Zusatzkosten		✓		
Datendeduplizierung sowohl auf dem Quellenserver als auch auf dem Zielserver		✓		
Kostengünstige Skalierbarkeit, für die langfristige Aufbewahrung optimiert				✓
Effizienz und Kosten				
Für Hochgeschwindigkeitssicherungsoperationen im Speicherbereichsnetz optimiert			✓	✓
Für Hochgeschwindigkeitsoperationen im lokalen Netz (LAN) optimiert	✓	✓	✓	
Globale Datendeduplizierung für alle Datentypen und Quellen	✓	✓	✓	
Bandbreiteneffiziente Replikation		✓	✓	
Niedrigere Energiekosten				✓
Option einer zweiten Kopie ohne weitere Plattenhardware				✓
Verfügbarkeit				
Möglichkeit von Kopien an einem anderen Standort		✓	✓	✓
Appliance-basierte Replikation			✓	
Clientwiederherstellung von einem Hochverfügbarkeitsserver		✓		
Replikationsziel in der Cloud		✓		
Unabhängige Verwaltung von Aufbewahrungsmaßnahmen für Replikationsdaten; Möglichkeit, am Wiederherstellungsstandort mehr oder weniger Daten aufzubewahren		✓		
Replikation auf Anwendungsebene; Möglichkeit, die Systeme und Anwendungen auszuwählen, die repliziert werden		✓		
Skalierbarkeit				
Globale Datendeduplizierung für alle Server			✓	
Direkte SAN-optimierte Sicherung auf Band für große Datentypen				✓
Skalierbarkeit von Einzelinstanzen im Petabytebereich				✓

Nächste Schritte

Lesen Sie die für die Lösungen verfügbare Dokumentation (siehe Roadmap für die Implementierung einer Datenschutzlösung).
Zugehörige Verweise:
Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort
Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte
Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte
Bandbasierte Implementierung einer Datenschutzlösung

Roadmap für die Implementierung einer Datenschutzlösung

Planen und implementieren Sie die geeignetste Datenschutzlösung für Ihre Geschäftsumgebung mit IBM Spectrum Protect.

Plattenspeicherlösung für einen einzelnen Standort

Die Schritte, die die Planung, Implementierung, Überwachung und Ausführung einer Plattenspeicherlösung für einen einzelnen Standort beschreiben, finden Sie in Plattenspeicherlösung für einen einzelnen Standort.

Plattenspeicherlösung für mehrere Standorte

Die Schritte, die die Planung, Implementierung, Überwachung und Ausführung einer Plattenspeicherlösung für mehrere Standorte beschreiben, finden Sie in Plattenspeicherlösung für mehrere Standorte.

Bandspeicherlösung

Die Schritte, die die Planung, Implementierung, Überwachung und Ausführung einer Bandeinheitenlösung beschreiben, finden Sie in Bandspeicherlösung.

Appliance-Lösung für mehrere Standorte

Eine Übersicht über die Tasks, die zur Implementierung einer Appliance-Lösung für mehrere Standorte erforderlich sind, liefern die folgenden Schritte:

1. Starten Sie die Planung für die Lösung, indem Sie die Informationen unter den folgenden Links lesen:
   - AIX: Kapazitätsplanung
   - Linux: Kapazitätsplanung
   - Windows: Kapazitätsplanung
2. Installieren Sie den Server und wahlweise das Operations Center. Lesen Sie die Informationen unter den folgenden Links:
   - Server installieren
   - Installation und Upgrade für das Operations Center durchführen
3. Konfigurieren Sie den Server für Speicher in einem virtuellen Bandarchiv.
   - Virtuelle Bandarchive verwalten
   - Bandeinheiten für den Server anschließen

   Eine Anleitung zur Verbesserung der Systemleistung finden Sie in Bewährte Verfahren bei der Konfiguration.
4. Konfigurieren Sie Maßnahmen zum Schützen Ihrer Daten. Lesen Sie die Informationen in Maßnahmen anpassen.
5. Definieren Sie Clientzeitpläne. Lesen Sie die Informationen in Sicherungs- und Archivierungsoperationen planen.
6. Installieren und konfigurieren Sie Clients. Ausführliche Informationen zur Bestimmung des Typs der erforderlichen Client-Software finden Sie in Clients hinzufügen.
7. Konfigurieren Sie die Überwachung für Ihr System. Lesen Sie die Informationen in Speicherlösungen überwachen.

Zugehörige Verweise:
Vergleich der Datenschutzlösungen
Plattenbasierte Implementierung einer Datenschutzlösung für einen einzelnen Standort
Plattenbasierte Implementierung einer Datenschutzlösung für mehrere Standorte
Appliance-basierte Implementierung einer Datenschutzlösung für mehrere Standorte
Bandbasierte Implementierung einer Datenschutzlösung

Plattenspeicherlösung für einen einzelnen Standort

Diese Datenschutzlösung stellt kosteneffizienten Datenspeicher an einem einzelnen Standort mit minimaler Hardwarekonfiguration bereit.

- Planung für eine Plattenspeicherdatenschutzlösung für einen einzelnen Standort
  Führen Sie die Planung für eine Datenschutzimplementierung durch, die einen Server an einem einzelnen Standort umfasst, der Datendeduplizierung verwendet.
- Implementierung einer Plattenspeicherdatenschutzlösung für einen einzelnen Standort
  Die Plattenspeicherlösung für einen einzelnen Standort wird an einem einzelnen Standort konfiguriert und verwendet Datendeduplizierung und Replikation.
- Plattenspeicherlösung für einen einzelnen Standort überwachen
  Überwachen Sie nach der Implementierung einer Plattenspeicherlösung für einen einzelnen Standort mit IBM Spectrum Protect die Lösung auf ihre korrekte Funktionsweise. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.
- Operationen für eine Plattenspeicherlösung für einen einzelnen Standort verwalten
  Verwenden Sie diese Informationen, um Operationen für eine Plattenspeicherlösung für einen einzelnen Standort mit IBM Spectrum Protect zu verwalten, die einen Server umfasst und Datendeduplizierung für einen einzelnen Standort verwendet.

Planung für eine Plattenspeicherdatenschutzlösung für einen einzelnen Standort

Führen Sie die Planung für eine Datenschutzimplementierung durch, die einen Server an einem einzelnen Standort umfasst, der Datendeduplizierung verwendet.

Implementierungsoptionen

Sie können den Server für eine Plattenspeicherlösung für einen einzelnen Standort wie folgt konfigurieren:

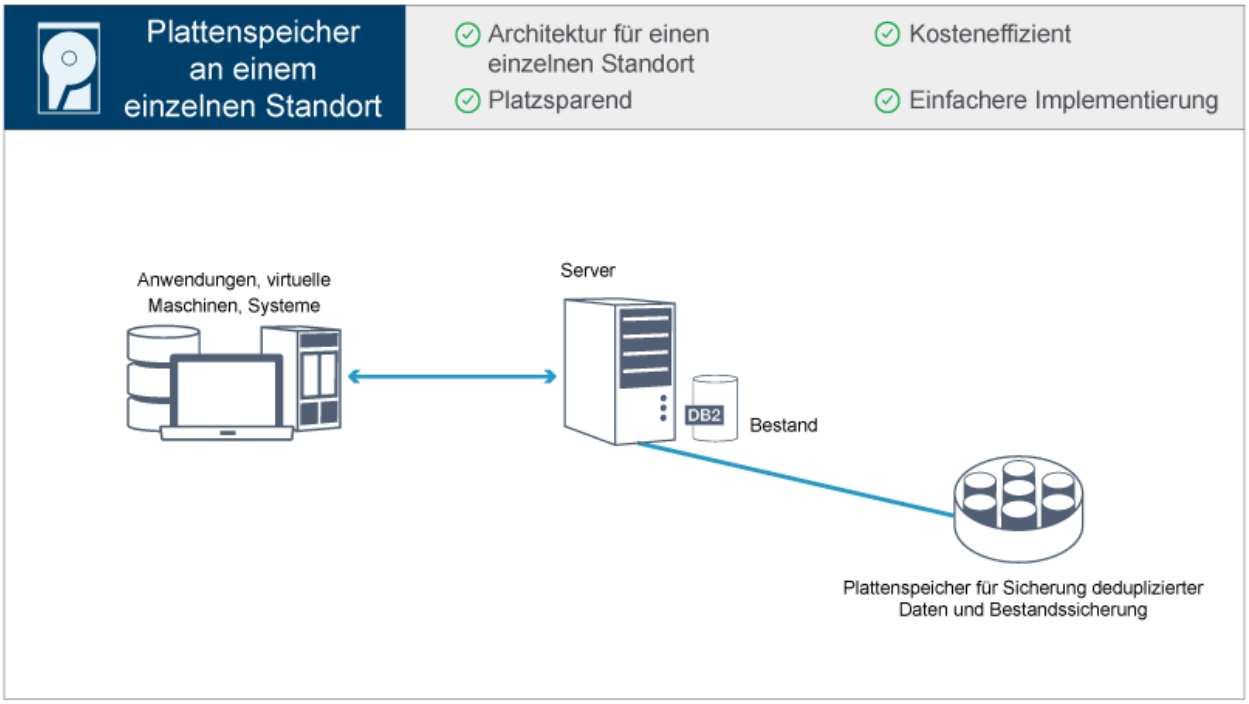
Server unter Verwendung des Operations Center und von Verwaltungsbefehlen konfigurieren
: In dieser Dokumentation werden Schritte zum Konfigurieren einer Reihe von Speichersystemen und der Server-Software für Ihre Lösung bereitgestellt. Konfigurationstasks werden mithilfe von Assistenten und Optionen im Operations Center und mithilfe von IBM Spectrum Protect-Befehlen ausgeführt. Informationen zu ersten Schritten finden Sie in Planungsroadmap.

Server mithilfe automatisierter Scripts konfigurieren
: Eine ausführliche Anleitung zur Implementierung einer Plattenspeicherlösung für einen einzelnen Standort mit bestimmten IBM® Storwize-Speichersystemen sowie zur Verwendung automatisierter Scripts zur Konfiguration des Servers finden Sie in den IBM Spectrum Protect-Blueprints. Die Dokumentation und Scripts sind unter IBM developerWorks verfügbar: IBM Spectrum Protect Blueprints.

  Die Blueprint-Dokumentation umfasst keine Schritte zum Installieren und Konfigurieren des Operations Center oder zum Konfigurieren der sicheren Kommunikation mithilfe von Transport Security Layer (TLS). Eine Option zur Verwendung von Elastic Storage Server-Speicher auf der Basis der Technologie von IBM Spectrum Scale ist eingeschlossen.

Planungsroadmap

Planen Sie eine Plattenspeicherlösung für einen einzelnen Standort, indem Sie das Architekturlayout in der folgenden Abbildung überprüfen und dann die Roadmap-Tasks ausführen, die auf die Abbildung folgen.



Die folgenden Schritte sind für die Planung für eine Plattenspeicherumgebung an einem einzelnen Standort erforderlich.

1. Wählen Sie Ihre Systemgröße aus.
2. Erfüllen Sie die Systemvoraussetzungen für Hardware und Software.
3. Notieren Sie die Werte für Ihre Systemkonfiguration in den Arbeitsblättern zur Planung.
4. Führen Sie die Planung für den Speicher durch.
5. Führen Sie die Planung für die Sicherheit durch.
   a. Führen Sie die Planung für Administratorrollen durch.
   b. Führen Sie die Planung für die sichere Kommunikation durch.
   c. Führen Sie die Planung für verschlüsselte Daten durch.
   d. Führen Sie die Planung für den Firewallzugriff durch.

Systemgröße auswählen

Wählen Sie die Größe des IBM Spectrum Protect-Servers auf der Basis des verwalteten Datenvolumens und der Systeme, die geschützt werden müssen, aus.

Informationen zu diesem Vorgang

Mithilfe der Informationen in der Tabelle können Sie auf der Basis des verwalteten Datenvolumens die erforderliche Größe des Servers bestimmen.

In der folgenden Tabelle ist das Datenvolumen aufgeführt, das von einem Server verwaltet wird. Dieses Volumen umfasst alle Versionen. Das tägliche Datenvolumen gibt an, wie viele neue Daten täglich gesichert werden. Sowohl das Gesamtvolumen der verwalteten Daten als auch das tägliche Volumen an neuen Daten wird als Größe vor jeglicher Datenreduktion gemessen.

Tabelle 1. Größe des Servers bestimmen

Gesamtvolumen der verwalteten Daten	Volumen an täglich zu sichernden neuen Daten	Erforderliche Servergröße
48 TB bis 192 TB	Bis zu 10 TB pro Tag	Klein
200 TB bis 800 TB	10 bis 20 TB pro Tag	Mittelgroß
1000 TB bis 4000 TB	20 bis 100 TB pro Tag	Groß

Die Werte für die tägliche Sicherung in der Tabelle basieren auf Testergebnissen für Objekte mit einer Größe von 128 MB, die von IBM Spectrum Protect for Virtual Environments verwendet werden. Bei Workloads, die aus Objekten bestehen, die kleiner als 128 KB sind, werden diese Grenzwerte für tägliche Sicherungen möglicherweise nicht erreicht.

Systemvoraussetzungen für eine Plattenspeicherlösung für einen einzelnen Standort

Überprüfen Sie nach der Auswahl der besten IBM Spectrum Protect-Lösung für Ihre Datenschutzanforderungen die Systemvoraussetzungen, um die Planung für die Implementierung der Datenschutzlösung auszuführen.

Stellen Sie sicher, dass Ihr System die Hardware- und Softwarevoraussetzungen für die geplante Größe des Servers erfüllt.

- Hardwarevoraussetzungen
  Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.
- Softwarevoraussetzungen
  Die Dokumentation für die IBM Spectrum Protect-Plattenspeicherlösung für einen einzelnen Standort umfasst Installations- und Konfigurationstasks für die folgenden Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

Zugehörige Informationen:
IBM Spectrum Protect Supported Operating Systems

Hardwarevoraussetzungen

Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.

Eine Definition der Systemgrößen finden Sie in Systemgröße auswählen.

In der folgenden Tabelle sind die Hardwaremindestvoraussetzungen für den Server und Speicher auf der Basis der Größe Servers aufgelistet, der erstellt werden soll. Wenn Sie logische Partitionen (LPARs) oder Arbeitspartitionen (WPARs) verwenden, passen Sie die Netzvoraussetzungen an, um den Partitionsgrößen Rechnung zu tragen.

Hardwarekomponente	Kleines System	Mittelgroßes System	Großes System
Serverprozessor	AIX-Betriebssysteme6 Prozessorkerne, 3,42 GHz oder schneller Linux-Betriebssysteme Windows-Betriebssysteme12 Prozessorkerne, 1,9 GHz oder schneller	AIX-Betriebssysteme8 Prozessorkerne, 3,42 GHz oder schneller Linux-Betriebssysteme Windows-Betriebssysteme16 Prozessorkerne, 2,0 GHz oder schneller	AIX-Betriebssysteme20 Prozessorkerne, 3,42 GHz Linux-Betriebssysteme Windows-Betriebssysteme32 Prozessorkerne, 2,0 GHz oder schneller
Serverspeicher	64 GB RAM	128 GB RAM	192 GB RAM

Hardwarekomponente	Kleines System	Mittelgroßes System	Großes System
Netz	• 10 GB Ethernet (1 Port) • 8 GB Fibre Channel-Adapter (2 Ports)	• 10 GB Ethernet (2 Ports) • 8 GB Fibre Channel-Adapter (2 Ports)	• 10 GB Ethernet (4 Ports) • 8 GB Fibre Channel-Adapter (4 Ports)
Speicher	• 1,3 TB Bestand plus Speicherbereich für Operations Center-Datensätze • 46 TB deduplizierter Verzeichniscontainerspeicherpool	• 2 TB Bestand plus Speicherbereich für Operations Center-Datensätze • 200 TB deduplizierter Verzeichniscontainerspeicherpool	• 6 TB Bestand plus Speicherbereich für Operations Center-Datensätze • 1000 TB deduplizierter Verzeichniscontainerspeicherpool

Speicherbedarf für die Datenbank für das Operations Center schätzen

Hardwarevoraussetzungen für das Operations Center sind mit Ausnahme des Speicherbereichs für die Datenbank und das Archivprotokoll (Bestand), den das Operations Center zum Aufnehmen von Datensätzen für verwaltete Clients verwendet, in die vorherige Tabelle eingeschlossen.

Wenn Sie nicht planen, das Operations Center auf demselben System wie den Server zu installieren, können Sie die Systemanforderungen separat schätzen. Informationen zum Berechnen der Systemanforderungen für das Operations Center enthält die Technote 1641684 für die Berechnungsfunktion der Systemanforderungen.

Die Verwaltung des Operations Center auf dem Server stellt eine Workload dar, die zusätzlichen Speicherbereich für Datenbankoperationen erfordert. Wie viel Speicherbereich erforderlich ist, ist von der Anzahl Clients abhängig, die auf einem Server überwacht werden. Lesen Sie die folgenden Richtlinien, um schätzen zu können, wie viel Speicherbereich Ihr Server erfordert.

Speicherbereich in der Datenbank
: Das Operations Center benötigt ungefähr 1,2 GB Speicherbereich in der Datenbank pro 1000 Clients, die auf einem Server überwacht werden. Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1500 Clients. Bei dieser Konfiguration sind insgesamt 6500 Clients auf den vier Servern vorhanden und ungefähr 8,4 GB Speicherbereich in der Datenbank erforderlich. Bei der Berechnung dieses Werts werden die 6500 Clients auf den nächsthöheren Tausenderwert aufgerundet, d. h. auf 7000:

```
7 x 1,2 GB = 8,4 GB
```

Speicherbereich für das Archivprotokoll
: Das Operations Center verwendet alle 24 Stunden ungefähr 8 GB Speicherbereich für das Archivprotokoll pro 1000 Clients. In dem Beispiel mit den 6500 Clients auf dem Hub-Server und den Peripherieservern werden in einem Zeitraum von 24 Stunden für den Hub-Server 56 GB Speicherbereich für das Archivprotokoll verwendet.
Für jeden Peripherieserver in dem Beispiel werden im Verlauf von 24 Stunden etwa 16 GB Speicherbereich für das Archivprotokoll verwendet. Diese Schätzungen basieren auf dem Standardintervall von 5 Minuten zur Erfassung von Statusdaten. Wenn Sie das Erfassungsintervall von einmal alle 5 Minuten auf einmal alle 3 Minuten reduzieren, erhöht sich der Speicherbedarf. Das folgende Beispiel zeigt die ungefähre Erhöhung des Protokollspeicherbedarfs bei einem Erfassungsintervall von einmal alle 3 Minuten:

- Hub-Server: von 56 GB auf ungefähr 94 GB
- Jeder Peripherieserver: von 16 GB auf ungefähr 28 GB

Vergrößern Sie den Speicherbereich für das Archivprotokoll, sodass genügend Speicherbereich zur Unterstützung des Operations Center ohne Auswirkungen auf die vorhandenen Serveroperationen verfügbar ist.

Softwarevoraussetzungen

Die Dokumentation für die IBM Spectrum Protect-Plattenspeicherlösung für einen einzelnen Standort umfasst Installations- und Konfigurationstasks für die folgenden Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

Informationen zu den Softwarevoraussetzungen für IBM® lin_tape-Einheitentreiber finden Sie in der Veröffentlichung IBM Tape Device Drivers Installation and User's Guide.

AIX-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	IBM AIX 7.1 Weitere Informationen zu Betriebssystemvoraussetzungen finden Sie in AIX: Systemmindestvoraussetzungen für AIX-Systeme.

Softwaretyp	Softwaremindestvoraussetzungen
Dienstprogramm gunzip	Das Dienstprogramm gunzip muss auf Ihrem System verfügbar sein, bevor Sie die Installation oder das Upgrade für den IBM Spectrum Protect-Server ausführen. Stellen Sie sicher, dass das Dienstprogramm gunzip installiert ist und der Pfad zu diesem Dienstprogramm in der Umgebungsvariablen PATH definiert ist.
Dateisystemtyp	JFS2-Dateisysteme AIX-Systeme können ein großes Volumen an Dateisystemdaten zwischenspeichern, wodurch der Speicherplatz, der für Server- und IBM DB2-Prozesse erforderlich ist, reduziert werden kann. Um beim AIX-Server eine Auslagerung zu verhindern, verwenden Sie die Mountoption rbrw für das JFS2-Dateisystem. Für den Dateisystemcache wird weniger Speicher verwendet und für IBM Spectrum Protect ist mehr Speicher verfügbar. Verwenden Sie nicht die Mountoptionen für Dateisysteme, gleichzeitige E/A (CIO = Concurrent I/O) und direkte E/A (DIO = Direct I/O) für Dateisysteme, die die IBM Spectrum Protect-Datenbank, Protokolle oder Speicherpooldatenträger enthalten. Diese Optionen können eine Leistungsverschlechterung vieler Serveroperationen zur Folge haben. IBM Spectrum Protect und DB2 können, wenn dies von Vorteil ist, weiterhin DIO verwenden, IBM Spectrum Protect erfordert die Mountoptionen jedoch nicht, um die Vorteile dieser Verfahren selektiv nutzen zu können.
Andere Software	Korn-Shell (ksh)

Linux-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Red Hat Enterprise Linux 7 (x86_64)
Bibliotheken	GNU C-Bibliotheken, Version 2.3.3-98.38 oder höher, die auf dem IBM Spectrum Protect-System installiert sind. Red Hat Enterprise Linux-Server: • libaio • libstdc++.so.6 (32-Bit- und 64-Bit-Pakete sind erforderlich) • numactl.x86_64
Dateisystemtyp	Formatieren Sie datenbankbezogene Dateisysteme mit ext3 oder ext4. Verwenden Sie für speicherpoolbezogene Dateisysteme XFS.
Andere Software	Korn-Shell (ksh)

Windows-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Microsoft Windows Server 2012 R2 (64-Bit) oder Windows Server 2016
Dateisystemtyp	NTFS
Andere Software	Windows 2012 R2 oder Windows 2016 mit .NET Framework 3.5 ist installiert und aktiviert. Die folgenden Benutzerkontensteuerungsrichtlinien müssen inaktiviert sein: • Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto • Benutzerkontensteuerung: Alle Administratoren im Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen

Zugehörige Tasks:
AIX-Netzoptionen definieren

Arbeitsblätter zur Planung

Verwenden Sie die Arbeitsblätter zur Planung für die Aufzeichnung von Werten, die Sie bei der Konfiguration Ihres Systems und bei der Konfiguration des IBM Spectrum Protect-Servers verwenden. Verwenden Sie die Best-Practice-Standardwerte, die in den Arbeitsblättern aufgeführt sind.

Jedes Arbeitsblatt unterstützt Sie bei den Vorbereitungen für unterschiedliche Teile der Systemkonfiguration mithilfe der Best-Practice-Werte:

Vorkonfiguration des Serversystems

Führen Sie mithilfe der Arbeitsblätter zur Vorkonfiguration die Planung für die Dateisysteme und Verzeichnisse aus, die erstellt werden sollen, wenn Sie während der Systemkonfiguration Dateisysteme für IBM Spectrum Protect konfigurieren. Alle Verzeichnisse, die Sie für den Server erstellen, müssen leer sein.

Serverkonfiguration

Verwenden Sie die Arbeitsblätter zur Konfiguration, wenn Sie den Server konfigurieren. Für die meisten Elemente werden Standardwerte vorgeschlagen; andernfalls ist ein entsprechender Hinweis vorhanden.

AIX

Tabelle 1. Arbeitsblatt für die Vorkonfiguration eines AIX-Serversystems

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
TCP/IP-Portadresse für die Kommunikation mit dem Server	1500		Nicht zutreffend	Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren. Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein.
Verzeichnis für die Serverinstanz	/home/tsminst1/tsminst1		50 GB	Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 2.
Verzeichnis für Serverinstallation	/		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	/usr		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	/var		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	/tmp		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	/opt		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 10 GB	
Verzeichnis für die aktive Protokolldatei	/tsminst1/TSMalog		• Klein und mittel: 140 GB • Groß: 300 GB	Wenn Sie die aktive Protokolldatei während der Erstkonfiguration des Servers erstellen, setzen Sie die Größe auf 128 GB.
Verzeichnis für das Archivprotokoll	/tsminst1/TSMarchlog		• Klein: 1 TB • Mittel: 3 TB • Groß: 4 TB	
Verzeichnisse für die Datenbank	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 1 TB • Mittel: Mindestens 2 TB • Groß: Mindestens 4 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank: • Klein: Mindestens 4 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 8 Dateisysteme

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
Verzeichnisse für Speicher	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 38 TB • Mittel: Mindestens 180 TB • Groß: Mindestens 500 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher: • Klein: Mindestens 10 Dateisysteme • Mittel: Mindestens 20 Dateisysteme • Groß: Mindestens 40 Dateisysteme
Verzeichnisse für Datenbanksicherung	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 3 TB • Mittel: Mindestens 10 TB • Groß: Mindestens 16 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank: • Klein: Mindestens 2 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6 Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet.

Tabelle 2. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

Element	Standardwert	Eigener Wert	Anmerkungen
DB2-Instanzeigner	tsminst1		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 1 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner.
Kennwort des DB2-Instanzeigners	passw0rd		Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Primärgruppe für den DB2-Instanzeigner	tsmsrvrs		
Servername	Der Standardwert für den Servernamen ist der Systemhostname.		
Serverkennwort	passw0rd		Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Administrator-ID: Benutzer-ID für die Serverinstanz	admin		
Kennwort für die Administrator-ID	passw0rd		Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Startzeit des Zeitplans	22:00		Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt. Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen.

Linux

Tabelle 3. Arbeitsblatt für die Vorkonfiguration eines Linux-Serversystems

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
TCP/IP-Portadresse für die Kommunikation mit dem Server	1500		Nicht zutreffend	Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren. Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein.
Verzeichnis für die Serverinstanz	/home/tsminst1/tsminst1		25 GB	Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 4.
Verzeichnis für die aktive Protokolldatei	/tsminst1/TSMalog		• Klein und mittel: 140 GB • Groß: 300 GB	
Verzeichnis für das Archivprotokoll	/tsminst1/TSMarchlog		• Klein: 1 TB • Mittel: 3 TB • Groß: 4 TB	
Verzeichnisse für die Datenbank	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 1 TB • Mittel: Mindestens 2 TB • Groß: Mindestens 4 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank: • Klein: Mindestens 4 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 8 Dateisysteme
Verzeichnisse für Speicher	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 38 TB • Mittel: Mindestens 180 TB • Groß: Mindestens 500 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher: • Klein: Mindestens 10 Dateisysteme • Mittel: Mindestens 20 Dateisysteme • Groß: Mindestens 40 Dateisysteme
Verzeichnisse für Datenbanksicherung	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 3 TB • Mittel: Mindestens 10 TB • Groß: Mindestens 16 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank: • Klein: Mindestens 2 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6 Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet.

Tabelle 4. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

Element	Standardwert	Eigener Wert	Anmerkungen

Element	Standardwert	Eigener Wert	Anmerkungen
DB2-Instanzeigner	tsminst1		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 3 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner.
Kennwort des DB2-Instanzeigners	passw0rd		Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Primärgruppe für den DB2-Instanzeigner	tsmsrvrs		
Servername	Der Standardwert für den Servernamen ist der Systemhostname.		
Serverkennwort	passw0rd		Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Administrator-ID: Benutzer-ID für die Serverinstanz	admin		
Kennwort für die Administrator-ID	passw0rd		Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Startzeit des Zeitplans	22:00		Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt. Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen.

Windows

Da für den Server viele Datenträger erstellt werden, konfigurieren Sie den Server mithilfe der Windows-Funktion zum Zuordnen von Plattendatenträgern zu Verzeichnissen (statt der Funktion zum Zuordnen von Plattendatenträgern zu Laufwerkbuchstaben).

Beispielsweise ist C:\tsminst1\TSMdbpsace00 ein Mountpunkt für einen Datenträger mit eigenem Speicherbereich. Der Datenträger wird einem Verzeichnis unter dem Laufwerk C: zugeordnet, nimmt aber keinen Speicherbereich auf Laufwerk C: in Anspruch. Einzige Ausnahme ist das Serverinstanzverzeichnis, C:\tsminst1, das ein Mountpunkt oder ein normales Verzeichnis sein kann.

Tabelle 5. Arbeitsblatt für die Vorkonfiguration eines Windows-Serversystems

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
TCP/IP-Portadresse für die Kommunikation mit dem Server	1500		Nicht zutreffend	Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren. Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein.
Verzeichnis für die Serverinstanz	C:\tsminst1		25 GB	Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 6.

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
Verzeichnis für die aktive Protokolldatei	C:\tsminst1\TSMalog		• Klein und mittel: 140 GB • Groß: 300 GB	
Verzeichnis für das Archivprotokoll	C:\tsminst1\TSMarchlog		• Klein: 1 TB • Mittel: 3 TB • Groß: 4 TB	
Verzeichnisse für die Datenbank	C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 1 TB • Mittel: Mindestens 2 TB • Groß: Mindestens 4 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank: • Klein: Mindestens 4 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 8 Dateisysteme
Verzeichnisse für Speicher	C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 38 TB • Mittel: Mindestens 180 TB • Groß: Mindestens 500 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher: • Klein: Mindestens 10 Dateisysteme • Mittel: Mindestens 20 Dateisysteme • Groß: Mindestens 40 Dateisysteme
Verzeichnisse für Datenbanksicherung	C:\tsminst1\TSMbkup00 C:\tsminst1\TSMbkup01 C:\tsminst1\TSMbkup02 C:\tsminst1\TSMbkup03		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 3 TB • Mittel: Mindestens 10 TB • Groß: Mindestens 16 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank: • Klein: Mindestens 2 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6 Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet.

Tabelle 6. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

Element	Standardwert	Eigener Wert	Anmerkungen
DB2-Instanzeigner	tsminst1		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 5 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner.
Kennwort des DB2-Instanzeigners	pAssW0rd		Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Servername	Der Standardwert für den Servernamen ist der Systemhostname.		

Element	Standardwert	Eigener Wert	Anmerkungen
Serverkennwort	passw0rd		Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Administrator-ID: Benutzer-ID für die Serverinstanz	admin		
Kennwort für die Administrator-ID	passw0rd		Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Startzeit des Zeitplans	22:00		Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt. Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen.

Planung für Speicher

Wählen Sie die effektivste Speichertechnologie für IBM Spectrum Protect-Komponenten aus, um effiziente Serverleistung und Serveroperationen zu gewährleisten.

Speicherhardwareeinheiten haben unterschiedliche Kapazitäts- und Leistungsmerkmale, die festlegen, wie die Einheiten effizient mit IBM Spectrum Protect verwendet werden können. Die folgenden Richtlinien stellen eine allgemeine Anleitung zur Auswahl der für Ihre Lösung geeigneten Speicherhardware und Konfiguration dar.

Datenbank und aktive Protokolldatei

- Verwenden Sie eine schnelle Platte für die IBM Spectrum Protect-Datenbank und die aktive Protokolldatei, die beispielsweise die folgenden Merkmale hat:
  - Hochleistungsplatte mit 15.000 Umdrehungen pro Minute mit Fibre Channel- oder SAS-Schnittstelle
  - Solid-State-Platte (SSD)
- Trennen Sie die aktive Protokolldatei von der Datenbank, es sei denn, Sie verwenden SSD oder Flash-Hardware.
- Verwenden Sie beim Erstellen von Arrays für die Datenbank RAID-Stufe 5.

Speicherpool

- Sie können kostengünstigere und langsamere Platten für den Speicherpool verwenden.
- Der Speicherpool kann Platten für den Speicher für das Archivprotokoll und die Datenbanksicherung gemeinsam nutzen.
- Verwenden Sie RAID-Stufe 6 für Speicherpoolarrays, um bei Verwendung von Typen großer Platten Schutz vor Laufwerkdoppelfehlern hinzuzufügen.

- Planung der Speicherarrays
  Bereiten Sie die Konfiguration des Plattenspeichers vor, indem Sie die Planung für RAID-Arrays und Datenträger gemäß der Größe Ihres IBM Spectrum Protect-Systems ausführen.

Zugehörige Verweise:
Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten

Planung für Sicherheit

Planen Sie den Schutz der Sicherheit von Systemen in der IBM Spectrum Protect-Lösung mithilfe von Steuerelementen für Zugriff und Authentifizierung und ziehen Sie das Verschlüsseln von Daten und der Übertragung von Kennwörtern in Erwägung.

- Planung für Administratorrollen
  Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.

- Planung für sichere Kommunikation
  Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.
- Planung für die Speicherung verschlüsselter Daten
  Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie für Ihre Anforderungen am besten geeignete Option aus.
- Planung des Firewallzugriffs
  Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

Planung für Administratorrollen

Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.

Sie können Administratoren eine der folgenden Berechtigungsstufen zuordnen:

Systemberechtigung
: Administratoren mit Systemberechtigung verfügen über die höchste Berechtigungsstufe. Administratoren mit dieser Berechtigungsstufe können jede Task ausführen. Sie können alle Maßnahmendomänen und Speicherpools verwalten und anderen Administratoren Berechtigung erteilen.

Maßnahmenberechtigung
: Administratoren mit Maßnahmenberechtigung können alle Tasks verwalten, die sich auf die Maßnahmenverwaltung beziehen. Diese Berechtigung kann uneingeschränkt sein oder auf bestimmte Maßnahmendomänen eingeschränkt werden.

Speicherberechtigung
: Administratoren mit Speicherberechtigung können Speicherressourcen für den Server zuordnen und steuern.

Bedienerberechtigung
: Administratoren mit Bedienerberechtigung können den sofortigen Betrieb des Servers und die Verfügbarkeit von Speichermedien wie beispielsweise Bandarchiven und -laufwerken steuern.

Die Szenarios in Tabelle 1 enthalten Beispiele, die zeigen, warum es sinnvoll ist, Administratoren für die Ausführung von Tasks unterschiedliche Berechtigungsstufen zuzuordnen:

Tabelle 1. Szenarios für Administratorrollen

Szenario	Typ der zu konfigurierenden Administrator-ID
Ein Administrator in einem kleinen Unternehmen verwaltet den Server und ist für alle Serveraktivitäten verantwortlich.	• Systemberechtigung: 1 Administrator-ID
Ein Administrator für mehrere Server verwaltet auch das gesamte System. Mehrere andere Administratoren verwalten ihre eigenen Speicherpools.	• Systemberechtigung auf allen Servern: 1 Administrator-ID für den Administrator des gesamten Systems • Speicherberechtigung für bestimmte Speicherpools: 1 Administrator-ID für jeden der anderen Administratoren
Ein Administrator verwaltet 2 Server. Eine andere Person unterstützt ihn bei den Verwaltungstasks. Zwei Assistenten müssen sicherstellen, dass wichtige Systeme gesichert werden. Jeder Assistent ist für die Überwachung der geplanten Sicherungen auf einem der IBM Spectrum Protect-Server verantwortlich.	• Systemberechtigung auf beiden Servern: 2 Administrator-IDs • Bedienerberechtigung: 2 Administrator-IDs für die Assistenten mit Zugriff auf den Server, für den die jeweilige Person verantwortlich ist.

Planung für sichere Kommunikation

Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.

Bestimmen Sie auf der Basis der Regelungen und Geschäftsanforderungen für Ihr Unternehmen, welche Stufe des Schutzes für Ihre Daten erforderlich ist.

Wenn Ihr Unternehmen ein hohes Maß an Sicherheit für Kennwörter und die Datenübertragung erfordert, planen Sie die Implementierung der sicheren Kommunikation mit dem Protokoll Transport Layer Security (TLS) oder Secure Sockets Layer (SSL).

TLS und SSL stellen sichere Kommunikation zwischen dem Server und dem Client bereit, können sich jedoch auf die Systemleistung auswirken. Um die Systemleistung zu verbessern, verwenden Sie TLS für die Authentifizierung, ohne Objektdaten zu verschlüsseln. Informationen zur Angabe, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, finden Sie in der Beschreibung der Clientoption SSL für die Client/Server-Kommunikation und der Beschreibung des Parameters UPDATE SERVER=SSL für die Kommunikation zwischen Servern. Ab Version 8.1.2 wird TLS standardmäßig für die Authentifizierung verwendet. Wenn Sie sich für die Verwendung von TLS entscheiden, um vollständige Sitzungen zu verschlüsseln, verwenden Sie das Protokoll nur für Sitzungen, für die es erforderlich ist; fügen Sie außerdem auf dem Server Prozessorressourcen hinzu, um den wachsenden Datenaustausch im Netz handhaben zu können. Sie können auch versuchsweise andere Optionen verwenden. Beispielsweise stellen einige Netzeinheiten wie Router und Switches die TLS- oder SSL-Funktion bereit.

Mithilfe von TLS und SSL können Sie einige oder alle der unterschiedlichen möglichen Kommunikationspfade schützen, beispielsweise:

- Operations Center: vom Browser zum Hub-Server; vom Hub-Server zum Peripherieserver

- Vom Client zum Server
- Vom Server zum Server: Knotenreplikation

Zugehörige Tasks:
Kommunikation schützen

Planung für die Speicherung verschlüsselter Daten

Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie für Ihre Anforderungen am besten geeignete Option aus.

Wenn Ihr Unternehmen die Verschlüsselung der Daten in Speicherpools erfordert, können Sie entweder die IBM Spectrum Protect-Verschlüsselung oder eine externe Einheit wie beispielsweise ein Band für die Verschlüsselung verwenden.

Wenn Sie IBM Spectrum Protect zum Verschlüsseln der Daten auswählen, sind zusätzliche IT-Ressourcen auf dem Client erforderlich, die sich auf die Leistung von Sicherungs- und Zurückschreibungsprozessen auswirken können.

Zugehörige Informationen:
Technote 1963635

Planung des Firewallzugriffs

Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

In Tabelle 1 sind die Ports beschrieben, die vom Server, vom Client und vom Operations Center verwendet werden.

Tabelle 1. Vom Server, Client und Operations Center verwendete Ports

Element	Standardwert	Richtung	Beschreibung
Basisport (TCPPORT)	1500	Abgehend/Eingehend	Jede Serverinstanz erfordert einen eindeutigen Port. Sie können eine alternative Portnummer angeben, anstatt den Standardwert zu verwenden. Der mit der Option TCPPORT angegebene Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen vom Client empfangsbereit. Für den Datenverkehr des Verwaltungsclients können Sie zum Festlegen von Portwerten die Optionen TCPADMINPORT und ADMINONCLIENTPORT verwenden.
Port ausschließlich für SSL (SSLTCPPORT)	Kein Standardwert	Abgehend/Eingehend	Dieser Port wird verwendet, wenn die Kommunikation am Port auf ausschließlich SSL-fähige Sitzungen beschränkt werden soll. Um sowohl die SSL-Kommunikation als auch die Nicht-SSL-Kommunikation zu unterstützen, verwenden Sie die Option TCPPORT oder TCPADMINPORT.
SMB	45	Eingehend/Abgehend	Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.
SSH	22	Eingehend/Abgehend	Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.
SMTP	25	Abgehend	Dieser Port wird zum Senden von E-Mail-Alerts vom Server verwendet.
NDMP	Kein Standardwert	Eingehend/Abgehend	Der Server muss eine abgehende NDMP-Steuerportverbindung zu der NAS-Einheit öffnen können. Der abgehende Steuerport ist die Adresse der unteren Ebene in der Definition der Einheit zum Versetzen von Daten für die NAS-Einheit. Während einer NDMP-Zurückschreibung vom Dateiserver auf den Server muss der Server eine abgehende NDMP-Datenverbindung zu der NAS-Einheit öffnen können. Der Datenverbindungsport, der während einer Zurückschreibung verwendet wird, kann auf der NAS-Einheit konfiguriert werden. Während NDMP-Sicherungen vom Dateiserver auf den Server muss die NAS-Einheit abgehende Datenverbindungen zum Server öffnen können und der Server muss eingehende NDMP-Datenverbindungen akzeptieren können. Mithilfe der Serveroption NDMPPORTRANGE können Sie die für die Verwendung als NDMP-Datenverbindungen verfügbare Gruppe von Ports einschränken. Sie können eine Firewall für Verbindungen zu diesen Ports konfigurieren.

Element	Standardwert	Richtung	Beschreibung
Replikation	Kein Standardwert	Abgehend/Eingehend	Der Port und das Protokoll für den Port für abgehende Daten für die Replikation werden mit dem Befehl DEFINE SERVER festgelegt, der zum Konfigurieren der Replikation verwendet wird. Bei den Ports für eingehende Daten für die Replikation handelt es sich um die TCP-Ports und SSL-Ports, die für den Quellenserver im Befehl DEFINE SERVER angegeben werden.
Port für Clientzeitplan	Client-Port: 1501	Abgehend	Der Client ist an dem angegebenen Port empfangsbereit und teilt die Portnummer dem Server mit. Der Server kontaktiert den Client, wenn die servergesteuerte Zeitplanung verwendet wird. Sie können eine alternative Portnummer in der Clientoptionsdatei angeben.
Lange laufende Sitzungen	Einstellung für KEEPALIVE: YES	Abgehend	Wenn die Option KEEPALIVE aktiviert ist, werden während Client/Server-Sitzungen Keepalive-Pakete gesendet, um zu verhindern, dass die Firewall-Software lange laufende inaktive Verbindungen schließt.
Operations Center	HTTPS: 11090	Eingehend	Diese Ports werden für den Web-Browser des Operations Center verwendet. Sie können eine alternative Portnummer angeben.
Port für den Clientverwal-tungsservice	Client-Port: 9028	Eingehend	Der Zugriff auf den Port für den Clientverwaltungsservice muss über das Operations Center möglich sein. Stellen Sie sicher, dass Verbindungen nicht durch Firewalls verhindert werden können. Der Clientverwaltungsservice verwendet den TCP-Port des Servers für den Clientknoten für die Authentifizierung unter Verwendung einer Verwaltungssitzung.

Implementierung einer Plattenspeicherdatenschutzlösung für einen einzelnen Standort

Die Plattenspeicherlösung für einen einzelnen Standort wird an einem einzelnen Standort konfiguriert und verwendet Datendeduplizierung und Replikation.

Implementierungsroadmap

Die folgenden Schritte sind zum Konfigurieren der IBM Spectrum Protect-Plattenspeicherumgebung an einem einzelnen Standort erforderlich.

1. Konfigurieren Sie das System.
    a. Konfigurieren Sie die Speicherhardware und Speicherarrays für Ihre Umgebungsgröße.
    b. Installieren Sie das Serverbetriebssystem.
    c. Konfigurieren Sie Multipath I/O.
    d. Erstellen Sie die Benutzer-ID für die Serverinstanz.
    e. Bereiten Sie Dateisysteme für IBM Spectrum Protect vor.
2. Installieren Sie den Server und das Operations Center.
3. Konfigurieren Sie den Server und das Operations Center.
    a. Führen Sie die Erstkonfiguration des Servers aus.
    b. Legen Sie Serveroptionen fest.
    c. Konfigurieren Sie Secure Sockets Layer für den Server und den Client.
    d. Konfigurieren Sie das Operations Center.
    e. Registrieren Sie Ihre IBM Spectrum Protect-Lizenz.
    f. Konfigurieren Sie die Datendeduplizierung.
    g. Definieren Sie Datenaufbewahrungsregeln für Ihr Unternehmen.
    h. Definieren Sie Zeitpläne für die Serververwaltung.
    i. Definieren Sie Clientzeitpläne.
4. Installieren und konfigurieren Sie Clients.
    a. Registrieren Sie Clients und ordnen Sie Clients Zeitplänen zu.
    b. Installieren und überprüfen Sie den Clientverwaltungsservice.
    c. Konfigurieren Sie das Operations Center für die Verwendung des Clientverwaltungsservice.
5. Schließen Sie die Implementierung ab.

System konfigurieren

Um das System konfigurieren zu können, müssen Sie zunächst Ihre Plattenspeicherhardware und das Serversystem für IBM Spectrum Protect konfigurieren.

- Speicherhardware konfigurieren
  Um Ihre Speicherhardware zu konfigurieren, lesen Sie die allgemeine Anleitung für Plattensysteme und IBM Spectrum Protect.
- Serverbetriebssystem installieren
  Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.
- Multipath I/O konfigurieren
  Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.
- Benutzer-ID für den Server erstellen
  Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.
- Dateisysteme für den Server vorbereiten
  Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

Speicherhardware konfigurieren

Um Ihre Speicherhardware zu konfigurieren, lesen Sie die allgemeine Anleitung für Plattensysteme und IBM Spectrum Protect.

Vorgehensweise

1. Stellen Sie unter Berücksichtigung der folgenden Richtlinien eine Verbindung zwischen dem Server und den Speichereinheiten her:
   - Verwenden Sie einen Switch oder eine Direktverbindung für Fibre Channel-Verbindungen.
   - Berücksichtigen Sie die Anzahl Ports, die verbunden sind, und die erforderliche Bandbreite.
   - Berücksichtigen Sie die Anzahl Ports auf dem Server und die Anzahl Host-Ports auf dem Plattensystem, die verbunden sind.
2. Stellen Sie sicher, dass die Einheitentreiber und die Firmware für das Serversystem, die Adapter und das Betriebssystem aktuell sind und die empfohlenen Versionen haben.
3. Konfigurieren Sie Speicherarrays. Stellen Sie sicher, dass Sie entsprechend geplant haben, um die optimale Leistung zu gewährleisten. Weitere Informationen finden Sie in Planung für Speicher.
4. Stellen Sie sicher, dass das Serversystem Zugriff auf Plattendatenträger hat, die erstellt werden. Führen Sie die folgenden Schritte aus:
   a. Wenn das System mit einem Fibre Channel-Switch verbunden ist, verzonen Sie den Server, um die Platten anzuzeigen.
   b. Ordnen Sie alle Datenträger zu, um dem Plattensystem mitzuteilen, dass diesem spezifischen Server die Anzeige jeder Platte ermöglicht werden soll.

Serverbetriebssystem installieren

Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.

- Installation auf AIX-Systemen
  Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.
- Installation auf Linux-Systemen
  Führen Sie die folgenden Schritte aus, um Linux x86_64 auf dem Serversystem zu installieren.
- Installation auf Windows-Systemen
  Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

Installation auf AIX-Systemen

Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.

Vorgehensweise

1. Installieren Sie AIX Version 7.1, TL4, SP2 oder höher gemäß den Anweisungen des Herstellers.
2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.
3. Öffnen Sie die Datei /etc/hosts und führen Sie die folgenden Aktionen aus:
   - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

     ```
     127.0.0.1  localhost
     ```

4. Aktivieren Sie die AIX-I/O Completion Ports (IOCP), indem Sie den folgenden Befehl eingeben:

   ```
   chdev -l iocp0 -P
   ```

   Die Olson-Zeitzonendefinition kann sich auf die Serverleistung auswirken.

5. Um die Leistung zu optimieren, ändern Sie Ihr Systemzeitzonenformat von Olson in POSIX. Verwenden Sie das folgende Befehlsformat zum Aktualisieren der Zeitzoneneinstellung:

   ```
   chtz=Ortszeitzone,Datum/Uhrzeit,Datum/Uhrzeit
   ```

   Beispielsweise würden Sie in Tucson, Arizona, wo die Mountain Standard Time gilt, den folgenden Befehl ausgeben, um das Format in das POSIX-Format zu ändern:

   ```
   chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
   ```

6. Fügen Sie in .profile des Instanzbenutzers einen Eintrag hinzu, um die folgende Umgebung festzulegen:

   ```
   export MALLOCOPTIONS=multiheap:16
   ```

7. Legen Sie fest, dass das System vollständige Anwendungskerndateien erstellen soll. Geben Sie den folgenden Befehl aus:

   ```
   chdev -l sys0 -a fullcore=true -P
   ```

8. Stellen Sie für die Kommunikation mit dem Server und dem Operations Center sicher, dass die folgenden Ports für alle Firewalls, die gegebenenfalls vorhanden sind, offen sind:
   - Öffnen Sie für die Kommunikation mit dem Server Port 1500.
   - Öffnen Sie für die sichere Kommunikation mit dem Operations Center Port 11090 auf dem Hub-Server.

   Wenn Sie nicht die Standardwerte für Ports verwenden, stellen Sie sicher, dass die verwendeten Ports offen sind.

9. Aktivieren Sie TCP-Hochleistungsverbesserungen. Geben Sie den folgenden Befehl aus:

   ```
   no -p -o rfc1323=1
   ```

10. Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, kombinieren Sie vier 10-Gb-Ethernet-Ports durch Bonding miteinander. Verwenden Sie das System Management Interface Tool (SMIT), um die Ports durch Bonding unter Verwendung von Etherchannel zu kombinieren. Beim Testen wurden die folgenden Einstellungen verwendet:

    ```
    mode            8023ad
    auto_recovery   yes             Automatische Wiederherstellung nach
                                    Übernahme aktivieren
    backup_adapter  NONE            Adapter, der beim Fehlschlagen des
                                    gesamten Kanals verwendet wird
    hash_mode       src_dst_port    Legt fest, wie der abgehende Adapter
                                    ausgewählt wird
    interval        long            Legt den Intervallwert für den IEEE-Modus
                                    802.3ad fest
    mode            8023ad          EtherChannel-Betriebsart
    netaddr         0               Mit Ping zu überprüfende Adresse
    noloss_failover yes             Verlustfreie Übernahme nach dem Fehl-
                                    schlagen des Pingbefehls aktivieren
    num_retries     3               Anzahl Wiederholungen für Pingbefehl vor
                                    dem Fehlschlagen
    retry_time      1               Wartezeit (in Sekunden) zwischen
                                    Pingbefehlen
    use_alt_addr    no              Alternative EtherChannel-Adresse
                                    aktivieren
    use_jumbo_frame no              Jumbo-Frames für Gigabit Ethernet
                                    aktivieren
    ```

11. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 1 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

    Tabelle 1. Benutzergrenzwerte (ulimit-Werte)

Typ des Benutzergrenzwerts	Einstellung	Wert	Befehl zum Abfragen des Werts
Maximale Größe der erstellten Kerndateien	core	Unlimited	`ulimit -Hc`
Maximale Größe eines Datensegments für einen Prozess	data	Unlimited	`ulimit -Hd`
Maximale Dateigröße	fsize	Unlimited	`ulimit -Hf`
Maximale Anzahl offener Dateien	nofile	65536	`ulimit -Hn`
Maximale Prozessorzeit in Sekunden	cpu	Unlimited	`ulimit -Ht`
Maximale Anzahl Benutzerprozesse	nproc	16384	`ulimit -Hu`

    Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

Installation auf Linux-Systemen

Führen Sie die folgenden Schritte aus, um Linux x86_64 auf dem Serversystem zu installieren.

Vorbereitende Schritte

Das Betriebssystem wird auf den internen Festplatten installiert. Konfigurieren Sie die internen Festplatten für die Verwendung eines RAID 1-Hardware-Arrays. Wenn Sie beispielsweise ein kleines System konfigurieren, werden die beiden internen 300-GB-Platten in RAID 1 gespiegelt, sodass es aussieht, als würde dem Installationsprogramm des Betriebssystems eine einzelne 300-GB-Platte zur Verfügung stehen.

Vorgehensweise

1. Installieren Sie Red Hat Enterprise Linux Version 7.1 oder höher gemäß den Anweisungen des Herstellers. Fordern Sie eine bootfähige DVD an, die Red Hat Enterprise Linux Version 7.1 enthält, und starten Sie Ihr System von dieser DVD. Für Installationsoptionen siehe die folgende Anleitung. Wenn ein Element in der folgenden Liste nicht aufgeführt ist, übernehmen Sie die Standardauswahl unverändert.
   a. Wählen Sie nach dem Starten der DVD im Menü Install or upgrade an existing system (Installation oder Aktualisierung eines bestehenden Systems) aus.
   b. Wählen Sie in der Eingangsanzeige Test this media & install Red Hat Enterprise Linux 7.1 (Diese Median überprüfen & Red Hat Enterprise Linux 7.1 installieren) aus.
   c. Wählen Sie Ihre Sprache und Tastaturbelegung aus.
   d. Wählen Sie Ihren Standort aus, um die korrekte Zeitzone festzulegen.
   e. Wählen Sie Software Selection (Softwareauswahl) und in der nächsten Anzeige Server with GUI (Server mit GUI) aus.
   f. Klicken Sie auf der Installationszusammenfassungsseite auf Installation Destination (Installationsziel) und überprüfen Sie die folgenden Einträge:
      - Die lokale 300-GB-Platte ist als Installationsziel ausgewählt.
      - Unter 'Other Storage Options' (Weitere Speicheroptionen) ist Automatically configure partitioning (Partitionierung automatisch konfigurieren) ausgewählt.

      Klicken Sie auf Done (Fertig).
   g. Klicken Sie auf Begin Installation (Installation starten). Legen Sie nach dem Start der Installation das Rootkennwort für Ihr Rootbenutzerkonto fest.

   Führen Sie nach dem Abschluss der Installation einen Neustart für das System durch und melden Sie sich als Rootbenutzer an. Geben Sie den Befehl df aus, um die Basispartitionierung zu überprüfen. Auf einem Testsystem hatte die Erstpartitionierung beispielsweise das folgende Ergebnis zur Folge:

```
[root@tvapp02]# df -h
Filesystem             Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G   1% /dev/shm
tmpfs                   32G  8.8M   32G   1% /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.
   Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, sollten Sie das Bonding mehrerer Netzports in Erwägung ziehen. Erstellen Sie dazu eine LACP-Netzverbindung (LACP = Link Aggregation Control Protocol), bei der mehrere untergeordnete Ports in einer einzigen logischen Verbindung aggregiert werden. Die bevorzugte Methode ist die Verwendung des Bondmodus 802.3ad, des Werts 100 für die Einstellung miimon und der Angabe 'layer3+4' für die Einstellung xmit_hash_policy.
   Einschränkung: Um eine LACP-Netzverbindung verwenden zu können, muss ein Netzswitch vorhanden sein, der LACP unterstützt.

   Weitere Anweisungen zur Konfiguration von Bonding-Netzverbindungen mit Red Hat Enterprise Linux Version 7 finden Sie unter Create a Channel Bonding Interface.

3. Öffnen Sie die Datei /etc/hosts und führen Sie die folgenden Aktionen aus:
   - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

     ```
     127.0.0.1  localhost
     ```

4. Installieren Sie Komponenten, die für die Serverinstallation erforderlich sind. Führen Sie die folgenden Schritte aus, um ein YUM-Repository (YUM = Yellowdog Updater, Modified) zu erstellen und die vorausgesetzten Pakete zu installieren.
   a. Stellen Sie die DVD für die Installation von Red Hat Enterprise Linux in einem Systemverzeichnis bereit. Um sie beispielsweise im Verzeichnis /mnt bereitzustellen, geben Sie den folgenden Befehl aus:

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

   b. Überprüfen Sie, ob die DVD bereitgestellt wurde, indem Sie den Befehl mount ausgeben. Es sollte eine ähnliche Ausgabe wie in dem folgenden Beispiel angezeigt werden:

```
/dev/sr0 on /mnt type iso9660
```

c. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

```
cd /etc/yum/repos.d
```

Wenn das Verzeichnis repos.d nicht vorhanden ist, erstellen Sie es.

d. Listen Sie den Verzeichnisinhalt auf:

```
ls rhel-source.repo
```

e. Benennen Sie die ursprüngliche repo-Datei um, indem Sie den Befehl mv ausgeben. Beispiel:

```
mv rhel-source.repo rhel-source.repo.orig
```

f. Erstellen Sie mithilfe eines Texteditors eine neue repo-Datei. Um beispielsweise den Editor vi zu verwenden, geben Sie den folgenden Befehl aus:

```
vi rhel71_dvd.repo
```

g. Fügen Sie der neuen repo-Datei die folgenden Zeilen hinzu. Der Parameter baseurl gibt den Verzeichnismountpunkt an:

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

h. Installieren Sie das vorausgesetzte Paket ksh.x86_64, indem Sie den Befehl yum ausgeben. Beispiel:

```
yum install ksh.x86_64
```

Ausnahme: Sie müssen die Bibliotheken compat-libstdc++-33-3.2.3-69.el6.i686 und libstdc++.i686 für Red Hat Enterprise Linux Version 7.1 nicht installieren.

5. Wenn die Softwareinstallation abgeschlossen ist, können Sie die ursprünglichen YUM-Repository-Werte zurückschreiben, indem Sie die folgenden Schritte ausführen:
   a. Heben Sie die Bereitstellung der DVD für die Installation von Red Hat Enterprise Linux auf, indem Sie den folgenden Befehl ausgeben:

```
unmount /mnt
```

   b. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

```
cd /etc/yum/repos.d
```

   c. Benennen Sie die von Ihnen erstellte repo-Datei um:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

   d. Benennen Sie die ursprüngliche Datei wieder in den ursprünglichen Namen um:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Bestimmen Sie, ob Änderungen an Kernelparametern erforderlich sind. Führen Sie die folgenden Schritte aus:
   a. Listen Sie mithilfe des Befehls sysctl -a die Parameterwerte auf.
   b. Analysieren Sie die Ergebnisse anhand der Richtlinien in Tabelle 1, um zu bestimmen, ob Änderungen erforderlich sind.
   c. Wenn Änderungen erforderlich sind, definieren Sie die Parameter in der Datei /etc/sysctl.conf. Die Dateiänderungen werden angewendet, wenn das System gestartet wird.

Tipp: Passen Sie Kernelparametereinstellungen automatisch an und eliminieren Sie die Notwendigkeit manueller Aktualisierungen dieser Einstellungen. Unter Linux passt die DB2-Datenbanksoftware automatisch die Werte der Kernelparameter für die Interprozesskommunikation (IPC) an und setzt sie auf die bevorzugten Einstellungen. Weitere Informationen zu Kernelparametereinstellungen finden Sie bei Verwendung des Suchbegriffs Linux-Kernelparameter im IBM DB2 Version 11.1 Knowledge Center.

Tabelle 1. Optimale Einstellungen für Linux-Kernelparameter

Parameter	**Beschreibung**
kernel.shmmni	Die maximale Anzahl Segmente.
kernel.shmmax	Die maximale Größe eines gemeinsam genutzten Speichersegments (Byte). Dieser Parameter muss definiert werden, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird.
kernel.shmall	Die maximale Zuordnung von Seiten im gemeinsam genutzten Speicher (Seiten).

Parameter	Beschreibung
kernel.sem Für den Parameter kernel.sem gibt es vier Werte.	(SEMMSL) Die maximale Anzahl Semaphore pro Array.
	(SEMMNS) Die maximale Anzahl Semaphore pro System.
	(SEMOPM) Die maximale Anzahl Operationen pro Semaphoraufruf.
	(SEMMNI) Die maximale Anzahl Arrays.
kernel.msgmni	Die maximale Anzahl systemweiter Nachrichtenwarteschlangen.
kernel.msgmax	Die maximale Größe von Nachrichten (Byte).
kernel.msgmnb	Die standardmäßige maximale Größe der Warteschlange (Byte).
kernel.randomize_va_space	Mit dem Parameter kernel.randomize_va_space wird die Verwendung von Speicher-ASLR für den Kernel konfiguriert. Inaktivieren Sie ASLR, da ASLR Fehler der DB2-Software zur Folge haben kann. Weitere ausführliche Informationen zu Linux-ASLR und DB2 enthält die Technote 1365583.
vm.swappiness	Der Parameter vm.swappiness definiert, ob der Kernel Anwendungsspeicher aus physischem Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.
vm.overcommit_memory	Der Parameter vm.overcommit_memory hat Auswirkungen darauf, wie viel virtueller Speicher gemäß dem Kernel zugeordnet werden kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.

7. Öffnen Sie Firewall-Ports für die Kommunikation mit dem Server. Führen Sie die folgenden Schritte aus:
   a. Legen Sie die von der Netzschnittstelle verwendete Zone fest. Die Zone ist standardmäßig 'public'.
      Geben Sie den folgenden Befehl aus:

      ```
      #  firewall-cmd --get-active-zones
      public
        interfaces: ens4f0
      ```

   b. Um die Standardportadresse für die Kommunikation mit dem Server zu verwenden, öffnen Sie TCP/IP-Port 1500 in der Linux-Firewall.
      Geben Sie den folgenden Befehl aus:

      ```
      firewall-cmd --zone=public --add-port=1500/tcp --permanent
      ```

      Wenn ein anderer Wert als der Standardwert verwendet werden soll, können Sie eine Zahl zwischen 1024 und 32767 angeben. Wenn ein anderer Port als der Standardport geöffnet wird, müssen Sie diesen Port bei der Ausführung des Konfigurationsscripts angeben.

   c. Wenn Sie planen, dieses System als einen Hub zu verwenden, öffnen Sie Port 11090, den Standardport für die sichere Kommunikation (HTTPS).
      Geben Sie den folgenden Befehl aus:

      ```
      firewall-cmd --zone=public --add-port=11090/tcp --permanent
      ```

   d. Laden Sie die Firewalldefinitionen erneut, damit die Änderungen wirksam werden.
      Geben Sie den folgenden Befehl aus:

      ```
      firewall-cmd --reload
      ```

8. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 2 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 2. Benutzergrenzwerte (ulimit-Werte)

Typ des Benutzergrenzwerts	Einstellung	Wert	Befehl zum Abfragen des Werts
Maximale Größe der erstellten Kerndateien	core	Unlimited	`ulimit -Hc`

Typ des Benutzergrenzwerts	Einstellung	Wert	Befehl zum Abfragen des Werts
Maximale Größe eines Datensegments für einen Prozess	data	Unlimited	`ulimit -Hd`
Maximale Dateigröße	fsize	Unlimited	`ulimit -Hf`
Maximale Anzahl offener Dateien	nofile	65536	`ulimit -Hn`
Maximale Prozessorzeit in Sekunden	cpu	Unlimited	`ulimit -Ht`
Maximale Anzahl Benutzerprozesse	nproc	16384	`ulimit -Hu`

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

Installation auf Windows-Systemen

Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

Vorgehensweise

1. Installieren Sie Microsoft Windows Server 2012 R2 Standard Edition gemäß den Anweisungen des Herstellers.
2. Ändern Sie die Windows-Kontensteuerungsrichtlinien, indem Sie die folgenden Schritte ausführen.
   a. Öffnen Sie den Editor für lokale Sicherheitsrichtlinien, indem Sie secpol.msc ausführen.
   b. Klicken Sie auf Lokale Richtlinien > Sicherheitsoptionen und stellen Sie sicher, dass die folgenden Benutzerkontensteuerungsrichtlinien inaktiviert sind:
      - Administratorbestätigungsmodus für das integrierte Administratorkonto
      - Alle Administratoren im Administratorbestätigungsmodus ausführen
3. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Installationsanweisungen für das Betriebssystem.
4. Wenden Sie Windows-Updates an und aktivieren Sie Zusatzfunktionen (optionale Features), indem Sie die folgenden Schritte ausführen:
   a. Wenden Sie die neuesten Windows 2012 R2-Updates an.
   b. Installieren und aktivieren Sie das Windows 2012 R2-Feature Microsoft .NET Framework 3.5 über den Windows Server-Manager.
   c. Aktualisieren Sie, falls erforderlich, die FC- und Ethernet-HBA-Einheitentreiber mit neueren Versionen.
   d. Installieren Sie den für das verwendete Plattensystem geeigneten Multipath I/O-Treiber.
5. Öffnen Sie den TCP/IP-Standardport (1500) für die Kommunikation mit dem IBM Spectrum Protect-Server. Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   netsh advfirewall firewall add rule name="Sicherungsserver-Port 1500"
   dir=in action=allow protocol=TCP localport=1500
   ```

6. Öffnen Sie auf dem Operations Center-Hub-Server den Standardport für die sichere Kommunikation (HTTPS) mit dem Operations Center. Die Portnummer ist 11090. Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   netsh advfirewall firewall add rule name="Operations Center-Port 11090"
   dir=in action=allow protocol=TCP localport=11090
   ```

Multipath I/O konfigurieren

Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.

- AIX-Systeme
- Linux-Systeme
- Windows-Systeme

AIX-Systeme

Vorgehensweise

1. Bestimmen Sie die Fibre Channel-Portadresse, die für die Hostdefinition auf dem Plattensubsystem verwendet werden muss. Geben Sie den Befehl lscfg für jeden Port aus.
   - Geben Sie auf kleinen und mittelgroßen Systemen die folgenden Befehle aus:

     ```
     lscfg -vps -l fcs0 | grep "Netzadresse"
     lscfg -vps -l fcs1 | grep "Netzadresse"
     ```

- Geben Sie auf großen Systemen die folgenden Befehle aus:

```
lscfg -vps -l fcs0 | grep "Netzadresse"
lscfg -vps -l fcs1 | grep "Netzadresse"
lscfg -vps -l fcs2 | grep "Netzadresse"
lscfg -vps -l fcs3 | grep "Netzadresse"
```

2. Stellen Sie sicher, dass die folgenden AIX-Dateigruppen installiert sind:
   - devices.common.IBM.mpio.rte
   - devices.fcp.disk.array.rte
   - devices.fcp.disk.rte
3. Geben Sie den Befehl cfgmgr aus, damit AIX die Hardware erneut überprüft und verfügbare Platten erkennt. Beispiel:

```
cfgmgr
```

4. Um die verfügbaren Platten aufzulisten, geben Sie den folgenden Befehl aus:

```
lsdev -Ccdisk
```

   Es sollte eine ähnliche Ausgabe wie die folgende angezeigt werden:

```
hdisk0  Available 00-00-00 SAS Disk Drive
hdisk1  Available 00-00-00 SAS Disk Drive
hdisk2  Available 01-00-00 SAS Disk Drive
hdisk3  Available 01-00-00 SAS Disk Drive
hdisk4  Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5  Available 07-01-02 MPIO IBM 2076 FC Disk
...
```

5. Verwenden Sie die Ausgabe des Befehls lsdev, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

   Beispielsweise könnte eine Einheiten-ID `hdisk4` lauten. Sichern Sie die Liste der Einheiten-IDs für die Verwendung bei der Erstellung von Dateisystemen für den IBM Spectrum Protect-Server.

6. Korrelieren Sie die SCSI-Einheiten-IDs zu bestimmten Platten-LUNs aus dem Plattensystem, indem Sie detaillierte Informationen zu allen physischen Datenträgern im System auflisten. Geben Sie den folgenden Befehl aus:

```
lspv -u
```

   Auf einem IBM® Storwize-System werden beispielsweise die folgenden Informationen für jede Einheit angezeigt:

```
hdisk4  00f8cf083fd97327  None  active
 3321360050763008101057800000000000003004214503IBMfcp
```

   In dem Beispiel ist *600507630081010578000000000000030* die UID für den Datenträger, die von der Storwize-Managementschnittstelle zurückgemeldet wurde.
   Um die Plattengröße in Megabyte zu überprüfen und den Wert mit dem für das System aufgelisteten Wert zu vergleichen, geben Sie den folgenden Befehl aus:

```
bootinfo -s hdisk4
```

Linux-Systeme

Vorgehensweise

1. Editieren Sie die Datei /etc/multipath.conf, um Multipathing für Linux-Hosts zu aktivieren. Wenn die Datei multipath.conf nicht vorhanden ist, können Sie die Datei erstellen, indem Sie den folgenden Befehl ausgeben:

```
mpathconf --enable
```

   Die folgenden Parameter wurden in multipath.conf zu Testzwecken auf einem IBM Storwize-System festgelegt:

```
defaults {
            user_friendly_names no
}

devices {
            device {
                        vendor "IBM "
                        product "2145"
                        path_grouping_policy group_by_prio
                        user_friendly_names no
                        path_selector "round-robin 0"
                        prio "alua"
                        path_checker "tur"
                        failback "immediate"
                        no_path_retry 5
                        rr_weight uniform
```

```
                        rr_min_io_rq "1"
                        dev_loss_tmo 120
                }
}
```

2. Definieren Sie die Multipath-Option so, dass Multipath zusammen mit dem System gestartet wird. Geben Sie die folgenden Befehle aus:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath verwaltet werden, geben Sie den folgenden Befehl aus:

```
multipath -l
```

4. Stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheiten-ID können Sie die aufgelisteten Platten identifizieren.
   Beispielsweise zeigt die folgende Ausgabe, dass einer 2-TB-Platte zwei Pfadgruppen und vier aktive Pfade zugeordnet sind. Die Größe von 2 TB bestätigt, dass die Platte einem Pooldateisystem entspricht. Suchen Sie anhand eines Teils der langen Einheiten-ID-Nummer (in diesem Beispiel 12) in der Managementschnittstelle des Plattensystems nach dem Datenträger.

```
[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
 size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64   active undef running
| `- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
  |- 1:0:1:18 sdat 66:208  active undef running
  `- 3:0:0:18 sddy 128:0   active undef running
```

   a. Korrigieren Sie, falls erforderlich, Platten-LUN/Host-Zuordnungen und erzwingen Sie eine erneute Busüberprüfung. Beispiel:

```
echo "- - -" > /sys/class/scsi_host/host0/scan
echo "- - -" > /sys/class/scsi_host/host1/scan
echo "- - -" > /sys/class/scsi_host/host2/scan
```

      Sie können für eine erneute Überprüfung der Platten-LUN/Host-Zuordnungen auch das System erneut starten.
   b. Stellen Sie sicher, dass Platten jetzt für Multipath I/O verfügbar sind, indem Sie den Befehl multipath -l erneut ausgeben.
5. Verwenden Sie die Multipath-Ausgabe, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

   Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte `36005076802810c509800000000000012`.

   Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

Windows-Systeme

Vorgehensweise

1. Stellen Sie sicher, dass Multipath I/O installiert ist. Installieren Sie, falls erforderlich, weitere anbieterspezifische Multipath-Treiber.
2. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath I/O verwaltet werden, geben Sie den folgenden Befehl aus:

```
c:\Programme\IBM\SDDDSM\datapath.exe query device
```

3. Überprüfen Sie die Multipath-Ausgabe und stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheitenseriennummer können Sie die aufgelisteten Platten identifizieren.
   Beispielsweise können Sie anhand eines Teils der langen Einheitenseriennummer (in diesem Beispiel 34) in der Managementschnittstelle des Plattensystems nach dem Datenträger suchen. Die Größe von 2 TB bestätigt, dass die Platte einem Speicherpooldateisystem entspricht.

```
DEV#:   4  DEVICE NAME: Disk5 Part0   TYPE: 2145    POLICY: OPTIMIZED
SERIAL: 600507630081010578000000000000034          LUN SIZE: 2.0TB
============================================================================
Path#          Adapter/Hard Disk       State   Mode    Select  Errors
    0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
    1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176       0
    2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494       0
    3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
```

4. Erstellen Sie unter Verwendung der in der Multipath-Ausgabe im vorherigen Schritt zurückgegebenen Seriennummern eine Liste der Platteneinheiten-IDs.

   Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte `600507630081010578000000000000034`.

   Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

5. Um neue Platten online zu schalten und das Lesezugriffsattribut zu löschen, führen Sie diskpart.exe mit den folgenden Befehlen aus. Wiederholen Sie diesen Schritt für jede der Platten:

```
diskpart
   select Disk 1
   online disk
   attribute disk clear readonly
   select Disk 2
   online disk
   attribute disk clear readonly
   < ... >
   select Disk 49
   online disk
   attribute disk clear readonly
   exit
```

Benutzer-ID für den Server erstellen

Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.

Informationen zu diesem Vorgang

Sie können nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstreichungszeichen (_) für die Benutzer-ID angeben. Die Benutzer-ID und der Gruppenname müssen den folgenden Regeln entsprechen:

- Die Länge darf 8 Zeichen nicht überschreiten.
- Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder einer Ziffer beginnen.
- Die Benutzer-ID und der Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* oder ein in SQL reserviertes Wortes sein.

Vorgehensweise

1. Erstellen Sie mithilfe von Betriebssystembefehlen eine Benutzer-ID.
   - AIX-BetriebssystemeLinux-BetriebssystemeErstellen Sie eine Gruppe und eine Benutzer-ID im Ausgangsverzeichnis des Benutzers, der Eigner der Serverinstanz ist.

     Um beispielsweise die Benutzer-ID tsminst1 in der Gruppe tsmsrvrs mit dem Kennwort tsminst1 zu erstellen, geben Sie die folgenden Befehle mit einer ID für einen Benutzer mit Verwaltungsaufgaben aus:

     AIX-Betriebssysteme

     ```
     mkgroup id=1001 tsmsrvrs
     mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
     passwd tsminst1
     ```

     Linux-Betriebssysteme

     ```
     groupadd tsmsrvrs
     useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
     passwd tsminst1
     ```

     Melden Sie sich von Ihrem System ab und anschließend wieder an. Wechseln Sie zu dem von Ihnen erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, wie beispielsweise Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es, falls erforderlich, ändern können.
   - Windows-BetriebssystemeErstellen Sie eine Benutzer-ID und fügen Sie dann die neue ID der Gruppe 'Administratoren' hinzu. Um beispielsweise die Benutzer-ID tsminst1 zu erstellen, geben Sie den folgenden Befehl aus:

     ```
     net user tsminst1 * /add
     ```

     Fügen Sie, nachdem Sie für den neuen Benutzer ein Kennwort erstellt und bestätigt haben, die Benutzer-ID der Gruppe 'Administratoren' hinzu, indem Sie die folgenden Befehle ausgeben:

     ```
     net localgroup Administratoren tsminst1 /add
     net localgroup DB2ADMNS tsminst1 /add
     ```

2. Melden Sie die neue Benutzer-ID ab.

Dateisysteme für den Server vorbereiten

Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

- Dateisysteme auf AIX-Systemen vorbereiten
  Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager

erstellen.

- Dateisysteme auf Linux-Systemen vorbereiten
  Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.
- Dateisysteme auf Windows-Systemen vorbereiten
  Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

Dateisysteme auf AIX-Systemen vorbereiten

Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.

Vorgehensweise

1. Erhöhen Sie die Warteschlangenlänge und die maximale Übertragungsgröße für alle verfügbaren *hdiskX*-Platten. Geben Sie für jede Platte die folgenden Befehle aus:

   ```
   chdev -l hdisk4 -a max_transfer=0x100000
   chdev -l hdisk4 -a queue_depth=32
   chdev -l hdisk4 -a reserve_policy=no_reserve
   chdev -l hdisk4 -a algorithm=round_robin
   ```

   Sie dürfen diese Befehle nicht für interne Betriebssystemplatten, beispielsweise *hdisk0*, ausführen.
2. Erstellen Sie Datenträgergruppen für die IBM Spectrum Protect-Datenbank, die aktive Protokolldatei, das Archivprotokoll, die Datenbanksicherung und den Speicherpool. Geben Sie den Befehl mkvg unter Angabe der Einheiten-IDs für die entsprechenden zuvor ermittelten Platten aus.
   Wenn beispielsweise die Einheitennamen *hdisk4, hdisk5* und *hdisk6* Datenbankplatten entsprechen, schließen Sie diese in die Datenbankdatenträgergruppe ein.
   Systemgröße: Die folgenden Befehle basieren auf einer Konfiguration für ein mittelgroßes System. Für kleine und große Systeme müssen Sie die Syntax wie erforderlich anpassen.

   ```
   mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
   mkvg -S -y tsmactlog hdisk5
   mkvg -S -y tsmarchlog hdisk6
   mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
   mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
   ```

3. Bestimmen Sie die Namen der physischen Datenträger und die Anzahl freier physischer Partitionen, die beim Erstellen logischer Datenträger verwendet werden sollen. Geben Sie den Befehl lsvg für jede Datenträgergruppe aus, die Sie im vorherigen Schritt erstellt haben.
   Beispiel:

   ```
   lsvg -p tsmdb
   ```

   Die Ausgabe sieht ähnlich wie die folgende aus. Die Spalte *FREE PPs* gibt die freien physischen Partitionen an:

   ```
   tsmdb:
   PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
   hdisk4   active     1631       1631      327..326..326..326..326
   hdisk5   active     1631       1631      327..326..326..326..326
   hdisk6   active     1631       1631      327..326..326..326..326
   ```

4. Erstellen Sie mit dem Befehl mklv logische Datenträger in jeder Datenträgergruppe. Die Datenträgergröße, die Datenträgergruppe und die Einheitennamen sind, abhängig von der Größe Ihres Systems und Variationen in Ihrer Plattenkonfiguration, unterschiedlich.
   Um beispielsweise die Datenträger für die IBM Spectrum Protect-Datenbank auf einem mittelgroßen System zu erstellen, geben Sie die folgenden Befehle aus:

   ```
   mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
   mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
   mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
   ```

5. Formatieren Sie Dateisysteme auf jedem logischen Datenträger mit dem Befehl crfs.
   Um beispielsweise die Dateisysteme für die Datenbank auf einem mittelgroßen System zu formatieren, geben Sie die folgenden Befehle aus:

   ```
   crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
   crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
   crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
   ```

6. Führen Sie für alle neu erstellten Dateisysteme einen Mount durch, indem Sie den folgenden Befehl eingeben:

   ```
   mount -a
   ```

7. Listen Sie alle Dateisysteme auf, indem Sie den Befehl df ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.
   Das folgende Beispiel der Befehlsausgabe zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

   ```
   tapsrv07> df -g /tsminst1/*
   Filesystem      GB blocks  Free     %Used   Iused   %Iused   Mounted on
   /dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
   ```

8. Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den Server hat.

Dateisysteme auf Linux-Systemen vorbereiten

Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

Vorgehensweise

1. Verwenden Sie die zuvor generierte Liste der Einheiten-IDs und geben Sie den Befehl mkfs aus, um für jede LUN-Speichereinheit ein Dateisystem zu erstellen und zu formatieren. Geben Sie die Einheiten-ID im Befehl an. Siehe die folgenden Beispiele. Formatieren Sie für die Datenbank ext4-Dateisysteme:

   ```
   mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
   ```

   Formatieren Sie für Speicherpool-LUNs xfs-Dateisysteme:

   ```
   mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
   ```

   Abhängig davon, wie viele verschiedene Einheiten vorhanden sind, können Sie den Befehl mkfs bis zu 50 Mal ausgeben.

2. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.

   Geben Sie den Befehl mkdir für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte.

   Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

   ```
   mkdir /tsminst1
   ```

   Wiederholen Sie den Befehl mkdir für jedes Dateisystem.
3. Fügen Sie in der Datei /etc/fstab für jedes Dateisystem einen Eintrag hinzu, damit für die Dateisysteme beim Serverstart automatisch ein Mount durchgeführt wird.
   Beispiel:

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
   ```

4. Führen Sie für die Dateisysteme, die der Datei /etc/fstab hinzugefügt wurden, einen Mount durch, indem Sie den Befehl mount -a ausgeben.
5. Listen Sie alle Dateisysteme auf, indem Sie den Befehl df ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.
   Das folgende Beispiel für ein IBM® Storwize-System zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

   ```
   [root@tapsrv04 ~]# df -h /tsminst1/*
   Filesystem                                      Size  Used Avail Use% Mounted on
   /dev/mapper/360050763008101057800000000000003 134G  188M 132G  1%   /tsminst1/TSMalog
   ```

6. Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den IBM Spectrum Protect-Server hat.

Dateisysteme auf Windows-Systemen vorbereiten

Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

Vorgehensweise

1. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.
   Geben Sie den Befehl md für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte. Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

   ```
   md c:\tsminst1
   ```

   Wiederholen Sie den Befehl md für jedes Dateisystem.

2. Erstellen Sie für jede Platten-LUN, die einem Verzeichnis unter dem Serverinstanzverzeichnis zugeordnet ist, unter Verwendung des Windows-Datenträgermanagers (Volume-Manager) einen Datenträger.

   Rufen Sie Server-Manager > Datei- und Speicherdienste auf und führen Sie die folgenden Schritte für jede Platte aus, die der im vorherigen Schritt erstellten LUN-Zuordnung entspricht:

   a. Schalten Sie die Platte online.
   b. Initialisieren Sie die Platte mit dem GPT-Basistyp, dem Standardwert.
   c. Erstellen Sie einen einfachen Datenträger, der den gesamten Speicherbereich auf der Platte belegt. Formatieren Sie das Dateisystem mit NTFS und ordnen Sie einen Kennsatz zu, der den Zweck des Datenträgers angibt, wie beispielsweise TSMfile00. Ordnen Sie den neuen Datenträger keinem Laufwerkbuchstaben zu. Ordnen Sie den Datenträger stattdessen einem Verzeichnis unter dem Instanzverzeichnis zu, wie beispielsweise C:\tsminst1\TSMfile00.
      Tipp: Legen Sie den Datenträgerkennsatz und die Bezeichnungen für Verzeichniszuordnungen auf der Basis der Größe der aufgelisteten Platte fest.
3. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Listen Sie alle Dateisysteme auf, indem Sie den Befehl mountvol ausgeben; überprüfen Sie dann die Ausgabe. Beispiel:

   ```
   \\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
     C:\tsminst1\TSMdbspace00\
   ```

4. Starten Sie nach dem Abschluss der Plattenkonfiguration das System erneut.

Nächste Schritte

Mithilfe von Windows Explorer können Sie den Umfang des freien Speicherbereichs für jeden Datenträger prüfen.

Server und das Operations Center installieren

Verwenden Sie den grafisch orientierten Assistenten von IBM® Installation Manager, um die Komponenten zu installieren.

- Installation auf AIX- und Linux-Systemen
  Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.
- Installation auf Windows-Systemen
  Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

Installation auf AIX- und Linux-Systemen

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

Vorbereitende Schritte

Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.

Vorgehensweise

1. AIX-BetriebssystemeÜberprüfen Sie, ob die erforderlichen RPM-Dateien auf Ihrem System installiert sind.

   Ausführliche Informationen befinden sich in Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren.

2. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042992.
3. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
4. Stellen Sie sicher, dass für das Paket die Berechtigung zur Ausführung festgelegt ist. Ändern Sie, falls erforderlich, die Dateiberechtigungen, indem Sie den folgenden Befehl ausgeben:

   ```
   chmod a+x Paketname.bin
   ```

5. Extrahieren Sie das Paket, indem Sie den folgenden Befehl ausgeben:

   ```
   ./Paketname.bin
   ```

   Dabei ist *Paketname* der Name der Downloaddatei.
6. AIX-BetriebssystemeStellen Sie sicher, dass der folgende Befehl aktiviert ist, damit die Assistenten korrekt ausgeführt werden:

   ```
   lsuser
   ```

   Standardmäßig ist der Befehl aktiviert.
7. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
8. Starten Sie den Installationsassistenten, indem Sie den folgenden Befehl ausgeben:

```
./install.sh
```

Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM Installation Manager gespeichert sind.

  Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.

- Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren
  RPM-Dateien sind für den grafisch orientierten Assistenten von IBM Installation Manager erforderlich.

Zugehörige Tasks:
Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten (AIX)
Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten (Linux)

Installation auf Windows-Systemen

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.
- Stellen Sie sicher, dass die Benutzer-ID, die während der Installation verwendet werden soll, für einen Benutzer mit der Berechtigung eines lokalen Administrators gilt.

Vorgehensweise

1. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042993.
2. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
3. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
4. Doppelklicken Sie auf die ausführbare Datei, um die Datei in das aktuelle Verzeichnis zu extrahieren.
5. Starten Sie in dem Verzeichnis, in das die Installationsdateien extrahiert wurden, den Installationsassistenten, indem Sie auf die Datei install.bat doppelklicken. Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM® Installation Manager gespeichert sind.

  Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.

Zugehörige Tasks:
Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten

Server und das Operations Center konfigurieren

Nachdem Sie die Komponenten installiert haben, führen Sie die Konfiguration für den IBM Spectrum Protect-Server und das Operations Center aus.

- Serverinstanz konfigurieren
  Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.

- Client für Sichern/Archivieren installieren
  Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.
- Optionen für den Server festlegen
  Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.
- Sichere Kommunikation mit Transport Layer Security konfigurieren
  Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.
- Operations Center konfigurieren
  Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.
- Produktlizenz registrieren
  Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.
- Datendeduplizierung konfigurieren
  Erstellen Sie einen Verzeichniscontainerspeicherpool und mindestens ein Verzeichnis für die Verwendung der Inline-Datendeduplizierung.
- Datenaufbewahrungsregeln für Ihr Unternehmen definieren
  Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datendeduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.
- Zeitpläne für Serververwaltungsaktivitäten definieren
  Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.
- Clientzeitpläne definieren
  Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

Serverinstanz konfigurieren

Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
AIX-Betriebssysteme  Linux-Betriebssysteme

- Auf dem System, auf dem IBM Spectrum Protect installiert wurde, muss der X Window System-Client vorhanden sein. Außerdem muss ein X Window System-Server auf Ihrem Desktop ausgeführt werden.
- Für das System muss das Secure Shell-Protokoll (SSH-Protokoll) aktiviert sein. Stellen Sie sicher, dass der Port auf den Standardwert 22 gesetzt ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei sshd_config im Verzeichnis /etc/ssh/ aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämonservice über die Zugriffsberechtigungen verfügt, um mithilfe des Werts *localhost* eine Verbindung zum System herstellen zu können.
- Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt hatten, unter Verwendung des SSH-Protokolls bei IBM Spectrum Protect anmelden können. Wenn Sie den Assistenten verwenden, müssen Sie diese Benutzer-ID und das Kennwort für den Zugriff auf dieses System angeben.
- Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

 Windows-BetriebssystemeÜberprüfen Sie, ob der Remoteregistrierungsdienst gestartet wurde, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf Start > Verwaltung > Dienste. Wählen Sie im Fenster Dienste Remoteregistrierung aus. Wurde der Dienst nicht gestartet, klicken Sie auf Starten.
2. Stellen Sie sicher, dass die Ports 137, 139 und 445 nicht durch eine Firewall blockiert sind:
   a. Klicken Sie auf Start > Systemsteuerung > Windows-Firewall.
   b. Wählen Sie Erweiterte Einstellungen aus.
   c. Wählen Sie Eingehende Regeln aus.
   d. Wählen Sie Neue Regel aus.
   e. Erstellen Sie eine Portregel für die TCP-Ports 137, 139 und 445, um Verbindungen für Domänennetze und private Netze zu ermöglichen.
3. Konfigurieren Sie die Benutzerkontensteuerung, indem Sie auf die Optionen für die lokale Sicherheitsrichtlinie zugreifen und die folgenden Schritte ausführen.
   a. Klicken Sie auf Start > Verwaltung > Lokale Sicherheitsrichtlinie. Erweitern Sie Lokale Richtlinien > Sicherheitsoptionen.
   b. Falls noch nicht bereits aktiviert, aktivieren Sie das integrierte Administratorkonto, indem Sie Konten: Administratorkontostatus > Aktivieren > OK auswählen.
   c. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für alle Windows-Administratoren, indem Sie Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen > Inaktivieren > OK auswählen.
   d. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für das integrierte Administratorkonto, indem Sie Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto > Inaktivieren > OK auswählen.

4. Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

Informationen zu diesem Vorgang

Der Assistent kann gestoppt und erneut gestartet werden, der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

Vorgehensweise

1. Starten Sie die lokale Version des Assistenten.
   -  AIX-Betriebssysteme  Linux-BetriebssystemeÖffnen Sie das Programm dsmicfgx im Verzeichnis /opt/tivoli/tsm/server/bin. Dieser Assistent kann nur als Rootbenutzer ausgeführt werden.
   -  Windows-BetriebssystemeKlicken Sie auf Start > Alle Programme > IBM Spectrum Protect > Konfigurationsassistent.
2. Führen Sie die Anweisungen aus, um die Konfiguration auszuführen. Verwenden Sie die während der IBM Spectrum Protect-Systemkonfiguration aufgezeichneten Informationen (siehe Arbeitsblätter zur Planung), um Verzeichnisse und Optionen im Assistenten anzugeben.

    AIX-Betriebssysteme  Linux-BetriebssystemeLegen Sie im Fenster Serverinformationen fest, dass der Server automatisch unter Verwendung der Instanzbenutzer-ID gestartet werden soll, wenn das System bootet.

    Windows-BetriebssystemeMithilfe des Konfigurationsassistenten wird festgelegt, dass der Server automatisch gestartet werden soll, wenn ein Warmstart durchgeführt wird.

Client für Sichern/Archivieren installieren

Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.

Vorgehensweise

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

Optionen für den Server festlegen

Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.

Vorgehensweise

1. Wechseln Sie in das Serverinstanzverzeichnis und öffnen Sie die Datei dsmserv.opt.
2. Überprüfen Sie die Werte in der folgenden Tabelle und Ihre Serveroptionseinstellungen auf der Basis der Systemgröße.

Serveroption	**Wert für kleine Systeme**	**Wert für mittelgroße Systeme**	**Wert für große Systeme**
ACTIVELOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Yes	No	No
ARCHLOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	No	No	No
DEVCONFIG	devconf.dat	devconf.dat	devconf.dat
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60

Serveroption	Wert für kleine Systeme	Wert für mittelgroße Systeme	Wert für große Systeme
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	volhist.dat	volhist.dat	volhist.dat

Aktualisieren Sie, falls erforderlich, Serveroptionseinstellungen in Übereinstimmung mit den Werten in der Tabelle. Um Aktualisierungen durchzuführen, schließen Sie die Datei dsmserv.opt und definieren Sie die Optionen mit dem Befehl SETOPT in der Verwaltungsbefehlszeilenschnittstelle.
Um beispielsweise die Option IDLETIMEOUT mit 60 zu aktualisieren, geben Sie den folgenden Befehl aus:

```
setopt idletimeout 60
```

3. Um für den Server, die Clients und das Operations Center die sichere Kommunikation zu konfigurieren, überprüfen Sie die Optionen in der folgenden Tabelle.

Serveroption	Alle Systemgrößen
SSLFIPSMODE	NO
TCPPORT	Geben Sie die Nummer des Ports an, an dem der Server auf Anforderungen von TCP/IP- und SSL-fähigen Sitzungen des Clients wartet.
TCPADMINPORT	Geben Sie die Adresse des Ports an, an dem der Server auf Anforderungen von TCP/IP- und SSL-fähigen Sitzungen des Verwaltungsbefehlszeilenclients wartet.

Wenn einer der Optionswerte aktualisiert werden muss, editieren Sie die Datei dsmserv.opt unter Verwendung der folgenden Anleitungen:
   - Entfernen Sie den Stern am Anfang einer Zeile, um eine Option zu aktivieren.
   - Geben Sie in jeder Zeile nur eine einzige Option und den für die Option angegebenen Wert ein.
   - Wenn eine Option in mehreren Einträgen in der Datei vorkommt, verwendet der Server den letzten Eintrag.

Sichern Sie Ihre Änderungen und schließen Sie die Datei. Wenn Sie die Datei dsmserv.opt direkt editieren, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

Zugehörige Verweise:
Referenz für Serveroptionen
SETOPT (Serveroption für dynamische Aktualisierung definieren)

Sichere Kommunikation mit Transport Layer Security konfigurieren

Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.

Informationen zu diesem Vorgang

Wie in der folgenden Abbildung gezeigt können Sie die sichere Kommunikation zwischen dem Server und dem Client für Sichern/Archivieren manuell konfigurieren, indem Sie Optionen in der Server- und der Clientoptionsdatei definieren und dann das selbst signierte Zertifikat, das auf dem Server generiert wird, an den Client übertragen. Sie können auch stattdessen ein eindeutiges Zertifikat, das von einer Zertifizierungsstelle (CA) signiert ist, anfordern und übertragen.

Weitere Informationen zum Konfigurieren des Servers und von Clients für die SSL- oder TLS-Kommunikation finden Sie in Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren.

Operations Center konfigurieren

Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.

Vorbereitende Schritte

Wenn Sie zum ersten Mal die Verbindung zum Operations Center herstellen, müssen Sie die folgenden Informationen angeben:

- Verbindungsinformationen für den Server, der als Hub-Server festgelegt werden soll
- Anmeldeberechtigungsnachweise für eine Administrator-ID, die für diesen Server definiert ist

Vorgehensweise

1. Legen Sie den Hub-Server fest. Geben Sie in einem Web-Browser die folgende Adresse ein:

   ```
   https://Hostname:sicherer_Port/oc
   ```

   Erläuterungen:
   - *Hostname* gibt den Namen des Computers an, auf dem das Operations Center installiert ist.
   - *Sicherer_Port* gibt die Portnummer an, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet.

   Wenn beispielsweise der Hostname tsm.storage.mylocation.com lautet und der standardmäßige sichere Port für das Operations Center (Port 11090) verwendet wird, ist die Adresse wie folgt:

   ```
   https://tsm.storage.mylocation.com:11090/oc
   ```

   Wenn Sie sich zum ersten Mal beim Operations Center anmelden, führt Sie ein Assistent durch eine Erstkonfiguration, um einen neuen Administrator mit Systemberechtigung auf dem Server zu konfigurieren.

2. Konfigurieren Sie die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server, indem Sie das Protokoll Secure Sockets Layer (SSL) konfigurieren.

   Führen Sie die Anweisungen in Kommunikation zwischen dem Operations Center und dem Hub-Server schützen aus.

3. Optional: Um einen täglichen E-Mail-Bericht mit einer Zusammenfassung des Systemstatus zu empfangen, konfigurieren Sie Ihre E-Mail-Einstellungen im Operations Center.

   Führen Sie die Anweisungen in Systemstatus mithilfe von E-Mail-Berichten verfolgen aus.

- Kommunikation zwischen dem Operations Center und dem Hub-Server schützen
  Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server zu ermöglichen, fügen Sie das TLS-Zertifikat des Hub-Servers der Truststore-Datei des Operations Center hinzu.

Produktlizenz registrieren

Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.

Informationen zu diesem Vorgang

Lizenzen werden in Registrierungszertifikatsdateien gespeichert, die Lizenzinformationen für das Produkt enthalten. Die Registrierungszertifikatsdateien befinden sich auf den Installationsmedien und werden während der Installation auf den Server gestellt. Wenn Sie das Produkt registrieren, werden die Lizenzen in einer NODELOCK-Datei im aktuellen Verzeichnis gespeichert.

Vorgehensweise

Registrieren Sie eine Lizenz, indem Sie den Namen der Registrierungszertifikatsdatei angeben, die die Lizenz enthält. Um den Command Builder des Operations Center für diese Task zu verwenden, führen Sie die folgenden Schritte aus.

1. Öffnen Sie das Operations Center.
2. Öffnen Sie den Command Builder des Operations Center, indem Sie den Mauszeiger über das Symbol für Einstellungen bewegen und auf Command Builder klicken.
3. Geben Sie den Befehl REGISTER LICENSE aus. Um beispielsweise eine IBM Spectrum Protect-Basislizenz zu registrieren, geben Sie den folgenden Befehl aus:

   ```
   register license file=tsmbasic.lic
   ```

Nächste Schritte

Sichern Sie die Installationsmedien, die Ihre Registrierungszertifikatsdateien enthalten. Möglicherweise müssen Sie Ihre Lizenz erneut registrieren, wenn beispielsweise eine der folgenden Bedingungen erfüllt ist:

- Der Server wird auf einen anderen Computer versetzt.
- Die NODELOCK-Datei ist beschädigt. Der Server speichert Lizenzinformationen in der NODELOCK-Datei, die sich in dem Verzeichnis befindet, von dem aus der Server gestartet wird.
- Linux-BetriebssystemeSie ändern den Prozessorchip, der dem Server zugeordnet ist, auf dem der Server installiert ist.

Zugehörige Verweise:
REGISTER LICENSE (Neue Lizenz registrieren)

Datendeduplizierung konfigurieren

Erstellen Sie einen Verzeichniscontainerspeicherpool und mindestens ein Verzeichnis für die Verwendung der Inline-Datendeduplizierung.

Vorbereitende Schritte

Verwenden Sie für diese Task die aufgezeichneten Informationen zu Speicherpoolverzeichnissen (siehe Arbeitsblätter zur Planung).

Vorgehensweise

1. Öffnen Sie das Operations Center.
2. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher.
3. Klicken Sie in der angezeigten Liste auf Speicherpools.
4. Klicken Sie auf die Schaltfläche +Speicherpool.
5. Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus:
   - Um die Inline-Datendeduplizierung verwenden zu können, wählen Sie einen Speicherpool Verzeichnis unter dem containerbasierten Speicher aus.
   - Wenn Sie Verzeichnisse für den Verzeichniscontainerspeicherpool konfigurieren, geben Sie die Verzeichnispfade an, die während der Systemkonfiguration für Speicher erstellt wurden.
6. Klicken Sie nach dem Konfigurieren des neuen Verzeichniscontainerspeicherpools auf Schließen & Maßnahmen anzeigen, um eine Verwaltungsklasse zu aktualisieren und mit der Verwendung des Speicherpools zu beginnen.

Datenaufbewahrungsregeln für Ihr Unternehmen definieren

Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datendeduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.

Vorgehensweise

1. Wählen Sie auf der Seite Services im Operations Center die Domäne STANDARD aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen. Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.
3. Klicken Sie auf die Umschaltfläche Konfigurieren und führen Sie die folgenden Änderungen durch:
   - Ändern Sie das Sicherungsziel für die Verwaltungsklasse STANDARD in den Verzeichniscontainerspeicherpool.
   - Ändern Sie den Wert für die Spalte 'Sicherungen' in Keine Begrenzung.
   - Ändern Sie den Aufbewahrungszeitraum. Setzen Sie den Wert für die Spalte 'Zusätzliche Sicherungen aufbewahren' abhängig von Ihren Geschäftsanforderungen auf 30 Tage oder mehr.
4. Sichern Sie Ihre Änderungen und klicken Sie erneut auf die Umschaltfläche Konfigurieren, damit die Maßnahmengruppe nicht mehr editierbar ist.
5. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.

Zugehörige Tasks:
Regeln zum Sichern und Archivieren von Clientdaten angeben

Zeitpläne für Serververwaltungsaktivitäten definieren

Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.

Informationen zu diesem Vorgang

Planen Sie die Ausführung von Serververwaltungsoperationen im Anschluss an Clientsicherungsoperationen. Sie können das Timing von Zeitplänen steuern, indem Sie die Startzeit in Kombination mit der Dauer für jede Operation definieren.

Das folgende Beispiel zeigt die Planung von Serververwaltungsoperationen in Kombination mit dem Clientsicherungszeitplan für eine Plattenspeicherlösung für einen einzelnen Standort.

Operation	Zeitplan
Clientsicherung	Startet um 22:00 Uhr.

Operation	Zeitplan
Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall	• Die Datenbanksicherungsoperation startet um 11:00 Uhr bzw. 13 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt. • Die Sicherungsoperationen für Einheitenkonfigurationsinformationen und das Datenträgerprotokoll starten um 17:00 Uhr bzw. 6 Stunden nach dem Start der Datenbanksicherungsoperation. • Das Löschen des Datenträgerprotokolls startet um 20:00 Uhr bzw. 9 Stunden nach dem Start der Datenbanksicherungsoperation.
Bestandsverfall	Startet um 12:00 Uhr bzw. 14 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt.

Vorgehensweise

Erstellen Sie nach dem Konfigurieren der Einheitenklasse für die Datenbanksicherungsoperationen Zeitpläne für Datenbanksicherungsoperationen und andere erforderliche Verwaltungsoperationen mithilfe des Befehls DEFINE SCHEDULE. Abhängig von der Größe Ihrer Umgebung müssen Sie die Startzeiten für jeden Zeitplan in dem Beispiel gegebenenfalls anpassen.

1. Definieren Sie eine Einheitenklasse für die Sicherungsoperationen. Erstellen Sie beispielsweise mit dem Befehl DEFINE DEVCLASS eine Einheitenklasse mit dem Namen DBBACK_FILEDEV:

   ```
   define devclass dbback_filedev devtype=file
     directory=Datenbanksicherungsverzeichnisse
   ```

   Dabei ist *Datenbanksicherungsverzeichnisse* eine Liste der für die Datenbanksicherung erstellten Verzeichnisse.
    AIX-Betriebssysteme  Linux-BetriebssystemeWenn beispielsweise vier Verzeichnisse für Datenbanksicherungen mit /tsminst1/TSMbkup00 als Startpunkt vorhanden sind, geben Sie den folgenden Befehl aus:

   ```
   define devclass dbback_filedev devtype=file
     directory=/tsminst1/TSMbkup00,
     /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
     /tsminst1/TSMbkup03"
   ```

    Windows-BetriebssystemeWenn beispielsweise vier Verzeichnisse für Datenbanksicherungen mit C:\tsminst1\TSMbkup00 als Startpunkt vorhanden sind, geben Sie den folgenden Befehl aus:

   ```
   define devclass dbback_filedev devtype=file
     directory="c:\tsminst1\TSMbkup00,
     c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
   ```

2. Legen Sie die Einheitenklasse für automatische Datenbanksicherungsoperationen fest. Geben Sie mit dem Befehl SET DBRECOVERY die im vorhergehenden Schritt erstellte Einheitenklasse an. Wenn beispielsweise die Einheitenklasse den Namen dbback_filedev hat, geben Sie den folgenden Befehl aus:

   ```
   set dbrecovery dbback_filedev
   ```

3. Erstellen Sie mithilfe des Befehls DEFINE SCHEDULE Zeitpläne für die Verwaltungsoperationen. Die folgende Tabelle enthält die erforderlichen Operationen und Beispiele der Befehle.

Operation	Beispielbefehl
Sichern der Datenbank	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DB. Wenn Sie ein kleines System konfigurieren, setzen Sie den Parameter COMPRESS auf YES. Geben Sie beispielsweise auf einem kleinen System den folgenden Befehl aus, um einen Sicherungszeitplan zu erstellen, der die neue Einheitenklasse verwendet: `define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Datenbank sichern." startdate=today starttime=11:00:00 duration=45 durunits=minutes`
Sichern der Einheitenkonfigurationsinformationen	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DEVCONFIG: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Einheitenkonfigurations- datei sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes`

Operation	Beispielbefehl
Sichern des Datenträgerprotokolls	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP VOLHISTORY: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Datenträgerprotokoll sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Entfernen älterer Versionen von Datenbanksicherungen, die nicht mehr erforderlich sind	Erstellen Sie einen Zeitplan für die Ausführung des Befehls DELETE VOLHISTORY: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Alte Datenbanksicherungen entfernen." startdate=today starttime=20:00:00 duration=45 durunits=minutes`
Entfernen von Objekten, deren zulässige Aufbewahrungsdauer überschritten wurde	Erstellen Sie einen Zeitplan für die Ausführung des Befehls EXPIRE INVENTORY. Definieren Sie den Parameter RESOURCE auf der Basis der Systemgröße, die Sie konfigurieren: ○ Kleine Systeme: 10 ○ Mittelgroße Systeme: 30 ○ Große Systeme: 40 Geben Sie beispielsweise auf einem mittelgroßen System den folgenden Befehl aus, um einen Zeitplan mit dem Namen EXPINVENTORY zu erstellen: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Verfallene Objekte entfernen." startdate=today starttime=12:00:00 duration=45 durunits=minutes`

Nächste Schritte

Nachdem Sie Zeitpläne für die Serververwaltungstasks erstellt haben, können Sie diese im Operations Center anzeigen, indem Sie die folgenden Schritte ausführen:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Server.
2. Klicken Sie auf Verwaltung.

Zugehörige Verweise:
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

Clientzeitpläne definieren

Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

Vorgehensweise

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Clients.
2. Klicken Sie auf Zeitpläne.
3. Klicken Sie auf +Zeitplan.
4. Führen Sie die Schritte im Assistenten Zeitplan erstellen aus. Definieren Sie auf der Basis der in Zeitpläne für Serververwaltungsaktivitäten definieren geplanten Serververwaltungsaktivitäten für Clientsicherungszeitpläne eine Startzeit von 22:00 Uhr.

Clients für Sichern/Archivieren installieren und konfigurieren

Installieren und konfigurieren Sie im Anschluss an die erfolgreiche Konfiguration Ihres IBM Spectrum Protect-Serversystems die Client-Software, um mit dem Sichern von Daten beginnen zu können.

Vorgehensweise

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

Nächste Schritte

Registrieren Sie Ihre Clients und ordnen Sie Ihre Clients Zeitplänen zu.

- Clients registrieren und Zeitplänen zuordnen
  Sie können Ihre Clients über das Operations Center mithilfe des Assistenten Client hinzufügen hinzufügen und registrieren.
- Clientverwaltungsservice installieren
  Installieren Sie den Clientverwaltungsservice für Clients für Sichern/Archivieren, die unter Linux- und Windows-Betriebssystemen ausgeführt werden. Der Clientverwaltungsservice erfasst Diagnoseinformationen zu Clients für Sichern/Archivieren und stellt die Informationen dem Operations Center für die grundlegende Überwachungsfunktion zur Verfügung.

Clients registrieren und Zeitplänen zuordnen

Sie können Ihre Clients über das Operations Center mithilfe des Assistenten Client hinzufügen hinzufügen und registrieren.

Vorbereitende Schritte

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963. Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

Vorgehensweise

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

  ```
  register node Knotenname Kennwort userid=Knotenname
  ```

  Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.
- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  a. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  b. Klicken Sie in der Tabelle 'Clients' auf + Client.
  c. Führen Sie die Schritte im Assistenten Client hinzufügen aus:
     i. Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Datendeduplizierung' das Kontrollkästchen Aktivieren aus.
     ii. Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEDUPLICATION.
     Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
     iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
     iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
     v. Klicken Sie auf Client hinzufügen.

Clientverwaltungsservice installieren

Installieren Sie den Clientverwaltungsservice für Clients für Sichern/Archivieren, die unter Linux- und Windows-Betriebssystemen ausgeführt werden. Der Clientverwaltungsservice erfasst Diagnoseinformationen zu Clients für Sichern/Archivieren und stellt die Informationen dem Operations Center für die grundlegende Überwachungsfunktion zur Verfügung.

Vorgehensweise

Installieren Sie den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das Installationspaket für den Clientverwaltungsservice von einer IBM® Download-Site, wie beispielsweise IBM Passport Advantage® oder IBM Fix Central, herunter. Suchen Sie nach einem ähnlichen Dateinamen wie `<Version>-IBM_Spectrum_Protect-CMS-Betriebssystem.bin`.
2. Erstellen Sie auf dem Clientsystem, das verwaltet werden soll, ein Verzeichnis und kopieren Sie das Installationspaket in dieses Verzeichnis.
3. Extrahieren Sie den Inhalt der Installationspaketdatei.

4. Führen Sie die Installationsstapeldatei in dem Verzeichnis aus, in das die Installationsdateien und die zugehörigen Dateien extrahiert wurden. Dabei handelt es sich um das in Schritt 2 erstellte Verzeichnis.
5. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen im Assistenten von IBM Installation Manager aus. Wenn IBM Installation Manager noch nicht auf dem Clientsystem installiert ist, müssen Sie sowohl IBM Installation Manager als auch die IBM Spectrum Protect-Clientverwaltungsservices auswählen.

- Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen
  Bevor Sie den Clientverwaltungsservice zum Erfassen von Diagnoseinformationen zu einem Client für Sichern/Archivieren verwenden, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist.
- Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren
  Wenn für den Clientverwaltungsservice nicht die Standardkonfiguration verwendet wurde, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

Zugehörige Tasks:
Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren

Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen

Bevor Sie den Clientverwaltungsservice zum Erfassen von Diagnoseinformationen zu einem Client für Sichern/Archivieren verwenden, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist.

Vorgehensweise

Führen Sie auf dem Clientsystem in der Befehlszeile die folgenden Befehle aus, um die Konfiguration des Clientverwaltungsservice anzuzeigen:

- Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

  ```
  Clientinstallationsverzeichnis/cms/bin/CmsConfig.sh list
  ```

  Dabei ist *Clientinstallationsverzeichnis* das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie beispielsweise bei der Standardclientinstallation den folgenden Befehl aus:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  Die Ausgabe sieht ähnlich wie die folgende aus:

  ```
  Listing CMS configuration

  server1.example.com:1500 NO_SSL HOSTNAME
  Capabilities: [LOG_QUERY]
      Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
      Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

- Geben Sie auf Windows-Clientsystemen den folgenden Befehl aus:

  ```
  Clientinstallationsverzeichnis\cms\bin\CmsConfig.bat list
  ```

  Dabei ist *Clientinstallationsverzeichnis* das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie beispielsweise bei der Standardclientinstallation den folgenden Befehl aus:

  ```
  C:\"Programme"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  Die Ausgabe sieht ähnlich wie die folgende aus:

  ```
  Listing CMS configuration

  server1.example.com:1500 NO_SSL HOSTNAME
  Capabilities: [LOG_QUERY]
      Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
      Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

Wenn der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist, wird in der Ausgabe die Position der Fehlerprotokolldatei angezeigt.
Der Ausgabetext wird aus der folgenden Konfigurationsdatei extrahiert:

- Auf Linux-Clientsystemen:

  ```
  Clientinstallationsverzeichnis/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
  ```

- Auf Windows-Clientsystemen:

  Clientinstallationsverzeichnis\cms\Liberty\usr\servers\cmsServer\client-configuration.xml

Wenn die Ausgabe keine Einträge enthält, müssen Sie die Datei client-configuration.xml konfigurieren. Anweisungen zum Konfigurieren dieser Datei finden Sie in Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren. Mit dem Befehl CmsConfig verify können Sie überprüfen, ob eine Knotendefinition in der Datei client-configuration.xml korrekt erstellt wurde.

Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren

Wenn für den Clientverwaltungsservice nicht die Standardkonfiguration verwendet wurde, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

Vorbereitende Schritte

Stellen Sie sicher, dass der Clientverwaltungsservice auf dem Clientsystem installiert und gestartet wurde. Überprüfen Sie, ob die Standardkonfiguration verwendet wird. Die Standardkonfiguration wird nicht verwendet, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Clientverwaltungsservice verwendet nicht die Standardportnummer 9028.
- Der Zugriff auf den Client für Sichern/Archivieren erfolgt nicht über dieselbe IP-Adresse wie für das Clientsystem, auf dem der Client für Sichern/Archivieren installiert ist. Eine andere IP-Adresse kann beispielsweise in den folgenden Situationen verwendet werden:
  - Das Computersystem verfügt über zwei Netzkarten. Der Client für Sichern/Archivieren ist für die Kommunikation in einem Netz konfiguriert, der Clientverwaltungsservice kommuniziert jedoch in dem anderen Netz.
  - Das Clientsystem ist mit DHCP (Dynamic Host Configuration Protocol) konfiguriert. Demzufolge wird dem Clientsystem dynamisch eine IP-Adresse zugeordnet, die während der vorherigen Operation des Clients für Sichern/Archivieren auf dem Server gespeichert wurde. Wenn das Clientsystem erneut gestartet wird, wird ihm möglicherweise eine andere IP-Adresse zugeordnet. Um sicherzustellen, dass das Operations Center das Clientsystem immer finden kann, müssen Sie einen vollständig qualifizierten Domänennamen angeben.

Vorgehensweise

Um das Operations Center für die Verwendung des Clientverwaltungsservice zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus.
2. Klicken Sie auf Details > Merkmale.
3. Geben Sie im Feld 'URL für Ferndiagnose' im Abschnitt 'Allgemein' die URL für den Clientverwaltungsservice auf dem Clientsystem an. Die Adresse muss mit `https` beginnen. In der folgenden Tabelle sind Beispiele für die URL für Ferndiagnose aufgeführt.

Typ der URL	**Beispiel**
Mit DNS-Hostname und Standardport 9028	https://server.example.com
Mit DNS-Hostname und einem anderen Port als dem Standardport	https://server.example.com:1599
Mit IP-Adresse und einem anderen Port als dem Standardport	https://192.0.2.0:1599

4. Klicken Sie auf Sichern.

Nächste Schritte

Über die Registerkarte Diagnose im Operations Center können Sie auf Clientdiagnoseinformationen, wie beispielsweise Clientprotokolldateien, zugreifen.

Implementierung abschließen

Nachdem die IBM Spectrum Protect- Lösung konfiguriert wurde und aktiv ist, testen Sie Sicherungsoperationen und konfigurieren Sie die Überwachung, um sicherzustellen, dass alles ordnungsgemäß funktioniert.

Vorgehensweise

1. Testen Sie Sicherungsoperationen, um sicherzustellen, dass Ihre Daten wie erwartet geschützt werden.
   a. Wählen Sie auf der Seite Clients im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf Sichern.
   b. Wählen Sie auf der Seite Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Datenbank sichern aus.
   c. Überprüfen Sie, ob die Sicherungsoperationen erfolgreich ohne Warnungen oder Fehlernachrichten ausgeführt wurden.
   Tipp: Sie können auch stattdessen die GUI des Clients für Sichern/Archivieren zum Sichern von Clientdaten verwenden und die Serverdatenbank sichern, indem Sie den Befehl BACKUP DB in einer Verwaltungsbefehlszeile ausgeben.
2. Konfigurieren Sie die Überwachung für Ihre Lösung, indem Sie die Anweisungen in Plattenspeicherlösung für einen einzelnen Standort überwachen ausführen.

Plattenspeicherlösung für einen einzelnen Standort überwachen

Überwachen Sie nach der Implementierung einer Plattenspeicherlösung für einen einzelnen Standort mit IBM Spectrum Protect die Lösung auf ihre korrekte Funktionsweise. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.

Informationen zu diesem Vorgang

Die Überwachung einer Lösung erfolgt bevorzugt über die Verwendung des Operations Center, das den Gesamtsystemstatus und den detaillierten Systemstatus in einer grafischen Benutzerschnittstelle bereitstellt. Darüber hinaus können Sie das Operations Center zum Generieren eines täglichen E-Mail-Berichts mit einer Zusammenfassung des Systemstatus konfigurieren.

In einigen Fällen möchten Sie vielleicht erweiterte Überwachungstools verwenden, um bestimmte Überwachungs- oder Fehlerbehebungstasks auszuführen.

Tipp: Wenn Sie planen, Probleme bei Clients für Sichern/Archivieren unter Linux- oder Windows-Betriebssystemen zu diagnostizieren, installieren Sie IBM Spectrum Protect-Clientverwaltungsservices auf jedem Computer, auf dem ein Client für Sichern/Archivieren installiert ist. Auf diese Art und Weise können Sie sicherstellen, dass die Schaltfläche Diagnose im Operations Center zur Diagnose von Problemen bei Clients für Sichern/Archivieren verfügbar ist. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen in Clientverwaltungsservice installieren aus.

Vorgehensweise

1. Führen Sie tägliche Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für tägliche Tasks.
2. Führen Sie regelmäßige Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für regelmäßige Tasks.
3. Um zu überprüfen, ob Ihre IBM Spectrum Protect-Lösung die die Lizenzierungsanforderungen erfüllt, führen Sie die Anweisungen in Lizenzeinhaltung überprüfen aus.
4. Informationen zur Konfiguration des Operations Center zum Erstellen von E-Mail-Statusberichten finden Sie in Systemstatus mithilfe von E-Mail-Berichten verfolgen.

Nächste Schritte

Beheben Sie alle erkannten Probleme. Wenn ein Problem durch Ändern der Konfiguration Ihrer Lösung behoben werden soll, führen Sie die Anweisungen in Operationen für eine Plattenspeicherlösung für einen einzelnen Standort verwalten aus. Die folgenden Ressourcen sind ebenfalls verfügbar:

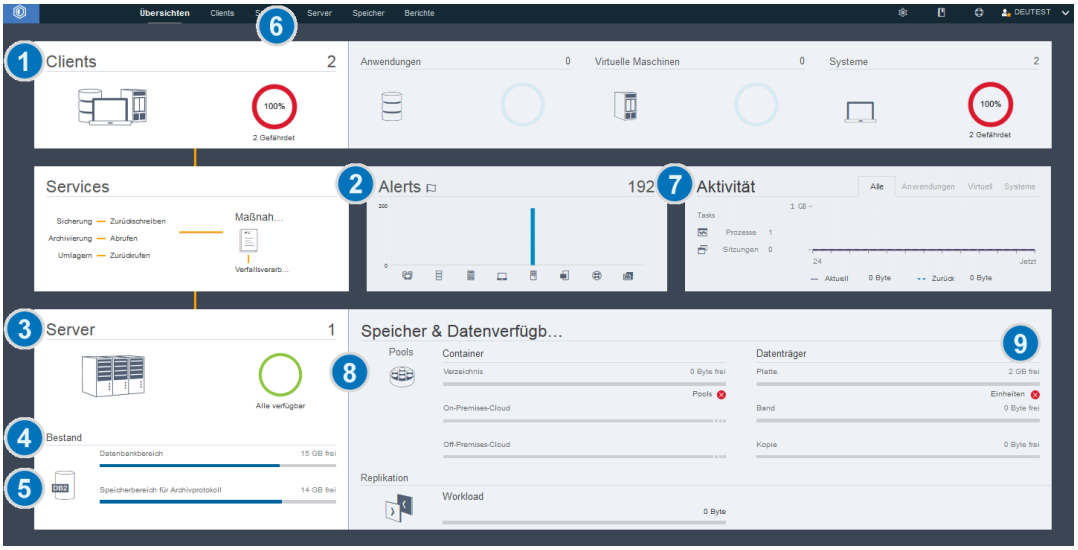
- Informationen zur Behebung von Leistungsproblemen finden Sie in Leistung.
- Informationen zur Behebung anderer Typen von Problemen finden Sie in Fehlerbehebung.

Prüfliste für tägliche Überwachungstasks

Um sicherzustellen, dass die täglichen Überwachungstasks für Ihre IBM Spectrum Protect-Lösung ausgeführt werden, überprüfen Sie die Prüfliste für tägliche Überwachungstasks.

Führen Sie die täglichen Überwachungstasks über die Seite Übersicht im Operations Center aus. Sie können auf die Seite Übersicht zugreifen, indem Sie das Operations Center öffnen und auf Übersichten klicken.

Die folgende Abbildung zeigt die Position zur Ausführung der jeweiligen Task.



Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.

In der folgenden Tabelle sind die täglichen Überwachungstasks sowie Anweisungen zur Ausführung jeder Task aufgeführt.

Tabelle 1. Tägliche Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
1 Bestimmen Sie, ob Clients vorhanden sind, bei denen die Gefahr besteht, dass sie aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen ungeschützt sind.	Um zu überprüfen, ob Clients gefährdet sind, suchen Sie nach einem Hinweis Gefährdet. Um Details anzuzeigen, klicken Sie auf den Bereich 'Clients'. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie die Clientfehler- und -planungsprotokolle anzeigen, indem Sie die folgenden Schritte ausführen: 1. Wählen Sie in der Tabelle 'Clients' den Client aus und klicken Sie auf Details. 2. Um ein Problem zu diagnostizieren, klicken Sie auf Diagnose.	Greifen Sie bei Clients, für die der Clientverwaltungsservice nicht installiert ist, auf das Clientsystem zu, um die Clientfehlerprotokolle zu überprüfen.
2 Bestimmen Sie, ob clientbezogene oder serverbezogene Fehler einen Bedienereingriff erfordern.	Um die Bewertung jedes zurückgemeldeten Alerts zu bestimmen, bewegen Sie den Mauszeiger im Bereich 'Alerts' über die Spalten.	Um zusätzliche Informationen zu Alerts anzuzeigen, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Alerts'. 2. Wählen Sie in der Tabelle 'Alerts' einen Alert aus. 3. Überprüfen Sie die Nachrichten im Fenster 'Aktivitätenprotokoll'. In dem Fenster werden zugehörige Nachrichten angezeigt, die vor und nach dem Auftreten des ausgewählten Alerts ausgegeben wurden.
3 Bestimmen Sie, ob die vom Operations Center verwalteten Server verfügbar sind, um Datenschutzservices für Clients bereitzustellen.	1. Um zu überprüfen, ob Server gefährdet sind, suchen Sie im Bereich 'Server' nach einem Hinweis Nicht verfügbar. 2. Um zusätzliche Informationen anzuzeigen, klicken Sie auf den Bereich 'Server'. 3. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.	Tipp: Wenn Sie ein Problem erkennen, das sich auf die Servermerkmale bezieht, aktualisieren Sie die Servermerkmale: 1. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details. 2. Um die Servermerkmale zu aktualisieren, klicken Sie auf Merkmale.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
4 Bestimmen Sie, ob für den Serverbestand, der aus der Serverdatenbank, der aktiven Protokolldatei und dem Archivprotokoll besteht, genügend Speicherbereich verfügbar ist.	1. Klicken Sie auf den Bereich 'Server'. 2. Zeigen Sie in der Spalte 'Status' der Tabelle den Status des Servers an und beheben Sie alle Probleme: ○ Normal Für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll ist genügend Speicherbereich verfügbar. ○ Kritisch Für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll ist nicht genügend Speicherbereich verfügbar. Sie müssen unverzüglich Speicherbereich hinzufügen; andernfalls werden die vom Server bereitgestellten Datenschutzservices unterbrochen. ○ Warnung Der Der Speicherbereich für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll wird knapp. Wenn diese Bedingung bestehen bleibt, müssen Sie Speicherbereich hinzufügen. ○ Nicht verfügbar Der Status kann nicht abgerufen werden. Stellen Sie sicher, dass der Server aktiv ist und keine Netzprobleme vorliegen. Dieser Status wird auch angezeigt, wenn die Überwachungsadministrator-ID gesperrt ist oder aus anderen Gründen auf dem Server nicht verfügbar ist. Diese ID hat den Namen IBM-OC-Name_des_Hub-Servers. ○ Nicht überwacht Nicht überwachte Server sind für den Hub-Server definiert, aber nicht für die Verwaltung durch das Operations Center konfiguriert. Um einen nicht überwachten Server zu konfigurieren, wählen Sie den Server aus und klicken Sie auf Peripherieserver überwachen.	Sie können auch auf der Seite Alerts nach zugehörigen Alerts suchen. Weitere Anweisungen zur Fehlerbehebung finden Sie in Serverprobleme beheben.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
5 Überprüfen Sie Operationen zur Sicherung der Serverdatenbank.	Um zu bestimmen, ob ein Server kürzlich gesichert wurde, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Server'. 2. Überprüfen Sie in der Tabelle 'Server' die Spalte 'Letzte Datenbanksicherung'.	Um detaillierte Informationen zu Sicherungsoperationen abzurufen, führen Sie die folgenden Schritte aus: 1. Wählen Sie in der Tabelle 'Server' eine Zeile aus und klicken Sie auf Details. 2. Bewegen Sie im Bereich 'Datenbanksicherung' den Mauszeiger über die Häkchen, um Informationen zu Sicherungsoperation zu überprüfen. Wenn eine Datenbank nicht kürzlich (beispielsweise innerhalb der letzten 24 Stunden) gesichert wurde, können Sie eine Sicherungsoperation starten: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Server'. 2. Wählen Sie in der Tabelle einen Server aus und klicken Sie auf Sichern. Um zu bestimmen, ob die Serverdatenbank für automatische Sicherungsoperationen konfiguriert ist, führen Sie die folgenden Schritte aus: 1. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Geben Sie den Befehl QUERY DB aus: `query db f=d` 3. Überprüfen Sie in der Ausgabe das Feld `Einheitenklassenname für Gesamtsicherungen`. Wenn eine Einheitenklasse angegeben ist, ist der Server für automatische Datenbanksicherungen konfiguriert.
6 Überwachen Sie andere Serververwaltungstasks. Serververwaltungstasks können die Ausführung von Zeitplänen für Verwaltungsbefehle, Verwaltungsscripts und zugehörigen Befehlen umfassen.	Um nach Informationen zu Prozessen zu suchen, die aufgrund von Serverproblemen fehlgeschlagen sind, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf Server > Verwaltung. 2. Um das zwei Wochen umfassende Verlaufsprotokoll eines Prozesses abzurufen, zeigen Sie Spalte 'History' an. 3. Um weitere Informationen zu einem geplanten Prozess abzurufen, bewegen Sie den Mauszeiger über das Kontrollkästchen, das dem Prozess zugeordnet ist.	Weitere Informationen zum Überwachen von Prozessen und Beheben von Problemen, finden Sie in der Onlinehilfe des Operations Center.
7 Überprüfen Sie, ob das Datenvolumen, das kürzlich an Server bzw. von Servern gesendet wurde, innerhalb des erwarteten Bereichs liegt.	• Um eine Übersicht über die Aktivität der letzten 24 Stunden abzurufen, zeigen Sie den Bereich 'Aktivität' an. • Um die Aktivität der letzten 24 Stunden mit der Aktivität der vorherigen 24 Stunden zu vergleichen, studieren Sie die Zahlen in den Bereichen 'Aktuell' und 'Vorherig'.	• Wenn mehr Daten als erwartet an den Server gesendet wurden, bestimmen Sie die Clients, die mehr Daten sichern und ermitteln Sie die Ursache. Möglicherweise funktioniert die clientseitige Datendeduplizierung nicht ordnungsgemäß. • Wenn weniger Daten als erwartet an den Server gesendet wurden, überprüfen Sie, ob Clientsicherungsoperationen gemäß Zeitplan ausgeführt werden.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
8 Stellen Sie sicher, dass Speicherpools zum Sichern von Clientdaten verfügbar sind.	1. Wenn im Bereich 'Speicher & Datenverfügbarkeit' Probleme angezeigt werden, klicken Sie auf Pools, um die Details anzuzeigen: ○ Wenn der Status Kritisch angezeigt wird, ist in dem Speicherpool nicht genügend Speicherbereich verfügbar oder der Speicherpool hat den Zugriffsstatus UNAVAILABLE (Nicht verfügbar). ○ Wenn der Status Warnung angezeigt wird, wird der Speicherbereich für den Speicherpool knapp oder der Speicherpool hat den Zugriffsstatus READONLY (Lesezugriff). 2. Um den verwendeten Speicherbereich, den freien Speicherbereich und den Gesamtspeicherbereich für Ihren ausgewählten Speicherpool anzuzeigen, bewegen Sie den Mauszeiger über die Einträge in der Spalte 'Verwendete Kapazität'.	Um die Speicherpoolkapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie eine Zeile in der Tabelle 'Speicherpools' aus und klicken Sie auf Details.
9 Stellen Sie sicher, dass Speichereinheiten für Sicherungsoperationen verfügbar sind.	Überprüfen Sie im Bereich 'Speicher & Datenverfügbarkeit' im Abschnitt 'Datenträger' unterhalb der Balken für die Kapazität den Status, der neben Einheiten angegeben ist. Wenn der Status Kritisch oder Warnung für eine Einheit angezeigt wird, müssen Sie das Problem untersuchen. Um Details anzuzeigen, klicken Sie auf Einheiten.	Platteneinheiten können aus den folgenden Gründen den Status 'Kritisch' oder 'Warnung' haben: • Für Einheitenklassen DISK können Datenträger offline sein oder den Zugriffsstatus READONLY (Lesezugriff) haben. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Datenträger angezeigt. • Für nicht gemeinsam genutzte Einheitenklassen FILE können Verzeichnisse offline sein. Außerdem ist unter Umständen nicht genügend freier Speicherbereich für die Zuordnung von Arbeitsdatenträgern verfügbar. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Verzeichnisse angezeigt. • Für gemeinsam genutzte Einheitenklassen FILE sind Laufwerke unter Umständen nicht verfügbar. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. In anderen Spalten der Tabelle 'Platteneinheiten' wird der Status der Laufwerke und Pfade angezeigt.

Prüfliste für regelmäßige Überwachungstasks

Um sicherzustellen, dass Ihre IBM Spectrum Protect-Lösung ordnungsgemäß funktioniert, führen Sie die Tasks in der Prüfliste für regelmäßige Überwachungstasks aus. Planen Sie regelmäßige Tasks häufig genug, sodass Sie potenzielle Probleme erkennen können, bevor diese wirklich problematisch werden.

Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder.

Tabelle 1. Regelmäßige Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie die Systemleistung.	Bestimmen Sie den für Clientsicherungsoperationen erforderlichen Zeitraum: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Suchen Sie den Server, der dem Client zugeordnet ist. 2. Klicken Sie auf Server. Wählen Sie den Server aus und klicken Sie auf Details. 3. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die in den letzten 24 Stunden abgeschlossenen wurden, klicken Sie auf Abgeschlossene Tasks. 4. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die vor mehr als 24 Stunden abgeschlossen wurden, verwenden Sie den Befehl QUERY ACTLOG. Führen Sie die Anweisungen in QUERY ACTLOG (Aktivitätenprotokoll abfragen) aus. 5. Wenn die Dauer von Clientsicherungsoperationen zunimmt, ohne dass ein offensichtlicher Grund erkennbar ist, überprüfen Sie Ursache. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie Leistungsprobleme für den Client für Sichern/Archivieren diagnostizieren, indem Sie die folgenden Schritte ausführen: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. 2. Wählen Sie einen Client für Sichern/Archivieren aus und klicken Sie auf Details. 3. Um Clientprotokolle abzurufen, klicken Sie auf Diagnose.	Informationen zur Verkürzung der Zeit, die der Client zum Sichern von Daten auf dem Server benötigt, finden Sie in Häufig auftretende Clientleistungsprobleme lösen. Suchen Sie nach Leistungsengpässen. Anweisungen finden Sie in Leistungsengpässe identifizieren. Informationen zur Identifikation und Behebung anderer Leistungsprobleme finden Sie in Leistung.
Bestimmen Sie die Platteneinsparungen, die durch die Datendeduplizierung bereitgestellt werden.	1. Klicken Sie auf der Seite Übersicht im Operations Center auf Pools. 2. Wählen Sie einen Pool aus und klicken Sie auf Kurzübersicht. 3. Zeigen Sie im Bereich 'Datendeduplizierung' die Zeile 'Eingesparter Speicherbereich' an.	Um für die erweiterte Überwachung detaillierte Statistikdaten zu dem Datendeduplizierungsprozess für einen bestimmten Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abzurufen, führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Fordern Sie einen Statistikbericht an, indem Sie den Befehl GENERATE DEDUPSTATS ausgeben. Führen Sie die Anweisungen in GENERATE DEDUPSTATS (Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool generieren) aus. 3. Zeigen Sie den Statistikbericht an, indem Sie den Befehl QUERY DEDUPSTATS ausgeben. Führen Sie die Anweisungen in QUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen) aus.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Stellen Sie sicher, dass aktuelle Sicherungsdateien für Einheitenkonfigurations- und Datenträgerprotokolldaten gesichert werden.	Greifen Sie auf Ihre Speicherpositionen zu, um sicherzustellen, dass die Dateien verfügbar sind. Die bevorzugte Methode ist die Sicherung der Dateien an zwei Positionen.
	Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, führen Sie die folgenden Schritte aus:
	1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.
	2. Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, geben Sie die folgenden Befehle aus:
	`query option volhistory`
	`query option devconfig`
	3. Überprüfen Sie in der Ausgabe die Spalte 'Optionseinstellung', um die Dateipositionen zu finden.
	Wenn ein Katastrophenfall eintritt, sind sowohl die Protokolldatei für Datenträger als auch die Einheitenkonfigurationsdatei für die Zurückschreibung der Serverdatenbank erforderlich.	

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Bestimmen Sie, ob für das Instanzverzeichnisdateisystem genügend Speicherbereich verfügbar ist.	Stellen Sie sicher, dass im Instanzverzeichnisdateisystem mindestens 20 % freier Speicherbereich verfügbar ist. Führen Sie die für Ihr Betriebssystem zutreffende Aktion aus:
	• AIX-BetriebssystemeUm den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -g Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Linux-BetriebssystemeUm den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -h Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Windows-BetriebssystemeKlicken Sie in Windows-Explorer mit der rechten Maustaste auf das Dateisystem und klicken Sie auf Eigenschaften. Zeigen Sie die Kapazitätsdaten an.
	Die bevorzugte Position des Instanzverzeichnisses ist von dem Betriebssystem abhängig, unter dem der Server installiert ist:
	• AIX-Betriebssysteme Linux-Betriebssysteme /home/tsminst1/tsminst1
	• Windows-Betriebssysteme C:\tsminst1
	Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.	

Ermitteln Sie nicht erwartete Clientaktivität.	Um im Rahmen der Überwachung der Clientaktivität zu bestimmen, ob das Datenvolumen das erwartete Volumen überschreitet, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Clients'. 2. Um die Aktivität der vergangen zwei Wochen anzuzeigen, doppelklicken Sie auf einen beliebigen Client. 3. Um die Anzahl Byte anzuzeigen, die an den Client gesendet wurden, klicken Sie auf die Registerkarte Merkmale. 4. Zeigen Sie im Bereich 'Letzte Sitzung' die Zeile 'An Client gesendet' an.	Wenn Sie auf einen Client in der Tabelle 'Clients' doppelklicken, wird im Bereich Aktivität im Lauf von 2 Wochen das Datenvolumen angezeigt, das vom Client jeden Tag an den Server gesendet wurde.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie das Speicherpoolwachstum im Laufe der Zeit.	1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Pools'. 2. Um die Kapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie einen Pool aus und klicken Sie auf Details.	Tipps: • Um die Zeit anzugeben, die verstreichen muss, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool oder einem Cloud-Containerspeicherpool entfernt werden, nachdem sie nicht mehr vom Bestand referenziert werden, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus. 2. Klicken Sie auf Details > Merkmale. 3. Geben Sie im Feld `Verzögerungszeitraum für Containerwiederverwendung` den Zeitraum an. • Bestimmen Sie die Datendeduplizierungsleistung für Verzeichniscontainer- und Cloud-Containerspeicherpools mithilfe des Befehls GENERATE DEDUPSTATS. • Um Deduplizierungsstatistikdaten für einen Speicherpool anzuzeigen, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus. 2. Klicken Sie auf Details > Merkmale. Verwenden Sie dementsprechend den Befehl QUERY EXTENTUPDATES, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainer- oder Cloud-Containerspeicherpools anzuzeigen. Anhand der Befehlsausgabe können Sie die Datenbereiche bestimmen, die nicht mehr referenziert werden, sowie die Datenbereiche, die zum Löschen vom System auswählbar sind. Überwachen Sie in der Ausgabe die Anzahl Datenbereiche, die zum Löschen vom System auswählbar sind. Diese Messgröße steht in direkten Zusammenhang mit dem Umfang des freien Speicherbereichs in dem Containerspeicherpool. • Um den Umfang des physischen Speicherbereichs anzuzeigen, der von einem Dateibereich nach dem Entfernen der Datendeduplizierungseinsparungen belegt wird, verwenden Sie den Befehl select * from occupancy. Die Befehlsausgabe umfasst den Wert für LOGICAL_MB. LOGICAL_MB gibt an, wie viel Speicherbereich von diesem Dateibereich belegt wird.
Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass die Start- und Endzeiten von Clientzeitplänen Ihre Geschäftsanforderungen erfüllen.	Klicken Sie auf der Seite Übersicht im Operations Center auf Clients > Zeitpläne. In der Tabelle 'Zeitpläne' wird in der Spalte 'Start' die konfigurierte Startzeit für die geplante Operation angezeigt. Um anzuzeigen, wann die letzte Operation gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	Tipp: Wenn die Ausführung einer Clientoperation länger als erwartet dauert, empfangen Sie unter Umständen eine Warnung. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite 'Übersicht' im Operations Center den Mauszeiger über Clients und klicken Sie auf Zeitpläne. 2. Wählen Sie einen Zeitplan aus und klicken Sie auf Details. 3. Zeigen Sie die Details eines Zeitplans an, indem Sie auf den blauen Pfeil neben der Zeile klicken. 4. Geben Sie im Feld Ausführungszeitalert die Uhrzeit an, zu der eine Warnung ausgegeben wird, wenn die geplante Operation nicht ausgeführt wird. 5. Klicken Sie auf Sichern.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass die Start- und Endzeiten von Verwaltungstasks Ihre Geschäftsanforderungen erfüllen.	Klicken Sie auf der Seite Übersicht im Operations Center auf Server > Verwaltung. Überprüfen Sie in der Tabelle 'Verwaltung' die Informationen in der Spalte 'Letzte Ausführungsdauer'. Um anzuzeigen, wann die letzte Verwaltungstask gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	Tipp: Wenn die Ausführung einer Verwaltungstask zu lange dauert, ändern Sie die Startzeit oder die maximale Ausführungszeit. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Um die Startzeit oder die maximale Ausführungszeit für eine Task zu ändern, geben Sie den Befehl UPDATE SCHEDULE aus. Anweisungen finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).

Zugehörige Verweise:
QUERY ACTLOG (Aktivitätenprotokoll abfragen)
UPDATE STGPOOL (Speicherpool aktualisieren)
QUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)

Lizenzeinhaltung überprüfen

Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen. Planen Sie anhand dieser Informationen den weiteren Kauf von Lizenzen.

Informationen zu diesem Vorgang

Die Methode zur Überprüfung der Einhaltung der Lizenzbedingungen durch Ihre Lösung variiert abhängig von den Bedingungen Ihrer IBM Spectrum Protect-Lizenzvereinbarung.

Front-End-Kapazitätslizenzierung
: Das Front-End-Modell bestimmt die Lizenzvoraussetzungen auf der Basis des zurückgemeldeten Volumens an primären Daten, das von Clients gesichert wird. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme.

Back-End-Kapazitätslizenzierung
: Das Back-End-Modell bestimmt Lizenzvoraussetzungen auf der Basis der Terabyte Daten, die in primären Speicherpools und Repositorys gespeichert werden.
Tipps:

- Um die Genauigkeit von Schätzungen der Front-End- und Back-End-Kapazität zu gewährleisten, installieren Sie die neueste Version der Client-Software auf jedem Clientknoten.
- Die Informationen zur Front-End- und Back-End-Kapazität im Operations Center dienen zum Zweck der Planung und Schätzung.

PVU-Lizenzierung
: Das PVU-Modell basiert auf der Nutzung von PVUs durch Servereinheiten.
Wichtig: Die von IBM Spectrum Protect bereitgestellten PVU-Berechnungen werden als Schätzungen betrachtet und sind nicht rechtsverbindlich. Die von IBM Spectrum Protect zurückgemeldeten PVU-Lizenzinformationen werden nicht als zulässiger Ersatz für das IBM® License Metric Tool angesehen.

Die neuesten Informationen zu Lizenzierungsmodellen finden Sie in den Informationen zu Produktdetails und Lizenzen auf der Website der IBM Spectrum Protect-Produktfamilie. Wenden Sie sich bei Fragen oder Problemstellungen zu Lizenzierungsanforderungen an Ihren IBM Spectrum Protect-Software-Provider.

Vorgehensweise

Führen Sie zur Überwachung der Lizenzeinhaltung die Schritte aus, die den Bedingungen Ihrer Lizenzvereinbarung entsprechen.
Tipp: Das Operations Center stellt einen E-Mail-Bericht bereit, in dem die Front-End- und Back-End-Kapazitätsnutzung zusammengefasst sind. Berichte können automatisch regelmäßig an einen oder mehrere Empfänger gesendet werden. Klicken Sie für die Konfiguration und Verwaltung von E-Mail-Berichten in der Menüleiste des Operations Center auf Berichte.

Option	Bezeichnung

Option	Bezeichnung
Front-End-Modell	a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen und klicken Sie auf Lizenzierung. Die Schätzung der Front-End-Kapazität wird auf der Seite 'Front-End-Nutzung' angezeigt. b. Wenn in der Spalte 'Keine Zurückmeldung' ein Wert angezeigt wird, klicken Sie auf die Zahl, um Clients zu identifizieren, von denen keine Kapazitätsnutzung zurückgemeldet wurde. c. Um die Kapazität für Clients zu schätzen, für die keine Kapazitätsnutzung zurückgemeldet wurde, rufen Sie die folgende FTP-Site auf, auf der Tools und Anweisungen zum Messen der Kapazität bereitgestellt werden: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Um die Front-End-Kapazität mithilfe eines Scripts zu messen, führen Sie die Anweisungen im aktuellen Lizenzierungshandbuch aus. d. Addieren Sie den Operations Center-Schätzwert und alle Schätzwerte, die Sie mithilfe eines Scripts ermittelt haben. e. Überprüfen Sie, ob die geschätzte Kapazität die Bedingungen Ihrer Lizenzvereinbarung einhält.
Back-End-Modell	Einschränkung: Wenn der Quellen- und der Zielreplikationsserver nicht dieselben Maßnahmeneinstellungen verwenden, können Sie das Operations Center nicht zur Überwachung der Back-End-Kapazitätsnutzung für replizierte Clients verwenden. Informationen zur Schätzung der Kapazitätsnutzung für diese Clients finden Sie in Technote 1656476. a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen und klicken Sie auf Lizenzierung. b. Klicken Sie auf die Registerkarte Back-End. c. Überprüfen Sie, ob das geschätzte Datenvolumen die Bedingungen Ihrer Lizenzvereinbarung einhält.
PVU-Modell	Informationen zur Vorgehensweise beim Prüfen der Einhaltung der PVU-Lizenzbedingungen finden Sie in Einhaltung des PVU-Lizenzierungsmodells prüfen.

Systemstatus mithilfe von E-Mail-Berichten verfolgen

Konfigurieren Sie das Operations Center für die Generierung von E-Mail-Berichten zur Zusammenfassung des Systemstatus. Sie können eine Mail-Server-Verbindung konfigurieren, Berichtseinstellungen ändern und wahlweise angepasste SQL-Berichte erstellen.

Vorbereitende Schritte

Bevor Sie E-Mail-Berichte konfigurieren, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Es ist ein SMTP-Host-Server (SMTP = Simple Mail Transfer Protocol) verfügbar, um Berichte als E-Mail senden und empfangen zu können. Der SMTP-Server muss als offenes Mail-Relay konfiguriert sein. Außerdem müssen Sie sicherstellen, dass der IBM Spectrum Protect-Server, der E-Mail-Nachrichten sendet, Zugriff auf den SMTP-Server hat. Wenn das Operations Center auf einem anderen Computer installiert ist, ist für diesen Computer kein Zugriff auf den SMTP-Server erforderlich.
- Um E-Mail-Berichte konfigurieren zu können, müssen Sie über Systemberechtigung für den Server verfügen.
- Um die Empfänger anzugeben, können Sie eine oder mehrere E-Mail-Adressen oder Administrator-IDs eingeben. Wenn eine Administrator-ID eingegeben werden soll, muss die ID auf dem Hub-Server registriert sein und der ID muss eine E-Mail-Adresse zugeordnet sein. Eine E-Mail-Adresse für einen Administrator können Sie mithilfe des Parameters EMAILADDRESS im Befehl UPDATE ADMIN angeben.

Informationen zu diesem Vorgang

Sie können das Operations Center zum Senden eines Berichts über allgemeine Operationen, eines Lizenzeinhaltungsberichts und eines oder mehrerer angepasster Berichte, die SQL-Anweisungen SELECT zum Abfragen verwalteter Server verwenden, konfigurieren.

Vorgehensweise

Um E-Mail-Berichte zu konfigurieren und zu verwalten, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Berichte.
2. Wenn noch keine E-Mail-Server-Verbindung konfiguriert ist, klicken Sie auf Mail-Server konfigurieren und füllen Sie die Felder aus. Nach der Konfiguration des Mail-Servers sind der Bericht über allgemeine Operationen und der Lizenzeinhaltungsbericht aktiviert.
3. Um Berichtseinstellungen zu ändern, wählen Sie einen Bericht aus, klicken Sie auf Details und aktualisieren Sie das Formular.
4. Optional: Um einen angepassten SQL-Bericht hinzuzufügen, klicken Sie auf + Bericht und füllen Sie die Felder aus.

Tipp: Um einen Bericht sofort auszuführen und zu senden, wählen Sie den Bericht aus und klicken Sie auf Senden.

Ergebnisse

Aktivierte Berichte werden gemäß den angegebenen Einstellungen gesendet.
Zugehörige Verweise:
UPDATE ADMIN (Administrator aktualisieren)

Operationen für eine Plattenspeicherlösung für einen einzelnen Standort verwalten

Verwenden Sie diese Informationen, um Operationen für eine Plattenspeicherlösung für einen einzelnen Standort mit IBM Spectrum Protect zu verwalten, die einen Server umfasst und Datendeduplizierung für einen einzelnen Standort verwendet.

- Operations Center verwalten
  Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.
- Anwendungen, virtuelle Maschinen und Systeme schützen
  Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherungszeitplan zum Schützen der Clientdaten auswählen.
- Datenspeicher verwalten
  Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.
- IBM Spectrum Protect-Server schützen
  Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.
- Server stoppen und starten
  Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.
- Durchführung eines Upgrades für den Server planen
  Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.
- Vorbereitungen für einen Ausfall oder eine Systemaktualisierung
  Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.
- Plan zur Wiederherstellung nach einem Katastrophenfall implementieren
  Implementieren Sie eine Strategie zur Wiederherstellung nach einem Katastrophenfall, um Ihre Anwendungen in einem Katastrophenfall wiederherstellen und hohe Serververfügbarkeit sicherstellen zu können.
- Wiederherstellung nach einem Systemausfall
  Bei IBM Spectrum Protect-Plattenspeicherlösungen für einen einzelnen Standort können Sie den Bestand nur lokal wiederherstellen und die Datenbank zum Schutz Ihrer Daten zurückschreiben.

Operations Center verwalten

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.

- Peripherieserver hinzufügen und entfernen
  In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.
- Web-Server starten und stoppen
  Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Assistenten für die Erstkonfiguration erneut starten
  Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Hub-Server ändern
  Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.
- Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben
  Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

Peripherieserver hinzufügen und entfernen

In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.

Informationen zu diesem Vorgang

Die Peripherieserver senden Alerts und Statusinformationen an den Hub-Server. Das Operations Center zeigt eine konsolidierte Sicht der Alerts und Statusinformationen für den Hub-Server und alle Peripherieserver.

- Peripherieserver hinzufügen
  Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.
- Peripherieserver entfernen
  Sie können einen Peripherieserver aus dem Operations Center entfernen.

Peripherieserver hinzufügen

Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.

Vorbereitende Schritte

Die Kommunikation zwischen dem Peripherieserver und dem Hub-Server muss unter Verwendung des Protokolls Transport Layer Security (TLS) geschützt werden. Um die Kommunikation zu schützen, fügen Sie das Zertifikat des Peripherieservers der Truststore-Datei des Hub-Servers hinzu.

Vorgehensweise

1. Klicken Sie in der Menüleiste des Operations Center auf Server. Die Seite Server wird geöffnet.

   In der Tabelle auf der Seite Server könnte ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass - obwohl ein Administrator diesen Server mit dem Befehl DEFINE SERVER für den Hub-Server definiert hat - der Server noch nicht als Peripherieserver konfiguriert ist.

2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
   - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird und die sichere SSL-/TLS-Kommunikation nicht erforderlich ist, klicken Sie in der Menüleiste der Tabelle auf +Peripherieserver.
3. Geben Sie die erforderlichen Informationen an und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.
   Tipp: Wenn der Aufbewahrungszeitraum für Ereignissätze des Servers weniger als 14 Tage beträgt, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

Peripherieserver entfernen

Sie können einen Peripherieserver aus dem Operations Center entfernen.

Informationen zu diesem Vorgang

Unter Umständen müssen Sie einen Peripherieserver in den folgenden Situationen entfernen:

- Der Peripherieserver soll von einem Hub-Server auf einen anderen Hub-Server versetzt werden.
- Der Peripherieserver soll stillgelegt werden.

Vorgehensweise

Um den Peripherieserver aus der Gruppe der Server zu entfernen, die vom Hub-Server verwaltet werden, führen Sie die folgenden Schritte aus:

1. Geben Sie in der IBM Spectrum Protect-Befehlszeile auf dem Hub-Server den folgenden Befehl aus:

   ```
   QUERY MONITORSETTINGS
   ```

2. Kopieren Sie in der Ausgabe des Befehls den Namen im Feld Überwachte Gruppe.
3. Geben Sie auf dem Hub-Server den folgenden Befehl aus; dabei ist *Gruppenname* der Name der überwachten Gruppe und *Mitgliedsname* der Name des Peripherieservers:

   ```
   DELETE GRPMEMBER Gruppenname Mitgliedsname
   ```

4. Optional: Wenn der Peripherieserver von einem Hub-Server auf einen anderen Hub-Server versetzt werden soll, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Alertausgabe und Überwachung auf dem Peripherieserver inaktivieren, indem Sie auf dem Peripherieserver die folgenden Befehle ausgeben:

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. Optional: Wenn die Definition des Peripherieservers für andere Zwecke verwendet wird, wie beispielsweise unternehmensweite Konfiguration, Befehlsweiterleitung, Speichern virtueller Datenträger oder Speicherarchivverwaltung, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Definition des Peripherieservers auf dem Hub-Server löschen, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

   ```
   DELETE SERVER Name_des_Peripherieservers
   ```

Web-Server starten und stoppen

Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.

Vorgehensweise

1. Stoppen Sie den Web-Server.
   - AIX-BetriebssystemeGeben Sie im Verzeichnis /*Installationsverzeichnis*/ui/utils (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:

     ```
     ./stopserver.sh
     ```

   - Linux-BetriebssystemeGeben Sie den folgenden Befehl aus:

     ```
     service opscenter.rc stop
     ```

   - Windows-BetriebssystemeStoppen Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.
2. Starten Sie den Web-Server.
   - AIX-BetriebssystemeGeben Sie im Verzeichnis /*Installationsverzeichnis*/ui/utils (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:

     ```
     ./startserver.sh
     ```

   - Linux-BetriebssystemeGeben Sie die folgenden Befehle aus:

     Starten Sie den Server:

     ```
     service opscenter.rc start
     ```

     Starten Sie den Server erneut:

     ```
     service opscenter.rc restart
     ```

     Bestimmen Sie, ob der Server aktiv ist:

     ```
     service opscenter.rc status
     ```

   - Windows-BetriebssystemeStarten Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.

Assistenten für die Erstkonfiguration erneut starten

Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.

Vorbereitende Schritte

Um die folgenden Einstellungen zu ändern, verwenden Sie die Seite Einstellungen im Operations Center, anstatt den Assistenten für die Erstkonfiguration erneut zu starten:

- Häufigkeit, mit der Statusdaten aktualisiert werden
- Dauer, die Alerts aktiv, inaktiv oder geschlossen bleiben
- Bedingungen, die angeben, dass Clients gefährdet sind

Die Hilfe des Operations Center enthält weitere Informationen zum Ändern dieser Einstellungen.

Informationen zu diesem Vorgang

Um den Assistenten für die Erstkonfiguration erneut zu starten, müssen Sie eine Merkmaldatei löschen, die Informationen zur Hub-Server-Verbindung enthält. Alle für den Hub-Server konfigurierten Einstellungen für Alertausgabe, Überwachung oder Gefährdung bzw. serverübergreifenden Einstellungen werden nicht gelöscht. Diese Einstellungen werden als Standardeinstellungen im Konfigurationsassistenten verwendet, wenn der Assistent erneut gestartet wird.

Vorgehensweise

1. Stoppen Sie den Web-Server des Operations Center.
2. Wechseln Sie auf dem Computer, auf dem das Operations Center installiert ist, in das folgende Verzeichnis (dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist):
   - AIX-Betriebssysteme Linux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

   Beispiel:
   - AIX-Betriebssysteme Linux-Betriebssysteme/opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssysteme:\Programme\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. Löschen Sie im Verzeichnis guiServer die Datei serverConnection.properties.
4. Starten Sie den Web-Server des Operations Center.
5. Öffnen Sie das Operations Center.
6. Rekonfigurieren Sie mithilfe des Konfigurationsassistenten das Operations Center. Geben Sie ein neues Kennwort für die Überwachungsadministrator-ID an.
7. Aktualisieren auf jedem Peripherieserver, der bereits zuvor mit dem Hub-Server verbunden war, das Kennwort für die Überwachungsadministrator-ID, indem Sie den folgenden Befehl in der IBM Spectrum Protect-Befehlszeilenschnittstelle ausgeben:

   ```
   UPDATE ADMIN IBM-OC-Name_des_Hub-Servers neues_Kennwort
   ```

   Einschränkung: Übernehmen Sie alle anderen Einstellungen für diese Administrator-ID unverändert. Nachdem Sie das Anfangskennwort angegeben haben, wird dieses Kennwort automatisch vom Operations Center verwaltet.

Hub-Server ändern

Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.

Vorgehensweise

1. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut. Im Rahmen dieser Prozedur löschen Sie die bestehende Hub-Server-Verbindung.
2. Verwenden Sie den Assistenten, um das Operations Center für die Verbindung zu dem neuen Hub-Server zu konfigurieren.

Zugehörige Tasks:
Assistenten für die Erstkonfiguration erneut starten

Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben

Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

Vorgehensweise

Um die Konfiguration zurückzuschreiben, führen Sie die folgenden Schritte aus:

1. Stoppen Sie den Web-Server des Operations Center.
2. Dekonfigurieren Sie den Hub-Server, indem Sie die folgenden Schritte ausführen:
   a. Geben Sie auf dem Hub-Server die folgenden Befehle aus:

      ```
      SET MONITORINGADMIN ""
      SET MONITOREDSERVERGROUP ""
      SET STATUSMONITOR OFF
      SET ALERTMONITOR OFF
      REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
      ```

      Tipp: `IBM-OC-Name_des_Hub-Servers` ist die Überwachungsadministrator-ID, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.
   b. Setzen Sie das Kennwort für den Hub-Server zurück, indem Sie den folgenden Befehl auf dem Hub-Server ausgeben:

      ```
      SET SERVERPASSWORD ""
      ```

      Achtung: Führen Sie diesen Schritt nicht aus, wenn der Hub-Server für andere Server für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation konfiguriert ist.
3. Dekonfigurieren Sie alle Peripherieserver, indem Sie die folgenden Schritte ausführen:

a. Um zu bestimmen, ob noch Peripherieserver vorhanden sind, die als Mitglieder der Servergruppe definiert sind, geben Sie auf dem Hub-Server den folgenden Befehl aus:

```
QUERY SERVERGROUP IBM-OC-Name_des_Hub-Servers
```

Tipp: `IBM-OC-Name_des_Hub-Servers` ist der Name der überwachten Servergruppe, die bei der Konfiguration des ersten Peripherieservers automatisch erstellt wurde. Dieser Servergruppenname stimmt auch mit der Überwachungsadministrator-ID überein, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.

b. Um Peripherieserver aus der Servergruppe zu löschen, geben Sie auf dem Hub-Server für jeden Peripherieserver den folgenden Befehl aus:

```
DELETE GRPMEMBER IBM-OC-Name_des_Hub-Servers Name_des_Peripherieservers
```

c. Nachdem alle Peripherieserver aus der Servergruppe gelöscht wurden, geben Sie auf dem Hub-Server die folgenden Befehle aus:

```
DELETE SERVERGROUP IBM-OC-Name_des_Hub-Servers
SET MONITOREDSERVERGROUP ""
```

d. Geben Sie auf jedem Peripherieserver die folgenden Befehle aus:

```
REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

e. Löschen Sie die Definition des Hub-Servers, indem Sie auf jedem Peripherieserver den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Hub-Servers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Definition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

f. Löschen Sie die Definition jedes Peripherieservers, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Peripherieservers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Serverdefinition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

4. Schreiben Sie die Standardeinstellungen auf jeden Server zurück, indem Sie die folgenden Befehle ausgeben:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut.

Zugehörige Tasks:
Assistenten für die Erstkonfiguration erneut starten
Web-Server starten und stoppen

Anwendungen, virtuelle Maschinen und Systeme schützen

Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherungszeitplan zum Schützen der Clientdaten auswählen.

- Clients hinzufügen
  Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.
- Clientoperationen verwalten
  Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.
- Client-Upgrades verwalten
  Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.
- Clientknoten stilllegen
  Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.

- Daten zum Freigeben von Speicherbereich inaktivieren
  In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegeben Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

Clients hinzufügen

Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.

Informationen zu diesem Vorgang

Die Prozedur beschreibt grundlegende Schritte zum Hinzufügen eines Clients. Spezifischere Anweisungen zum Konfigurieren von Clients enthält die Dokumentation für das auf dem Clientknoten installierte Produkt. Folgende Typen von Clients können vorhanden sein:

Anwendungsclientknoten
: Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Systemclientknoten
: Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

VM-Clientknoten
: Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Vorgehensweise

Um einen Client hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Software aus, die auf dem Clientknoten installiert werden soll, und planen Sie die Installation. Führen Sie die Anweisungen in Client-Software auswählen und Installation planen aus.
2. Geben Sie an, wie Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Regeln zum Sichern und Archivieren von Clientdaten angeben aus.
3. Geben Sie an, wann Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Sicherungs- und Archivierungsoperationen planen aus.
4. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, registrieren Sie den Client. Führen Sie die Anweisungen in Clients registrieren aus.
5. Um einen Clientknoten zu schützen, installieren und konfigurieren Sie die ausgewählte Software auf dem Clientknoten. Führen Sie die Anweisungen in Clients installieren und konfigurieren aus.

Client-Software auswählen und Installation planen

Unterschiedliche Typen von Daten erfordern unterschiedliche Typen von Schutz. Geben Sie den Typ der Daten an, die geschützt werden müssen, und wählen Sie die geeignete Software aus.

Informationen zu diesem Vorgang

Das bevorzugte Verfahren ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installieren, für das der Clientakzeptor keine Zeitpläne ausführt, müssen Sie die Konfigurationsanweisungen in der Produktdokumentation ausführen, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

Vorgehensweise

Wählen Sie abhängig von Ihrer Zielsetzung die zu installierenden Produkte aus und lesen Sie die Installationsanweisungen.
Tipp: Wenn Sie die Client-Software jetzt installieren, müssen Sie auch die in Clients installieren und konfigurieren beschriebenen Clientkonfigurationstasks ausführen, bevor Sie den Client verwenden können.

Ziel	Produkt und Beschreibung	Installationsanweisungen

Ziel	Produkt und Beschreibung	Installationsanweisungen
Schutz eines Dateiservers oder einer Workstation	Der Client für Sichern/Archivieren sichert und archiviert Dateien und Verzeichnisse von Dateiservern und Workstations in Speicher. Es ist auch möglich, Sicherungsversionen und archivierte Kopien von Dateien zurückzuschreiben und abzurufen.	• Anforderungen für den Client für Sichern/Archivieren • UNIX- und Linux-Clients für Sichern/Archivieren installieren • Windows-Client für Sichern/Archivieren installieren
Schutz von Anwendungen mit Momentaufnahmesicherungs- und -zurückschreibungsfunktionalität	IBM Spectrum Protect Snapshot schützt Daten mit integrierter anwendungsgesteuerter Momentaufnahmesicherungs- und -zurückschreibungsfunktionalität. Sie können Daten schützen, die von IBM DB2-Datenbanksoftware sowie SAP-, Oracle-, Microsoft Exchange Server- und Microsoft SQL Server-Anwendungen gespeichert werden.	• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
Schutz einer E-Mail-Anwendung auf einem IBM Domino-Server	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass IBM Domino-Server heruntergefahren werden.	• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) • Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)
Schutz einer E-Mail-Anwendung auf einem Server mit Microsoft Exchange Server	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass Server mit Microsoft Exchange Server heruntergefahren werden.	Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Schutz einer IBM DB2-Datenbank	Mithilfe der Anwendungsprogrammierschnittstelle (API) des Clients für Sichern/Archivieren können DB2-Daten auf dem IBM Spectrum Protect-Server gesichert werden.	IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Schutz einer IBM Informix-Datenbank	Mithilfe der API des Clients für Sichern/Archivieren können Informix-Daten auf dem IBM Spectrum Protect-Server gesichert werden.	IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Schutz einer Microsoft SQL-Datenbank	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server schützt Microsoft SQL-Daten.	Data Protection for SQL Server unter Windows Server Core installieren
Schutz einer Oracle-Datenbank	IBM Spectrum Protect for Databases: Data Protection for Oracle schützt Oracle-Daten.	Installation von Data Protection for Oracle
Schutz einer SAP-Umgebung	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP stellt Schutz bereit, der für SAP-Umgebungen angepasst ist. Das Produkt dient der Verbesserung der Verfügbarkeit von SAP-Datenbankservern und der Verringerung des Verwaltungsaufwands.	• IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren • IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren

Ziel	Produkt und Beschreibung	Installationsanweisungen
Schutz einer virtuellen Maschine	IBM Spectrum Protect for Virtual Environments stellt Schutz bereit, der für virtuelle Microsoft Hyper-V- und VMware-Umgebungen angepasst ist. Mithilfe von IBM Spectrum Protect for Virtual Environments können Sie immer inkrementelle Sicherungen erstellen, die auf einem zentralen Server gespeichert werden, Sicherungsmaßnahmen erstellen und virtuelle Maschinen oder einzelne Dateien zurückschreiben. Sie können auch stattdessen den Client für Sichern/Archivieren zum Sichern und Zurückschreiben einer vollständigen virtuellen VMware- oder Microsoft Hyper-V-Maschine verwenden. Es ist auch möglich, Dateien oder Verzeichnisse von einer virtuellen VMware-Maschine zu sichern und zurückzuschreiben.	• Data Protection for Microsoft Hyper-V installieren • Installation und Upgrade für Data Protection for VMware durchführen • IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)

Tipp: Um den Client für die Speicherbereichsverwaltung zu verwenden, können Sie IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows installieren.

Regeln zum Sichern und Archivieren von Clientdaten angeben

Stellen Sie vor dem Hinzufügen eines Clients sicher, dass entsprechende Regeln zum Sichern und Archivieren der Clientdaten angegeben sind. Während des Clientregistrierungsprozesses ordnen Sie den Clientknoten einer Maßnahmendomäne zu, die die Regeln enthält, die die Regeln enthält, die steuern, wie und wann Clientdaten gespeichert werden.

Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Maßnahmen, die für Ihre Lösung konfiguriert sind, vertraut sind und wissen, dass für die Maßnahmen keine Änderungen erforderlich sind, fahren Sie mit Sicherungs- und Archivierungsoperationen planen fort.
- Wenn Sie mit den Maßnahmen nicht vertraut sind, führen Sie die Schritte in dieser Prozedur aus.

Informationen zu diesem Vorgang

Maßnahmen haben Auswirkungen auf das Datenvolumen, das im Laufe der Zeit gespeichert wird, und den Zeitraum, den Daten aufbewahrt werden und für die Zurückschreibung durch Clients verfügbar sind. Um Datenschutzziele zu erreichen, können Sie die Standardmaßnahme aktualisieren und eigene Maßnahmen erstellen. Eine Maßnahme umfasst die folgenden Regeln:

- Angabe, wie und wann Dateien in Serverspeicher gesichert und archiviert werden
- Anzahl Kopien einer Datei und Zeitraum, den Kopien im Serverspeicher aufbewahrt werden

Während des Clientregistrierungsprozesses ordnen Sie einen Client einer *Maßnahmendomäne* zu. Die Maßnahme für einen bestimmten Client wird durch die Regeln in der Maßnahmendomäne festgelegt, der der Client zugeordnet ist. In der Maßnahmendomäne befinden sich die Regeln, die wirksam sind, in der aktiven *Maßnahmengruppe*.

Wenn ein Client eine Datei sichert oder archiviert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Eine *Verwaltungsklasse* ist die wichtigste Gruppe von Regeln zur Verwaltung von Clientdaten. Die Sicherungs- und Archivierungsoperationen auf dem Client verwenden die Einstellungen in der Standardverwaltungsklasse der Maßnahmendomäne, es sei denn, Sie passen die Maßnahme weiter an. Eine Maßnahme kann angepasst werden, indem weitere Verwaltungsklassen definiert werden und ihre Verwendung über Clientoptionen zugeordnet wird.

Clientoptionen können in einer lokalen, editierbaren Datei auf dem Clientsystem und in einer Clientoptionsgruppe auf dem Server angegeben werden. Die Optionen in der Clientoptionsgruppe auf dem Server können die Optionen in der lokalen Clientoptionsdatei überschreiben oder den Optionen in der lokalen Clientoptionsdatei hinzugefügt werden.

Vorgehensweise

1. Überprüfen Sie die Maßnahmen, die für Ihre Lösung konfiguriert sind, indem Sie die Anweisungen in Maßnahmen anzeigen ausführen.
2. Wenn geringfügige Änderungen erforderlich sind, um die Datenaufbewahrungsanforderungen zu erfüllen, führen Sie die Anweisungen in Maßnahmen editieren aus.
3. Optional: Wenn Maßnahmendomänen erstellt oder umfangreiche Änderungen an Maßnahmen durchgeführt werden müssen, um Datenaufbewahrungsanforderungen zu erfüllen, lesen Sie die Informationen in Maßnahmen anpassen.

Maßnahmen anzeigen

Zeigen Sie Maßnahmen an, um zu bestimmen, ob die Maßnahmen zur Erfüllung Ihrer Anforderungen editiert werden müssen.

Vorgehensweise

1. Um die aktive Maßnahmengruppe für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
   b. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.
2. Um inaktive Maßnahmengruppen für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf der Seite Maßnahmengruppen auf die Umschaltfläche Konfigurieren. Jetzt können Sie die inaktiven Maßnahmengruppen anzeigen und editieren.
   b. Blättern Sie mithilfe der vorwärts und rückwärts gerichteten Pfeile durch die inaktiven Maßnahmengruppen. Wenn Sie eine inaktive Maßnahmengruppe anzeigen, sind die unterschiedlichen Einstellungen für die inaktive und aktive Maßnahmengruppe hervorgehoben.
   c. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.

Maßnahmen editieren

Um die Regeln zu ändern, die für eine Maßnahmendomäne gelten, editieren Sie die aktive Maßnahmengruppe für die Maßnahmendomäne. Sie können auch eine andere Maßnahmengruppe für eine Domäne aktivieren.

Vorbereitende Schritte

Änderungen an Maßnahmen können sich auf die Datenaufbewahrung auswirken. Stellen Sie sicher, dass weiterhin Daten gesichert werden, die für Ihr Unternehmen von entscheidender Bedeutung sind, sodass Sie diese Daten in einem Katastrophenfall zurückschreiben können. Stellen Sie außerdem sicher, dass Ihr System über genügend Speicherbereich für geplante Sicherungsoperationen verfügt.

Informationen zu diesem Vorgang

Sie editieren eine Maßnahmengruppe, indem Sie eine oder mehrere Verwaltungsklassen in der Maßnahmengruppe ändern. Wenn Sie die aktive Maßnahmengruppe editieren, stehen die Änderungen den Clients erst zur Verfügung, nachdem Sie die Maßnahmengruppe reaktiviert haben. Um die editierte Maßnahmengruppe Clients zur Verfügung zu stellen, aktivieren Sie die Maßnahmengruppe.

Obwohl Sie mehrere Maßnahmengruppen für eine Maßnahmendomäne definieren können, kann nur eine einzige Maßnahmengruppe aktiv sein. Wenn Sie eine andere Maßnahmengruppe aktivieren, ersetzt diese die momentan aktive Maßnahmengruppe.

Informationen zu bevorzugten Verfahren zum Definieren von Maßnahmen finden Sie in Maßnahmen anpassen.

Vorgehensweise

1. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.

   Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.

3. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppe ist editierbar.
4. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
5. Editieren Sie die Maßnahmengruppe, indem Sie eine der folgenden Aktionen ausführen:

Option	Bezeichnung
Verwaltungsklasse hinzufügen	a. Klicken Sie in der Tabelle 'Maßnahmengruppen' auf + Verwaltungsklasse. b. Um die Regeln zum Sichern und Archivieren von Daten anzugeben, füllen Sie die Felder im Fenster Verwaltungsklasse hinzufügen aus. c. Um die Verwaltungsklasse als Standardverwaltungsklasse festzulegen, wählen Sie das Kontrollkästchen Als Standardwert definieren aus. d. Klicken Sie auf Hinzufügen.
Verwaltungsklasse löschen	Klicken Sie in der Spalte 'Verwaltungsklasse' auf -. Tipp: Um die Standardverwaltungsklasse zu löschen, müssen Sie zunächst eine andere Verwaltungsklasse als Standardverwaltungsklasse zuordnen.

Option	Bezeichnung
Legen Sie eine Verwaltungsklasse als Standardverwaltungsklasse fest.	Klicken Sie in der Spalte 'Standard' für die Verwaltungsklasse auf das Optionsfeld. Tipp: Die Standardverwaltungsklasse verwaltet Clientdateien, wenn einer Datei keine andere Verwaltungsklasse zugeordnet ist oder keine andere Verwaltungsklasse zur Verwaltung geeignet ist. Um sicherzustellen, dass Clients immer Dateien sichern und archivieren können, wählen Sie eine Standardverwaltungsklasse aus, die sowohl Regeln für das Sichern als auch für das Archivieren von Dateien enthält.
Verwaltungsklasse ändern	Um die Merkmale einer Verwaltungsklasse zu ändern, aktualisieren Sie die Felder in der Tabelle.

6. Klicken Sie auf Sichern.
   Achtung: Wenn Sie eine neue Maßnahmengruppe aktivieren, können Daten verloren gehen. Daten, die unter einer Maßnahmengruppe geschützt werden, werden möglicherweise unter einer anderen Maßnahmengruppe nicht geschützt. Daher müssen Sie vor dem Aktivieren einer Maßnahmengruppe sicherstellen, dass die Unterschiede zwischen der vorherigen Maßnahmengruppe und der neuen Maßnahmengruppe keinen Datenverlust zur Folge haben.
7. Klicken Sie auf Aktivieren. Es wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt. Stellen Sie sicher, dass die Änderungen in der neuen Maßnahmengruppe mit Ihren Datenaufbewahrungsanforderungen konsistent sind, indem Sie die folgenden Schritte ausführen:
   a. Überprüfen Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der aktiven Maßnahmengruppe gebunden sind, werden in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
   b. Ermitteln Sie Verwaltungsklassen in der aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
   c. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden sollen, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.

Sicherungs- und Archivierungsoperationen planen

Bevor Sie einen neuen Client beim Server registrieren, müssen Sie sicherstellen, dass ein Zeitplan verfügbar ist, um anzugeben, wann Sicherungs- und Archivierungsoperationen ausgeführt werden. Während des Registrierungsprozesses können Sie dem Client einen Zeitplan zuordnen.

Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Zeitplänen, die für die Lösung konfiguriert sind, vertraut sind und für die Zeitpläne keine Änderungen erforderlich sind, fahren Sie mit Clients registrieren fort.
- Wenn Sie mit den Zeitplänen nicht vertraut sind oder für die Zeitpläne Änderungen erforderlich sind, führen Sie die Schritte in dieser Prozedur aus.

Informationen zu diesem Vorgang

Normalerweise müssen Sicherungsoperationen für alle Clients täglich ausgeführt werden. Planen Sie Client- und Server-Workloads mit Bedacht, um die beste Leistung für Ihre Speicherumgebung zu erzielen. Um die Überschneidung von Client- und Serveroperationen zu verhindern, planen Sie die Ausführung von Clientsicherungs- und -archivierungsoperationen gegebenenfalls für die Nacht. Wenn sich Client- und Serveroperationen überschneiden oder ihnen nicht genügend Zeit und Ressourcen zur Verarbeitung zur Verfügung gestellt werden, können eine Verschlechterung der Systemleistung, fehlgeschlagene Operationen und andere Probleme die Folge sein.

Vorgehensweise

1. Überprüfen Sie die verfügbaren Zeitpläne, indem Sie den Mauszeiger in der Menüleiste des Operations Center über Clients bewegen. Klicken Sie auf Zeitpläne.
2. Optional: Ändern oder Erstellen Sie einen Zeitplan, indem Sie die folgenden Schritte ausführen:

Option	Bezeichnung
Zeitplan ändern	a. Wählen Sie in der Sicht Zeitpläne den Zeitplan aus und klicken Sie auf Details. b. Zeigen Sie auf der Seite Zeitplandetails Details an, indem Sie auf die blauen Pfeile am Anfang der Zeilen klicken. c. Ändern Sie die Einstellungen im Zeitplan und klicken Sie auf Sichern.
Zeitplan erstellen	Klicken Sie in der Sicht Zeitpläne auf +Zeitplan und führen Sie die Schritte zum Erstellen eines Zeitplans aus.

3. Optional: Verwenden Sie zum Konfigurieren von Zeitplaneinstellungen, die im Operations Center nicht sichtbar sind, einen Serverbefehl. Angenommen, Sie möchten eine Clientoperation planen, mit der ein bestimmtes Verzeichnis gesichert und einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zugeordnet wird.

a. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder.
b. Geben Sie zum Erstellen eines Zeitplans den Befehl DEFINE SCHEDULE und zum Ändern eines Zeitplans den Befehl UPDATE SCHEDULE aus. Ausführliche Informationen zu den Befehlen finden Sie in DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren) bzw. UPDATE SCHEDULE (Clientzeitplan aktualisieren).

Zugehörige Tasks:
Zeitplan für tägliche Operationen optimieren

Clients registrieren

Registrieren Sie einen Client, um sicherzustellen, dass der Client die Verbindung zum Server herstellen und der Server Clientdaten schützen kann.

Vorbereitende Schritte

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963. Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

Vorgehensweise

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

  ```
  register node Knotenname Kennwort userid=Knotenname
  ```

  Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.
- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  a. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  b. Klicken Sie in der Tabelle 'Clients' auf + Client.
  c. Führen Sie die Schritte im Assistenten Client hinzufügen aus:
     i. Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Datendeduplizierung' das Kontrollkästchen Aktivieren aus.
     ii. Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEDUPLICATION.
     Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
     iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
     iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
     v. Klicken Sie auf Client hinzufügen.

Zugehörige Verweise:
Option 'tcpserveraddress'
Option 'tcpport'
Option 'nodename'
Option 'deduplication'

Clients installieren und konfigurieren

Bevor Sie einen Clientknoten schützen können, müssen Sie die ausgewählte Software installieren und konfigurieren.

Vorgehensweise

Wenn Sie die Software bereits installiert haben, starten Sie mit Schritt 2.

1. Führen Sie eine der folgenden Aktionen aus:
   - Um Software auf einem Anwendungs- oder Clientknoten zu installieren, führen Sie die Anweisungen aus.

Software	Link zu Anweisungen

Software	Link zu Anweisungen
IBM Spectrum Protect-Client für Sichern/Archivieren	▪ UNIX- und Linux-Clients für Sichern/Archivieren installieren ▪ Windows-Client für Sichern/Archivieren installieren Informationen zur manuellen Implementierung von Clientaktualisierungen vom Server finden Sie in den folgenden Dokumenten: ▪ Für IBM Spectrum Protect-Server der Version 8.1.2 oder höher siehe Technote 2004596. ▪ Für IBM® Tivoli Storage Manager-Server der Version 7.1 und IBM Spectrum Protect-Server der Version 8.1.1 siehe Technote 1673299.
IBM Spectrum Protect for Databases	▪ Installation von Data Protection for Oracle ▪ Data Protection for SQL Server unter Windows Server Core installieren
IBM Spectrum Protect for Mail	▪ Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) ▪ Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0) ▪ Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	▪ Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen ▪ Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen ▪ Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
IBM Spectrum Protect for Enterprise Resource Planning	▪ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren ▪ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren

- Um Software auf einem VM-Clientknoten zu installieren, führen Sie die Anweisungen für den ausgewählten Sicherungstyp aus.

Sicherungstyp	Link zu Anweisungen
Wenn Sie planen, VMware-Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie den IBM Spectrum Protect-Client für Sichern/Archivieren.	▪ UNIX- und Linux-Clients für Sichern/Archivieren installieren ▪ Windows-Client für Sichern/Archivieren installieren
Wenn Sie planen, immer inkrementelle Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren auf demselben Clientknoten oder auf unterschiedlichen Clientknoten.	▪ IBM Spectrum Protect for Virtual Environments-Onlineproduktdokumentation Tipp: Die Software für IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren sind im IBM Spectrum Protect for Virtual Environments-Installationspaket enthalten.

2. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, fügen Sie die Werte für die Optionen TCPSERVERADDRESS, TCPPORT und NODENAME in der Clientoptionsdatei hinzu oder aktualisieren Sie diese. Verwenden Sie die Werte, die Sie beim Registrieren des Clients notiert haben (Clients registrieren).
   - Fügen Sie für Clients, die unter einem AIX-, Linux- oder Mac OS X-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.sys hinzu.
   - Fügen Sie für Clients, die unter einem Windows-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.opt hinzu.

   Standardmäßig befinden sich die Optionsdateien im Installationsverzeichnis.
3. Wenn ein Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem installiert wurde, installieren Sie den Clientverwaltungsservice auf dem Client. Führen Sie die Anweisungen in Clientverwaltungsservice installieren aus.
4. Konfigurieren Sie den Client für die Ausführung geplanter Operationen. Führen Sie die Anweisungen in Client für die Ausführung geplanter Operationen konfigurieren aus.
5. Optional: Konfigurieren Sie die Kommunikation durch eine Firewall. Führen Sie die Anweisungen in Client/Server-Kommunikation durch eine Firewall konfigurieren aus.
6. Führen Sie eine Testsicherung aus, um sicherzustellen, dass Daten wie geplant geschützt werden. Führen Sie beispielsweise für einen Client für Sichern/Archivieren die folgenden Schritte aus:
   a. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus, der gesichert werden soll, und klicken Sie auf Sichern.
   b. Überprüfen Sie, ob die Sicherung erfolgreich ausgeführt wird und keine Warnungen oder Fehlernachrichten vorhanden sind.
7. Überwachen Sie die Ergebnisse der geplanten Operationen für den Client im Operations Center.

Nächste Schritte

Wenn geändert werden muss, welche Daten vom Client gesichert werden, führen Sie die Anweisungen in Bereich einer Clientsicherung ändern aus.

Client für die Ausführung geplanter Operationen konfigurieren

Sie müssen einen Client-Scheduler auf dem Clientknoten konfigurieren und starten. Der Client-Scheduler ermöglicht die Kommunikation zwischen dem Client und dem Server, sodass geplante Operationen erfolgen können. Beispielsweise umfassen geplante Operationen normalerweise das Sichern von Dateien von einem Client.

Informationen zu diesem Vorgang

Die bevorzugte Methode ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert. Der Clientakzeptor verwaltet den Client-Scheduler derart, dass der Scheduler nur in erforderlichen Fällen ausgeführt wird:

- Wenn der Zeitpunkt erreicht ist, an dem der Server nach der nächsten geplanten Operation abgefragt werden soll
- Wenn der Zeitpunkt erreicht ist, an dem die nächste geplante Operation gestartet werden soll

Durch die Verwendung des Clientakzeptors ist es möglich, die Anzahl Hintergrundprozesse auf dem Client zu reduzieren und Probleme in Bezug auf die Speicheraufbewahrungsdauer zu vermeiden.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installiert hatten, für das der Clientakzeptor keine Zeitpläne ausführt, führen Sie die Konfigurationsanweisungen in der Produktdokumentation aus, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

Wenn Ihr Unternehmen standardmäßig ein Zeitplanungstool eines anderen Anbieters verwendet, können Sie statt des Clientakzeptors dieses Zeitplanungstool verwenden. Normalerweise starten Zeitplanungstools anderer Anbieter Clientprogramme direkt mithilfe von Betriebssystembefehlen. Informationen zum Konfigurieren eines Zeitplanungstools eines anderen Anbieters enthält die Produktdokumentation.

Vorgehensweise

Um den Client-Scheduler mithilfe des Clientakzeptors zu konfigurieren und zu starten, führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
b. Klicken Sie auf die Registerkarte Web-Client.
c. Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
d. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei dsm.sys die Option passwordaccess auf `generate`.
e. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkennwort ein:

```
dsmc query sess
```

f. Starten Sie den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
/usr/bin/dsmcad
```

g. Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie der Systemstartdatei (normalerweise /etc/inittab) den folgenden Eintrag hinzu:

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Clientakzeptordämon
```

Linux

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
b. Klicken Sie auf die Registerkarte Web-Client.
c. Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
d. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei dsm.sys die Option passwordaccess auf `generate`.
e. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkennwort ein:

```
dsmc query sess
```

f. Starten Sie den Clientakzeptor, indem Sie sich mit der Rootbenutzer-ID anmelden und den folgenden Befehl ausgeben:

```
service dsmcad start
```

g. Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie den Service hinzu, indem Sie in einer Shelleingabeaufforderung den folgenden Befehl ausgeben:

```
# chkconfig --add dsmcad
```

MAC OS X

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
b. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, klicken Sie auf Berechtigung, wählen Sie Kennwort generieren aus und klicken Sie auf Anwenden.
c. Um anzugeben, wie Services verwaltet werden, klicken Sie auf Web-Client, wählen Sie Zeitplan aus, klicken Sie auf Anwenden und dann auf OK.
d. Um sicherzustellen, dass das generierte Kennwort gespeichert wird, starten Sie den Client für Sichern/Archivieren erneut.
e. Starten Sie den Clientakzeptor mithilfe der Anwendung 'IBM Spectrum Protect Tools for Administrators'.

Windows

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Dienstprogramme > Setup-Assistent > Hilfe zum Konfigurieren des Client-Schedulers. Klicken Sie auf Weiter.
b. Lesen Sie die Informationen auf der Seite Schedulerassistent und klicken Sie auf Weiter.
c. Wählen Sie auf der Seite Scheduler-Task die Option Neuen oder zusätzlichen Scheduler installieren aus und klicken Sie auf Weiter.
d. Geben Sie auf der Seite Schedulername und -position einen Namen für den Client-Scheduler an, der hinzugefügt wird. Wählen Sie dann Scheduler mit Clientakzeptordämon (CAD) verwalten aus, um den Scheduler zu verwalten, und klicken Sie auf Weiter.
e. Geben Sie den Namen ein, der diesem Clientakzeptor zugeordnet werden soll. Der Standardname ist 'Clientakzeptor'. Klicken Sie auf Weiter.
f. Schließen Sie die Konfiguration ab, indem Sie den Assistenten durchlaufen.
g. Aktualisieren Sie die Clientoptionsdatei, dsm.opt, und setzen Sie die Option passwordaccess auf generate.
h. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl in der Eingabeaufforderung aus:

```
dsmc query sess
```

Geben Sie auf Anforderung das Clientknotenkennwort ein.
i. Starten Sie den Clientakzeptorservice über die Seite Systemsteuerung. Wenn Sie beispielsweise den Standardnamen verwendet haben, starten Sie den Service 'Clientakzeptor'. Starten Sie nicht den Scheduler-Service, den Sie auf der Seite Schedulername und -position angegeben haben. Der Scheduler-Service wird wie erforderlich automatisch vom Clientakzeptorservice gestartet und gestoppt.

Client/Server-Kommunikation durch eine Firewall konfigurieren

Wenn ein Client durch eine Firewall mit einem Server kommunizieren muss, müssen Sie die Client/Server-Kommunikation durch die Firewall ermöglichen.

Vorbereitende Schritte

Wenn Sie den Assistenten 'Client hinzufügen' zum Registrieren eines Clients verwendet hatten, bestimmen Sie die Optionswerte in der Clientoptionsdatei, die während dieses Prozesses abgerufen wurden. Sie können die Werte zur Angabe von Ports verwenden.

Informationen zu diesem Vorgang

Achtung: Konfigurieren Sie eine Firewall nicht derart, dass dies eine Beendigung der Sitzungen zur Folge hätte, die von einem Server oder Speicheragenten verwendet werden. Die Beendigung einer gültigen Sitzung kann zu unvorhersehbaren Ergebnissen führen. Prozesse und Sitzungen scheinen unter Umständen aufgrund von Ein-/Ausgabefehlern gestoppt zu werden. Um das Ausschließen von Sitzungen von Zeitlimitbeschränkungen zu erleichtern, konfigurieren Sie bekannte Ports für IBM Spectrum Protect-Komponenten. Stellen Sie sicher, dass die Serveroption KEEPALIVE auf den Standardwert YES gesetzt bleibt. Auf diese Art und Weise kann sichergestellt werden, dass die Client/Server-Kommunikation unterbrechungsfrei erfolgt. Anweisungen zum Definieren der Serveroption KEEPALIVE finden Sie in KEEPALIVE.

Vorgehensweise

Öffnen Sie die folgenden Ports, um Zugriff durch die Firewall zu ermöglichen:

TCP/IP-Port für den Client für Sichern/Archivieren, den Verwaltungsbefehlszeilenclient und den Client-Scheduler
: Geben Sie den Port über die Option tcpport in der Clientoptionsdatei an. Die Option tcpport in der Clientoptionsdatei muss mit der Option TCPPORT in der Serveroptionsdatei übereinstimmen. Der Standardwert ist 1500. Wenn ein anderer Wert als der Standardwert verwendet werden soll, geben Sie eine Zahl zwischen 1024 und 32767 an.

HTTP-Port, um die Kommunikation zwischen dem Web-Client und fernen Workstations zu ermöglichen
: Geben Sie den Port für die ferne Workstation an, indem Sie die Option httpport in der Clientoptionsdatei der fernen Workstation festlegen. Der Standardwert ist 1581.

TCP/IP-Ports für die ferne Workstation
: Der Standardwert von 0 (null) hat zur Folge, dass zwei freie Portnummern der fernen Workstation nach dem Zufallsprinzip zugeordnet werden. Wenn die Portnummern nicht nach dem Zufallsprinzip zugeordnet werden sollen, geben Sie über die Option webports in der Clientoptionsdatei der fernen Workstation Werte an.

TCP/IP-Port für Verwaltungssitzungen
: Geben Sie den Port an, an dem der Server auf Anforderungen von Verwaltungsclientsitzungen wartet. Der Wert der Clientoption tcpadminport muss mit dem Wert der Serveroption TCPADMINPORT übereinstimmen. Auf diese Art und Weise können Sie sichere Verwaltungssitzungen in einem privaten Netz gewährleisten.

Clientoperationen verwalten

Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.

Informationen zu diesem Vorgang

In einigen Fällen können Clientfehler behoben werden, indem der Clientakzeptor gestoppt und gestartet wird. Wenn Clientknoten oder Administrator-IDs gesperrt sind, können Sie das Problem beheben, indem Sie den Clientknoten bzw. die Administrator-ID entsperren und dann das Kennwort zurücksetzen.

Ausführliche Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in Clientprobleme lösen.

- Fehler in Clientfehlerprotokollen auswerten
  Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.
- Clientakzeptor stoppen und erneut starten
  Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.
- Kennwörter zurücksetzen
  Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.
- Bereich einer Clientsicherung ändern
  Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

Fehler in Clientfehlerprotokollen auswerten

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

Vorbereitende Schritte

Um Fehler in einem Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem zu beheben, stellen Sie sicher, dass der Clientverwaltungsservice installiert und gestartet wurde. Installationsanweisungen finden Sie in Clientverwaltungsservice installieren. Anweisungen zur Überprüfung der Installation finden Sie in Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen.

Vorgehensweise

Um Clientfehler zu diagnostizieren und zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn der Clientverwaltungsservice auf dem Clientknoten installiert ist, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Details.
  3. Klicken Sie auf der Seite 'Zusammenfassung' auf die Registerkarte Diagnose.
  4. Überprüfen Sie die abgerufenen Protokollnachrichten.
     Tipps:
     - Um das Fenster 'Clientprotokolle' ein- oder auszublenden, doppelklicken Sie auf den Rahmen des Fensters 'Clientprotokolle'.
     - Um die Größe des Fensters 'Clientprotokolle' zu ändern, klicken Sie auf den Rahmen des Fensters 'Clientprotokolle' und ziehen Sie den Rahmen.

     Wenn auf der Seite 'Diagnose' Vorschläge angezeigt werden, wählen Sie einen Vorschlag aus. Im Fenster 'Clientprotokolle' sind die Clientprotokollnachrichten, auf die sich der Vorschlag bezieht, hervorgehoben.
  5. Lösen Sie die in den Fehlernachrichten angegebenen Probleme mithilfe der Vorschläge.
     Tipp: Vorschläge werden nur für einen Teil der Clientnachrichten bereitgestellt.

- Wenn der Clientverwaltungsservice nicht auf dem Clientknoten installiert ist, überprüfen Sie die Fehlerprotokolle für den installierten Client.

Clientakzeptor stoppen und erneut starten

Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.

Informationen zu diesem Vorgang

In einigen Fällen können Clientzeitplanungsprobleme behoben werden, indem der Clientakzeptor gestoppt und erneut gestartet wird. Der Clientakzeptor muss aktiv sein, um sicherzustellen, dass geplante Operationen auf dem Client ausgeführt werden können. Wenn Sie beispielsweise die IP-Adresse oder den Domänennamen des Servers ändern, müssen Sie den Clientakzeptor erneut starten.

Vorgehensweise

Führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

- Um den Clientakzeptor zu stoppen, führen Sie die folgenden Schritte aus:
  a. Bestimmen Sie die Prozess-ID für den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

     ```
     ps -ef | grep dsmcad
     ```

     Überprüfen Sie die Ausgabe. In der folgenden Beispielausgabe lautet die Prozess-ID für den Clientakzeptor 6764:

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```

  b. Geben Sie in der Befehlszeile den folgenden Befehl aus:

     ```
     kill -9 PID
     ```

     Dabei gibt *PID* die Prozess-ID für den Clientakzeptor an.
- Um den Clientakzeptor zu starten, geben Sie in der Befehlszeile den folgenden Befehl aus:

  ```
  /usr/bin/dsmcad
  ```

Linux

- Um den Clientakzeptor zu stoppen, ohne ihn erneut zu starten, geben Sie den folgenden Befehl aus:

  ```
  # service dsmcad stop
  ```

- Um den Clientakzeptor zu stoppen und erneut zu starten, geben Sie den folgenden Befehl aus:

  ```
  # service dsmcad restart
  ```

MAC OS X

Klicken Sie auf Applications > Utilities > Terminal.

- Um den Clientakzeptor zu stoppen, geben Sie den folgenden Befehl aus:

  ```
  /bin/launchctl unload -w com.ibm.tivoli.dsmcad
  ```

- Um den Clientakzeptor zu starten, geben Sie den folgenden Befehl aus:

  ```
  /bin/launchctl load -w com.ibm.tivoli.dsmcad
  ```

Windows

- Um den Clientakzeptorservice zu stoppen, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf Start > Verwaltung > Dienste.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf Beenden und OK.
- Um den Clientakzeptorservice erneut zu starten, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf Start > Verwaltung > Dienste.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf Starten und OK.

Zugehörige Verweise:
Fehler für Clientzeitplanung beheben

Kennwörter zurücksetzen

Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.

Vorgehensweise

Um Kennwortprobleme zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn ein Client für Sichern/Archivieren auf einem Clientknoten installiert ist und das Kennwort verloren gegangen ist oder Sie das Kennwort vergessen haben, führen Sie die folgenden Schritte aus:
  1. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Knotenname* den Clientknoten und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
  2. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.
     Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf `generate` gesetzt haben.
- Wenn ein Administrator aufgrund von Kennwortproblemen ausgesperrt ist, führen Sie die folgenden Schritte aus:
  1. Um dem Administrator den Zugriff auf den Server zu ermöglichen, geben Sie den Befehl UNLOCK ADMIN aus. Anweisungen finden Sie in UNLOCK ADMIN (Administrator entsperren).
  2. Legen Sie mit dem Befehl UPDATE ADMIN ein neues Kennwort fest:

     ```
     update admin Administratorname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Administratorname* den Namen des Administrators und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
- Wenn ein Clientknoten gesperrt ist, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, warum der Clientknoten gesperrt ist und ob er entsperrt werden muss. Wenn beispielsweise der Clientknoten stillgelegt ist, wird der Clientknoten aus der Produktionsumgebung entfernt. Sie können die Stilllegungsoperation nicht zurücknehmen und der Clientknoten bleibt gesperrt. Ein Clientknoten kann auch gesperrt sein, wenn die Clientdaten Gegenstand einer rechtlichen Untersuchung sind.
  2. Verwenden Sie zum Entsperren eines Clientknotens den Befehl UNLOCK NODE. Anweisungen finden Sie in UNLOCK NODE (Clientknoten entsperren).
  3. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Knotenname* den Namen des Knotens und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
  4. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.
     Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf `generate` gesetzt haben.

Bereich einer Clientsicherung ändern

Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

Informationen zu diesem Vorgang

Indem Sie nicht benötigte Objekte von Sicherungsoperationen ausschließen, können Sie die Größe des Speicherbereichs, der für Sicherungsoperationen erforderlich ist, und die Speicherkosten besser steuern. Abhängig von Ihrem Lizenzpaket ist es unter Umständen auch möglich, die Lizenzierungskosten zu begrenzen.

Vorgehensweise

Die Vorgehensweise beim Ändern des Bereichs von Sicherungsoperationen ist von dem Produkt abhängig, das auf dem Clientknoten installiert ist:

- Bei einem Client für Sichern/Archivieren können Sie eine Einschluss-/Ausschlussliste erstellen, um eine Datei, Dateigruppen oder Verzeichnisse in Sicherungsoperationen einzuschließen oder von Sicherungsoperationen auszuschließen. Um eine Einschluss-/Ausschlussliste zu erstellen, führen Sie die Anweisungen in Einschluss-/Ausschlussliste erstellen aus.

Um die konsistente Verwendung einer Einschluss-/Ausschlussliste für alle Clients eines bestimmten Typs zu gewährleisten, können Sie auf dem Server eine Clientoptionsgruppe erstellen, die die erforderlichen Optionen enthält. Anschließend ordnen Sie die Clientoptionsgruppe jedem Client desselben Typs zu. Ausführliche Informationen finden Sie in Clientoperationen über Clientoptionsgruppen steuern.

- Für einen Client für Sichern/Archivieren können Sie die Objekte, die in eine Teilsicherungsoperation eingeschlossen werden sollen, mithilfe der Option domain angeben. Führen Sie die Anweisungen in Clientoption 'domain' aus.
- Führen Sie für andere Produkte die Anweisungen in der Produktdokumentation aus, um zu definieren, welche Objekte in Sicherungsoperationen eingeschlossen und von Sicherungsoperationen ausgeschlossen werden sollen.

Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

Vorbereitende Schritte

1. Überprüfen Sie die Voraussetzungen für die Client/Server-Kompatibilität in Technote 1053218. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden.
2. Überprüfen Sie die Systemvoraussetzungen für den Client in IBM Spectrum Protect Supported Operating Systems.
3. Wenn die Lösung Speicheragenten oder Speicherarchivclients umfasst, überprüfen Sie die Informationen zur Kompatibilität von Speicheragenten bzw. Speicherarchivclients mit Servern, die als Speicherarchivmanager konfiguriert sind. Siehe Technote 1302789.

   Wenn Sie planen, ein Upgrade für einen Speicherarchivmanager und einen Speicherarchivclient durchzuführen, müssen Sie zuerst das Upgrade für den Speicherarchivmanager durchführen.

Vorgehensweise

Um ein Software-Upgrade durchzuführen, führen Sie die in der folgenden Tabelle aufgelisteten Anweisungen aus.

Software	Link zu Anweisungen
IBM Spectrum Protect-Client für Sichern/Archivieren	• Upgrade des Clients für Sichern/Archivieren durchführen
IBM Spectrum Protect Snapshot	• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
IBM Spectrum Protect for Databases	• Upgrade für Data Protection for SQL Server durchführen • Installation von Data Protection for Oracle • Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 durchführen • Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle durchführen
IBM Spectrum Protect for Mail	• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) • Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0) • Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Installation und Upgrade für Data Protection for VMware durchführen • Data Protection for Microsoft Hyper-V installieren

Clientknoten stilllegen

Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet

wird, können Sie die Workstation stilllegen.

Informationen zu diesem Vorgang

Wenn Sie den Stilllegungsprozess starten, sperrt der Server den Clientknoten, um zu verhindern, dass dieser auf den Server zugreift. Dateien, die zu dem Clientknoten gehören, werden nacheinander gelöscht; anschließend wird der Clientknoten gelöscht. Sie können die folgenden Typen von Clientknoten stilllegen:

Anwendungsclientknoten
: Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Systemclientknoten
: Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

VM-Clientknoten
: Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Die einfachste Methode zur Stilllegung eines Clientknotens ist die Verwendung des Operations Center. Der Stilllegungsprozess wird im Hintergrund ausgeführt. Wenn der Client für die Replikation von Clientdaten konfiguriert ist, entfernt das Operations Center den Client automatisch aus der Replikation auf dem Quellen- und dem Zielreplikationsserver, bevor es den Client stilllegt.
Tipp: Sie können einen Clientknoten auch stilllegen, indem Sie den Befehl DECOMMISSION NODE oder DECOMMISSION VM ausgeben. Diese Methode kann beispielsweise in den folgenden Fällen verwendet werden:

- Um den Stilllegungsprozess für einen späteren Zeitpunkt zu planen oder eine Serie von Befehlen unter Verwendung eines Scripts auszuführen, geben Sie die Ausführung des Stilllegungsprozesses im Hintergrund an.
- Um den Stilllegungsprozess zu Zwecken der Fehlerbehebung zu überwachen, geben Sie die Ausführung des Stilllegungsprozesses im Vordergrund an. Wenn Sie den Prozess im Vordergrund ausführen, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor Sie die Arbeit mit anderen Tasks fortsetzen können.

Vorgehensweise

Führen Sie eine der folgenden Aktionen aus:

- Um einen Client mithilfe des Operations Center im Hintergrund stillzulegen, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Weitere > Stilllegen.
- Um einen Clientknoten mithilfe eines Verwaltungsbefehls stillzulegen, führen Sie eine der folgenden Aktionen aus:
  - Um einen Anwendungs- oder Systemclientknoten im Hintergrund stillzulegen, geben Sie den Befehl DECOMMISSION NODE aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

    ```
    decommission node austin
    ```

  - Um einen Anwendungs- oder Systemclientknoten im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION NODE unter Angabe des Parameters `wait=yes` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

    ```
    decommission node austin wait=yes
    ```

  - Um eine virtuelle Maschine im Hintergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM aus. Wenn beispielsweise die virtuelle Maschine den Namen AUSTIN hat, der Dateibereich 7 ist und der Dateibereichsname über die Dateibereichs-ID angegeben wird, geben Sie den folgenden Befehl aus:

    ```
    decommission vm austin 7 nametype=fsid
    ```

    Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

    ```
    decommission vm "austin 2" 7 nametype=fsid
    ```

  - Um eine virtuelle Maschine im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM unter Angabe des Parameters `wait=yes` aus. Geben Sie beispielsweise den folgenden Befehl aus:

    ```
    decommission vm austin 7 nametype=fsid wait=yes
    ```

    Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

Nächste Schritte

Achten Sie auf Fehlernachrichten, die unter Umständen in der Benutzerschnittstelle oder in der Befehlsausgabe unmittelbar nach der Ausführung des Prozesses angezeigt werden.

Um zu überprüfen, ob der Clientknoten stillgelegt wurde, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
2. Überprüfen Sie in der Tabelle 'Clients' in der Spalte 'Gefährdet' den Status:
   - Der Status 'Stillgelegt' (DECOMMISSIONED) gibt an, dass der Knoten stillgelegt wurde.
   - Ein Nullwert gibt an, dass der Knoten nicht stillgelegt wurde.
   - Der Status 'Anstehend' (PENDING) gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

   Tipp: Wenn der Status eines anstehenden Stilllegungsprozesses bestimmt werden soll, geben Sie den folgenden Befehl aus:

   ```
   query process
   ```

3. Überprüfen Sie die Befehlsausgabe:
   - Wenn für den Stilllegungsprozess ein Status angegeben ist, ist der Prozess in Bearbeitung. Beispiel:

     ```
     query process
      Prozess-     Prozessbeschreibung           Prozessstatus
      nummer
     ---------     --------------------     -------------------------------------------
             3     DECOMMISSION NODE        Anzahl der für Knoten NODE1 inaktivierten
                                            Sicherungsobjekte: 8 Objekte inaktiviert.
     ```

   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie keine Fehlernachricht empfangen haben, ist der Prozess unvollständig. Ein Prozess kann unvollständig sein, wenn Dateien, die dem Knoten zugeordnet sind, noch nicht inaktiviert wurden. Führen Sie nach der Inaktivierung der Dateien den Stilllegungsprozess erneut aus.
   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie eine Fehlernachricht empfangen, ist der Prozess fehlgeschlagen. Führen Sie den Stilllegungsprozess erneut aus.

Zugehörige Verweise:
DECOMMISSION NODE (Clientknoten stilllegen)
DECOMMISSION VM (Virtuelle Maschine stilllegen)

Daten zum Freigeben von Speicherbereich inaktivieren

In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegeben Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

Informationen zu diesem Vorgang

Einige Anwendungsclients sichern Daten immer als aktive Sicherungsdaten auf dem Server. Da aktive Sicherungsdaten nicht durch die Bestandsverfallsmaßnahmen verwaltet werden, werden die Daten nicht automatisch gelöscht und belegen unbegrenzt Serverspeicher. Um den Speicherbereich freizugeben, der von veralteten Daten belegt wird, können Sie die Daten inaktivieren.

Wenn Sie den Inaktivierungsprozess ausführen, werden alle aktiven Sicherungsdaten, die vor dem angegeben Datum gespeichert wurden, inaktiv. Die Daten werden gelöscht, sobald sie verfallen, und können nicht zurückgeschrieben werden. Die Inaktivierungsfunktion gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

Vorgehensweise

1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients.
2. Wählen Sie in der Tabelle 'Clients' einen oder mehrere Clients aus und klicken Sie auf Weitere > Bereinigen.
   Befehlszeilenmethode: Inaktivieren Sie Daten mit dem Befehl DEACTIVATE DATA.

Zugehörige Verweise:
DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)

Datenspeicher verwalten

Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.

- Speicherpoolcontainer prüfen
  Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.

- Bestandskapazität verwalten
  Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.
- Speichernutzung und Prozessorauslastung verwalten
  Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datendeduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.
- Geplante Aktivitäten optimieren
  Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

Zugehörige Verweise:
Speicherpooltypen

Speicherpoolcontainer prüfen

Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.

Informationen zu diesem Vorgang

Sie prüfen einen Speicherpoolcontainer in den folgenden Situationen:

- Sie geben den Befehl QUERY DAMAGED aus und es wird ein Problem erkannt.
- Der Server zeigt Nachrichten zu beschädigten Datenbereichen an.
- Ihre Hardware meldet ein Problem und es werden Fehlernachrichten angezeigt, die sich auf den Speicherpoolcontainer beziehen.

Vorgehensweise

1. Um einen Speicherpoolcontainer zu prüfen, geben Sie den Befehl AUDIT CONTAINER aus. Geben Sie beispielsweise den folgenden Befehl aus, um den Container 000000000000076c.dcf zu prüfen:

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Überprüfen Sie die Ausgabe der Nachricht ANR4891I auf Informationen zu allen beschädigten Datenbereichen.

Nächste Schritte

Wenn Sie Probleme mit dem Speicherpoolcontainer erkennen, können Sie Daten auf der Basis Ihrer Konfiguration zurückschreiben. Geben Sie den Befehl AUDIT CONTAINER aus und geben Sie den Containernamen an.

Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool abfragen)

Bestandskapazität verwalten

Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.

Vorbereitende Schritte

Die aktive Protokolldatei und das Archivprotokoll haben die folgenden Merkmale:

- Die Größe der aktiven Protokolldatei kann maximal 512 GB betragen. Weitere Informationen zum Festlegen der Größe der aktiven Protokolldatei für Ihr System finden Sie in Planung der Speicherarrays.
- Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist. Die Größe des Archivprotokolls ist im Gegensatz zur Größe der aktiven Protokolldatei nicht auf eine vordefinierte Größe festgelegt. Archivprotokolldateien werden automatisch gelöscht, wenn sie nicht mehr benötigt werden.

Als Best Practice können Sie wahlweise ein Archivübernahmeprotokoll erstellen, in dem Archivprotokolldateien gespeichert werden, wenn das Archivprotokollverzeichnis voll ist.

Bestimmen Sie über das Operations Center, welche Komponente des Bestands voll ist. Stellen Sie sicher, dass der Server gestoppt wird, bevor Sie eine der Bestandskomponenten vergrößern.

Vorgehensweise

- Um die Datenbank zu vergrößern, führen Sie die folgenden Schritte aus:
  - Erstellen Sie in unterschiedlichen Laufwerken oder Dateisystemen ein oder mehrere Verzeichnisse für die Datenbank.
  - Geben Sie den Befehl EXTEND DBSPACE aus, um der Datenbank das Verzeichnis oder die Verzeichnisse hinzuzufügen. Die Instanzbenutzer-ID des Datenbankmanagers muss Zugriff auf die Verzeichnisse haben. Standardmäßig erfolgt eine Neuverteilung der Daten auf alle Datenbankverzeichnisse und eine Konsolidierung des Speicherbereichs.
    Tipps:
    - Die Zeit, die für die vollständige Neuverteilung von Daten und die Konsolidierung von Speicherbereich erforderlich ist, variiert abhängig von der Größe Ihrer Datenbank. Stellen Sie sicher, dass Sie dies bei der Planung berücksichtigen.
    - Stellen Sie sicher, dass die Verzeichnisse, die Sie angeben, dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.
  - Stoppen Sie den Server und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig nutzen zu können.
  - Reorganisieren Sie die Datenbank, falls erforderlich. Die Index- und Tabellenreorganisation für die Serverdatenbank kann dazu beitragen, unerwartetes Datenbankwachstum und Leistungsprobleme zu verhindern. Weitere Informationen zur Reorganisation der Datenbank finden Sie in Technote 1683633.
- Um die Datenbank für Server der Version 7.1 und höher zu verkleinern, geben Sie im Serverinstanzverzeichnis die folgenden DB2-Befehle aus:
  Einschränkung: Die Befehle können die E/A-Aktivität erhöhen und sich unter Umständen auf die Serverleistung auswirken. Um Leistungsprobleme auf ein Mindestmaß zu reduzieren, warten Sie, bis ein Befehl abgeschlossen ist, bevor Sie den nächsten Befehl ausgeben. Die DB2-Befehle können ausgegeben werden, wenn der Server aktiv ist.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
```

- Um die aktive Protokolldatei zu vergrößern oder zu verkleinern, führen Sie die folgenden Schritte aus:
  1. Stellen Sie sicher, dass die Position für die aktive Protokolldatei über genügend Speicherbereich für die erhöhte Protokollgröße verfügt. Wenn ein Protokollspiegel vorhanden ist, muss auch die Position für den Spiegel über genügend Speicherbereich für die erhöhte Protokollgröße verfügen.
  2. Stoppen Sie den Server.
  3. Aktualisieren Sie in der Datei dsmserv.opt die Option ACTIVELOGSIZE mit der neuen Größe der aktiven Protokolldatei (angegeben in Megabyte).
     Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Die folgende Tabelle enthält Richtlinien für den Speicherbedarf:

     Tabelle 1. Schätzen des Speicherbedarfs für Datenträger und Dateibereiche

Wert für die Option ACTIVELOGSize	**Größe des im Verzeichnis für aktive Protokolldateien zu reservierender freier Speicherbereich zusätzlich zum Speicherbereich für ACTIVELOGSize**
16 GB bis 128 GB	5120 MB
129 GB bis 256 GB	10240 MB
257 GB bis 512 GB	20480 MB

     Um die Größe der aktiven Protokolldatei in die maximale Größe von 512 GB zu ändern, geben Sie die folgende Serveroption ein:

     ```
     activelogsize 524288
     ```

  4. Wenn Sie planen, ein neues Verzeichnis für aktive Protokolldateien zu verwenden, aktualisieren Sie den in der Serveroption ACTIVELOGDIRECTORY angegebenen Verzeichnisnamen. Das neue Verzeichnis muss leer sein und die Benutzer-ID des Datenbankmanagers muss Zugriff auf dieses Verzeichnis haben.
  5. Starten Sie den Server erneut.

- Komprimieren Sie die Archivprotokolle, um die Größe des Speicherbereichs, der zum Speichern benötigt wird, zu reduzieren. Aktivieren Sie die dynamische Komprimierung für das Archivprotokoll, indem Sie den folgenden Befehl ausgeben:

  ```
  setopt archlogcompress yes
  ```

  Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hohen Workloads aktivieren. Ein Aktivieren dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Dateisystem für Archivprotokolle haben. Diese Verzögerung kann zur Folge haben, dass der Speicherbereich im Dateisystem für aktive Protokolldateien knapp wird. Sie müssen den verfügbaren Speicherbereich im Dateisystem für aktive Protokolldateien überwachen, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn für das Dateisystem für das Verzeichnis für aktive Protokolldateien fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT können Sie die Komprimierung für das Archivprotokoll sofort inaktivieren, ohne den Server stoppen zu müssen.

Zugehörige Verweise:
Serveroption ACTIVELOGSIZE
EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)
SETOPT (Serveroption für dynamische Aktualisierung definieren)

Speichernutzung und Prozessorauslastung verwalten

Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datendeduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.

Vorbereitende Schritte

- Stellen Sie sicher, dass Ihre Konfiguration die erforderliche Hardware und Software verwendet. Weitere Informationen finden Sie in IBM Spectrum Protect Supported Operating Systems.
- Weitere Informationen zur Verwaltung von Ressourcen, wie beispielsweise Datenbank und Wiederherstellungsprotokoll, finden Sie in Planung der Speicherarrays.
- Fügen Sie zusätzlichen Systemspeicher hinzu, um festzustellen, ob sich die Leistung verbessert. Überwachen Sie die Speichernutzung regelmäßig, um zu bestimmen, ob weiterer Speicher erforderlich ist.

Vorgehensweise

1. Geben Sie, falls möglich, Speicherbereich aus dem Dateisystemcache frei.
2. Verwenden Sie zur Verwaltung des Systemspeichers, den jeder Server auf einem System verwendet, die Serveroption DBMEMPERCENT. Begrenzen Sie den Prozentsatz des Systemspeichers, der vom Datenbankmanager jedes Servers verwendet werden kann. Wenn alle Server gleich wichtig sind, verwenden Sie denselben Wert für jeden Server. Wenn ein Server der Produktionsserver ist und die anderen Server Testserver sind, definieren Sie für den Produktionsserver einen höheren Wert als für die Testserver.
3. Definieren Sie den Benutzerdatengrenzwert und den privaten Speicher für die Datenbank, um sicherzustellen, dass immer genügend privater Speicher verfügbar ist. Wenn der private Speicher knapp wird, kann dies Fehler, eine nicht optimale Leistung und Instabilität zur Folge haben.

Geplante Aktivitäten optimieren

Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

Vorgehensweise

1. Überwachen Sie die Systemleistung regelmäßig, um sicherzustellen, dass Sicherungs- und Verwaltungstasks erfolgreich ausgeführt werden. Weitere Informationen zur Überwachung finden Sie in Plattenspeicherlösung für einen einzelnen Standort überwachen.
2. Wenn die Überwachungsdaten anzeigen, dass sich die Server-Workload erhöht hat, müssen Sie die Planungsinformationen gegebenenfalls überprüfen. Überprüfen Sie, ob die Kapazität des Systems in den folgenden Fällen ausreichend ist:
   - Erhöhung der Anzahl Clients
   - Zunahme des Datenvolumens, das gesichert wird
   - Änderung des Zeitraums, der für Sicherungen verfügbar ist
3. Bestimmen Sie, ob für Ihre Lösung Leistungsprobleme vorliegen. Überprüfen Sie die Clientzeitpläne dahingehend, ob Tasks innerhalb des geplanten Zeitrahmens ausgeführt werden:
   a. Wählen Sie auf der Seite Clients im Operations Center den Client aus.
   b. Klicken Sie auf Details.
   c. Überprüfen Sie auf der Seite Zusammenfassung des Clients die für Gesichert und Repliziert angegebene Aktivität, um alle Risiken zu ermitteln.

   Passen Sie, falls erforderlich, den Zeitpunkt und die Häufigkeit für die Ausführung von Clientsicherungsoperationen an.
4. Planen Sie ausreichend Zeit ein, um die folgenden Verwaltungstasks innerhalb von 24 Stunden erfolgreich ausführen zu können:
   a. Sichern der Datenbank

b. Ausführen der Verfallsverarbeitung, um Clientsicherungen und Archivierungsdateikopien aus dem Serverspeicher zu entfernen

Zugehörige Konzepte:
Leistung
Zugehörige Tasks:
Daten deduplizieren (Version 7.1.1)

IBM Spectrum Protect-Server schützen

Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

- Sicherheitskonzepte
  Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.
- Administratoren verwalten
  Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.
- Kennwortanforderungen ändern
  Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.
- Server auf dem System schützen
  Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

Sicherheitskonzepte

Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

Transport Layer Security

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtsicherheit für eine sichere Verbindung zwischen Servern, Clients und Speicheragenten bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, verwenden Sie SSL oder TLS zum Verschlüsseln der Daten.

Tipp: In der gesamten IBM Spectrum Protect-Dokumentation gilt jede Angabe von "SSL" oder zum "Auswählen von SSL" für TLS.

SSL wird von Global Security Kit (GSKit) bereitgestellt, das zusammen mit dem IBM Spectrum Protect-Server installiert wird, der vom Server, vom Client und vom Speicheragenten verwendet wird.

Einschränkung: Sie dürfen die SSL- oder TLS-Protokolle nicht für die Kommunikation mit einer DB2-Datenbankinstanz verwenden, die von IBM Spectrum Protect-Servern verwendet wird.

Jeder Server, Client oder Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdiges selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle (CA) signiert ist. Sie können Ihre eigenen Zertifikate verwenden oder Zertifikate bei einer Zertifizierungsstelle (CA) kaufen. Jedes der Zertifikate muss installiert und der Schlüsseldatenbank auf dem IBM Spectrum Protect-Server, -Client oder -Speicheragenten hinzugefügt werden. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet. Einige CA-Zertifikate sind in der Schlüsseldatenbank standardmäßig vorinstalliert.

SSL wird auf dem IBM Spectrum Protect-Server, -Client und -Speicheragenten unabhängig voneinander konfiguriert.

Berechtigungsstufen

Für jeden IBM Spectrum Protect-Server sind verschiedene Administratorberechtigungsstufen verfügbar, die die Tasks festlegen, die ein Administrator ausführen kann.

Nach der Registrierung muss einem Administrator Berechtigung erteilt werden, indem ihm eine oder mehrere Administratorberechtigungsstufen zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen und anderen Administratoren über den Befehl GRANT AUTHORITY Berechtigungsstufen zuordnen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Ein Administrator kann andere Administrator-IDs registrieren, den IDs Berechtigungsstufen zuordnen, IDs umbenennen, IDs entfernen und IDs für den Server sperren oder entsperren.

Ein Administrator kann den Zugriff auf bestimmte Clientknoten für Rootbenutzer-IDs und Nicht-Rootbenutzer-IDs steuern. Standardmäßig kann eine Nicht-Rootbenutzer-ID keine Daten auf dem Knoten sichern. Ändern Sie mit dem Befehl UPDATE NODE die Knoteneinstellungen, um Sicherungen zu ermöglichen.

Kennwörter

Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer beim Zugriff auf den Server ein Kennwort eingeben.

Verwenden Sie LDAP (Lightweight Directory Access Protocol), um striktere Anforderungen für Kennwörter anzuwenden. Weitere Informationen finden Sie in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1).

Tabelle 1. Merkmale der Kennwortauthentifizierung

Merkmale	Weitere Informationen
Abhängigkeit von der Groß-/Kleinschreibung	Nicht von der Groß-/Kleinschreibung abhängig.
Standardwert für Kennwortablauf	90 Tage. Der Ablaufzeitraum beginnt mit der ersten Registrierung einer Administrator-ID oder eines Clientknotens beim Server. Wenn das Kennwort innerhalb dieses Zeitraums nicht geändert wird, muss das Kennwort beim nächsten Zugriff des Benutzers auf den Server geändert werden.
Ungültige Kennworteingabeversuche	Sie können einen Grenzwert für aufeinanderfolgende ungültige Kennworteingabeversuche für alle Clientknoten definieren. Wenn der Grenzwert überschritten wird, sperrt der Server den Knoten.
Kennwortlänge	Der Administrator kann eine Mindestlänge angeben.

Sitzungssicherheit

Die Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, -Verwaltungsclients und -Servern verwendet wird und mit dem Parameter SESSIONSECURITY festgelegt wird.

Der Parameter SESSIONSECURITY kann auf einen der folgenden Werte gesetzt werden:

- Mit dem Wert STRICT wird die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, -Knoten und -Administratoren durchgesetzt.
- Der Wert TRANSITIONAL gibt an, dass das vorhandene Kommunikationsprotokoll verwendet wird, wenn Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Wenn SESSIONSECURITY=TRANSITIONAL angegeben ist, werden strengere Sicherheitseinstellungen automatisch durchgesetzt, da höhere Versionen des TLS-Protokolls verwendet werden, wenn die Software auf Version 8.1.2 oder höher aktualisiert wird. Nachdem ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch in den Wert STRICT geändert und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder unter Verwendung früherer TLS-Protokolle authentifizieren.

Weitere Informationen zu den Werten für den Parameter SESSIONSECURITY enthalten die Beschreibungen der folgenden Befehle.

Tabelle 2. Befehle zum Festlegen des Parameters SESSIONSECURITY

Entität	Befehl
Clientknoten	• REGISTER NODE • UPDATE NODE
Administratoren	• REGISTER ADMIN • UPDATE ADMIN
Server	• DEFINE SERVER • UPDATE SERVER

Administratoren, die sich unter Verwendung des Befehls DSMADMC, des Befehls DSMC oder des Programms dsm authentifizieren, können sich nach der Authentifizierung unter Verwendung von Version 8.1.2 oder höher nicht unter Verwendung einer früheren Version authentifizieren. Die folgenden Tipps liefern Informationen zur Behebung von Authentifizierungsproblemen für Administratoren:
Tipps:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die das Administratorkonto für die Anmeldung verwendet, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto über mehrere Systeme anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf jedem System installiert ist.
- Nachdem sich ein Administrator bei einem Server der Version 8.1.2 oder höher unter Verwendung eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich der Administrator nur auf Clients oder Servern authentifizieren, die Version 8.1.2 oder höher verwenden. Ein Administratorbefehl kann von jedem beliebigen System ausgegeben werden.
- Erstellen Sie, falls erforderlich, ein separates Administratorkonto, das nur mit Clients und Servern verwendet wird, die Software der Version 8.1.1 oder früher verwenden.

Setzen Sie die höchste Sicherheitsstufe für die Kommunikation mit dem IBM Spectrum Protect-Server durch, indem Sie sicherstellen, dass alle Knoten, Administratoren und Server die Sitzungssicherheit STRICT verwenden. Mithilfe des Befehls SELECT können Sie feststellen, welche Server, Knoten und Administratoren die Sitzungssicherheit TRANSITIONAL verwenden und für die Verwendung der Sitzungssicherheit STRICT aktualisiert werden sollten.

Zugehörige Tasks:
Kommunikation schützen

Administratoren verwalten

Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Administratoreinstellungen zu ändern.

Task	Prozedur

Administrator hinzufügen	Um einen Administrator, ADMIN1, mit Systemberechtigung hinzuzufügen und ein Kennwort anzugeben, führen Sie die folgenden Schritte aus:
	a. Registrieren Sie den Administrator und geben Sie Pa$#$twO als Kennwort an, indem Sie den folgenden Befehl ausgeben:
	`register admin admin1 Pa$#$twO`
	b. Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`

Administratorberechtigung ändern	Ändern Sie die Berechtigungsstufe für einen Administrator, ADMIN1.
	• Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`
	• Entziehen Sie dem Administrator die Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`revoke authority admin1 classes=system`

Administratoren entfernen	Entfernen Sie einen Administrator, ADMIN1, sodass er nicht mehr auf den IBM Spectrum Protect-Server zuzugreifen kann, indem Sie den folgenden Befehl ausgeben: `remove admin admin1`
Zugriff auf den Server vorübergehend verhindern	Sperren oder entsperren Sie einen Administrator, indem Sie den Befehl LOCK ADMIN bzw. UNLOCK ADMIN verwenden.

Kennwortanforderungen ändern

Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.

Informationen zu diesem Vorgang

Indem Sie die Kennwortauthentifizierung durchsetzen und Kennworteinschränkungen verwalten, können Sie Ihre Daten und Ihre Server vor möglichen Sicherheitsrisiken schützen.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Kennwortanforderungen für IBM Spectrum Protect-Server zu ändern.

Tabelle 1. Authentifizierungstasks für IBM Spectrum Protect-Server

Task	Prozedur

Task	Prozedur
Grenzwert für ungültige Kennworteingabeversuche festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl ungültiger Versuche im Feld Grenzwert für ungültige Anmeldeversuche an. Der Standardwert bei der Installation ist 0.
Mindestlänge für Kennwörter festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl Zeichen im Feld Mindestlänge für Kennwort an.
Ablaufzeitraum für Kennwörter festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl Tage im Feld Allgemeine Kennwortablaufdauer an.
Kennwortauthentifizierung inaktivieren	Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer ein Kennwort eingeben, um auf den Server zugreifen zu können. Sie können die Kennwortauthentifizierung nur für Kennwörter inaktivieren, die mit dem Server (LOCAL) authentifiziert werden. Durch das Inaktivieren der Kennwortauthentifizierung erhöht sich das Sicherheitsrisiko für den Server.

Standardauthentifizierungsmethode festlegen	Geben Sie den Befehl SET DEFAULTAUTHENTICATION aus. Um beispielsweise den Server als die Standardauthentifizierungsmethode zu verwenden, geben Sie den folgenden Befehl aus:
	
	`set defaultauthentication local`
	
	Um einen Clientknoten für die Authentifizierung mit dem Server zu aktualisieren, schließen Sie `AUTHENTICATION=LOCAL` in den Befehl UPDATE NODE ein:
	
	`update node authentication=local`

Zugehörige Konzepte:

IBM Spectrum Protect-Benutzer mithilfe eines LDAP-Servers authentifizieren

Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1)

Server auf dem System schützen

Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

Vorgehensweise

Stellen Sie sicher, dass nicht berechtigte Benutzer nicht auf die Verzeichnisse für die Serverdatenbank und die Serverinstanz zugreifen können. Behalten Sie die Zugriffseinstellungen für diese Verzeichnisse bei, die Sie während der Implementierung konfiguriert haben.

- Benutzerzugriff auf den Server einschränken
  Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.
- Zugriff über Porteinschränkungen einschränken
  Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

Benutzerzugriff auf den Server einschränken

Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Vorgehensweise

1. Nachdem Sie einen Administrator mit dem Befehl REGISTER ADMIN registriert haben, legen Sie die Berechtigungsstufe des Administrators mithilfe des Befehls GRANT AUTHORITY fest. Ausführliche Informationen zum Festlegen und Ändern der Berechtigung finden Sie in Administratoren verwalten.
2. Um die Berechtigung eines Administrators zur Ausführung bestimmter Tasks zu steuern, verwenden Sie die beiden folgenden Serveroptionen:
   a. Über die Serveroption QUERYAUTH können Sie die Berechtigungsstufe auswählen, die ein Administrator haben muss, um Befehle QUERY und SELECT ausgeben zu können. Standardmäßig ist keine Berechtigungsstufe erforderlich. Sie können die Anforderung in eine der Berechtigungsstufen, einschließlich Systemberechtigung, ändern.
   b. Über die Serveroption REQSYSAUTHOUTFILE können Sie angeben, dass Systemberechtigung für Befehle erforderlich ist, die zur Folge haben, dass der Server Daten in eine externe Datei schreibt. Standardmäßig ist für diese Befehle Systemberechtigung erforderlich.
3. Sie können die Datensicherung auf einem Clientknoten ausschließlich auf Rootbenutzer-IDs oder berechtigte Benutzer beschränken. Um beispielsweise Sicherungen auf die Rootbenutzer-ID zu beschränken, geben Sie den Befehl REGISTER NODE oder UPDATE NODE unter Angabe des Parameters BACKUPINITIATION=root aus:

```
update node backupinitiation=root
```

Zugriff über Porteinschränkungen einschränken

Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

Informationen zu diesem Vorgang

Gegebenenfalls müssen Sie abhängig von Ihren Sicherheitsanforderungen den Zugriff auf bestimmte Server einschränken. Der IBM Spectrum Protect-Server kann so konfiguriert werden, dass er an vier TCP/IP-Ports empfangsbereit ist: zwei Ports, die für reguläre TCP/IP-Protokolle oder SSL-/TLS-Protokolle verwendet werden können, und zwei Ports, die nur für das SSL-/TLS-Protokoll verwendet werden können.

Vorgehensweise

Sie können die Serveroptionen wie in Tabelle 1 aufgeführt zur Angabe des erforderlichen Ports festlegen.

Tabelle 1. Serveroptionen und Portzugriff

Serveroption	Portzugriff
TCPPORT	Gibt die Nummer des Ports an, dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist 1500.
TCPADMINPORT	Gibt die Nummer des Ports an, an dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von anderen Sitzungen als Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist der Wert für TCPPORT. Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPPORT verwendet, zu trennen.
SSLTCPPORT	Gibt die SSL-TCP/-IP-Portadresse für einen Server an. Dieser Port ist nur für SSL-fähige Sitzungen empfangsbereit. Ein Standardwert für den Port ist nicht verfügbar.
SSLTCPADMINPORT	Gibt die Portadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen von SSL-fähigen Sitzungen wartet. Ein Standardwert für den Port ist nicht verfügbar. Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPPORT verwendet, zu trennen.

Zugehörige Verweise:
Planung des Firewallzugriffs

Server stoppen und starten

Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.

Vorbereitende Schritte

Um den IBM Spectrum Protect-Server stoppen und starten zu können, müssen Sie über System- oder Bedienerberechtigung verfügen.

- Server stoppen
  Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.
- Server für Verwaltungs- oder Rekonfigurationstasks starten
  Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

Server stoppen

Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

Informationen zu diesem Vorgang

Wenn Sie den Befehl HALT zum Stoppen des Servers ausgeben, werden die folgenden Aktionen ausgeführt:

- Alle Prozesse und Clientknotensitzungen werden abgebrochen.
- Alle aktuellen Transaktionen werden gestoppt. (Die Transaktionen werden rückgängig gemacht, wenn der Server erneut gestartet wird.)

Vorgehensweise

Um das System vorzubereiten und den Server zu stoppen, führen Sie die folgenden Schritte aus:

1. Verhindern Sie, dass neue Clientknotensitzungen gestartet werden, indem Sie den Befehl DISABLE SESSIONS ausgeben:

   ```
   disable sessions all
   ```

2. Bestimmen Sie, ob Clientknotensitzungen oder -prozesse aktiv sind, indem Sie die folgenden Schritte ausführen:
   a. Rufen Sie die Seite Übersicht im Operations Center auf, auf der im Bereich Aktivität die Gesamtzahl Prozesse und Sitzungen angezeigt wird, die derzeit aktiv sind. Wenn die Zahlen erheblich von den Zahlen abweichen, die normalerweise während Ihrer täglichen Speicherverwaltungsroutine angezeigt werden, überprüfen Sie mithilfe weiterer Statusanzeiger im Operations Center, ob ein Problem vorliegt.
   b. Zeigen Sie das Diagramm im Bereich Aktivität an, um den Umfang des Datenaustauschs im Netz für die folgenden Perioden zu vergleichen:
      - Die laufende Periode, d. h. die letzte 24-Stunden-Periode
      - Die vorherige Periode, d. h. die 24 Stunden vor der laufenden Periode

      Wenn das Diagramm für die vorherige Periode den erwarteten Umfang des Datenaustauschs darstellt, können deutliche Abweichungen in dem Diagramm für die laufende Periode auf ein Problem hindeuten.
   c. Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details. Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, rufen Sie mithilfe von Verwaltungsbefehlen Informationen zu Prozessen ab. Geben Sie den Befehl QUERY PROCESS aus, um Prozesse abzufragen; geben Sie den Befehl QUERY SESSION aus, um Informationen zu Sitzungen abzurufen.
3. Warten Sie, bis die Clientknotensitzungen abgeschlossen sind oder brechen Sie diese ab. Um Prozesse und Sitzungen abzubrechen, führen Sie die folgenden Schritte aus:
   - Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
   - Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
   - Klicken Sie auf Abbrechen.
   - Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, brechen Sie Sitzungen mithilfe von Verwaltungsbefehlen ab. Geben Sie den Befehl CANCEL SESSION aus, um eine Sitzung abzubrechen; geben Sie den Befehl CANCEL PROCESS aus, um Prozesse abzubrechen.
     Tipp: Wenn der Prozess, der abgebrochen werden soll, auf die Bereitstellung eines Banddatenträgers wartet, wird die Mountanforderung abgebrochen. Wenn Sie beispielsweise einen Befehl EXPORT, IMPORT oder MOVE DATA ausgeben, leitet der Befehl möglicherweise einen Prozess ein, der die Bereitstellung eines Banddatenträgers erfordert. Wenn jedoch ein Banddatenträger durch ein automatisiertes Speicherarchiv bereitgestellt wird, wird die Abbruchoperation unter Umständen erst wirksam, wenn der Bereitstellungsprozess abgeschlossen ist. Abhängig von Ihrer Systemumgebung kann dies mehrere Minuten dauern.
4. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

   ```
   halt
   ```

Server für Verwaltungs- oder Rekonfigurationstasks starten

Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

Informationen zu diesem Vorgang

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm DSMSERV mit dem Parameter MAINTENANCE ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.
Tipps:

- Sie müssen die Serveroptionsdatei, dsmserv.opt, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung, den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

Vorgehensweise

Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

```
dsmserv maintenance
```

Tipp: Informationen zum Anzeigen eines Ein Video zum Starten des Servers im Verwaltungsmodus kann über Server im Verwaltungsmodus starten angezeigt werden.

Nächste Schritte

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl HALT ausgeben:

   ```
   halt
   ```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden. Führen Sie die Anweisungen für Ihr Betriebssystem aus:
   - AIX-BetriebssystemeServerinstanz starten
   - Linux-BetriebssystemeServerinstanz starten
   - Windows-BetriebssystemeServerinstanz starten

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

Durchführung eines Upgrades für den Server planen

Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.

Informationen zu diesem Vorgang

Beachten Sie diese Richtlinien:

- Bei der bevorzugten Methode erfolgt das Upgrade für den Server mithilfe des Installationsassistenten. Nachdem Sie den Assistenten gestartet haben, klicken Sie im Fenster IBM Installation Manager auf das Symbol zum Aktualisieren; klicken Sie nicht auf das Symbol zum Installieren oder Ändern!
- Wenn sowohl für die Serverkomponente als auch für die Operations Center-Komponente Upgrades verfügbar sind, wählen Sie die Kontrollkästchen aus, um das Upgrade für beide Komponenten durchzuführen.

Vorgehensweise

1. Überprüfen Sie die Liste der Fixpacks und vorläufigen Fixes. Siehe Technote 1239415.
2. Studieren Sie die Produktverbesserungen, die in der Readme-Datei beschrieben sind.
   Tipp: Wenn Sie die Installationspaketdatei von der IBM Spectrum Protect-Unterstützungssite abrufen, können Sie auch auf die Readme-Datei zugreifen.

3. Stellen Sie sicher, dass die Version, auf die das Upgrade für Ihren Server durchgeführt wird, mit anderen Komponenten, wie beispielsweise Speicheragenten und Speicherarchivclients, kompatibel ist. Siehe Technote 1302789.
4. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden. Siehe Technote 1053218.
5. Lesen Sie die Upgradeanweisungen. Stellen Sie sicher, dass Sie die Serverdatenbank, die Einheitenkonfigurationsinformationen und die Protokolldatei für Datenträger sichern.

Nächste Schritte

Um ein Fixpack oder einen vorläufigen Fix zu installieren, führen Sie die Anweisungen für Ihr Betriebssystem aus:

- AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
- Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
- Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren

Zugehörige Informationen:
Upgrade- und Umlagerungsprozess - Häufig gestellte Fragen

Vorbereitungen für einen Ausfall oder eine Systemaktualisierung

Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass Sie die regelmäßige Ausführung von Aktivitäten planen, um den Server zu verwalten und zu schützen.

Vorgehensweise

1. Brechen Sie Prozesse und Sitzungen, die aktiv sind, ab, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie im Operations Center auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
   b. Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
   c. Klicken Sie auf Abbrechen.
2. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

   ```
   halt
   ```

   Tipp: Sie können den Befehl HALT im Operations Center ausgeben, indem Sie den Mauszeiger über das Symbol für Einstellungen bewegen und auf Command Builder klicken. Wählen Sie dann den Server aus, geben Sie `halt` ein und drücken Sie die Eingabetaste.

Plan zur Wiederherstellung nach einem Katastrophenfall implementieren

Implementieren Sie eine Strategie zur Wiederherstellung nach einem Katastrophenfall, um Ihre Anwendungen in einem Katastrophenfall wiederherstellen und hohe Serververfügbarkeit sicherstellen zu können.

Informationen zu diesem Vorgang

Bestimmen Sie Ihre Anforderungen für die Wiederherstellung nach einem Katastrophenfall, indem Sie die Geschäftsprioritäten für die Clientknotenwiederherstellung und die Systeme, die zum Wiederherstellen von Daten verwendet werden, angeben und prüfen, ob Clientknoten über eine Verbindung zu einem Wiederherstellungsserver verfügen. Verwenden Sie zum Schützen von Daten Replikation und Speicherpoolschutz. Außerdem müssen Sie bestimmen, wie oft Verzeichniscontainerspeicherpools geschützt werden.

- Wiederherstellungsdrilloperationen ausführen
  Planen Sie Drilloperationen für die Wiederherstellung nach einem Katastrophenfall als Vorbereitung für Prüfungen, mit denen die Wiederherstellbarkeit des IBM Spectrum Protect-Servers bestätigt wird, und um sicherzustellen, dass nach einem Ausfall Daten zurückgeschrieben und Operationen wiederaufgenommen werden können. Mithilfe einer Drilloperation können Sie außerdem vor dem Eintreten einer kritischen Situation sicherstellen, dass alle Daten zurückgeschrieben und Operationen wiederaufgenommen werden können.

Wiederherstellung nach einem Systemausfall

Bei IBM Spectrum Protect-Plattenspeicherlösungen für einen einzelnen Standort können Sie den Bestand nur lokal wiederherstellen und die Datenbank zum Schutz Ihrer Daten zurückschreiben.

Vorgehensweise

Verwenden Sie abhängig vom Typ der gesicherten Informationen eine der folgenden Methoden, um den Bestand an einem lokalen Standort wiederherzustellen.
Einschränkung: Da bei Plattenspeicherlösungen für einen einzelnen Standort keine zweite Kopie des Speicherpools vorhanden ist, können Speicherpools nicht zurückgeschrieben werden. Informationen zur Architektur von Plattenspeicherlösungen finden Sie in IBM Spectrum Protect-Lösung auswählen.

Tabelle 1. Szenarios für die Wiederherstellung nach einem Katastrophenfall

Szenario	Prozedur
Der Zugriff auf Ihr System ist nicht möglich und das System soll mithilfe von Systemtools lokal mit dem Stand einer früheren Version zurückgeschrieben werden.	• Verwenden Sie IBM Spectrum Protect, um den Server auf einem anderen Server zu sichern. • Verwenden Sie Betriebssystemtools, um Ihr System zu sichern und mit dem Stand einer früheren Version zurückzuschreiben.
Bei einem Ausfall oder einer Katastrophe sollen Ihre Daten aus gesicherten Versionen der Daten zurückgeschrieben werden.	• Um einen Client zu sichern, wählen Sie auf der Seite TSM-Clients im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf Sichern. • Wählen Sie auf der Seite TSM-Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Serverdatenbank sichern aus. Um einen Speicherpool aus einer gesicherten Version des Speicherpools zurückzuschreiben, müssen Sie die Datenbank zurückschreiben. Geben Sie den Befehl DSMSERV RESTORE DB aus, um die Datenbank und zugehörige Speicherpools mit dem Stand einer gesicherten Version zurückzuschreiben.

- Datenbank zurückschreiben
  Unter Umständen müssen Sie die IBM Spectrum Protect-Datenbank nach einem Katastrophenfall zurückschreiben. Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Zum Zurückschreiben der Datenbank benötigen Sie Datenträger mit einer Datenbankgesamt-, -teil- oder -momentaufnahmesicherung.

Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
DSMSERV RESTORE DB (Datenbank zurückschreiben)

Plattenspeicherlösung für mehrere Standorte

Diese Datenschutzlösung stellt Replikation an mehreren Standorten bereit, sodass jeder Server Daten für den jeweils anderen Standort schützt.

- Planung für eine Plattenspeicherdatenschutzlösung für mehrere Standorte
  Planung für eine Plattenspeicherdatenschutzlösung für mehrere Standorte mit Servern an zwei Standorten, die Datendeduplizierung und Replikation verwenden.
- Implementierung einer Plattenspeicherdatenschutzlösung für mehrere Standorte
  Die Plattenspeicherlösung für mehrere Standorte wird an zwei Standorten konfiguriert und verwendet Datendeduplizierung und Replikation.
- Plattenspeicherlösung für mehrere Standorte überwachen
  Überwachen Sie nach der Implementierung einer Plattenspeicherlösung für mehrere Standorte mit IBM Spectrum Protect die Lösung, um ihre korrekte Funktionsweise sicherzustellen. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.
- Operationen für eine Plattenspeicherlösung für mehrere Standorte verwalten
  Verwenden Sie diese Informationen, um Operationen für eine Plattenspeicherlösung für mehrere Standorte mit IBM Spectrum Protect zu verwalten, die einen Server umfasst und Datendeduplizierung für mehrere Standorte verwendet.

Planung für eine Plattenspeicherdatenschutzlösung für mehrere Standorte

Planung für eine Plattenspeicherdatenschutzlösung für mehrere Standorte mit Servern an zwei Standorten, die Datendeduplizierung und Replikation verwenden.

Implementierungsmethoden

Sie können Server für eine Plattenspeicherlösung für mehrere Standorte wie folgt konfigurieren:

Server unter Verwendung des Operations Center und von Verwaltungsbefehlen konfigurieren

Sie können eine Reihe von Speichersystemen und die Server-Software für Ihre Lösung konfigurieren. Konfigurationstasks werden mithilfe von Assistenten und Optionen im Operations Center und mithilfe von IBM Spectrum Protect-Befehlen ausgeführt. Informationen zu ersten Schritten finden Sie in Planungsroadmap.

Server mithilfe automatisierter Scripts konfigurieren

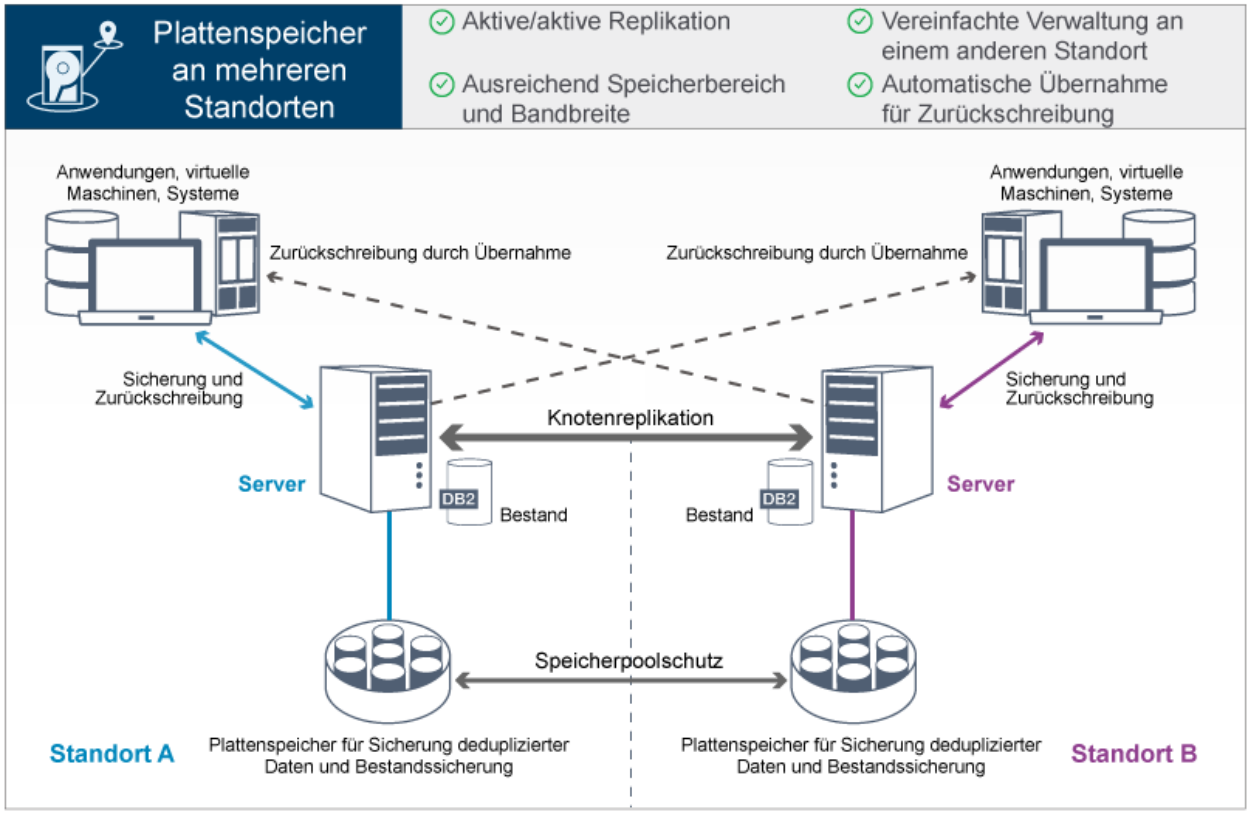
Eine ausführliche Anleitung zur Konfiguration mit bestimmten IBM® Storwize-Speichersystemen sowie zur Verwendung automatisierter Scripts zur Konfiguration jedes Servers finden Sie in den IBM Spectrum Protect-Blueprints. Die Dokumentation und Scripts sind unter IBM developerWorks verfügbar: IBM Spectrum Protect Blueprints.

Die Blueprint-Dokumentation umfasst keine Schritte zum Installieren und Konfigurieren des Operations Center oder zum Konfigurieren der sicheren Kommunikation mithilfe von Transport Security Layer (TLS). Die Replikation wird unter Verwendung von Befehlen im Anschluss an die Konfiguration des Servers konfiguriert. Eine Option zur Verwendung von Elastic Storage Server-Speicher auf der Basis der Technologie von IBM Spectrum Scale ist eingeschlossen.

Planungsroadmap

Planen Sie eine Plattenspeicherlösung für mehrere Standorte, indem Sie das Architekturlayout in der folgenden Abbildung überprüfen und dann die Roadmap-Tasks ausführen, die auf die Abbildung folgen.

Abbildung 1. Plattenspeicherlösung für mehrere Standorte



Die folgenden Schritte sind für die korrekte Planung für eine Plattenspeicherumgebung an mehreren Standorten erforderlich.

1. Wählen Sie Ihre Systemgröße aus.
2. Führen Sie die Planung für die Standorte aus.
3. Erfüllen Sie die Systemvoraussetzungen für Hardware und Software.
4. Notieren Sie die Werte für Ihre Systemkonfiguration in den Arbeitsblättern zur Planung.
5. Führen Sie die Planung für den Speicher durch.
6. Führen Sie die Planung für die Sicherheit durch.
    a. Führen Sie die Planung für Administratorrollen durch.
    b. Führen Sie die Planung für die sichere Kommunikation durch.
    c. Führen Sie die Planung für verschlüsselte Daten durch.
    d. Führen Sie die Planung für den Firewallzugriff durch.

Systemgröße auswählen

Wählen Sie die Größe des IBM Spectrum Protect-Servers auf der Basis des verwalteten Datenvolumens und der Systeme, die geschützt werden müssen, aus.

Informationen zu diesem Vorgang

Mithilfe der Informationen in der Tabelle können Sie auf der Basis des verwalteten Datenvolumens die erforderliche Größe des Servers bestimmen.

In der folgenden Tabelle ist das Datenvolumen aufgeführt, das von einem Server verwaltet wird. Dieses Volumen umfasst alle Versionen. Das tägliche Datenvolumen gibt an, wie viele neue Daten täglich gesichert werden. Sowohl das Gesamtvolumen der verwalteten Daten als auch das tägliche Volumen an neuen Daten wird als Größe vor jeglicher Datenreduktion gemessen.

Tabelle 1. Größe des Servers bestimmen

Gesamtvolumen der verwalteten Daten	**Volumen an täglich zu sichernden neuen Daten**	**Erforderliche Servergröße**
48 TB bis 192 TB	Bis zu 10 TB pro Tag	Klein
200 TB bis 800 TB	10 bis 20 TB pro Tag	Mittelgroß
1000 TB bis 4000 TB	20 bis 100 TB pro Tag	Groß

Die Werte für die tägliche Sicherung in der Tabelle basieren auf Testergebnissen für Objekte mit einer Größe von 128 MB, die von IBM Spectrum Protect for Virtual Environments verwendet werden. Bei Workloads, die aus Objekten bestehen, die kleiner als 128 KB sind, werden diese Grenzwerte für tägliche Sicherungen möglicherweise nicht erreicht.

Planung der Standorte

Überprüfen Sie Anwendungsfälle und bewerten Sie die Faktoren, um den effizientesten Datenschutz für die Plattenspeicherlösung für mehrere Standorte in IBM Spectrum Protect bereitzustellen.

Anwendungsfälle

Bei der Plattenspeicherlösung für mehrere Standorte wird mindestens eine Kopie gesicherter Daten erstellt. Wenn sich die IBM Spectrum Protect-Server an unterschiedlichen Standorten befinden, werden die gesicherten Replikate an einem anderen Standort aufbewahrt. Ihr Unternehmen könnte aus verschiedenen Gründen von einer Plattenspeicherlösung für mehrere Standorte profitieren, die häufigsten Gründe für die Verwendung einer Plattenspeicherlösung für mehrere Standorte umfassen jedoch die folgenden Replikationsszenarios:

Replikation vom primären Standort zum Standort für die Wiederherstellung nach einem Katastrophenfall

In diesem Szenario werden Daten, die am primären Standort (Standort A) gesichert werden, auf einen Server am sekundären Standort (Standort B), dem Standort für die Wiederherstellung nach einem Katastrophenfall, repliziert. Bei einer Katastrophe an Standort A, beispielsweise dem Ausfall des Servers, können Sie Systeme mithilfe des Servers an Standort B wiederherstellen. Sie können auch stattdessen mithilfe des Servers an Standort A Daten in primären Speicherpools an Standort B zurückschreiben, beispielsweise nach einem Plattenspeicherfehler an Standort B.

Gegenseitige Replikation an zwei aktiven Standorten

In diesem Szenario werden lokale Daten an jedem Standort von den Servern an beiden Standorten, Standort A und Standort B, gesichert. Daten, die an Standort A gesichert werden, werden an Standort B repliziert und Daten, die an Standort B gesichert werden, werden an Standort A repliziert. Wenn Daten, die gesichert wurden, an Standort A verloren gehen, können Sie Speicherpooldaten mithilfe des Servers an Standort B auf dem Server an Standort A wiederherstellen. Wenn Standort A nicht mehr verfügbar ist, können Sie die replizierten Daten für Standort A auf einem neuen System an Standort B wiederherstellen. Sie müssen die Größe der Serverressourcen ändern, um sicherzustellen, dass beide Server über ausreichend Kapazität zum Sichern und Zurückschreiben aller Clientknoten im Rahmen Ihres Plans zur Wiederherstellung nach einem Katastrophenfall verfügen.

Schutz ferner Server am primären Standort

In diesem Szenario konfigurieren Sie ferne Server, die relativ klein sind, für die Replikation von Daten, die auf einem größeren Server am primären Standort gesichert werden. Wenn die Bandbreite begrenzt ist, ist die Zurückschreibung von Systemen an die fernen Standorte unter Umständen nicht praktikabel. In diesem Fall können Sie Systeme, falls gewünscht, am primären Standort wiederherstellen, bevor die gesicherten Daten auf die fernen Server repliziert werden.

Zu bewertende Faktoren

Bewerten Sie vor der Implementierung einer Plattenspeicherlösung für mehrere Standorte die folgenden Faktoren:

Netzbandbreite

Das Netz muss über genügend Bandbreite für die erwarteten Datenübertragungen zwischen Knoten, für die Replikation und für die standortübergreifenden Zurückschreibungsoperationen verfügen, die für die Wiederherstellung nach einem Katastrophenfall erforderlich sind. Bevor Sie mit dem Testen des Replikationsdurchsatzes fortfahren, müssen Sie sicherstellen, dass Ihr Netz den Replikationsdatenverkehr handhaben kann. Berechnen Sie die für den stabilen Zustand erforderliche Netzbandbreite, indem Sie die Richtlinien in Für die Replikation erforderliche Netzbandbreite schätzen (Version 7.1.1) anwenden.

Die Netzverbindung ist häufig eine gemeinsam genutzte Ressource. Planen Sie die Uhrzeit, zu der die Knotenreplikation ausgeführt werden soll, um einen Konflikt mit anderen Ressourcennutzern zu verhindern. Gegebenenfalls kann die Aktivität mithilfe von Netzsteuerelementen

auch auf einen Teil der Bandbreite beschränkt werden. In IBM Spectrum Protect sind keine Steuerelemente zur Beschränkung der Netzauslastung verfügbar.

Ressourcen für die Erstreplikation

Um eine Datenschutzlösung für zwei Standorte zu konfigurieren, müssen Sie Daten zunächst von Standort A auf den Zielserver an Standort B replizieren. Um sicherzustellen, dass die Erstreplikation erfolgreich ist, müssen Sie bestimmen, ob die zum Replizieren der Daten erforderliche Netzbandbreite, Prozessorressourcen und Zeit verfügbar sind. Unter Umständen müssen Sie die Replikation der ersten Gesamtsicherungen für mehrere Tage planen. Wenn der Zeitplan für die Erstsicherungen nicht erweitert werden kann, können Sie Daten von Standort A an Standort B replizieren, ohne das Netz zu verwenden. Sie können beispielsweise die gesicherten Daten mithilfe von Datenträgern exportieren und importieren oder den Quellen- und Zielserver vorübergehend an denselben Standort verlegen.

Tägliche Datenaufnahme

Bei der Plattenspeicherlösung für mehrere Standorte muss die tägliche Datenaufnahme und die Aufbewahrung aller Daten innerhalb der Kapazität der Konfigurationen liegen. Beispielsweise liegt bei einer großen Konfiguration die Kapazität der Datenaufnahme bei bis zu 100 TB pro Tag einschließlich Knotenreplikation. In Fällen, in denen die Sicherungsanforderungen die Kapazität eines einzelnen Servers überschreiten, können Sie eine Lösung konfigurieren, die mehrere Server zum Erreichen der erforderlichen Kapazität verwendet.

Serverkonfiguration

Die Serverkonfiguration muss die Anforderungen der Plattenspeicherlösung für mehrere Standorte erfüllen oder überschreiten.

Einzelnes Replikat gesicherter Daten

Die Plattenspeicherlösung für mehrere Standorte ist am effizientesten, wenn eine einzelne ausgelagerte Kopie der gesicherten Daten Ihre Anforderungen in Bezug auf Datenschutz und Risikominderung erfüllt. In diesem Fall wird die einzelne ausgelagerte Kopie der Daten am Standort eines Replikationsservers aufbewahrt.

Zugehörige Verweise:
Systemvoraussetzungen für eine Plattenspeicherlösung für mehrere Standorte

Systemvoraussetzungen für eine Plattenspeicherlösung für mehrere Standorte

Überprüfen Sie nach der Auswahl der besten IBM Spectrum Protect-Lösung für Ihre Datenschutzanforderungen die Systemvoraussetzungen, um die Planung für die Implementierung der Datenschutzlösung auszuführen.

Stellen Sie sicher, dass Ihr System die Hardware- und Softwarevoraussetzungen für die geplante Größe des Servers erfüllt.

- Hardwarevoraussetzungen
  Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.
- Softwarevoraussetzungen
  Die Dokumentation für die IBM Spectrum Protect-Plattenspeicherlösung für mehrere Standorte umfasst Installations- und Konfigurationstasks für die folgenden Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

Zugehörige Informationen:
IBM Spectrum Protect Supported Operating Systems

Hardwarevoraussetzungen

Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.

Eine Definition der Systemgrößen finden Sie in Systemgröße auswählen.

In der folgenden Tabelle sind die Hardwaremindestvoraussetzungen für den Server und Speicher auf der Basis der Größe Servers aufgelistet, der erstellt werden soll. Wenn Sie logische Partitionen (LPARs) oder Arbeitspartitionen (WPARs) verwenden, passen Sie die Netzvoraussetzungen an, um den Partitionsgrößen Rechnung zu tragen.

Hardwarekomponente	Kleines System	Mittelgroßes System	Großes System
Serverprozessor	AIX-Betriebssysteme6 Prozessorkerne, 3,42 GHz oder schneller Linux-Betriebssysteme Windows-Betriebssysteme12 Prozessorkerne, 1,9 GHz oder schneller	AIX-Betriebssysteme8 Prozessorkerne, 3,42 GHz oder schneller Linux-Betriebssysteme Windows-Betriebssysteme16 Prozessorkerne, 2,0 GHz oder schneller	AIX-Betriebssysteme20 Prozessorkerne, 3,42 GHz Linux-Betriebssysteme Windows-Betriebssysteme32 Prozessorkerne, 2,0 GHz oder schneller
Serverspeicher	64 GB RAM	128 GB RAM	192 GB RAM

Hardwarekomponente	Kleines System	Mittelgroßes System	Großes System
Netz	• 10 GB Ethernet (1 Port) • 8 GB Fibre Channel-Adapter (2 Ports)	• 10 GB Ethernet (2 Ports) • 8 GB Fibre Channel-Adapter (2 Ports)	• 10 GB Ethernet (4 Ports) • 8 GB Fibre Channel-Adapter (4 Ports)
Speicher	• 1,3 TB Bestand plus Speicherbereich für Operations Center-Datensätze • 46 TB deduplizierter Verzeichniscontainerspeicherpool	• 2 TB Bestand plus Speicherbereich für Operations Center-Datensätze • 200 TB deduplizierter Verzeichniscontainerspeicherpool	• 6 TB Bestand plus Speicherbereich für Operations Center-Datensätze • 1000 TB deduplizierter Verzeichniscontainerspeicherpool

Speicherbedarf für die Datenbank für das Operations Center schätzen

Hardwarevoraussetzungen für das Operations Center sind mit Ausnahme des Speicherbereichs für die Datenbank und das Archivprotokoll (Bestand), den das Operations Center zum Aufnehmen von Datensätzen für verwaltete Clients verwendet, in die vorherige Tabelle eingeschlossen.

Wenn Sie nicht planen, das Operations Center auf demselben System wie den Server zu installieren, können Sie die Systemanforderungen separat schätzen. Informationen zum Berechnen der Systemanforderungen für das Operations Center enthält die Technote 1641684 für die Berechnungsfunktion der Systemanforderungen.

Die Verwaltung des Operations Center auf dem Server stellt eine Workload dar, die zusätzlichen Speicherbereich für Datenbankoperationen erfordert. Wie viel Speicherbereich erforderlich ist, ist von der Anzahl Clients abhängig, die auf einem Server überwacht werden. Lesen Sie die folgenden Richtlinien, um schätzen zu können, wie viel Speicherbereich Ihr Server erfordert.

Speicherbereich in der Datenbank
: Das Operations Center benötigt ungefähr 1,2 GB Speicherbereich in der Datenbank pro 1000 Clients, die auf einem Server überwacht werden. Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1500 Clients. Bei dieser Konfiguration sind insgesamt 6500 Clients auf den vier Servern vorhanden und ungefähr 8,4 GB Speicherbereich in der Datenbank erforderlich. Bei der Berechnung dieses Werts werden die 6500 Clients auf den nächsthöheren Tausenderwert aufgerundet, d. h. auf 7000:

```
7 x 1,2 GB = 8,4 GB
```

Speicherbereich für das Archivprotokoll
: Das Operations Center verwendet alle 24 Stunden ungefähr 8 GB Speicherbereich für das Archivprotokoll pro 1000 Clients. In dem Beispiel mit den 6500 Clients auf dem Hub-Server und den Peripherieservern werden in einem Zeitraum von 24 Stunden für den Hub-Server 56 GB Speicherbereich für das Archivprotokoll verwendet.
Für jeden Peripherieserver in dem Beispiel werden im Verlauf von 24 Stunden etwa 16 GB Speicherbereich für das Archivprotokoll verwendet. Diese Schätzungen basieren auf dem Standardintervall von 5 Minuten zur Erfassung von Statusdaten. Wenn Sie das Erfassungsintervall von einmal alle 5 Minuten auf einmal alle 3 Minuten reduzieren, erhöht sich der Speicherbedarf. Das folgende Beispiel zeigt die ungefähre Erhöhung des Protokollspeicherbedarfs bei einem Erfassungsintervall von einmal alle 3 Minuten:

- Hub-Server: von 56 GB auf ungefähr 94 GB
- Jeder Peripherieserver: von 16 GB auf ungefähr 28 GB

Vergrößern Sie den Speicherbereich für das Archivprotokoll, sodass genügend Speicherbereich zur Unterstützung des Operations Center ohne Auswirkungen auf die vorhandenen Serveroperationen verfügbar ist.

Hardwarevoraussetzungen für den zweiten Server

Wenn Sie planen, Ihre Standorte so zu konfigurieren, dass alle Daten am ersten Standort an den zweiten Standort repliziert werden, sind die Hardwarevoraussetzungen an beiden Standorten identisch. Soll nur ein Teil der Daten an Ihren zweiten Standort repliziert werden, können die Speicher- und Netzvoraussetzungen geringer ausfallen.

Softwarevoraussetzungen

Die Dokumentation für die IBM Spectrum Protect-Plattenspeicherlösung für mehrere Standorte umfasst Installations- und Konfigurationstasks für die folgenden Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

Informationen zu den Softwarevoraussetzungen für IBM® lin_tape-Einheitentreiber finden Sie in der Veröffentlichung IBM Tape Device Drivers Installation and User's Guide.

AIX-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	IBM AIX 7.1 Weitere Informationen zu Betriebssystemvoraussetzungen finden Sie in AIX: Systemmindestvoraussetzungen für AIX-Systeme.
Dienstprogramm gunzip	Das Dienstprogramm gunzip muss auf Ihrem System verfügbar sein, bevor Sie die Installation oder das Upgrade für den IBM Spectrum Protect-Server ausführen. Stellen Sie sicher, dass das Dienstprogramm gunzip installiert ist und der Pfad zu diesem Dienstprogramm in der Umgebungsvariablen PATH definiert ist.
Dateisystemtyp	JFS2-Dateisysteme AIX-Systeme können ein großes Volumen an Dateisystemdaten zwischenspeichern, wodurch der Speicherplatz, der für Server- und IBM DB2-Prozesse erforderlich ist, reduziert werden kann. Um beim AIX-Server eine Auslagerung zu verhindern, verwenden Sie die Mountoption rbrw für das JFS2-Dateisystem. Für den Dateisystemcache wird weniger Speicher verwendet und für IBM Spectrum Protect ist mehr Speicher verfügbar. Verwenden Sie nicht die Mountoptionen für Dateisysteme, gleichzeitige E/A (CIO = Concurrent I/O) und direkte E/A (DIO = Direct I/O) für Dateisysteme, die die IBM Spectrum Protect-Datenbank, Protokolle oder Speicherpooldatenträger enthalten. Diese Optionen können eine Leistungsverschlechterung vieler Serveroperationen zur Folge haben. IBM Spectrum Protect und DB2 können, wenn dies von Vorteil ist, weiterhin DIO verwenden, IBM Spectrum Protect erfordert die Mountoptionen jedoch nicht, um die Vorteile dieser Verfahren selektiv nutzen zu können.
Andere Software	Korn-Shell (ksh)

Linux-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Red Hat Enterprise Linux 7 (x86_64)
Bibliotheken	GNU C-Bibliotheken, Version 2.3.3-98.38 oder höher, die auf dem IBM Spectrum Protect-System installiert sind. Red Hat Enterprise Linux-Server: • libaio • libstdc++.so.6 (32-Bit- und 64-Bit-Pakete sind erforderlich) • numactl.x86_64
Dateisystemtyp	Formatieren Sie datenbankbezogene Dateisysteme mit ext3 oder ext4. Verwenden Sie für speicherpoolbezogene Dateisysteme XFS.
Andere Software	Korn-Shell (ksh)

Windows-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Microsoft Windows Server 2012 R2 (64-Bit) oder Windows Server 2016
Dateisystemtyp	NTFS
Andere Software	Windows 2012 R2 oder Windows 2016 mit .NET Framework 3.5 ist installiert und aktiviert. Die folgenden Benutzerkontensteuerungsrichtlinien müssen inaktiviert sein: • Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto • Benutzerkontensteuerung: Alle Administratoren im Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen

Zugehörige Tasks:
AIX-Netzoptionen definieren

Arbeitsblätter zur Planung

Verwenden Sie die Arbeitsblätter zur Planung für die Aufzeichnung von Werten, die Sie bei der Konfiguration Ihres Systems und bei der Konfiguration des IBM Spectrum Protect-Servers verwenden. Verwenden Sie die Best-Practice-Standardwerte, die in den Arbeitsblättern

aufgeführt sind.

Jedes Arbeitsblatt unterstützt Sie bei den Vorbereitungen für unterschiedliche Teile der Systemkonfiguration mithilfe der Best-Practice-Werte:

Vorkonfiguration des Serversystems
: Führen Sie mithilfe der Arbeitsblätter zur Vorkonfiguration die Planung für die Dateisysteme und Verzeichnisse aus, die erstellt werden sollen, wenn Sie während der Systemkonfiguration Dateisysteme für IBM Spectrum Protect konfigurieren. Alle Verzeichnisse, die Sie für den Server erstellen, müssen leer sein.

Serverkonfiguration
: Verwenden Sie die Arbeitsblätter zur Konfiguration, wenn Sie den Server konfigurieren. Für die meisten Elemente werden Standardwerte vorgeschlagen; andernfalls ist ein entsprechender Hinweis vorhanden.

AIX

Tabelle 1. Arbeitsblatt für die Vorkonfiguration eines AIX-Serversystems

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
TCP/IP-Portadresse für die Kommunikation mit dem Server	1500		Nicht zutreffend	Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren. Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein.
Verzeichnis für die Serverinstanz	/home/tsminst1/tsminst1		50 GB	Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 2.
Verzeichnis für Serverinstallation	/		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	/usr		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	/var		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	/tmp		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	/opt		Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 10 GB	
Verzeichnis für die aktive Protokolldatei	/tsminst1/TSMalog		• Klein und mittel: 140 GB • Groß: 300 GB	Wenn Sie die aktive Protokolldatei während der Erstkonfiguration des Servers erstellen, setzen Sie die Größe auf 128 GB.
Verzeichnis für das Archivprotokoll	/tsminst1/TSMarchlog		• Klein: 1 TB • Mittel: 3 TB • Groß: 4 TB	
Verzeichnisse für die Datenbank	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 1 TB • Mittel: Mindestens 2 TB • Groß: Mindestens 4 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank: • Klein: Mindestens 4 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 8 Dateisysteme

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
Verzeichnisse für Speicher	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 38 TB • Mittel: Mindestens 180 TB • Groß: Mindestens 500 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher: • Klein: Mindestens 10 Dateisysteme • Mittel: Mindestens 20 Dateisysteme • Groß: Mindestens 40 Dateisysteme
Verzeichnisse für Datenbanksicherung	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 3 TB • Mittel: Mindestens 10 TB • Groß: Mindestens 16 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank: • Klein: Mindestens 2 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6 Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet.

Tabelle 2. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

Element	Standardwert	Eigener Wert	Anmerkungen
DB2-Instanzeigner	tsminst1		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 1 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner.
Kennwort des DB2-Instanzeigners	passw0rd		Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Primärgruppe für den DB2-Instanzeigner	tsmsrvrs		
Servername	Der Standardwert für den Servernamen ist der Systemhostname.		
Serverkennwort	passw0rd		Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Administrator-ID: Benutzer-ID für die Serverinstanz	admin		
Kennwort für die Administrator-ID	passw0rd		Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.

Element	Standardwert	Eigener Wert	Anmerkungen
Startzeit des Zeitplans	22:00		Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt. Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen.

Linux

Tabelle 3. Arbeitsblatt für die Vorkonfiguration eines Linux-Serversystems

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
TCP/IP-Portadresse für die Kommunikation mit dem Server	1500		Nicht zutreffend	Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren. Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein.
Verzeichnis für die Serverinstanz	/home/tsminst1/tsminst1		25 GB	Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 4.
Verzeichnis für die aktive Protokolldatei	/tsminst1/TSMalog		• Klein und mittel: 140 GB • Groß: 300 GB	
Verzeichnis für das Archivprotokoll	/tsminst1/TSMarchlog		• Klein: 1 TB • Mittel: 3 TB • Groß: 4 TB	
Verzeichnisse für die Datenbank	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 1 TB • Mittel: Mindestens 2 TB • Groß: Mindestens 4 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank: • Klein: Mindestens 4 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 8 Dateisysteme
Verzeichnisse für Speicher	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 38 TB • Mittel: Mindestens 180 TB • Groß: Mindestens 500 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher: • Klein: Mindestens 10 Dateisysteme • Mittel: Mindestens 20 Dateisysteme • Groß: Mindestens 40 Dateisysteme

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
Verzeichnisse für Datenbanksicherung	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 3 TB • Mittel: Mindestens 10 TB • Groß: Mindestens 16 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank: • Klein: Mindestens 2 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6 Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet.

Tabelle 4. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

Element	Standardwert	Eigener Wert	Anmerkungen
DB2-Instanzeigner	tsminst1		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 3 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner.
Kennwort des DB2-Instanzeigners	passw0rd		Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Primärgruppe für den DB2-Instanzeigner	tsmsrvrs		
Servername	Der Standardwert für den Servernamen ist der Systemhostname.		
Serverkennwort	passw0rd		Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Administrator-ID: Benutzer-ID für die Serverinstanz	admin		
Kennwort für die Administrator-ID	passw0rd		Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Startzeit des Zeitplans	22:00		Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt. Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen.

Windows

Da für den Server viele Datenträger erstellt werden, konfigurieren Sie den Server mithilfe der Windows-Funktion zum Zuordnen von Plattendatenträgern zu Verzeichnissen (statt der Funktion zum Zuordnen von Plattendatenträgern zu Laufwerkbuchstaben).

Beispielsweise ist C:\tsminst1\TSMdbpsace00 ein Mountpunkt für einen Datenträger mit eigenem Speicherbereich. Der Datenträger wird einem Verzeichnis unter dem Laufwerk C: zugeordnet, nimmt aber keinen Speicherbereich auf Laufwerk C: in Anspruch. Einzige Ausnahme ist das Serverinstanzverzeichnis, C:\tsminst1, das ein Mountpunkt oder ein normales Verzeichnis sein kann.

Tabelle 5. Arbeitsblatt für die Vorkonfiguration eines Windows-Serversystems

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Anmerkungen
TCP/IP-Portadresse für die Kommunikation mit dem Server	1500		Nicht zutreffend	Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren. Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein.
Verzeichnis für die Serverinstanz	C:\tsminst1		25 GB	Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 6.
Verzeichnis für die aktive Protokolldatei	C:\tsminst1\TSMalog		• Klein und mittel: 140 GB • Groß: 300 GB	
Verzeichnis für das Archivprotokoll	C:\tsminst1\TSMarchlog		• Klein: 1 TB • Mittel: 3 TB • Groß: 4 TB	
Verzeichnisse für die Datenbank	C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 1 TB • Mittel: Mindestens 2 TB • Groß: Mindestens 4 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Datenbank: • Klein: Mindestens 4 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 8 Dateisysteme
Verzeichnisse für Speicher	C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 38 TB • Mittel: Mindestens 180 TB • Groß: Mindestens 500 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für den Speicher: • Klein: Mindestens 10 Dateisysteme • Mittel: Mindestens 20 Dateisysteme • Groß: Mindestens 40 Dateisysteme
Verzeichnisse für Datenbanksicherung	C:\tsminst1\TSMbkup00 C:\tsminst1\TSMbkup01 C:\tsminst1\TSMbkup02 C:\tsminst1\TSMbkup03		Mindestens erforderlicher Gesamtspeicherbereich für alle Verzeichnisse: • Klein: Mindestens 3 TB • Mittel: Mindestens 10 TB • Groß: Mindestens 16 TB	Erstellen Sie abhängig von der Größe Ihres Systems eine minimale Anzahl Dateisysteme für die Sicherung der Datenbank: • Klein: Mindestens 2 Dateisysteme • Mittel: Mindestens 4 Dateisysteme • Groß: Mindestens 4 Dateisysteme, vorzugsweise jedoch 6 Das erste Datenbanksicherungsverzeichnis wird auch für das Übernahmeverzeichnis für Archivprotokolle und eine zweite Kopie der Protokolldatei für Datenträger und der Einheitenkonfigurationsdatei verwendet.

Tabelle 6. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

Element	Standardwert	Eigener Wert	Anmerkungen

Element	Standardwert	Eigener Wert	Anmerkungen
DB2-Instanzeigner	tsminst1		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 5 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner.
Kennwort des DB2-Instanzeigners	pAssW0rd		Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Servername	Der Standardwert für den Servernamen ist der Systemhostname.		
Serverkennwort	passw0rd		Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Administrator-ID: Benutzer-ID für die Serverinstanz	admin		
Kennwort für die Administrator-ID	passw0rd		Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Startzeit des Zeitplans	22:00		Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt. Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen.

Planung für Speicher

Wählen Sie die effektivste Speichertechnologie für IBM Spectrum Protect-Komponenten aus, um effiziente Serverleistung und Serveroperationen zu gewährleisten.

Speicherhardwareeinheiten haben unterschiedliche Kapazitäts- und Leistungsmerkmale, die festlegen, wie die Einheiten effizient mit IBM Spectrum Protect verwendet werden können. Die folgenden Richtlinien stellen eine allgemeine Anleitung zur Auswahl der für Ihre Lösung geeigneten Speicherhardware und Konfiguration dar.

Datenbank und aktive Protokolldatei

- Verwenden Sie eine schnelle Platte für die IBM Spectrum Protect-Datenbank und die aktive Protokolldatei, die beispielsweise die folgenden Merkmale hat:
  - Hochleistungsplatte mit 15.000 Umdrehungen pro Minute mit Fibre Channel- oder SAS-Schnittstelle
  - Solid-State-Platte (SSD)
- Trennen Sie die aktive Protokolldatei von der Datenbank, es sei denn, Sie verwenden SSD oder Flash-Hardware.
- Verwenden Sie beim Erstellen von Arrays für die Datenbank RAID-Stufe 5.

Speicherpool

- Sie können kostengünstigere und langsamere Platten für den Speicherpool verwenden.
- Der Speicherpool kann Platten für den Speicher für das Archivprotokoll und die Datenbanksicherung gemeinsam nutzen.
- Verwenden Sie RAID-Stufe 6 für Speicherpoolarrays, um bei Verwendung von Typen großer Platten Schutz vor Laufwerkdoppelfehlern hinzuzufügen.

- Planung der Speicherarrays
  Bereiten Sie die Konfiguration des Plattenspeichers vor, indem Sie die Planung für RAID-Arrays und Datenträger gemäß der Größe Ihres

IBM Spectrum Protect-Systems ausführen.

Zugehörige Verweise:
Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten

Planung für Sicherheit

Planen Sie den Schutz der Sicherheit von Systemen in der IBM Spectrum Protect-Lösung mithilfe von Steuerelementen für Zugriff und Authentifizierung und ziehen Sie das Verschlüsseln von Daten und der Übertragung von Kennwörtern in Erwägung.

- Planung für Administratorrollen
  Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.
- Planung für sichere Kommunikation
  Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.
- Planung für die Speicherung verschlüsselter Daten
  Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie für Ihre Anforderungen am besten geeignete Option aus.
- Planung des Firewallzugriffs
  Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

Planung für Administratorrollen

Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.

Sie können Administratoren eine der folgenden Berechtigungsstufen zuordnen:

Systemberechtigung
: Administratoren mit Systemberechtigung verfügen über die höchste Berechtigungsstufe. Administratoren mit dieser Berechtigungsstufe können jede Task ausführen. Sie können alle Maßnahmendomänen und Speicherpools verwalten und anderen Administratoren Berechtigung erteilen.

Maßnahmenberechtigung
: Administratoren mit Maßnahmenberechtigung können alle Tasks verwalten, die sich auf die Maßnahmenverwaltung beziehen. Diese Berechtigung kann uneingeschränkt sein oder auf bestimmte Maßnahmendomänen eingeschränkt werden.

Speicherberechtigung
: Administratoren mit Speicherberechtigung können Speicherressourcen für den Server zuordnen und steuern.

Bedienerberechtigung
: Administratoren mit Bedienerberechtigung können den sofortigen Betrieb des Servers und die Verfügbarkeit von Speichermedien wie beispielsweise Bandarchiven und -laufwerken steuern.

Die Szenarios in Tabelle 1 enthalten Beispiele, die zeigen, warum es sinnvoll ist, Administratoren für die Ausführung von Tasks unterschiedliche Berechtigungsstufen zuzuordnen:

Tabelle 1. Szenarios für Administratorrollen

Szenario	Typ der zu konfigurierenden Administrator-ID
Ein Administrator in einem kleinen Unternehmen verwaltet den Server und ist für alle Serveraktivitäten verantwortlich.	• Systemberechtigung: 1 Administrator-ID
Ein Administrator für mehrere Server verwaltet auch das gesamte System. Mehrere andere Administratoren verwalten ihre eigenen Speicherpools.	• Systemberechtigung auf allen Servern: 1 Administrator-ID für den Administrator des gesamten Systems • Speicherberechtigung für bestimmte Speicherpools: 1 Administrator-ID für jeden der anderen Administratoren
Ein Administrator verwaltet 2 Server. Eine andere Person unterstützt ihn bei den Verwaltungstasks. Zwei Assistenten müssen sicherstellen, dass wichtige Systeme gesichert werden. Jeder Assistent ist für die Überwachung der geplanten Sicherungen auf einem der IBM Spectrum Protect-Server verantwortlich.	• Systemberechtigung auf beiden Servern: 2 Administrator-IDs • Bedienerberechtigung: 2 Administrator-IDs für die Assistenten mit Zugriff auf den Server, für den die jeweilige Person verantwortlich ist.

Planung für sichere Kommunikation

Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.

Bestimmen Sie auf der Basis der Regelungen und Geschäftsanforderungen für Ihr Unternehmen, welche Stufe des Schutzes für Ihre Daten erforderlich ist.

Wenn Ihr Unternehmen ein hohes Maß an Sicherheit für Kennwörter und die Datenübertragung erfordert, planen Sie die Implementierung der sicheren Kommunikation mit dem Protokoll Transport Layer Security (TLS) oder Secure Sockets Layer (SSL).

TLS und SSL stellen sichere Kommunikation zwischen dem Server und dem Client bereit, können sich jedoch auf die Systemleistung auswirken. Um die Systemleistung zu verbessern, verwenden Sie TLS für die Authentifizierung, ohne Objektdaten zu verschlüsseln. Informationen zur Angabe, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, finden Sie in der Beschreibung der Clientoption SSL für die Client/Server-Kommunikation und der Beschreibung des Parameters UPDATE SERVER=SSL für die Kommunikation zwischen Servern. Ab Version 8.1.2 wird TLS standardmäßig für die Authentifizierung verwendet. Wenn Sie sich für die Verwendung von TLS entscheiden, um vollständige Sitzungen zu verschlüsseln, verwenden Sie das Protokoll nur für Sitzungen, für die es erforderlich ist; fügen Sie außerdem auf dem Server Prozessorressourcen hinzu, um den wachsenden Datenaustausch im Netz handhaben zu können. Sie können auch versuchsweise andere Optionen verwenden. Beispielsweise stellen einige Netzeinheiten wie Router und Switches die TLS- oder SSL-Funktion bereit.

Mithilfe von TLS und SSL können Sie einige oder alle der unterschiedlichen möglichen Kommunikationspfade schützen, beispielsweise:

- Operations Center: vom Browser zum Hub-Server; vom Hub-Server zum Peripherieserver
- Vom Client zum Server
- Vom Server zum Server: Knotenreplikation

Zugehörige Tasks:
Kommunikation schützen

Planung für die Speicherung verschlüsselter Daten

Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie für Ihre Anforderungen am besten geeignete Option aus.

Wenn Ihr Unternehmen die Verschlüsselung der Daten in Speicherpools erfordert, können Sie entweder die IBM Spectrum Protect-Verschlüsselung oder eine externe Einheit wie beispielsweise ein Band für die Verschlüsselung verwenden.

Wenn Sie IBM Spectrum Protect zum Verschlüsseln der Daten auswählen, sind zusätzliche IT-Ressourcen auf dem Client erforderlich, die sich auf die Leistung von Sicherungs- und Zurückschreibungsprozessen auswirken können.

Zugehörige Informationen:
Technote 1963635

Planung des Firewallzugriffs

Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

In Tabelle 1 sind die Ports beschrieben, die vom Server, vom Client und vom Operations Center verwendet werden.

Tabelle 1. Vom Server, Client und Operations Center verwendete Ports

Element	Standardwert	Richtung	Beschreibung
Basisport (TCPPORT)	1500	Abgehend/Eingehend	Jede Serverinstanz erfordert einen eindeutigen Port. Sie können eine alternative Portnummer angeben, anstatt den Standardwert zu verwenden. Der mit der Option TCPPORT angegebene Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen vom Client empfangsbereit. Für den Datenverkehr des Verwaltungsclients können Sie zum Festlegen von Portwerten die Optionen TCPADMINPORT und ADMINONCLIENTPORT verwenden.
Port ausschließlich für SSL (SSLTCPPORT)	Kein Standardwert	Abgehend/Eingehend	Dieser Port wird verwendet, wenn die Kommunikation am Port auf ausschließlich SSL-fähige Sitzungen beschränkt werden soll. Um sowohl die SSL-Kommunikation als auch die Nicht-SSL-Kommunikation zu unterstützen, verwenden Sie die Option TCPPORT oder TCPADMINPORT.
SMB	45	Eingehend/Abgehend	Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.
SSH	22	Eingehend/Abgehend	Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.
SMTP	25	Abgehend	Dieser Port wird zum Senden von E-Mail-Alerts vom Server verwendet.

Element	Standardwert	Richtung	Beschreibung
NDMP	Kein Standardwert	Eingehend/Abgehend	Der Server muss eine abgehende NDMP-Steuerportverbindung zu der NAS-Einheit öffnen können. Der abgehende Steuerport ist die Adresse der unteren Ebene in der Definition der Einheit zum Versetzen von Daten für die NAS-Einheit. Während einer NDMP-Zurückschreibung vom Dateiserver auf den Server muss der Server eine abgehende NDMP-Datenverbindung zu der NAS-Einheit öffnen können. Der Datenverbindungsport, der während einer Zurückschreibung verwendet wird, kann auf der NAS-Einheit konfiguriert werden. Während NDMP-Sicherungen vom Dateiserver auf den Server muss die NAS-Einheit abgehende Datenverbindungen zum Server öffnen können und der Server muss eingehende NDMP-Datenverbindungen akzeptieren können. Mithilfe der Serveroption NDMPPORTRANGE können Sie die für die Verwendung als NDMP-Datenverbindungen verfügbare Gruppe von Ports einschränken. Sie können eine Firewall für Verbindungen zu diesen Ports konfigurieren.
Replikation	Kein Standardwert	Abgehend/Eingehend	Der Port und das Protokoll für den Port für abgehende Daten für die Replikation werden mit dem Befehl DEFINE SERVER festgelegt, der zum Konfigurieren der Replikation verwendet wird. Bei den Ports für eingehende Daten für die Replikation handelt es sich um die TCP-Ports und SSL-Ports, die für den Quellenserver im Befehl DEFINE SERVER angegeben werden.
Port für Clientzeitplan	Client-Port: 1501	Abgehend	Der Client ist an dem angegebenen Port empfangsbereit und teilt die Portnummer dem Server mit. Der Server kontaktiert den Client, wenn die servergesteuerte Zeitplanung verwendet wird. Sie können eine alternative Portnummer in der Clientoptionsdatei angeben.
Lange laufende Sitzungen	Einstellung für KEEPALIVE: YES	Abgehend	Wenn die Option KEEPALIVE aktiviert ist, werden während Client/Server-Sitzungen Keepalive-Pakete gesendet, um zu verhindern, dass die Firewall-Software lange laufende inaktive Verbindungen schließt.
Operations Center	HTTPS: 11090	Eingehend	Diese Ports werden für den Web-Browser des Operations Center verwendet. Sie können eine alternative Portnummer angeben.
Port für den Clientverwal-tungsservice	Client-Port: 9028	Eingehend	Der Zugriff auf den Port für den Clientverwaltungsservice muss über das Operations Center möglich sein. Stellen Sie sicher, dass Verbindungen nicht durch Firewalls verhindert werden können. Der Clientverwaltungsservice verwendet den TCP-Port des Servers für den Clientknoten für die Authentifizierung unter Verwendung einer Verwaltungssitzung.

Implementierung einer Plattenspeicherdatenschutzlösung für mehrere Standorte

Die Plattenspeicherlösung für mehrere Standorte wird an zwei Standorten konfiguriert und verwendet Datendeduplizierung und Replikation.

Implementierungsroadmap

Die folgenden Schritte sind zum Konfigurieren einer Plattenspeicherumgebung an mehreren Standorten erforderlich.

1. Konfigurieren Sie das System.
    a. Konfigurieren Sie die Speicherhardware und Speicherarrays für Ihre Umgebungsgröße.
    b. Installieren Sie das Serverbetriebssystem.
    c. Konfigurieren Sie Multipath I/O.
    d. Erstellen Sie die Benutzer-ID für die Serverinstanz.
    e. Bereiten Sie Dateisysteme für IBM Spectrum Protect vor.
2. Installieren Sie den Server und das Operations Center.
3. Konfigurieren Sie den Server und das Operations Center.
    a. Führen Sie die Erstkonfiguration des Servers aus.
    b. Legen Sie Serveroptionen fest.
    c. Konfigurieren Sie Secure Sockets Layer für den Server und den Client.
    d. Konfigurieren Sie das Operations Center.
    e. Registrieren Sie Ihre IBM Spectrum Protect-Lizenz.

f. Konfigurieren Sie die Datendeduplizierung.
g. Definieren Sie Datenaufbewahrungsregeln für Ihr Unternehmen.
h. Definieren Sie Zeitpläne für die Serververwaltung.
i. Definieren Sie Clientzeitpläne.

4. Installieren und konfigurieren Sie Clients.
   a. Registrieren Sie Clients und ordnen Sie Clients Zeitplänen zu.
   b. Installieren und überprüfen Sie den Clientverwaltungsservice.
   c. Konfigurieren Sie das Operations Center für die Verwendung des Clientverwaltungsservice.
5. Konfigurieren Sie den zweiten Server.
   a. Konfigurieren Sie die SSL-Kommunikation zwischen dem Hub-Server und dem Peripherieserver.
   b. Fügen Sie den zweiten Server als Peripherieserver hinzu.
   c. Aktivieren Sie die Replikation.
6. Schließen Sie die Implementierung ab.

System konfigurieren

Um das System konfigurieren zu können, müssen Sie zunächst Ihre Plattenspeicherhardware und das Serversystem für IBM Spectrum Protect konfigurieren.

- Speicherhardware konfigurieren
  Um Ihre Speicherhardware zu konfigurieren, lesen Sie die allgemeine Anleitung für Plattensysteme und IBM Spectrum Protect.
- Serverbetriebssystem installieren
  Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.
- Multipath I/O konfigurieren
  Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.
- Benutzer-ID für den Server erstellen
  Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.
- Dateisysteme für den Server vorbereiten
  Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

Speicherhardware konfigurieren

Um Ihre Speicherhardware zu konfigurieren, lesen Sie die allgemeine Anleitung für Plattensysteme und IBM Spectrum Protect.

Vorgehensweise

1. Stellen Sie unter Berücksichtigung der folgenden Richtlinien eine Verbindung zwischen dem Server und den Speichereinheiten her:
   - Verwenden Sie einen Switch oder eine Direktverbindung für Fibre Channel-Verbindungen.
   - Berücksichtigen Sie die Anzahl Ports, die verbunden sind, und die erforderliche Bandbreite.
   - Berücksichtigen Sie die Anzahl Ports auf dem Server und die Anzahl Host-Ports auf dem Plattensystem, die verbunden sind.
2. Stellen Sie sicher, dass die Einheitentreiber und die Firmware für das Serversystem, die Adapter und das Betriebssystem aktuell sind und die empfohlenen Versionen haben.
3. Konfigurieren Sie Speicherarrays. Stellen Sie sicher, dass Sie entsprechend geplant haben, um die optimale Leistung zu gewährleisten. Weitere Informationen finden Sie in Planung für Speicher.
4. Stellen Sie sicher, dass das Serversystem Zugriff auf Plattendatenträger hat, die erstellt werden. Führen Sie die folgenden Schritte aus:
   a. Wenn das System mit einem Fibre Channel-Switch verbunden ist, verzonen Sie den Server, um die Platten anzuzeigen.
   b. Ordnen Sie alle Datenträger zu, um dem Plattensystem mitzuteilen, dass diesem spezifischen Server die Anzeige jeder Platte ermöglicht werden soll.

Zugehörige Tasks:
Speicher konfigurieren

Serverbetriebssystem installieren

Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.

- Installation auf AIX-Systemen
  Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.
- Installation auf Linux-Systemen
  Führen Sie die folgenden Schritte aus, um Linux x86_64 auf dem Serversystem zu installieren.
- Installation auf Windows-Systemen
  Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

Installation auf AIX-Systemen

Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.

Vorgehensweise

1. Installieren Sie AIX Version 7.1, TL4, SP2 oder höher gemäß den Anweisungen des Herstellers.
2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.
3. Öffnen Sie die Datei /etc/hosts und führen Sie die folgenden Aktionen aus:
   - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

     ```
     127.0.0.1  localhost
     ```

4. Aktivieren Sie die AIX-I/O Completion Ports (IOCP), indem Sie den folgenden Befehl eingeben:

   ```
   chdev -l iocp0 -P
   ```

   Die Olson-Zeitzonendefinition kann sich auf die Serverleistung auswirken.
5. Um die Leistung zu optimieren, ändern Sie Ihr Systemzeitzonenformat von Olson in POSIX. Verwenden Sie das folgende Befehlsformat zum Aktualisieren der Zeitzoneneinstellung:

   ```
   chtz=Ortszeitzone,Datum/Uhrzeit,Datum/Uhrzeit
   ```

   Beispielsweise würden Sie in Tucson, Arizona, wo die Mountain Standard Time gilt, den folgenden Befehl ausgeben, um das Format in das POSIX-Format zu ändern:

   ```
   chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
   ```

6. Fügen Sie in .profile des Instanzbenutzers einen Eintrag hinzu, um die folgende Umgebung festzulegen:

   ```
   export MALLOCOPTIONS=multiheap:16
   ```

7. Legen Sie fest, dass das System vollständige Anwendungskerndateien erstellen soll. Geben Sie den folgenden Befehl aus:

   ```
   chdev -l sys0 -a fullcore=true -P
   ```

8. Stellen Sie für die Kommunikation mit dem Server und dem Operations Center sicher, dass die folgenden Ports für alle Firewalls, die gegebenenfalls vorhanden sind, offen sind:
   - Öffnen Sie für die Kommunikation mit dem Server Port 1500.
   - Öffnen Sie für die sichere Kommunikation mit dem Operations Center Port 11090 auf dem Hub-Server.

   Wenn Sie nicht die Standardwerte für Ports verwenden, stellen Sie sicher, dass die verwendeten Ports offen sind.

9. Aktivieren Sie TCP-Hochleistungsverbesserungen. Geben Sie den folgenden Befehl aus:

   ```
   no -p -o rfc1323=1
   ```

10. Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, kombinieren Sie vier 10-Gb-Ethernet-Ports durch Bonding miteinander. Verwenden Sie das System Management Interface Tool (SMIT), um die Ports durch Bonding unter Verwendung von Etherchannel zu kombinieren. Beim Testen wurden die folgenden Einstellungen verwendet:

    ```
    mode             8023ad
    auto_recovery    yes             Automatische Wiederherstellung nach
                                     Übernahme aktivieren
    backup_adapter   NONE            Adapter, der beim Fehlschlagen des
                                     gesamten Kanals verwendet wird
    hash_mode        src_dst_port    Legt fest, wie der abgehende Adapter
                                     ausgewählt wird
    interval         long            Legt den Intervallwert für den IEEE-Modus
                                     802.3ad fest
    mode             8023ad          EtherChannel-Betriebsart
    netaddr          0               Mit Ping zu überprüfende Adresse
    noloss_failover  yes             Verlustfreie Übernahme nach dem Fehl-
                                     schlagen des Pingbefehls aktivieren
    num_retries      3               Anzahl Wiederholungen für Pingbefehl vor
                                     dem Fehlschlagen
    retry_time       1               Wartezeit (in Sekunden) zwischen
                                     Pingbefehlen
    use_alt_addr     no              Alternative EtherChannel-Adresse
                                     aktivieren
    use_jumbo_frame  no              Jumbo-Frames für Gigabit Ethernet
                                     aktivieren
    ```

11. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 1 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 1. Benutzergrenzwerte (ulimit-Werte)

Typ des Benutzergrenzwerts	Einstellung	Wert	Befehl zum Abfragen des Werts
Maximale Größe der erstellten Kerndateien	core	Unlimited	`ulimit -Hc`
Maximale Größe eines Datensegments für einen Prozess	data	Unlimited	`ulimit -Hd`
Maximale Dateigröße	fsize	Unlimited	`ulimit -Hf`
Maximale Anzahl offener Dateien	nofile	65536	`ulimit -Hn`
Maximale Prozessorzeit in Sekunden	cpu	Unlimited	`ulimit -Ht`
Maximale Anzahl Benutzerprozesse	nproc	16384	`ulimit -Hu`

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

Installation auf Linux-Systemen

Führen Sie die folgenden Schritte aus, um Linux x86_64 auf dem Serversystem zu installieren.

Vorbereitende Schritte

Das Betriebssystem wird auf den internen Festplatten installiert. Konfigurieren Sie die internen Festplatten für die Verwendung eines RAID 1-Hardware-Arrays. Wenn Sie beispielsweise ein kleines System konfigurieren, werden die beiden internen 300-GB-Platten in RAID 1 gespiegelt, sodass es aussieht, als würde dem Installationsprogramm des Betriebssystems eine einzelne 300-GB-Platte zur Verfügung stehen.

Vorgehensweise

1. Installieren Sie Red Hat Enterprise Linux Version 7.1 oder höher gemäß den Anweisungen des Herstellers. Fordern Sie eine bootfähige DVD an, die Red Hat Enterprise Linux Version 7.1 enthält, und starten Sie Ihr System von dieser DVD. Für Installationsoptionen siehe die folgende Anleitung. Wenn ein Element in der folgenden Liste nicht aufgeführt ist, übernehmen Sie die Standardauswahl unverändert.
   a. Wählen Sie nach dem Starten der DVD im Menü Install or upgrade an existing system (Installation oder Aktualisierung eines bestehenden Systems) aus.
   b. Wählen Sie in der Eingangsanzeige Test this media & install Red Hat Enterprise Linux 7.1 (Diese Median überprüfen & Red Hat Enterprise Linux 7.1 installieren) aus.
   c. Wählen Sie Ihre Sprache und Tastaturbelegung aus.
   d. Wählen Sie Ihren Standort aus, um die korrekte Zeitzone festzulegen.
   e. Wählen Sie Software Selection (Softwareauswahl) und in der nächsten Anzeige Server with GUI (Server mit GUI) aus.
   f. Klicken Sie auf der Installationszusammenfassungsseite auf Installation Destination (Installationsziel) und überprüfen Sie die folgenden Einträge:
      - Die lokale 300-GB-Platte ist als Installationsziel ausgewählt.
      - Unter 'Other Storage Options' (Weitere Speicheroptionen) ist Automatically configure partitioning (Partitionierung automatisch konfigurieren) ausgewählt.

      Klicken Sie auf Done (Fertig).
   g. Klicken Sie auf Begin Installation (Installation starten). Legen Sie nach dem Start der Installation das Rootkennwort für Ihr Rootbenutzerkonto fest.

   Führen Sie nach dem Abschluss der Installation einen Neustart für das System durch und melden Sie sich als Rootbenutzer an. Geben Sie den Befehl df aus, um die Basispartitionierung zu überprüfen. Auf einem Testsystem hatte die Erstpartitionierung beispielsweise das folgende Ergebnis zur Folge:

```
[root@tvapp02]# df -h
Filesystem             Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G   1% /dev/shm
tmpfs                   32G  8.8M   32G   1% /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.
   Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, sollten Sie das Bonding mehrerer Netzports in Erwägung ziehen. Erstellen Sie dazu eine LACP-Netzverbindung (LACP = Link Aggregation Control Protocol), bei der mehrere untergeordnete Ports in einer

einzigen logischen Verbindung aggregiert werden. Die bevorzugte Methode ist die Verwendung des Bondmodus 802.3ad, des Werts 100 für die Einstellung miimon und der Angabe 'layer3+4' für die Einstellung xmit_hash_policy.
Einschränkung: Um eine LACP-Netzverbindung verwenden zu können, muss ein Netzswitch vorhanden sein, der LACP unterstützt.

Weitere Anweisungen zur Konfiguration von Bonding-Netzverbindungen mit Red Hat Enterprise Linux Version 7 finden Sie unter Create a Channel Bonding Interface.

3. Öffnen Sie die Datei /etc/hosts und führen Sie die folgenden Aktionen aus:
   - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

     ```
     127.0.0.1  localhost
     ```

4. Installieren Sie Komponenten, die für die Serverinstallation erforderlich sind. Führen Sie die folgenden Schritte aus, um ein YUM-Repository (YUM = Yellowdog Updater, Modified) zu erstellen und die vorausgesetzten Pakete zu installieren.
   a. Stellen Sie die DVD für die Installation von Red Hat Enterprise Linux in einem Systemverzeichnis bereit. Um sie beispielsweise im Verzeichnis /mnt bereitzustellen, geben Sie den folgenden Befehl aus:

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

   b. Überprüfen Sie, ob die DVD bereitgestellt wurde, indem Sie den Befehl mount ausgeben. Es sollte eine ähnliche Ausgabe wie in dem folgenden Beispiel angezeigt werden:

      ```
      /dev/sr0 on /mnt type iso9660
      ```

   c. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

      ```
      cd /etc/yum/repos.d
      ```

      Wenn das Verzeichnis repos.d nicht vorhanden ist, erstellen Sie es.
   d. Listen Sie den Verzeichnisinhalt auf:

      ```
      ls rhel-source.repo
      ```

   e. Benennen Sie die ursprüngliche repo-Datei um, indem Sie den Befehl mv ausgeben. Beispiel:

      ```
      mv rhel-source.repo rhel-source.repo.orig
      ```

   f. Erstellen Sie mithilfe eines Texteditors eine neue repo-Datei. Um beispielsweise den Editor vi zu verwenden, geben Sie den folgenden Befehl aus:

      ```
      vi rhel71_dvd.repo
      ```

   g. Fügen Sie der neuen repo-Datei die folgenden Zeilen hinzu. Der Parameter baseurl gibt den Verzeichnismountpunkt an:

      ```
      [rhel71_dvd]
      name=DVD Redhat Enterprise Linux 7.1
      baseurl=file:///mnt
      enabled=1
      gpgcheck=0
      ```

   h. Installieren Sie das vorausgesetzte Paket ksh.x86_64, indem Sie den Befehl yum ausgeben. Beispiel:

      ```
      yum install ksh.x86_64
      ```

      Ausnahme: Sie müssen die Bibliotheken compat-libstdc++-33-3.2.3-69.el6.i686 und libstdc++.i686 für Red Hat Enterprise Linux Version 7.1 nicht installieren.
5. Wenn die Softwareinstallation abgeschlossen ist, können Sie die ursprünglichen YUM-Repository-Werte zurückschreiben, indem Sie die folgenden Schritte ausführen:
   a. Heben Sie die Bereitstellung der DVD für die Installation von Red Hat Enterprise Linux auf, indem Sie den folgenden Befehl ausgeben:

      ```
      unmount /mnt
      ```

   b. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

      ```
      cd /etc/yum/repos.d
      ```

   c. Benennen Sie die von Ihnen erstellte repo-Datei um:

      ```
      mv rhel71_dvd.repo rhel71_dvd.repo.orig
      ```

   d. Benennen Sie die ursprüngliche Datei wieder in den ursprünglichen Namen um:

      ```
      mv rhel-source.repo.orig rhel-source.repo
      ```

6. Bestimmen Sie, ob Änderungen an Kernelparametern erforderlich sind. Führen Sie die folgenden Schritte aus:
   a. Listen Sie mithilfe des Befehls sysctl -a die Parameterwerte auf.
   b. Analysieren Sie die Ergebnisse anhand der Richtlinien in Tabelle 1, um zu bestimmen, ob Änderungen erforderlich sind.
   c. Wenn Änderungen erforderlich sind, definieren Sie die Parameter in der Datei /etc/sysctl.conf. Die Dateiänderungen werden angewendet, wenn das System gestartet wird.

   Tipp: Passen Sie Kernelparametereinstellungen automatisch an und eliminieren Sie die Notwendigkeit manueller Aktualisierungen dieser Einstellungen. Unter Linux passt die DB2-Datenbanksoftware automatisch die Werte der Kernelparameter für die Interprozesskommunikation (IPC) an und setzt sie auf die bevorzugten Einstellungen. Weitere Informationen zu Kernelparametereinstellungen finden Sie bei Verwendung des Suchbegriffs Linux-Kernelparameter im IBM DB2 Version 11.1 Knowledge Center.

Tabelle 1. Optimale Einstellungen für Linux-Kernelparameter

Parameter	**Beschreibung**
kernel.shmmni	Die maximale Anzahl Segmente.
kernel.shmmax	Die maximale Größe eines gemeinsam genutzten Speichersegments (Byte). Dieser Parameter muss definiert werden, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird.
kernel.shmall	Die maximale Zuordnung von Seiten im gemeinsam genutzten Speicher (Seiten).
kernel.sem Für den Parameter kernel.sem gibt es vier Werte.	(SEMMSL) Die maximale Anzahl Semaphore pro Array.
	(SEMMNS) Die maximale Anzahl Semaphore pro System.
	(SEMOPM) Die maximale Anzahl Operationen pro Semaphoraufruf.
	(SEMMNI) Die maximale Anzahl Arrays.
kernel.msgmni	Die maximale Anzahl systemweiter Nachrichtenwarteschlangen.
kernel.msgmax	Die maximale Größe von Nachrichten (Byte).
kernel.msgmnb	Die standardmäßige maximale Größe der Warteschlange (Byte).
kernel.randomize_va_space	Mit dem Parameter kernel.randomize_va_space wird die Verwendung von Speicher-ASLR für den Kernel konfiguriert. Inaktivieren Sie ASLR, da ASLR Fehler der DB2-Software zur Folge haben kann. Weitere ausführliche Informationen zu Linux-ASLR und DB2 enthält die Technote 1365583.
vm.swappiness	Der Parameter vm.swappiness definiert, ob der Kernel Anwendungsspeicher aus physischem Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.
vm.overcommit_memory	Der Parameter vm.overcommit_memory hat Auswirkungen darauf, wie viel virtueller Speicher gemäß dem Kernel zugeordnet werden kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.

7. Öffnen Sie Firewall-Ports für die Kommunikation mit dem Server. Führen Sie die folgenden Schritte aus:
   a. Legen Sie die von der Netzschnittstelle verwendete Zone fest. Die Zone ist standardmäßig 'public'.
   Geben Sie den folgenden Befehl aus:

```
#  firewall-cmd --get-active-zones
public
  interfaces: ens4f0
```

   b. Um die Standardportadresse für die Kommunikation mit dem Server zu verwenden, öffnen Sie TCP/IP-Port 1500 in der Linux-Firewall.
   Geben Sie den folgenden Befehl aus:

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

   Wenn ein anderer Wert als der Standardwert verwendet werden soll, können Sie eine Zahl zwischen 1024 und 32767 angeben. Wenn ein anderer Port als der Standardport geöffnet wird, müssen Sie diesen Port bei der Ausführung des Konfigurationsscripts

angeben.

c. Wenn Sie planen, dieses System als einen Hub zu verwenden, öffnen Sie Port 11090, den Standardport für die sichere Kommunikation (HTTPS).
Geben Sie den folgenden Befehl aus:

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

d. Laden Sie die Firewalldefinitionen erneut, damit die Änderungen wirksam werden.
Geben Sie den folgenden Befehl aus:

```
firewall-cmd --reload
```

8. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 2 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 2. Benutzergrenzwerte (ulimit-Werte)

Typ des Benutzergrenzwerts	Einstellung	Wert	Befehl zum Abfragen des Werts
Maximale Größe der erstellten Kerndateien	core	Unlimited	`ulimit -Hc`
Maximale Größe eines Datensegments für einen Prozess	data	Unlimited	`ulimit -Hd`
Maximale Dateigröße	fsize	Unlimited	`ulimit -Hf`
Maximale Anzahl offener Dateien	nofile	65536	`ulimit -Hn`
Maximale Prozessorzeit in Sekunden	cpu	Unlimited	`ulimit -Ht`
Maximale Anzahl Benutzerprozesse	nproc	16384	`ulimit -Hu`

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

Installation auf Windows-Systemen

Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

Vorgehensweise

1. Installieren Sie Microsoft Windows Server 2012 R2 Standard Edition gemäß den Anweisungen des Herstellers.
2. Ändern Sie die Windows-Kontensteuerungsrichtlinien, indem Sie die folgenden Schritte ausführen.
   a. Öffnen Sie den Editor für lokale Sicherheitsrichtlinien, indem Sie secpol.msc ausführen.
   b. Klicken Sie auf Lokale Richtlinien > Sicherheitsoptionen und stellen Sie sicher, dass die folgenden Benutzerkontensteuerungsrichtlinien inaktiviert sind:
      - Administratorbestätigungsmodus für das integrierte Administratorkonto
      - Alle Administratoren im Administratorbestätigungsmodus ausführen
3. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Installationsanweisungen für das Betriebssystem.
4. Wenden Sie Windows-Updates an und aktivieren Sie Zusatzfunktionen (optionale Features), indem Sie die folgenden Schritte ausführen:
   a. Wenden Sie die neuesten Windows 2012 R2-Updates an.
   b. Installieren und aktivieren Sie das Windows 2012 R2-Feature Microsoft .NET Framework 3.5 über den Windows Server-Manager.
   c. Aktualisieren Sie, falls erforderlich, die FC- und Ethernet-HBA-Einheitentreiber mit neueren Versionen.
   d. Installieren Sie den für das verwendete Plattensystem geeigneten Multipath I/O-Treiber.
5. Öffnen Sie den TCP/IP-Standardport (1500) für die Kommunikation mit dem IBM Spectrum Protect-Server. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Sicherungsserver-Port 1500"
dir=in action=allow protocol=TCP localport=1500
```

6. Öffnen Sie auf dem Operations Center-Hub-Server den Standardport für die sichere Kommunikation (HTTPS) mit dem Operations Center. Die Portnummer ist 11090. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Operations Center-Port 11090"
dir=in action=allow protocol=TCP localport=11090
```

Multipath I/O konfigurieren

Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.

- AIX-Systeme
- Linux-Systeme
- Windows-Systeme

AIX-Systeme

Vorgehensweise

1. Bestimmen Sie die Fibre Channel-Portadresse, die für die Hostdefinition auf dem Plattensubsystem verwendet werden muss. Geben Sie den Befehl lscfg für jeden Port aus.
   - Geben Sie auf kleinen und mittelgroßen Systemen die folgenden Befehle aus:

     ```
     lscfg -vps -l fcs0 | grep "Netzadresse"
     lscfg -vps -l fcs1 | grep "Netzadresse"
     ```

   - Geben Sie auf großen Systemen die folgenden Befehle aus:

     ```
     lscfg -vps -l fcs0 | grep "Netzadresse"
     lscfg -vps -l fcs1 | grep "Netzadresse"
     lscfg -vps -l fcs2 | grep "Netzadresse"
     lscfg -vps -l fcs3 | grep "Netzadresse"
     ```

2. Stellen Sie sicher, dass die folgenden AIX-Dateigruppen installiert sind:
   - devices.common.IBM.mpio.rte
   - devices.fcp.disk.array.rte
   - devices.fcp.disk.rte
3. Geben Sie den Befehl cfgmgr aus, damit AIX die Hardware erneut überprüft und verfügbare Platten erkennt. Beispiel:

   ```
   cfgmgr
   ```

4. Um die verfügbaren Platten aufzulisten, geben Sie den folgenden Befehl aus:

   ```
   lsdev -Ccdisk
   ```

   Es sollte eine ähnliche Ausgabe wie die folgende angezeigt werden:

   ```
   hdisk0  Available 00-00-00 SAS Disk Drive
   hdisk1  Available 00-00-00 SAS Disk Drive
   hdisk2  Available 01-00-00 SAS Disk Drive
   hdisk3  Available 01-00-00 SAS Disk Drive
   hdisk4  Available 06-01-02 MPIO IBM 2076 FC Disk
   hdisk5  Available 07-01-02 MPIO IBM 2076 FC Disk
   ...
   ```

5. Verwenden Sie die Ausgabe des Befehls lsdev, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

   Beispielsweise könnte eine Einheiten-ID `hdisk4` lauten. Sichern Sie die Liste der Einheiten-IDs für die Verwendung bei der Erstellung von Dateisystemen für den IBM Spectrum Protect-Server.

6. Korrelieren Sie die SCSI-Einheiten-IDs zu bestimmten Platten-LUNs aus dem Plattensystem, indem Sie detaillierte Informationen zu allen physischen Datenträgern im System auflisten. Geben Sie den folgenden Befehl aus:

   ```
   lspv -u
   ```

   Auf einem IBM® Storwize-System werden beispielsweise die folgenden Informationen für jede Einheit angezeigt:

   ```
   hdisk4  00f8cf083fd97327  None  active
    3321360050763008101057800000000000003004214503IBMfcp
   ```

   In dem Beispiel ist *600507630081010578000000000000030* die UID für den Datenträger, die von der Storwize-Managementschnittstelle zurückgemeldet wurde.
   Um die Plattengröße in Megabyte zu überprüfen und den Wert mit dem für das System aufgelisteten Wert zu vergleichen, geben Sie den folgenden Befehl aus:

   ```
   bootinfo -s hdisk4
   ```

Linux-Systeme

Vorgehensweise

1. Editieren Sie die Datei /etc/multipath.conf, um Multipathing für Linux-Hosts zu aktivieren. Wenn die Datei multipath.conf nicht vorhanden ist, können Sie die Datei erstellen, indem Sie den folgenden Befehl ausgeben:

   ```
   mpathconf --enable
   ```

   Die folgenden Parameter wurden in multipath.conf zu Testzwecken auf einem IBM Storwize-System festgelegt:

   ```
   defaults {
               user_friendly_names no
   }

   devices {
               device {
                           vendor "IBM "
                           product "2145"
                           path_grouping_policy group_by_prio
                           user_friendly_names no
                           path_selector "round-robin 0"
                           prio "alua"
                           path_checker "tur"
                           failback "immediate"
                           no_path_retry 5
                           rr_weight uniform
                           rr_min_io_rq "1"
                           dev_loss_tmo 120
              }
   }
   ```

2. Definieren Sie die Multipath-Option so, dass Multipath zusammen mit dem System gestartet wird. Geben Sie die folgenden Befehle aus:

   ```
   systemctl enable multipathd.service
   systemctl start multipathd.service
   ```

3. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath verwaltet werden, geben Sie den folgenden Befehl aus:

   ```
   multipath -l
   ```

4. Stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheiten-ID können Sie die aufgelisteten Platten identifizieren.
   Beispielsweise zeigt die folgende Ausgabe, dass einer 2-TB-Platte zwei Pfadgruppen und vier aktive Pfade zugeordnet sind. Die Größe von 2 TB bestätigt, dass die Platte einem Pooldateisystem entspricht. Suchen Sie anhand eines Teils der langen Einheiten-ID-Nummer (in diesem Beispiel 12) in der Managementschnittstelle des Plattensystems nach dem Datenträger.

   ```
   [root@tapsrv01 code]# multipath -l
   36005076802810c509800000000000012 dm-43 IBM,2145
    size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='round-robin 0' prio=0 status=active
   | |- 2:0:1:18 sdcw 70:64   active undef running
   | `- 4:0:0:18 sdgb 131:112 active undef running
   `-+- policy='round-robin 0' prio=0 status=enabled
     |- 1:0:1:18 sdat 66:208  active undef running
     `- 3:0:0:18 sddy 128:0   active undef running
   ```

   a. Korrigieren Sie, falls erforderlich, Platten-LUN/Host-Zuordnungen und erzwingen Sie eine erneute Busüberprüfung. Beispiel:

      ```
      echo "- - -" > /sys/class/scsi_host/host0/scan
      echo "- - -" > /sys/class/scsi_host/host1/scan
      echo "- - -" > /sys/class/scsi_host/host2/scan
      ```

      Sie können für eine erneute Überprüfung der Platten-LUN/Host-Zuordnungen auch das System erneut starten.
   b. Stellen Sie sicher, dass Platten jetzt für Multipath I/O verfügbar sind, indem Sie den Befehl multipath -l erneut ausgeben.
5. Verwenden Sie die Multipath-Ausgabe, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

   Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte `36005076802810c509800000000000012`.

   Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

Windows-Systeme

Vorgehensweise

1. Stellen Sie sicher, dass Multipath I/O installiert ist. Installieren Sie, falls erforderlich, weitere anbieterspezifische Multipath-Treiber.
2. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath I/O verwaltet werden, geben Sie den folgenden Befehl aus:

   ```
   c:\Programme\IBM\SDDDSM\datapath.exe query device
   ```

3. Überprüfen Sie die Multipath-Ausgabe und stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheitenseriennummer können Sie die aufgelisteten Platten identifizieren.
   Beispielsweise können Sie anhand eines Teils der langen Einheitenseriennummer (in diesem Beispiel 34) in der Managementschnittstelle des Plattensystems nach dem Datenträger suchen. Die Größe von 2 TB bestätigt, dass die Platte einem Speicherpooldateisystem entspricht.

```
DEV#:   4  DEVICE NAME: Disk5 Part0   TYPE: 2145    POLICY: OPTIMIZED
SERIAL: 600507630081010578000000000000034          LUN SIZE: 2.0TB
============================================================================
Path#          Adapter/Hard Disk       State   Mode    Select  Errors
    0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
    1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176       0
    2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494       0
    3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
```

4. Erstellen Sie unter Verwendung der in der Multipath-Ausgabe im vorherigen Schritt zurückgegebenen Seriennummern eine Liste der Platteneinheiten-IDs.

   Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte `600507630081010578000000000000034`.

   Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

5. Um neue Platten online zu schalten und das Lesezugriffsattribut zu löschen, führen Sie diskpart.exe mit den folgenden Befehlen aus. Wiederholen Sie diesen Schritt für jede der Platten:

```
diskpart
   select Disk 1
   online disk
   attribute disk clear readonly
   select Disk 2
   online disk
   attribute disk clear readonly
   < ... >
   select Disk 49
   online disk
   attribute disk clear readonly
   exit
```

Benutzer-ID für den Server erstellen

Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.

Informationen zu diesem Vorgang

Sie können nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstreichungszeichen (_) für die Benutzer-ID angeben. Die Benutzer-ID und der Gruppenname müssen den folgenden Regeln entsprechen:

- Die Länge darf 8 Zeichen nicht überschreiten.
- Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder einer Ziffer beginnen.
- Die Benutzer-ID und der Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* oder ein in SQL reserviertes Wortes sein.

Vorgehensweise

1. Erstellen Sie mithilfe von Betriebssystembefehlen eine Benutzer-ID.
   - AIX-BetriebssystemeLinux-BetriebssystemeErstellen Sie eine Gruppe und eine Benutzer-ID im Ausgangsverzeichnis des Benutzers, der Eigner der Serverinstanz ist.

     Um beispielsweise die Benutzer-ID tsminst1 in der Gruppe tsmsrvrs mit dem Kennwort tsminst1 zu erstellen, geben Sie die folgenden Befehle mit einer ID für einen Benutzer mit Verwaltungsaufgaben aus:

     AIX-Betriebssysteme

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

     Linux-Betriebssysteme

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

     Melden Sie sich von Ihrem System ab und anschließend wieder an. Wechseln Sie zu dem von Ihnen erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, wie beispielsweise Telnet, damit Sie zur Eingabe des Kennworts aufgefordert

werden und es, falls erforderlich, ändern können.

- Windows-BetriebssystemeErstellen Sie eine Benutzer-ID und fügen Sie dann die neue ID der Gruppe 'Administratoren' hinzu. Um beispielsweise die Benutzer-ID tsminst1 zu erstellen, geben Sie den folgenden Befehl aus:

  ```
  net user tsminst1 * /add
  ```

  Fügen Sie, nachdem Sie für den neuen Benutzer ein Kennwort erstellt und bestätigt haben, die Benutzer-ID der Gruppe 'Administratoren' hinzu, indem Sie die folgenden Befehle ausgeben:

  ```
  net localgroup Administratoren tsminst1 /add
  net localgroup DB2ADMNS tsminst1 /add
  ```

2. Melden Sie die neue Benutzer-ID ab.

Dateisysteme für den Server vorbereiten

Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

- Dateisysteme auf AIX-Systemen vorbereiten
  Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.
- Dateisysteme auf Linux-Systemen vorbereiten
  Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.
- Dateisysteme auf Windows-Systemen vorbereiten
  Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

Dateisysteme auf AIX-Systemen vorbereiten

Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.

Vorgehensweise

1. Erhöhen Sie die Warteschlangenlänge und die maximale Übertragungsgröße für alle verfügbaren *hdiskX*-Platten. Geben Sie für jede Platte die folgenden Befehle aus:

   ```
   chdev -l hdisk4 -a max_transfer=0x100000
   chdev -l hdisk4 -a queue_depth=32
   chdev -l hdisk4 -a reserve_policy=no_reserve
   chdev -l hdisk4 -a algorithm=round_robin
   ```

   Sie dürfen diese Befehle nicht für interne Betriebssystemplatten, beispielsweise *hdisk0*, ausführen.
2. Erstellen Sie Datenträgergruppen für die IBM Spectrum Protect-Datenbank, die aktive Protokolldatei, das Archivprotokoll, die Datenbanksicherung und den Speicherpool. Geben Sie den Befehl mkvg unter Angabe der Einheiten-IDs für die entsprechenden zuvor ermittelten Platten aus.
   Wenn beispielsweise die Einheitennamen *hdisk4, hdisk5* und *hdisk6* Datenbankplatten entsprechen, schließen Sie diese in die Datenbankdatenträgergruppe ein.
   Systemgröße: Die folgenden Befehle basieren auf einer Konfiguration für ein mittelgroßes System. Für kleine und große Systeme müssen Sie die Syntax wie erforderlich anpassen.

   ```
   mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
   mkvg -S -y tsmactlog hdisk5
   mkvg -S -y tsmarchlog hdisk6
   mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
   mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
   ```

3. Bestimmen Sie die Namen der physischen Datenträger und die Anzahl freier physischer Partitionen, die beim Erstellen logischer Datenträger verwendet werden sollen. Geben Sie den Befehl lsvg für jede Datenträgergruppe aus, die Sie im vorherigen Schritt erstellt haben.
   Beispiel:

   ```
   lsvg -p tsmdb
   ```

   Die Ausgabe sieht ähnlich wie die folgende aus. Die Spalte *FREE PPs* gibt die freien physischen Partitionen an:

   ```
   tsmdb:
   PV_NAME   PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
   hdisk4    active     1631       1631      327..326..326..326..326
   hdisk5    active     1631       1631      327..326..326..326..326
   hdisk6    active     1631       1631      327..326..326..326..326
   ```

4. Erstellen Sie mit dem Befehl mklv logische Datenträger in jeder Datenträgergruppe. Die Datenträgergröße, die Datenträgergruppe und die Einheitennamen sind, abhängig von der Größe Ihres Systems und Variationen in Ihrer Plattenkonfiguration, unterschiedlich.
   Um beispielsweise die Datenträger für die IBM Spectrum Protect-Datenbank auf einem mittelgroßen System zu erstellen, geben Sie die folgenden Befehle aus:

   ```
   mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
   mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
   mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
   ```

5. Formatieren Sie Dateisysteme auf jedem logischen Datenträger mit dem Befehl crfs.
   Um beispielsweise die Dateisysteme für die Datenbank auf einem mittelgroßen System zu formatieren, geben Sie die folgenden Befehle aus:

   ```
   crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
   crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
   crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
   ```

6. Führen Sie für alle neu erstellten Dateisysteme einen Mount durch, indem Sie den folgenden Befehl eingeben:

   ```
   mount -a
   ```

7. Listen Sie alle Dateisysteme auf, indem Sie den Befehl df ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.
   Das folgende Beispiel der Befehlsausgabe zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

   ```
   tapsrv07> df -g /tsminst1/*
   Filesystem      GB blocks  Free     %Used   Iused   %Iused   Mounted on
   /dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
   ```

8. Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den IBM Spectrum Protect-Server hat.

Dateisysteme auf Linux-Systemen vorbereiten

Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

Vorgehensweise

1. Verwenden Sie die zuvor generierte Liste der Einheiten-IDs und geben Sie den Befehl mkfs aus, um für jede LUN-Speichereinheit ein Dateisystem zu erstellen und zu formatieren. Geben Sie die Einheiten-ID im Befehl an. Siehe die folgenden Beispiele. Formatieren Sie für die Datenbank ext4-Dateisysteme:

   ```
   mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
   ```

   Formatieren Sie für Speicherpool-LUNs xfs-Dateisysteme:

   ```
   mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
   ```

   Abhängig davon, wie viele verschiedene Einheiten vorhanden sind, können Sie den Befehl mkfs bis zu 50 Mal ausgeben.

2. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.

   Geben Sie den Befehl mkdir für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte.

   Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

   ```
   mkdir /tsminst1
   ```

   Wiederholen Sie den Befehl mkdir für jedes Dateisystem.
3. Fügen Sie in der Datei /etc/fstab für jedes Dateisystem einen Eintrag hinzu, damit für die Dateisysteme beim Serverstart automatisch ein Mount durchgeführt wird.
   Beispiel:

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
   ```

4. Führen Sie für die Dateisysteme, die der Datei /etc/fstab hinzugefügt wurden, einen Mount durch, indem Sie den Befehl mount -a ausgeben.
5. Listen Sie alle Dateisysteme auf, indem Sie den Befehl df ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.
   Das folgende Beispiel für ein IBM® Storwize-System zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem                                      Size  Used Avail Use% Mounted on
/dev/mapper/3600507630081010578000000000000003 134G  188M 132G  1%   /tsminst1/TSMalog
```

6. Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für IBM Spectrum Protect hat.

Dateisysteme auf Windows-Systemen vorbereiten

Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

Vorgehensweise

1. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.
   Geben Sie den Befehl md für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte. Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

   ```
   md c:\tsminst1
   ```

   Wiederholen Sie den Befehl md für jedes Dateisystem.
2. Erstellen Sie für jede Platten-LUN, die einem Verzeichnis unter dem Serverinstanzverzeichnis zugeordnet ist, unter Verwendung des Windows-Datenträgermanagers (Volume-Manager) einen Datenträger.

   Rufen Sie Server-Manager > Datei- und Speicherdienste auf und führen Sie die folgenden Schritte für jede Platte aus, die der im vorherigen Schritt erstellten LUN-Zuordnung entspricht:

   a. Schalten Sie die Platte online.
   b. Initialisieren Sie die Platte mit dem GPT-Basistyp, dem Standardwert.
   c. Erstellen Sie einen einfachen Datenträger, der den gesamten Speicherbereich auf der Platte belegt. Formatieren Sie das Dateisystem mit NTFS und ordnen Sie einen Kennsatz zu, der den Zweck des Datenträgers angibt, wie beispielsweise TSMfile00. Ordnen Sie den neuen Datenträger keinem Laufwerkbuchstaben zu. Ordnen Sie den Datenträger stattdessen einem Verzeichnis unter dem Instanzverzeichnis zu, wie beispielsweise C:\tsminst1\TSMfile00.
      Tipp: Legen Sie den Datenträgerkennsatz und die Bezeichnungen für Verzeichniszuordnungen auf der Basis der Größe der aufgelisteten Platte fest.
3. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Listen Sie alle Dateisysteme auf, indem Sie den Befehl mountvol ausgeben; überprüfen Sie dann die Ausgabe. Beispiel:

   ```
   \\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
     C:\tsminst1\TSMdbspace00\
   ```

4. Starten Sie nach dem Abschluss der Plattenkonfiguration das System erneut.

Nächste Schritte

Mithilfe von Windows Explorer können Sie den Umfang des freien Speicherbereichs für jeden Datenträger prüfen.

Server und das Operations Center installieren

Verwenden Sie den grafisch orientierten Assistenten von IBM® Installation Manager, um die Komponenten zu installieren.

- Installation auf AIX- und Linux-Systemen
  Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf dem ersten Serversystem.
- Installation auf Windows-Systemen
  Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf dem ersten Serversystem.

Installation auf AIX- und Linux-Systemen

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf dem ersten Serversystem.

Vorbereitende Schritte

Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.

Vorgehensweise

1. AIX-BetriebssystemeÜberprüfen Sie, ob die erforderlichen RPM-Dateien auf Ihrem System installiert sind.

Ausführliche Informationen finden Sie in Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren.

2. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042992.
3. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
4. Stellen Sie sicher, dass für das Paket die Berechtigung zur Ausführung festgelegt ist. Ändern Sie, falls erforderlich, die Dateiberechtigungen, indem Sie den folgenden Befehl ausgeben:

   ```
   chmod a+x Paketname.bin
   ```

5. Extrahieren Sie das Paket, indem Sie den folgenden Befehl ausgeben:

   ```
   ./Paketname.bin
   ```

   Dabei ist *Paketname* der Name der Downloaddatei.
6. AIX-BetriebssystemeStellen Sie sicher, dass der folgende Befehl aktiviert ist, damit die Assistenten korrekt ausgeführt werden:

   ```
   lsuser
   ```

   Standardmäßig ist der Befehl aktiviert.
7. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
8. Starten Sie den Installationsassistenten, indem Sie den folgenden Befehl ausgeben:

   ```
   ./install.sh
   ```

   Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM Installation Manager gespeichert sind.

  Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.

- Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren
  RPM-Dateien sind für den grafisch orientierten Assistenten von IBM Installation Manager erforderlich.

Zugehörige Tasks:
Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten (AIX)
Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten (Linux)

Installation auf Windows-Systemen

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf dem ersten Serversystem.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.
- Stellen Sie sicher, dass die Benutzer-ID, die während der Installation verwendet werden soll, für einen Benutzer mit der Berechtigung eines lokalen Administrators gilt.

Vorgehensweise

1. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042993.
2. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
3. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
4. Doppelklicken Sie auf die ausführbare Datei, um die Datei in das aktuelle Verzeichnis zu extrahieren.
5. Starten Sie in dem Verzeichnis, in das die Installationsdateien extrahiert wurden, den Installationsassistenten, indem Sie auf die Datei install.bat doppelklicken. Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM® Installation Manager gespeichert sind.

  Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.

Zugehörige Tasks:
Andere Methoden zum Installieren von IBM Spectrum Protect-Komponenten

Server und das Operations Center konfigurieren

Nachdem Sie die Komponenten installiert haben, führen Sie die Konfiguration für den IBM Spectrum Protect-Server und das Operations Center aus.

- Serverinstanz konfigurieren
  Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.
- Client für Sichern/Archivieren installieren
  Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.
- Optionen für den Server festlegen
  Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.
- Sichere Kommunikation mit Transport Layer Security konfigurieren
  Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.
- Operations Center konfigurieren
  Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.
- Produktlizenz registrieren
  Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.
- Datendeduplizierung konfigurieren
  Erstellen Sie einen Verzeichniscontainerspeicherpool und mindestens ein Verzeichnis für die Verwendung der Inline-Datendeduplizierung.
- Datenaufbewahrungsregeln für Ihr Unternehmen definieren
  Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datendeduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.
- Zeitpläne für Serververwaltungsaktivitäten definieren
  Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.
- Clientzeitpläne definieren
  Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

Serverinstanz konfigurieren

Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
AIX-Betriebssysteme  Linux-Betriebssysteme

- Auf dem System, auf dem IBM Spectrum Protect installiert wurde, muss der X Window System-Client vorhanden sein. Außerdem muss ein X Window System-Server auf Ihrem Desktop ausgeführt werden.
- Für das System muss das Secure Shell-Protokoll (SSH-Protokoll) aktiviert sein. Stellen Sie sicher, dass der Port auf den Standardwert 22 gesetzt ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei sshd_config im Verzeichnis /etc/ssh/ aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämonservice über die Zugriffsberechtigungen verfügt, um mithilfe des Werts *localhost* eine Verbindung zum System herstellen zu können.
- Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt hatten, unter Verwendung des SSH-Protokolls bei IBM Spectrum Protect anmelden können. Wenn Sie den Assistenten verwenden, müssen Sie diese Benutzer-ID und das Kennwort für den Zugriff auf dieses System angeben.

- Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

Windows-BetriebssystemeÜberprüfen Sie, ob der Remoteregistrierungsdienst gestartet wurde, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf Start > Verwaltung > Dienste. Wählen Sie im Fenster Dienste Remoteregistrierung aus. Wurde der Dienst nicht gestartet, klicken Sie auf Starten.
2. Stellen Sie sicher, dass die Ports 137, 139 und 445 nicht durch eine Firewall blockiert sind:
   a. Klicken Sie auf Start > Systemsteuerung > Windows-Firewall.
   b. Wählen Sie Erweiterte Einstellungen aus.
   c. Wählen Sie Eingehende Regeln aus.
   d. Wählen Sie Neue Regel aus.
   e. Erstellen Sie eine Portregel für die TCP-Ports 137, 139 und 445, um Verbindungen für Domänennetze und private Netze zu ermöglichen.
3. Konfigurieren Sie die Benutzerkontensteuerung, indem Sie auf die Optionen für die lokale Sicherheitsrichtlinie zugreifen und die folgenden Schritte ausführen.
   a. Klicken Sie auf Start > Verwaltung > Lokale Sicherheitsrichtlinie. Erweitern Sie Lokale Richtlinien > Sicherheitsoptionen.
   b. Falls noch nicht bereits aktiviert, aktivieren Sie das integrierte Administratorkonto, indem Sie Konten: Administratorkontostatus > Aktivieren > OK auswählen.
   c. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für alle Windows-Administratoren, indem Sie Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen > Inaktivieren > OK auswählen.
   d. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für das integrierte Administratorkonto, indem Sie Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto > Inaktivieren > OK auswählen.
4. Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

Informationen zu diesem Vorgang

Der Assistent kann gestoppt und erneut gestartet werden, der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

Vorgehensweise

1. Starten Sie die lokale Version des Assistenten.
   - AIX-BetriebssystemeLinux-BetriebssystemeÖffnen Sie das Programm dsmicfgx im Verzeichnis /opt/tivoli/tsm/server/bin. Dieser Assistent kann nur als Rootbenutzer ausgeführt werden.
   - Windows-BetriebssystemeKlicken Sie auf Start > Alle Programme > IBM Spectrum Protect > Konfigurationsassistent.
2. Führen Sie die Anweisungen aus, um die Konfiguration auszuführen. Verwenden Sie die während der IBM Spectrum Protect-Systemkonfiguration aufgezeichneten Informationen (siehe Arbeitsblätter zur Planung), um Verzeichnisse und Optionen im Assistenten anzugeben.

   AIX-BetriebssystemeLinux-BetriebssystemeLegen Sie im Fenster Serverinformationen fest, dass der Server automatisch unter Verwendung der Instanzbenutzer-ID gestartet werden soll, wenn das System bootet.

   Windows-BetriebssystemeMithilfe des Konfigurationsassistenten wird festgelegt, dass der Server automatisch gestartet werden soll, wenn ein Warmstart durchgeführt wird.

Client für Sichern/Archivieren installieren

Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.

Vorgehensweise

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

Optionen für den Server festlegen

Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.

Vorgehensweise

1. Wechseln Sie in das Serverinstanzverzeichnis und öffnen Sie die Datei dsmserv.opt.
2. Überprüfen Sie die Werte in der folgenden Tabelle und Ihre Serveroptionseinstellungen auf der Basis der Systemgröße.

Serveroption	Wert für kleine Systeme	Wert für mittelgroße Systeme	Wert für große Systeme
ACTIVELOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Yes	No	No
ARCHLOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad	Während der Konfiguration angegebener Verzeichnispfad
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	No	No	No
DEVCONFIG	devconf.dat	devconf.dat	devconf.dat
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	volhist.dat	volhist.dat	volhist.dat

Aktualisieren Sie, falls erforderlich, Serveroptionseinstellungen in Übereinstimmung mit den Werten in der Tabelle. Um Aktualisierungen durchzuführen, schließen Sie die Datei dsmserv.opt und definieren Sie die Optionen mit dem Befehl SETOPT in der Verwaltungsbefehlszeilenschnittstelle.
Um beispielsweise die Option IDLETIMEOUT mit 60 zu aktualisieren, geben Sie den folgenden Befehl aus:

```
setopt idletimeout 60
```

3. Um für den Server, die Clients und das Operations Center die sichere Kommunikation zu konfigurieren, überprüfen Sie die Optionen in der folgenden Tabelle.

Serveroption	Alle Systemgrößen
SSLFIPSMODE	NO
TCPPORT	Geben Sie die Nummer des Ports an, an dem der Server auf Anforderungen von TCP/IP- und SSL-fähigen Sitzungen des Clients wartet.
TCPADMINPORT	Geben Sie die Adresse des Ports an, an dem der Server auf Anforderungen von TCP/IP- und SSL-fähigen Sitzungen des Verwaltungsbefehlszeilenclients wartet.

Wenn einer der Optionswerte aktualisiert werden muss, editieren Sie die Datei dsmserv.opt unter Verwendung der folgenden Anleitungen:
   - Entfernen Sie den Stern am Anfang einer Zeile, um eine Option zu aktivieren.
   - Geben Sie in jeder Zeile nur eine einzige Option und den für die Option angegebenen Wert ein.
   - Wenn eine Option in mehreren Einträgen in der Datei vorkommt, verwendet der Server den letzten Eintrag.

Sichern Sie Ihre Änderungen und schließen Sie die Datei. Wenn Sie die Datei dsmserv.opt direkt editieren, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

Zugehörige Verweise:
Referenz für Serveroptionen
SETOPT (Serveroption für dynamische Aktualisierung definieren)

Sichere Kommunikation mit Transport Layer Security konfigurieren

Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.

Informationen zu diesem Vorgang

Ab IBM Spectrum Protect Version 8.1.2 ist SSL standardmäßig aktiviert und der IBM Spectrum Protect-Server und der Client für Sichern/Archivieren werden automatisch für die gegenseitige Kommunikation unter Verwendung des TLS 1.2-Protokolls konfiguriert.

Wie in der folgenden Abbildung gezeigt können Sie die sichere Kommunikation zwischen dem Server und dem Client für Sichern/Archivieren manuell konfigurieren, indem Sie Optionen in der Server- und der Clientoptionsdatei definieren und dann das selbst signierte Zertifikat, das auf dem Server generiert wird, an den Client übertragen. Sie können auch stattdessen ein eindeutiges Zertifikat, das von einer Zertifizierungsstelle (CA) signiert ist, anfordern und übertragen.

Weitere Informationen zum Konfigurieren des Servers und von Clients für die SSL- oder TLS-Kommunikation finden Sie in Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren.

Operations Center konfigurieren

Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.

Vorbereitende Schritte

Wenn Sie zum ersten Mal die Verbindung zum Operations Center herstellen, müssen Sie die folgenden Informationen angeben:

- Verbindungsinformationen für den Server, der als Hub-Server festgelegt werden soll
- Anmeldeberechtigungsnachweise für eine Administrator-ID, die für diesen Server definiert ist

Vorgehensweise

1. Legen Sie den Hub-Server fest. Geben Sie in einem Web-Browser die folgende Adresse ein:

   `https://Hostname:sicherer_Port/oc`

   Erläuterungen:
   - *Hostname* gibt den Namen des Computers an, auf dem das Operations Center installiert ist.
   - *Sicherer_Port* gibt die Portnummer an, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet.

   Wenn beispielsweise der Hostname tsm.storage.mylocation.com lautet und der standardmäßige sichere Port für das Operations Center (Port 11090) verwendet wird, ist die Adresse wie folgt:

   `https://tsm.storage.mylocation.com:11090/oc`

   Wenn Sie sich zum ersten Mal beim Operations Center anmelden, führt Sie ein Assistent durch eine Erstkonfiguration, um einen neuen Administrator mit Systemberechtigung auf dem Server zu konfigurieren.

2. Konfigurieren Sie die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server, indem Sie das Protokoll Secure Sockets Layer (SSL) konfigurieren.

   Führen Sie die Anweisungen in Kommunikation zwischen dem Operations Center und dem Hub-Server schützen aus.

3. Optional: Um einen täglichen E-Mail-Bericht mit einer Zusammenfassung des Systemstatus zu empfangen, konfigurieren Sie Ihre E-Mail-Einstellungen im Operations Center.

   Führen Sie die Anweisungen in Systemstatus mithilfe von E-Mail-Berichten verfolgen aus.

- Kommunikation zwischen dem Operations Center und dem Hub-Server schützen
  Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server zu ermöglichen, fügen Sie das TLS-Zertifikat des Hub-Servers der Truststore-Datei des Operations Center hinzu.

Produktlizenz registrieren

Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.

Informationen zu diesem Vorgang

Lizenzen werden in Registrierungszertifikatsdateien gespeichert, die Lizenzinformationen für das Produkt enthalten. Die Registrierungszertifikatsdateien befinden sich auf den Installationsmedien und werden während der Installation auf den Server gestellt. Wenn Sie das Produkt registrieren, werden die Lizenzen in einer NODELOCK-Datei im aktuellen Verzeichnis gespeichert.

Vorgehensweise

Registrieren Sie eine Lizenz, indem Sie den Namen der Registrierungszertifikatsdatei angeben, die die Lizenz enthält. Um den Command Builder des Operations Center für diese Task zu verwenden, führen Sie die folgenden Schritte aus.

1. Öffnen Sie das Operations Center.
2. Öffnen Sie den Command Builder des Operations Center, indem Sie den Mauszeiger über das Symbol für Einstellungen bewegen und auf Command Builder klicken.
3. Geben Sie den Befehl REGISTER LICENSE aus. Um beispielsweise eine IBM Spectrum Protect-Basislizenz zu registrieren, geben Sie den folgenden Befehl aus:

   ```
   register license file=tsmbasic.lic
   ```

Nächste Schritte

Sichern Sie die Installationsmedien, die Ihre Registrierungszertifikatsdateien enthalten. Möglicherweise müssen Sie Ihre Lizenz erneut registrieren, wenn beispielsweise eine der folgenden Bedingungen erfüllt ist:

- Der Server wird auf einen anderen Computer versetzt.
- Die NODELOCK-Datei ist beschädigt. Der Server speichert Lizenzinformationen in der NODELOCK-Datei, die sich in dem Verzeichnis befindet, von dem aus der Server gestartet wird.
- Linux-BetriebssystemeSie ändern den Prozessorchip, der dem Server zugeordnet ist, auf dem der Server installiert ist.

Zugehörige Verweise:
REGISTER LICENSE (Neue Lizenz registrieren)

Datendeduplizierung konfigurieren

Erstellen Sie einen Verzeichniscontainerspeicherpool und mindestens ein Verzeichnis für die Verwendung der Inline-Datendeduplizierung.

Vorbereitende Schritte

Verwenden Sie für diese Task die aufgezeichneten Informationen zu Speicherpoolverzeichnissen (siehe Arbeitsblätter zur Planung).

Vorgehensweise

1. Öffnen Sie das Operations Center.
2. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher.
3. Klicken Sie in der angezeigten Liste auf Speicherpools.
4. Klicken Sie auf die Schaltfläche +Speicherpool.
5. Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus:
   - Um die Inline-Datendeduplizierung verwenden zu können, wählen Sie einen Speicherpool Verzeichnis unter dem containerbasierten Speicher aus.
   - Wenn Sie Verzeichnisse für den Verzeichniscontainerspeicherpool konfigurieren, geben Sie die Verzeichnispfade an, die während der Systemkonfiguration für Speicher erstellt wurden.
6. Klicken Sie nach dem Konfigurieren des neuen Verzeichniscontainerspeicherpools auf Schließen & Maßnahmen anzeigen, um eine Verwaltungsklasse zu aktualisieren und mit der Verwendung des Speicherpools zu beginnen.

Datenaufbewahrungsregeln für Ihr Unternehmen definieren

Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datendeduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.

Vorgehensweise

1. Wählen Sie auf der Seite Services im Operations Center die Domäne STANDARD aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen. Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.
3. Klicken Sie auf die Umschaltfläche Konfigurieren und führen Sie die folgenden Änderungen durch:
   - Ändern Sie das Sicherungsziel für die Verwaltungsklasse STANDARD in den Verzeichniscontainerspeicherpool.
   - Ändern Sie den Wert für die Spalte 'Sicherungen' in Keine Begrenzung.
   - Ändern Sie den Aufbewahrungszeitraum. Setzen Sie den Wert für die Spalte 'Zusätzliche Sicherungen aufbewahren' abhängig von Ihren Geschäftsanforderungen auf 30 Tage oder mehr.
4. Sichern Sie Ihre Änderungen und klicken Sie erneut auf die Umschaltfläche Konfigurieren, damit die Maßnahmengruppe nicht mehr editierbar ist.

5. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.

Zugehörige Tasks:
Regeln zum Sichern und Archivieren von Clientdaten angeben

Zeitpläne für Serververwaltungsaktivitäten definieren

Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.

Informationen zu diesem Vorgang

Planen Sie die Ausführung von Serververwaltungsoperationen im Anschluss an Clientsicherungsoperationen. Sie können das Timing von Zeitplänen steuern, indem Sie die Startzeit in Kombination mit der Dauer für jede Operation definieren.

Das folgende Beispiel zeigt die Planung von Serververwaltungsprozessen in Kombination mit dem Clientsicherungszeitplan für eine Plattenspeicherlösung für mehrere Standorte.

Operation	**Zeitplan**
Clientsicherung	Startet um 22:00 Uhr.
Knotenreplikation	Startet um 08:00 Uhr bzw. 10 Stunden nach dem Start der Clientsicherung.
Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall	• Die Datenbanksicherung startet um 11:00 Uhr bzw. 13 Stunden nach dem Start der Clientsicherung. Dieser Prozess wird bis zum Abschluss ausgeführt. • Die Sicherung von Einheitenkonfigurationsinformationen und des Datenträgerprotokolls startet um 17:00 Uhr bzw. 6 Stunden nach dem Start der Datenbanksicherung. • Das Löschen des Datenträgerprotokolls startet um 20:00 Uhr bzw. 9 Stunden nach dem Start der Datenbanksicherung.
Bestandsverfall	Startet um 12:00 Uhr bzw. 14 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen. Dieser Prozess wird bis zum Abschluss ausgeführt.

Vorgehensweise

Erstellen Sie nach dem Konfigurieren der Einheitenklasse für die Datenbanksicherungsoperationen Zeitpläne für Datenbanksicherungsoperationen und andere erforderliche Verwaltungsoperationen mithilfe des Befehls DEFINE SCHEDULE. Abhängig von der Größe Ihrer Umgebung müssen Sie die Startzeiten für jeden Zeitplan in dem Beispiel gegebenenfalls anpassen.

1. Definieren Sie eine Einheitenklasse für die Sicherungsoperationen. Erstellen Sie beispielsweise mit dem Befehl DEFINE DEVCLASS eine Einheitenklasse mit dem Namen DBBACK_FILEDEV:

   ```
   define devclass dbback_filedev devtype=file
     directory=Datenbanksicherungsverzeichnisse
   ```

   Dabei ist *Datenbanksicherungsverzeichnisse* eine Liste der für die Datenbanksicherung erstellten Verzeichnisse.
   AIX-BetriebssystemeLinux-BetriebssystemeWenn beispielsweise vier Verzeichnisse für Datenbanksicherungen mit /tsminst1/TSMbkup00 als Startpunkt vorhanden sind, geben Sie den folgenden Befehl aus:

   ```
   define devclass dbback_filedev devtype=file
     directory=/tsminst1/TSMbkup00,
     /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
     /tsminst1/TSMbkup03"
   ```

   Windows-BetriebssystemeWenn beispielsweise vier Verzeichnisse für Datenbanksicherungen mit C:\tsminst1\TSMbkup00 als Startpunkt vorhanden sind, geben Sie den folgenden Befehl aus:

   ```
   define devclass dbback_filedev devtype=file
     directory="c:\tsminst1\TSMbkup00,
     c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
   ```

2. Legen Sie die Einheitenklasse für automatische Datenbanksicherungsoperationen fest. Geben Sie mit dem Befehl SET DBRECOVERY die im vorhergehenden Schritt erstellte Einheitenklasse an. Wenn beispielsweise die Einheitenklasse den Namen dbback_filedev hat, geben Sie den folgenden Befehl aus:

   ```
   set dbrecovery dbback_filedev
   ```

3. Erstellen Sie mithilfe des Befehls DEFINE SCHEDULE Zeitpläne für die Verwaltungsoperationen. Die folgende Tabelle enthält die erforderlichen Operationen und Beispiele der Befehle.
   Tipp: Der Zeitplan für die Replikation wird separat in einem späteren Schritt erstellt, wenn Sie die Replikation mithilfe des Operations Center konfigurieren.

Operation	**Beispielbefehl**

Operation	Beispielbefehl
Sichern der Datenbank	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DB. Wenn Sie ein kleines System konfigurieren, setzen Sie den Parameter COMPRESS auf YES. Geben Sie beispielsweise auf einem kleinen System den folgenden Befehl aus, um einen Sicherungszeitplan zu erstellen, der die neue Einheitenklasse verwendet: `define schedule DBBACKUP type=admin cmd="backup db devclass=dbback_filedev type=full numstreams=3 wait=yes compress=yes" active=yes desc="Datenbank sichern." startdate=today starttime=11:00:00 duration=45 durunits=minutes`
Sichern der Einheitenkonfigurationsinformationen	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DEVCONFIG: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Einheitenkonfigurations-datei sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Sichern des Datenträgerprotokolls	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP VOLHISTORY: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Datenträgerprotokoll sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Entfernen älterer Versionen von Datenbanksicherungen, die nicht mehr erforderlich sind	Erstellen Sie einen Zeitplan für die Ausführung des Befehls DELETE VOLHISTORY: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Alte Datenbanksicherungen entfernen." startdate=today starttime=20:00:00 duration=45 durunits=minutes`
Entfernen von Objekten, deren zulässige Aufbewahrungsdauer überschritten wurde	Erstellen Sie einen Zeitplan für die Ausführung des Befehls EXPIRE INVENTORY. Definieren Sie den Parameter RESOURCE auf der Basis der Systemgröße, die Sie konfigurieren: ◦ Kleine Systeme: 10 ◦ Mittelgroße Systeme: 30 ◦ Große Systeme: 40 Geben Sie beispielsweise auf einem mittelgroßen System den folgenden Befehl aus, um einen Zeitplan mit dem Namen EXPINVENTORY zu erstellen: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Verfallene Objekte entfernen." startdate=today starttime=12:00:00 duration=45 durunits=minutes`

Nächste Schritte

Nachdem Sie Zeitpläne für die Serververwaltungstasks erstellt haben, können Sie diese im Operations Center anzeigen, indem Sie die folgenden Schritte ausführen:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Server.
2. Klicken Sie auf Verwaltung.

Zugehörige Verweise:
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

Clientzeitpläne definieren

Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

Vorgehensweise

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Clients.
2. Klicken Sie auf Zeitpläne.
3. Klicken Sie auf +Zeitplan.

4. Führen Sie die Schritte im Assistenten Zeitplan erstellen aus. Definieren Sie auf der Basis der in Zeitpläne für Serververwaltungsaktivitäten definieren geplanten Serververwaltungsaktivitäten für Clientsicherungszeitpläne eine Startzeit von 22:00 Uhr.

Clients für Sichern/Archivieren installieren und konfigurieren

Installieren und konfigurieren Sie im Anschluss an die erfolgreiche Konfiguration Ihres IBM Spectrum Protect-Serversystems die Client-Software, um mit dem Sichern von Daten beginnen zu können.

Vorgehensweise

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

Nächste Schritte

Registrieren Sie Ihre Clients und ordnen Sie Ihre Clients Zeitplänen zu.

- Clients registrieren und Zeitplänen zuordnen
  Sie können Ihre Clients über das Operations Center mithilfe des Assistenten Client hinzufügen hinzufügen und registrieren.
- Clientverwaltungsservice installieren
  Installieren Sie den Clientverwaltungsservice für Clients für Sichern/Archivieren, die unter Linux- und Windows-Betriebssystemen ausgeführt werden. Der Clientverwaltungsservice erfasst Diagnoseinformationen zu Clients für Sichern/Archivieren und stellt die Informationen dem Operations Center für die grundlegende Überwachungsfunktion zur Verfügung.

Clients registrieren und Zeitplänen zuordnen

Sie können Ihre Clients über das Operations Center mithilfe des Assistenten Client hinzufügen hinzufügen und registrieren.

Vorbereitende Schritte

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963. Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

Vorgehensweise

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

  ```
  register node Knotenname Kennwort userid=Knotenname
  ```

  Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.
- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  a. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  b. Klicken Sie in der Tabelle 'Clients' auf + Client.
  c. Führen Sie die Schritte im Assistenten Client hinzufügen aus:
     i. Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Datendeduplizierung' das Kontrollkästchen Aktivieren aus.
     ii. Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEDUPLICATION.
     Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
     iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
     iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
     v. Klicken Sie auf Client hinzufügen.

Clientverwaltungsservice installieren

Installieren Sie den Clientverwaltungsservice für Clients für Sichern/Archivieren, die unter Linux- und Windows-Betriebssystemen ausgeführt werden. Der Clientverwaltungsservice erfasst Diagnoseinformationen zu Clients für Sichern/Archivieren und stellt die Informationen dem Operations Center für die grundlegende Überwachungsfunktion zur Verfügung.

Vorgehensweise

Installieren Sie den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren, indem Sie die folgenden Schritte ausführen:

1. Laden Sie das Installationspaket für den Clientverwaltungsservice von einer IBM® Download-Site, wie beispielsweise IBM Passport Advantage® oder IBM Fix Central, herunter. Suchen Sie nach einem ähnlichen Dateinamen wie `<Version>-IBM_Spectrum_Protect-CMS-Betriebssystem.bin`.
2. Erstellen Sie auf dem Clientsystem, das verwaltet werden soll, ein Verzeichnis und kopieren Sie das Installationspaket in dieses Verzeichnis.
3. Extrahieren Sie den Inhalt der Installationspaketdatei.
4. Führen Sie die Installationsstapeldatei in dem Verzeichnis aus, in das die Installationsdateien und die zugehörigen Dateien extrahiert wurden. Dabei handelt es sich um das in Schritt 2 erstellte Verzeichnis.
5. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen im Assistenten von IBM Installation Manager aus. Wenn IBM Installation Manager noch nicht auf dem Clientsystem installiert ist, müssen Sie sowohl IBM Installation Manager als auch die IBM Spectrum Protect-Clientverwaltungsservices auswählen.

- Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen
  Bevor Sie den Clientverwaltungsservice zum Erfassen von Diagnoseinformationen zu einem Client für Sichern/Archivieren verwenden, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist.
- Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren
  Wenn für den Clientverwaltungsservice nicht die Standardkonfiguration verwendet wurde, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

Zugehörige Tasks:
Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren

Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen

Bevor Sie den Clientverwaltungsservice zum Erfassen von Diagnoseinformationen zu einem Client für Sichern/Archivieren verwenden, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist.

Vorgehensweise

Führen Sie auf dem Clientsystem in der Befehlszeile die folgenden Befehle aus, um die Konfiguration des Clientverwaltungsservice anzuzeigen:

- Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

  ```
  Clientinstallationsverzeichnis/cms/bin/CmsConfig.sh list
  ```

  Dabei ist *Clientinstallationsverzeichnis* das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie beispielsweise bei der Standardclientinstallation den folgenden Befehl aus:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  Die Ausgabe sieht ähnlich wie die folgende aus:

  ```
  Listing CMS configuration

  server1.example.com:1500 NO_SSL HOSTNAME
  Capabilities: [LOG_QUERY]
      Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
      Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

- Geben Sie auf Windows-Clientsystemen den folgenden Befehl aus:

  ```
  Clientinstallationsverzeichnis\cms\bin\CmsConfig.bat list
  ```

  Dabei ist *Clientinstallationsverzeichnis* das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie beispielsweise bei der Standardclientinstallation den folgenden Befehl aus:

  ```
  C:\"Programme"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

Die Ausgabe sieht ähnlich wie die folgende aus:

```
Listing CMS configuration

server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
    Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

    Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
    Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

Wenn der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist, wird in der Ausgabe die Position der Fehlerprotokolldatei angezeigt.
Der Ausgabetext wird aus der folgenden Konfigurationsdatei extrahiert:

- Auf Linux-Clientsystemen:

  Clientinstallationsverzeichnis/cms/Liberty/usr/servers/cmsServer/client-configuration.xml

- Auf Windows-Clientsystemen:

  Clientinstallationsverzeichnis\cms\Liberty\usr\servers\cmsServer\client-configuration.xml

Wenn die Ausgabe keine Einträge enthält, müssen Sie die Datei client-configuration.xml konfigurieren. Anweisungen zum Konfigurieren dieser Datei finden Sie in Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren. Mit dem Befehl CmsConfig verify können Sie überprüfen, ob eine Knotendefinition in der Datei client-configuration.xml korrekt erstellt wurde.

Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren

Wenn für den Clientverwaltungsservice nicht die Standardkonfiguration verwendet wurde, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

Vorbereitende Schritte

Stellen Sie sicher, dass der Clientverwaltungsservice auf dem Clientsystem installiert und gestartet wurde. Überprüfen Sie, ob die Standardkonfiguration verwendet wird. Die Standardkonfiguration wird nicht verwendet, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Clientverwaltungsservice verwendet nicht die Standardportnummer 9028.
- Der Zugriff auf den Client für Sichern/Archivieren erfolgt nicht über dieselbe IP-Adresse wie für das Clientsystem, auf dem der Client für Sichern/Archivieren installiert ist. Eine andere IP-Adresse kann beispielsweise in den folgenden Situationen verwendet werden:
  - Das Computersystem verfügt über zwei Netzkarten. Der Client für Sichern/Archivieren ist für die Kommunikation in einem Netz konfiguriert, der Clientverwaltungsservice kommuniziert jedoch in dem anderen Netz.
  - Das Clientsystem ist mit DHCP (Dynamic Host Configuration Protocol) konfiguriert. Demzufolge wird dem Clientsystem dynamisch eine IP-Adresse zugeordnet, die während der vorherigen Operation des Clients für Sichern/Archivieren auf dem Server gespeichert wurde. Wenn das Clientsystem erneut gestartet wird, wird ihm möglicherweise eine andere IP-Adresse zugeordnet. Um sicherzustellen, dass das Operations Center das Clientsystem immer finden kann, müssen Sie einen vollständig qualifizierten Domänennamen angeben.

Vorgehensweise

Um das Operations Center für die Verwendung des Clientverwaltungsservice zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus.
2. Klicken Sie auf Details > Merkmale.
3. Geben Sie im Feld 'URL für Ferndiagnose' im Abschnitt 'Allgemein' die URL für den Clientverwaltungsservice auf dem Clientsystem an. Die Adresse muss mit `https` beginnen. In der folgenden Tabelle sind Beispiele für die URL für Ferndiagnose aufgeführt.

Typ der URL	**Beispiel**
Mit DNS-Hostname und Standardport 9028	https://server.example.com
Mit DNS-Hostname und einem anderen Port als dem Standardport	https://server.example.com:1599
Mit IP-Adresse und einem anderen Port als dem Standardport	https://192.0.2.0:1599

4. Klicken Sie auf Sichern.

Nächste Schritte

Über die Registerkarte Diagnose im Operations Center können Sie auf Clientdiagnoseinformationen, wie beispielsweise Clientprotokolldateien, zugreifen.

Zweiten Server konfigurieren

Nachdem Sie die Konfiguration für den ersten Server in Ihrem System abgeschlossen haben, konfigurieren Sie den zweiten Server.

Vorgehensweise

Führen Sie die Anweisungen in den folgenden Abschnitten aus:

1. Konfigurieren Sie einen zweiten Server, der mit dem ersten Server identisch ist, indem Sie die Anweisungen in den folgenden Abschnitten ausführen:
   a. System konfigurieren
   b. Server und das Operations Center installieren

      Da in der Plattenspeicherlösung für mehrere Standorte nur ein einziger Server als Hub-Server konfiguriert ist, müssen Sie das Operations Center nicht auf dem zweiten Server installieren. Wenn Sie die Installationspakete für die Installation auf dem zweiten Server auswählen, wählen Sie nicht das Operations Center aus.

   c. Server und das Operations Center konfigurieren

      Überspringen Sie die Tasks zum Konfigurieren des Operations Center.

   d. Clients für Sichern/Archivieren installieren und konfigurieren
2. SSL-Kommunikation zwischen dem Hub-Server und einem Peripherieserver konfigurieren
3. Zweiten Server als Peripherieserver hinzufügen
4. Replikation aktivieren

SSL-Kommunikation zwischen dem Hub-Server und einem Peripherieserver konfigurieren

Um die sichere Kommunikation zwischen dem Hub-Server und einem Peripherieserver unter Verwendung des Protokolls Transport Layer Security (TLS) zu ermöglichen, müssen Sie das Zertifikat des Peripherieservers für den Hub-Server definieren. Außerdem müssen Sie das Operations Center für die Überwachung des Peripherieservers konfigurieren.

Vorgehensweise

1. Wechseln Sie auf dem Peripherieserver in das Verzeichnis der Peripherieserverinstanz.
2. Geben Sie das erforderliche Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Peripherieservers an. Geben Sie den folgenden Befehl aus:

   ```
   gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
    -label "TSM Server SelfSigned SHA Key"
   ```

3. Überprüfen Sie die Zertifikate in der Schlüsseldatenbankdatei des Peripherieservers. Geben Sie den folgenden Befehl aus:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

4. Übertragen Sie die Datei cert256.arm des Peripherieservers sicher auf den Hub-Server.
5. Wechseln Sie auf dem Hub-Server in das Verzeichnis der Hub-Server-Instanz.
6. Definieren Sie das Zertifikat des Peripherieservers für den Hub-Server. Geben Sie im Verzeichnis der Hub-Server-Instanz den folgenden Befehl aus; dabei ist *Name_des_Peripherieservers* der Name des Peripherieservers und *cert256.arm_für_Peripherieserver* der Dateiname des Zertifikats des Peripherieservers:

   ```
   gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
    -label Name_des_Peripherieservers -file cert256.arm_für_Peripherieserver
   ```

   Der Peripherieserver erfordert nicht das Zertifikat des Hub-Servers für die Kommunikation zwischen Hub-Server und Peripherieserver. Bei anderen Serverkonfigurationen, die mithilfe der Überkreuzdefinition konfigurierte Server erfordern, ist jedoch für den Peripherieserver das Zertifikat des Hub-Servers erforderlich.
7. Starten Sie den Hub-Server und den Peripherieserver erneut.
8. Geben Sie auf dem Hub-Server den Befehl DEFINE SERVER gemäß dem folgenden Beispiel aus:

   ```
   DEFINE SERVER Name_des_Peripherieservers HLA=Adresse_des_Peripherieservers
    LLA=spoke_SSLTCPADMINPort SERVERPA=Kennwort_für_Peripherieserver
   ```

   Tipp: Standardmäßig wird die Serverkommunikation verschlüsselt, es sei denn, der Server sendet oder empfängt Objektdaten. Objektdaten werden unter Verwendung von TCP/IP gesendet und empfangen. Wenn die Objektdaten nicht verschlüsselt werden, ist die Serverleistung ähnlich wie bei der Kommunikation über eine TCP/IP-Sitzung und die Sitzung ist sicher. Um die gesamte Kommunikation mit dem angegebenen Server selbst dann zu verschlüsseln, wenn der Server Objektdaten sendet und empfängt, geben Sie den Parameter SSL=YES im Befehl DEFINE SERVER an.
9. Klicken Sie in der Menüleiste des Operations Center auf Server.

In der Tabelle auf der Seite Server hat der in Schritt 8 definierte Peripherieserver in der Regel den Status 'Nicht überwacht'. Abhängig von der Einstellung für das Statusaktualisierungsintervall wird der Peripherieserver unter Umständen nicht sofort angezeigt.

10. Klicken Sie auf den Peripherieserver, um den Eintrag hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.

Zugehörige Verweise:
DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
QUERY OPTION (Serveroptionen abfragen)

Zweiten Server als Peripherieserver hinzufügen

Nachdem Sie beide Server in Ihrer Umgebung konfiguriert haben, fügen Sie den zweiten Server dem Hub-Server als Peripherieserver hinzu.

Vorgehensweise

1. Öffnen Sie das Operations Center.
2. Klicken Sie in der Menüleiste des Operations Center auf Server.
3. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
   - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird, klicken Sie auf +Peripherieserver.
4. Führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.

Replikation aktivieren

Aktivieren Sie, um Ihre Daten zu schützen, die Knotenreplikation zusätzlich zum Schutz Ihrer Speicherpools.

Vorgehensweise

Um die Knotenreplikation für alle Clients zu aktivieren, die auf dem Quellenserver registriert sind, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Operations Center.
2. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher und klicken Sie auf Replikation.
3. Klicken Sie auf der Seite Replikation auf +Serverpaar.
4. Führen Sie die Schritte im Assistenten Serverpaar hinzufügen aus:
   - Legen Sie den Quellenserver als den ersten Server fest, der für die Plattenspeicherlösung für mehrere Standorte konfiguriert wurde. Der Zielserver ist der zweite Server.
   - Definieren Sie auf der Basis der in Zeitpläne für Serververwaltungsaktivitäten definieren geplanten Serververwaltungsaktivitäten für den Knotenreplikationszeitplan eine Startzeit von 10 Stunden nach dem Fenster zum Durchführen von Clientsicherungen.
   - Der Assistent definiert auf der Basis des Datenvolumens, das geschützt wird, und auf der Basis des geplanten Zeitpunkts der Clientreplikation Speicherpoolschutzzeitpläne für Sie.

Nächste Schritte

Wenn Sie planen, die gegenseitige Replikation zwischen zwei Standorten zu definieren, führen Sie den Assistenten Serverpaar hinzufügen erneut aus, und legen Sie den zweiten Server als Quellenserver und den ersten Server als Zielserver fest.

Implementierung abschließen

Nachdem die IBM Spectrum Protect- Lösung konfiguriert wurde und aktiv ist, testen Sie Sicherungsoperationen und konfigurieren Sie die Überwachung, um sicherzustellen, dass alles ordnungsgemäß funktioniert.

Vorgehensweise

1. Testen Sie Sicherungsoperationen, um sicherzustellen, dass Ihre Daten wie erwartet geschützt werden.
   a. Wählen Sie auf der Seite Clients im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf Sichern.
   b. Wählen Sie auf der Seite Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Datenbank sichern aus.
   c. Überprüfen Sie, ob die Sicherungsoperationen erfolgreich ohne Warnungen oder Fehlernachrichten ausgeführt wurden.
   Tipp: Sie können auch stattdessen die GUI des Clients für Sichern/Archivieren zum Sichern von Clientdaten verwenden und die Serverdatenbank sichern, indem Sie den Befehl BACKUP DB in einer Verwaltungsbefehlszeile ausgeben.
2. Konfigurieren Sie die Überwachung für Ihre Lösung, indem Sie die Anweisungen in Plattenspeicherlösung für mehrere Standorte überwachen ausführen.

Plattenspeicherlösung für mehrere Standorte überwachen

Überwachen Sie nach der Implementierung einer Plattenspeicherlösung für mehrere Standorte mit IBM Spectrum Protect die Lösung, um ihre korrekte Funktionsweise sicherzustellen. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.

Informationen zu diesem Vorgang

Die Überwachung einer Lösung erfolgt bevorzugt über die Verwendung des Operations Center, das den Gesamtsystemstatus und den detaillierten Systemstatus in einer grafischen Benutzerschnittstelle bereitstellt. Darüber hinaus können Sie das Operations Center zum Generieren eines täglichen E-Mail-Berichts mit einer Zusammenfassung des Systemstatus konfigurieren.

In einigen Fällen möchten Sie vielleicht erweiterte Überwachungstools verwenden, um bestimmte Überwachungs- oder Fehlerbehebungstasks auszuführen.

Tipp: Wenn Sie planen, Probleme bei Clients für Sichern/Archivieren unter Linux- oder Windows-Betriebssystemen zu diagnostizieren, installieren Sie IBM Spectrum Protect-Clientverwaltungsservices auf jedem Computer, auf dem ein Client für Sichern/Archivieren installiert ist. Auf diese Art und Weise können Sie sicherstellen, dass die Schaltfläche Diagnose im Operations Center zur Diagnose von Problemen bei Clients für Sichern/Archivieren verfügbar ist. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen in Clientverwaltungsservice installieren aus.

Vorgehensweise

1. Führen Sie tägliche Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für tägliche Überwachungstasks.
2. Führen Sie regelmäßige Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für regelmäßige Überwachungstasks.
3. Um zu überprüfen, ob Ihre IBM Spectrum Protect-Lösung die die Lizenzierungsanforderungen erfüllt, führen Sie die Anweisungen in Lizenzeinhaltung überprüfen aus.
4. Informationen zur Konfiguration des Operations Center zum Erstellen von E-Mail-Statusberichten finden Sie in Systemstatus mithilfe von E-Mail-Berichten verfolgen.

Nächste Schritte

Beheben Sie alle erkannten Probleme. Wenn ein Problem durch Ändern der Konfiguration Ihrer Lösung behoben werden soll, führen Sie die Anweisungen in Operationen für eine Plattenspeicherlösung für mehrere Standorte verwalten aus. Die folgenden Ressourcen sind ebenfalls verfügbar:

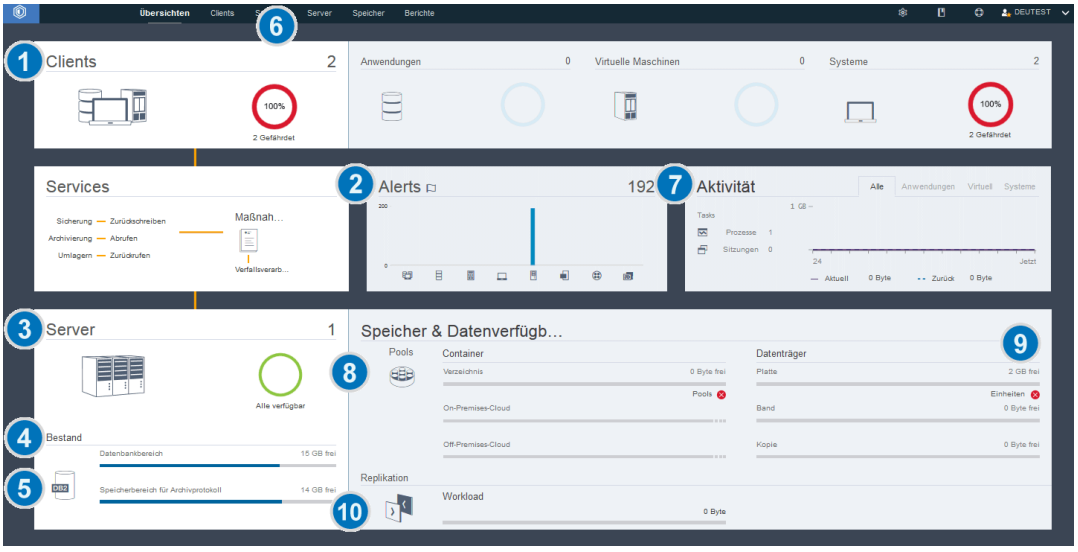
- Informationen zur Behebung von Leistungsproblemen finden Sie in Leistung.
- Informationen zur Behebung anderer Typen von Problemen finden Sie in Fehlerbehebung.

Prüfliste für tägliche Überwachungstasks

Um sicherzustellen, dass die täglichen Überwachungstasks für Ihre IBM Spectrum Protect-Lösung ausgeführt werden, überprüfen Sie die Prüfliste für tägliche Überwachungstasks.

Führen Sie die täglichen Überwachungstasks über die Seite Übersicht im Operations Center aus. Sie können auf die Seite Übersicht zugreifen, indem Sie das Operations Center öffnen und auf Übersichten klicken.

Die folgende Abbildung zeigt die Position zur Ausführung der jeweiligen Task.



Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen  und klicken Sie auf Command Builder.

In der folgenden Tabelle sind die täglichen Überwachungstasks sowie Anweisungen zur Ausführung jeder Task aufgeführt.

Tabelle 1. Tägliche Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
1 Bestimmen Sie, ob Clients vorhanden sind, bei denen die Gefahr besteht, dass sie aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen ungeschützt sind.	Um zu überprüfen, ob Clients gefährdet sind, suchen Sie nach einem Hinweis Gefährdet. Um Details anzuzeigen, klicken Sie auf den Bereich 'Clients'. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie die Clientfehler- und -planungsprotokolle anzeigen, indem Sie die folgenden Schritte ausführen: 1. Wählen Sie in der Tabelle 'Clients' den Client aus und klicken Sie auf Details. 2. Um ein Problem zu diagnostizieren, klicken Sie auf Diagnose.	Greifen Sie bei Clients, für die der Clientverwaltungsservice nicht installiert ist, auf das Clientsystem zu, um die Clientfehlerprotokolle zu überprüfen.
2 Bestimmen Sie, ob clientbezogene oder serverbezogene Fehler einen Bedienereingriff erfordern.	Um die Bewertung jedes zurückgemeldeten Alerts zu bestimmen, bewegen Sie den Mauszeiger im Bereich 'Alerts' über die Spalten.	Um zusätzliche Informationen zu Alerts anzuzeigen, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Alerts'. 2. Wählen Sie in der Tabelle 'Alerts' einen Alert aus. 3. Überprüfen Sie die Nachrichten im Fenster 'Aktivitätenprotokoll'. In dem Fenster werden zugehörige Nachrichten angezeigt, die vor und nach dem Auftreten des ausgewählten Alerts ausgegeben wurden.
3 Bestimmen Sie, ob die vom Operations Center verwalteten Server verfügbar sind, um Datenschutzservices für Clients bereitzustellen.	1. Um zu überprüfen, ob Server gefährdet sind, suchen Sie im Bereich 'Server' nach einem Hinweis Nicht verfügbar. 2. Um zusätzliche Informationen anzuzeigen, klicken Sie auf den Bereich 'Server'. 3. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.	Tipp: Wenn Sie ein Problem erkennen, das sich auf die Servermerkmale bezieht, aktualisieren Sie die Servermerkmale: 1. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details. 2. Um die Servermerkmale zu aktualisieren, klicken Sie auf Merkmale.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
4 Bestimmen Sie, ob für den Serverbestand, der aus der Serverdatenbank, der aktiven Protokolldatei und dem Archivprotokoll besteht, genügend Speicherbereich verfügbar ist.	1. Klicken Sie auf den Bereich 'Server'. 2. Zeigen Sie in der Spalte 'Status' der Tabelle den Status des Servers an und beheben Sie alle Probleme: ○ Normal Für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll ist genügend Speicherbereich verfügbar. ○ Kritisch Für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll ist nicht genügend Speicherbereich verfügbar. Sie müssen unverzüglich Speicherbereich hinzufügen; andernfalls werden die vom Server bereitgestellten Datenschutzservices unterbrochen. ○ Warnung Der Der Speicherbereich für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll wird knapp. Wenn diese Bedingung bestehen bleibt, müssen Sie Speicherbereich hinzufügen. ○ Nicht verfügbar Der Status kann nicht abgerufen werden. Stellen Sie sicher, dass der Server aktiv ist und keine Netzprobleme vorliegen. Dieser Status wird auch angezeigt, wenn die Überwachungsadministrator-ID gesperrt ist oder aus anderen Gründen auf dem Server nicht verfügbar ist. Diese ID hat den Namen IBM-OC-Name_des_Hub-Servers. ○ Nicht überwacht Nicht überwachte Server sind für den Hub-Server definiert, aber nicht für die Verwaltung durch das Operations Center konfiguriert. Um einen nicht überwachten Server zu konfigurieren, wählen Sie den Server aus und klicken Sie auf Peripherieserver überwachen.	Sie können auch auf der Seite Alerts nach zugehörigen Alerts suchen. Weitere Anweisungen zur Fehlerbehebung finden Sie in Serverprobleme beheben.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
5 Überprüfen Sie Operationen zur Sicherung der Serverdatenbank.	Um zu bestimmen, ob ein Server kürzlich gesichert wurde, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Server'. 2. Überprüfen Sie in der Tabelle 'Server' die Spalte 'Letzte Datenbanksicherung'.	Um detaillierte Informationen zu Sicherungsoperationen abzurufen, führen Sie die folgenden Schritte aus: 1. Wählen Sie in der Tabelle 'Server' eine Zeile aus und klicken Sie auf Details. 2. Bewegen Sie im Bereich 'Datenbanksicherung' den Mauszeiger über die Häkchen, um Informationen zu Sicherungsoperation zu überprüfen. Wenn eine Datenbank nicht kürzlich (beispielsweise innerhalb der letzten 24 Stunden) gesichert wurde, können Sie eine Sicherungsoperation starten: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Server'. 2. Wählen Sie in der Tabelle einen Server aus und klicken Sie auf Sichern. Um zu bestimmen, ob die Serverdatenbank für automatische Sicherungsoperationen konfiguriert ist, führen Sie die folgenden Schritte aus: 1. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Geben Sie den Befehl QUERY DB aus: `query db f=d` 3. Überprüfen Sie in der Ausgabe das Feld `Einheitenklassenname für Gesamtsicherungen`. Wenn eine Einheitenklasse angegeben ist, ist der Server für automatische Datenbanksicherungen konfiguriert.
6 Überwachen Sie andere Serververwaltungstasks. Serververwaltungstasks können die Ausführung von Zeitplänen für Verwaltungsbefehle, Verwaltungsscripts und zugehörigen Befehlen umfassen.	Um nach Informationen zu Prozessen zu suchen, die aufgrund von Serverproblemen fehlgeschlagen sind, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf Server > Verwaltung. 2. Um das zwei Wochen umfassende Verlaufsprotokoll eines Prozesses abzurufen, zeigen Sie Spalte 'History' an. 3. Um weitere Informationen zu einem geplanten Prozess abzurufen, bewegen Sie den Mauszeiger über das Kontrollkästchen, das dem Prozess zugeordnet ist.	Weitere Informationen zum Überwachen von Prozessen und Beheben von Problemen, finden Sie in der Onlinehilfe des Operations Center.
7 Überprüfen Sie, ob das Datenvolumen, das kürzlich an Server bzw. von Servern gesendet wurde, innerhalb des erwarteten Bereichs liegt.	• Um eine Übersicht über die Aktivität der letzten 24 Stunden abzurufen, zeigen Sie den Bereich 'Aktivität' an. • Um die Aktivität der letzten 24 Stunden mit der Aktivität der vorherigen 24 Stunden zu vergleichen, studieren Sie die Zahlen in den Bereichen 'Aktuell' und 'Vorherig'.	• Wenn mehr Daten als erwartet an den Server gesendet wurden, bestimmen Sie die Clients, die mehr Daten sichern und ermitteln Sie die Ursache. Möglicherweise funktioniert die clientseitige Datendeduplizierung nicht ordnungsgemäß. • Wenn weniger Daten als erwartet an den Server gesendet wurden, überprüfen Sie, ob Clientsicherungsoperationen gemäß Zeitplan ausgeführt werden.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
8 Stellen Sie sicher, dass Speicherpools zum Sichern von Clientdaten verfügbar sind.	1. Wenn im Bereich 'Speicher & Datenverfügbarkeit' Probleme angezeigt werden, klicken Sie auf Pools, um die Details anzuzeigen: ○ Wenn der Status Kritisch angezeigt wird, ist in dem Speicherpool nicht genügend Speicherbereich verfügbar oder der Speicherpool hat den Zugriffsstatus UNAVAILABLE (Nicht verfügbar). ○ Wenn der Status Warnung angezeigt wird, wird der Speicherbereich für den Speicherpool knapp oder der Speicherpool hat den Zugriffsstatus READONLY (Lesezugriff). 2. Um den verwendeten Speicherbereich, den freien Speicherbereich und den Gesamtspeicherbereich für Ihren ausgewählten Speicherpool anzuzeigen, bewegen Sie den Mauszeiger über die Einträge in der Spalte 'Verwendete Kapazität'.	Um die Speicherpoolkapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie eine Zeile in der Tabelle 'Speicherpools' aus und klicken Sie auf Details.
9 Stellen Sie sicher, dass Speichereinheiten für Sicherungsoperationen verfügbar sind.	Überprüfen Sie im Bereich 'Speicher & Datenverfügbarkeit' im Abschnitt 'Datenträger' unterhalb der Balken für die Kapazität den Status, der neben Einheiten angegeben ist. Wenn der Status Kritisch oder Warnung für eine Einheit angezeigt wird, müssen Sie das Problem untersuchen. Um Details anzuzeigen, klicken Sie auf Einheiten.	Platteneinheiten können aus den folgenden Gründen den Status 'Kritisch' oder 'Warnung' haben: • Für Einheitenklassen DISK können Datenträger offline sein oder den Zugriffsstatus READONLY (Lesezugriff) haben. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Datenträger angezeigt. • Für nicht gemeinsam genutzte Einheitenklassen FILE können Verzeichnisse offline sein. Außerdem ist unter Umständen nicht genügend freier Speicherbereich für die Zuordnung von Arbeitsdatenträgern verfügbar. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Verzeichnisse angezeigt. • Für gemeinsam genutzte Einheitenklassen FILE sind Laufwerke unter Umständen nicht verfügbar. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. In anderen Spalten der Tabelle 'Platteneinheiten' wird der Status der Laufwerke und Pfade angezeigt.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
10 Überwachen Sie Knotenreplikationsprozesse.	1. Um den Gesamtstatus der Knotenreplikationsprozesse abzurufen, zeigen Sie den Bereich 'Replikation' auf der Seite Übersicht im Operations Center an. 2. Um Informationen zu jedem replizierten Serverpaar anzuzeigen, klicken Sie auf den Bereich 'Replikation'. 3. Um das Datenvolumen, das im Laufe der letzten zwei Wochen repliziert wurde, und die Geschwindigkeit der Replikation anzuzeigen, wählen Sie ein Serverpaar aus und klicken Sie auf Details. 4. Um Replikationsinformationen für einen Client anzuzeigen, klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Studieren Sie die Informationen in der Spalte 'Replikationsworkload'.	Zeigen Sie für die erweiterte Überwachung mithilfe von Befehlen Informationen zu aktiven und beendeten Knotenreplikationsprozessen an: 1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Geben Sie den Befehl QUERY REPLICATION aus. Anweisungen finden Sie in QUERY REPLICATION (Knotenreplikationsprozesse abfragen). Wenn die Replikationsoperation erfolgreich ausgeführt wurde, stimmt der Wert für `Gesamtzahl der zu replizierenden Dateien` mit dem Wert für `Gesamtzahl der replizierten Dateien` überein. Um Nachrichten anzuzeigen, die sich auf einen Knotenreplikationsprozess auf einem Quellen- oder Zielreplikationsserver beziehen, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Server. 2. Wählen Sie den Quellen- oder Zielreplikationsserver aus und klicken Sie auf Details: ○ Um aktive Tasks anzuzeigen, klicken Sie auf Aktive Tasks, wählen die Task aus und überprüfen, ob der Status Aktiv angezeigt wird. Ausführliche Informationen enthalten die zugehörigen Aktivitätenprotokolle. ○ Um abgeschlossene Tasks anzuzeigen, klicken Sie auf Abgeschlossene Tasks, wählen die Task aus und überprüfen, ob der Status Abgeschlossen angezeigt wird. Ausführliche Informationen enthalten die zugehörigen Aktivitätenprotokolle.

Prüfliste für regelmäßige Überwachungstasks

Um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert, führen Sie die Tasks in der Prüfliste für regelmäßige Überwachungstasks aus. Planen Sie regelmäßige Tasks häufig genug, sodass Sie potenzielle Probleme erkennen können, bevor diese wirklich problematisch werden.

Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder.

Tabelle 1. Regelmäßige Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie die Systemleistung.	Bestimmen Sie den für Clientsicherungsoperationen erforderlichen Zeitraum: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Suchen Sie den Server, der dem Client zugeordnet ist. 2. Klicken Sie auf Server. Wählen Sie den Server aus und klicken Sie auf Details. 3. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die in den letzten 24 Stunden abgeschlossenen wurden, klicken Sie auf Abgeschlossene Tasks. 4. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die vor mehr als 24 Stunden abgeschlossen wurden, verwenden Sie den Befehl QUERY ACTLOG. Führen Sie die Anweisungen in QUERY ACTLOG (Aktivitätenprotokoll abfragen) aus. 5. Wenn die Dauer von Clientsicherungsoperationen zunimmt, ohne dass ein offensichtlicher Grund erkennbar ist, überprüfen Sie Ursache. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie Leistungsprobleme für den Client für Sichern/Archivieren diagnostizieren, indem Sie die folgenden Schritte ausführen: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. 2. Wählen Sie einen Client für Sichern/Archivieren aus und klicken Sie auf Details. 3. Um Clientprotokolle abzurufen, klicken Sie auf Diagnose.	Informationen zur Verkürzung der Zeit, die der Client zum Sichern von Daten auf dem Server benötigt, finden Sie in Häufig auftretende Clientleistungsprobleme lösen. Suchen Sie nach Leistungsengpässen. Anweisungen finden Sie in Leistungsengpässe identifizieren. Informationen zur Identifikation und Behebung anderer Leistungsprobleme finden Sie in Leistung.
Bestimmen Sie die Platteneinsparungen, die durch die Datendeduplizierung bereitgestellt werden.	1. Klicken Sie auf der Seite Übersicht im Operations Center auf Pools. 2. Wählen Sie einen Pool aus und klicken Sie auf Kurzübersicht. 3. Zeigen Sie im Bereich 'Datendeduplizierung' die Zeile 'Eingesparter Speicherbereich' an.	Um für die erweiterte Überwachung detaillierte Statistikdaten zu dem Datendeduplizierungsprozess für einen bestimmten Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abzurufen, führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Fordern Sie einen Statistikbericht an, indem Sie den Befehl GENERATE DEDUPSTATS ausgeben. Führen Sie die Anweisungen in GENERATE DEDUPSTATS (Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool generieren) aus. 3. Zeigen Sie den Statistikbericht an, indem Sie den Befehl QUERY DEDUPSTATS ausgeben. Führen Sie die Anweisungen in QUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen) aus.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Stellen Sie sicher, dass aktuelle Sicherungsdateien für Einheitenkonfigurations- und Datenträgerprotokolldaten gesichert werden.	Greifen Sie auf Ihre Speicherpositionen zu, um sicherzustellen, dass die Dateien verfügbar sind. Die bevorzugte Methode ist die Sicherung der Dateien an zwei Positionen.
	Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, führen Sie die folgenden Schritte aus:
	1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.
	2. Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, geben Sie die folgenden Befehle aus:
	`query option volhistory`
	`query option devconfig`
	3. Überprüfen Sie in der Ausgabe die Spalte 'Optionseinstellung', um die Dateipositionen zu finden.
	Wenn ein Katastrophenfall eintritt, sind sowohl die Protokolldatei für Datenträger als auch die Einheitenkonfigurationsdatei für die Zurückschreibung der Serverdatenbank erforderlich.	

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Bestimmen Sie, ob für das Instanzverzeichnisdateisystem genügend Speicherbereich verfügbar ist.	Stellen Sie sicher, dass im Instanzverzeichnisdateisystem mindestens 20 % freier Speicherbereich verfügbar ist. Führen Sie die für Ihr Betriebssystem zutreffende Aktion aus:
	• AIX-BetriebssystemeUm den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -g Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Linux-BetriebssystemeUm den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -h Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Windows-BetriebssystemeKlicken Sie in Windows-Explorer mit der rechten Maustaste auf das Dateisystem und klicken Sie auf Eigenschaften. Zeigen Sie die Kapazitätsdaten an.
	Die bevorzugte Position des Instanzverzeichnisses ist von dem Betriebssystem abhängig, unter dem der Server installiert ist:
	• AIX-Betriebssysteme Linux-Betriebssysteme /home/tsminst1/tsminst1
	• Windows-Betriebssysteme C:\tsminst1
	Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.	

Ermitteln Sie nicht erwartete Clientaktivität.	Um im Rahmen der Überwachung der Clientaktivität zu bestimmen, ob das Datenvolumen das erwartete Volumen überschreitet, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Clients'. 2. Um die Aktivität der vergangen zwei Wochen anzuzeigen, doppelklicken Sie auf einen beliebigen Client. 3. Um die Anzahl Byte anzuzeigen, die an den Client gesendet wurden, klicken Sie auf die Registerkarte Merkmale. 4. Zeigen Sie im Bereich 'Letzte Sitzung' die Zeile 'An Client gesendet' an.	Wenn Sie auf einen Client in der Tabelle 'Clients' doppelklicken, wird im Bereich Aktivität im Lauf von 2 Wochen das Datenvolumen angezeigt, das vom Client jeden Tag an den Server gesendet wurde.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie das Speicherpoolwachstum im Laufe der Zeit.	1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Pools'. 2. Um die Kapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie einen Pool aus und klicken Sie auf Details.	Tipps: • Um die Zeit anzugeben, die verstreichen muss, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool oder einem Cloud-Containerspeicherpool entfernt werden, nachdem sie nicht mehr vom Bestand referenziert werden, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus. 2. Klicken Sie auf Details > Merkmale. 3. Geben Sie im Feld `Verzögerungszeitraum für Containerwiederverwendung` den Zeitraum an. • Bestimmen Sie die Datendeduplizierungsleistung für Verzeichniscontainer- und Cloud-Containerspeicherpools mithilfe des Befehls GENERATE DEDUPSTATS. • Um Deduplizierungsstatistikdaten für einen Speicherpool anzuzeigen, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus. 2. Klicken Sie auf Details > Merkmale. Verwenden Sie dementsprechend den Befehl QUERY EXTENTUPDATES, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainer- oder Cloud-Containerspeicherpools anzuzeigen. Anhand der Befehlsausgabe können Sie die Datenbereiche bestimmen, die nicht mehr referenziert werden, sowie die Datenbereiche, die zum Löschen vom System auswählbar sind. Überwachen Sie in der Ausgabe die Anzahl Datenbereiche, die zum Löschen vom System auswählbar sind. Diese Messgröße steht in direkten Zusammenhang mit dem Umfang des freien Speicherbereichs in dem Containerspeicherpool. • Um den Umfang des physischen Speicherbereichs anzuzeigen, der von einem Dateibereich nach dem Entfernen der Datendeduplizierungseinsparungen belegt wird, verwenden Sie den Befehl select * from occupancy. Die Befehlsausgabe umfasst den Wert für LOGICAL_MB. LOGICAL_MB gibt an, wie viel Speicherbereich von diesem Dateibereich belegt wird.
Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass die Start- und Endzeiten von Clientzeitplänen Ihre Geschäftsanforderungen erfüllen.	Klicken Sie auf der Seite Übersicht im Operations Center auf Clients > Zeitpläne. In der Tabelle 'Zeitpläne' wird in der Spalte 'Start' die konfigurierte Startzeit für die geplante Operation angezeigt. Um anzuzeigen, wann die letzte Operation gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	Tipp: Wenn die Ausführung einer Clientoperation länger als erwartet dauert, empfangen Sie unter Umständen eine Warnung. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite 'Übersicht' im Operations Center den Mauszeiger über Clients und klicken Sie auf Zeitpläne. 2. Wählen Sie einen Zeitplan aus und klicken Sie auf Details. 3. Zeigen Sie die Details eines Zeitplans an, indem Sie auf den blauen Pfeil neben der Zeile klicken. 4. Geben Sie im Feld Ausführungszeitalert die Uhrzeit an, zu der eine Warnung ausgegeben wird, wenn die geplante Operation nicht ausgeführt wird. 5. Klicken Sie auf Sichern.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass die Start- und Endzeiten von Verwaltungstasks Ihre Geschäftsanforderungen erfüllen.	Klicken Sie auf der Seite Übersicht im Operations Center auf Server > Verwaltung. Überprüfen Sie in der Tabelle 'Verwaltung' die Informationen in der Spalte 'Letzte Ausführungsdauer'. Um anzuzeigen, wann die letzte Verwaltungstask gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	Tipp: Wenn die Ausführung einer Verwaltungstask zu lange dauert, ändern Sie die Startzeit oder die maximale Ausführungszeit. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Um die Startzeit oder die maximale Ausführungszeit für eine Task zu ändern, geben Sie den Befehl UPDATE SCHEDULE aus. Anweisungen finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).

Zugehörige Verweise:
QUERY ACTLOG (Aktivitätenprotokoll abfragen)
UPDATE STGPOOL (Speicherpool aktualisieren)
QUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)

Lizenzeinhaltung überprüfen

Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen. Planen Sie anhand dieser Informationen den weiteren Kauf von Lizenzen.

Informationen zu diesem Vorgang

Die Methode zur Überprüfung der Einhaltung der Lizenzbedingungen durch Ihre Lösung variiert abhängig von den Bedingungen Ihrer IBM Spectrum Protect-Lizenzvereinbarung.

Front-End-Kapazitätslizenzierung
: Das Front-End-Modell bestimmt die Lizenzvoraussetzungen auf der Basis des zurückgemeldeten Volumens an primären Daten, das von Clients gesichert wird. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme.

Back-End-Kapazitätslizenzierung
: Das Back-End-Modell bestimmt Lizenzvoraussetzungen auf der Basis der Terabyte Daten, die in primären Speicherpools und Repositorys gespeichert werden.
Tipps:

- Um die Genauigkeit von Schätzungen der Front-End- und Back-End-Kapazität zu gewährleisten, installieren Sie die neueste Version der Client-Software auf jedem Clientknoten.
- Die Informationen zur Front-End- und Back-End-Kapazität im Operations Center dienen zum Zweck der Planung und Schätzung.

PVU-Lizenzierung
: Das PVU-Modell basiert auf der Nutzung von PVUs durch Servereinheiten.
Wichtig: Die von IBM Spectrum Protect bereitgestellten PVU-Berechnungen werden als Schätzungen betrachtet und sind nicht rechtsverbindlich. Die von IBM Spectrum Protect zurückgemeldeten PVU-Lizenzinformationen werden nicht als zulässiger Ersatz für das IBM® License Metric Tool angesehen.

Die neuesten Informationen zu Lizenzierungsmodellen finden Sie in den Informationen zu Produktdetails und Lizenzen auf der Website der IBM Spectrum Protect-Produktfamilie. Wenden Sie sich bei Fragen oder Problemstellungen zu Lizenzierungsanforderungen an Ihren IBM Spectrum Protect-Software-Provider.

Vorgehensweise

Führen Sie zur Überwachung der Lizenzeinhaltung die Schritte aus, die den Bedingungen Ihrer Lizenzvereinbarung entsprechen.
Tipp: Das Operations Center stellt einen E-Mail-Bericht bereit, in dem die Front-End- und Back-End-Kapazitätsnutzung zusammengefasst sind. Berichte können automatisch regelmäßig an einen oder mehrere Empfänger gesendet werden. Klicken Sie für die Konfiguration und Verwaltung von E-Mail-Berichten in der Menüleiste des Operations Center auf Berichte.

Option	Bezeichnung

Option	Bezeichnung
Front-End-Modell	a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen und klicken Sie auf Lizenzierung. Die Schätzung der Front-End-Kapazität wird auf der Seite 'Front-End-Nutzung' angezeigt. b. Wenn in der Spalte 'Keine Zurückmeldung' ein Wert angezeigt wird, klicken Sie auf die Zahl, um Clients zu identifizieren, von denen keine Kapazitätsnutzung zurückgemeldet wurde. c. Um die Kapazität für Clients zu schätzen, für die keine Kapazitätsnutzung zurückgemeldet wurde, rufen Sie die folgende FTP-Site auf, auf der Tools und Anweisungen zum Messen der Kapazität bereitgestellt werden: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Um die Front-End-Kapazität mithilfe eines Scripts zu messen, führen Sie die Anweisungen im aktuellen Lizenzierungshandbuch aus. d. Addieren Sie den Operations Center-Schätzwert und alle Schätzwerte, die Sie mithilfe eines Scripts ermittelt haben. e. Überprüfen Sie, ob die geschätzte Kapazität die Bedingungen Ihrer Lizenzvereinbarung einhält.
Back-End-Modell	Einschränkung: Wenn der Quellen- und der Zielreplikationsserver nicht dieselben Maßnahmeneinstellungen verwenden, können Sie das Operations Center nicht zur Überwachung der Back-End-Kapazitätsnutzung für replizierte Clients verwenden. Informationen zur Schätzung der Kapazitätsnutzung für diese Clients finden Sie in Technote 1656476. a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen und klicken Sie auf Lizenzierung. b. Klicken Sie auf die Registerkarte Back-End. c. Überprüfen Sie, ob das geschätzte Datenvolumen die Bedingungen Ihrer Lizenzvereinbarung einhält.
PVU-Modell	Informationen zur Vorgehensweise beim Prüfen der Einhaltung der PVU-Lizenzbedingungen finden Sie in Einhaltung des PVU-Lizenzierungsmodells prüfen.

Systemstatus mithilfe von E-Mail-Berichten verfolgen

Konfigurieren Sie das Operations Center für die Generierung von E-Mail-Berichten zur Zusammenfassung des Systemstatus. Sie können eine Mail-Server-Verbindung konfigurieren, Berichtseinstellungen ändern und wahlweise angepasste SQL-Berichte erstellen.

Vorbereitende Schritte

Bevor Sie E-Mail-Berichte konfigurieren, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Es ist ein SMTP-Host-Server (SMTP = Simple Mail Transfer Protocol) verfügbar, um Berichte als E-Mail senden und empfangen zu können. Der SMTP-Server muss als offenes Mail-Relay konfiguriert sein. Außerdem müssen Sie sicherstellen, dass der IBM Spectrum Protect-Server, der E-Mail-Nachrichten sendet, Zugriff auf den SMTP-Server hat. Wenn das Operations Center auf einem anderen Computer installiert ist, ist für diesen Computer kein Zugriff auf den SMTP-Server erforderlich.
- Um E-Mail-Berichte konfigurieren zu können, müssen Sie über Systemberechtigung für den Server verfügen.
- Um die Empfänger anzugeben, können Sie eine oder mehrere E-Mail-Adressen oder Administrator-IDs eingeben. Wenn eine Administrator-ID eingegeben werden soll, muss die ID auf dem Hub-Server registriert sein und der ID muss eine E-Mail-Adresse zugeordnet sein. Eine E-Mail-Adresse für einen Administrator können Sie mithilfe des Parameters EMAILADDRESS im Befehl UPDATE ADMIN angeben.

Informationen zu diesem Vorgang

Sie können das Operations Center zum Senden eines Berichts über allgemeine Operationen, eines Lizenzeinhaltungsberichts und eines oder mehrerer angepasster Berichte, die SQL-Anweisungen SELECT zum Abfragen verwalteter Server verwenden, konfigurieren.

Vorgehensweise

Um E-Mail-Berichte zu konfigurieren und zu verwalten, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Berichte.
2. Wenn noch keine E-Mail-Server-Verbindung konfiguriert ist, klicken Sie auf Mail-Server konfigurieren und füllen Sie die Felder aus. Nach der Konfiguration des Mail-Servers sind der Bericht über allgemeine Operationen und der Lizenzeinhaltungsbericht aktiviert.
3. Um Berichtseinstellungen zu ändern, wählen Sie einen Bericht aus, klicken Sie auf Details und aktualisieren Sie das Formular.
4. Optional: Um einen angepassten SQL-Bericht hinzuzufügen, klicken Sie auf + Bericht und füllen Sie die Felder aus.

Tipp: Um einen Bericht sofort auszuführen und zu senden, wählen Sie den Bericht aus und klicken Sie auf Senden.

Ergebnisse

Aktivierte Berichte werden gemäß den angegebenen Einstellungen gesendet.
Zugehörige Verweise:
UPDATE ADMIN (Administrator aktualisieren)

Operationen für eine Plattenspeicherlösung für mehrere Standorte verwalten

Verwenden Sie diese Informationen, um Operationen für eine Plattenspeicherlösung für mehrere Standorte mit IBM Spectrum Protect zu verwalten, die einen Server umfasst und Datendeduplizierung für mehrere Standorte verwendet.

- Operations Center verwalten
  Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.
- Anwendungen, virtuelle Maschinen und Systeme schützen
  Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherungszeitplan zum Schützen der Clientdaten auswählen.
- Datenspeicher verwalten
  Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.
- Replikation verwalten
  Verwenden Sie die Replikation für die Wiederherstellen von Daten an einem Standort zur Wiederherstellung nach einem Katastrophenfall und zur Beibehaltung desselben Stands von Dateien auf dem Quellenserver und dem Zielserver. Sie können die Replikation auf Knotenebene verwalten. Sie können Daten auch auf Speicherpoolebene schützen.
- Server schützen
  Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.
- Server stoppen und starten
  Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.
- Durchführung eines Upgrades für den Server planen
  Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.
- Vorbereitungen für einen Ausfall oder eine Systemaktualisierung
  Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.
- Plan zur Wiederherstellung nach einem Katastrophenfall implementieren
  Implementieren Sie eine Strategie zur Wiederherstellung nach einem Katastrophenfall, um Ihre Anwendungen in einem Katastrophenfall wiederherstellen und hohe Serververfügbarkeit sicherstellen zu können.
- Wiederherstellung nach einem Datenverlust oder Systemausfall
  Mithilfe von IBM Spectrum Protect können Sie Daten wiederherstellen, die bei einem Katastrophenfall oder Systemausfall verloren gegangen sind. Sie können Verzeichniscontainerspeicherpools, Clientdaten und Datenbanken wiederherstellen.

Operations Center verwalten

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.

- Peripherieserver hinzufügen und entfernen
  In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.
- Web-Server starten und stoppen
  Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Assistenten für die Erstkonfiguration erneut starten
  Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Hub-Server ändern
  Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.
- Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben
  Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten

Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

Peripherieserver hinzufügen und entfernen

In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.

Informationen zu diesem Vorgang

Die Peripherieserver senden Alerts und Statusinformationen an den Hub-Server. Das Operations Center zeigt eine konsolidierte Sicht der Alerts und Statusinformationen für den Hub-Server und alle Peripherieserver.

- Peripherieserver hinzufügen
  Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.
- Peripherieserver entfernen
  Sie können einen Peripherieserver aus dem Operations Center entfernen.

Peripherieserver hinzufügen

Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.

Vorbereitende Schritte

Die Kommunikation zwischen dem Peripherieserver und dem Hub-Server muss unter Verwendung des Protokolls Transport Layer Security (TLS) geschützt werden. Um die Kommunikation zu schützen, fügen Sie das Zertifikat des Peripherieservers der Truststore-Datei des Hub-Servers hinzu.

Vorgehensweise

1. Klicken Sie in der Menüleiste des Operations Center auf Server. Die Seite Server wird geöffnet.

   In der Tabelle auf der Seite Server könnte ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass - obwohl ein Administrator diesen Server mit dem Befehl DEFINE SERVER für den Hub-Server definiert hat - der Server noch nicht als Peripherieserver konfiguriert ist.

2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
   - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird und die sichere SSL-/TLS-Kommunikation nicht erforderlich ist, klicken Sie in der Menüleiste der Tabelle auf +Peripherieserver.
3. Geben Sie die erforderlichen Informationen an und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.
   Tipp: Wenn der Aufbewahrungszeitraum für Ereignissätze des Servers weniger als 14 Tage beträgt, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

Peripherieserver entfernen

Sie können einen Peripherieserver aus dem Operations Center entfernen.

Informationen zu diesem Vorgang

Unter Umständen müssen Sie einen Peripherieserver in den folgenden Situationen entfernen:

- Der Peripherieserver soll von einem Hub-Server auf einen anderen Hub-Server versetzt werden.
- Der Peripherieserver soll stillgelegt werden.

Vorgehensweise

Um den Peripherieserver aus der Gruppe der Server zu entfernen, die vom Hub-Server verwaltet werden, führen Sie die folgenden Schritte aus:

1. Geben Sie in der IBM Spectrum Protect-Befehlszeile auf dem Hub-Server den folgenden Befehl aus:

   ```
   QUERY MONITORSETTINGS
   ```

2. Kopieren Sie in der Ausgabe des Befehls den Namen im Feld Überwachte Gruppe.
3. Geben Sie auf dem Hub-Server den folgenden Befehl aus; dabei ist *Gruppenname* der Name der überwachten Gruppe und *Mitgliedsname* der Name des Peripherieservers:

```
DELETE GRPMEMBER Gruppenname Mitgliedsname
```

4. Optional: Wenn der Peripherieserver von einem Hub-Server auf einen anderen Hub-Server versetzt werden soll, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Alertausgabe und Überwachung auf dem Peripherieserver inaktivieren, indem Sie auf dem Peripherieserver die folgenden Befehle ausgeben:

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. Optional: Wenn die Definition des Peripherieservers für andere Zwecke verwendet wird, wie beispielsweise unternehmensweite Konfiguration, Befehlsweiterleitung, Speichern virtueller Datenträger oder Speicherarchivverwaltung, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Definition des Peripherieservers auf dem Hub-Server löschen, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

   ```
   DELETE SERVER Name_des_Peripherieservers
   ```

Web-Server starten und stoppen

Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.

Vorgehensweise

1. Stoppen Sie den Web-Server.
   - AIX-BetriebssystemeGeben Sie im Verzeichnis /*Installationsverzeichnis*/ui/utils (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:

     ```
     ./stopserver.sh
     ```

   - Linux-BetriebssystemeGeben Sie den folgenden Befehl aus:

     ```
     service opscenter.rc stop
     ```

   - Windows-BetriebssystemeStoppen Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.
2. Starten Sie den Web-Server.
   - AIX-BetriebssystemeGeben Sie im Verzeichnis /*Installationsverzeichnis*/ui/utils (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:

     ```
     ./startserver.sh
     ```

   - Linux-BetriebssystemeGeben Sie die folgenden Befehle aus:

     Starten Sie den Server:

     ```
     service opscenter.rc start
     ```

     Starten Sie den Server erneut:

     ```
     service opscenter.rc restart
     ```

     Bestimmen Sie, ob der Server aktiv ist:

     ```
     service opscenter.rc status
     ```

   - Windows-BetriebssystemeStarten Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.

Assistenten für die Erstkonfiguration erneut starten

Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.

Vorbereitende Schritte

Um die folgenden Einstellungen zu ändern, verwenden Sie die Seite Einstellungen im Operations Center, anstatt den Assistenten für die Erstkonfiguration erneut zu starten:

- Häufigkeit, mit der Statusdaten aktualisiert werden
- Dauer, die Alerts aktiv, inaktiv oder geschlossen bleiben
- Bedingungen, die angeben, dass Clients gefährdet sind

Die Hilfe des Operations Center enthält weitere Informationen zum Ändern dieser Einstellungen.

Informationen zu diesem Vorgang

Um den Assistenten für die Erstkonfiguration erneut zu starten, müssen Sie eine Merkmaldatei löschen, die Informationen zur Hub-Server-Verbindung enthält. Alle für den Hub-Server konfigurierten Einstellungen für Alertausgabe, Überwachung oder Gefährdung bzw. serverübergreifenden Einstellungen werden nicht gelöscht. Diese Einstellungen werden als Standardeinstellungen im Konfigurationsassistenten verwendet, wenn der Assistent erneut gestartet wird.

Vorgehensweise

1. Stoppen Sie den Web-Server des Operations Center.
2. Wechseln Sie auf dem Computer, auf dem das Operations Center installiert ist, in das folgende Verzeichnis (dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist):
   - AIX-Betriebssysteme Linux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

   Beispiel:
   - AIX-Betriebssysteme Linux-Betriebssysteme/opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssysteme:\Programme\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. Löschen Sie im Verzeichnis guiServer die Datei serverConnection.properties.
4. Starten Sie den Web-Server des Operations Center.
5. Öffnen Sie das Operations Center.
6. Rekonfigurieren Sie mithilfe des Konfigurationsassistenten das Operations Center. Geben Sie ein neues Kennwort für die Überwachungsadministrator-ID an.
7. Aktualisieren auf jedem Peripherieserver, der bereits zuvor mit dem Hub-Server verbunden war, das Kennwort für die Überwachungsadministrator-ID, indem Sie den folgenden Befehl in der IBM Spectrum Protect-Befehlszeilenschnittstelle ausgeben:

   ```
   UPDATE ADMIN IBM-OC-Name_des_Hub-Servers neues_Kennwort
   ```

   Einschränkung: Übernehmen Sie alle anderen Einstellungen für diese Administrator-ID unverändert. Nachdem Sie das Anfangskennwort angegeben haben, wird dieses Kennwort automatisch vom Operations Center verwaltet.

Hub-Server ändern

Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.

Vorgehensweise

1. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut. Im Rahmen dieser Prozedur löschen Sie die bestehende Hub-Server-Verbindung.
2. Verwenden Sie den Assistenten, um das Operations Center für die Verbindung zu dem neuen Hub-Server zu konfigurieren.

Zugehörige Tasks:
Assistenten für die Erstkonfiguration erneut starten

Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben

Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

Vorgehensweise

Um die Konfiguration zurückzuschreiben, führen Sie die folgenden Schritte aus:

1. Stoppen Sie den Web-Server des Operations Center.
2. Dekonfigurieren Sie den Hub-Server, indem Sie die folgenden Schritte ausführen:
   a. Geben Sie auf dem Hub-Server die folgenden Befehle aus:

      ```
      SET MONITORINGADMIN ""
      SET MONITOREDSERVERGROUP ""
      SET STATUSMONITOR OFF
      SET ALERTMONITOR OFF
      REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
      ```

      Tipp: `IBM-OC-Name_des_Hub-Servers` ist die Überwachungsadministrator-ID, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.
   b. Setzen Sie das Kennwort für den Hub-Server zurück, indem Sie den folgenden Befehl auf dem Hub-Server ausgeben:

      ```
      SET SERVERPASSWORD ""
      ```

      Achtung: Führen Sie diesen Schritt nicht aus, wenn der Hub-Server für andere Server für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation konfiguriert ist.
3. Dekonfigurieren Sie alle Peripherieserver, indem Sie die folgenden Schritte ausführen:

a. Um zu bestimmen, ob noch Peripherieserver vorhanden sind, die als Mitglieder der Servergruppe definiert sind, geben Sie auf dem Hub-Server den folgenden Befehl aus:

```
QUERY SERVERGROUP IBM-OC-Name_des_Hub-Servers
```

Tipp: `IBM-OC-Name_des_Hub-Servers` ist der Name der überwachten Servergruppe, die bei der Konfiguration des ersten Peripherieservers automatisch erstellt wurde. Dieser Servergruppenname stimmt auch mit der Überwachungsadministrator-ID überein, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.

b. Um Peripherieserver aus der Servergruppe zu löschen, geben Sie auf dem Hub-Server für jeden Peripherieserver den folgenden Befehl aus:

```
DELETE GRPMEMBER IBM-OC-Name_des_Hub-Servers Name_des_Peripherieservers
```

c. Nachdem alle Peripherieserver aus der Servergruppe gelöscht wurden, geben Sie auf dem Hub-Server die folgenden Befehle aus:

```
DELETE SERVERGROUP IBM-OC-Name_des_Hub-Servers
SET MONITOREDSERVERGROUP ""
```

d. Geben Sie auf jedem Peripherieserver die folgenden Befehle aus:

```
REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

e. Löschen Sie die Definition des Hub-Servers, indem Sie auf jedem Peripherieserver den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Hub-Servers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Definition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

f. Löschen Sie die Definition jedes Peripherieservers, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

```
DELETE SERVER Name_des_Peripherieservers
```

Achtung: Führen Sie diesen Schritt nicht aus, wenn die Serverdefinition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.

4. Schreiben Sie die Standardeinstellungen auf jeden Server zurück, indem Sie die folgenden Befehle ausgeben:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut.

Zugehörige Tasks:
Assistenten für die Erstkonfiguration erneut starten
Web-Server starten und stoppen

Anwendungen, virtuelle Maschinen und Systeme schützen

Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherungszeitplan zum Schützen der Clientdaten auswählen.

- Clients hinzufügen
  Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.
- Clientoperationen verwalten
  Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.
- Client-Upgrades verwalten
  Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.
- Clientknoten stilllegen
  Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.

- Daten zum Freigeben von Speicherbereich inaktivieren
  In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegeben Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

Clients hinzufügen

Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.

Informationen zu diesem Vorgang

Die Prozedur beschreibt grundlegende Schritte zum Hinzufügen eines Clients. Spezifischere Anweisungen zum Konfigurieren von Clients enthält die Dokumentation für das auf dem Clientknoten installierte Produkt. Folgende Typen von Clients können vorhanden sein:

Anwendungsclientknoten
: Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Systemclientknoten
: Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

VM-Clientknoten
: Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Vorgehensweise

Um einen Client hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Software aus, die auf dem Clientknoten installiert werden soll, und planen Sie die Installation. Führen Sie die Anweisungen in Client-Software auswählen und Installation planen aus.
2. Geben Sie an, wie Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Regeln zum Sichern und Archivieren von Clientdaten angeben aus.
3. Geben Sie an, wann Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Sicherungs- und Archivierungsoperationen planen aus.
4. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, registrieren Sie den Client. Führen Sie die Anweisungen in Clients registrieren aus.
5. Um einen Clientknoten zu schützen, installieren und konfigurieren Sie die ausgewählte Software auf dem Clientknoten. Führen Sie die Anweisungen in Clients installieren und konfigurieren aus.

Client-Software auswählen und Installation planen

Unterschiedliche Typen von Daten erfordern unterschiedliche Typen von Schutz. Geben Sie den Typ der Daten an, die geschützt werden müssen, und wählen Sie die geeignete Software aus.

Informationen zu diesem Vorgang

Das bevorzugte Verfahren ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installieren, für das der Clientakzeptor keine Zeitpläne ausführt, müssen Sie die Konfigurationsanweisungen in der Produktdokumentation ausführen, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

Vorgehensweise

Wählen Sie abhängig von Ihrer Zielsetzung die zu installierenden Produkte aus und lesen Sie die Installationsanweisungen.
Tipp: Wenn Sie die Client-Software jetzt installieren, müssen Sie auch die in Clients installieren und konfigurieren beschriebenen Clientkonfigurationstasks ausführen, bevor Sie den Client verwenden können.

Ziel	Produkt und Beschreibung	Installationsanweisungen

Ziel	Produkt und Beschreibung	Installationsanweisungen
Schutz eines Dateiservers oder einer Workstation	Der Client für Sichern/Archivieren sichert und archiviert Dateien und Verzeichnisse von Dateiservern und Workstations in Speicher. Es ist auch möglich, Sicherungsversionen und archivierte Kopien von Dateien zurückzuschreiben und abzurufen.	• Anforderungen für den Client für Sichern/Archivieren • UNIX- und Linux-Clients für Sichern/Archivieren installieren • Windows-Client für Sichern/Archivieren installieren
Schutz von Anwendungen mit Momentaufnahmesicherungs- und -zurückschreibungsfunktionalität	IBM Spectrum Protect Snapshot schützt Daten mit integrierter anwendungsgesteuerter Momentaufnahmesicherungs- und -zurückschreibungsfunktionalität. Sie können Daten schützen, die von IBM DB2-Datenbanksoftware sowie SAP-, Oracle-, Microsoft Exchange Server- und Microsoft SQL Server-Anwendungen gespeichert werden.	• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
Schutz einer E-Mail-Anwendung auf einem IBM Domino-Server	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass IBM Domino-Server heruntergefahren werden.	• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) • Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)
Schutz einer E-Mail-Anwendung auf einem Server mit Microsoft Exchange Server	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass Server mit Microsoft Exchange Server heruntergefahren werden.	Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Schutz einer IBM DB2-Datenbank	Mithilfe der Anwendungsprogrammierschnittstelle (API) des Clients für Sichern/Archivieren können DB2-Daten auf dem IBM Spectrum Protect-Server gesichert werden.	IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Schutz einer IBM Informix-Datenbank	Mithilfe der API des Clients für Sichern/Archivieren können Informix-Daten auf dem IBM Spectrum Protect-Server gesichert werden.	IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Schutz einer Microsoft SQL-Datenbank	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server schützt Microsoft SQL-Daten.	Data Protection for SQL Server unter Windows Server Core installieren
Schutz einer Oracle-Datenbank	IBM Spectrum Protect for Databases: Data Protection for Oracle schützt Oracle-Daten.	Installation von Data Protection for Oracle
Schutz einer SAP-Umgebung	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP stellt Schutz bereit, der für SAP-Umgebungen angepasst ist. Das Produkt dient der Verbesserung der Verfügbarkeit von SAP-Datenbankservern und der Verringerung des Verwaltungsaufwands.	• IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren • IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren

Ziel	Produkt und Beschreibung	Installationsanweisungen
Schutz einer virtuellen Maschine	IBM Spectrum Protect for Virtual Environments stellt Schutz bereit, der für virtuelle Microsoft Hyper-V- und VMware-Umgebungen angepasst ist. Mithilfe von IBM Spectrum Protect for Virtual Environments können Sie immer inkrementelle Sicherungen erstellen, die auf einem zentralen Server gespeichert werden, Sicherungsmaßnahmen erstellen und virtuelle Maschinen oder einzelne Dateien zurückschreiben. Sie können auch stattdessen den Client für Sichern/Archivieren zum Sichern und Zurückschreiben einer vollständigen virtuellen VMware- oder Microsoft Hyper-V-Maschine verwenden. Es ist auch möglich, Dateien oder Verzeichnisse von einer virtuellen VMware-Maschine zu sichern und zurückzuschreiben.	• Data Protection for Microsoft Hyper-V installieren • Installation und Upgrade für Data Protection for VMware durchführen • IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)

Tipp: Um den Client für die Speicherbereichsverwaltung zu verwenden, können Sie IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows installieren.

Regeln zum Sichern und Archivieren von Clientdaten angeben

Stellen Sie vor dem Hinzufügen eines Clients sicher, dass entsprechende Regeln zum Sichern und Archivieren der Clientdaten angegeben sind. Während des Clientregistrierungsprozesses ordnen Sie den Clientknoten einer Maßnahmendomäne zu, die die Regeln enthält, die die Regeln enthält, die steuern, wie und wann Clientdaten gespeichert werden.

Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Maßnahmen, die für Ihre Lösung konfiguriert sind, vertraut sind und wissen, dass für die Maßnahmen keine Änderungen erforderlich sind, fahren Sie mit Sicherungs- und Archivierungsoperationen planen fort.
- Wenn Sie mit den Maßnahmen nicht vertraut sind, führen Sie die Schritte in dieser Prozedur aus.

Informationen zu diesem Vorgang

Maßnahmen haben Auswirkungen auf das Datenvolumen, das im Laufe der Zeit gespeichert wird, und den Zeitraum, den Daten aufbewahrt werden und für die Zurückschreibung durch Clients verfügbar sind. Um Datenschutzziele zu erreichen, können Sie die Standardmaßnahme aktualisieren und eigene Maßnahmen erstellen. Eine Maßnahme umfasst die folgenden Regeln:

- Angabe, wie und wann Dateien in Serverspeicher gesichert und archiviert werden
- Anzahl Kopien einer Datei und Zeitraum, den Kopien im Serverspeicher aufbewahrt werden

Während des Clientregistrierungsprozesses ordnen Sie einen Client einer *Maßnahmendomäne* zu. Die Maßnahme für einen bestimmten Client wird durch die Regeln in der Maßnahmendomäne festgelegt, der der Client zugeordnet ist. In der Maßnahmendomäne befinden sich die Regeln, die wirksam sind, in der aktiven *Maßnahmengruppe*.

Wenn ein Client eine Datei sichert oder archiviert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Eine *Verwaltungsklasse* ist die wichtigste Gruppe von Regeln zur Verwaltung von Clientdaten. Die Sicherungs- und Archivierungsoperationen auf dem Client verwenden die Einstellungen in der Standardverwaltungsklasse der Maßnahmendomäne, es sei denn, Sie passen die Maßnahme weiter an. Eine Maßnahme kann angepasst werden, indem weitere Verwaltungsklassen definiert werden und ihre Verwendung über Clientoptionen zugeordnet wird.

Clientoptionen können in einer lokalen, editierbaren Datei auf dem Clientsystem und in einer Clientoptionsgruppe auf dem Server angegeben werden. Die Optionen in der Clientoptionsgruppe auf dem Server können die Optionen in der lokalen Clientoptionsdatei überschreiben oder den Optionen in der lokalen Clientoptionsdatei hinzugefügt werden.

Vorgehensweise

1. Überprüfen Sie die Maßnahmen, die für Ihre Lösung konfiguriert sind, indem Sie die Anweisungen in Maßnahmen anzeigen ausführen.
2. Wenn geringfügige Änderungen erforderlich sind, um die Datenaufbewahrungsanforderungen zu erfüllen, führen Sie die Anweisungen in Maßnahmen editieren aus.
3. Optional: Wenn Maßnahmendomänen erstellt oder umfangreiche Änderungen an Maßnahmen durchgeführt werden müssen, um Datenaufbewahrungsanforderungen zu erfüllen, lesen Sie die Informationen in Maßnahmen anpassen.

Maßnahmen anzeigen

Zeigen Sie Maßnahmen an, um zu bestimmen, ob die Maßnahmen zur Erfüllung Ihrer Anforderungen editiert werden müssen.

Vorgehensweise

1. Um die aktive Maßnahmengruppe für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
   b. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.
2. Um inaktive Maßnahmengruppen für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf der Seite Maßnahmengruppen auf die Umschaltfläche Konfigurieren. Jetzt können Sie die inaktiven Maßnahmengruppen anzeigen und editieren.
   b. Blättern Sie mithilfe der vorwärts und rückwärts gerichteten Pfeile durch die inaktiven Maßnahmengruppen. Wenn Sie eine inaktive Maßnahmengruppe anzeigen, sind die unterschiedlichen Einstellungen für die inaktive und aktive Maßnahmengruppe hervorgehoben.
   c. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.

Maßnahmen editieren

Um die Regeln zu ändern, die für eine Maßnahmendomäne gelten, editieren Sie die aktive Maßnahmengruppe für die Maßnahmendomäne. Sie können auch eine andere Maßnahmengruppe für eine Domäne aktivieren.

Vorbereitende Schritte

Änderungen an Maßnahmen können sich auf die Datenaufbewahrung auswirken. Stellen Sie sicher, dass weiterhin Daten gesichert werden, die für Ihr Unternehmen von entscheidender Bedeutung sind, sodass Sie diese Daten in einem Katastrophenfall zurückschreiben können. Stellen Sie außerdem sicher, dass Ihr System über genügend Speicherbereich für geplante Sicherungsoperationen verfügt.

Informationen zu diesem Vorgang

Sie editieren eine Maßnahmengruppe, indem Sie eine oder mehrere Verwaltungsklassen in der Maßnahmengruppe ändern. Wenn Sie die aktive Maßnahmengruppe editieren, stehen die Änderungen den Clients erst zur Verfügung, nachdem Sie die Maßnahmengruppe reaktiviert haben. Um die editierte Maßnahmengruppe Clients zur Verfügung zu stellen, aktivieren Sie die Maßnahmengruppe.

Obwohl Sie mehrere Maßnahmengruppen für eine Maßnahmendomäne definieren können, kann nur eine einzige Maßnahmengruppe aktiv sein. Wenn Sie eine andere Maßnahmengruppe aktivieren, ersetzt diese die momentan aktive Maßnahmengruppe.

Informationen zu bevorzugten Verfahren zum Definieren von Maßnahmen finden Sie in Maßnahmen anpassen.

Vorgehensweise

1. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.

   Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.

3. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppe ist editierbar.
4. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
5. Editieren Sie die Maßnahmengruppe, indem Sie eine der folgenden Aktionen ausführen:

Option	Bezeichnung
Verwaltungsklasse hinzufügen	a. Klicken Sie in der Tabelle 'Maßnahmengruppen' auf + Verwaltungsklasse. b. Um die Regeln zum Sichern und Archivieren von Daten anzugeben, füllen Sie die Felder im Fenster Verwaltungsklasse hinzufügen aus. c. Um die Verwaltungsklasse als Standardverwaltungsklasse festzulegen, wählen Sie das Kontrollkästchen Als Standardwert definieren aus. d. Klicken Sie auf Hinzufügen.
Verwaltungsklasse löschen	Klicken Sie in der Spalte 'Verwaltungsklasse' auf -. Tipp: Um die Standardverwaltungsklasse zu löschen, müssen Sie zunächst eine andere Verwaltungsklasse als Standardverwaltungsklasse zuordnen.

Option	Bezeichnung
Legen Sie eine Verwaltungsklasse als Standardverwaltungsklasse fest.	Klicken Sie in der Spalte 'Standard' für die Verwaltungsklasse auf das Optionsfeld. Tipp: Die Standardverwaltungsklasse verwaltet Clientdateien, wenn einer Datei keine andere Verwaltungsklasse zugeordnet ist oder keine andere Verwaltungsklasse zur Verwaltung geeignet ist. Um sicherzustellen, dass Clients immer Dateien sichern und archivieren können, wählen Sie eine Standardverwaltungsklasse aus, die sowohl Regeln für das Sichern als auch für das Archivieren von Dateien enthält.
Verwaltungsklasse ändern	Um die Merkmale einer Verwaltungsklasse zu ändern, aktualisieren Sie die Felder in der Tabelle.

6. Klicken Sie auf Sichern.
   Achtung: Wenn Sie eine neue Maßnahmengruppe aktivieren, können Daten verloren gehen. Daten, die unter einer Maßnahmengruppe geschützt werden, werden möglicherweise unter einer anderen Maßnahmengruppe nicht geschützt. Daher müssen Sie vor dem Aktivieren einer Maßnahmengruppe sicherstellen, dass die Unterschiede zwischen der vorherigen Maßnahmengruppe und der neuen Maßnahmengruppe keinen Datenverlust zur Folge haben.
7. Klicken Sie auf Aktivieren. Es wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt. Stellen Sie sicher, dass die Änderungen in der neuen Maßnahmengruppe mit Ihren Datenaufbewahrungsanforderungen konsistent sind, indem Sie die folgenden Schritte ausführen:
   a. Überprüfen Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der aktiven Maßnahmengruppe gebunden sind, werden in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
   b. Ermitteln Sie Verwaltungsklassen in der aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
   c. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden sollen, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.

Sicherungs- und Archivierungsoperationen planen

Bevor Sie einen neuen Client beim Server registrieren, müssen Sie sicherstellen, dass ein Zeitplan verfügbar ist, um anzugeben, wann Sicherungs- und Archivierungsoperationen ausgeführt werden. Während des Registrierungsprozesses können Sie dem Client einen Zeitplan zuordnen.

Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Zeitplänen, die für die Lösung konfiguriert sind, vertraut sind und für die Zeitpläne keine Änderungen erforderlich sind, fahren Sie mit Clients registrieren fort.
- Wenn Sie mit den Zeitplänen nicht vertraut sind oder für die Zeitpläne Änderungen erforderlich sind, führen Sie die Schritte in dieser Prozedur aus.

Informationen zu diesem Vorgang

Normalerweise müssen Sicherungsoperationen für alle Clients täglich ausgeführt werden. Planen Sie Client- und Server-Workloads mit Bedacht, um die beste Leistung für Ihre Speicherumgebung zu erzielen. Um die Überschneidung von Client- und Serveroperationen zu verhindern, planen Sie die Ausführung von Clientsicherungs- und -archivierungsoperationen gegebenenfalls für die Nacht. Wenn sich Client- und Serveroperationen überschneiden oder ihnen nicht genügend Zeit und Ressourcen zur Verarbeitung zur Verfügung gestellt werden, können eine Verschlechterung der Systemleistung, fehlgeschlagene Operationen und andere Probleme die Folge sein.

Vorgehensweise

1. Überprüfen Sie die verfügbaren Zeitpläne, indem Sie den Mauszeiger in der Menüleiste des Operations Center über Clients bewegen. Klicken Sie auf Zeitpläne.
2. Optional: Ändern oder Erstellen Sie einen Zeitplan, indem Sie die folgenden Schritte ausführen:

Option	Bezeichnung
Zeitplan ändern	a. Wählen Sie in der Sicht Zeitpläne den Zeitplan aus und klicken Sie auf Details. b. Zeigen Sie auf der Seite Zeitplandetails Details an, indem Sie auf die blauen Pfeile am Anfang der Zeilen klicken. c. Ändern Sie die Einstellungen im Zeitplan und klicken Sie auf Sichern.
Zeitplan erstellen	Klicken Sie in der Sicht Zeitpläne auf +Zeitplan und führen Sie die Schritte zum Erstellen eines Zeitplans aus.

3. Optional: Verwenden Sie zum Konfigurieren von Zeitplaneinstellungen, die im Operations Center nicht sichtbar sind, einen Serverbefehl. Angenommen, Sie möchten eine Clientoperation planen, mit der ein bestimmtes Verzeichnis gesichert und einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zugeordnet wird.

a. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder.
b. Geben Sie zum Erstellen eines Zeitplans den Befehl DEFINE SCHEDULE und zum Ändern eines Zeitplans den Befehl UPDATE SCHEDULE aus. Ausführliche Informationen zu den Befehlen finden Sie in DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren) bzw. UPDATE SCHEDULE (Clientzeitplan aktualisieren).

Zugehörige Tasks:
Zeitplan für tägliche Operationen optimieren

Clients registrieren

Registrieren Sie einen Client, um sicherzustellen, dass der Client die Verbindung zum Server herstellen und der Server Clientdaten schützen kann.

Vorbereitende Schritte

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963. Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

Vorgehensweise

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

  ```
  register node Knotenname Kennwort userid=Knotenname
  ```

  Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.
- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  a. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  b. Klicken Sie in der Tabelle 'Clients' auf + Client.
  c. Führen Sie die Schritte im Assistenten Client hinzufügen aus:
     i. Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Datendeduplizierung' das Kontrollkästchen Aktivieren aus.
     ii. Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEDUPLICATION.
     Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
     iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
     iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
     v. Klicken Sie auf Client hinzufügen.

Zugehörige Verweise:
Option 'tcpserveraddress'
Option 'tcpport'
Option 'nodename'
Option 'deduplication'

Clients installieren und konfigurieren

Bevor Sie einen Clientknoten schützen können, müssen Sie die ausgewählte Software installieren und konfigurieren.

Vorgehensweise

Wenn Sie die Software bereits installiert haben, starten Sie mit Schritt 2.

1. Führen Sie eine der folgenden Aktionen aus:
   - Um Software auf einem Anwendungs- oder Clientknoten zu installieren, führen Sie die Anweisungen aus.

Software	Link zu Anweisungen

Software	Link zu Anweisungen
IBM Spectrum Protect-Client für Sichern/Archivieren	▪ UNIX- und Linux-Clients für Sichern/Archivieren installieren ▪ Windows-Client für Sichern/Archivieren installieren Informationen zur manuellen Implementierung von Clientaktualisierungen vom Server finden Sie in den folgenden Dokumenten: ▪ Für IBM Spectrum Protect-Server der Version 8.1.2 oder höher siehe Technote 2004596. ▪ Für IBM® Tivoli Storage Manager-Server der Version 7.1 und IBM Spectrum Protect-Server der Version 8.1.1 siehe Technote 1673299.
IBM Spectrum Protect for Databases	▪ Installation von Data Protection for Oracle ▪ Data Protection for SQL Server unter Windows Server Core installieren
IBM Spectrum Protect for Mail	▪ Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) ▪ Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0) ▪ Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	▪ Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen ▪ Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen ▪ Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
IBM Spectrum Protect for Enterprise Resource Planning	▪ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren ▪ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren

- Um Software auf einem VM-Clientknoten zu installieren, führen Sie die Anweisungen für den ausgewählten Sicherungstyp aus.

Sicherungstyp	Link zu Anweisungen
Wenn Sie planen, VMware-Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie den IBM Spectrum Protect-Client für Sichern/Archivieren.	▪ UNIX- und Linux-Clients für Sichern/Archivieren installieren ▪ Windows-Client für Sichern/Archivieren installieren
Wenn Sie planen, immer inkrementelle Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren auf demselben Clientknoten oder auf unterschiedlichen Clientknoten.	▪ IBM Spectrum Protect for Virtual Environments-Onlineproduktdokumentation Tipp: Die Software für IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren sind im IBM Spectrum Protect for Virtual Environments-Installationspaket enthalten.

2. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, fügen Sie die Werte für die Optionen TCPSERVERADDRESS, TCPPORT und NODENAME in der Clientoptionsdatei hinzu oder aktualisieren Sie diese. Verwenden Sie die Werte, die Sie beim Registrieren des Clients notiert haben (Clients registrieren).
   - Fügen Sie für Clients, die unter einem AIX-, Linux- oder Mac OS X-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.sys hinzu.
   - Fügen Sie für Clients, die unter einem Windows-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.opt hinzu.

   Standardmäßig befinden sich die Optionsdateien im Installationsverzeichnis.
3. Wenn ein Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem installiert wurde, installieren Sie den Clientverwaltungsservice auf dem Client. Führen Sie die Anweisungen in Clientverwaltungsservice installieren aus.
4. Konfigurieren Sie den Client für die Ausführung geplanter Operationen. Führen Sie die Anweisungen in Client für die Ausführung geplanter Operationen konfigurieren aus.
5. Optional: Konfigurieren Sie die Kommunikation durch eine Firewall. Führen Sie die Anweisungen in Client/Server-Kommunikation durch eine Firewall konfigurieren aus.
6. Führen Sie eine Testsicherung aus, um sicherzustellen, dass Daten wie geplant geschützt werden. Führen Sie beispielsweise für einen Client für Sichern/Archivieren die folgenden Schritte aus:
   a. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus, der gesichert werden soll, und klicken Sie auf Sichern.
   b. Überprüfen Sie, ob die Sicherung erfolgreich ausgeführt wird und keine Warnungen oder Fehlernachrichten vorhanden sind.
7. Überwachen Sie die Ergebnisse der geplanten Operationen für den Client im Operations Center.

Nächste Schritte

Um zu ändern, welche Daten vom Client gesichert werden, führen Sie die Anweisungen in Bereich einer Clientsicherung ändern aus.

Client für die Ausführung geplanter Operationen konfigurieren

Sie müssen einen Client-Scheduler auf dem Clientknoten konfigurieren und starten. Der Client-Scheduler ermöglicht die Kommunikation zwischen dem Client und dem Server, sodass geplante Operationen erfolgen können. Beispielsweise umfassen geplante Operationen normalerweise das Sichern von Dateien von einem Client.

Informationen zu diesem Vorgang

Die bevorzugte Methode ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert. Der Clientakzeptor verwaltet den Client-Scheduler derart, dass der Scheduler nur in erforderlichen Fällen ausgeführt wird:

- Wenn der Zeitpunkt erreicht ist, an dem der Server nach der nächsten geplanten Operation abgefragt werden soll
- Wenn der Zeitpunkt erreicht ist, an dem die nächste geplante Operation gestartet werden soll

Durch die Verwendung des Clientakzeptors ist es möglich, die Anzahl Hintergrundprozesse auf dem Client zu reduzieren und Probleme in Bezug auf die Speicheraufbewahrungsdauer zu vermeiden.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installiert hatten, für das der Clientakzeptor keine Zeitpläne ausführt, führen Sie die Konfigurationsanweisungen in der Produktdokumentation aus, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

Wenn Ihr Unternehmen standardmäßig ein Zeitplanungstool eines anderen Anbieters verwendet, können Sie statt des Clientakzeptors dieses Zeitplanungstool verwenden. Normalerweise starten Zeitplanungstools anderer Anbieter Clientprogramme direkt mithilfe von Betriebssystembefehlen. Informationen zum Konfigurieren eines Zeitplanungstools eines anderen Anbieters enthält die Produktdokumentation.

Vorgehensweise

Um den Client-Scheduler mithilfe des Clientakzeptors zu konfigurieren und zu starten, führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
b. Klicken Sie auf die Registerkarte Web-Client.
c. Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
d. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei dsm.sys die Option passwordaccess auf `generate`.
e. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkennwort ein:

```
dsmc query sess
```

f. Starten Sie den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

```
/usr/bin/dsmcad
```

g. Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie der Systemstartdatei (normalerweise /etc/inittab) den folgenden Eintrag hinzu:

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Clientakzeptordämon
```

Linux

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
b. Klicken Sie auf die Registerkarte Web-Client.
c. Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
d. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei dsm.sys die Option passwordaccess auf `generate`.
e. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkennwort ein:

```
dsmc query sess
```

f. Starten Sie den Clientakzeptor, indem Sie sich mit der Rootbenutzer-ID anmelden und den folgenden Befehl ausgeben:

```
service dsmcad start
```

g. Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie den Service hinzu, indem Sie in einer Shelleingabeaufforderung den folgenden Befehl ausgeben:

```
# chkconfig --add dsmcad
```

MAC OS X

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
b. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, klicken Sie auf Berechtigung, wählen Sie Kennwort generieren aus und klicken Sie auf Anwenden.
c. Um anzugeben, wie Services verwaltet werden, klicken Sie auf Web-Client, wählen Sie Zeitplan aus, klicken Sie auf Anwenden und dann auf OK.
d. Um sicherzustellen, dass das generierte Kennwort gespeichert wird, starten Sie den Client für Sichern/Archivieren erneut.
e. Starten Sie den Clientakzeptor mithilfe der Anwendung 'IBM Spectrum Protect Tools for Administrators'.

Windows

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Dienstprogramme > Setup-Assistent > Hilfe zum Konfigurieren des Client-Schedulers. Klicken Sie auf Weiter.
b. Lesen Sie die Informationen auf der Seite Schedulerassistent und klicken Sie auf Weiter.
c. Wählen Sie auf der Seite Scheduler-Task die Option Neuen oder zusätzlichen Scheduler installieren aus und klicken Sie auf Weiter.
d. Geben Sie auf der Seite Schedulername und -position einen Namen für den Client-Scheduler an, der hinzugefügt wird. Wählen Sie dann Scheduler mit Clientakzeptordämon (CAD) verwalten aus, um den Scheduler zu verwalten, und klicken Sie auf Weiter.
e. Geben Sie den Namen ein, der diesem Clientakzeptor zugeordnet werden soll. Der Standardname ist 'Clientakzeptor'. Klicken Sie auf Weiter.
f. Schließen Sie die Konfiguration ab, indem Sie den Assistenten durchlaufen.
g. Aktualisieren Sie die Clientoptionsdatei, dsm.opt, und setzen Sie die Option passwordaccess auf generate.
h. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl in der Eingabeaufforderung aus:

```
dsmc query sess
```

Geben Sie auf Anforderung das Clientknotenkennwort ein.
i. Starten Sie den Clientakzeptorservice über die Seite Systemsteuerung. Wenn Sie beispielsweise den Standardnamen verwendet haben, starten Sie den Service 'Clientakzeptor'. Starten Sie nicht den Scheduler-Service, den Sie auf der Seite Schedulername und -position angegeben haben. Der Scheduler-Service wird wie erforderlich automatisch vom Clientakzeptorservice gestartet und gestoppt.

Client/Server-Kommunikation durch eine Firewall konfigurieren

Wenn ein Client durch eine Firewall mit einem Server kommunizieren muss, müssen Sie die Client/Server-Kommunikation durch die Firewall ermöglichen.

Vorbereitende Schritte

Wenn Sie den Assistenten 'Client hinzufügen' zum Registrieren eines Clients verwendet hatten, bestimmen Sie die Optionswerte in der Clientoptionsdatei, die während dieses Prozesses abgerufen wurden. Sie können die Werte zur Angabe von Ports verwenden.

Informationen zu diesem Vorgang

Achtung: Konfigurieren Sie eine Firewall nicht derart, dass dies eine Beendigung der Sitzungen zur Folge hätte, die von einem Server oder Speicheragenten verwendet werden. Die Beendigung einer gültigen Sitzung kann zu unvorhersehbaren Ergebnissen führen. Prozesse und Sitzungen scheinen unter Umständen aufgrund von Ein-/Ausgabefehlern gestoppt zu werden. Um das Ausschließen von Sitzungen von Zeitlimitbeschränkungen zu erleichtern, konfigurieren Sie bekannte Ports für IBM Spectrum Protect-Komponenten. Stellen Sie sicher, dass die Serveroption KEEPALIVE auf den Standardwert YES gesetzt bleibt. Auf diese Art und Weise kann sichergestellt werden, dass die Client/Server-Kommunikation unterbrechungsfrei erfolgt. Anweisungen zum Definieren der Serveroption KEEPALIVE finden Sie in KEEPALIVE.

Vorgehensweise

Öffnen Sie die folgenden Ports, um Zugriff durch die Firewall zu ermöglichen:

TCP/IP-Port für den Client für Sichern/Archivieren, den Verwaltungsbefehlszeilenclient und den Client-Scheduler
Geben Sie den Port über die Option tcpport in der Clientoptionsdatei an. Die Option tcpport in der Clientoptionsdatei muss mit der Option TCPPORT in der Serveroptionsdatei übereinstimmen. Der Standardwert ist 1500. Wenn ein anderer Wert als der Standardwert verwendet werden soll, geben Sie eine Zahl zwischen 1024 und 32767 an.

HTTP-Port, um die Kommunikation zwischen dem Web-Client und fernen Workstations zu ermöglichen
Geben Sie den Port für die ferne Workstation an, indem Sie die Option httpport in der Clientoptionsdatei der fernen Workstation festlegen. Der Standardwert ist 1581.

TCP/IP-Ports für die ferne Workstation

Der Standardwert von 0 (null) hat zur Folge, dass zwei freie Portnummern der fernen Workstation nach dem Zufallsprinzip zugeordnet werden. Wenn die Portnummern nicht nach dem Zufallsprinzip zugeordnet werden sollen, geben Sie über die Option webports in der Clientoptionsdatei der fernen Workstation Werte an.

TCP/IP-Port für Verwaltungssitzungen
: Geben Sie den Port an, an dem der Server auf Anforderungen von Verwaltungsclientsitzungen wartet. Der Wert der Clientoption tcpadminport muss mit dem Wert der Serveroption TCPADMINPORT übereinstimmen. Auf diese Art und Weise können Sie sichere Verwaltungssitzungen in einem privaten Netz gewährleisten.

Clientoperationen verwalten

Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.

Informationen zu diesem Vorgang

In einigen Fällen können Clientfehler behoben werden, indem der Clientakzeptor gestoppt und gestartet wird. Wenn Clientknoten oder Administrator-IDs gesperrt sind, können Sie das Problem beheben, indem Sie den Clientknoten bzw. die Administrator-ID entsperren und dann das Kennwort zurücksetzen.

Ausführliche Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in Clientprobleme lösen.

- Fehler in Clientfehlerprotokollen auswerten
  Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.
- Clientakzeptor stoppen und erneut starten
  Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.
- Kennwörter zurücksetzen
  Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.
- Bereich einer Clientsicherung ändern
  Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

Fehler in Clientfehlerprotokollen auswerten

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

Vorbereitende Schritte

Um Fehler in einem Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem zu beheben, stellen Sie sicher, dass der Clientverwaltungsservice installiert und gestartet wurde. Installationsanweisungen finden Sie in Clientverwaltungsservice installieren. Anweisungen zur Überprüfung der Installation finden Sie in Ordnungsgemäße Installation des Clientverwaltungsservice überprüfen.

Vorgehensweise

Um Clientfehler zu diagnostizieren und zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn der Clientverwaltungsservice auf dem Clientknoten installiert ist, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Details.
  3. Klicken Sie auf der Seite 'Zusammenfassung' auf die Registerkarte Diagnose.
  4. Überprüfen Sie die abgerufenen Protokollnachrichten.
     Tipps:
     - Um das Fenster 'Clientprotokolle' ein- oder auszublenden, doppelklicken Sie auf den Rahmen des Fensters 'Clientprotokolle'.
     - Um die Größe des Fensters 'Clientprotokolle' zu ändern, klicken Sie auf den Rahmen des Fensters 'Clientprotokolle' und ziehen Sie den Rahmen.

     Wenn auf der Seite 'Diagnose' Vorschläge angezeigt werden, wählen Sie einen Vorschlag aus. Im Fenster 'Clientprotokolle' sind die Clientprotokollnachrichten, auf die sich der Vorschlag bezieht, hervorgehoben.
  5. Lösen Sie die in den Fehlernachrichten angegebenen Probleme mithilfe der Vorschläge.
     Tipp: Vorschläge werden nur für einen Teil der Clientnachrichten bereitgestellt.

- Wenn der Clientverwaltungsservice nicht auf dem Clientknoten installiert ist, überprüfen Sie die Fehlerprotokolle für den installierten Client.

Clientakzeptor stoppen und erneut starten

Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.

Informationen zu diesem Vorgang

In einigen Fällen können Clientzeitplanungsprobleme behoben werden, indem der Clientakzeptor gestoppt und erneut gestartet wird. Der Clientakzeptor muss aktiv sein, um sicherzustellen, dass geplante Operationen auf dem Client ausgeführt werden können. Wenn Sie beispielsweise die IP-Adresse oder den Domänennamen des Servers ändern, müssen Sie den Clientakzeptor erneut starten.

Vorgehensweise

Führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

- Um den Clientakzeptor zu stoppen, führen Sie die folgenden Schritte aus:
  a. Bestimmen Sie die Prozess-ID für den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

     ```
     ps -ef | grep dsmcad
     ```

     Überprüfen Sie die Ausgabe. In der folgenden Beispielausgabe lautet die Prozess-ID für den Clientakzeptor 6764:

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```

  b. Geben Sie in der Befehlszeile den folgenden Befehl aus:

     ```
     kill -9 PID
     ```

     Dabei gibt *PID* die Prozess-ID für den Clientakzeptor an.
- Um den Clientakzeptor zu starten, geben Sie in der Befehlszeile den folgenden Befehl aus:

  ```
  /usr/bin/dsmcad
  ```

Linux

- Um den Clientakzeptor zu stoppen, ohne ihn erneut zu starten, geben Sie den folgenden Befehl aus:

  ```
  # service dsmcad stop
  ```

- Um den Clientakzeptor zu stoppen und erneut zu starten, geben Sie den folgenden Befehl aus:

  ```
  # service dsmcad restart
  ```

MAC OS X

Klicken Sie auf Applications > Utilities > Terminal.

- Um den Clientakzeptor zu stoppen, geben Sie den folgenden Befehl aus:

  ```
  /bin/launchctl unload -w com.ibm.tivoli.dsmcad
  ```

- Um den Clientakzeptor zu starten, geben Sie den folgenden Befehl aus:

  ```
  /bin/launchctl load -w com.ibm.tivoli.dsmcad
  ```

Windows

- Um den Clientakzeptorservice zu stoppen, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf Start > Verwaltung > Dienste.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf Beenden und OK.
- Um den Clientakzeptorservice erneut zu starten, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf Start > Verwaltung > Dienste.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf Starten und OK.

Zugehörige Verweise:
Fehler für Clientzeitplanung beheben

Kennwörter zurücksetzen

Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.

Vorgehensweise

Um Kennwortprobleme zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn ein Client für Sichern/Archivieren auf einem Clientknoten installiert ist und das Kennwort verloren gegangen ist oder Sie das Kennwort vergessen haben, führen Sie die folgenden Schritte aus:
  1. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Knotenname* den Clientknoten und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
  2. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.
     Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf `generate` gesetzt haben.
- Wenn ein Administrator aufgrund von Kennwortproblemen ausgesperrt ist, führen Sie die folgenden Schritte aus:
  1. Um dem Administrator den Zugriff auf den Server zu ermöglichen, geben Sie den Befehl UNLOCK ADMIN aus. Anweisungen finden Sie in UNLOCK ADMIN (Administrator entsperren).
  2. Legen Sie mit dem Befehl UPDATE ADMIN ein neues Kennwort fest:

     ```
     update admin Administratorname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Administratorname* den Namen des Administrators und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
- Wenn ein Clientknoten gesperrt ist, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, warum der Clientknoten gesperrt ist und ob er entsperrt werden muss. Wenn beispielsweise der Clientknoten stillgelegt ist, wird der Clientknoten aus der Produktionsumgebung entfernt. Sie können die Stilllegungsoperation nicht zurücknehmen und der Clientknoten bleibt gesperrt. Ein Clientknoten kann auch gesperrt sein, wenn die Clientdaten Gegenstand einer rechtlichen Untersuchung sind.
  2. Verwenden Sie zum Entsperren eines Clientknotens den Befehl UNLOCK NODE. Anweisungen finden Sie in UNLOCK NODE (Clientknoten entsperren).
  3. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Knotenname* den Namen des Knotens und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
  4. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.
     Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf `generate` gesetzt haben.

Bereich einer Clientsicherung ändern

Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

Informationen zu diesem Vorgang

Indem Sie nicht benötigte Objekte von Sicherungsoperationen ausschließen, können Sie die Größe des Speicherbereichs, der für Sicherungsoperationen erforderlich ist, und die Speicherkosten besser steuern. Abhängig von Ihrem Lizenzpaket ist es unter Umständen auch möglich, die Lizenzierungskosten zu begrenzen.

Vorgehensweise

Die Vorgehensweise beim Ändern des Bereichs von Sicherungsoperationen ist von dem Produkt abhängig, das auf dem Clientknoten installiert ist:

- Bei einem Client für Sichern/Archivieren können Sie eine Einschluss-/Ausschlussliste erstellen, um eine Datei, Dateigruppen oder Verzeichnisse in Sicherungsoperationen einzuschließen oder von Sicherungsoperationen auszuschließen. Um eine Einschluss-/Ausschlussliste zu erstellen, führen Sie die Anweisungen in Einschluss-/Ausschlussliste erstellen aus.

Um die konsistente Verwendung einer Einschluss-/Ausschlussliste für alle Clients eines bestimmten Typs zu gewährleisten, können Sie auf dem Server eine Clientoptionsgruppe erstellen, die die erforderlichen Optionen enthält. Anschließend ordnen Sie die Clientoptionsgruppe jedem Client desselben Typs zu. Ausführliche Informationen finden Sie in Clientoperationen über Clientoptionsgruppen steuern.

- Für einen Client für Sichern/Archivieren können Sie die Objekte, die in eine Teilsicherungsoperation eingeschlossen werden sollen, mithilfe der Option domain angeben. Führen Sie die Anweisungen in Clientoption 'domain' aus.
- Führen Sie für andere Produkte die Anweisungen in der Produktdokumentation aus, um zu definieren, welche Objekte in Sicherungsoperationen eingeschlossen und von Sicherungsoperationen ausgeschlossen werden sollen.

Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

Vorbereitende Schritte

1. Überprüfen Sie die Voraussetzungen für die Client/Server-Kompatibilität in Technote 1053218. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden.
2. Überprüfen Sie die Systemvoraussetzungen für den Client in IBM Spectrum Protect Supported Operating Systems.
3. Wenn die Lösung Speicheragenten oder Speicherarchivclients umfasst, überprüfen Sie die Informationen zur Kompatibilität von Speicheragenten bzw. Speicherarchivclients mit Servern, die als Speicherarchivmanager konfiguriert sind. Siehe Technote 1302789.

   Wenn Sie planen, ein Upgrade für einen Speicherarchivmanager und einen Speicherarchivclient durchzuführen, müssen Sie zuerst das Upgrade für den Speicherarchivmanager durchführen.

Vorgehensweise

Um ein Software-Upgrade durchzuführen, führen Sie die in der folgenden Tabelle aufgelisteten Anweisungen aus.

Software	Link zu Anweisungen
IBM Spectrum Protect-Client für Sichern/Archivieren	• Upgrade des Clients für Sichern/Archivieren durchführen
IBM Spectrum Protect Snapshot	• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
IBM Spectrum Protect for Databases	• Upgrade für Data Protection for SQL Server durchführen • Installation von Data Protection for Oracle • Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 durchführen • Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle durchführen
IBM Spectrum Protect for Mail	• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) • Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0) • Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Installation und Upgrade für Data Protection for VMware durchführen • Data Protection for Microsoft Hyper-V installieren

Clientknoten stilllegen

Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet

wird, können Sie die Workstation stilllegen.

Informationen zu diesem Vorgang

Wenn Sie den Stilllegungsprozess starten, sperrt der Server den Clientknoten, um zu verhindern, dass dieser auf den Server zugreift. Dateien, die zu dem Clientknoten gehören, werden nacheinander gelöscht; anschließend wird der Clientknoten gelöscht. Sie können die folgenden Typen von Clientknoten stilllegen:

Anwendungsclientknoten
: Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Systemclientknoten
: Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

VM-Clientknoten
: Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Die einfachste Methode zur Stilllegung eines Clientknotens ist die Verwendung des Operations Center. Der Stilllegungsprozess wird im Hintergrund ausgeführt. Wenn der Client für die Replikation von Clientdaten konfiguriert ist, entfernt das Operations Center den Client automatisch aus der Replikation auf dem Quellen- und dem Zielreplikationsserver, bevor es den Client stilllegt.
Tipp: Sie können einen Clientknoten auch stilllegen, indem Sie den Befehl DECOMMISSION NODE oder DECOMMISSION VM ausgeben. Diese Methode kann beispielsweise in den folgenden Fällen verwendet werden:

- Um den Stilllegungsprozess für einen späteren Zeitpunkt zu planen oder eine Serie von Befehlen unter Verwendung eines Scripts auszuführen, geben Sie die Ausführung des Stilllegungsprozesses im Hintergrund an.
- Um den Stilllegungsprozess zu Zwecken der Fehlerbehebung zu überwachen, geben Sie die Ausführung des Stilllegungsprozesses im Vordergrund an. Wenn Sie den Prozess im Vordergrund ausführen, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor Sie die Arbeit mit anderen Tasks fortsetzen können.

Vorgehensweise

Führen Sie eine der folgenden Aktionen aus:

- Um einen Client mithilfe des Operations Center im Hintergrund stillzulegen, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Weitere > Stilllegen.
- Um einen Clientknoten mithilfe eines Verwaltungsbefehls stillzulegen, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, ob der Clientknoten für die Knotenreplikation konfiguriert ist, indem Sie den Befehl QUERY NODE ausgeben. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, führen Sie den folgenden Befehl aus:

     ```
     query node austin format=detailed
     ```

     Überprüfen Sie das Ausgabefeld 'Replikationsstatus'.
  2. Wenn der Clientknoten für die Replikation konfiguriert ist, entfernen Sie den Clientknoten aus der Replikation, indem Sie den Befehl REMOVE REPLNODE ausgeben. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

     ```
     remove replnode austin
     ```

  3. Führen Sie eine der folgenden Aktionen aus:
     - Um einen Anwendungs- oder Systemclientknoten im Hintergrund stillzulegen, geben Sie den Befehl DECOMMISSION NODE aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

       ```
       decommission node austin
       ```

     - Um einen Anwendungs- oder Systemclientknoten im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION NODE unter Angabe des Parameters `wait=yes` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

       ```
       decommission node austin wait=yes
       ```

     - Um eine virtuelle Maschine im Hintergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM aus. Wenn beispielsweise die virtuelle Maschine den Namen AUSTIN hat, der Dateibereich 7 ist und der Dateibereichsname über die Dateibereichs-ID angegeben wird, geben Sie den folgenden Befehl aus:

       ```
       decommission vm austin 7 nametype=fsid
       ```

Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Um eine virtuelle Maschine im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM unter Angabe des Parameters `wait=yes` aus. Geben Sie beispielsweise den folgenden Befehl aus:

  ```
  decommission vm austin 7 nametype=fsid wait=yes
  ```

  Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

  ```
  decommission vm "austin 2" 7 nametype=fsid wait=yes
  ```

Nächste Schritte

Achten Sie auf Fehlernachrichten, die unter Umständen in der Benutzerschnittstelle oder in der Befehlsausgabe unmittelbar nach der Ausführung des Prozesses angezeigt werden.

Um zu überprüfen, ob der Clientknoten stillgelegt wurde, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
2. Überprüfen Sie in der Tabelle 'Clients' in der Spalte 'Gefährdet' den Status:
   - Der Status 'Stillgelegt' (DECOMMISSIONED) gibt an, dass der Knoten stillgelegt wurde.
   - Ein Nullwert gibt an, dass der Knoten nicht stillgelegt wurde.
   - Der Status 'Anstehend' (PENDING) gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

   Tipp: Wenn der Status eines anstehenden Stilllegungsprozesses bestimmt werden soll, geben Sie den folgenden Befehl aus:

   ```
   query process
   ```

3. Überprüfen Sie die Befehlsausgabe:
   - Wenn für den Stilllegungsprozess ein Status angegeben ist, ist der Prozess in Bearbeitung. Beispiel:

     ```
     query process
      Prozess-     Prozessbeschreibung           Prozessstatus
      nummer
     ---------     --------------------     -------------------------------------------
             3     DECOMMISSION NODE        Anzahl der für Knoten NODE1 inaktivierten
                                            Sicherungsobjekte: 8 Objekte inaktiviert.
     ```

   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie keine Fehlernachricht empfangen haben, ist der Prozess unvollständig. Ein Prozess kann unvollständig sein, wenn Dateien, die dem Knoten zugeordnet sind, noch nicht inaktiviert wurden. Führen Sie nach der Inaktivierung der Dateien den Stilllegungsprozess erneut aus.
   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie eine Fehlernachricht empfangen, ist der Prozess fehlgeschlagen. Führen Sie den Stilllegungsprozess erneut aus.

Zugehörige Verweise:
DECOMMISSION NODE (Clientknoten stilllegen)
DECOMMISSION VM (Virtuelle Maschine stilllegen)
QUERY NODE (Knoten abfragen)
REMOVE REPLNODE (Clientknoten aus Replikation entfernen)

Daten zum Freigeben von Speicherbereich inaktivieren

In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegeben Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

Informationen zu diesem Vorgang

Einige Anwendungsclients sichern Daten immer als aktive Sicherungsdaten auf dem Server. Da aktive Sicherungsdaten nicht durch die Bestandsverfallsmaßnahmen verwaltet werden, werden die Daten nicht automatisch gelöscht und belegen unbegrenzt Serverspeicher. Um den Speicherbereich freizugeben, der von veralteten Daten belegt wird, können Sie die Daten inaktivieren.

Wenn Sie den Inaktivierungsprozess ausführen, werden alle aktiven Sicherungsdaten, die vor dem angegeben Datum gespeichert wurden, inaktiv. Die Daten werden gelöscht, sobald sie verfallen, und können nicht zurückgeschrieben werden. Die Inaktivierungsfunktion gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

Vorgehensweise

1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients.

2. Wählen Sie in der Tabelle 'Clients' einen oder mehrere Clients aus und klicken Sie auf Weitere > Bereinigen.
   Befehlszeilenmethode: Inaktivieren Sie Daten mit dem Befehl DEACTIVATE DATA.

Zugehörige Verweise:
DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)

Datenspeicher verwalten

Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.

- Speicherpoolcontainer prüfen
  Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.
- Bestandskapazität verwalten
  Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.
- Speichernutzung und Prozessorauslastung verwalten
  Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datendeduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.
- Geplante Aktivitäten optimieren
  Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

Zugehörige Verweise:
Speicherpooltypen

Speicherpoolcontainer prüfen

Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.

Informationen zu diesem Vorgang

Sie prüfen einen Speicherpoolcontainer in den folgenden Situationen:

- Sie geben den Befehl QUERY DAMAGED aus und es wird ein Problem erkannt.
- Der Server zeigt Nachrichten zu beschädigten Datenbereichen an.
- Ihre Hardware meldet ein Problem und es werden Fehlernachrichten angezeigt, die sich auf den Speicherpoolcontainer beziehen.

Vorgehensweise

1. Um einen Speicherpoolcontainer zu prüfen, geben Sie den Befehl AUDIT CONTAINER aus. Geben Sie beispielsweise den folgenden Befehl aus, um den Container 000000000000076c.dcf zu prüfen:

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Überprüfen Sie die Ausgabe der Nachricht ANR4891I auf Informationen zu allen beschädigten Datenbereichen.

Nächste Schritte

Wenn Sie Probleme mit dem Speicherpoolcontainer erkennen, können Sie Daten auf der Basis Ihrer Konfiguration zurückschreiben. Sie können den Inhalt des Speicherpools mit dem Befehl REPAIR STGPOOL reparieren.
Einschränkung: Sie können den Inhalt des Speicherpools nur reparieren, wenn der Speicherpool mit dem Befehl PROTECT STGPOOL geschützt wurde.
Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool abfragen)

Bestandskapazität verwalten

Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.

Vorbereitende Schritte

Die aktive Protokolldatei und das Archivprotokoll haben die folgenden Merkmale:

- Die Größe der aktiven Protokolldatei kann maximal 512 GB betragen. Weitere Informationen zum Festlegen der Größe der aktiven Protokolldatei für Ihr System finden Sie in Planung der Speicherarrays.
- Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist. Die Größe des Archivprotokolls ist im Gegensatz zur Größe der aktiven Protokolldatei nicht auf eine vordefinierte Größe festgelegt. Archivprotokolldateien werden automatisch gelöscht, wenn sie nicht mehr benötigt werden.

Als Best Practice können Sie wahlweise ein Archivübernahmeprotokoll erstellen, in dem Archivprotokolldateien gespeichert werden, wenn das Archivprotokollverzeichnis voll ist.

Bestimmen Sie über das Operations Center, welche Komponente des Bestands voll ist. Stellen Sie sicher, dass der Server gestoppt wird, bevor Sie eine der Bestandskomponenten vergrößern.

Vorgehensweise

- Um die Datenbank zu vergrößern, führen Sie die folgenden Schritte aus:
  - Erstellen Sie in unterschiedlichen Laufwerken oder Dateisystemen ein oder mehrere Verzeichnisse für die Datenbank.
  - Geben Sie den Befehl EXTEND DBSPACE aus, um der Datenbank das Verzeichnis oder die Verzeichnisse hinzuzufügen. Die Instanzbenutzer-ID des Datenbankmanagers muss Zugriff auf die Verzeichnisse haben. Standardmäßig erfolgt eine Neuverteilung der Daten auf alle Datenbankverzeichnisse und eine Konsolidierung des Speicherbereichs.
    Tipps:
    - Die Zeit, die für die vollständige Neuverteilung von Daten und die Konsolidierung von Speicherbereich erforderlich ist, variiert abhängig von der Größe Ihrer Datenbank. Stellen Sie sicher, dass Sie dies bei der Planung berücksichtigen.
    - Stellen Sie sicher, dass die Verzeichnisse, die Sie angeben, dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.
  - Stoppen Sie den Server und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig nutzen zu können.
  - Reorganisieren Sie die Datenbank, falls erforderlich. Die Index- und Tabellenreorganisation für die Serverdatenbank kann dazu beitragen, unerwartetes Datenbankwachstum und Leistungsprobleme zu verhindern. Weitere Informationen zur Reorganisation der Datenbank finden Sie in Technote 1683633.
- Um die Datenbank für Server der Version 7.1 und höher zu verkleinern, geben Sie im Serverinstanzverzeichnis die folgenden DB2-Befehle aus:
  Einschränkung: Die Befehle können die E/A-Aktivität erhöhen und sich unter Umständen auf die Serverleistung auswirken. Um Leistungsprobleme auf ein Mindestmaß zu reduzieren, warten Sie, bis ein Befehl abgeschlossen ist, bevor Sie den nächsten Befehl ausgeben. Die DB2-Befehle können ausgegeben werden, wenn der Server aktiv ist.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
```

- Um die aktive Protokolldatei zu vergrößern oder zu verkleinern, führen Sie die folgenden Schritte aus:
  1. Stellen Sie sicher, dass die Position für die aktive Protokolldatei über genügend Speicherbereich für die erhöhte Protokollgröße verfügt. Wenn ein Protokollspiegel vorhanden ist, muss auch die Position für den Spiegel über genügend Speicherbereich für die erhöhte Protokollgröße verfügen.
  2. Stoppen Sie den Server.
  3. Aktualisieren Sie in der Datei dsmserv.opt die Option ACTIVELOGSIZE mit der neuen Größe der aktiven Protokolldatei (angegeben in Megabyte).
     Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Die folgende Tabelle enthält Richtlinien für den Speicherbedarf:

Tabelle 1. Schätzen des Speicherbedarfs für Datenträger und Dateibereiche

Wert für die Option ACTIVELOGSize	Größe des im Verzeichnis für aktive Protokolldateien zu reservierender freier Speicherbereich zusätzlich zum Speicherbereich für ACTIVELOGSize
16 GB bis 128 GB	5120 MB
129 GB bis 256 GB	10240 MB
257 GB bis 512 GB	20480 MB

Um die Größe der aktiven Protokolldatei in die maximale Größe von 512 GB zu ändern, geben Sie die folgende Serveroption ein:

```
activelogsize 524288
```

4. Wenn Sie planen, ein neues Verzeichnis für aktive Protokolldateien zu verwenden, aktualisieren Sie den in der Serveroption ACTIVELOGDIRECTORY angegebenen Verzeichnisnamen. Das neue Verzeichnis muss leer sein und die Benutzer-ID des Datenbankmanagers muss Zugriff auf dieses Verzeichnis haben.
5. Starten Sie den Server erneut.

- Komprimieren Sie die Archivprotokolle, um die Größe des Speicherbereichs, der zum Speichern benötigt wird, zu reduzieren. Aktivieren Sie die dynamische Komprimierung für das Archivprotokoll, indem Sie den folgenden Befehl ausgeben:

  ```
  setopt archlogcompress yes
  ```

  Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hohen Workloads aktivieren. Ein Aktivieren dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Dateisystem für Archivprotokolle haben. Diese Verzögerung kann zur Folge haben, dass der Speicherbereich im Dateisystem für aktive Protokolldateien knapp wird. Sie müssen den verfügbaren Speicherbereich im Dateisystem für aktive Protokolldateien überwachen, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn für das Dateisystem für das Verzeichnis für aktive Protokolldateien fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT können Sie die Komprimierung für das Archivprotokoll sofort inaktivieren, ohne den Server stoppen zu müssen.

Zugehörige Verweise:
Serveroption ACTIVELOGSIZE
EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)
SETOPT (Serveroption für dynamische Aktualisierung definieren)

Speichernutzung und Prozessorauslastung verwalten

Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datendeduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.

Vorbereitende Schritte

- Stellen Sie sicher, dass Ihre Konfiguration die erforderliche Hardware und Software verwendet. Weitere Informationen finden Sie in IBM Spectrum Protect Supported Operating Systems.
- Weitere Informationen zur Verwaltung von Ressourcen, wie beispielsweise Datenbank und Wiederherstellungsprotokoll, finden Sie in Planung der Speicherarrays.
- Fügen Sie zusätzlichen Systemspeicher hinzu, um festzustellen, ob sich die Leistung verbessert. Überwachen Sie die Speichernutzung regelmäßig, um zu bestimmen, ob weiterer Speicher erforderlich ist.

Vorgehensweise

1. Geben Sie, falls möglich, Speicherbereich aus dem Dateisystemcache frei.
2. Verwenden Sie zur Verwaltung des Systemspeichers, den jeder Server auf einem System verwendet, die Serveroption DBMEMPERCENT. Begrenzen Sie den Prozentsatz des Systemspeichers, der vom Datenbankmanager jedes Servers verwendet werden kann. Wenn alle Server gleich wichtig sind, verwenden Sie denselben Wert für jeden Server. Wenn ein Server der Produktionsserver ist und die anderen Server Testserver sind, definieren Sie für den Produktionsserver einen höheren Wert als für die Testserver.
3. Definieren Sie den Benutzerdatengrenzwert und den privaten Speicher für die Datenbank, um sicherzustellen, dass immer genügend privater Speicher verfügbar ist. Wenn der private Speicher knapp wird, kann dies Fehler, eine nicht optimale Leistung und Instabilität zur Folge haben.

Geplante Aktivitäten optimieren

Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

Vorgehensweise

1. Überwachen Sie die Systemleistung regelmäßig, um sicherzustellen, dass Clientsicherungs- und Serververwaltungstasks erfolgreich ausgeführt werden. Führen Sie die Anweisungen in Plattenspeicherlösung für mehrere Standorte überwachen aus.

2. Optional: Wenn die Überwachungsdaten anzeigen, dass sich die Server-Workload erhöht hat, überprüfen Sie die Planungsinformationen. Überprüfen Sie, ob die Kapazität des Systems in den folgenden Fällen ausreichend ist:
    - Erhöhung der Anzahl Clients
    - Zunahme des Datenvolumens, das gesichert wird
    - Änderung des Zeitraums, der für Sicherungen verfügbar ist
3. Bestimmen Sie, ob Ihre Lösung auf dem von Ihnen erwarteten Niveau ausgeführt wird. Überprüfen Sie die Clientzeitpläne dahingehend, ob Tasks innerhalb des geplanten Zeitrahmens ausgeführt werden:
    a. Wählen Sie auf der Seite Clients im Operations Center den Client aus.
    b. Klicken Sie auf Details.
    c. Überprüfen Sie auf der Seite Zusammenfassung des Clients die für Gesichert und Repliziert angegebene Aktivität, um alle Risiken zu ermitteln.

    Passen Sie, falls erforderlich, den Zeitpunkt und die Häufigkeit für die Ausführung von Clientsicherungsoperationen an.
4. Planen Sie ausreichend Zeit ein, um die folgenden Verwaltungstasks innerhalb von 24 Stunden erfolgreich ausführen zu können:
    a. Schützen von Speicherpools
    b. Replizieren von Knotendaten
    c. Sichern der Datenbank
    d. Ausführen der Verfallsverarbeitung, um Clientsicherungen und Archivierungsdateikopien aus dem Serverspeicher zu entfernen

    Tipp: Planen Sie einen geeigneten Zeitpunkt für den Start von Verwaltungstasks und die Ausführung in der korrekten Reihenfolge. Planen Sie beispielsweise Replikationstasks im Anschluss an die erfolgreiche Ausführung von Clientsicherungen.

- Clients von einem Server auf einen anderen versetzen
  Um zu verhindern, dass der Speicherbereich auf einem Server knapp wird, oder um Workloadprobleme zu beheben, müssen Sie unter Umständen Clientknoten von einem Server auf einen anderen versetzen.

Zugehörige Konzepte:
Leistung
Zugehörige Tasks:
Zeitpläne für Serververwaltungsaktivitäten definieren
Daten deduplizieren (Version 7.1.1)

Replikation verwalten

Verwenden Sie die Replikation für die Wiederherstellen von Daten an einem Standort zur Wiederherstellung nach einem Katastrophenfall und zur Beibehaltung desselben Stands von Dateien auf dem Quellenserver und dem Zielserver. Sie können die Replikation auf Knotenebene verwalten. Sie können Daten auch auf Speicherpoolebene schützen.

- Replikationskompatibilität
  Vor dem Konfigurieren von Replikationsoperationen mit IBM Spectrum Protect müssen Sie sicherstellen, dass die Quellen- und Zielreplikationsserver für die Replikation kompatibel sind.
- Knotenreplikation aktivieren
  Sie können die Knotenreplikation zum Schützen Ihrer Daten aktivieren.
- Daten in Verzeichniscontainerspeicherpools schützen
  Schützen Sie Daten in Verzeichniscontainerspeicherpools, um die Knotenreplikationszeit zu reduzieren und die Reparatur von Daten in Verzeichniscontainerspeicherpools zu ermöglichen.
- Replikationseinstellungen ändern
  Ändern Sie Replikationseinstellungen im Operations Center. Ändern Sie Einstellungen wie die Anzahl Replikationssitzungen, Replikationsregeln, die Daten, die repliziert werden sollen, den Replikationszeitplan und die Replikationsworkload.
- Unterschiedliche Aufbewahrungsmaßnahmen für den Quellenserver und den Zielserver festlegen
  Auf dem Zielreplikationsserver können Sie Maßnahmen festlegen, mit denen die replizierten Clientknotendaten anders als auf dem Quellenserver verwaltet werden. Beispielsweise können Sie auf dem Quellen- und dem Zielserver eine unterschiedliche Anzahl Versionen von Dateien aufbewahren.

Replikationskompatibilität

Vor dem Konfigurieren von Replikationsoperationen mit IBM Spectrum Protect müssen Sie sicherstellen, dass die Quellen- und Zielreplikationsserver für die Replikation kompatibel sind.

Tabelle 1. Replikationskompatibilität von Serverversionen

Version des Quellenreplikationsservers	Kompatible Versionen für den Zielreplikationsserver
Version 6.3.0 - Version 6.3.2	Version 6.3.0 - Version 6.3.2
Version 6.3.3	Version 6.3.3 oder höhere Stufen von Version 6.3
Version 6.3.4 oder höhere Stufen von Version 6.3	Version 6.3.4 oder höher
Version 7.1	Version 7.1 oder höher
Version 7.1.1	Version 7.1 oder höher

Version des Quellenreplikationsservers	Kompatible Versionen für den Zielreplikationsserver
Version 7.1.3	Version 7.1.3 oder höher
Version 7.1.4	Version 7.1.3 oder höher
Version 7.1.5	Version 7.1.3 oder höher
Version 7.1.6	Version 7.1.3 oder höher
Version 7.1.7	Version 7.1.3 oder höher
Version 8.1	Version 7.1.3 oder höher
Version 8.1.1	Version 7.1.3 oder höher
Version 8.1.2	Version 7.1.3 oder höher

Knotenreplikation aktivieren

Sie können die Knotenreplikation zum Schützen Ihrer Daten aktivieren.

Vorbereitende Schritte

Stellen Sie sicher, dass die Quellen- und Zielserver für die Replikation kompatibel sind.

Informationen zu diesem Vorgang

Replizieren Sie den Clientknoten, um alle Clientdaten, einschließlich Metadaten, zu replizieren. Standardmäßig ist die Knotenreplikation inaktiviert, wenn Sie den Server zum ersten Mal starten.
Tipps:

- Um die Replikationsverarbeitungszeit zu reduzieren, schützen Sie den Speicherpool vor dem Replizieren von Clientknoten. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch den Speicherpoolschutz repliziert werden, übersprungen.
- Die Replikation erfordert mehr Speicherkapazität und genügend Bandbreite für die Ausführung der Verarbeitung. Ändern Sie die Größe der Datenbank und der zugehörigen Protokolle, um sicherzustellen, dass Transaktionen ausgeführt werden können.

Vorgehensweise

Um die Knotenreplikation zu aktivieren, führen Sie im Operations Center die folgenden Schritte aus:

a. Klicken Sie auf der Seite Server auf Details.
b. Klicken Sie auf der Seite Details auf Merkmale.
c. Wählen Sie im Abschnitt Replikation im Feld Abgehende Replikation die Option Aktiviert aus.
d. Klicken Sie auf Sichern.

Nächste Schritte

Führen Sie die folgenden Aktionen aus:

1. Informationen zur Überprüfung, ob die Replikation erfolgreich war, finden Sie in Prüfliste für tägliche Überwachungstasks.
2. Linux-BetriebssystemeWenn der IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Führen Sie die Anweisungen in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann aus.

Zugehörige Verweise:
Replikationskompatibilität

Daten in Verzeichniscontainerspeicherpools schützen

Schützen Sie Daten in Verzeichniscontainerspeicherpools, um die Knotenreplikationszeit zu reduzieren und die Reparatur von Daten in Verzeichniscontainerspeicherpools zu ermöglichen.

Vorbereitende Schritte

Stellen Sie sicher, dass mindestens ein Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver vorhanden ist. Wenn Sie die Replikation im Operations Center aktivieren, können Sie den Speicherpoolschutz planen. Um die Replikation zu konfigurieren und den Speicherpoolschutz zu aktivieren, führen Sie die folgenden Schritte aus:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher und klicken Sie auf Replikation.

2. Klicken Sie auf der Seite 'Replikation' auf Serverpaar.
3. Führen Sie die Schritte im Assistenten 'Serverpaar hinzufügen' aus.

Informationen zu diesem Vorgang

Durch das Schützen eines Verzeichniscontainerspeicherpools werden Datenbereiche in einem anderen Speicherpool gesichert und die Leistung bei der Knotenreplikation wird gegebenenfalls verbessert. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch Speicherpoolschutz gesichert werden, übersprungen und die Replikationsverarbeitungszeit wird somit reduziert. Sie können den Schutz von Speicherpools mehrmals am Tag planen, um den Änderungen an Daten Rechnung zu tragen.

Indem ein Speicherpool geschützt wird, werden keine Ressourcen verwendet, die vorhandene Daten und Metadaten replizieren, wodurch die Serverleistung verbessert wird. Sie müssen Verzeichniscontainerspeicherpools verwenden, wenn nur der Speicherpool geschützt und gesichert werden soll.

Alternative Schutzstrategie: Als Alternative zur Verwendung der Replikation können Sie Daten in Verzeichniscontainerspeicherpools schützen, indem Sie die Daten in Containerkopienspeicherpools kopieren. Daten in Containerkopienspeicherpools werden auf Banddatenträgern gespeichert. Bandkopien, die an einem anderen Standort aufbewahrt werden, stellen zusätzlichen Schutz für die Wiederherstellung nach einem Katastrophenfall in einer replizierten Umgebung bereit.

Vorgehensweise

1. Um den Speicherpoolschutz zu aktivieren, können Sie auch stattdessen den Befehl PROTECT STGPOOL auf dem Quellenserver verwenden, um Datenbereiche in einem Verzeichniscontainerspeicherpool zu sichern. Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen POOL1 zu schützen, geben Sie den folgenden Befehl aus:

   ```
   protect stgpool pool1
   ```

   Im Rahmen der Ausführung des Befehls PROTECT STGPOOL werden beschädigte Speicherbereiche im Zielspeicherpool repariert. Eine Reparatur ist nur möglich, wenn die Speicherbereiche auf dem Zielserver bereits als beschädigt markiert sind. Beispielsweise kann vor der Ausgabe des Befehls PROTECT STGPOOL mit einem Befehl AUDIT CONTAINER eine Beschädigung im Zielspeicherpool identifiziert werden.
2. Optional: Wenn beschädigte Speicherbereiche im Zielspeicherpool repariert wurden und Sie mehrere Quellenspeicherpools in einem einzigen Zielspeicherpool schützen, führen Sie die folgenden Schritte aus, um eine vollständige Reparatur zu gewährleisten:
   a. Geben Sie den Befehl PROTECT STGPOOL für alle Quellenspeicherpools aus, um die Beschädigung möglichst vollständig zu reparieren.
   b. Geben Sie den Befehl PROTECT STGPOOL erneut für alle Quellenspeicherpools aus. Verwenden Sie bei dieser zweiten Operation den Parameter FORCERECONCILE=YES. Mit diesem Schritt wird sichergestellt, dass alle Reparaturen anderer Quellenpools korrekt für alle Quellenspeicherpools erkannt werden.

Ergebnisse

Wenn ein Verzeichniscontainerspeicherpool geschützt wird, können Sie den Speicherpool für den Fall, dass eine Beschädigung auftritt, mit dem Befehl REPAIR STGPOOL reparieren.
Einschränkung: Wenn Sie Clientknoten replizieren, den Verzeichniscontainerspeicherpool aber nicht schützen, können Sie den Speicherpool nicht reparieren.

Nächste Schritte

Führen Sie die folgenden Aktionen aus:

1. Um den Replikationsworkloadstatus anzuzeigen, führen Sie die Anweisungen in Prüfliste für tägliche Überwachungstasks aus.
2. Linux-BetriebssystemeWenn der IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Führen Sie die Anweisungen in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann aus.

Zugehörige Verweise:
Daten reparieren und wiederherstellen
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
PROTECT STGPOOL (Speicherpooldaten schützen)
Zugehörige Informationen:
Häufig gestellte Fragen (FAQs) zu Verzeichniscontainerspeicherpools
Häufig gestellte Fragen (FAQs) zu Cloud-Containerspeicherpools

Replikationseinstellungen ändern

Ändern Sie Replikationseinstellungen im Operations Center. Ändern Sie Einstellungen wie die Anzahl Replikationssitzungen, Replikationsregeln, die Daten, die repliziert werden sollen, den Replikationszeitplan und die Replikationsworkload.

Informationen zu diesem Vorgang

In den folgenden Szenarios müssen Sie möglicherweise Ihre Replikationseinstellungen ändern:

- Änderungen an Datenprioritäten
- Änderungen an Replikationsregeln
- Erfordernis eines anderen Servers als Zielserver
- Geplante Prozesse, die sich negativ auf die Serverleistung auswirken

Vorgehensweise

Ändern Sie mithilfe des Operations Center die Replikationseinstellungen.

Task	Prozedur
Ändern einer Replikationsregel	a. Klicken Sie auf der Seite Server auf Details. b. Klicken Sie auf der Seite Details auf Merkmale. c. Wählen Sie im Abschnitt Replikation die Replikationsregel aus, die angewendet werden soll: Standardregel für Archivierungsdaten, Standardregel für Sicherungsdaten oder Standardregel für speicherverwaltete Daten. d. Klicken Sie auf Sichern.
Aufbewahrungsdauer für Replikationsdatensätze angeben	a. Klicken Sie auf der Seite Server auf Details. b. Klicken Sie auf der Seite Details auf Merkmale. c. Geben Sie im Abschnitt Replikation im Feld Replikationsprotokoll aufbewahren die Anzahl Tage ein, die Replikationsdatensätze beibehalten werden müssen. Sie können auch das Kontrollkästchen Nicht aufbewahren auswählen, wenn Replikationsdatensätze nicht erforderlich sind. d. Klicken Sie auf Sichern.
Zielreplikationsserver angeben	a. Klicken Sie auf der Seite Server auf Details. b. Klicken Sie auf der Seite Details auf Merkmale. c. Geben Sie im Abschnitt Replikation den Zielserver an. d. Klicken Sie auf Sichern.
Replikationsprozess abbrechen	a. Klicken Sie auf der Seite Server auf Aktive Tasks. b. Wählen Sie den Prozess oder die Sitzung aus, der bzw. die abgebrochen werden soll. c. Klicken Sie auf Abbrechen.

Unterschiedliche Aufbewahrungsmaßnahmen für den Quellenserver und den Zielserver festlegen

Auf dem Zielreplikationsserver können Sie Maßnahmen festlegen, mit denen die replizierten Clientknotendaten anders als auf dem Quellenserver verwaltet werden. Beispielsweise können Sie auf dem Quellen- und dem Zielserver eine unterschiedliche Anzahl Versionen von Dateien aufbewahren.

Vorgehensweise

1. Überprüfen Sie auf dem Quellenreplikationsserver die Replikationskonfiguration und stellen Sie sicher, dass der Quellenreplikationsserver mit dem Zielreplikationsserver kommunizieren kann, indem Sie den Befehl VALIDATE REPLICATION ausgeben. Überprüfen Sie beispielsweise die Konfiguration unter Angabe des Namens eines Clientknotens, der repliziert wird:

   ```
   validate replication node1 verifyconnection=yes
   ```

2. Geben Sie auf dem Quellenreplikationsserver den Befehl VALIDATE REPLPOLICY aus, um die Unterschiede zwischen den Maßnahmen auf dem Quellenreplikationsserver und den Maßnahmen auf dem Zielreplikationsserver zu überprüfen. Um beispielsweise die Unterschiede zwischen den Maßnahmen auf dem Quellenserver und den Maßnahmen auf dem Zielserver CVT_SRV2 anzuzeigen, geben Sie auf dem Quellenserver den folgenden Befehl aus:

   ```
   validate replpolicy cvt_srv2
   ```

3. Aktualisieren Sie die Maßnahmen auf dem Zielserver, falls erforderlich.
   Tipp: Sie können die Maßnahmen auf dem Zielserver mithilfe des Operations Center ändern. Führen Sie die Anweisungen in Maßnahmen editieren aus.
   Um beispielsweise inaktive Dateiversionen auf dem Zielserver für einen kürzeren Zeitraum als auf dem Quellenserver aufzubewahren, reduzieren Sie die Einstellung Sicherungen in den Verwaltungsklassen, die für replizierte Clientdaten gelten.

4. Ermöglichen Sie dem Zielreplikationsserver die Verwendung seiner Maßnahmen zur Verwaltung der replizierten Clientknotendaten, indem Sie auf dem Quellenserver den Befehl SET DISSIMILARPOLICIES ausgeben. Um beispielsweise die Maßnahmen auf dem Zielreplikationsserver CVT_SRV2 zu aktivieren, geben Sie auf dem Quellenserver den folgenden Befehl aus:

   ```
   set dissimilarpolicies cvt_srv2 on
   ```

   Bei der nächsten Ausführung des Replikationsprozesses werden die Maßnahmen auf dem Zielreplikationsserver zur Verwaltung der replizierten Clientknotendaten verwendet.
   Tipp: Wenn Sie die Replikation mithilfe des Operations Center konfigurieren und die Maßnahmen auf dem Quellen- und dem Zielreplikationsserver nicht übereinstimmen, wird die für den Quellenreplikationsserver angegebene Maßnahme verwendet. Wenn die Maßnahmen auf dem Zielreplikationsserver mithilfe des Befehls SET DISSIMILARPOLICIES aktiviert wurden, wird die für den Zielreplikationsserver angegebene Maßnahme verwendet. Wenn der Zielreplikationsserver nicht über die von dem Knoten auf dem Quellenreplikationsserver verwendete Maßnahme verfügt, wird die Maßnahme STANDARD verwendet.

Zugehörige Verweise:
EXPORT POLICY (Maßnahmeninformationen exportieren)
SET DISSIMILARPOLICIES (Maßnahmen auf dem Zielreplikationsserver zum Verwalten replizierter Daten aktivieren)
VALIDATE REPLICATION (Replikation für einen Clientknoten überprüfen)
VALIDATE REPLPOLICY (Maßnahmen auf dem Zielreplikationsserver überprüfen)

Server schützen

Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

- Sicherheitskonzepte
  Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.
- Administratoren verwalten
  Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.
- Kennwortanforderungen ändern
  Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.
- IBM Spectrum Protect auf dem System schützen
  Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

Sicherheitskonzepte

Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

Transport Layer Security

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtsicherheit für eine sichere Verbindung zwischen Servern, Clients und Speicheragenten bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, verwenden Sie SSL oder TLS zum Verschlüsseln der Daten.

Tipp: In der gesamten IBM Spectrum Protect-Dokumentation gilt jede Angabe von "SSL" oder zum "Auswählen von SSL" für TLS.

SSL wird von Global Security Kit (GSKit) bereitgestellt, das zusammen mit dem IBM Spectrum Protect-Server installiert wird, der vom Server, vom Client und vom Speicheragenten verwendet wird.

Einschränkung: Sie dürfen die SSL- oder TLS-Protokolle nicht für die Kommunikation mit einer DB2-Datenbankinstanz verwenden, die von IBM Spectrum Protect-Servern verwendet wird.

Jeder Server, Client oder Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdiges selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle (CA) signiert ist. Sie können Ihre eigenen Zertifikate verwenden oder Zertifikate bei einer Zertifizierungsstelle (CA) kaufen. Jedes der Zertifikate muss installiert und der Schlüsseldatenbank auf dem IBM Spectrum Protect-Server, -Client oder -Speicheragenten hinzugefügt werden. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet. Einige CA-Zertifikate sind in der Schlüsseldatenbank standardmäßig vorinstalliert.

SSL wird auf dem IBM Spectrum Protect-Server, -Client und -Speicheragenten unabhängig voneinander konfiguriert.

Berechtigungsstufen

Für jeden IBM Spectrum Protect-Server sind verschiedene Administratorberechtigungsstufen verfügbar, die die Tasks festlegen, die ein Administrator ausführen kann.

Nach der Registrierung muss einem Administrator Berechtigung erteilt werden, indem ihm eine oder mehrere Administratorberechtigungsstufen zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen und anderen Administratoren über den Befehl GRANT AUTHORITY Berechtigungsstufen zuordnen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Ein Administrator kann andere Administrator-IDs registrieren, den IDs Berechtigungsstufen zuordnen, IDs umbenennen, IDs entfernen und IDs für den Server sperren oder entsperren.

Ein Administrator kann den Zugriff auf bestimmte Clientknoten für Rootbenutzer-IDs und Nicht-Rootbenutzer-IDs steuern. Standardmäßig kann eine Nicht-Rootbenutzer-ID keine Daten auf dem Knoten sichern. Ändern Sie mit dem Befehl UPDATE NODE die Knoteneinstellungen, um Sicherungen zu ermöglichen.

Kennwörter

Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer beim Zugriff auf den Server ein Kennwort eingeben.

Verwenden Sie LDAP (Lightweight Directory Access Protocol), um striktere Anforderungen für Kennwörter anzuwenden. Weitere Informationen finden Sie in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1).

Tabelle 1. Merkmale der Kennwortauthentifizierung

Merkmale	Weitere Informationen
Abhängigkeit von der Groß-/Kleinschreibung	Nicht von der Groß-/Kleinschreibung abhängig.
Standardwert für Kennwortablauf	90 Tage. Der Ablaufzeitraum beginnt mit der ersten Registrierung einer Administrator-ID oder eines Clientknotens beim Server. Wenn das Kennwort innerhalb dieses Zeitraums nicht geändert wird, muss das Kennwort beim nächsten Zugriff des Benutzers auf den Server geändert werden.
Ungültige Kennworteingabeversuche	Sie können einen Grenzwert für aufeinanderfolgende ungültige Kennworteingabeversuche für alle Clientknoten definieren. Wenn der Grenzwert überschritten wird, sperrt der Server den Knoten.
Kennwortlänge	Der Administrator kann eine Mindestlänge angeben.

Sitzungssicherheit

Die Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, -Verwaltungsclients und -Servern verwendet wird und mit dem Parameter SESSIONSECURITY festgelegt wird.

Der Parameter SESSIONSECURITY kann auf einen der folgenden Werte gesetzt werden:

- Mit dem Wert STRICT wird die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, -Knoten und -Administratoren durchgesetzt.
- Der Wert TRANSITIONAL gibt an, dass das vorhandene Kommunikationsprotokoll verwendet wird, wenn Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Wenn SESSIONSECURITY=TRANSITIONAL angegeben ist, werden strengere Sicherheitseinstellungen automatisch durchgesetzt, da höhere Versionen des TLS-Protokolls verwendet werden, wenn die Software auf Version 8.1.2 oder höher aktualisiert wird. Nachdem ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch in den Wert STRICT geändert und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder unter Verwendung früherer TLS-Protokolle authentifizieren.

Weitere Informationen zu den Werten für den Parameter SESSIONSECURITY enthalten die Beschreibungen der folgenden Befehle.

Tabelle 2. Befehle zum Festlegen des Parameters SESSIONSECURITY

Entität	Befehl
Clientknoten	• REGISTER NODE • UPDATE NODE
Administratoren	• REGISTER ADMIN • UPDATE ADMIN
Server	• DEFINE SERVER • UPDATE SERVER

Administratoren, die sich unter Verwendung des Befehls DSMADMC, des Befehls DSMC oder des Programms dsm authentifizieren, können sich nach der Authentifizierung unter Verwendung von Version 8.1.2 oder höher nicht unter Verwendung einer früheren Version authentifizieren. Die

folgenden Tipps liefern Informationen zur Behebung von Authentifizierungsproblemen für Administratoren:
Tipps:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die das Administratorkonto für die Anmeldung verwendet, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto über mehrere Systeme anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf jedem System installiert ist.
- Nachdem sich ein Administrator bei einem Server der Version 8.1.2 oder höher unter Verwendung eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich der Administrator nur auf Clients oder Servern authentifizieren, die Version 8.1.2 oder höher verwenden. Ein Administratorbefehl kann von jedem beliebigen System ausgegeben werden.
- Erstellen Sie, falls erforderlich, ein separates Administratorkonto, das nur mit Clients und Servern verwendet wird, die Software der Version 8.1.1 oder früher verwenden.

Setzen Sie die höchste Sicherheitsstufe für die Kommunikation mit dem IBM Spectrum Protect-Server durch, indem Sie sicherstellen, dass alle Knoten, Administratoren und Server die Sitzungssicherheit STRICT verwenden. Mithilfe des Befehls SELECT können Sie feststellen, welche Server, Knoten und Administratoren die Sitzungssicherheit TRANSITIONAL verwenden und für die Verwendung der Sitzungssicherheit STRICT aktualisiert werden sollten.

Zugehörige Tasks:
Kommunikation schützen

Administratoren verwalten

Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Administratoreinstellungen zu ändern.

Task	Prozedur

Administrator hinzufügen	Um einen Administrator, ADMIN1, mit Systemberechtigung hinzuzufügen und ein Kennwort anzugeben, führen Sie die folgenden Schritte aus:
	a. Registrieren Sie den Administrator und geben Sie Pa$#$twO als Kennwort an, indem Sie den folgenden Befehl ausgeben:
	`register admin admin1 Pa$#$twO`
	b. Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`

Administratorberechtigung ändern	Ändern Sie die Berechtigungsstufe für einen Administrator, ADMIN1.
	• Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`
	• Entziehen Sie dem Administrator die Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`revoke authority admin1 classes=system`

Administratoren entfernen	Entfernen Sie einen Administrator, ADMIN1, sodass er nicht mehr auf den IBM Spectrum Protect-Server zuzugreifen kann, indem Sie den folgenden Befehl ausgeben: `remove admin admin1`
Zugriff auf den Server vorübergehend verhindern	Sperren oder entsperren Sie einen Administrator, indem Sie den Befehl LOCK ADMIN bzw. UNLOCK ADMIN verwenden.

Kennwortanforderungen ändern

Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.

Informationen zu diesem Vorgang

Indem Sie die Kennwortauthentifizierung durchsetzen und Kennworteinschränkungen verwalten, können Sie Ihre Daten und Ihre Server vor möglichen Sicherheitsrisiken schützen.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Kennwortanforderungen für IBM Spectrum Protect-Server zu ändern.

Tabelle 1. Authentifizierungstasks für IBM Spectrum Protect-Server

Task	Prozedur
Grenzwert für ungültige Kennworteingabeversuche festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl ungültiger Versuche im Feld Grenzwert für ungültige Anmeldeversuche an. Der Standardwert bei der Installation ist 0.
Mindestlänge für Kennwörter festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl Zeichen im Feld Mindestlänge für Kennwort an.
Ablaufzeitraum für Kennwörter festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl Tage im Feld Allgemeine Kennwortablaufdauer an.
Kennwortauthentifizierung inaktivieren	Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer ein Kennwort eingeben, um auf den Server zugreifen zu können. Sie können die Kennwortauthentifizierung nur für Kennwörter inaktivieren, die mit dem Server (LOCAL) authentifiziert werden. Durch das Inaktivieren der Kennwortauthentifizierung erhöht sich das Sicherheitsrisiko für den Server.

Standardauthentifizierungsmethode festlegen	Geben Sie den Befehl SET DEFAULTAUTHENTICATION aus. Um beispielsweise den Server als die Standardauthentifizierungsmethode zu verwenden, geben Sie den folgenden Befehl aus:
	
	`set defaultauthentication local`
	
	Um einen Clientknoten für die Authentifizierung mit dem Server zu aktualisieren, schließen Sie `AUTHENTICATION=LOCAL` in den Befehl UPDATE NODE ein:
	
	`update node authentication=local`

Zugehörige Konzepte:

IBM Spectrum Protect-Benutzer mithilfe eines LDAP-Servers authentifizieren

Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1)

IBM Spectrum Protect auf dem System schützen

Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

Vorgehensweise

Stellen Sie sicher, dass nicht berechtigte Benutzer nicht auf die Verzeichnisse für die Serverdatenbank und die Serverinstanz zugreifen können. Behalten Sie die Zugriffseinstellungen für diese Verzeichnisse bei, die Sie während der Implementierung konfiguriert haben.

- Benutzerzugriff auf den Server einschränken
  Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.
- Zugriff über Porteinschränkungen einschränken
  Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

Benutzerzugriff auf den Server einschränken

Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Vorgehensweise

1. Nachdem Sie einen Administrator mit dem Befehl REGISTER ADMIN registriert haben, legen Sie die Berechtigungsstufe des Administrators mithilfe des Befehls GRANT AUTHORITY fest. Ausführliche Informationen zum Festlegen und Ändern der Berechtigung finden Sie in Administratoren verwalten.
2. Um die Berechtigung eines Administrators zur Ausführung bestimmter Tasks zu steuern, verwenden Sie die beiden folgenden Serveroptionen:
   a. Über die Serveroption QUERYAUTH können Sie die Berechtigungsstufe auswählen, die ein Administrator haben muss, um Befehle QUERY und SELECT ausgeben zu können. Standardmäßig ist keine Berechtigungsstufe erforderlich. Sie können die Anforderung in eine der Berechtigungsstufen, einschließlich Systemberechtigung, ändern.
   b. Über die Serveroption REQSYSAUTHOUTFILE können Sie angeben, dass Systemberechtigung für Befehle erforderlich ist, die zur Folge haben, dass der Server Daten in eine externe Datei schreibt. Standardmäßig ist für diese Befehle Systemberechtigung erforderlich.
3. Sie können die Datensicherung auf einem Clientknoten ausschließlich auf Rootbenutzer-IDs oder berechtigte Benutzer beschränken. Um beispielsweise Sicherungen auf die Rootbenutzer-ID zu beschränken, geben Sie den Befehl REGISTER NODE oder UPDATE NODE unter Angabe des Parameters BACKUPINITIATION=root aus:

   ```
   update node backupinitiation=root
   ```

Zugriff über Porteinschränkungen einschränken

Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

Informationen zu diesem Vorgang

Gegebenenfalls müssen Sie abhängig von Ihren Sicherheitsanforderungen den Zugriff auf bestimmte Server einschränken. Der IBM Spectrum Protect-Server kann so konfiguriert werden, dass er an vier TCP/IP-Ports empfangsbereit ist: zwei Ports, die für reguläre TCP/IP-Protokolle oder SSL-/TLS-Protokolle verwendet werden können, und zwei Ports, die nur für das SSL-/TLS-Protokoll verwendet werden können.

Vorgehensweise

Sie können die Serveroptionen wie in Tabelle 1 aufgeführt zur Angabe des erforderlichen Ports festlegen.

Tabelle 1. Serveroptionen und Portzugriff

Serveroption	Portzugriff
TCPPORT	Gibt die Nummer des Ports an, dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist 1500.
TCPADMINPORT	Gibt die Nummer des Ports an, an dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von anderen Sitzungen als Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist der Wert für TCPPORT. Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPPORT verwendet, zu trennen.
SSLTCPPORT	Gibt die SSL-TCP/-IP-Portadresse für einen Server an. Dieser Port ist nur für SSL-fähige Sitzungen empfangsbereit. Ein Standardwert für den Port ist nicht verfügbar.
SSLTCPADMINPORT	Gibt die Portadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen von SSL-fähigen Sitzungen wartet. Ein Standardwert für den Port ist nicht verfügbar. Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPPORT verwendet, zu trennen.

Zugehörige Verweise:
Planung des Firewallzugriffs

Server stoppen und starten

Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.

Vorbereitende Schritte

Um den IBM Spectrum Protect-Server stoppen und starten zu können, müssen Sie über System- oder Bedienerberechtigung verfügen.

- Server stoppen
  Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.
- Server für Verwaltungs- oder Rekonfigurationstasks starten
  Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

Server stoppen

Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

Informationen zu diesem Vorgang

Wenn Sie den Befehl HALT zum Stoppen des Servers ausgeben, werden die folgenden Aktionen ausgeführt:

- Alle Prozesse und Clientknotensitzungen werden abgebrochen.
- Alle aktuellen Transaktionen werden gestoppt. (Die Transaktionen werden rückgängig gemacht, wenn der Server erneut gestartet wird.)

Vorgehensweise

Um das System vorzubereiten und den Server zu stoppen, führen Sie die folgenden Schritte aus:

1. Verhindern Sie, dass neue Clientknotensitzungen gestartet werden, indem Sie den Befehl DISABLE SESSIONS ausgeben:

   ```
   disable sessions all
   ```

2. Bestimmen Sie, ob Clientknotensitzungen oder -prozesse aktiv sind, indem Sie die folgenden Schritte ausführen:
   a. Rufen Sie die Seite Übersicht im Operations Center auf, auf der im Bereich Aktivität die Gesamtzahl Prozesse und Sitzungen angezeigt wird, die derzeit aktiv sind. Wenn die Zahlen erheblich von den Zahlen abweichen, die normalerweise während Ihrer täglichen Speicherverwaltungsroutine angezeigt werden, überprüfen Sie mithilfe weiterer Statusanzeiger im Operations Center, ob ein Problem vorliegt.
   b. Zeigen Sie das Diagramm im Bereich Aktivität an, um den Umfang des Datenaustauschs im Netz für die folgenden Perioden zu vergleichen:
      - Die laufende Periode, d. h. die letzte 24-Stunden-Periode
      - Die vorherige Periode, d. h. die 24 Stunden vor der laufenden Periode

      Wenn das Diagramm für die vorherige Periode den erwarteten Umfang des Datenaustauschs darstellt, können deutliche Abweichungen in dem Diagramm für die laufende Periode auf ein Problem hindeuten.
   c. Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details. Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, rufen Sie mithilfe von Verwaltungsbefehlen Informationen zu Prozessen ab. Geben Sie den Befehl QUERY PROCESS aus, um Prozesse abzufragen; geben Sie den Befehl QUERY SESSION aus, um Informationen zu Sitzungen abzurufen.
3. Warten Sie, bis die Clientknotensitzungen abgeschlossen sind oder brechen Sie diese ab. Um Prozesse und Sitzungen abzubrechen, führen Sie die folgenden Schritte aus:
   - Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
   - Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
   - Klicken Sie auf Abbrechen.
   - Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, brechen Sie Sitzungen mithilfe von Verwaltungsbefehlen ab. Geben Sie den Befehl CANCEL SESSION aus, um eine Sitzung abzubrechen; geben Sie den Befehl CANCEL PROCESS aus, um Prozesse abzubrechen.
     Tipp: Wenn der Prozess, der abgebrochen werden soll, auf die Bereitstellung eines Banddatenträgers wartet, wird die Mountanforderung abgebrochen. Wenn Sie beispielsweise einen Befehl EXPORT, IMPORT oder MOVE DATA ausgeben, leitet der Befehl möglicherweise einen Prozess ein, der die Bereitstellung eines Banddatenträgers erfordert. Wenn jedoch ein Banddatenträger durch ein automatisiertes Speicherarchiv bereitgestellt wird, wird die Abbruchoperation unter Umständen erst

wirksam, wenn der Bereitstellungsprozess abgeschlossen ist. Abhängig von Ihrer Systemumgebung kann dies mehrere Minuten dauern.

4. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

```
halt
```

Server für Verwaltungs- oder Rekonfigurationstasks starten

Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

Informationen zu diesem Vorgang

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm DSMSERV mit dem Parameter MAINTENANCE ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.
Tipps:

- Sie müssen die Serveroptionsdatei, dsmserv.opt, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung, den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

Vorgehensweise

Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

```
dsmserv maintenance
```

Tipp: Informationen zum Anzeigen eines Ein Video zum Starten des Servers im Verwaltungsmodus kann über Server im Verwaltungsmodus starten angezeigt werden.

Nächste Schritte

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl HALT ausgeben:

```
halt
```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden. Führen Sie die Anweisungen für Ihr Betriebssystem aus:
   - AIX-BetriebssystemeServerinstanz starten
   - Linux-BetriebssystemeServerinstanz starten
   - Windows-BetriebssystemeServerinstanz starten

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

Durchführung eines Upgrades für den Server planen

Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.

Informationen zu diesem Vorgang

Beachten Sie diese Richtlinien:

- Bei der bevorzugten Methode erfolgt das Upgrade für den Server mithilfe des Installationsassistenten. Nachdem Sie den Assistenten gestartet haben, klicken Sie im Fenster IBM Installation Manager auf das Symbol zum Aktualisieren; klicken Sie nicht auf das Symbol zum Installieren oder Ändern!

- Wenn sowohl für die Serverkomponente als auch für die Operations Center-Komponente Upgrades verfügbar sind, wählen Sie die Kontrollkästchen aus, um das Upgrade für beide Komponenten durchzuführen.

Vorgehensweise

1. Überprüfen Sie die Liste der Fixpacks und vorläufigen Fixes. Siehe Technote 1239415.
2. Studieren Sie die Produktverbesserungen, die in der Readme-Datei beschrieben sind.
   Tipp: Wenn Sie die Installationspaketdatei von der IBM Spectrum Protect-Unterstützungssite abrufen, können Sie auch auf die Readme-Datei zugreifen.
3. Stellen Sie sicher, dass die Version, auf die das Upgrade für Ihren Server durchgeführt wird, mit anderen Komponenten, wie beispielsweise Speicheragenten und Speicherarchivclients, kompatibel ist. Siehe Technote 1302789.
4. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden. Siehe Technote 1053218.
5. Lesen Sie die Upgradeanweisungen. Stellen Sie sicher, dass Sie die Serverdatenbank, die Einheitenkonfigurationsinformationen und die Protokolldatei für Datenträger sichern.

Nächste Schritte

Um ein Fixpack oder einen vorläufigen Fix zu installieren, führen Sie die Anweisungen für Ihr Betriebssystem aus:

- AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
- Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
- Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren

Zugehörige Informationen:
Upgrade- und Umlagerungsprozess - Häufig gestellte Fragen

Vorbereitungen für einen Ausfall oder eine Systemaktualisierung

Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass Sie die regelmäßige Ausführung von Aktivitäten planen, um den Server zu verwalten und zu schützen.

Vorgehensweise

1. Brechen Sie Prozesse und Sitzungen, die aktiv sind, ab, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie im Operations Center auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
   b. Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
   c. Klicken Sie auf Abbrechen.
2. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

   ```
   halt
   ```

   Tipp: Sie können den Befehl HALT im Operations Center ausgeben, indem Sie den Mauszeiger über das Symbol für Einstellungen bewegen und auf Command Builder klicken. Wählen Sie dann den Server aus, geben Sie `halt` ein und drücken Sie die Eingabetaste.

Plan zur Wiederherstellung nach einem Katastrophenfall implementieren

Implementieren Sie eine Strategie zur Wiederherstellung nach einem Katastrophenfall, um Ihre Anwendungen in einem Katastrophenfall wiederherstellen und hohe Serververfügbarkeit sicherstellen zu können.

Informationen zu diesem Vorgang

Bestimmen Sie Ihre Anforderungen für die Wiederherstellung nach einem Katastrophenfall, indem Sie die Geschäftsprioritäten für die Clientknotenwiederherstellung und die Systeme, die zum Wiederherstellen von Daten verwendet werden, angeben und prüfen, ob Clientknoten über eine Verbindung zu einem Wiederherstellungsserver verfügen. Verwenden Sie zum Schützen von Daten Replikation und Speicherpoolschutz. Außerdem müssen Sie bestimmen, wie oft Verzeichniscontainerspeicherpools geschützt werden.

- Wiederherstellungsdrilloperationen ausführen
  Planen Sie Drilloperationen für die Wiederherstellung nach einem Katastrophenfall als Vorbereitung für Prüfungen, mit denen die Wiederherstellbarkeit des IBM Spectrum Protect-Servers bestätigt wird, und um sicherzustellen, dass nach einem Ausfall Daten zurückgeschrieben und Operationen wiederaufgenommen werden können. Mithilfe einer Drilloperation können Sie außerdem vor dem

Eintreten einer kritischen Situation sicherstellen, dass alle Daten zurückgeschrieben und Operationen wiederaufgenommen werden können.

Wiederherstellung nach einem Datenverlust oder Systemausfall

Mithilfe von IBM Spectrum Protect können Sie Daten wiederherstellen, die bei einem Katastrophenfall oder Systemausfall verloren gegangen sind. Sie können Verzeichniscontainerspeicherpools, Clientdaten und Datenbanken wiederherstellen.

Vorbereitende Schritte

Planen Sie Client- und Server-Workloads, um die beste Leistung für Ihre Speicherumgebung zu erzielen. Geben Sie die Befehle PROTECT STGPOOL und REPLICATE NODE im Rahmen des Zeitplans aus. Schützen Sie den Speicherpool vor dem Replizieren des Clientknotens. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch den Speicherpoolschutz repliziert werden, übersprungen und die Replikationsverarbeitungszeit wird somit reduziert.

Vorgehensweise

Verwenden Sie abhängig von der Komponente, die wiederhergestellt werden muss, die folgenden Wiederherstellungsmethoden.

Wiederherzustellende Komponente	Prozedur	Weitere Informationen
Verzeichniscontainerspeicherpool	Um Verzeichniscontainerspeicherpools wiederherzustellen, führen Sie die folgenden Schritte aus: a. Suchen Sie in dem Verzeichniscontainerspeicherpool nach beschädigten Datenbereichen, indem Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=SCANALL ausgeben. b. Reparieren Sie beschädigte Datenbereiche in dem Verzeichniscontainerspeicherpool mit dem Befehl REPAIR STGPOOL. Einschränkung: Sie können einen Speicherpool nur reparieren, wenn der Speicherpool geschützt wird. c. Entfernen Sie beschädigte Datenbereiche, indem Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED ausgeben.	Speicherpools reparieren

Wiederherzustellende Komponente	Prozedur	Weitere Informationen
Clientdaten	Voraussetzungen: • Der Quellenreplikationsserver, der Zielreplikationsserver und der Client müssen Version 7.1 oder höher haben. Wenn einer der Server eine frühere Version hat, wird die automatische Übernahme inaktiviert und Sie müssen die Übernahme manuell ausführen. Konfigurieren Sie den Client für die automatische Übernahme durch den Zielserver für die Datenwiederherstellung. Wenn der Client für die automatisierte Clientübernahme aktiviert wurde, können Sie die Daten mithilfe der Funktion für die automatische Übernahme wiederherstellen. Überprüfen Sie, ob die Option usereplicationfailover in der Clientoptionsdatei entweder nicht vorhanden ist oder auf `yes` gesetzt ist. Stellen Sie mithilfe der automatischen Übernahme Daten vom Zielserver wieder her, wenn der Quellenserver aufgrund eines Ausfalls nicht verfügbar ist. Tipp: • Geben Sie mit dem Befehl SET FAILOVERHLADDRESS die IP-Adresse für den Replikationsserver während der Übernahme an, wenn die Adresse nicht mit der IP-Adresse übereinstimmt, die für den Replikationsprozess angegeben ist.	• Beschädigte Daten aus einer replizierten Kopie wiederherstellen • SET FAILOVERHLADDRESS (Adresse höherer Ebene für Übernahme definieren)
Datenbank	Voraussetzungen: • Um die Datenbank nach einem Katastrophenfall zurückzuschreiben, muss eine Kopie der aktuellen Einheitenkonfigurationsdatei vorhanden sein. Die Einheitenkonfigurationsdatei kann nicht erneut erstellt werden. • Stellen Sie sicher, dass eine gesicherte Version der Datenbank vorhanden ist. Schreiben Sie die IBM Spectrum Protect-Datenbank mit dem neuesten Stand oder mit dem Stand eines bestimmten Zeitpunkts unter Verwendung des Serverdienstprogramms DSMSERV RESTORE DB zurück.	DSMSERV RESTORE DB (Datenbank zurückschreiben)

- Datenbank zurückschreiben
  Unter Umständen müssen Sie die IBM Spectrum Protect-Datenbank nach einem Katastrophenfall zurückschreiben. Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Zum Zurückschreiben der Datenbank benötigen Sie Datenträger mit einer Datenbankgesamt-, -teil- oder -momentaufnahmesicherung.
- Beschädigte Daten aus einer replizierten Kopie wiederherstellen
  Wenn ein Quellenreplikationsserver nicht verfügbar ist, können Sie beschädigte Daten aus einer replizierten Kopie, die auf dem Zielreplikationsserver gespeichert ist, wiederherstellen.
- Speicherpools reparieren
  Bei einer Katastrophe oder einem Systemausfall können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool reparieren.

Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
DSMSERV RESTORE DB (Datenbank zurückschreiben)

Datenbank zurückschreiben

Unter Umständen müssen Sie die IBM Spectrum Protect-Datenbank nach einem Katastrophenfall zurückschreiben. Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Zum Zurückschreiben der Datenbank benötigen Sie Datenträger mit einer Datenbankgesamt-, -teil- oder -momentaufnahmesicherung.

Vorbereitende Schritte

Wenn die Verzeichnisse für die Datenbank und das Wiederherstellungsprotokoll nicht mehr vorhanden sind, erstellen Sie diese erneut, bevor Sie das Serverdienstprogramm DSMSERV RESTORE DB verwenden. Verwenden Sie beispielsweise die folgenden Befehle:  AIX-Betriebssysteme
Linux-Betriebssysteme

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

 Windows-Betriebssysteme

```
mkdir e:\tsm\db001
mkdir f:\tsm\db001
mkdir g:\tsm\db001
mkdir h:\tsm\activelog
mkdir i:\tsm\archlog
mkdir j:\tsm\archfaillog
```

Einschränkungen:

- Um die Datenbank mit der neuesten Version zurückzuschreiben, müssen Sie das Archivprotokollverzeichnis lokalisieren. Wenn Sie das Verzeichnis nicht lokalisieren können, kann die Datenbank nur mit dem Stand eines bestimmten Zeitpunkts zurückgeschrieben werden.
- Sie können Secure Sockets Layer (SSL) nicht für Datenbankzurückschreibungsoperationen verwenden.
- Wenn der Release-Level der Datenbanksicherung und der Release-Level des Servers, für den die Zurückschreibung erfolgt, unterschiedlich sind, können Sie die Serverdatenbank nicht zurückschreiben. Wenn Sie beispielsweise einen Server der Version 8.1 verwenden und versuchen, eine Datenbank der Version 7.1 zurückzuschreiben, tritt ein Fehler auf.

Informationen zu diesem Vorgang

Operationen für die Zurückschreibung nach Zeitpunkt werden normalerweise bei der Wiederherstellung nach einem Katastrophenfall oder zum Entfernen der Auswirkungen von Fehlern verwendet, die Inkonsistenzen in der Datenbank zur Folge haben können. Um die Datenbank mit dem Stand wiederherzustellen, den sie zu dem Zeitpunkt hatte, zu dem sie verloren ging, stellen Sie die Datenbank mit der neuesten Version wieder her.

Vorgehensweise

Verwenden Sie das Serverdienstprogramm DSMSERV RESTORE DB, um die Datenbank zurückzuschreiben. Wählen Sie abhängig von der Version der Datenbank, die zurückgeschrieben werden soll, eine der folgenden Methoden aus:

- Zurückschreiben einer Datenbank mit der neuesten Version. Verwenden Sie beispielsweise den folgenden Befehl:

  ```
  dsmserv restore db
  ```

- Zurückschreiben einer Datenbank mit dem Stand eines bestimmten Zeitpunkts. Um beispielsweise die Datenbank mit einer Sicherungsserie zurückzuschreiben, die am 19. April 2015 erstellt wurde, verwenden Sie den folgenden Befehl:

  ```
  dsmserv restore db todate=04/19/2015
  ```

Nächste Schritte

Wenn Sie die Datenbank zurückgeschrieben haben und Verzeichniscontainerspeicherpools auf dem Server vorhanden sind, müssen Sie Inkonsistenzen zwischen der Datenbank und dem Dateisystem ermitteln.

1. Wenn Sie die Datenbank mit dem Stand eines bestimmten Zeitpunkts zurückgeschrieben haben und die Wiederverwendung des Verzeichniscontainerspeicherpools nicht verzögert wurde, müssen Sie alle Container prüfen. Um alle Container zu prüfen, geben Sie den folgenden Befehl aus:

   ```
   audit container stgpool
   ```

2. Wenn der Server keine Container auf dem System identifizieren kann, führen Sie die folgenden Schritte aus, um eine Liste der Container anzuzeigen:
    a. Geben Sie über einen Verwaltungsclient den folgenden Befehl aus:

    ```
    select container_name from containers
    ```

    b. Geben Sie für das Dateisystem den folgenden Befehl für das Speicherpoolverzeichnis auf dem Quellenserver aus:
    Tipp: Das Speicherpoolverzeichnis wird in der Befehlsausgabe angezeigt:
     AIX-BetriebssystemeLinux-Betriebssysteme

    ```
    [Root@Quelle]$ ls -l
    ```

     Windows-Betriebssysteme

    ```
    c:\Quellenspeicherpoolverz>Verz
    ```

    c. Vergleichen Sie die für das Dateisystem und den Server aufgelisteten Container.
    d. Geben Sie den Befehl AUDIT CONTAINER unter Angabe des Containers aus, der in der Serverausgabe fehlt. Geben Sie den Parameter ACTION=REMOVEDAMAGED an, um den Container zu löschen.
    e. Um sicherzustellen, dass die Container im Dateisystem gelöscht wurden, überprüfen Sie die angezeigten Nachrichten.

Zugehörige Tasks:
Clientknotendaten nach einer Datenbankzurückschreibung replizieren (Version 7.1.1)
Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
DSMSERV RESTORE DB (Datenbank zurückschreiben)

Beschädigte Daten aus einer replizierten Kopie wiederherstellen

Wenn ein Quellenreplikationsserver nicht verfügbar ist, können Sie beschädigte Daten aus einer replizierten Kopie, die auf dem Zielreplikationsserver gespeichert ist, wiederherstellen.

Vorbereitende Schritte

Der Servername, den Sie im Befehl SET REPLSERVER angeben, muss mit dem Namen einer vorhandenen Serverdefinition übereinstimmen. Außerdem muss es sich um den Namen des Servers handeln, der als Zielreplikationsserver verwendet werden soll. Wenn der in diesem Befehl angegebene Servername nicht mit dem Servernamen einer vorhandenen Serverdefinition übereinstimmt, schlägt der Befehl fehl.
Tipp:

- Gehen Sie beim Ändern oder Entfernen eines Zielreplikationsservers mit Sorgfalt vor. Wenn Sie einen Zielreplikationsserver ändern, werden Clientknotendaten, die repliziert werden, an einen anderen Zielreplikationsserver gesendet. Wenn Sie einen Zielreplikationsserver entfernen, werden Clientknotendaten nicht repliziert.

Vorgehensweise

1. Überprüfen Sie den Replikationsstatus der Daten auf dem Zielserver. Der Replikationsstatus gibt an, ob die neueste Sicherung auf den sekundären Server repliziert wurde.
2. Schreiben Sie Daten von einem Zielreplikationsserver zurück, indem Sie den Quellenreplikationsserver als Zielreplikationsserver festlegen. Wenn beispielsweise der Quellenreplikationsserver als Zielreplikationsserver server1 festgelegt werden soll, geben Sie den folgenden Befehl aus:

    ```
    set replserver server1
    ```

Nächste Schritte

Wenn Sie die IBM Spectrum Protect-Datenbank auf einen Quellenreplikationsserver zurückschreiben, wird die Replikation automatisch inaktiviert. Bevor Sie die Replikation erneut aktivieren, müssen Sie bestimmen, ob Kopien der Daten, die sich auf dem Zielreplikationsserver befinden, benötigt werden.

Zugehörige Tasks:
Clientknotendaten nach einer Datenbankzurückschreibung replizieren (Version 7.1.1)

Speicherpools reparieren

Bei einer Katastrophe oder einem Systemausfall können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool reparieren.

Vorbereitende Schritte

Identifizieren Sie Inkonsistenzen zwischen der Datenbank und dem Verzeichniscontainerspeicherpool mit dem Befehl AUDIT CONTAINER. Indem Sie beschädigte Datenbereiche im Verzeichniscontainerspeicherpool identifizieren, können Sie die zu reparierenden Datenbereiche bestimmen.

Bevor Sie einen Speicherpool reparieren können, müssen Sie mithilfe des Befehls PROTECT STGPOOL sicherstellen, dass der Speicherpool geschützt wird.

Vorgehensweise

1. Verwenden Sie zum Reparieren eines Verzeichniscontainerspeicherpools den Befehl REPAIR STGPOOL. Um beispielsweise den Speicherpool STGPOOL1 zu reparieren, geben Sie den folgenden Befehl aus:

   ```
   repair stgpool stgpool1
   ```

2. Wenn der beschädigte Speicherpool im Befehl PROTECT STGPOOL für einen oder mehrere Quellenspeicherpools als Zielspeicherpool angegeben ist, geben Sie den Befehl PROTECT STGPOOL für alle Quellenspeicherpools aus.
3. Um sicherzustellen, dass alle beschädigten Daten mithilfe anderer Quellenspeicherpools identifiziert und repariert werden, geben Sie den Befehl PROTECT STGPOOL erneut für alle Quellenspeicherpools unter Angabe des Parameters FORCERECONCILE=YES aus.
4. Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus.
5. Wenn es sich bei dem beschädigten Speicherpool um einen Zielspeicherpool für die Knotenreplikation von einem oder mehreren Quellenservern handelt, geben Sie den Befehl REPLICATE NODE erneut auf allen Quellenservern aus.
6. Geben Sie, nachdem die Beschädigung repariert wurde, den Befehl PROTECT STGPOOL aus, um sicherzustellen, dass der Speicherpool in einem anderen Verzeichniscontainerspeicherpool geschützt wird.

Nächste Schritte

Stellen Sie durch Ausgabe des Befehls QUERY DAMAGED sicher, dass keine beschädigten Datenbereiche in der Ausgabe angezeigt werden.
Zugehörige Verweise:
Daten reparieren und wiederherstellen
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool abfragen)
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)

Bandspeicherlösung

Diese Datenschutzlösung stellt Speicher für Banddatenträger bereit, eine flexible und kosteneffiziente Option für die langfristige Aufbewahrung von Daten.

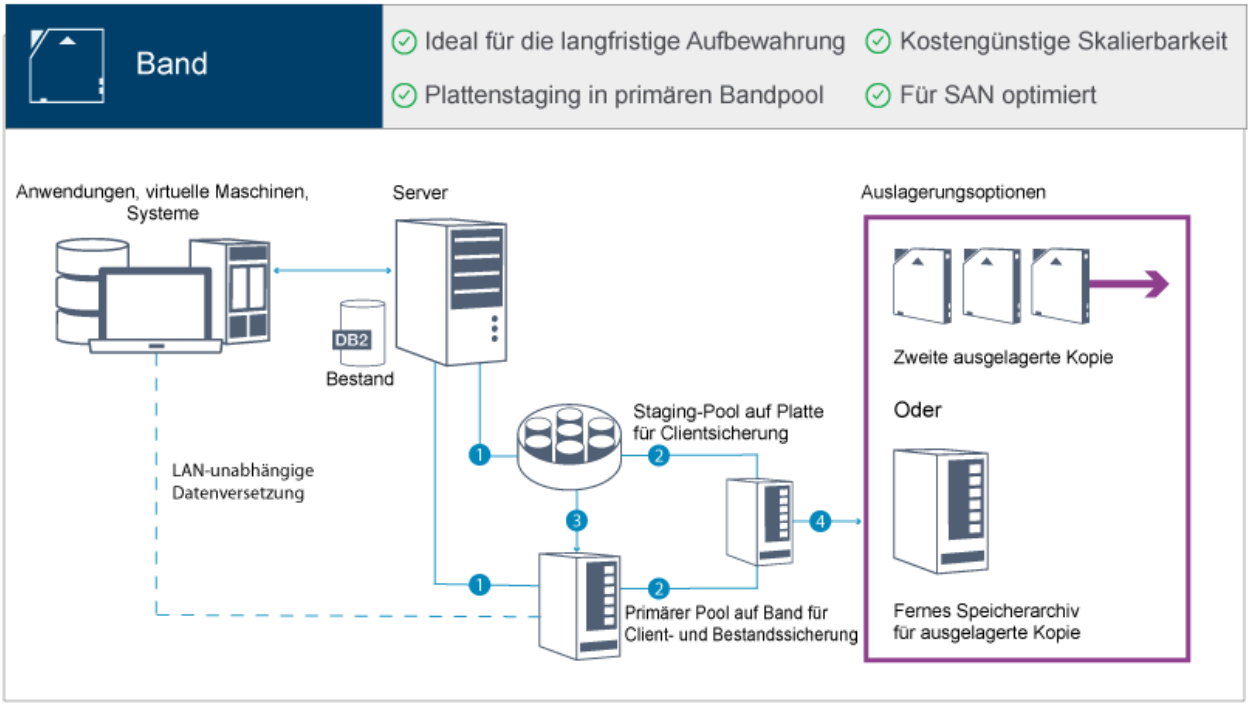
- Planung für eine bandbasierte Datenschutzlösung
  Führen Sie die Planung für eine Datenschutzlösung durch, die Platte-Platte-Band-Sicherungsoperationen und Sicherungsoperationen von Platte auf Band zur Optimierung des Speichers umfasst.
- Implementierung einer bandbasierten Datenschutzlösung
  Implementieren Sie die bandbasierte Lösung, die die Platte-Platte-Band-Sicherung und Plattenstaging zur Optimierung des Speichers verwendet. Durch die Implementierung der Bandspeicherlösung können Sie die langfristige Aufbewahrung von Daten ermöglichen und kostengünstige Skalierbarkeit erzielen.
- Bandspeicherlösung überwachen
  Überwachen Sie nach der Implementierung einer bandbasierten Lösung in IBM Spectrum Protect die Lösung, um ihre korrekte Funktionsweise sicherzustellen. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.
- Operationen für eine Bandspeicherlösung verwalten
  Verwenden Sie diese Informationen, um Operationen für eine Bandspeicherimplementierung für einen IBM Spectrum Protect-Server zu verwalten.

Planung für eine bandbasierte Datenschutzlösung

Führen Sie die Planung für eine Datenschutzlösung durch, die Platte-Platte-Band-Sicherungsoperationen und Sicherungsoperationen von Platte auf Band zur Optimierung des Speichers umfasst.

Planungsroadmap

Führen Sie die Planung für die Bandspeicherlösung durch, indem Sie das Architekturlayout in Abbildung 1 überprüfen und dann die Roadmap-Tasks ausführen, die auf die Abbildung folgen.
Abbildung 1. Bandspeicherlösung



Bei dieser Datenschutzkonfiguration verwendet der Server sowohl Platten- als auch Bandspeicherhardware. Es wird Speicherpoolstaging verwendet, bei dem Clientdaten anfänglich in Plattenspeicherpools gespeichert und dann später in Bandspeicherpools umgelagert werden. Für die Wiederherstellung nach einem Katastrophenfall können Banddatenträger an einem anderen Standort gespeichert werden. Auslagerungsoptionen umfassen den physischen Transport einer zweiten Kopie an einen anderen Standort durch einen Kurier oder das Schützen von Kopien an einem anderen Standort durch elektronisches Vaulting in einem fernen Speicherarchiv.

Tipp: Die beschriebene Lösung umfasst keine Knotenreplikation. Wenn die Knotenreplikation jedoch zum Sichern eines Speicherpools von Platte auf Platte verwendet werden soll, müssen Sie sicherstellen, dass die Replikationsoperation abgeschlossen ist, bevor Daten von Platte auf Band umgelagert werden. Sie können die Knotenreplikation auch verwenden, um einen Speicherpool auf einer lokalen Bandeinheit in einem Kopienspeicherpool auf einer lokalen Bandeinheit zu sichern.
Um die Planung für eine bandbasierte Lösung durchzuführen, führen Sie die folgenden Tasks aus:

1. Erfüllen Sie die Systemvoraussetzungen für Hardware und Software.
2. Notieren Sie die Werte für Ihre Systemkonfiguration in den Arbeitsblättern zur Planung.
3. Führen Sie die Planung für den Plattenspeicher durch.
4. Führen Sie die Planung für den Bandspeicher durch.
5. Führen Sie die Planung für die Sicherheit durch.

Planungsvoraussetzungen für Bänder

Bevor Sie eine Bandspeicherlösung implementieren, lesen Sie die allgemeinen Richtlinien zu Systemvoraussetzungen. Legen Sie fest, ob Daten auf Platte und/oder Band gesichert werden sollen.

Netzbandbreite
: Das Netz muss über genügend Bandbreite für die erwarteten Datenübertragungen zwischen dem Client und dem Server sowie für die standortübergreifenden Zurückschreibungsoperationen verfügen, die für die Wiederherstellung nach einem Katastrophenfall erforderlich sind. Verwenden Sie ein Speicherbereichsnetz (SAN) für Datenübertragungen zwischen dem Server, Platteneinheiten und Bandeinheiten. Weitere Informationen finden Sie in Hardwarevoraussetzungen.

Datenumlagerung
: Lagern Sie täglich alle Daten von Platte auf Band um. Geben Sie die Einheitenklasse FILE für plattenbasierte Speicherpools an. Planen Sie die Umlagerung, um zu steuern, wann die Verarbeitung erfolgt. Um die automatische Umlagerung auf der Basis des Umlagerungsschwellenwerts zu verhindern, geben Sie den Wert 100 für den Parameter HIGHMIG und den Wert 0 für den Parameter LOWMIG an, wenn Sie den Befehl DEFINE STGPOOL ausgeben. Es müssen immer mindestens 20 % der Bandlaufwerke für Zurückschreibungsoperationen verfügbar bleiben. Um bis zu 80 % der verfügbaren Bandlaufwerke zu verwenden und den Durchsatz zu verbessern, geben Sie den Parameter MIGPROCESS an.
  Berücksichtigen Sie, abhängig vom Typ der Daten, die umgelagert werden, die folgenden Informationen:

  - Verwenden Sie Bänder, um Daten von Clients zu sichern, die über große Objekte, wie beispielsweise Datenbanken, verfügen.
    Tipp: Der Hersteller Ihres Bandlaufwerks kann Ihnen Auskunft über die Größe der Datenbank geben, die für das Schreiben auf Band geeignet ist.
  - Verwenden Sie Platten, um Daten von Clients zu sichern, die über kleinere Objekte verfügen.

- Um Daten direkt auf Band zu sichern, verwenden Sie die LAN-unabhängige Datenversetzung. Weitere Informationen finden Sie in LAN-unabhängige Datenversetzung konfigurieren.
- Sichern Sie keine virtuellen Maschinen auf Band. Verwenden Sie einen separaten plattenbasierten Speicherpool, der nicht in einen bandbasierten Speicherpool umgelagert wird. Weitere Informationen zur Unterstützung virtueller Maschinen finden Sie in Technote 1239546.

Speicherpoolkapazität
: Stellen Sie sicher, dass immer genügend Speicherpoolkapazität für 2 Tage mit Clientsicherungen und ein Puffer von 20 % verfügbar ist. Möglicherweise müssen Sie Gesamtsicherungen für einige Tage planen, um sicherzustellen, dass genügend Speicherbereich im Speicherpool vorhanden ist.

Bandlaufwerk
: Lesen Sie die Herstellerspezifikationen und schätzen Sie die Kapazität eines Bandlaufwerks. Bestimmen Sie die Größe des Speicherbereichs, der für Sicherungs- und Umlagerungsoperationen erforderlich ist. Reservieren Sie 20 % der Bandlaufwerke für Zurückschreibungsoperationen.

Zugehörige Verweise:
MIGRATE STGPOOL (Speicherpool in den nächsten Speicherpool umlagern)

Systemvoraussetzungen für eine bandbasierte Lösung

Hardware- und Softwarevoraussetzungen werden für eine bandbasierte Speicherlösung mit einer Datenaufnahmerate von 14 TB pro Stunde bereitgestellt.

Lesen Sie die Informationen, um die Hardware- und Softwarevoraussetzungen für Ihre Speicherumgebung zu bestimmen. Unter Umständen müssen Sie auf der Basis Ihrer Systemgröße Anpassungen vornehmen.

- Hardwarevoraussetzungen
  Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.
- Softwarevoraussetzungen
  Die Dokumentation für die bandbasierte IBM Spectrum Protect-Lösung umfasst Installations- und Konfigurationstasks für IBM® AIX-, Linux- und Microsoft Windows-Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

Hardwarevoraussetzungen

Hardwarevoraussetzungen für Ihre IBM Spectrum Protect-Lösung basieren auf der Systemgröße. Wählen Sie funktional entsprechende oder bessere Komponenten als die aufgelisteten aus, um optimale Leistung für Ihre Umgebung zu gewährleisten.

Weitere Informationen zur Planung für Platteneinheiten finden Sie in Planung für Plattenspeicher.

Weitere Informationen zur Planung für Bandeinheiten finden Sie in Planung für Bandspeicher.

Die folgende Tabelle enthält Hardwaremindestvoraussetzungen für den Server und Speicher. Wenn Sie logische Partitionen (LPARs) oder Arbeitspartitionen (WPARs) verwenden, passen Sie die Netzvoraussetzungen an, um den Partitionsgrößen Rechnung zu tragen. Die Zahlen in der Tabelle basieren auf einer Datenaufnahmerate von 14 TB pro Stunde.

Hardwarekomponente	**Systemvoraussetzungen**
Serverprozessor	AIX-Betriebssysteme8 Prozessorkerne, 3,42 GHz oder schneller Verwenden Sie beispielsweise einen POWER8-prozessorbasierten Server. Linux-Betriebssysteme Windows-Betriebssysteme16 Prozessorkerne, 2,0 GHz oder schneller Verwenden Sie beispielsweise einen Intel Xeon-Prozessor.
Serverspeicher	64 GB Arbeitsspeicher.
Netz	Gemäß der folgenden Größe werden etwa 14 TB Daten pro Stunde verwaltet: • 10 Gb Ethernet (mindestens vier Ports) • 8 Gb Fibre Channel-Adapter (mindestens vier Ports) Die Anzahl Ports ist vom Prozentsatz der täglichen Datenaufnahme in Plattenspeicherpools gegenüber Bandspeicher abhängig. Verwenden Sie separate Fibre Channel-Adapter für Band- und Plattendaten.

Hardwarekomponente	Systemvoraussetzungen

Speicher	Platte
	Geben Sie auf der Basis des Datenvolumens, das auf Platte geschrieben wird, die Anzahl Platten an, die erforderlich sind.
	
	Stellen Sie sicher, dass der Durchsatz der sequenziellen Ein-/Ausgabe des Speicherbereichsnetzes (SAN) mit dem Durchsatz der Ein-/Ausgabe für das Netz (siehe oben) übereinstimmt.
	
	Wenn Sie beispielsweise 10 TB Daten in einem 4-Stunden-Fenster sichern müssen, beträgt der Durchsatz ungefähr 700 MB pro Sekunde. In diesem Fall erfordert der Server ein Front-End-Netz (Pfad vom Client zum Server), das einen Mindestdurchsatz von 700 MB pro Sekunde unterstützt. Das Back-End-SAN (Pfad vom Server zur Speichereinheit) muss ebenfalls einen Mindestdurchsatz von 700 MB pro Sekunde unterstützen.
	
	Verwenden Sie zur Berechnung der erforderlichen Plattengeschwindigkeit die folgenden Formeln:
	
	`(Gesamtvolumen der täglichen Datenaufnahme –`
	`Volumen der täglichen Datenaufnahme direkt auf Band) ÷`
	`(Anzahl Stunden für tägliche Clientsicherungsoperationen)`
	`=Megabyte der Datenaufnahme auf Platte pro Stunde`
	
	`(Megabyte der Datenaufnahme auf Platte pro Stunde) ÷`
	`(3600 Sekunden pro Stunde) =`
	`Megabyte der Datenaufnahme pro Sekunde,`
	`die von der Plattentechnologie unterstützt werden müssen`
	
	Band
	Wählen Sie die Bandtechnologie aus, die für Ihre Geschäftsanforderungen am besten geeignet ist. Verwenden Sie beispielsweise IBM Linear Tape-Open-Bandlaufwerke (LTO-Bandlaufwerke) oder IBM TS1150-Bandlaufwerke. Stellen Sie sicher, dass genügend Mountpunkte für Clientsicherungsoperationen und für die Umlagerung vorhanden sind. Weitere Informationen zur Planung für Bandspeicher finden Sie in Planung für Bandspeicher. Eine Liste der unterstützten Bandeinheiten finden Sie im IBM® Support Portal for IBM Spectrum Protect.
	Tipp: Um die Datenversetzung zu optimieren, verwenden Sie die LAN-unabhängige Datenversetzung.

SAN-E/A-Adapter	Trennen Sie die Platten- und Bandein-/ausgabe voneinander. Weitere Informationen zum Auswählen eines Adapters finden Sie in der Dokumentation für Brocade-Hardwareprodukte und für IBM Storwize-Speicherlösungen. Platte Verwenden Sie mindestens zwei Adapter. Band Verwenden Sie mindestens zwei Adapter.

Speicherbedarf für das Operations Center schätzen

Hardwarevoraussetzungen für das Operations Center sind mit Ausnahme des Speicherbereichs für die Datenbank und das Archivprotokoll (Bestand), den das Operations Center zum Speichern von Datensätzen für verwaltete Clients verwendet, in die vorherige Tabelle eingeschlossen.

Wenn Sie nicht planen, das Operations Center auf demselben System wie den IBM Spectrum Protect-Server zu installieren, können Sie die Systemanforderungen separat schätzen. Informationen zum Berechnen der Systemanforderungen für das Operations Center enthält die Technote 1641684 für die Berechnungsfunktion der Systemanforderungen.

Die Verwaltung des Operations Center auf dem IBM Spectrum Protect-Server stellt eine Workload dar, die zusätzlichen Speicherbereich für Datenbankoperationen auf dem Hub-Server und allen Peripherieservern erfordert. Der Speicherbedarf auf dem Hub-Server für das Archivprotokoll ist höher, wenn der Hub-Server einen oder mehrere Peripherieserver überwacht. Lesen Sie die folgenden Richtlinien, um schätzen zu können, wie viel Speicherbereich Ihr IBM Spectrum Protect-Server erfordert.

Speicherbereich in der Datenbank für das Operations Center
: Das Operations Center benötigt ungefähr 4,4 GB Speicherbereich in der Datenbank pro 1000 Clients, die auf diesem Server überwacht werden. Diese Berechnung gilt sowohl für Hub-Server als auch für Peripherieserver in einer Konfiguration.
Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1000 Clients. Bei dieser Konfiguration sind insgesamt 5000 Clients auf den vier Servern vorhanden. Jeder der Peripherieserver erfordert 4,4 GB Speicherbereich in der Datenbank. Bei Peripherieservern der IBM Spectrum Protect Version 8.1.2 oder höher erfordert der Hub-Server 8,8 GB Speicherbereich in der Datenbank allein für die Überwachung seiner 2000 Clients:

```
(4,4 GB x 2) = 8,8 GB
```

Speicherbereich in der Datenbank für verwaltete Daten
: *Verwaltete Daten* ist das Datenvolumen, das geschützt wird, einschließlich des Datenvolumens aller aufbewahrten Versionen.

- Bei Clienttypen, die immer inkrementelle Sicherungen ausführen, kann die folgende Formel zum Schätzen des Gesamtvolumens der verwalteten Daten verwendet werden:

  ```
  Front-End-Daten + (Front-End-Daten * Änderungsrate *
  (Aufbewahrungszeitraum - 1))
  ```

  Wenn Sie beispielsweise 100 TB Front-End-Daten sichern, einen Aufbewahrungszeitraum von 30 Tagen verwenden und eine Änderungsrate von 5 % haben, berechnen Sie das Gesamtvolumen der verwalteten Daten wie folgt:

  ```
  100 TB + (100 TB × 0,05 × (30-1)) = 245 TB Gesamtvolumen der
                                      verwalteten Daten
  ```

- Bei Clienttypen, die täglich Gesamtsicherungen ausführen, kann die folgende Formel zum Schätzen des Gesamtvolumens der verwalteten Daten verwendet werden:

  ```
  Front-End-Daten × Aufbewahrungszeitraum × (1 + Änderungsrate)
  ```

  Wenn Sie beispielsweise 10 TB Front-End-Daten sichern, einen Aufbewahrungszeitraum von 30 Tagen verwenden und eine Änderungsrate von 3 % haben, berechnen Sie das Gesamtvolumen der verwalteten Daten wie folgt:

  ```
  10 TB × 30 × (1 + 0,03) = 309 TB Gesamtvolumen der verwalteten Daten
  ```

  Unstrukturierte Daten; durchschnittliche Objektgröße: 4 MB

  Strukturierte Daten; durchschnittliche Objektgröße: 128 MB

  Unstrukturierte Daten; Anzahl Objekte =

  ```
  (245 TB × 1024 × 1024) / 4 MB = 64225280
  ```

  Strukturierte Daten; Anzahl Objekte =

  ```
  (309 TB × 1024 × 1024) / 128 MB = 2531328
  ```

  Gesamtzahl Objekte: 66756608

  Kosten der verwalteten Daten (1 KB pro Objekt) =

  ```
  (66756608 KB) / (1024 × 1024) = 63,66 GB
  ```

  Planen Sie 20 % zusätzlichen Speicherbereich ein, damit Datenbanksysteme nicht 100 % ihrer Kapazität nutzen:

  ```
  Gesamtbedarf des physischen Speicherbereichs in der Datenbank =
  (Speicherbereich für verwaltete Daten + Speicherbereich für das
  Operations Center) × (1,20)
  ```

  In diesem Beispiel würden Sie den Speicherbereich unter Verwendung der folgenden Zahlen berechnen:

  ```
  (66,33 GB + 8,4 GB) × 1,20 = 76,41 GB
  ```

Speicherbereich für das Archivprotokoll

Das Operations Center verwendet alle 24 Stunden ungefähr 18 GB Speicherbereich für das Archivprotokoll pro Server für jeweils 1000 Clients, die auf diesem Server überwacht werden. Darüber hinaus wird für jeweils 1000 Clients, die auf Peripherieservern überwacht werden, zusätzlicher Speicherbereich für das Archivprotokoll auf dem Hub-Server benötigt. Für Peripherieserver der Version 8.1.2 oder höher beträgt dieses zusätzliche Volumen 1,2 GB Speicherbereich für das Archivprotokoll auf dem Hub-Server pro 100 Clients, die alle 24 Stunden überwacht werden.

Angenommen, ein Hub-Server überwacht 2000 Clients und verwaltet außerdem drei Peripherieserver mit jeweils 1000 Clients. Bei dieser Konfiguration sind insgesamt 5000 Clients auf den vier Servern vorhanden. Sie können den Speicherbereich für das Archivprotokoll für den Hub-Server mithilfe der folgenden Formel berechnen:

```
((18 GB x 2) + (1,2 GB x 3)) = 39,6 GB Speicherbereich für das Archivprotokoll
```

Diese Schätzungen basieren auf dem Standardintervall von 5 Minuten zur Erfassung von Statusdaten. Wenn Sie das Erfassungsintervall von einmal alle 5 Minuten auf einmal alle 3 Minuten reduzieren, erhöht sich der Speicherbedarf. Die folgenden Beispiele zeigen die ungefähre Erhöhung des Protokollspeicherbedarfs bei einem Erfassungsintervall von einmal alle 3 Minuten für eine Konfiguration, in der Peripherieserver der Version 8.1.2 oder höher überwacht werden:

- Hub-Server: im Bereich von 39,6 GB bis 66 GB
- Jeder Peripherieserver: im Bereich von 18 GB bis 30 GB

Ordnen Sie Speicherbereich für das Archivprotokoll zu, damit das Operations Center ohne Auswirkungen auf Serveroperationen unterstützt werden kann.

Softwarevoraussetzungen

Die Dokumentation für die bandbasierte IBM Spectrum Protect-Lösung umfasst Installations- und Konfigurationstasks für IBM® AIX-, Linux- und Microsoft Windows-Betriebssysteme. Die aufgelisteten Softwaremindestvoraussetzungen müssen erfüllt sein.

Informationen zu den Softwarevoraussetzungen für IBM lin_tape-Einheitentreiber finden Sie in der Veröffentlichung IBM Tape Device Drivers Installation and User's Guide.

AIX-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	IBM AIX 7.1 Weitere Informationen zu Betriebssystemvoraussetzungen finden Sie in AIX: Systemmindestvoraussetzungen für AIX-Systeme.
Dienstprogramm gunzip	Das Dienstprogramm gunzip muss auf Ihrem System verfügbar sein, bevor Sie die Installation oder das Upgrade für den IBM Spectrum Protect-Server ausführen. Stellen Sie sicher, dass das Dienstprogramm gunzip installiert ist und der Pfad zu diesem Dienstprogramm in der Umgebungsvariablen PATH definiert ist.
Dateisystemtyp	JFS2-Dateisysteme AIX-Systeme können ein großes Volumen an Dateisystemdaten zwischenspeichern, wodurch der Speicherplatz, der für Server- und IBM DB2-Prozesse erforderlich ist, reduziert werden kann. Um beim AIX-Server eine Auslagerung zu verhindern, verwenden Sie die Mountoption rbrw für das JFS2-Dateisystem. Für den Dateisystemcache wird weniger Speicher verwendet und für IBM Spectrum Protect ist mehr Speicher verfügbar. Verwenden Sie nicht die Mountoptionen für Dateisysteme, gleichzeitige E/A (CIO = Concurrent I/O) und direkte E/A (DIO = Direct I/O) für Dateisysteme, die die IBM Spectrum Protect-Datenbank, Protokolle oder Speicherpooldatenträger enthalten. Diese Optionen können eine Leistungsverschlechterung vieler Serveroperationen zur Folge haben. IBM Spectrum Protect und DB2 können, wenn dies von Vorteil ist, weiterhin DIO verwenden, IBM Spectrum Protect erfordert die Mountoptionen jedoch nicht, um die Vorteile dieser Verfahren selektiv nutzen zu können.
Andere Software	Korn-Shell (ksh)

Linux-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Red Hat Enterprise Linux 7 (x86_64)
Bibliotheken	GNU C-Bibliotheken, Version 2.3.3-98.38 oder höher, die auf dem IBM Spectrum Protect-System installiert sind. Red Hat Enterprise Linux-Server: • libaio • libstdc++.so.6 (32-Bit- und 64-Bit-Pakete sind erforderlich) • numactl.x86_64
Dateisystemtyp	Formatieren Sie datenbankbezogene Dateisysteme mit ext3 oder ext4. Verwenden Sie für speicherpoolbezogene Dateisysteme XFS.
Andere Software	Korn-Shell (ksh)

Windows-Systeme

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Microsoft Windows Server 2012 R2 (64-Bit) oder Windows Server 2016
Dateisystemtyp	NTFS
Andere Software	Windows 2012 R2 oder Windows 2016 mit .NET Framework 3.5 ist installiert und aktiviert. Die folgenden Benutzerkontensteuerungsrichtlinien müssen inaktiviert sein: • Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto • Benutzerkontensteuerung: Alle Administratoren im Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen

Arbeitsblätter zur Planung

Verwenden Sie die Arbeitsblätter zur Planung für die Aufzeichnung von Werten, die Sie bei der Konfiguration Ihres Systems und bei der Konfiguration des IBM Spectrum Protect-Servers verwenden. Verwenden Sie die Best-Practice-Standardwerte, die in den Arbeitsblättern aufgeführt sind.

Jedes Arbeitsblatt unterstützt Sie bei den Vorbereitungen für unterschiedliche Teile der Systemkonfiguration mithilfe der Best-Practice-Werte:

Vorkonfiguration des Serversystems
: Führen Sie mithilfe der Arbeitsblätter zur Vorkonfiguration die Planung für die Dateisysteme und Verzeichnisse aus, die erstellt werden sollen, wenn Sie während der Systemkonfiguration Dateisysteme für IBM Spectrum Protect konfigurieren. Alle Verzeichnisse, die Sie für den Server erstellen, müssen leer sein.

Serverkonfiguration
: Verwenden Sie die Arbeitsblätter zur Konfiguration, wenn Sie den Server konfigurieren. Für die meisten Elemente werden Standardwerte vorgeschlagen; andernfalls ist ein entsprechender Hinweis vorhanden.

Tabelle 1. Arbeitsblatt für die Vorkonfiguration eines Serversystems

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Weitere Informationen
TCP/IP-Portadresse für die Kommunikation mit dem Server	1500		Nicht zutreffend	Stellen Sie sicher, dass dieser Port verfügbar ist, wenn Sie das Betriebssystem installieren und konfigurieren. Die Portnummer kann eine Zahl zwischen 1024 und 32767 sein.
Verzeichnis für die Serverinstanz	AIX-Betriebssysteme Linux-Betriebssysteme /home/tsminst1/tsminst1 Windows-Betriebssysteme C:\tsminst1		AIX-Betriebssysteme50 GB Linux-Betriebssysteme Windows-Betriebssysteme25 GB	Wenn Sie den Standardwert für das Serverinstanzverzeichnis in einen anderen Wert ändern, ändern Sie auch den Wert für den DB2-Instanzeigner in Tabelle 2.
Verzeichnis für Serverinstallation	• AIX-Betriebssysteme Linux-Betriebssysteme/ • Windows-BetriebssystemeC:		AIX-Betriebssysteme Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB Linux-Betriebssysteme Windows-Betriebssysteme Mindestspeicherbereich, der für das Verzeichnis erforderlich ist: 30 GB	
Verzeichnis für Serverinstallation	/usr		AIX-Betriebssysteme Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	AIX-Betriebssysteme/var		AIX-Betriebssysteme Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	AIX-Betriebssysteme/tmp		AIX-Betriebssysteme Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 5 GB	
Verzeichnis für Serverinstallation	AIX-Betriebssysteme/opt		AIX-Betriebssysteme Verfügbarer Speicherbereich, der für das Verzeichnis erforderlich ist: 10 GB	
Verzeichnis für die aktive Protokolldatei	AIX-Betriebssysteme Linux-Betriebssysteme /tsminst1/TSMalog Windows-Betriebssysteme C:\tsminst1\TSMalog		128 GB	Wenn Sie die aktive Protokolldatei während der Erstkonfiguration des Servers erstellen, setzen Sie die Größe auf 128 GB.

Element	Standardwert	Eigener Wert	Minimale Verzeichnisgröße	Weitere Informationen
Verzeichnis für das Archivprotokoll	AIX-Betriebssysteme Linux-Betriebssysteme /tsminst1/TSMarchlog Windows-Betriebssysteme C:\tsminst1\TSMarchlog		3 TB	
Verzeichnisse für die Datenbank	AIX-Betriebssysteme Linux-Betriebssysteme /tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 Windows-Betriebssysteme C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03		Anweisungen zum Berechnen des Speicherbedarfs finden Sie in Hardwarevoraussetzungen.	Erstellen Sie vier Dateisysteme für die Datenbank.
Verzeichnisse für Speicher	AIX-Betriebssysteme Linux-Betriebssysteme /tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ... Windows-Betriebssysteme C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Ermitteln Sie die minimale Gesamtkapazität für alle Verzeichnisse mithilfe der folgenden Berechnung: `Prozentsatz der täglich aufgenommenen Daten, die auf Platte geschrieben werden, + 20% = Minimale Gesamtkapazität`	Die bevorzugte Methode ist die Definition mindestens eines Verzeichnisses für jede Bandeinheit.

Tabelle 2. Arbeitsblatt für die Konfiguration von IBM Spectrum Protect

Element	Standardwert	Eigener Wert	Weitere Informationen
DB2-Instanzeigner	tsminst1		Wenn Sie den Standardwert für das Serverinstanzverzeichnis in Tabelle 1 in einen anderen Wert geändert haben, ändern Sie auch den Wert für den DB2-Instanzeigner.
Kennwort des DB2-Instanzeigners	AIX-Betriebssysteme Linux-Betriebssystemepassw0rd Windows-Betriebssysteme pAssW0rd		Wählen Sie für das Kennwort des Instanzeigners einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Primärgruppe für den DB2-Instanzeigner	AIX-Betriebssysteme Linux-Betriebssystemetsmsrvrs		
Servername	Der Standardwert für den Servernamen ist der Systemhostname.		
Serverkennwort	passw0rd		Wählen Sie für das Serverkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.
Administrator-ID: Benutzer-ID für die Serverinstanz	admin		
Kennwort für die Administrator-ID	passw0rd		Wählen Sie für das Administratorkennwort einen anderen Wert als den Standardwert aus. Sie müssen diesen Wert an einem sicheren Ort aufbewahren.

Element	Standardwert	Eigener Wert	Weitere Informationen
Startzeit des Zeitplans	23:00		Die standardmäßige Startzeit des Zeitplans gibt den Anfang der Client-Workload-Phase an, die sich in erster Linie auf die Clientsicherungs- und -archivierungsaktivitäten bezieht. Während der Client-Workload-Phase werden Clientoperationen durch Serverressourcen unterstützt. Normalerweise werden diese Operationen während des nächtlichen Zeitplanfensters ausgeführt. Zeitpläne für Serververwaltungsoperationen beginnen gemäß Definition 10 Stunden nach dem Start des Fensters zum Durchführen von Clientsicherungen. In diesem Handbuch wird 23:00 Uhr als Startzeit für Clientsicherungsoperationen vorgeschlagen.

Tabelle 3. Arbeitsblatt für die Bandkonfiguration

Element	Standardwert	Eigener Wert	Weitere Informationen
Dateien für automatische Einheiten	IBM® Einheiten mit einem IBM Bandeinheitentreiber: • AIX-Betriebssysteme /dev/smcX • Linux-Betriebssysteme /dev/IBMchangerX • Windows-Betriebssysteme ChangerX Einheiten eines anderen Herstellers als IBM mit einem IBM Spectrum Protect-Einheitentreiber: • AIX-Betriebssysteme /dev/lbX • Linux-Betriebssysteme /dev/tsmscsi/lbX • Windows-Betriebssysteme lbA.B.C.D		Um die Dateien für Speicherarchiveinheiten manuell zu definieren, verwenden Sie die folgenden Befehle: • DEFINE LIBRARY • DEFINE DRIVE • DEFINE PATH Für SCSI-Einheiten können Sie den Befehl PERFORM LIBACTION verwenden, um alle Laufwerke und zugehörigen Pfade für ein einzelnes Speicherarchiv in einem einzigen Schritt zu definieren. Um diesen Befehl zum Definieren aller Laufwerke und Pfade verwenden zu können, muss die Option SANDISCOVERY unterstützt werden und aktiviert sein.
Bandlaufwerke	IBM Einheiten mit einem IBM Bandeinheitentreiber: • AIX-Betriebssysteme /dev/rmtX • Linux-Betriebssysteme /dev/IBMtapeX • Windows-Betriebssysteme TapeX Einheiten eines anderen Herstellers als IBM mit einem IBM Spectrum Protect-Einheitentreiber: • AIX-Betriebssysteme /dev/mtX • Linux-Betriebssysteme /dev/tsmscsi/mtX • Windows-Betriebssysteme mtA.B.C.D		

Planung für Plattenspeicher

Wählen Sie die effektivste Speichertechnologie für IBM Spectrum Protect-Komponenten aus, um effiziente Serverleistung und Serveroperationen zu gewährleisten.

Speicherhardwareeinheiten haben unterschiedliche Kapazitäts- und Leistungsmerkmale, die festlegen, wie die Einheiten effizient mit IBM Spectrum Protect verwendet werden können. Die folgenden Richtlinien stellen eine allgemeine Anleitung zur Auswahl der für Ihre Lösung geeigneten Speicherhardware und Konfiguration dar.

Datenbank, aktive Protokolldatei und Archivprotokoll

- Verwenden Sie eine Solid-State-Platte (SSD) oder eine schnelle Platte mit 15.000 Umdrehungen pro Minute für die IBM Spectrum Protect-Datenbank und die aktive Protokolldatei.
- Verwenden Sie beim Erstellen von Arrays für die Datenbank RAID-Stufe 5.
- Verwenden Sie separate Platten für den Speicher für das Archivprotokoll und die Datenbanksicherung.

Speicherpool
Verwenden Sie RAID-Stufe 6 für Speicherpoolarrays, um bei Verwendung von Typen großer Platten Schutz vor dem Ausfall von zwei Laufwerken hinzuzufügen.

- Planung der Speicherarrays
  Bereiten Sie die Konfiguration des Plattenspeichers vor, indem Sie die Planung für RAID-Arrays und Datenträger gemäß der Größe Ihres IBM Spectrum Protect-Systems ausführen.

Planung für Bandspeicher

Bestimmen Sie, welche Bandeinheiten verwendet werden sollen und wie diese zu konfigurieren sind. Um die Systemleistung zu optimieren, planen Sie die Verwendung schneller Bandeinheiten mit hoher Speicherkapazität. Stellen Sie genügend Bandlaufwerke bereit, um Ihre Geschäftsanforderungen erfüllen zu können.

- Unterstützte Bandeinheiten und Speicherarchive
  Der Server kann eine Vielzahl von Bandeinheiten und Speicherarchiven verwenden. Wählen Sie für Ihre Geschäftsanforderungen geeignete Bandeinheiten und Speicherarchive aus.
- Unterstützte Bandeinheitenkonfigurationen
  Lesen Sie die Informationen zu lokalen Netzen (LAN) und Speicherbereichsnetzen (SAN). Um die Datenversetzung zu optimieren, planen Sie die Konfiguration der LAN-unabhängigen Datenversetzung. Überlegen Sie außerdem, ob die gemeinsame Speicherarchivnutzung verwendet werden soll.
- Erforderliche Definitionen für Bandspeichereinheiten
  Bevor der IBM Spectrum Protect-Server eine Bandeinheit verwenden kann, muss die Einheit für das Betriebssystem und den Server konfiguriert werden. Bestimmen Sie im Rahmen des Planungsprozesses, welche Definitionen für Ihre Bandspeichereinheiten erforderlich sind.
- Planung der Speicherpoolhierarchie
  Planen Sie die Speicherpoolhierarchie, um sicherzustellen, dass Daten täglich von Platte auf Band umgelagert werden. Bei der Umlagerung wird Speicherbereich auf der Platteneinheit freigegeben und die Daten werden für die langfristige Aufbewahrung auf Band versetzt. Auf diese Weise können Sie die Vorteile der Skalierbarkeit, Kosteneffizienz und Sicherheitsfunktionen von Bandspeicher nutzen.
- Auslagerung von Daten
  Um die Datenwiederherstellung zu erleichtern und in Ihre Strategie zur Wiederherstellung nach einem Katastrophenfall zu integrieren, speichern Sie Bandkopien an einen anderen Standort.

Unterstützte Bandeinheiten und Speicherarchive

Der Server kann eine Vielzahl von Bandeinheiten und Speicherarchiven verwenden. Wählen Sie für Ihre Geschäftsanforderungen geeignete Bandeinheiten und Speicherarchive aus.

Eine Liste der unterstützten Einheiten und gültigen Einheitenklassenformate finden Sie auf der Website für Ihr Betriebssystem:

- AIX-Betriebssysteme Windows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Weitere Informationen zu Speichereinheiten und Speicherobjekten finden Sie in Typen von Speichereinheiten.

Jede Einheit, die für IBM Spectrum Protect definiert ist, ist einer einzigen *Einheitenklasse* zugeordnet. Die Einheitenklasse gibt den Einheitentyp und die Datenträgerverwaltungsinformationen, wie beispielsweise Aufzeichnungsformat, geschätzte Kapazität und Kennzeichnungspräfixe, an.

Ein *Einheitentyp* kennzeichnet eine Einheit als Mitglied einer Gruppe von Einheiten mit gemeinsamen Datenträgermerkmalen. Beispielsweise gilt der Einheitentyp LTO für alle Generationen von LTO-Bandlaufwerken.

Eine Einheitenklasse für ein Bandlaufwerk muss auch ein Speicherarchiv angeben. Ein *physisches Speicherarchiv* besteht aus einem oder mehreren Laufwerken, die ähnliche Anforderungen in Bezug auf die Bereitstellung von Datenträgern haben. Das heißt, das Laufwerk kann von einem Bediener oder durch einen automatisierten Bereitstellungsmechanismus bereitgestellt werden.

Eine *Speicherarchivobjektdefinition* gibt den Speicherarchivtyp und andere Merkmale an, die diesem Speicherarchivtyp zugeordnet sind.

In der folgenden Tabelle sind die bevorzugten Speicherarchivtypen für eine Bandspeicherlösung in IBM Spectrum Protect Version 8.1.2 aufgelistet.

Tabelle 1. Speicherarchivtypen für eine Bandspeicherlösung in IBM Spectrum Protect 8.1.2

Speicherarchivtyp	Beschreibung	Weitere Informationen
SCSI	Ein SCSI-Speicherarchiv wird über eine SCSI-Schnittstelle gesteuert, die entweder direkt über SCSI-Verkabelung oder über ein Speicherbereichsnetz an den Host des Servers angeschlossen ist. Ein Robotermechanismus oder ein anderer Mechanismus handhabt automatisch das Bereitstellen von Banddatenträgern und das Aufheben der Bereitstellung von Banddatenträgern. Wenn Sie unterschiedliche Laufwerktypen für ein SCSI-Speicherarchiv erstellen, erstellen Sie mehrere logische Speicherarchive, die nicht auf verschiedene Typen von Laufwerken aufgeteilt werden können. Ein SCSI-Speicherarchiv kann Laufwerke mit gemischten Technologien enthalten, einschließlich LTO Ultrium- und DLT-Laufwerke. Beispiel: • Oracle StorageTek L700-Speicherarchiv • Bandeinheit IBM® 3592	Speicherarchive für die Verwendung durch einen Server konfigurieren Es gelten Einschränkungen, wenn Sie verschiedene Generationen von Datenträgern und Laufwerken kombiniert verwenden. Weitere Informationen finden Sie in: • Generationen von 3592-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen • LTO-Laufwerke und -Datenträger in einem Speicherarchiv mischen
SHARED	Gemeinsam genutzte Speicherarchive sind logische Speicherarchive, die durch SCSI-Speicherarchive dargestellt werden. Das Speicherarchiv wird durch den IBM Spectrum Protect-Server gesteuert, der als Speicherarchivmanager konfiguriert ist. IBM Spectrum Protect-Server, die den Speicherarchivtyp SHARED verwenden, sind Speicherarchivclients für den Speicherarchivmanager-Server. Gemeinsam genutzte Speicherarchive referenzieren einen Speicherarchivmanager.	

Unterstützte Bandeinheitenkonfigurationen

Lesen Sie die Informationen zu lokalen Netzen (LAN) und Speicherbereichsnetzen (SAN). Um die Datenversetzung zu optimieren, planen Sie die Konfiguration der LAN-unabhängigen Datenversetzung. Überlegen Sie außerdem, ob die gemeinsame Speicherarchivnutzung verwendet werden soll.

Wählen Sie die Einheitenkonfiguration aus, die für Ihre Geschäftsanforderungen am besten geeignet ist.

- LAN-gestützte und LAN-unabhängige Datenversetzung
  Sie können Daten zwischen Clients und Speichereinheiten, die an ein lokales Netz (LAN) angeschlossen sind, oder Speichereinheiten, die an ein Speicherbereichsnetz (SAN) angeschlossen sind, versetzen; dies wird als LAN-unabhängige Datenversetzung bezeichnet.
- Gemeinsame Speicherarchivnutzung
  Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie die gemeinsame Speicherarchivnutzung konfigurieren. Bei der gemeinsamen Speicherarchivnutzung können mehrere IBM Spectrum Protect-Server dasselbe Bandarchiv und dieselben Laufwerke in einem Speicherbereichsnetz (SAN) nutzen und die Sicherungs- und Wiederherstellungsleistung sowie die Nutzung der Bandhardware verbessern.
- LAN-unabhängige Datenversetzung
  Mit IBM Spectrum Protect wird einem Client über einen Speicheragenten die Funktionalität bereitgestellt, um Daten direkt in einem Bandarchiv in einem Speicherbereichsnetz (SAN) zu sichern und aus ihm zurückzuschreiben. Dieser Typ von Datenversetzung ist auch als LAN-unabhängige Datenversetzung bekannt.
- Gemischte Einheitentypen in Speicherarchiven
  IBM Spectrum Protect unterstützt das Mischen unterschiedlicher Einheitentypen in einem einzelnen automatisierten Speicherarchiv, sofern das Speicherarchiv die verschiedenen Datenträger für die unterschiedlichen Einheitentypen unterscheiden kann. Um den Konfigurationsprozess zu vereinfachen, sollten Sie keine unterschiedlichen Einheitentypen in einem Speicherarchiv mischen. Wenn das Mischen von Einheitentypen erforderlich ist, berücksichtigen Sie die Einschränkungen.

LAN-gestützte und LAN-unabhängige Datenversetzung

Sie können Daten zwischen Clients und Speichereinheiten, die an ein lokales Netz (LAN) angeschlossen sind, oder Speichereinheiten, die an ein Speicherbereichsnetz (SAN) angeschlossen sind, versetzen; dies wird als LAN-unabhängige Datenversetzung bezeichnet.

In einer konventionellen LAN-Konfiguration sind einem einzelnen IBM Spectrum Protect-Server ein oder mehrere Bandarchive zugeordnet. Durch die LAN-unabhängige Datenversetzung wird LAN-Bandbreite für andere Verwendungszwecke verfügbar gemacht und die IBM Spectrum Protect-Serverauslastung verringert.

In einer LAN-Konfiguration müssen Clientdaten, E-Mails, Terminalverbindung, Anwendungsprogramm und Einheitensteuerinformationen von demselben Netz gehandhabt werden. Einheitensteuerinformationen und Clientsicherungs- und -zurückschreibungsdaten fließen über das LAN.

Ein Speicherbereichsnetz (SAN) ist ein dediziertes Speichernetz, das die Systemleistung verbessern kann.

Durch die Verwendung von IBM Spectrum Protect in einem SAN profitieren Sie von den folgenden Funktionen:

- Gemeinsame Nutzung von Speichereinheiten durch mehrere IBM Spectrum Protect-Server.
  Einschränkung: Eine Speichereinheit mit dem Einheitentyp GENERICTAPE kann nicht von mehreren Servern gemeinsam genutzt werden.
- Versetzen von IBM Spectrum Protect-Clientdaten direkt auf Speichereinheiten (LAN-unabhängige Datenversetzung) durch die Konfiguration eines Speicheragenten auf dem Clientsystem.

In einem SAN können Sie Bandlaufwerke und Speicherarchive, die vom IBM Spectrum Protect-Server unterstützt werden, einschließlich der meisten SCSI-Bandeinheiten, gemeinsam nutzen.

Wenn IBM Spectrum Protect-Server ein SCSI-Bandarchiv gemeinsam nutzen, ist der *Speicherarchivmanager* der Eigner der Einheit und steuert die Einheit. Die Speicheragenten und andere IBM Spectrum Protect-Server, die die dieses Speicherarchiv gemeinsam nutzen, sind *Speicherarchivclients*. Ein Speicherarchivclient fordert gemeinsam genutzte Speicherarchivressourcen, wie beispielsweise Laufwerke oder Datenträger, vom Speicherarchivmanager an, verwendet die Ressourcen jedoch unabhängig. Der Speicherarchivmanager koordiniert den Zugriff auf diese Ressourcen. IBM Spectrum Protect-Server, die als Speicherarchivclients definiert sind, kontaktieren den Speicherarchivmanager mithilfe der Kommunikation zwischen Servern und fordern Einheitenservice an. Daten werden über das SAN zwischen den einzelnen Servern und der Speichereinheit versetzt.
Voraussetzung: Wenn Sie einen Speicherarchivmanager-Server definieren, der mit dem IBM Spectrum Protect-Server gemeinsam genutzt wird, muss die Option SANDISCOVERY auf ON gesetzt werden. Standardmäßig ist diese Option auf OFF gesetzt.
IBM Spectrum Protect-Server verwenden die folgenden Funktionen für die gemeinsame Nutzung eines automatisierten Speicherarchivs:

Partitionierung des Datenträgerbestands
: Der Bestand der Datenträger im gemeinsam genutzten Speicherarchiv wird unter den Servern aufgeteilt. Entweder ist ein einzelner Server Eigner eines bestimmten Datenträgers oder der Datenträger befindet sich im globalen Arbeitsdatenträgerpool. Keiner der Server ist Eigner des Arbeitsdatenträgerpools.

Serialisierter Laufwerkzugriff
: Es greift jeweils nur ein einziger Server auf das jeweilige Bandlaufwerk zu. Der Laufwerkzugriff erfolgt serialisiert. IBM Spectrum Protect steuert den Laufwerkzugriff, damit Server nicht die Bereitstellung von Datenträgern anderer Server aufheben oder nicht auf Laufwerke schreiben, in denen andere Server ihre Datenträger bereitstellen.

Serialisierter Mountzugriff
: Der Datenträgerwechsler des Speicherarchivs führt jeweils nur eine einzige Operation zum Bereitstellen (Mountoperation) oder Aufheben der Bereitstellung aus. Der Speicherarchivmanager führt alle Mountoperationen aus, um diese Serialisierung bereitzustellen.

Gemeinsame Speicherarchivnutzung

Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie die gemeinsame Speicherarchivnutzung konfigurieren. Bei der gemeinsamen Speicherarchivnutzung können mehrere IBM Spectrum Protect-Server dasselbe Bandarchiv und dieselben Laufwerke in einem Speicherbereichsnetz (SAN) nutzen und die Sicherungs- und Wiederherstellungsleistung sowie die Nutzung der Bandhardware verbessern.

Wenn IBM Spectrum Protect-Server ein Speicherarchiv gemeinsam nutzen, wird ein Server als Speicherarchivmanager konfiguriert, der Speicherarchivoperationen wie Bereitstellung und Aufhebung der Bereitstellung steuert. Der Speicherarchivmanager steuert auch das Eigentumsrecht für Datenträger und den Speicherarchivbestand. Weitere Server werden als Speicherarchivclients konfiguriert und kontaktieren den Speicherarchivmanager mithilfe der Kommunikation zwischen Servern und fordern Ressourcen an.

Speicherarchivclients müssen dieselbe Version oder eine frühere Version wie der Speicherarchivmanager-Server haben. Ein Speicherarchivmanager kann keine Speicherarchivclients unterstützen, die eine höhere Version haben. Weitere Informationen finden Sie in Storage-agent and library-client compatibility with an IBM Spectrum Protect server (Kompatibilität des Speicheragenten und des Speicherarchivclients mit einem IBM Spectrum Protect-Server).

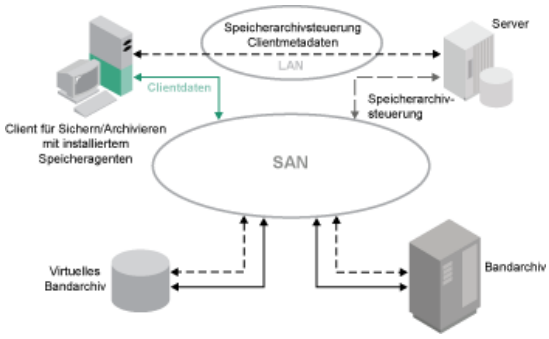
LAN-unabhängige Datenversetzung

Mit IBM Spectrum Protect wird einem Client über einen Speicheragenten die Funktionalität bereitgestellt, um Daten direkt in einem Bandarchiv in einem Speicherbereichsnetz (SAN) zu sichern und aus ihm zurückzuschreiben. Dieser Typ von Datenversetzung ist auch als LAN-unabhängige Datenversetzung bekannt.

Einschränkung: Centera-Speichereinheiten können keine Ziele für LAN-unabhängige Operationen sein.

Abbildung 1 zeigt eine SAN-Konfiguration, bei der ein Client direkt auf ein Bandarchiv zugreift, um Daten zu lesen oder zu schreiben.

Abbildung 1. LAN-unabhängige Datenversetzung



Die LAN-unabhängige Datenversetzung erfordert die Installation eines Speicheragenten auf dem Clientsystem. Der Server verwaltet die Datenbank und das Wiederherstellungsprotokoll und fungiert als Speicherarchivmanager, um Operationen der Einheiten zu steuern. Der Speicheragent auf dem Client handhabt die Datenübertragung zu der Einheit im SAN. Diese Implementierung gibt Bandbreite im LAN frei, die andernfalls für das Versetzen von Clientdaten verwendet würde.

Gemischte Einheitentypen in Speicherarchiven

IBM Spectrum Protect unterstützt das Mischen unterschiedlicher Einheitentypen in einem einzelnen automatisierten Speicherarchiv, sofern das Speicherarchiv die verschiedenen Datenträger für die unterschiedlichen Einheitentypen unterscheiden kann. Um den Konfigurationsprozess zu vereinfachen, sollten Sie keine unterschiedlichen Einheitentypen in einem Speicherarchiv mischen. Wenn das Mischen von Einheitentypen erforderlich ist, berücksichtigen Sie die Einschränkungen.

Bei Speicherarchiven mit dieser Funktionalität handelt es sich um Modelle, die über integrierte gemischte Laufwerke verfügen oder die das Hinzufügen gemischter Laufwerke unterstützen. Weitere Informationen zu bestimmten Modellen finden Sie in der Dokumentation des Herstellers. Informationen zu Speicherarchiven, die für IBM Spectrum Protect mit gemischten Einheitentypen getestet wurden, finden Sie in den Informationen für Ihr Betriebssystem:

- IBM Spectrum Protect Supported Devices for AIX, HP-UX, Solaris, and Windows
- IBM Spectrum Protect Supported Devices for Linux

Beispielsweise können LTO Ultrium-Laufwerke und IBM TS4500-Laufwerke in einem einzelnen Speicherarchiv vorhanden sein, das für den IBM Spectrum Protect-Server definiert ist.

- Verschiedene Datenträgergenerationen in einem Speicherarchiv
  Der IBM Spectrum Protect-Server erlaubt zwar unterschiedliche Einheitentypen in einem automatisierten Speicherarchiv, das Mischen verschiedener Generationen desselben Laufwerktyps wird jedoch im Allgemeinen nicht unterstützt. Neue Laufwerke können keine Daten mit den älteren Datenträgerformaten schreiben und alte Laufwerke können neue Formate nicht lesen. LTO Ultrium-Laufwerke sind eine Ausnahme von dieser Regel.
- Gemischte Datenträger und Speicherpools
  Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie Datenträgerformate in einem Speicherpool nicht mischen. Anstatt Formate zu mischen, ordnen Sie jedes eindeutige Datenträgerformat über seine eigene Einheitenklasse einem separaten Speicherpool zu. Diese Einschränkung gilt auch für LTO-Formate.

Verschiedene Datenträgergenerationen in einem Speicherarchiv

Der IBM Spectrum Protect-Server erlaubt zwar unterschiedliche Einheitentypen in einem automatisierten Speicherarchiv, das Mischen verschiedener Generationen desselben Laufwerktyps wird jedoch im Allgemeinen nicht unterstützt. Neue Laufwerke können keine Daten mit den älteren Datenträgerformaten schreiben und alte Laufwerke können neue Formate nicht lesen. LTO Ultrium-Laufwerke sind eine Ausnahme von dieser Regel.

Wenn mit der neuen Laufwerktechnologie keine Daten auf Datenträger geschrieben werden können, die von Laufwerken einer älteren Generation formatiert wurden, müssen die älteren Datenträger als schreibgeschützt markiert werden, um Probleme bei Serveroperationen zu verhindern. Außerdem müssen die älteren Laufwerke aus dem Speicherarchiv entfernt werden oder die Definitionen der älteren Laufwerke müssen vom Server entfernt werden. Beispielsweise unterstützt der IBM Spectrum Protect-Server nicht die Verwendung von Oracle StorageTek 9940A-Laufwerken mit 9940B-Laufwerken in Kombination mit anderen Einheitentypen in einem einzelnen Speicherarchiv.

Im Allgemeinen unterstützt IBM Spectrum Protect nicht das Mischen unterschiedlicher Generationen von LTO Ultrium-Laufwerken und -Datenträgern. Die folgenden Kombinationen werden jedoch unterstützt:

- LTO Ultrium Generation 3 (LTO-3) mit LTO Ultrium Generation 4 (LTO-4)
- LTO Ultrium Generation 4 (LTO-4) mit LTO Ultrium Generation 5 (LTO-5)
- LTO Ultrium Generation 5 (LTO-5) mit LTO Ultrium Generation 6 (LTO-6)
- LTO Ultrium Generation 6 (LTO-6) mit LTO Ultrium Generation 7 (LTO-7)

Der Server unterstützt diese Kombinationen, da die verschiedenen Laufwerke Daten von den unterschiedlichen Datenträgern lesen und auf diese schreiben können. Wenn Sie planen, für alle Laufwerke ein Upgrade auf Generation 4 (oder Generation 5, 6 oder 7) durchzuführen, müssen Sie

alle vorhandenen LTO Ultrium-Laufwerkdefinitionen und die Pfade, die ihnen zugeordnet sind, löschen. Anschließend können Sie die neuen Laufwerke und Pfade der Generation 4 (oder Generation 5, 6 oder 7) definieren.

Einschränkungen, die für das Mischen von LTO Ultrium-Bandlaufwerken und -Datenträgern gelten

- LTO-5-Laufwerke können nur LTO-3-Datenträger lesen. Wenn Sie LTO-3- und LTO-5-Laufwerke und -Datenträger in einem einzelnen Speicherarchiv mischen, müssen Sie die LTO-3-Datenträger als schreibgeschützt markieren. Sie müssen alle LTO-3-Arbeitsdatenträger entnehmen.
- LTO-6-Laufwerke können nur LTO-4-Datenträger lesen. Wenn Sie LTO-4- und LTO-6-Laufwerke und -Datenträger in einem einzelnen Speicherarchiv mischen, müssen Sie die LTO-4-Datenträger als schreibgeschützt markieren. Sie müssen alle LTO-4-Arbeitsdatenträger entnehmen.
- LTO-7-Laufwerke können nur LTO-5-Datenträger lesen. Wenn Sie LTO-5- und LTO-7-Laufwerke und -Datenträger in einem einzelnen Speicherarchiv mischen, müssen Sie die LTO-5-Datenträger als schreibgeschützt markieren. Sie müssen alle LTO-5-Arbeitsdatenträger entnehmen.

Einschränkungen, die für gemischte Generationen von LTO Ultrium-Bandlaufwerken in einem Speicherarchiv gelten
: Sie müssen Bandkassetten einer früheren Generation als das Bandlaufwerk verwenden. Ein Bandlaufwerk einer späteren Generation kann Daten von einer Bandkassette einer früheren Generation lesen und auf diese schreiben. Wenn beispielsweise ein Speicherarchiv über LTO-7- und LTO-6-Bandlaufwerke verfügt, müssen Sie LTO-6-Bandkassetten verwenden. Sowohl die LTO-7- als auch die LTO-6-Bandlaufwerke können Daten von LTO-6-Bandkassetten lesen und auf Bandkassetten dieser Generation schreiben.

Einschränkungen, die für gemischte Generationen von LTO Ultrium-Bandkassetten in einem Speicherarchiv gelten
: Sie müssen eine Bandkassette verwenden, die dieselbe Generation wie das Bandlaufwerk hat, oder exakt eine Generation früher. Wenn beispielsweise ein Speicherarchiv über LTO-7-Bandlaufwerke verfügt, können Sie LTO-7-Bandkassetten oder eine Kombination aus LTO-7- und LTO-6-Bandkassetten verwenden. Wenn dieses Speicherarchiv über LTO-7-, LTO-6- und LTO-5-Bandkassetten verfügt, müssen Sie den Zugriffsmodus für die LTO-5-Bandkassetten in READONLY (Lesezugriff) ändern.

Weitere Informationen zum Mischen von LTO Ultrium-Generationen finden Sie in Einheitenklassen LTO definieren.

Wenn Sie IBM Spectrum Protect verwenden, können Sie keine Laufwerke der Laufwerkgenerationen 3592, TS1130, TS1140, TS1150 oder späterer Laufwerkgenerationen mischen. Verwenden Sie eine von drei speziellen Konfigurationen. Ausführliche Informationen finden Sie in Einheitenklassen 3592 definieren.

Wenn Sie planen, Datenträger in einem Speicherarchiv zu verschlüsseln, mischen Sie keine Datenträgergenerationen in dem Speicherarchiv.

Gemischte Datenträger und Speicherpools

Sie können die Effizienz Ihrer Bandspeicherlösung optimieren, indem Sie Datenträgerformate in einem Speicherpool nicht mischen. Anstatt Formate zu mischen, ordnen Sie jedes eindeutige Datenträgerformat über seine eigene Einheitenklasse einem separaten Speicherpool zu. Diese Einschränkung gilt auch für LTO-Formate.

Mehrere Speicherpools und ihre Einheitenklassen verschiedenen Typs können auf dasselbe Speicherarchiv verweisen, das diese wie in Verschiedene Datenträgergenerationen in einem Speicherarchiv beschrieben unterstützen kann.

Sie können eine Migration auf eine neue Generation eines Datenträgertyps innerhalb desselben Speicherpools durchführen, indem Sie die folgenden Schritte ausführen:

1. Ersetzen Sie in dem Speicherarchiv alle älteren Laufwerke durch die Laufwerke der neueren Generation. Die Laufwerke dürfen nicht gemischt werden.
2. Markieren Sie die vorhandenen Datenträger mit den älteren Formaten als schreibgeschützt, wenn das neue Laufwerk diese Bänder im alten Format nicht hinzufügen kann. Wenn das neue Laufwerk auf die vorhandenen Datenträger mit ihrem alten Format schreiben kann, ist dies nicht notwendig; Schritt 1 ist jedoch dennoch erforderlich. Wenn verschiedene Laufwerkgenerationen, die lese- aber nicht schreibkompatibel sind, in demselben Speicherarchiv erforderlich sind, verwenden Sie für jede Laufwerkgeneration einen separaten Speicherpool.

Erforderliche Definitionen für Bandspeichereinheiten

Bevor der IBM Spectrum Protect-Server eine Bandeinheit verwenden kann, muss die Einheit für das Betriebssystem und den Server konfiguriert werden. Bestimmen Sie im Rahmen des Planungsprozesses, welche Definitionen für Ihre Bandspeichereinheiten erforderlich sind.

Tipp: Mithilfe des Befehls PERFORM LIBACTION können Sie den Prozess zum Hinzufügen von Einheiten zu SCSI- und VTL-Speicherarchiven vereinfachen.

In Tabelle 1 sind die Definitionen, die für die unterschiedlichen Einheitentypen erforderlich sind, zusammengefasst.

Tabelle 1. Erforderliche Definitionen für Speichereinheiten

		Erforderliche Definitionen			
Einheit	**Einheitentypen**	**Speicherarchiv**	**Laufwerk**	**Pfad**	**Einheiten-klasse**

Einheit	Einheitentypen	Erforderliche Definitionen			
		Speicherarchiv	Laufwerk	Pfad	Einheiten-klasse
Magnetplatte	DISK	—	—	—	Ja [1]
	FILE [2]	—	—	—	Ja
	AIX-Betriebssysteme Windows-BetriebssystemeCENTERA Linux-BetriebssystemeCENTERA [3]	—	—	—	Ja
Band	• 3590 • 3592 • DLT • LTO • NAS • VOLSAFE AIX-Betriebssysteme Windows-BetriebssystemeGENERICTAPE ECARTRIDGE [4]	Ja	Ja	Ja	Ja
Austauschbare Datenträger (Dateisystem)	REMOVABLEFILE	Ja	Ja	Ja	Ja

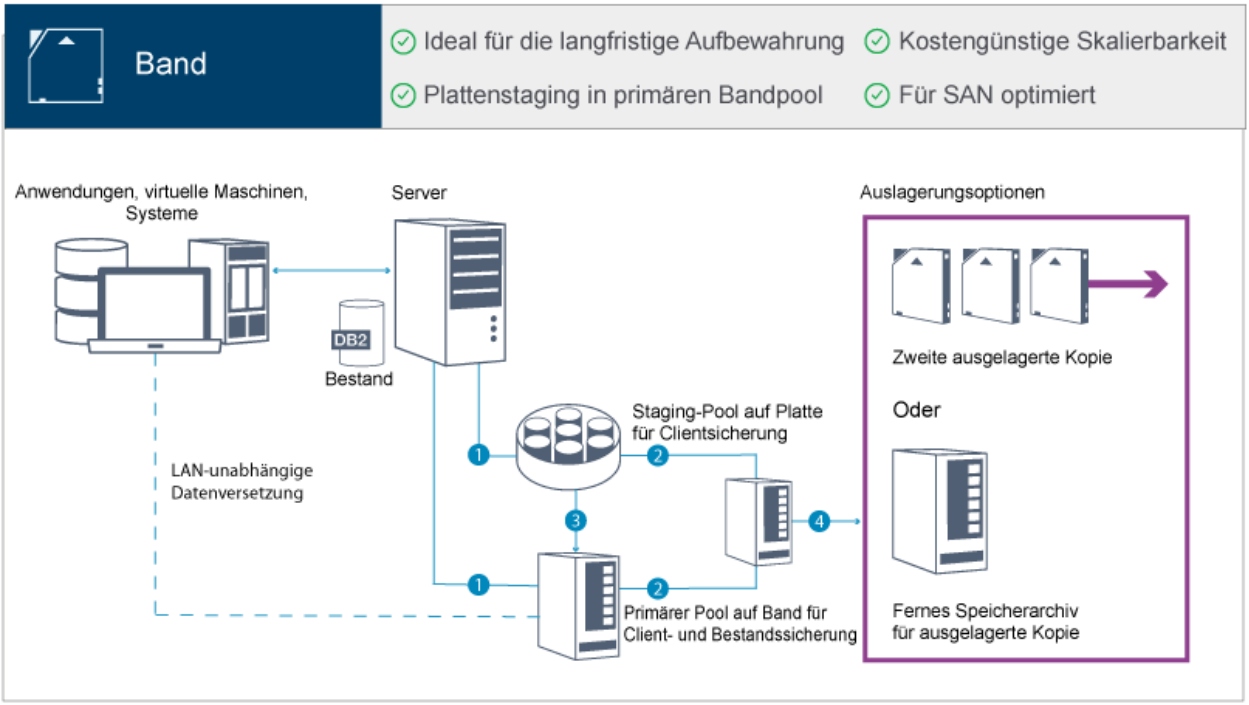
1. Die Einheitenklasse DISK ist bei der Installation vorhanden und kann nicht geändert werden.
2. FILE-Speicherarchive, -Laufwerke und -Pfade sind für die gemeinsame Nutzung mit Speicheragenten erforderlich.
3. Linux-BetriebssystemeDer Einheitentyp CENTERA ist nur für Linux x86_64-Systeme verfügbar.
4. Der Einheitentyp ECARTRIDGE gilt für Oracle StorageTek-Kassettenbandlaufwerke wie beispielsweise 9840- und T10000-Laufwerke.

Planung der Speicherpoolhierarchie

Planen Sie die Speicherpoolhierarchie, um sicherzustellen, dass Daten täglich von Platte auf Band umgelagert werden. Bei der Umlagerung wird Speicherbereich auf der Platteneinheit freigegeben und die Daten werden für die langfristige Aufbewahrung auf Band versetzt. Auf diese Weise können Sie die Vorteile der Skalierbarkeit, Kosteneffizienz und Sicherheitsfunktionen von Bandspeicher nutzen.

Vorbereitende Schritte

Die Speicherpoolhierarchie unterstützt Sie bei der Verwaltung des Datenflusses. Schauen Sie sich zum besseren Verständnis des Datenflusses Abbildung 1 an.
Abbildung 1. Bandspeicherlösung



Die folgenden Schritte entsprechen den Zahlen in der Abbildung:

1. Der Server empfängt Daten von Clients (Anwendungen, virtuelle Maschinen oder Systeme) und speichert die Daten in primären Speicherpools. Abhängig vom Clienttyp werden die Daten in einem primären Speicherpool auf Platte oder Band gespeichert.
2. Die Daten auf Platte und Band werden in einem Kopienspeicherpool auf Band gesichert.
3. Daten in dem primären Speicherpool auf Platte werden täglich in den primären Speicherpool auf Band umgelagert.
4. Daten aus dem Kopienspeicherpool auf Band werden an einen anderen Standort versetzt werden, um die langfristige Aufbewahrung und die Wiederherstellung nach einem Katastrophenfall zu unterstützen.

Vorgehensweise

Um die Speicherpoolhierarchie zu planen, beantworten Sie die folgenden Fragen:

a. Welche Clients sollten Daten auf Platte sichern und welche Clients sollten Daten auf Band sichern?
   - Die bevorzugte Methode ist das Sichern von Clients, die große Objekte wie beispielsweise Datenbanken enthalten, auf Band.
   - Die bevorzugte Methode ist das Sichern aller anderen Clients auf Platte.
   - Clients virtueller Maschinen (VMs) können auf Platte oder Band gesichert werden. Die bevorzugte Methode ist das Sichern eines VM-Clients in einem separaten Plattenspeicherpool, der nicht auf Band umgelagert wird. Wenn ein VM-Client auf Band umgelagert werden muss, erstellen Sie einen kleineren Plattenspeicherpool zum Speichern der VMware-Steuerdateien. Dieser kleinere Plattenspeicherpool darf nicht auf Band umgelagert werden. Weitere Informationen zum Sichern eines VM-Clients auf Band finden Sie in Richtlinien für Banddatenträger und Technote 1239546.

   Tipp: Wenn viele Clients Daten in einem einzigen Speicherpool sichern müssen, ziehen Sie die Verwendung eines Speicherpools auf Platte in Erwägung, da Sie viele Mountpunkte angeben können. Sie können einen Maximalwert von 999 für den Parameter MAXNUMMP im Befehl REGISTER NODE angeben.

b. Was ist bei der Angabe der Kapazität plattenbasierter Speicherpools zu beachten?

   Planen Sie zumindest genügend Kapazität zum Speichern der Daten von Sicherungsoperationen eines einzelnen Tages ein. Die bevorzugte Methode ist das Planen von genügend Kapazität, um Daten von Sicherungsoperationen zweier Tage zu speichern, zuzüglich eines Puffers von 20 %.

c. Was ist bei der Angabe der Einheitenklasse für den plattenbasierten Speicherpool zu beachten?

   Die bevorzugte Methode ist die Angabe der Einheitenklasse FILE. Setzen Sie den Parameter MOUNTLIMIT auf 4000. Stellen Sie außerdem sicher, dass der Knoten über eine ausreichend große Anzahl Mountpunkte verfügt; diesen Wert können Sie über den Parameter MAXNUMMP im Befehl REGISTER NODE angeben.

d. Sollte Datendeduplizierung für den Plattenspeicherpool angegeben werden?

   Nein, da die Daten nur für einen einzigen Tag auf Platte gespeichert werden, bevor die Daten auf Band umgelagert werden.

e. Sollte die automatische Umlagerung von Daten auf der Basis eines Umlagerungsschwellenwerts angegeben werden?

   Nein. Planen Sie stattdessen die tägliche Umlagerung mithilfe des Befehls MIGRATE STGPOOL. (Um die automatische Umlagerung auf der Basis des Umlagerungsschwellenwerts zu verhindern, geben Sie den Wert 100 für den Parameter HIGHMIG und den Wert 0 für den Parameter LOWMIG an, wenn Sie den Befehl DEFINE STGPOOL ausgeben.)

f. Sollte eine Umlagerungsverzögerung angegeben werden?

   Die bevorzugte Methode ist die Angabe der täglichen Umlagerung von Platte auf Band und nicht die Angabe einer Umlagerungsverzögerung, die weitere Planung erfordert. Weitere Informationen zur Umlagerungsverzögerung finden Sie in. Dateien in einer Speicherpoolhierarchie umlagern.

g. Wie kann die Anzahl Bandlaufwerke berechnet werden?
   i. Bestimmen Sie die native Datenübertragungsrate des Laufwerks anhand der Dokumentation des Herstellers. Um eine Schätzung der kontinuierlichen Datenübertragungsrate in Ihrer Speicherumgebung zu ermitteln, subtrahieren Sie 30 % von der nativen Datenübertragungsrate.
   ii. Berechnen Sie die erforderlich Datenaufnahmerate des Servers. Dividieren Sie dann diese Zahl durch die kontinuierliche Datenübertragungsrate einer einzelnen Bandeinheit. Das Ergebnis gibt die minimale Anzahl Laufwerke zur Unterstützung der Datenaufnahme an.
   iii. Berechnen Sie die Anzahl Mountpunkte, die für Clients erforderlich sind, die Daten auf Band sichern, einschließlich der Clients, die mehrere Sitzungen verwenden. Sie können die Mountpunkte über das Fenster zum Durchführen von Sicherungen verteilen; dabei müssen Sie beachten, dass Clients wahrscheinlich große Objekte sichern, die unter Umständen den größten Teil des Fensters in Anspruch nehmen.
   iv. Berechnen Sie die Leistungsanforderungen *und* Mountpunkte, die für Verwaltungstasks, wie beispielsweise Umlagerung von Platte auf Band und Kopieroperationen von Band auf Band, erforderlich sind. Durch die Sicherung von Daten auf Band, können Sie die Umlagerungsverarbeitung vermeiden, durch die Ausführung von Kopieroperationen von Band auf Band verdoppeln sich jedoch die Anforderungen für Bandlaufwerke.
   v. Berechnen Sie die Anzahl zusätzlicher Laufwerke, die gegebenenfalls erforderlich sind:
      - Wenn ein Bandlaufwerk nicht korrekt funktioniert, hat das Problem Auswirkungen auf die Anzahl verfügbarer Mountpunkte und die Aufnahmerate. Ziehen Sie die Bereitstellung von Ersatzlaufwerken in Erwägung. Wenn beispielsweise fünf Bandlaufwerke für normale Operationen erforderlich sind, sollten Sie die Bereitstellung von zwei Ersatzlaufwerken in Erwägung ziehen.
      - Für Zurückschreibungs- und Abrufoperationen sind unter Umständen zusätzliche Bandlaufwerke erforderlich, wenn Sie planen, die Operationen gleichzeitig mit Datenaufnahme- und Verwaltungsoperationen auszuführen. Stellen Sie, falls erforderlich, zusätzliche Bandlaufwerke bereit und stellen Sie sicher, dass diese noch nicht verwendet wurden, wenn Sie die Zurückschreibungs- oder Abrufoperationen starten.

h. Welche Alternativen sind für die Optimierung von Zurückschreibungsoperationen verfügbar?
   Sie können die Kollokation verwenden, um die Systemleistung zu verbessern und Organisation von Daten zu optimieren. Mithilfe der Kollokation kann die Anzahl Datenträger reduziert werden, auf die zugegriffen werden muss, wenn ein großes Datenvolumen zurückgeschrieben werden muss:
   - Für plattenbasierte Speicherpools ist die bevorzugte Methode die Verwendung der Kollokation nach Knoten. Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.
   - Für bandbasierte Speicherpools ist die bevorzugte Methode die Verwendung der Kollokation nach Gruppe. Die Kollokation nach Gruppe hat eine Verringerung der nicht genutzten Bandkapazität zur Folge, wodurch mehr kollokierte Daten auf einzelnen Bändern gespeichert werden können.

   Weitere Informationen zur Kollokation finden Sie in Operationen durch Aktivierung der Kollokation von Clientdateien optimieren.
   Wenn Sie ein erfahrener Systemadministrator sind, können Sie weitere Aktionen zur Optimierung von Zurückschreibungsoperationen planen. Siehe Zurückschreibungsoperationen für Clients optimieren, Dateisicherungsmethoden und MOVE NODEDATA (Daten nach Knoten in einen Speicherpool mit sequenziellem Zugriff versetzen).

Auslagerung von Daten

Um die Datenwiederherstellung zu erleichtern und in Ihre Strategie zur Wiederherstellung nach einem Katastrophenfall zu integrieren, speichern Sie Bandkopien an einen anderen Standort.

Verwenden Sie die Funktion 'Disaster Recovery Manager' (DRM), um einen Plan zur Wiederherstellung nach einem Katastrophenfall zu konfigurieren und automatisch zu generieren, der die Informationen, Scripts und Prozeduren enthält, die erforderlich sind, um den Server nach einem Katastrophenfall automatisch zurückzuschreiben und Clientdaten wiederherzustellen. Wählen Sie eine der folgenden Optionen für die Auslagerung von Daten als Strategie zur Wiederherstellung nach einem Katastrophenfall aus, um Bandkopien zu schützen:

Vaulting an einem anderen Standort für einen einzelnen Produktionsstandort
: Speicherdatenträger, wie beispielsweise Bandkassetten und Datenträger werden an einem anderen Standort durch Vaulting geschützt. Ein Kurier transportiert die Daten von der Speichereinrichtung an dem anderen Standort zum Wiederherstellungsstandort. Wenn ein Katastrophenfall eintritt, werden die Datenträger wieder an den Produktionsstandort gesendet, nachdem die Hardware und der IBM Spectrum Protect-Server wiederhergestellt wurden.

Vaulting an einem anderen Standort mit einem Wiederherstellungsstandort
: Ein Kurier transportiert Speicherdatenträger vom Produktionsstandort an eine Speichereinrichtung an einem anderen Standort. Da ein zugeordneter Wiederherstellungsstandort vorhanden ist, können Sie die Wiederherstellungszeit im Vergleich zur Wiederherstellungszeit bei einem einzelnen Produktionsstandort verringern. Diese Option erhöht jedoch die Kosten für die Wiederherstellung nach einem Katastrophenfall, da weitere Hardware und Software verwaltet werden muss. Beispielsweise muss der Wiederherstellungsstandort über kompatible Bandeinheiten und IBM Spectrum Protect-Server-Software verfügen. Bevor der Produktionsstandort wiederhergestellt werden kann, müssen die Hardware und Software am Wiederherstellungsstandort konfiguriert und aktiv sein.

Elektronisches Vaulting

Um elektronisches Vaulting als Strategie zur Wiederherstellung nach einem Katastrophenfall verwenden zu können, muss am Wiederherstellungsstandort ein aktiver IBM Spectrum Protect-Server vorhanden sein. Kritische Daten des Produktionsstandorts werden durch elektronisches Vaulting am Wiederherstellungsstandort geschützt. DRM wird auch für das Vaulting nicht kritischer Daten an einem anderen Standort verwendet. Beim elektronischen Vaulting werden kritische Daten schneller und häufiger als bei traditionellen Methoden mittels Kurier ausgelagert. Die Wiederherstellungszeit verkürzt sich, da kritische Daten bereits am Wiederherstellungsstandort gespeichert sind. Da der Wiederherstellungsstandort ständig aktiv ist, sind die Kosten der Strategie zur Wiederherstellung nach einem Katastrophenfall jedoch höher als beim Vaulting an einem anderen Standort.

Zugehörige Konzepte:
Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM

Planung für Sicherheit

Planen Sie den Schutz der Sicherheit von Systemen in der IBM Spectrum Protect-Lösung mithilfe von Steuerelementen für Zugriff und Authentifizierung und ziehen Sie das Verschlüsseln von Daten und der Übertragung von Kennwörtern in Erwägung.

- Planung für Administratorrollen
  Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.
- Planung für sichere Kommunikation
  Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.
- Planung für die Speicherung verschlüsselter Daten
  Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie das für Ihre Anforderungen am besten geeignete Verfahren aus.
- Planung des Firewallzugriffs
  Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

Planung für Administratorrollen

Definieren Sie die Berechtigungsstufen, die Administratoren zugeordnet werden sollen, die Zugriff auf die IBM Spectrum Protect-Lösung haben.

Sie können Administratoren eine der folgenden Berechtigungsstufen zuordnen:

Systemberechtigung
: Administratoren mit Systemberechtigung verfügen über die höchste Berechtigungsstufe. Administratoren mit dieser Berechtigungsstufe können jede Task ausführen. Sie können alle Maßnahmendomänen und Speicherpools verwalten und anderen Administratoren Berechtigung erteilen.

Maßnahmenberechtigung
: Administratoren mit Maßnahmenberechtigung können alle Tasks verwalten, die sich auf die Maßnahmenverwaltung beziehen. Diese Berechtigung kann uneingeschränkt sein oder auf bestimmte Maßnahmendomänen eingeschränkt werden.

Speicherberechtigung
: Administratoren mit Speicherberechtigung können Speicherressourcen für den Server zuordnen und steuern.

Bedienerberechtigung
: Administratoren mit Bedienerberechtigung können den sofortigen Betrieb des Servers und die Verfügbarkeit von Speichermedien wie beispielsweise Bandarchiven und -laufwerken steuern.

Die Szenarios in Tabelle 1 enthalten Beispiele, die zeigen, warum es sinnvoll ist, Administratoren für die Ausführung von Tasks unterschiedliche Berechtigungsstufen zuzuordnen:

Tabelle 1. Szenarios für Administratorrollen

Szenario	Typ der zu konfigurierenden Administrator-ID
Ein Administrator in einem kleinen Unternehmen verwaltet den Server und ist für alle Serveraktivitäten verantwortlich.	• Systemberechtigung: 1 Administrator-ID
Ein Administrator für mehrere Server verwaltet auch das gesamte System. Mehrere andere Administratoren verwalten ihre eigenen Speicherpools.	• Systemberechtigung auf allen Servern: 1 Administrator-ID für den Administrator des gesamten Systems • Speicherberechtigung für bestimmte Speicherpools: 1 Administrator-ID für jeden der anderen Administratoren
Ein Administrator verwaltet 2 Server. Eine andere Person unterstützt ihn bei den Verwaltungstasks. Zwei Assistenten müssen sicherstellen, dass wichtige Systeme gesichert werden. Jeder Assistent ist für die Überwachung der geplanten Sicherungen auf einem der IBM Spectrum Protect-Server verantwortlich.	• Systemberechtigung auf beiden Servern: 2 Administrator-IDs • Bedienerberechtigung: 2 Administrator-IDs für die Assistenten mit Zugriff auf den Server, für den die jeweilige Person verantwortlich ist.

Zugehörige Tasks:
Administratoren verwalten

Planung für sichere Kommunikation

Planen Sie den Schutz der Kommunikation zwischen den IBM Spectrum Protect-Lösungskomponenten.

Bestimmen Sie auf der Basis der Regelungen und Geschäftsanforderungen für Ihr Unternehmen, welche Stufe des Schutzes für Ihre Daten erforderlich ist.

Wenn Ihr Unternehmen ein hohes Maß an Sicherheit für Kennwörter und die Datenübertragung erfordert, planen Sie die Implementierung der sicheren Kommunikation mit dem Protokoll Transport Layer Security (TLS) oder Secure Sockets Layer (SSL).

TLS und SSL stellen sichere Kommunikation zwischen dem Server und dem Client bereit, können sich jedoch auf die Systemleistung auswirken. Um die Systemleistung zu verbessern, verwenden Sie TLS für die Authentifizierung, ohne Objektdaten zu verschlüsseln. Informationen zur Angabe, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, finden Sie in der Beschreibung der Clientoption SSL für die Client/Server-Kommunikation und der Beschreibung des Parameters UPDATE SERVER=SSL für die Kommunikation zwischen Servern. Ab Version 8.1.2 wird TLS standardmäßig für die Authentifizierung verwendet. Wenn Sie sich für die Verwendung von TLS entscheiden, um vollständige Sitzungen zu verschlüsseln, verwenden Sie das Protokoll nur für Sitzungen, für die es erforderlich ist; fügen Sie außerdem auf dem Server Prozessorressourcen hinzu, um den wachsenden Datenaustausch im Netz handhaben zu können. Sie können auch versuchsweise andere Optionen verwenden. Beispielsweise stellen einige Netzeinheiten wie Router und Switches die TLS- oder SSL-Funktion bereit.

Mithilfe von TLS und SSL können Sie einige oder alle der unterschiedlichen möglichen Kommunikationspfade schützen, beispielsweise:

- Operations Center: vom Browser zum Hub-Server; vom Hub-Server zum Peripherieserver
- Vom Client zum Server
- Vom Server zum Server: Knotenreplikation

Zugehörige Tasks:
Sichere Kommunikation mit Transport Layer Security konfigurieren

Planung für die Speicherung verschlüsselter Daten

Bestimmen Sie, ob Ihr Unternehmen die Verschlüsselung gespeicherter Daten erfordert, und wählen Sie das für Ihre Anforderungen am besten geeignete Verfahren aus.

Tabelle 1. Datenverschlüsselungsverfahren auswählen

Geschäftsanforderung	Verschlüsselungsverfahren	Weitere Informationen
Daten auf Clientebene schützen	IBM Spectrum Protect-Clientverschlüsselung	Sie können Daten auf Dateiebene unter Verwendung einer Einschluss-/Ausschlussliste verschlüsseln. Auf diese Weise haben Sie ein hohes Maß an Kontrolle darüber, welche Daten verschlüsselt werden. Auf dem Client sind sind zusätzliche IT-Ressourcen erforderlich, die sich auf die Leistung von Sicherungs- und Zurückschreibungsprozessen auswirken können. Weitere Informationen zu diesem Verfahren finden Sie in IBM Spectrum Protect-Clientverschlüsselung.
Daten in Speicherpooldatenträgern auf einem Bandlaufwerk schützen	Anwendungsverfahren	Wenn Sie das Anwendungsverfahren verwenden, verwaltet IBM Spectrum Protect die Verschlüsselungsschlüssel, um Daten in Speicherpooldatenträgern zu schützen. Sie müssen Sie besonders vorsichtig vorgehen, um Datenbanksicherungen zu schützen, da die Verschlüsselungsschlüssel in der Serverdatenbank gespeichert sind. Ohne Zugriff auf Datenbanksicherungen und zugehörige Verschlüsselungsschlüssel können Sie Ihre Daten nicht zurückschreiben. Sie können dieses Verfahren nicht verwenden, um Datenbanksicherungen, exportierte Daten oder Sicherungsgruppen zu verschlüsseln. Weitere Informationen zum Anwendungsverfahren finden Sie in Verschlüsselungsverfahren für Bänder.
Daten auf einem Bandlaufwerk schützen	Speicherarchivverfahren	Wenn Sie das Speicherarchivverfahren verwenden, werden die Verschlüsselungsschlüssel vom Speicherarchiv verwaltet. Sie können sowohl Daten in Speicherpools als auch andere Daten auf einem Bandlaufwerk verschlüsseln. Sie können steuern, welche Datenträger unter Verwendung ihrer Barcodeseriennummern verschlüsselt werden. Weitere Informationen zum Speicherarchivverfahren finden Sie in Verschlüsselungsverfahren für Bänder.

Geschäftsanforderung	Verschlüsselungsverfahren	Weitere Informationen
Daten auf einem Bandlaufwerk schützen	Systemverfahren	Wenn Sie das Systemverfahren verwenden, wird die Verschlüsselung von einem Einheitentreiber oder dem AIX-Betriebssystem verwaltet. Dieses Verschlüsselungsverfahren ist nur unter dem Betriebssystem AIX verfügbar. Sie können sowohl Daten in Speicherpools als auch andere Daten auf einem Bandlaufwerk verschlüsseln. Weitere Informationen zum Systemverfahren finden Sie in Verschlüsselungsverfahren für Bänder.

Planung des Firewallzugriffs

Bestimmen Sie die definierten Firewalls und die Ports, die offen sein müssen, damit die IBM Spectrum Protect-Lösung funktionsfähig ist.

In Tabelle 1 sind die Ports beschrieben, die vom Server, vom Client und vom Operations Center verwendet werden.

Tabelle 1. Vom Server, Client und Operations Center verwendete Ports

Element	Standardwert	Richtung	Beschreibung
Basisport (TCPPORT)	1500	Abgehend/Eingehend	Jede Serverinstanz erfordert einen eindeutigen Port. Sie können eine alternative Portnummer angeben. Der mit der Option TCPPORT angegebene Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen vom Client empfangsbereit. Mithilfe der Option TCPADMINPORT und der Option ADMINONCLIENTPORT können Sie Portwerte für den Datenverkehr des Verwaltungsclients festlegen.
Port nur für SSL (SSLTCPPORT)	Kein Standardwert	Abgehend/Eingehend	Dieser Port wird verwendet, wenn die Kommunikation am Port auf ausschließlich SSL-fähige Sitzungen beschränkt werden soll. Ein Server kann sowohl die SSL-Kommunikation als auch die Nicht-SSL-Kommunikation unterstützen, indem die Option TCPPORT oder die Option TCPADMINPORT verwendet wird.
SMB	45	Eingehend/Abgehend	Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.
SSH	22	Eingehend/Abgehend	Dieser Port wird von Konfigurationsassistenten verwendet, die unter Verwendung nativer Protokolle mit mehreren Hosts kommunizieren.
SMTP	25	Abgehend	Dieser Port wird zum Senden von E-Mail-Alerts vom Server verwendet.
Replikation	Kein Standardwert	Abgehend/Eingehend	Der Port und das Protokoll für den Port für abgehende Daten für die Replikation werden mit dem Befehl DEFINE SERVER festgelegt, der zum Konfigurieren der Replikation verwendet wird. Bei den Ports für eingehende Daten für die Replikation handelt es sich um die TCP-Ports und SSL-Ports, die für den Quellenserver im Befehl DEFINE SERVER angegeben werden.
Port für Clientzeitplan	Client-Port: 1501	Abgehend	Der Client ist an dem angegebenen Port empfangsbereit und teilt die Portnummer dem Server mit. Der Server kontaktiert den Client, wenn die servergesteuerte Zeitplanung verwendet wird. Sie können eine alternative Portnummer in der Clientoptionsdatei angeben.
Lange laufende Sitzungen	Einstellung für KEEPALIVE: YES	Abgehend	Wenn die Option KEEPALIVE aktiviert ist, werden während Client/Server-Sitzungen Keepalive-Pakete gesendet, um zu verhindern, dass die Firewall-Software lange laufende inaktive Verbindungen schließt.
Operations Center	HTTPS: 11090	Eingehend	Diese Ports werden für den Web-Browser des Operations Center verwendet. Sie können eine alternative Portnummer angeben.
Port für den Clientverwaltungsservice	Client-Port: 9028	Eingehend	Wenn Sie planen, IBM Spectrum Protect-Clientverwaltungsservices zu verwenden, muss der Zugriff auf den Port für den Clientverwaltungsservice über das Operations Center möglich sein. Stellen Sie sicher, dass Verbindungen nicht durch Firewalls verhindert werden können. Der Clientverwaltungsservice verwendet den TCP-Port des Servers für den Clientknoten für die Authentifizierung unter Verwendung einer Verwaltungssitzung.

Zugehörige Tasks:

Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen

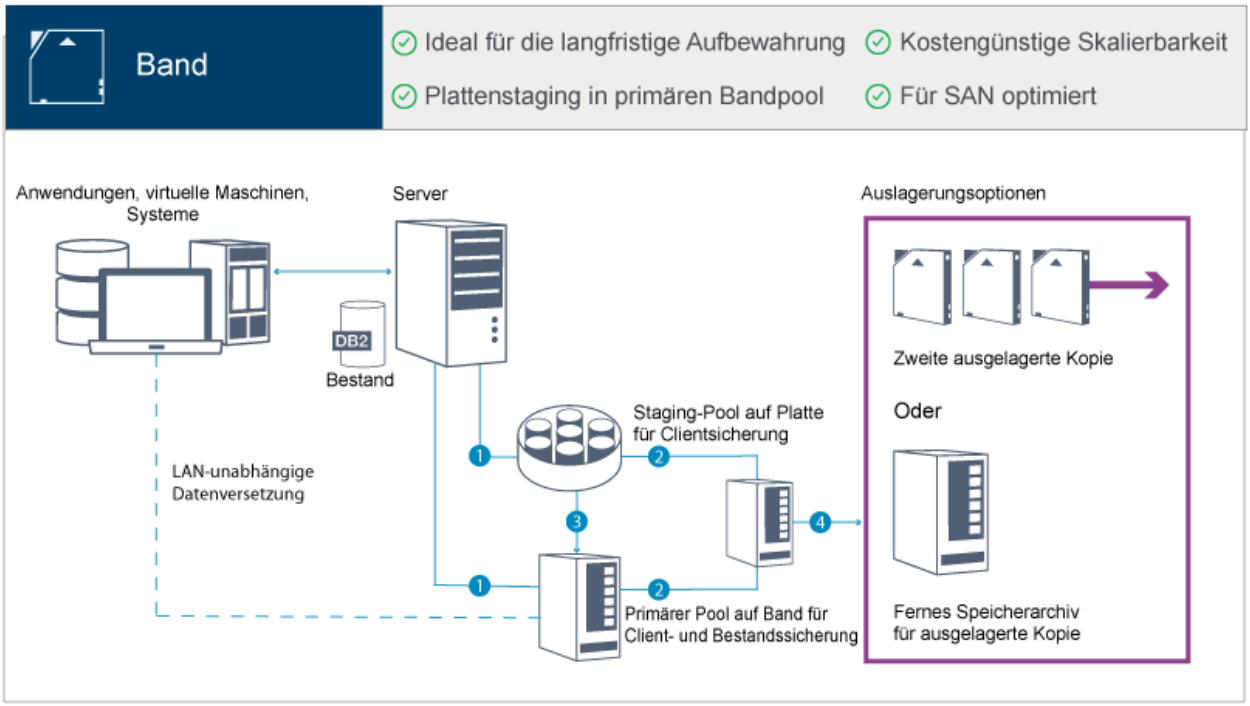
Zugehörige Verweise:

Serveroption ADMINONCLIENTPORT

DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
Serveroption TCPADMINPORT
Serveroption TCPPORT

Implementierung einer bandbasierten Datenschutzlösung

Implementieren Sie die bandbasierte Lösung, die die Platte-Platte-Band-Sicherung und Plattenstaging zur Optimierung des Speichers verwendet. Durch die Implementierung der Bandspeicherlösung können Sie die langfristige Aufbewahrung von Daten ermöglichen und kostengünstige Skalierbarkeit erzielen.



Tipp: Die beschriebene Lösung umfasst keine Knotenreplikation. Wenn die Knotenreplikation jedoch zum Sichern eines Speicherpools von Platte auf Platte verwendet werden soll, müssen Sie sicherstellen, dass die Replikationsoperation abgeschlossen ist, bevor Daten von Platte auf Band umgelagert werden. Sie können die Knotenreplikation auch verwenden, um einen Speicherpool auf einer lokalen Bandeinheit in einem Kopienspeicherpool auf einer lokalen Bandeinheit zu sichern.

Implementierungsroadmap

Die folgenden Schritte sind zum Konfigurieren einer bandbasierten Lösung erforderlich.

1. Konfigurieren Sie das System.
2. Installieren Sie den Server und das Operations Center.
3. Konfigurieren Sie den Server und das Operations Center.
4. Schließen Sie Bandeinheiten für den Server an.
5. Konfigurieren Sie Bandarchive für die Verwendung durch den Server.
6. Konfigurieren Sie eine Speicherpoolhierarchie.
7. Installieren und konfigurieren Sie Clients.
8. Konfigurieren Sie die LAN-unabhängige Datenversetzung.
9. Wählen Sie ein Verschlüsselungsverfahren aus und konfigurieren Sie die Verschlüsselung.
10. Konfigurieren Sie Bandspeicheroperationen.
11. Schließen Sie die Implementierung ab.

System konfigurieren

Um das System konfigurieren zu können, müssen Sie zunächst Ihre Plattenspeicherhardware und das Serversystem für IBM Spectrum Protect konfigurieren.

Informationen zu diesem Vorgang

Tipp: Es werden Prozeduren zum Konfigurieren des Servers und des Plattenspeichersystems beschrieben. Erste Schritte zum Konfigurieren von Bandeinheiten finden Sie in Bandeinheiten für den Server anschließen.

- Speicherhardware konfigurieren
  Um Plattenspeicher zu optimieren, prüfen Sie die Richtlinien zum Konfigurieren von Plattenspeicher mithilfe von IBM Spectrum Protect. Stellen Sie dann eine Verbindung zwischen dem Server und den Plattenspeichereinheiten her und führen Sie weitere Konfigurationstasks aus.
- Serverbetriebssystem installieren
  Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.
- Multipath I/O konfigurieren
  Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.
- Benutzer-ID für den Server erstellen
  Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.
- Dateisysteme für den Server vorbereiten
  Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

Speicherhardware konfigurieren

Um Plattenspeicher zu optimieren, prüfen Sie die Richtlinien zum Konfigurieren von Plattenspeicher mithilfe von IBM Spectrum Protect. Stellen Sie dann eine Verbindung zwischen dem Server und den Plattenspeichereinheiten her und führen Sie weitere Konfigurationstasks aus.

Vorbereitende Schritte

Richtlinien zum Konfigurieren von Plattenspeicher finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.

Vorgehensweise

1. Stellen Sie unter Berücksichtigung der folgenden Richtlinien eine Verbindung zwischen dem Server und den Speichereinheiten her:
   - Verwenden Sie einen Switch oder eine Direktverbindung für Fibre Channel-Verbindungen.
   - Berücksichtigen Sie die Anzahl Ports, die verbunden sind, und die erforderliche Bandbreite.
   - Berücksichtigen Sie die Anzahl Ports auf dem Server und die Anzahl Host-Ports auf dem Plattensystem, die verbunden sind.
2. Stellen Sie sicher, dass die Einheitentreiber und die Firmware für das Serversystem, die Adapter und das Betriebssystem aktuell sind und die empfohlenen Versionen haben.
3. Konfigurieren Sie Speicherarrays. Stellen Sie sicher, dass Sie entsprechend geplant haben, um die optimale Leistung zu gewährleisten. Weitere Informationen finden Sie in Planung für Plattenspeicher.
4. Stellen Sie sicher, dass das Serversystem Zugriff auf Plattendatenträger hat, die erstellt werden. Führen Sie die folgenden Schritte aus:
   a. Wenn das System mit einem Fibre Channel-Switch verbunden ist, verzonen Sie den Server, um die Platten anzuzeigen.
   b. Ordnen Sie alle Datenträger zu, um dem Plattensystem mitzuteilen, dass diesem spezifischen Server die Anzeige jeder Platte ermöglicht werden soll.
5. Stellen Sie sicher, dass Band- und Platteneinheiten unterschiedliche HBA-Ports verwenden. Steuern Sie die Band- und Platten-E/A mithilfe des Speicherbereichsnetzes (SAN).

Zugehörige Tasks:
Multipath I/O konfigurieren

Serverbetriebssystem installieren

Installieren Sie das Betriebssystem auf dem Serversystem und stellen Sie sicher, dass die Voraussetzungen für den IBM Spectrum Protect-Server erfüllt sind. Passen Sie Betriebssystemeinstellungen gemäß Anweisung an.

- Installation auf AIX-Systemen
  Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.
- Installation auf Linux-Systemen
  Führen Sie die folgenden Schritte aus, um Linux x86_64 auf dem Serversystem zu installieren.
- Installation auf Windows-Systemen
  Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

Installation auf AIX-Systemen

Führen Sie die folgenden Schritte aus, um AIX auf dem Serversystem zu installieren.

Vorgehensweise

1. Installieren Sie AIX Version 7.1, TL4, SP2 oder höher gemäß den Anweisungen des Herstellers.
2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.

3. Öffnen Sie die Datei /etc/hosts und führen Sie die folgenden Aktionen aus:
   - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

     ```
     127.0.0.1  localhost
     ```

4. Aktivieren Sie die AIX-I/O Completion Ports (IOCP), indem Sie den folgenden Befehl eingeben:

   ```
   chdev -l iocp0 -P
   ```

   Die Olson-Zeitzonendefinition kann sich auf die Serverleistung auswirken.
5. Um die Leistung zu optimieren, ändern Sie Ihr Systemzeitzonenformat von Olson in POSIX. Verwenden Sie das folgende Befehlsformat zum Aktualisieren der Zeitzoneneinstellung:

   ```
   chtz=Ortszeitzone,Datum/Uhrzeit,Datum/Uhrzeit
   ```

   Beispielsweise würden Sie in Tucson, Arizona, wo die Mountain Standard Time gilt, den folgenden Befehl ausgeben, um das Format in das POSIX-Format zu ändern:

   ```
   chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
   ```

6. Fügen Sie in .profile des Instanzbenutzers einen Eintrag hinzu, um die folgende Umgebung festzulegen:

   ```
   export MALLOCOPTIONS=multiheap:16
   ```

7. Legen Sie fest, dass das System vollständige Anwendungskerndateien erstellen soll. Geben Sie den folgenden Befehl aus:

   ```
   chdev -l sys0 -a fullcore=true -P
   ```

8. Stellen Sie für die Kommunikation mit dem Server und dem Operations Center sicher, dass die folgenden Ports für alle Firewalls, die gegebenenfalls vorhanden sind, offen sind:
   - Öffnen Sie für die Kommunikation mit dem Server Port 1500.
   - Öffnen Sie für die sichere Kommunikation mit dem Operations Center Port 11090 auf dem Hub-Server.

   Wenn Sie nicht die Standardwerte für Ports verwenden, stellen Sie sicher, dass die verwendeten Ports offen sind.

9. Aktivieren Sie TCP-Hochleistungsverbesserungen. Geben Sie den folgenden Befehl aus:

   ```
   no -p -o rfc1323=1
   ```

10. Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, kombinieren Sie vier 10-Gb-Ethernet-Ports durch Bonding miteinander. Verwenden Sie das System Management Interface Tool (SMIT), um die Ports durch Bonding unter Verwendung von Etherchannel zu kombinieren. Beim Testen wurden die folgenden Einstellungen verwendet:

    ```
    mode            8023ad
    auto_recovery   yes             Automatische Wiederherstellung nach
                                    Übernahme aktivieren
    backup_adapter  NONE            Adapter, der beim Fehlschlagen des
                                    gesamten Kanals verwendet wird
    hash_mode       src_dst_port    Legt fest, wie der abgehende Adapter
                                    ausgewählt wird
    interval        long            Legt den Intervallwert für den IEEE-Modus
                                    802.3ad fest
    mode            8023ad          EtherChannel-Betriebsart
    netaddr         0               Mit Ping zu überprüfende Adresse
    noloss_failover yes             Verlustfreie Übernahme nach dem Fehl-
                                    schlagen des Pingbefehls aktivieren
    num_retries     3               Anzahl Wiederholungen für Pingbefehl vor
                                    dem Fehlschlagen
    retry_time      1               Wartezeit (in Sekunden) zwischen
                                    Pingbefehlen
    use_alt_addr    no              Alternative EtherChannel-Adresse
                                    aktivieren
    use_jumbo_frame no              Jumbo-Frames für Gigabit Ethernet
                                    aktivieren
    ```

11. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 1 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 1. Benutzergrenzwerte (ulimit-Werte)

Typ des Benutzergrenzwerts	Einstellung	Wert	Befehl zum Abfragen des Werts
Maximale Größe der erstellten Kerndateien	core	Unlimited	`ulimit -Hc`

Typ des Benutzergrenzwerts	Einstellung	Wert	Befehl zum Abfragen des Werts
Maximale Größe eines Datensegments für einen Prozess	data	Unlimited	`ulimit -Hd`
Maximale Dateigröße	fsize	Unlimited	`ulimit -Hf`
Maximale Anzahl offener Dateien	nofile	65536	`ulimit -Hn`
Maximale Prozessorzeit in Sekunden	cpu	Unlimited	`ulimit -Ht`
Maximale Anzahl Benutzerprozesse	nproc	16384	`ulimit -Hu`

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

Installation auf Linux-Systemen

Führen Sie die folgenden Schritte aus, um Linux x86_64 auf dem Serversystem zu installieren.

Vorbereitende Schritte

Das Betriebssystem wird auf den internen Festplatten installiert. Konfigurieren Sie die internen Festplatten für die Verwendung eines RAID 1-Hardware-Arrays. Wenn Sie beispielsweise ein kleines System konfigurieren, werden die beiden internen 300-GB-Platten in RAID 1 gespiegelt, sodass es aussieht, als würde dem Installationsprogramm des Betriebssystems eine einzelne 300-GB-Platte zur Verfügung stehen.

Vorgehensweise

1. Installieren Sie Red Hat Enterprise Linux Version 7.1 oder höher gemäß den Anweisungen des Herstellers. Fordern Sie eine bootfähige DVD an, die Red Hat Enterprise Linux Version 7.1 enthält, und starten Sie Ihr System von dieser DVD. Für Installationsoptionen siehe die folgende Anleitung. Wenn ein Element in der folgenden Liste nicht aufgeführt ist, übernehmen Sie die Standardauswahl unverändert.
   a. Wählen Sie nach dem Starten der DVD im Menü Install or upgrade an existing system (Installation oder Aktualisierung eines bestehenden Systems) aus.
   b. Wählen Sie in der Eingangsanzeige Test this media & install Red Hat Enterprise Linux 7.1 (Diese Median überprüfen & Red Hat Enterprise Linux 7.1 installieren) aus.
   c. Wählen Sie Ihre Sprache und Tastaturbelegung aus.
   d. Wählen Sie Ihren Standort aus, um die korrekte Zeitzone festzulegen.
   e. Wählen Sie Software Selection (Softwareauswahl) und in der nächsten Anzeige Server with GUI (Server mit GUI) aus.
   f. Klicken Sie auf der Installationszusammenfassungsseite auf Installation Destination (Installationsziel) und überprüfen Sie die folgenden Einträge:
      - Die lokale 300-GB-Platte ist als Installationsziel ausgewählt.
      - Unter 'Other Storage Options' (Weitere Speicheroptionen) ist Automatically configure partitioning (Partitionierung automatisch konfigurieren) ausgewählt.

      Klicken Sie auf Done (Fertig).
   g. Klicken Sie auf Begin Installation (Installation starten). Legen Sie nach dem Start der Installation das Rootkennwort für Ihr Rootbenutzerkonto fest.

   Führen Sie nach dem Abschluss der Installation einen Neustart für das System durch und melden Sie sich als Rootbenutzer an. Geben Sie den Befehl df aus, um die Basispartitionierung zu überprüfen. Auf einem Testsystem hatte die Erstpartitionierung beispielsweise das folgende Ergebnis zur Folge:

```
[root@tvapp02]# df -h
Filesystem             Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root   50G  3.0G   48G   6% /
devtmpfs                32G     0   32G   0% /dev
tmpfs                   32G   92K   32G   1% /dev/shm
tmpfs                   32G  8.8M   32G   1% /run
tmpfs                   32G     0   32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home  220G   37M  220G   1% /home
/dev/sda1              497M  124M  373M  25% /boot
```

2. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Anweisungen zur Installation des Betriebssystems.
   Um optimalen Durchsatz und optimale Zuverlässigkeit zu gewährleisten, sollten Sie das Bonding mehrerer Netzports in Erwägung ziehen. Erstellen Sie dazu eine LACP-Netzverbindung (LACP = Link Aggregation Control Protocol), bei der mehrere untergeordnete Ports in einer einzigen logischen Verbindung aggregiert werden. Die bevorzugte Methode ist die Verwendung des Bondmodus 802.3ad, des Werts 100 für die Einstellung miimon und der Angabe 'layer3+4' für die Einstellung xmit_hash_policy.
   Einschränkung: Um eine LACP-Netzverbindung verwenden zu können, muss ein Netzswitch vorhanden sein, der LACP unterstützt.

   Weitere Anweisungen zur Konfiguration von Bonding-Netzverbindungen mit Red Hat Enterprise Linux Version 7 finden Sie unter Create a Channel Bonding Interface.

3. Öffnen Sie die Datei /etc/hosts und führen Sie die folgenden Aktionen aus:
   - Aktualisieren Sie die Datei, um die IP-Adresse und den Hostnamen des Servers einzuschließen. Beispiel:

     ```
     192.0.2.7  server.yourdomain.com  server
     ```

   - Überprüfen Sie, ob die Datei einen Eintrag für localhost mit der Adresse 127.0.0.1 enthält. Beispiel:

     ```
     127.0.0.1  localhost
     ```

4. Installieren Sie Komponenten, die für die Serverinstallation erforderlich sind. Führen Sie die folgenden Schritte aus, um ein YUM-Repository (YUM = Yellowdog Updater, Modified) zu erstellen und die vorausgesetzten Pakete zu installieren.
   a. Stellen Sie die DVD für die Installation von Red Hat Enterprise Linux in einem Systemverzeichnis bereit. Um sie beispielsweise im Verzeichnis /mnt bereitzustellen, geben Sie den folgenden Befehl aus:

      ```
      mount -t iso9660 -o ro /dev/cdrom /mnt
      ```

   b. Überprüfen Sie, ob die DVD bereitgestellt wurde, indem Sie den Befehl mount ausgeben. Es sollte eine ähnliche Ausgabe wie in dem folgenden Beispiel angezeigt werden:

      ```
      /dev/sr0 on /mnt type iso9660
      ```

   c. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

      ```
      cd /etc/yum/repos.d
      ```

      Wenn das Verzeichnis repos.d nicht vorhanden ist, erstellen Sie es.
   d. Listen Sie den Verzeichnisinhalt auf:

      ```
      ls rhel-source.repo
      ```

   e. Benennen Sie die ursprüngliche repo-Datei um, indem Sie den Befehl mv ausgeben. Beispiel:

      ```
      mv rhel-source.repo rhel-source.repo.orig
      ```

   f. Erstellen Sie mithilfe eines Texteditors eine neue repo-Datei. Um beispielsweise den Editor vi zu verwenden, geben Sie den folgenden Befehl aus:

      ```
      vi rhel71_dvd.repo
      ```

   g. Fügen Sie der neuen repo-Datei die folgenden Zeilen hinzu. Der Parameter baseurl gibt den Verzeichnismountpunkt an:

      ```
      [rhel71_dvd]
      name=DVD Redhat Enterprise Linux 7.1
      baseurl=file:///mnt
      enabled=1
      gpgcheck=0
      ```

   h. Installieren Sie das vorausgesetzte Paket ksh.x86_64, indem Sie den Befehl yum ausgeben. Beispiel:

      ```
      yum install ksh.x86_64
      ```

      Ausnahme: Sie müssen die Bibliotheken compat-libstdc++-33-3.2.3-69.el6.i686 und libstdc++.i686 für Red Hat Enterprise Linux Version 7.1 nicht installieren.
5. Wenn die Softwareinstallation abgeschlossen ist, können Sie die ursprünglichen YUM-Repository-Werte zurückschreiben, indem Sie die folgenden Schritte ausführen:
   a. Heben Sie die Bereitstellung der DVD für die Installation von Red Hat Enterprise Linux auf, indem Sie den folgenden Befehl ausgeben:

      ```
      unmount /mnt
      ```

   b. Wechseln Sie in das YUM-Repository-Verzeichnis, indem Sie den folgenden Befehl ausgeben:

      ```
      cd /etc/yum/repos.d
      ```

   c. Benennen Sie die von Ihnen erstellte repo-Datei um:

      ```
      mv rhel71_dvd.repo rhel71_dvd.repo.orig
      ```

   d. Benennen Sie die ursprüngliche Datei wieder in den ursprünglichen Namen um:

      ```
      mv rhel-source.repo.orig rhel-source.repo
      ```

6. Bestimmen Sie, ob Änderungen an Kernelparametern erforderlich sind. Führen Sie die folgenden Schritte aus:
   a. Listen Sie mithilfe des Befehls sysctl -a die Parameterwerte auf.
   b. Analysieren Sie die Ergebnisse anhand der Richtlinien in Tabelle 1, um zu bestimmen, ob Änderungen erforderlich sind.
   c. Wenn Änderungen erforderlich sind, definieren Sie die Parameter in der Datei /etc/sysctl.conf. Die Dateiänderungen werden angewendet, wenn das System gestartet wird.

   Tipp: Passen Sie Kernelparametereinstellungen automatisch an und eliminieren Sie die Notwendigkeit manueller Aktualisierungen dieser Einstellungen. Unter Linux passt die DB2-Datenbanksoftware automatisch die Werte der Kernelparameter für die

Interprozesskommunikation (IPC) an und setzt sie auf die bevorzugten Einstellungen. Weitere Informationen zu Kernelparametereinstellungen finden Sie bei Verwendung des Suchbegriffs Linux-Kernelparameter im IBM DB2 Version 11.1 Knowledge Center.

Tabelle 1. Optimale Einstellungen für Linux-Kernelparameter

Parameter	**Beschreibung**
kernel.shmmni	Die maximale Anzahl Segmente.
kernel.shmmax	Die maximale Größe eines gemeinsam genutzten Speichersegments (Byte). Dieser Parameter muss definiert werden, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird.
kernel.shmall	Die maximale Zuordnung von Seiten im gemeinsam genutzten Speicher (Seiten).
kernel.sem Für den Parameter kernel.sem gibt es vier Werte.	(SEMMSL) Die maximale Anzahl Semaphore pro Array.
	(SEMMNS) Die maximale Anzahl Semaphore pro System.
	(SEMOPM) Die maximale Anzahl Operationen pro Semaphoraufruf.
	(SEMMNI) Die maximale Anzahl Arrays.
kernel.msgmni	Die maximale Anzahl systemweiter Nachrichtenwarteschlangen.
kernel.msgmax	Die maximale Größe von Nachrichten (Byte).
kernel.msgmnb	Die standardmäßige maximale Größe der Warteschlange (Byte).
kernel.randomize_va_space	Mit dem Parameter kernel.randomize_va_space wird die Verwendung von Speicher-ASLR für den Kernel konfiguriert. Inaktivieren Sie ASLR, da ASLR Fehler der DB2-Software zur Folge haben kann. Weitere ausführliche Informationen zu Linux-ASLR und DB2 enthält die Technote 1365583.
vm.swappiness	Der Parameter vm.swappiness definiert, ob der Kernel Anwendungsspeicher aus physischem Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.
vm.overcommit_memory	Der Parameter vm.overcommit_memory hat Auswirkungen darauf, wie viel virtueller Speicher gemäß dem Kernel zugeordnet werden kann. Weitere Informationen zu Kernelparametern enthält die Produktinformation zu DB2.

7. Öffnen Sie Firewall-Ports für die Kommunikation mit dem Server. Führen Sie die folgenden Schritte aus:
   a. Legen Sie die von der Netzschnittstelle verwendete Zone fest. Die Zone ist standardmäßig 'public'.
   Geben Sie den folgenden Befehl aus:

   ```
   #  firewall-cmd --get-active-zones
   public
     interfaces: ens4f0
   ```

   b. Um die Standardportadresse für die Kommunikation mit dem Server zu verwenden, öffnen Sie TCP/IP-Port 1500 in der Linux-Firewall.
   Geben Sie den folgenden Befehl aus:

   ```
   firewall-cmd --zone=public --add-port=1500/tcp --permanent
   ```

   Wenn ein anderer Wert als der Standardwert verwendet werden soll, können Sie eine Zahl zwischen 1024 und 32767 angeben. Wenn ein anderer Port als der Standardport geöffnet wird, müssen Sie diesen Port bei der Ausführung des Konfigurationsscripts angeben.

   c. Wenn Sie planen, dieses System als einen Hub zu verwenden, öffnen Sie Port 11090, den Standardport für die sichere Kommunikation (HTTPS).
   Geben Sie den folgenden Befehl aus:

   ```
   firewall-cmd --zone=public --add-port=11090/tcp --permanent
   ```

d. Laden Sie die Firewalldefinitionen erneut, damit die Änderungen wirksam werden.
Geben Sie den folgenden Befehl aus:

```
firewall-cmd --reload
```

8. Überprüfen Sie, ob Benutzerprozessressourcengrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, gemäß den Richtlinien in Tabelle 2 definiert sind. Wenn ulimit-Werte nicht korrekt definiert sind, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann.

Tabelle 2. Benutzergrenzwerte (ulimit-Werte)

Typ des Benutzergrenzwerts	Einstellung	Wert	Befehl zum Abfragen des Werts
Maximale Größe der erstellten Kerndateien	core	Unlimited	`ulimit -Hc`
Maximale Größe eines Datensegments für einen Prozess	data	Unlimited	`ulimit -Hd`
Maximale Dateigröße	fsize	Unlimited	`ulimit -Hf`
Maximale Anzahl offener Dateien	nofile	65536	`ulimit -Hn`
Maximale Prozessorzeit in Sekunden	cpu	Unlimited	`ulimit -Ht`
Maximale Anzahl Benutzerprozesse	nproc	16384	`ulimit -Hu`

Wenn einer der Benutzergrenzwerte geändert werden muss, führen Sie die Anweisungen in der Dokumentation für Ihr Betriebssystem aus.

Installation auf Windows-Systemen

Installieren Sie Microsoft Windows Server 2012 Standard Edition auf dem Serversystem und bereiten Sie das System für die Installation und Konfiguration des IBM Spectrum Protect-Servers vor.

Vorgehensweise

1. Installieren Sie Microsoft Windows Server 2012 R2 Standard Edition gemäß den Anweisungen des Herstellers.
2. Ändern Sie die Windows-Kontensteuerungsrichtlinien, indem Sie die folgenden Schritte ausführen.
   a. Öffnen Sie den Editor für lokale Sicherheitsrichtlinien, indem Sie secpol.msc ausführen.
   b. Klicken Sie auf Lokale Richtlinien > Sicherheitsoptionen und stellen Sie sicher, dass die folgenden Benutzerkontensteuerungsrichtlinien inaktiviert sind:
      - Administratorbestätigungsmodus für das integrierte Administratorkonto
      - Alle Administratoren im Administratorbestätigungsmodus ausführen
3. Konfigurieren Sie Ihre TCP/IP-Einstellungen gemäß den Installationsanweisungen für das Betriebssystem.
4. Wenden Sie Windows-Updates an und aktivieren Sie Zusatzfunktionen (optionale Features), indem Sie die folgenden Schritte ausführen:
   a. Wenden Sie die neuesten Windows 2012 R2-Updates an.
   b. Installieren und aktivieren Sie das Windows 2012 R2-Feature Microsoft .NET Framework 3.5 über den Windows Server-Manager.
   c. Aktualisieren Sie, falls erforderlich, die FC- und Ethernet-HBA-Einheitentreiber mit neueren Versionen.
   d. Installieren Sie den für das verwendete Plattensystem geeigneten Multipath I/O-Treiber.
5. Öffnen Sie den TCP/IP-Standardport (1500) für die Kommunikation mit dem IBM Spectrum Protect-Server. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Sicherungsserver-Port 1500"
dir=in action=allow protocol=TCP localport=1500
```

6. Öffnen Sie auf dem Operations Center-Hub-Server den Standardport für die sichere Kommunikation (HTTPS) mit dem Operations Center. Die Portnummer ist 11090. Geben Sie beispielsweise den folgenden Befehl aus:

```
netsh advfirewall firewall add rule name="Operations Center-Port 11090"
dir=in action=allow protocol=TCP localport=11090
```

Multipath I/O konfigurieren

Sie können Multipathing für Plattenspeicher aktivieren und konfigurieren. Die mit Ihrer Hardware zur Verfügung gestellte Dokumentation enthält ausführliche Anweisungen.

- AIX-Systeme
  Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.
- Linux-Systeme
  Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

- Windows-Systeme
  Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

AIX-Systeme

Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

Vorgehensweise

1. Bestimmen Sie die Fibre Channel-Portadresse, die für die Hostdefinition auf dem Plattensubsystem verwendet werden muss. Geben Sie den Befehl lscfg für jeden Port aus.
   - Geben Sie auf kleinen und mittelgroßen Systemen die folgenden Befehle aus:

     ```
     lscfg -vps -l fcs0 | grep "Netzadresse"
     lscfg -vps -l fcs1 | grep "Netzadresse"
     ```

   - Geben Sie auf großen Systemen die folgenden Befehle aus:

     ```
     lscfg -vps -l fcs0 | grep "Netzadresse"
     lscfg -vps -l fcs1 | grep "Netzadresse"
     lscfg -vps -l fcs2 | grep "Netzadresse"
     lscfg -vps -l fcs3 | grep "Netzadresse"
     ```

2. Stellen Sie sicher, dass die folgenden AIX-Dateigruppen installiert sind:
   - devices.common.IBM.mpio.rte
   - devices.fcp.disk.array.rte
   - devices.fcp.disk.rte
3. Geben Sie den Befehl cfgmgr aus, damit AIX die Hardware erneut überprüft und verfügbare Platten erkennt. Beispiel:

   ```
   cfgmgr
   ```

4. Um die verfügbaren Platten aufzulisten, geben Sie den folgenden Befehl aus:

   ```
   lsdev -Ccdisk
   ```

   Es sollte eine ähnliche Ausgabe wie die folgende angezeigt werden:

   ```
   hdisk0  Available 00-00-00 SAS Disk Drive
   hdisk1  Available 00-00-00 SAS Disk Drive
   hdisk2  Available 01-00-00 SAS Disk Drive
   hdisk3  Available 01-00-00 SAS Disk Drive
   hdisk4  Available 06-01-02 MPIO IBM 2076 FC Disk
   hdisk5  Available 07-01-02 MPIO IBM 2076 FC Disk
   ...
   ```

5. Verwenden Sie die Ausgabe des Befehls lsdev, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

   Beispielsweise könnte eine Einheiten-ID `hdisk4` lauten. Sichern Sie die Liste der Einheiten-IDs für die Verwendung bei der Erstellung von Dateisystemen für den IBM Spectrum Protect-Server.

6. Korrelieren Sie die SCSI-Einheiten-IDs zu bestimmten Platten-LUNs aus dem Plattensystem, indem Sie detaillierte Informationen zu allen physischen Datenträgern im System auflisten. Geben Sie den folgenden Befehl aus:

   ```
   lspv -u
   ```

   Auf einem IBM® Storwize-System werden beispielsweise die folgenden Informationen für jede Einheit angezeigt:

   ```
   hdisk4  00f8cf083fd97327  None  active
    3321360050763008101057800000000000003004214503IBMfcp
   ```

   In dem Beispiel ist *600507630081010578000000000000030* die UID für den Datenträger, die von der Storwize-Managementschnittstelle zurückgemeldet wurde.
   Um die Plattengröße in Megabyte zu überprüfen und den Wert mit dem für das System aufgelisteten Wert zu vergleichen, geben Sie den folgenden Befehl aus:

   ```
   bootinfo -s hdisk4
   ```

Linux-Systeme

Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

Vorgehensweise

1. Editieren Sie die Datei /etc/multipath.conf, um Multipathing für Linux-Hosts zu aktivieren. Wenn die Datei multipath.conf nicht vorhanden ist, können Sie die Datei erstellen, indem Sie den folgenden Befehl ausgeben:

   ```
   mpathconf --enable
   ```

   Die folgenden Parameter wurden in multipath.conf zu Testzwecken auf einem IBM Storwize-System festgelegt:

   ```
   defaults {
               user_friendly_names no
   }

   devices {
               device {
                           vendor "IBM "
                           product "2145"
                           path_grouping_policy group_by_prio
                           user_friendly_names no
                           path_selector "round-robin 0"
                           prio "alua"
                           path_checker "tur"
                           failback "immediate"
                           no_path_retry 5
                           rr_weight uniform
                           rr_min_io_rq "1"
                           dev_loss_tmo 120
              }
   }
   ```

2. Definieren Sie die Multipath-Option so, dass Multipath zusammen mit dem System gestartet wird. Geben Sie die folgenden Befehle aus:

   ```
   systemctl enable multipathd.service
   systemctl start multipathd.service
   ```

3. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath verwaltet werden, geben Sie den folgenden Befehl aus:

   ```
   multipath -l
   ```

4. Stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheiten-ID können Sie die aufgelisteten Platten identifizieren.
   Beispielsweise zeigt die folgende Ausgabe, dass einer 2-TB-Platte zwei Pfadgruppen und vier aktive Pfade zugeordnet sind. Die Größe von 2 TB bestätigt, dass die Platte einem Pooldateisystem entspricht. Suchen Sie anhand eines Teils der langen Einheiten-ID-Nummer (in diesem Beispiel 12) in der Managementschnittstelle des Plattensystems nach dem Datenträger.

   ```
   [root@tapsrv01 code]# multipath -l
   36005076802810c509800000000000012 dm-43 IBM,2145
    size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='round-robin 0' prio=0 status=active
   | |- 2:0:1:18 sdcw 70:64   active undef running
   | `- 4:0:0:18 sdgb 131:112 active undef running
   `-+- policy='round-robin 0' prio=0 status=enabled
     |- 1:0:1:18 sdat 66:208  active undef running
     `- 3:0:0:18 sddy 128:0   active undef running
   ```

   a. Korrigieren Sie, falls erforderlich, Platten-LUN/Host-Zuordnungen und erzwingen Sie eine erneute Busüberprüfung. Beispiel:

      ```
      echo "- - -" > /sys/class/scsi_host/host0/scan
      echo "- - -" > /sys/class/scsi_host/host1/scan
      echo "- - -" > /sys/class/scsi_host/host2/scan
      ```

      Sie können für eine erneute Überprüfung der Platten-LUN/Host-Zuordnungen auch das System erneut starten.
   b. Stellen Sie sicher, dass Platten jetzt für Multipath I/O verfügbar sind, indem Sie den Befehl multipath -l erneut ausgeben.
5. Verwenden Sie die Multipath-Ausgabe, um die Einheiten-IDs für jede Platteneinheit zu ermitteln und aufzulisten.

   Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte `36005076802810c509800000000000012`.

   Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

Windows-Systeme

Führen Sie die folgenden Schritte aus, um Multipathing für Plattenspeicher zu konfigurieren und zu aktivieren.

Vorgehensweise

1. Stellen Sie sicher, dass Multipath I/O installiert ist. Installieren Sie, falls erforderlich, weitere anbieterspezifische Multipath-Treiber.
2. Um sicherzustellen, dass Platten für das Betriebssystem sichtbar sind und durch Multipath I/O verwaltet werden, geben Sie den folgenden Befehl aus:

```
c:\Programme\IBM\SDDDSM\datapath.exe query device
```

3. Überprüfen Sie die Multipath-Ausgabe und stellen Sie sicher, dass jede Einheit aufgelistet ist und über so viele Pfade wie erwartet verfügt. Anhand der Größe und Einheitenseriennummer können Sie die aufgelisteten Platten identifizieren.
   Beispielsweise können Sie anhand eines Teils der langen Einheitenseriennummer (in diesem Beispiel 34) in der Managementschnittstelle des Plattensystems nach dem Datenträger suchen. Die Größe von 2 TB bestätigt, dass die Platte einem Speicherpooldateisystem entspricht.

```
DEV#:   4  DEVICE NAME: Disk5 Part0   TYPE: 2145    POLICY: OPTIMIZED
SERIAL: 600507630081010578000000000000034          LUN SIZE: 2.0TB
============================================================================
Path#          Adapter/Hard Disk       State   Mode    Select  Errors
    0   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
    1   Scsi Port2 Bus0/Disk5 Part0    OPEN    NORMAL   27176       0
    2   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL   28494       0
    3   Scsi Port3 Bus0/Disk5 Part0    OPEN    NORMAL       0       0
```

4. Erstellen Sie unter Verwendung der in der Multipath-Ausgabe im vorherigen Schritt zurückgegebenen Seriennummern eine Liste der Platteneinheiten-IDs.

   Beispielsweise ist die Einheiten-ID für Ihre 2-TB-Platte `600507630081010578000000000000034`.

   Sichern Sie die Liste der Einheiten-IDs für die Verwendung im nächsten Schritt.

5. Um neue Platten online zu schalten und das Lesezugriffsattribut zu löschen, führen Sie diskpart.exe mit den folgenden Befehlen aus. Wiederholen Sie diesen Schritt für jede der Platten:

```
diskpart
   select Disk 1
   online disk
   attribute disk clear readonly
   select Disk 2
   online disk
   attribute disk clear readonly
   < ... >
   select Disk 49
   online disk
   attribute disk clear readonly
   exit
```

Benutzer-ID für den Server erstellen

Erstellen Sie die Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz ist. Sie geben diese Benutzer-ID an, wenn Sie die Serverinstanz im Rahmen der Erstkonfiguration des Servers erstellen.

Informationen zu diesem Vorgang

Sie können nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstreichungszeichen (_) für die Benutzer-ID angeben. Die Benutzer-ID und der Gruppenname müssen den folgenden Regeln entsprechen:

- Die Länge darf 8 Zeichen nicht überschreiten.
- Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder einer Ziffer beginnen.
- Die Benutzer-ID und der Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* oder ein in SQL reserviertes Wortes sein.

Vorgehensweise

1. Erstellen Sie mithilfe von Betriebssystembefehlen eine Benutzer-ID.
   - AIX-BetriebssystemeLinux-BetriebssystemeErstellen Sie eine Gruppe und eine Benutzer-ID im Ausgangsverzeichnis des Benutzers, der Eigner der Serverinstanz ist.

     Um beispielsweise die Benutzer-ID tsminst1 in der Gruppe tsmsrvrs mit dem Kennwort tsminst1 zu erstellen, geben Sie die folgenden Befehle mit einer ID für einen Benutzer mit Verwaltungsaufgaben aus:

     AIX-Betriebssysteme

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

     Linux-Betriebssysteme

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Melden Sie sich von Ihrem System ab und anschließend wieder an. Wechseln Sie zu dem von Ihnen erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, wie beispielsweise Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es, falls erforderlich, ändern können.

-  Windows-BetriebssystemeErstellen Sie eine Benutzer-ID und fügen Sie dann die neue ID der Gruppe 'Administratoren' hinzu. Um beispielsweise die Benutzer-ID tsminst1 zu erstellen, geben Sie den folgenden Befehl aus:

  ```
  net user tsminst1 * /add
  ```

  Fügen Sie, nachdem Sie für den neuen Benutzer ein Kennwort erstellt und bestätigt haben, die Benutzer-ID der Gruppe 'Administratoren' hinzu, indem Sie die folgenden Befehle ausgeben:

  ```
  net localgroup Administratoren tsminst1 /add
  net localgroup DB2ADMNS tsminst1 /add
  ```

2. Melden Sie die neue Benutzer-ID ab.

Dateisysteme für den Server vorbereiten

Sie müssen die Dateisystemkonfiguration ausführen, damit der Plattenspeicher vom Server verwendet werden kann.

- Dateisysteme auf AIX-Systemen vorbereiten
  Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.
- Dateisysteme auf Linux-Systemen vorbereiten
  Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.
- Dateisysteme auf Windows-Systemen vorbereiten
  Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

Dateisysteme auf AIX-Systemen vorbereiten

Sie müssen Datenträgergruppen, logische Datenträger und Dateisysteme für den Server mithilfe von AIX Logical Volume Manager erstellen.

Vorgehensweise

1. Erhöhen Sie die Warteschlangenlänge und die maximale Übertragungsgröße für alle verfügbaren *hdiskX*-Platten. Geben Sie für jede Platte die folgenden Befehle aus:

   ```
   chdev -l hdisk4 -a max_transfer=0x100000
   chdev -l hdisk4 -a queue_depth=32
   chdev -l hdisk4 -a reserve_policy=no_reserve
   chdev -l hdisk4 -a algorithm=round_robin
   ```

   Sie dürfen diese Befehle nicht für interne Betriebssystemplatten, beispielsweise *hdisk0*, ausführen.
2. Erstellen Sie Datenträgergruppen für die IBM Spectrum Protect-Datenbank, die aktive Protokolldatei, das Archivprotokoll, die Datenbanksicherung und den Speicherpool. Geben Sie den Befehl mkvg unter Angabe der Einheiten-IDs für die entsprechenden zuvor ermittelten Platten aus.
   Wenn beispielsweise die Einheitennamen *hdisk4, hdisk5* und *hdisk6* Datenbankplatten entsprechen, schließen Sie diese in die Datenbankdatenträgergruppe ein.
   Systemgröße: Die folgenden Befehle basieren auf einer Konfiguration für ein mittelgroßes System. Für kleine und große Systeme müssen Sie die Syntax wie erforderlich anpassen.

   ```
   mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
   mkvg -S -y tsmactlog hdisk5
   mkvg -S -y tsmarchlog hdisk6
   mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
   mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
   ```

3. Bestimmen Sie die Namen der physischen Datenträger und die Anzahl freier physischer Partitionen, die beim Erstellen logischer Datenträger verwendet werden sollen. Geben Sie den Befehl lsvg für jede Datenträgergruppe aus, die Sie im vorherigen Schritt erstellt haben.
   Beispiel:

   ```
   lsvg -p tsmdb
   ```

   Die Ausgabe sieht ähnlich wie die folgende aus. Die Spalte *FREE PPs* gibt die freien physischen Partitionen an:

   ```
   tsmdb:
   PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
   hdisk4   active     1631       1631      327..326..326..326..326
   hdisk5   active     1631       1631      327..326..326..326..326
   hdisk6   active     1631       1631      327..326..326..326..326
   ```

4. Erstellen Sie mit dem Befehl mklv logische Datenträger in jeder Datenträgergruppe. Die Datenträgergröße, die Datenträgergruppe und die Einheitennamen sind, abhängig von der Größe Ihres Systems und Variationen in Ihrer Plattenkonfiguration, unterschiedlich.
   Um beispielsweise die Datenträger für die IBM Spectrum Protect-Datenbank auf einem mittelgroßen System zu erstellen, geben Sie die folgenden Befehle aus:

   ```
   mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
   mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
   mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
   ```

5. Formatieren Sie Dateisysteme auf jedem logischen Datenträger mit dem Befehl crfs.
   Um beispielsweise die Dateisysteme für die Datenbank auf einem mittelgroßen System zu formatieren, geben Sie die folgenden Befehle aus:

   ```
   crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
   crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
   crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
    -a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
   ```

6. Führen Sie für alle neu erstellten Dateisysteme einen Mount durch, indem Sie den folgenden Befehl eingeben:

   ```
   mount -a
   ```

7. Listen Sie alle Dateisysteme auf, indem Sie den Befehl df ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.
   Das folgende Beispiel der Befehlsausgabe zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

   ```
   tapsrv07> df -g /tsminst1/*
   Filesystem      GB blocks  Free     %Used   Iused   %Iused   Mounted on
   /dev/tsmact00   195.12     194.59   1%      4       1%       /tsminst1/TSMalog
   ```

8. Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den Server hat.

Dateisysteme auf Linux-Systemen vorbereiten

Sie müssen ext4- oder xfs-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

Vorgehensweise

1. Verwenden Sie die zuvor generierte Liste der Einheiten-IDs und geben Sie den Befehl mkfs aus, um für jede LUN-Speichereinheit ein Dateisystem zu erstellen und zu formatieren. Geben Sie die Einheiten-ID im Befehl an. Siehe die folgenden Beispiele. Formatieren Sie für die Datenbank ext4-Dateisysteme:

   ```
   mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c509800000000000012
   ```

   Formatieren Sie für Speicherpool-LUNs xfs-Dateisysteme:

   ```
   mkfs -t xfs /dev/mapper/360050763008101057800000000002c3
   ```

   Abhängig davon, wie viele verschiedene Einheiten vorhanden sind, können Sie den Befehl mkfs bis zu 50 Mal ausgeben.

2. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.

   Geben Sie den Befehl mkdir für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte.

   Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

   ```
   mkdir /tsminst1
   ```

   Wiederholen Sie den Befehl mkdir für jedes Dateisystem.
3. Fügen Sie in der Datei /etc/fstab für jedes Dateisystem einen Eintrag hinzu, damit für die Dateisysteme beim Serverstart automatisch ein Mount durchgeführt wird.
   Beispiel:

   ```
   /dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
   ```

4. Führen Sie für die Dateisysteme, die der Datei /etc/fstab hinzugefügt wurden, einen Mount durch, indem Sie den Befehl mount -a ausgeben.
5. Listen Sie alle Dateisysteme auf, indem Sie den Befehl df ausgeben. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Überprüfen Sie außerdem den verfügbaren Speicherbereich.
   Das folgende Beispiel für ein IBM® Storwize-System zeigt, dass der Umfang des belegten Speicherbereichs normalerweise 1 % beträgt:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem                                      Size  Used Avail Use% Mounted on
/dev/mapper/3600507630081010578000000000000003 134G  188M 132G  1%   /tsminst1/TSMalog
```

6. Überprüfen Sie, ob die in Benutzer-ID für den Server erstellen erstellte Benutzer-ID Schreib-/Lesezugriff auf die Verzeichnisse für den IBM Spectrum Protect-Server hat.

Dateisysteme auf Windows-Systemen vorbereiten

Sie müssen NTFS-Dateisysteme für jede der Platten-LUNs formatieren, die vom IBM Spectrum Protect-Server verwendet werden sollen.

Vorgehensweise

1. Erstellen Sie Mountpunktverzeichnisse für Dateisysteme.
   Geben Sie den Befehl md für jedes Verzeichnis aus, das erstellt werden muss. Verwenden Sie die in den Arbeitsblättern zur Planung verwendeten Verzeichniswerte. Um beispielsweise das Serverinstanzverzeichnis unter Verwendung des Standardwerts zu erstellen, geben Sie den folgenden Befehl aus:

   ```
   md c:\tsminst1
   ```

   Wiederholen Sie den Befehl md für jedes Dateisystem.
2. Erstellen Sie für jede Platten-LUN, die einem Verzeichnis unter dem Serverinstanzverzeichnis zugeordnet ist, unter Verwendung des Windows-Datenträgermanagers (Volume-Manager) einen Datenträger.

   Rufen Sie Server-Manager > Datei- und Speicherdienste auf und führen Sie die folgenden Schritte für jede Platte aus, die der im vorherigen Schritt erstellten LUN-Zuordnung entspricht:

   a. Schalten Sie die Platte online.
   b. Initialisieren Sie die Platte mit dem GPT-Basistyp, dem Standardwert.
   c. Erstellen Sie einen einfachen Datenträger, der den gesamten Speicherbereich auf der Platte belegt. Formatieren Sie das Dateisystem mit NTFS und ordnen Sie einen Kennsatz zu, der den Zweck des Datenträgers angibt, wie beispielsweise TSMfile00. Ordnen Sie den neuen Datenträger keinem Laufwerkbuchstaben zu. Ordnen Sie den Datenträger stattdessen einem Verzeichnis unter dem Instanzverzeichnis zu, wie beispielsweise C:\tsminst1\TSMfile00.
      Tipp: Legen Sie den Datenträgerkennsatz und die Bezeichnungen für Verzeichniszuordnungen auf der Basis der Größe der aufgelisteten Platte fest.
3. Stellen Sie sicher, dass Dateisysteme an der korrekten LUN und am korrekten Mountpunkt bereitgestellt werden. Listen Sie alle Dateisysteme auf, indem Sie den Befehl mountvol ausgeben; überprüfen Sie dann die Ausgabe. Beispiel:

   ```
   \\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\
     C:\tsminst1\TSMdbspace00\
   ```

4. Starten Sie nach dem Abschluss der Plattenkonfiguration das System erneut.

Nächste Schritte

Mithilfe von Windows Explorer können Sie den Umfang des freien Speicherbereichs für jeden Datenträger prüfen.

Server und das Operations Center installieren

Verwenden Sie den grafisch orientierten Assistenten von IBM® Installation Manager, um die Komponenten zu installieren.

- Installation auf AIX- und Linux-Systemen
  Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.
- Installation auf Windows-Systemen
  Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

Installation auf AIX- und Linux-Systemen

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

Vorbereitende Schritte

Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.

Vorgehensweise

1. AIX-BetriebssystemeÜberprüfen Sie, ob die erforderlichen RPM-Dateien auf Ihrem System installiert sind.

Ausführliche Informationen finden Sie in Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren.

2. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042992.
3. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
4. Stellen Sie sicher, dass für das Paket die Berechtigung zur Ausführung festgelegt ist. Ändern Sie, falls erforderlich, die Dateiberechtigungen, indem Sie den folgenden Befehl ausgeben:

   ```
   chmod a+x Paketname.bin
   ```

5. Extrahieren Sie das Paket, indem Sie den folgenden Befehl ausgeben:

   ```
   ./Paketname.bin
   ```

   Dabei ist *Paketname* der Name der Downloaddatei.
6. AIX-BetriebssystemeStellen Sie sicher, dass der folgende Befehl aktiviert ist, damit die Assistenten korrekt ausgeführt werden:

   ```
   lsuser
   ```

   Standardmäßig ist der Befehl aktiviert.
7. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
8. Starten Sie den Installationsassistenten, indem Sie den folgenden Befehl ausgeben:

   ```
   ./install.sh
   ```

   Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM Installation Manager gespeichert sind.

  Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.

- Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren
  RPM-Dateien sind für den grafisch orientierten Assistenten von IBM Installation Manager erforderlich.

Installation auf Windows-Systemen

Installieren Sie den IBM Spectrum Protect-Server und das Operations Center auf demselben System.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Überprüfen Sie, ob das Betriebssystem auf die erforderliche Sprache gesetzt ist. Standardmäßig entspricht die Sprache für das Betriebssystem der Sprache für den Installationsassistenten.
- Stellen Sie sicher, dass die Benutzer-ID, die während der Installation verwendet werden soll, für einen Benutzer mit der Berechtigung eines lokalen Administrators gilt.

Vorgehensweise

1. Überprüfen Sie vor dem Herunterladen des Installationspakets, ob genügend Speicherbereich zum Speichern der Installationsdateien vorhanden ist, wenn die Dateien aus dem Produktpaket extrahiert werden. Informationen zum Speicherbedarf enthält das Downloaddokument unter Technote 4042993.
2. Rufen Sie Passport Advantage auf und laden Sie die Paketdatei in ein leeres Verzeichnis Ihrer Wahl herunter.
3. Wechseln Sie in das Verzeichnis, in das die ausführbare Datei gestellt wurde.
4. Doppelklicken Sie auf die ausführbare Datei, um die Datei in das aktuelle Verzeichnis zu extrahieren.
5. Starten Sie in dem Verzeichnis, in das die Installationsdateien extrahiert wurden, den Installationsassistenten, indem Sie auf die Datei install.bat doppelklicken. Wenn Sie die zu installierenden Pakete auswählen, wählen Sie sowohl den Server als auch das Operations Center aus.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden die Fehler in Protokolldateien aufgezeichnet, die im Protokollverzeichnis von IBM® Installation Manager gespeichert sind.

Um Installationsprotokolldateien in Installation Manager anzuzeigen, klicken Sie auf Datei > Protokoll anzeigen. Um diese Protokolldateien in Installation Manager zu erfassen, klicken Sie auf Hilfe > Daten zur Fehleranalyse exportieren.

- Rufen Sie nach der Installation des Servers, aber vor der Anpassung des Servers für Ihre Verwendung die IBM Spectrum Protect-Unterstützungssite auf. Klicken Sie auf Support und Downloads und wenden Sie alle zutreffenden Fixes an.

Server und das Operations Center konfigurieren

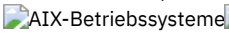
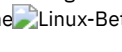
Nachdem Sie die Komponenten installiert haben, führen Sie die Konfiguration für den IBM Spectrum Protect-Server und das Operations Center aus.

- Serverinstanz konfigurieren
  Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.
- Client für Sichern/Archivieren installieren
  Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.
- Optionen für den Server festlegen
  Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.
- Sicherheitskonzepte
  Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.
- Operations Center konfigurieren
  Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.
- Produktlizenz registrieren
  Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.
- Datenaufbewahrungsregeln für Ihr Unternehmen definieren
  Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datendeduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.
- Zeitpläne für Serververwaltungsaktivitäten definieren
  Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.
- Clientzeitpläne definieren
  Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

Serverinstanz konfigurieren

Verwenden Sie den IBM Spectrum Protect-Assistenten für die Serverinstanzkonfiguration, um die Erstkonfiguration für den Server auszuführen.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:
 AIX-Betriebssysteme  Linux-Betriebssysteme

- Auf dem System, auf dem IBM Spectrum Protect installiert wurde, muss der X Window System-Client vorhanden sein. Außerdem muss ein X Window System-Server auf Ihrem Desktop ausgeführt werden.
- Für das System muss das Secure Shell-Protokoll (SSH-Protokoll) aktiviert sein. Stellen Sie sicher, dass der Port auf den Standardwert 22 gesetzt ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei sshd_config im Verzeichnis /etc/ssh/ aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämonservice über die Zugriffsberechtigungen verfügt, um mithilfe des Werts *localhost* eine Verbindung zum System herstellen zu können.
- Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt hatten, unter Verwendung des SSH-Protokolls bei IBM Spectrum Protect anmelden können. Wenn Sie den Assistenten verwenden, müssen Sie diese Benutzer-ID und das Kennwort für den Zugriff auf dieses System angeben.
- Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

 Windows-BetriebssystemeÜberprüfen Sie, ob der Remoteregistrierungsdienst gestartet wurde, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf Start > Verwaltung > Dienste. Wählen Sie im Fenster Dienste Remoteregistrierung aus. Wurde der Dienst nicht gestartet, klicken Sie auf Starten.
2. Stellen Sie sicher, dass die Ports 137, 139 und 445 nicht durch eine Firewall blockiert sind:
   a. Klicken Sie auf Start > Systemsteuerung > Windows-Firewall.
   b. Wählen Sie Erweiterte Einstellungen aus.
   c. Wählen Sie Eingehende Regeln aus.
   d. Wählen Sie Neue Regel aus.

e. Erstellen Sie eine Portregel für die TCP-Ports 137, 139 und 445, um Verbindungen für Domänennetze und private Netze zu ermöglichen.

3. Konfigurieren Sie die Benutzerkontensteuerung, indem Sie auf die Optionen für die lokale Sicherheitsrichtlinie zugreifen und die folgenden Schritte ausführen.
   a. Klicken Sie auf Start > Verwaltung > Lokale Sicherheitsrichtlinie. Erweitern Sie Lokale Richtlinien > Sicherheitsoptionen.
   b. Falls noch nicht bereits aktiviert, aktivieren Sie das integrierte Administratorkonto, indem Sie Konten: Administratorkontostatus > Aktivieren > OK auswählen.
   c. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für alle Windows-Administratoren, indem Sie Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen > Inaktivieren > OK auswählen.
   d. Falls noch nicht bereits inaktiviert, inaktivieren Sie die Benutzerkontensteuerung für das integrierte Administratorkonto, indem Sie Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto > Inaktivieren > OK auswählen.
4. Wenn Sie in den vorhergehenden Schritten Änderungen an den Einstellungen vorgenommen haben, starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.

Informationen zu diesem Vorgang

Der Assistent kann gestoppt und erneut gestartet werden, der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

Vorgehensweise

1. Starten Sie die lokale Version des Assistenten.
   - AIX-BetriebssystemeLinux-BetriebssystemeÖffnen Sie das Programm dsmicfgx im Verzeichnis /opt/tivoli/tsm/server/bin. Dieser Assistent kann nur als Rootbenutzer ausgeführt werden.
   - Windows-BetriebssystemeKlicken Sie auf Start > Alle Programme > IBM Spectrum Protect > Konfigurationsassistent.
2. Führen Sie die Anweisungen aus, um die Konfiguration auszuführen. Verwenden Sie die während der IBM Spectrum Protect-Systemkonfiguration aufgezeichneten Informationen (siehe Arbeitsblätter zur Planung), um Verzeichnisse und Optionen im Assistenten anzugeben.

   AIX-BetriebssystemeLinux-BetriebssystemeLegen Sie im Fenster Serverinformationen fest, dass der Server automatisch unter Verwendung der Instanzbenutzer-ID gestartet werden soll, wenn das System bootet.

   Windows-BetriebssystemeMithilfe des Konfigurationsassistenten wird festgelegt, dass der Server automatisch gestartet werden soll, wenn ein Warmstart durchgeführt wird.

Client für Sichern/Archivieren installieren

Installieren Sie als Best Practice den IBM Spectrum Protect-Client für Sichern/Archivieren auf dem Serversystem, sodass der Verwaltungsbefehlszeilenclient und der Scheduler verfügbar sind.

Vorgehensweise

Um den Client für Sichern/Archivieren zu installieren, führen Sie die Installationsanweisungen für Ihr Betriebssystem aus.

- UNIX- und Linux-Clients für Sichern/Archivieren installieren
- Windows-Client für Sichern/Archivieren installieren

Optionen für den Server festlegen

Überprüfen Sie die Serveroptionsdatei, die mit dem IBM Spectrum Protect-Server installiert wird, um sicherzustellen, dass die korrekten Werte für Ihr System festgelegt sind.

Vorgehensweise

1. Wechseln Sie in das Serverinstanzverzeichnis und öffnen Sie die Datei dsmserv.opt.
2. Überprüfen Sie die Werte in der folgenden Tabelle und Ihre Serveroptionseinstellungen auf der Basis der Systemgröße.

Serveroption	**Wert**
ACTIVELOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad
ACTIVELOGSIZE	131072
ARCHLOGCOMPRESS	No
ARCHLOGDIRECTORY	Während der Konfiguration angegebener Verzeichnispfad
COMMMETHOD	TCPIP

Serveroption	Wert
COMMTIMEOUT	3600
DEVCONFIG	devconf.dat
EXPINTERVAL	0
IDLETIMEOUT	60
MAXSESSIONS	500
NUMOPENVOLSALLOWED	20
TCPADMINPORT	1500
TCPPORT	1500
VOLUMEHISTORY	volhist.dat

Aktualisieren Sie, falls erforderlich, Serveroptionseinstellungen in Übereinstimmung mit den Werten in der Tabelle. Um Aktualisierungen durchzuführen, schließen Sie die Datei dsmserv.opt und definieren Sie die Optionen mit dem Befehl SETOPT in der Verwaltungsbefehlszeilenschnittstelle.
Um beispielsweise die Option IDLETIMEOUT mit 60 zu aktualisieren, geben Sie den folgenden Befehl aus:

```
setopt idletimeout 60
```

3. Um für den Server, die Clients und das Operations Center die sichere Kommunikation zu konfigurieren, überprüfen Sie die Optionen in der folgenden Tabelle.

Serveroption	Alle Systemgrößen
SSLDISABLELEGACYTLS	YES
SSLFIPSMODE	NO
SSLTCPPORT	Geben Sie die SSL-Portnummer an. Der TCP/IP-DFV-Treiber des Servers wartet an diesem Port auf Anforderungen für SSL-fähige Sitzungen vom Client.
SSLTCPADMINPORT	Geben Sie die Adresse des Ports an, an dem der Server auf Anforderungen von SSL-fähigen Sitzungen des Verwaltungsbefehlszeilenclients wartet.
SSLTLS12	YES

Wenn einer der Optionswerte aktualisiert werden muss, editieren Sie die Datei dsmserv.opt unter Verwendung der folgenden Anleitungen:
   - Entfernen Sie den Stern am Anfang einer Zeile, um eine Option zu aktivieren.
   - Geben Sie in jeder Zeile nur eine einzige Option und den für die Option angegebenen Wert ein.
   - Wenn eine Option in mehreren Einträgen in der Datei vorkommt, verwendet der Server den letzten Eintrag.

Sichern Sie Ihre Änderungen und schließen Sie die Datei. Wenn Sie die Datei dsmserv.opt direkt editieren, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

Sicherheitskonzepte

Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

Transport Layer Security

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtsicherheit für eine sichere Verbindung zwischen Servern, Clients und Speicheragenten bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, verwenden Sie SSL oder TLS zum Verschlüsseln der Daten.

Tipp: In der gesamten IBM Spectrum Protect-Dokumentation gilt jede Angabe von "SSL" oder zum "Auswählen von SSL" für TLS.

SSL wird von Global Security Kit (GSKit) bereitgestellt, das zusammen mit dem IBM Spectrum Protect-Server installiert wird, der vom Server, vom Client und vom Speicheragenten verwendet wird.

Einschränkung: Sie dürfen die SSL- oder TLS-Protokolle nicht für die Kommunikation mit einer DB2-Datenbankinstanz verwenden, die von IBM Spectrum Protect-Servern verwendet wird.

Jeder Server, Client oder Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdiges selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle (CA) signiert ist. Sie können Ihre eigenen Zertifikate verwenden oder Zertifikate bei einer Zertifizierungsstelle (CA) kaufen. Jedes der Zertifikate muss installiert und der Schlüsseldatenbank auf dem IBM Spectrum Protect-Server, -Client oder -Speicheragenten hinzugefügt werden. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet. Einige CA-Zertifikate sind in der Schlüsseldatenbank standardmäßig vorinstalliert.

SSL wird auf dem IBM Spectrum Protect-Server, -Client und -Speicheragenten unabhängig voneinander konfiguriert.

Berechtigungsstufen

Für jeden IBM Spectrum Protect-Server sind verschiedene Administratorberechtigungsstufen verfügbar, die die Tasks festlegen, die ein Administrator ausführen kann.

Nach der Registrierung muss einem Administrator Berechtigung erteilt werden, indem ihm eine oder mehrere Administratorberechtigungsstufen zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen und anderen Administratoren über den Befehl GRANT AUTHORITY Berechtigungsstufen zuordnen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Ein Administrator kann andere Administrator-IDs registrieren, den IDs Berechtigungsstufen zuordnen, IDs umbenennen, IDs entfernen und IDs für den Server sperren oder entsperren.

Ein Administrator kann den Zugriff auf bestimmte Clientknoten für Rootbenutzer-IDs und Nicht-Rootbenutzer-IDs steuern. Standardmäßig kann eine Nicht-Rootbenutzer-ID keine Daten auf dem Knoten sichern. Ändern Sie mit dem Befehl UPDATE NODE die Knoteneinstellungen, um Sicherungen zu ermöglichen.

Kennwörter

Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer beim Zugriff auf den Server ein Kennwort eingeben.

Verwenden Sie LDAP (Lightweight Directory Access Protocol), um striktere Anforderungen für Kennwörter anzuwenden. Weitere Informationen finden Sie in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1).

Tabelle 1. Merkmale der Kennwortauthentifizierung

Merkmale	Weitere Informationen
Abhängigkeit von der Groß-/Kleinschreibung	Nicht von der Groß-/Kleinschreibung abhängig.
Standardwert für Kennwortablauf	90 Tage. Der Ablaufzeitraum beginnt mit der ersten Registrierung einer Administrator-ID oder eines Clientknotens beim Server. Wenn das Kennwort innerhalb dieses Zeitraums nicht geändert wird, muss das Kennwort beim nächsten Zugriff des Benutzers auf den Server geändert werden.
Ungültige Kennworteingabeversuche	Sie können einen Grenzwert für aufeinanderfolgende ungültige Kennworteingabeversuche für alle Clientknoten definieren. Wenn der Grenzwert überschritten wird, sperrt der Server den Knoten.
Kennwortlänge	Der Administrator kann eine Mindestlänge angeben.

Sitzungssicherheit

Die Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, -Verwaltungsclients und -Servern verwendet wird und mit dem Parameter SESSIONSECURITY festgelegt wird.

Der Parameter SESSIONSECURITY kann auf einen der folgenden Werte gesetzt werden:

- Mit dem Wert STRICT wird die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, -Knoten und -Administratoren durchgesetzt.
- Der Wert TRANSITIONAL gibt an, dass das vorhandene Kommunikationsprotokoll verwendet wird, wenn Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Wenn SESSIONSECURITY=TRANSITIONAL angegeben ist, werden strengere Sicherheitseinstellungen automatisch durchgesetzt, da höhere Versionen des TLS-Protokolls verwendet werden, wenn die Software auf Version 8.1.2 oder höher aktualisiert wird. Nachdem ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch in den Wert STRICT geändert und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder unter Verwendung früherer TLS-Protokolle authentifizieren.

Weitere Informationen zu den Werten für den Parameter SESSIONSECURITY enthalten die Beschreibungen der folgenden Befehle.

Tabelle 2. Befehle zum Festlegen des Parameters SESSIONSECURITY

Entität	Befehl
Clientknoten	• REGISTER NODE • UPDATE NODE
Administratoren	• REGISTER ADMIN • UPDATE ADMIN

Entität	Befehl
Server	• DEFINE SERVER • UPDATE SERVER

Administratoren, die sich unter Verwendung des Befehls DSMADMC, des Befehls DSMC oder des Programms dsm authentifizieren, können sich nach der Authentifizierung unter Verwendung von Version 8.1.2 oder höher nicht unter Verwendung einer früheren Version authentifizieren. Die folgenden Tipps liefern Informationen zur Behebung von Authentifizierungsproblemen für Administratoren:
Tipps:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die das Administratorkonto für die Anmeldung verwendet, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto über mehrere Systeme anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf jedem System installiert ist.
- Nachdem sich ein Administrator bei einem Server der Version 8.1.2 oder höher unter Verwendung eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich der Administrator nur auf Clients oder Servern authentifizieren, die Version 8.1.2 oder höher verwenden. Ein Administratorbefehl kann von jedem beliebigen System ausgegeben werden.
- Erstellen Sie, falls erforderlich, ein separates Administratorkonto, das nur mit Clients und Servern verwendet wird, die Software der Version 8.1.1 oder früher verwenden.

Setzen Sie die höchste Sicherheitsstufe für die Kommunikation mit dem IBM Spectrum Protect-Server durch, indem Sie sicherstellen, dass alle Knoten, Administratoren und Server die Sitzungssicherheit STRICT verwenden. Mithilfe des Befehls SELECT können Sie feststellen, welche Server, Knoten und Administratoren die Sitzungssicherheit TRANSITIONAL verwenden und für die Verwendung der Sitzungssicherheit STRICT aktualisiert werden sollten.

- Sichere Kommunikation mit Transport Layer Security konfigurieren
  Um Daten zu verschlüsseln und die sichere Kommunikation in Ihrer Umgebung zu ermöglichen, ist Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) auf dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren aktiviert. Kommunikationsanforderungen zwischen dem Server und dem Client werden mithilfe eines SSL-Zertifikats geprüft.

Zugehörige Tasks:
Kommunikation schützen

Operations Center konfigurieren

Führen Sie nach der Installation des Operations Center die folgenden Konfigurationsschritte aus, um mit der Verwaltung Ihrer Speicherumgebung zu beginnen.

Vorbereitende Schritte

Wenn Sie zum ersten Mal die Verbindung zum Operations Center herstellen, müssen Sie die folgenden Informationen angeben:

- Verbindungsinformationen für den Server, der als Hub-Server festgelegt werden soll
- Anmeldeberechtigungsnachweise für eine Administrator-ID, die für diesen Server definiert ist

Vorgehensweise

1. Legen Sie den Hub-Server fest. Geben Sie in einem Web-Browser die folgende Adresse ein:

   `https://`*`Hostname`*`:`*`sicherer_Port`*`/oc`

   Erläuterungen:
   - *Hostname* gibt den Namen des Computers an, auf dem das Operations Center installiert ist.
   - *Sicherer_Port* gibt die Portnummer an, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet.

   Wenn beispielsweise der Hostname tsm.storage.mylocation.com lautet und der standardmäßige sichere Port für das Operations Center (Port 11090) verwendet wird, ist die Adresse wie folgt:

   ```
   https://tsm.storage.mylocation.com:11090/oc
   ```

   Wenn Sie sich zum ersten Mal beim Operations Center anmelden, führt Sie ein Assistent durch eine Erstkonfiguration, um einen neuen Administrator mit Systemberechtigung auf dem Server zu konfigurieren.

2. Konfigurieren Sie die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server, indem Sie das Protokoll Secure Sockets Layer (SSL) konfigurieren.

   Führen Sie die Anweisungen in Kommunikation zwischen dem Operations Center und dem Hub-Server schützen aus.

3. Optional: Um einen täglichen E-Mail-Bericht mit einer Zusammenfassung des Systemstatus zu empfangen, konfigurieren Sie Ihre E-Mail-Einstellungen im Operations Center.

   Führen Sie die Anweisungen in Systemstatus mithilfe von E-Mail-Berichten verfolgen aus.

- Kommunikation zwischen dem Operations Center und dem Hub-Server schützen
  Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server zu ermöglichen, fügen Sie das TLS-Zertifikat des Hub-Servers der Truststore-Datei des Operations Center hinzu.

Produktlizenz registrieren

Verwenden Sie zum Registrieren Ihrer Lizenz für das Produkt IBM Spectrum Protect den Befehl REGISTER LICENSE.

Informationen zu diesem Vorgang

Lizenzen werden in Registrierungszertifikatsdateien gespeichert, die Lizenzinformationen für das Produkt enthalten. Die Registrierungszertifikatsdateien befinden sich auf den Installationsmedien und werden während der Installation auf den Server gestellt. Wenn Sie das Produkt registrieren, werden die Lizenzen in einer NODELOCK-Datei im aktuellen Verzeichnis gespeichert.

Vorgehensweise

Registrieren Sie eine Lizenz, indem Sie den Namen der Registrierungszertifikatsdatei angeben, die die Lizenz enthält. Um den Command Builder des Operations Center für diese Task zu verwenden, führen Sie die folgenden Schritte aus.

1. Öffnen Sie das Operations Center.
2. Öffnen Sie den Command Builder des Operations Center, indem Sie den Mauszeiger über das Symbol für Einstellungen bewegen und auf Command Builder klicken.
3. Geben Sie den Befehl REGISTER LICENSE aus. Um beispielsweise eine IBM Spectrum Protect-Basislizenz zu registrieren, geben Sie den folgenden Befehl aus:

   ```
   register license file=tsmbasic.lic
   ```

Nächste Schritte

Sichern Sie die Installationsmedien, die Ihre Registrierungszertifikatsdateien enthalten. Möglicherweise müssen Sie Ihre Lizenz erneut registrieren, wenn beispielsweise eine der folgenden Bedingungen erfüllt ist:

- Der Server wird auf einen anderen Computer versetzt.
- Die NODELOCK-Datei ist beschädigt. Der Server speichert Lizenzinformationen in der NODELOCK-Datei, die sich in dem Verzeichnis befindet, von dem aus der Server gestartet wird.
- Linux-BetriebssystemeSie ändern den Prozessorchip, der dem Server zugeordnet ist, auf dem der Server installiert ist.

Datenaufbewahrungsregeln für Ihr Unternehmen definieren

Nachdem Sie einen Verzeichniscontainerspeicherpool für die Datendeduplizierung erstellt haben, aktualisieren Sie die Serverstandardmaßnahme für die Verwendung des neuen Speicherpools. Die Seite Services im Operations Center wird vom Assistenten Speicherpool hinzufügen zur Ausführung dieser Task geöffnet.

Vorgehensweise

1. Wählen Sie auf der Seite Services im Operations Center die Domäne STANDARD aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen. Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.
3. Klicken Sie auf die Umschaltfläche Konfigurieren und führen Sie die folgenden Änderungen durch:
   - Ändern Sie das Sicherungsziel für die Verwaltungsklasse STANDARD in den Verzeichniscontainerspeicherpool.
   - Ändern Sie den Wert für die Spalte 'Sicherungen' in Keine Begrenzung.
   - Ändern Sie den Aufbewahrungszeitraum. Setzen Sie den Wert für die Spalte 'Zusätzliche Sicherungen aufbewahren' abhängig von Ihren Geschäftsanforderungen auf 30 Tage oder mehr.
4. Sichern Sie Ihre Änderungen und klicken Sie erneut auf die Umschaltfläche Konfigurieren, damit die Maßnahmengruppe nicht mehr editierbar ist.
5. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.

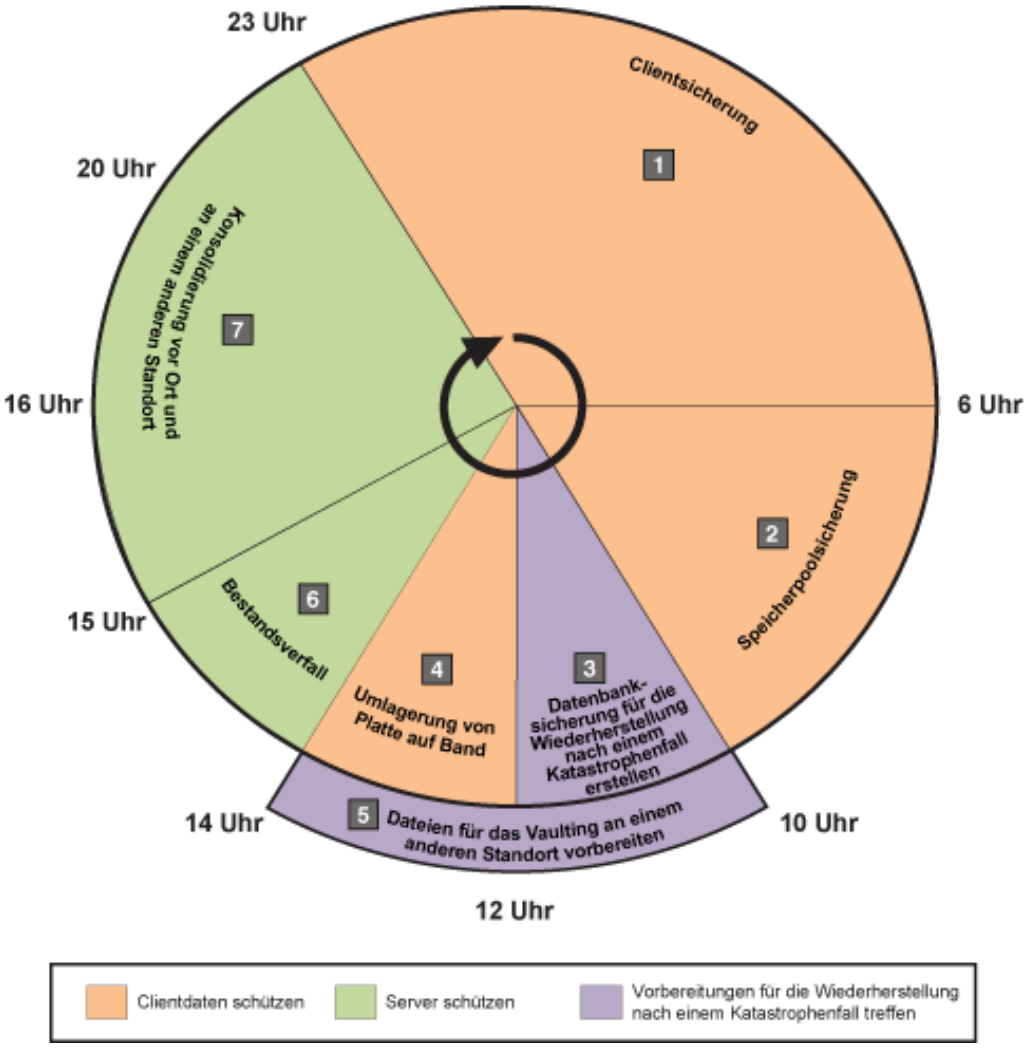
Zeitpläne für Serververwaltungsaktivitäten definieren

Erstellen Sie Zeitpläne für jede Serververwaltungsoperation, indem Sie den Befehl DEFINE SCHEDULE im Command Builder des Operations Center verwenden.

Informationen zu diesem Vorgang

Planen Sie die Ausführung von Serververwaltungsoperationen im Anschluss an Clientsicherungsoperationen. Sie können das Timing von Zeitplänen steuern, indem Sie die Startzeit in Kombination mit der Dauer für jede Operation definieren.

Die folgende Abbildung zeigt ein Beispiel für die Planung von Verwaltungsoperationen.
Abbildung 1. Tagesplan der Serveroperationen für eine Bandspeicherlösung



Die folgende Tabelle zeigt die Planung von Serververwaltungsprozessen in Kombination mit dem Clientsicherungszeitplan für eine Bandspeicherlösung.

Operation	Zeitplan
Clientsicherung	Startet um 23 Uhr.
Speicherpoolsicherung	Startet um 6 Uhr.
Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall	• Die Datenbanksicherungsoperation startet um 10 Uhr bzw. 11 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt. • Die Sicherungsoperationen für Einheitenkonfigurationsinformationen und das Datenträgerprotokoll starten um 17 Uhr bzw. 7 Stunden nach dem Start der Datenbanksicherungsoperation. • Das Löschen des Datenträgerprotokolls startet um 20 Uhr bzw. 10 Stunden nach dem Start der Datenbanksicherungsoperation.
Vorbereitung der Dateien für das Vaulting an einem anderen Standort	Startet um 10 Uhr zu demselben Zeitpunkt wie die Verarbeitung für die Datenbank und die Dateien zur Wiederherstellung nach einem Katastrophenfall.
Umlagerung von Platte auf Band	Startet um 12 Uhr bzw. 2 Stunden nach dem Start der Datenbanksicherungsoperation.
Bestandsverfall	Startet um 14 Uhr bzw. 15 Stunden nach dem Start der Clientsicherungsoperation. Dieser Prozess wird bis zum Abschluss ausgeführt.
Speicherbereichskonsolidierung	Startet um 15 Uhr bzw. 16 Stunden nach dem Start der Clientsicherungsoperation.

Vorgehensweise

Erstellen Sie nach dem Konfigurieren der Einheitenklasse für die Datenbanksicherungsoperationen Zeitpläne für Datenbanksicherungsoperationen und andere erforderliche Verwaltungsoperationen mithilfe des Befehls DEFINE SCHEDULE. Abhängig von der Größe Ihrer Umgebung müssen Sie die Startzeiten für jeden Zeitplan in dem Beispiel gegebenenfalls anpassen.

1. Definieren Sie eine Einheitenklasse für die Sicherungsoperation, bevor Sie den Zeitplan für Datenbanksicherungen erstellen. Erstellen Sie mit dem Befehl DEFINE DEVCLASS eine Einheitenklasse mit dem Namen LTOTAPE:

   ```
   define devclass ltotape devtype=lto library=ltolib
   ```

2. Legen Sie die Einheitenklasse für automatische Datenbanksicherungen fest. Geben Sie mit dem Befehl SET DBRECOVERY die im vorhergehenden Schritt für die Datenbanksicherung erstellte Einheitenklasse an. Wenn beispielsweise die Einheitenklasse den Namen LTOTAPE hat, geben Sie den folgenden Befehl aus:

   ```
   set dbrecovery ltotape
   ```

3. Erstellen Sie mithilfe des Befehls DEFINE SCHEDULE Zeitpläne für die Verwaltungsoperationen. Die folgende Tabelle enthält die erforderlichen Operationen und Beispiele der Befehle.

Operation	**Beispielbefehle und weitere Informationen**
Sichern von Speicherpools	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP STGPOOL. Geben Sie beispielsweise den folgenden Befehl aus, um einen Sicherungszeitplan für einen primären Speicherpool mit dem Namen PRIMARY_POOL zu erstellen. Der Pool wird in einem Kopienspeicherpool mit dem Namen COPYSTG gesichert: `define schedule BACKUPSTGPOOL type=administrative cmd="backup stgpool primary_pool copystg" active=yes starttime=06:00 period=1`
Sichern der Datenbank	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DB. Geben Sie beispielsweise den folgenden Befehl aus, um einen Sicherungszeitplan zu erstellen, der die neue Einheitenklasse verwendet: `define schedule DBBACKUP type=admin cmd="backup db devclass=ltotape type=full numstreams=3 wait=yes compress=yes" active=yes desc="Datenbank sichern." startdate=today starttime=10:00:00 duration=45 durunits=minutes`
Replizieren von Knoten	Verwenden Sie wahlweise die Knotenreplikation, um Clientdaten zu schützen, indem Sie die Daten auf einem sekundären Server sichern. Anweisungen finden Sie in Clientdaten auf einen anderen Server replizieren. Stellen Sie sicher, dass die Knotenreplikation abgeschlossen ist, bevor Umlagerungsoperationen beginnen.

Operation	Beispielbefehle und weitere Informationen
Tägliches Umlagern von Daten von Platte auf Band	Erstellen Sie einen Zeitplan für die Speicherpoolumlagerung. Wenn beispielsweise ein Plattenspeicherpool mit dem Namen DISKPOOL vorhanden ist und der nächste Speicherpool der Speicherpool mit dem Namen TAPEPOOL ist, können Sie die Speicherpoolumlagerung planen, indem Sie den folgenden Befehl ausgeben: `define schedule stgpool_migration type=administrative cmd="migrate stgpool diskpool lomig=0" active=yes description="Plattenspeicherpool in Bandpool umlagern" startdate=today starttime=12:00 duration=2 durunits=hours period=1 perunits=days` Um den Durchsatz zu maximieren, können Sie die Anzahl paralleler Prozesse angeben, die für die Umlagerung von Dateien verwendet werden soll, indem Sie die folgenden Schritte ausführen: a. Stellen Sie für den Bandspeicherpool sicher, dass die Kollokation aktiviert ist. Um zu überprüfen, ob die Kollokation aktiviert ist, führen Sie den Befehl QUERY STGPOOL aus. Stellen Sie sicher, dass der Wert `GROUP`, `NODE` oder `FILESPACE` im Feld `COLLOCATE` angegeben ist. Wenn der Wert `GROUP`, `NODE` oder `FILESPACE` nicht angegeben ist, verwenden Sie den Befehl UPDATE STGPOOL, um abhängig von Ihrer Systemkonfiguration `COLLOCATE=GROUP`, `COLLOCATE=NODE` oder `COLLOCATE=FILESPACE` anzugeben. b. Geben Sie für den Plattenspeicherpool mithilfe des Befehls DEFINE STGPOOL oder UPDATE STGPOOL einen Wert für den Parameter MIGPROCESS an. Wenn beispielsweise 12 Bandlaufwerke vorhanden sind, geben Sie `MIGPROCESS=10` an. Auf diese Weise werden maximal 10 Bandlaufwerke für Umlagerungsprozesse verwendet. Zwei Laufwerke sind für andere Tasks, wie beispielsweise Zurückschreibungs-, Datenbanksicherungs- und Clientsicherungsoperationen, reserviert.
Vorbereiten von Dateien für das Vaulting an einem anderen Standort	a. Versetzen Sie Banddatenträger an einen anderen Standort, indem Sie die Anweisungen in Sicherungsdatenträger versetzen ausführen. b. Erstellen Sie die Plandatei zur Wiederherstellung nach einem Katastrophenfall, indem Sie den Befehl PREPARE auf dem Quellenserver ausgeben: `prepare` c. Stellen Sie sicher, dass alle Datenträger, die für die Wiederherstellung nach einem Katastrophenfall erforderlich sind, in die Wiederherstellungsplandatei eingeschlossen sind. Weitere Informationen finden Sie in Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM.
Sichern der Einheitenkonfigurationsinformationen	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP DEVCONFIG: `define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig filenames=devconfig.dat" active=yes desc="Einheitenkonfigurations- datei sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Sichern des Datenträgerprotokolls	Erstellen Sie einen Zeitplan für die Ausführung des Befehls BACKUP VOLHISTORY: `define schedule VOLHISTBKUP type=admin cmd="backup volhistory filenames=volhist.dat" active=yes desc="Datenträgerprotokoll sichern." startdate=today starttime=17:00:00 duration=45 durunits=minutes`
Entfernen älterer Versionen von Datenbanksicherungen, die nicht mehr erforderlich sind	Erstellen Sie einen Zeitplan für die Ausführung des Befehls DELETE VOLHISTORY: `define schedule DELVOLHIST type=admin cmd="delete volhistory type=dbb todate=today-6 totime=now" active=yes desc="Alte Datenbanksicherungen entfernen." startdate=today starttime=20:00:00 duration=45 durunits=minutes`

Operation	Beispielbefehle und weitere Informationen
Entfernen von Objekten, deren zulässige Aufbewahrungsdauer überschritten wurde	Erstellen Sie einen Zeitplan für die Ausführung des Befehls EXPIRE INVENTORY. Legen Sie für den Parameter RESOURCE auf der Basis der Systemgröße, die Sie konfigurieren, einen Wert fest, der mit der Anzahl Prozessorkerne, die für Ihr System angegeben wurden, übereinstimmt. Geben Sie beispielsweise den folgenden Befehl aus, um einen Zeitplan mit dem Namen EXPINVENTORY zu erstellen: `define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=8 duration=120" active=yes desc="Verfallene Objekte entfernen." startdate=today starttime=14:00:00 duration=1 durunits=hours`
Konsolidieren von Speicherbereich	Erstellen Sie einen Zeitplan für die Ausführung des Befehls RECLAIM STGPOOL. Geben Sie beispielsweise den folgenden Befehl aus, um einen Zeitplan mit dem Namen RECLAIM zu erstellen: `define schedule RECLAIM type=admin cmd="reclaim stgpool tapepool duration=60" startdate=today starttime=15:00:00 duration=5 durunits=hours` Tipp: Um den Durchsatz zu maximieren, können Sie die Anzahl paralleler Prozesse angeben, die für die Konsolidierung von Speicherbereich verwendet werden soll. Aktualisieren Sie den Bandspeicherpool mithilfe des Befehls UPDATE STGPOOL und geben Sie einen Wert für den Parameter RECLAIMPROCESS an. Wenn beispielsweise 12 Bandlaufwerke vorhanden sind, geben Sie `RECLAIMPROCESS=5` an. Da für jeden Konsolidierungsprozess zwei Laufwerke verwendet werden, beträgt die Gesamtzahl Laufwerke, die für die Konsolidierung verwendet werden kann, 10. Zwei Laufwerke sind für Sicherungsoperationen reserviert.

Nächste Schritte

Nachdem Sie Zeitpläne für die Serververwaltungstasks erstellt haben, können Sie diese im Operations Center anzeigen, indem Sie die folgenden Schritte ausführen:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Server.
2. Klicken Sie auf Verwaltung.

- Sicherungsdatenträger versetzen
  Für die Wiederherstellung nach einem Katastrophenfall benötigen Sie Datenbanksicherungsdatenträger, Kopienspeicherpooldatenträger und weitere Dateien. Um auf einen Katastrophenfall vorbereitet zu sein, müssen Sie tägliche Tasks ausführen.

Zugehörige Verweise:
UPDATE STGPOOL (Speicherpool aktualisieren)
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Clientzeitpläne definieren

Erstellen Sie mithilfe des Operations Center Zeitpläne für Clientoperationen.

Vorgehensweise

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Clients.
2. Klicken Sie auf Zeitpläne.
3. Klicken Sie auf +Zeitplan.
4. Führen Sie die Schritte im Assistenten Zeitplan erstellen aus. Definieren Sie auf der Basis der in Zeitpläne für Serververwaltungsaktivitäten definieren geplanten Serververwaltungsaktivitäten für Clientsicherungszeitpläne eine Startzeit von 22:00 Uhr.

Bandeinheiten für den Server anschließen

Bevor der Server eine Bandeinheit verwenden kann, müssen Sie die Einheit an Ihr Serversystem anschließen und den entsprechenden Bandeinheitentreiber installieren.

Informationen zu diesem Vorgang

Um die Systemleistung zu optimieren, verwenden Sie schnelle Bandeinheiten mit hoher Speicherkapazität. Stellen Sie genügend Bandlaufwerke bereit, um Ihre Geschäftsanforderungen erfüllen zu können.

Schließen Sie Bandeinheiten an ihren eigenen Hostbusadapter (HBA) an, der nicht mit anderen Einheitentypen, wie beispielsweise Platte, gemeinsam genutzt wird. IBM® Bandlaufwerke haben einige spezielle Anforderungen in Bezug auf HBAs und zugehörige Treiber.

- AIX-BetriebssystemeLinux-BetriebssystemeAutomatisierte Speicherarchiveinheit an das System anschließen
  Sie können eine automatisierte Speicherarchiveinheit an Ihr System anschließen, um Ihre Daten auf Bändern zu speichern.
- Bandeinheitentreiber auswählen
  Um Bandeinheiten mit IBM Spectrum Protect verwenden zu können, müssen Sie den entsprechenden Bandeinheitentreiber installieren.
- AIX-BetriebssystemeLinux-BetriebssystemeGerätedateinamen für Bandeinheiten
  Ein Gerätedateiname für eine Bandeinheit ist für den IBM Spectrum Protect-Server für die Arbeit mit Bandeinheiten, Datenträgerwechslern oder Einheiten für austauschbare Datenträger erforderlich.
- Bandeinheitentreiber installieren und konfigurieren
  Sie können Bandeinheiten erst mit IBM Spectrum Protect verwenden, nachdem der korrekte Bandeinheitentreiber installiert wurde.

Automatisierte Speicherarchiveinheit an das System anschließen

Sie können eine automatisierte Speicherarchiveinheit an Ihr System anschließen, um Ihre Daten auf Bändern zu speichern.

Informationen zu diesem Vorgang

Berücksichtigen Sie die folgenden Einschränkungen, bevor Sie eine automatisierte Speicherarchiveinheit anschließen:

- Angeschlossene Einheiten müssen sich an ihrem eigenen Hostbusadapter (HBA) befinden.
- Ein HBA darf nicht mit anderen Einheitentypen, wie beispielsweise einer Platte, gemeinsam genutzt werden. .
- Bei Mehrfach-FC-HBAs müssen sich angeschlossene Einheiten an ihren eigenen Ports befinden. Diese Ports dürfen nicht mit anderen Einheitentypen gemeinsam genutzt werden.
- IBM® Bandlaufwerke haben einige spezielle Anforderungen in Bezug auf HBA und zugehörige Treiber. Weitere Informationen zu Einheiten finden Sie auf der Website für Ihr Betriebssystem:
  - Website mit den von IBM Spectrum Protect unterstützten Einheiten für AIX
  - Website mit den von IBM Spectrum Protect unterstützten Einheiten für Linux und Windows

Vorgehensweise

Um den Fibre Channel-Adapter (FC-Adapter) verwenden zu können, führen Sie die folgenden Schritte aus:

1. Installieren Sie den FC-Adapter und die zugehörigen Treiber.
2. Installieren Sie die geeigneten Einheitentreiber für die angeschlossenen Datenträgerwechsler.

- AIX-BetriebssystemeLinux-BetriebssystemeSpeicherarchivmodus festlegen
  Damit der IBM Spectrum Protect-Server auf ein SCSI-Speicherarchiv zugreifen kann, muss die Bandeinheit für den entsprechenden Modus definiert werden.

Zugehörige Konzepte:
Bandeinheitentreiber auswählen

Bandeinheitentreiber auswählen

Um Bandeinheiten mit IBM Spectrum Protect verwenden zu können, müssen Sie den entsprechenden Bandeinheitentreiber installieren.

- IBM Bandeinheitentreiber
  IBM® Einheitentreiber sind für die meisten IBM Bandeinheiten mit Kennsätzen verfügbar.
- IBM Spectrum Protect-Bandeinheitentreiber
  Bandeinheitentreiber werden vom IBM Spectrum Protect-Server bereitgestellt.

Zugehörige Verweise:
Bandeinheitentreiber installieren und konfigurieren

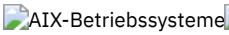
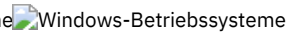
IBM Bandeinheitentreiber

IBM® Einheitentreiber sind für die meisten IBM Bandeinheiten mit Kennsätzen verfügbar.

Sie können IBM Bandeinheitentreiber von der Website für Fix Central herunterladen:

1. Rufen Sie die Website für Fix Central unter Website für Fix Central auf.

2. Klicken Sie auf Produkt auswählen.
3. Wählen Sie System Storage im Menü für die Produktgruppe aus.
4. Wählen Sie Tape systems im Menü für System Storage aus.
5. Wählen Sie Tape drivers and software im Menü für Tape systems aus.
6. Wählen Sie Tape device drivers im Menü für Tape drivers and software aus. Zusätzlich zu Bandtreibern erhalten Sie auch Zugriff auf Tools wie das IBM Tape Diagnostic Tool (ITDT).
7. Wählen Sie Ihr Betriebssystem im Menü Plattform aus.

 AIX-Betriebssysteme  Windows-Betriebssysteme

Die aktuelle Liste der Einheiten und Betriebssystemversionen, die von IBM Bandeinheitentreibern unterstützt werden, finden Sie auf der Website mit den von IBM Spectrum Protect unterstützten Einheiten unter Supported devices for AIX and Windows.

 Linux-Betriebssysteme

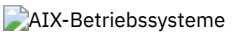
Die aktuelle Liste der Bandeinheiten und Betriebssystemversionen, die von IBM Bandeinheitentreibern unterstützt werden, finden Sie auf der Website mit den von IBM Spectrum Protect unterstützten Einheiten unter Supported devices for Linux.

IBM Bandeinheitentreiber unterstützen nur einige Linux-Kernel-Level. Informationen zu unterstützten Kernel-Leveln finden Sie in Website für Fix Central.

IBM Spectrum Protect-Bandeinheitentreiber

Bandeinheitentreiber werden vom IBM Spectrum Protect-Server bereitgestellt.

Ein IBM Spectrum Protect-Bandeinheitentreiber wird mit dem Server installiert.

 AIX-Betriebssysteme

Sie können den generischen SCSI-Bandeinheitentreiber, der vom IBM® AIX-Betriebssystem bereitgestellt wird, verwenden, um mit Bandeinheiten zu arbeiten, die nicht vom IBM Spectrum Protect-Einheitentreiber unterstützt werden. Wenn der generische SCSI-Bandeinheitentreiber unter AIX verwendet wird, muss die Einheitenklasse GENERICTAPE auf den Einheitentyp gesetzt werden, der im Befehl DEFINE DEVCLASS angegeben ist.

Bei den folgenden Bandeinheiten können Sie auswählen, ob der IBM Spectrum Protect-Bandeinheitentreiber oder der native Einheitentreiber für Ihr Betriebssystem installiert werden soll:

- ECART
- LTO (nicht von IBM)

Alle über SCSI angeschlossenen Speicherarchive, die Bandlaufwerke aus der Liste enthalten, müssen den IBM Spectrum Protect-Wechslertreiber verwenden.

Bandeinheitentreiber anderer Hardwareanbieter können verwendet werden, wenn sie der Einheitenklasse GENERICTAPE zugeordnet sind. Generische Einheitentreiber werden in Einheitenklassen WORM (Write Once Read Many) nicht unterstützt.

 Linux-Betriebssysteme

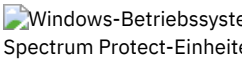
Sie können den IBM Spectrum Protect-Durchgriffseinheitentreiber verwenden. IBM Spectrum Protect-Durchgriffseinheitentreiber erfordern den generischen Linux-SCSI-Einheitentreiber (sg) zusammen mit dem Linux-Betriebssystem für die Installation der Kernel.

Sie können beispielsweise den IBM Spectrum Protect-Durchgriffseinheitentreiber für die folgenden Bandeinheiten installieren:

- ECART
- LTO (nicht von IBM)

Alle über SCSI angeschlossenen Speicherarchive, die Bandlaufwerke enthalten, die in der Liste nicht mit IBM gekennzeichnet sind, müssen ebenfalls den IBM Spectrum Protect-Durchgriffseinheitentreiber verwenden.

Sie können den generischen SCSI-Bandeinheitentreiber (st), der vom Linux-Betriebssystem bereitgestellt wird, nicht verwenden. Demzufolge wird der Einheitentyp GENERICTAPE für den Befehl DEFINE DEVCLASS nicht unterstützt.

 WindowsBetriebssystemeSie können einen durch Windows Hardware Quality Labs (WHQL) zertifizierten nativen Treiber anstelle des IBM Spectrum Protect-Einheitentreibers auswählen. Der durch die Windows Hardware Qualification Labs (WHQL) zertifizierte native Einheitentreiber kann nur für Einheiten verwendet werden, die keinen IBM Kennsatz haben, sowie für Bandlaufwerke eines anderen Herstellers als IBM. Für den durch die Windows Hardware Qualification Labs zertifizierten nativen Einheitentreiber können Sie entweder den IBM Spectrum Protect-SCSI-Durchgriffseinheitentreiber oder den nativen Windows-Bandeinheitentreiber auswählen. Wenn der SCSI-Durchgriffseinheitentreiber verwendet wird, darf die Einheitenklasse im Befehl DEFINE DEVCLASS nicht GENERICTAPE lauten. Wenn der native Einheitentreiber verwendet wird, muss die Einheitenklasse GENERICTAPE lauten.

Gerätedateinamen für Bandeinheiten

Ein Gerätedateiname für eine Bandeinheit ist für den IBM Spectrum Protect-Server für die Arbeit mit Bandeinheiten, Datenträgerwechslern oder Einheiten für austauschbare Datenträger erforderlich.


AIX-Betriebssysteme

Wenn eine Einheit erfolgreich konfiguriert wird, wird der Name einer logischen Datei zurückgegeben. In Tabelle 1 ist der Name der Einheit, der auch als Gerätedateiname bezeichnet wird, aufgeführt, der dem Laufwerk oder Speicherarchiv entspricht. Sie können den Betriebssystembefehl SMIT verwenden, um den Gerätedateinamen für die Einheit abzurufen. In den Beispielen gibt *x* eine ganze Zahl größer-gleich 0 an.

Tabelle 1. Beispiele für Einheiten

Einheit	**Beispiel für Einheit**	**Name der logischen Datei**
Bandlaufwerke, die vom IBM Spectrum Protect-Einheitentreiber verwendet werden können	/dev/mt*x*	mt*x*
Bandlaufwerke, die vom IBM Bandeinheitentreiber verwendet werden können	/dev/rmt*x*	rmt*x*
Bandlaufwerke, die vom generischen IBM AIX-Bandeinheitentreiber verwendet werden können	/dev/rmt*x*	rmt*x*
Speicherarchiveinheiten, die vom IBM Spectrum Protect-Einheitentreiber verwendet werden können	/dev/lb*x*	lb*x*
Speicherarchiveinheiten, die vom IBM Bandeinheitentreiber verwendet werden können	/dev/smc*x*	smc*x*


Linux-Betriebssysteme

Wenn eine Einheit erfolgreich konfiguriert wird, wird der Name einer logischen Datei zurückgegeben. In Tabelle 2 ist der Name der Einheit, der auch als Gerätedateiname bezeichnet wird, aufgeführt, der dem Laufwerk oder Speicherarchiv entspricht. In den Beispielen gibt *x* eine ganze Zahl größer-gleich 0 an.

Tabelle 2. Beispiele für Einheiten

Einheit	**Beispiel für Einheit**	**Name der logischen Datei**
Bandlaufwerke, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet werden können	/dev/tsmscsi/mt*x*	mt*x*
Bandlaufwerke, die vom IBM lin_tape-Einheitentreiber verwendet werden können	/dev/IBMtape*x*	IBMtape*x*
Speicherarchiveinheiten, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet werden können	/dev/tsmscsi/lb*x*	lb*x*
Speicherarchiveinheiten, die vom IBM lin_tape-Einheitentreiber verwendet werden können	/dev/IBMchanger*x*	IBMchanger*x*


Windows-Betriebssysteme

Wenn eine Einheit erfolgreich konfiguriert wird, wird der Name einer logischen Datei zurückgegeben. In Tabelle 3 ist der Name der Einheit, der auch als Gerätedateiname bezeichnet wird, aufgeführt, der dem Laufwerk oder Speicherarchiv entspricht. In den Beispielen geben *a*, *b*, *c*, *d* und *x* jeweils eine ganze Zahl größer-gleich 0 an; dabei gilt Folgendes:

- *a* gibt die Ziel-ID an.
- *b* gibt die Nummer der logischen Einheit (LUN) an.
- *c* gibt die SCSI-Bus-ID an.
- *d* gibt die Port-ID an.

Tabelle 3. Beispiele für Einheiten

Einheit	**Beispiel für Einheit**	**Konvertierter Einheitenname**
Bandlaufwerke, die vom IBM Spectrum Protect-Einheitentreiber unterstützt werden	mt*a.b.c.d*	mt*a.b.c.d*
Bandlaufwerke, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber unterstützt werden	mt*a.b.c.d*	mt*a.b.c.d*
Bandlaufwerke, die vom IBM Einheitentreiber unterstützt werden	Tape*x*	mt*a.b.c.d*
Speicherarchiveinheiten, die vom IBM Spectrum Protect-Einheitentreiber unterstützt werden	lb.*a.b.c.d*	lb*a.b.c.d*
Speicherarchiveinheiten, die vom IBM Spectrum Protect-Durchgriffseinheitentreiber unterstützt werden	lb*a.b.c.d*	lb*a.b.c.d*
Speicherarchiveinheiten, die vom IBM Einheitentreiber unterstützt werden	Changer*x*	lb*a.b.c.d*

Bandeinheitentreiber installieren und konfigurieren

Sie können Bandeinheiten erst mit IBM Spectrum Protect verwenden, nachdem der korrekte Bandeinheitentreiber installiert wurde.

IBM Spectrum Protect unterstützt alle Einheiten, die von IBM® Bandeinheitentreibern unterstützt werden. IBM Spectrum Protect unterstützt jedoch nicht alle Betriebssystemversionen, die von IBM Bandeinheitentreiber unterstützt werden.

- IBM Einheitentreiber für IBM Bandeinheiten installieren und konfigurieren
  Installieren und Konfigurieren Sie einen IBM Bandeinheitentreiber, um eine IBM Bandeinheit verwenden zu können.
- AIX-BetriebssystemeBandeinheitentreiber auf AIX-Systemen konfigurieren
  Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Bandeinheitentreibern anderer Hersteller als IBM auf AIX-Systemen.
- Linux-BetriebssystemeBandeinheitentreiber auf Linux-Systemen konfigurieren
  Lesen Sie die folgenden Abschnitte, wenn Sie Bandeinheitentreiber auf Linux-Systemen installieren und konfigurieren.
- Windows-BetriebssystemeBandeinheitentreiber auf Windows-Systemen konfigurieren
  Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Treibern für Bandeinheiten und Speicherarchive auf Windows-Systemen.

IBM Einheitentreiber für IBM Bandeinheiten installieren und konfigurieren

Installieren und Konfigurieren Sie einen IBM® Bandeinheitentreiber, um eine IBM Bandeinheit verwenden zu können.

Informationen zu diesem Vorgang

Anweisungen zum Installieren und Konfigurieren von IBM Bandeinheitentreibern finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*.

AIX-BetriebssystemeNachdem Sie die Installationsprozedur wie im Handbuch *IBM Tape Device Drivers Installation and User's Guide* beschrieben ausgeführt haben, werden, abhängig von dem Einheitentreiber, der installiert wird, unterschiedliche Nachrichten ausgegeben. Wenn Sie den Einheitentreiber für ein IBM Bandlaufwerk oder Speicherarchiv installieren, werden die folgenden Nachrichten zurückgegeben:

```
rmtx Verfügbar
```

oder

```
smcx Verfügbar
```

Notieren Sie den Wert von x, der vom IBM Bandeinheitentreiber zugeordnet wird. Um den Gerätedateinamen Ihrer Einheit zu bestimmen, geben Sie einen der folgenden Befehle aus:

- Für Bandlaufwerke: `ls -l /dev/rmt*`
- Für Bandarchive: `ls -l /dev/smc*`

Der Dateiname kann weitere Zeichen am Ende haben, um verschiedene Betriebsmerkmale anzugeben, die aber von IBM Spectrum Protect nicht benötigt werden. Verwenden Sie für IBM Einheitentreiber den Basisdateinamen im Parameter DEVICE des Befehls DEFINE PATH, um eine Einheit einem Laufwerk (/dev/rmtx) oder einem Speicherarchiv (/dev/smcx) zuzuordnen.
Nachdem Sie den Einheitentreiber installiert haben, können Sie mithilfe von SMIT (System Management Interface Tool) Bandlaufwerke und Bandarchive anderer Hersteller als IBM konfigurieren. Führen Sie die folgenden Schritte aus:

1. Führen Sie das Programm SMIT aus.
2. Klicken Sie auf Devices.
3. Klicken Sie auf IBM Spectrum Protect Devices.
4. Klicken Sie auf Fibre Channel SAN Attached devices.
5. Klicken Sie auf Discover Devices Supported by IBM Spectrum Protect. Warten Sie, bis der Erkennungsprozess abgeschlossen ist.
6. Kehren Sie zum Menü Fibre Channel SAN Attached devices zurück und klicken Sie auf List Attributes of a Discovered Device.

Linux-BetriebssystemeNachdem Sie die Installationsprozedur wie im Handbuch *IBM Tape Device Drivers Installation and User's Guide* beschrieben ausgeführt haben, werden, abhängig von dem Einheitentreiber, der installiert wird, unterschiedliche Nachrichten ausgegeben. Wenn Sie den Einheitentreiber für eine IBM LTO- oder 3592-Einheit installieren, werden die folgenden Nachrichten zurückgegeben:

```
IBMtapex Verfügbar
```

oder

```
IBMChangerx Verfügbar
```

Notieren Sie den Wert von x, der vom IBM Bandeinheitentreiber zugeordnet wird. Um den Gerätedateinamen Ihrer Einheit zu bestimmen, geben Sie einen der folgenden Befehle aus:

- Für Bandlaufwerke: `ls -l /dev/IBMtape*`
- Für Bandarchive: `ls -l /dev/IBMChange*`

Der Dateiname kann weitere Zeichen am Ende haben, um verschiedene Betriebsmerkmale anzugeben, die aber von IBM Spectrum Protect nicht benötigt werden. Verwenden Sie für IBM Einheitentreiber den Basisdateinamen im Parameter DEVICE des Befehls DEFINE PATH, um eine Einheit einem Laufwerk (/dev/IBMtapex) oder einem Speicherarchiv (/dev/IBMChangerx) zuzuordnen.
Einschränkung: Der Einheitentyp dieser Klasse darf nicht GENERICTAPE lauten.
Windows-BetriebssystemeFür Windows-Betriebssysteme stellt IBM Spectrum Protect zwei Einheitentreiber zur Verfügung:

Durchgriffseinheitentreiber

Wenn der Hersteller der Bandeinheit einen SCSI-Einheitentreiber bereitstellt, installieren Sie den IBM Spectrum Protect-Durchgriffseinheitentreiber.

SCSI-Einheitentreiber für Bandeinheiten
: Wenn der Hersteller der Bandeinheit keinen SCSI-Einheitentreiber bereitstellt, installieren Sie den IBM Spectrum Protect-SCSI-Einheitentreiber für Bandeinheiten. Der Name der Treiberdatei ist tsmscsi64.sys.

Anweisungen zum Installieren und Konfigurieren von IBM Bandeinheitentreibern finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*. Nach der Installation des IBM Bandeinheitentreibers gibt der Server einen Gerätedateinamen Tape*X* für IBM Bandlaufwerke und Changer*Y* für IBM Datenträgerwechsler an. Für einen IBM Spectrum Protect-SCSI-Einheitentreiber oder einen IBM Spectrum Protect-Durchgriffseinheitentreiber können Sie den Windows-Betriebssystembefehl regedit ausgeben, um den Namen der Gerätedatei für die Einheit zu überprüfen. Der IBM Spectrum Protect-Server stellt auch ein Dienstprogramm zur Überprüfung der Einheit für das Windows-Betriebssystem zur Verfügung. Das Dienstprogramm tsmdlst ist im Serverpaket enthalten. Um das Dienstprogramm zu verwenden, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Anwendungsprogrammierschnittstelle (API) des Hostbusadapters installiert ist.
2. Um Einheitendaten aus dem Hostsystem abzurufen, geben Sie Folgendes ein:

   ```
   tsmdlst
   ```

- AIX-BetriebssystemeLinux-BetriebssystemeMultipath I/O-Zugriff mit IBM Bandeinheiten
  Multipath I/O ist ein Verfahren, das unterschiedliche Pfade für den Zugriff auf dieselbe physische Einheit verwendet, beispielsweise über mehrere Hostbusadapter (HBA) oder Switches. Mithilfe des Multipathverfahrens kann sichergestellt werden, dass kein Single Point of Failure auftritt.

Zugehörige Konzepte:
Multipath I/O-Zugriff mit IBM Bandeinheiten
AIX-Betriebssysteme

Bandeinheitentreiber auf AIX-Systemen konfigurieren

Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Bandeinheitentreibern anderer Hersteller als IBM® auf AIX-Systemen.

Informationen zu diesem Vorgang

Anweisungen zum Installieren und Konfigurieren von IBM Bandeinheitentreibern finden Sie in der Veröffentlichung *IBM Tape Device Drivers Installation and User's Guide*.

- AIX-BetriebssystemeSCSI- und Fibre Channel-Einheiten
  Die Menüs und Eingabeaufforderungen zur Definition von IBM Spectrum Protect-Einheiten in SMIT ermöglichen die Verwaltung von Einheiten, die über SCSI und Fibre Channel (FC) angeschlossen sind.
- AIX-BetriebssystemeIBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler konfigurieren
  Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler für Speicherarchive anderer Hersteller zu konfigurieren.
- AIX-BetriebssystemeIBM Spectrum Protect-Einheitentreiber für Bandlaufwerke konfigurieren
  Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke für Speicherarchive anderer Hersteller zu konfigurieren.
- AIX-BetriebssystemeAn ein Fibre Channel-SAN angeschlossene Einheiten konfigurieren
  Um eine an ein Fibre Channel-SAN angeschlossene Einheit zu konfigurieren, führen Sie die Prozedur aus.

AIX-Betriebssysteme

SCSI- und Fibre Channel-Einheiten

Die Menüs und Eingabeaufforderungen zur Definition von IBM Spectrum Protect-Einheiten in SMIT ermöglichen die Verwaltung von Einheiten, die über SCSI und Fibre Channel (FC) angeschlossen sind.

Das Hauptmenü von IBM Spectrum Protect verfügt über zwei Optionen:

Über SCSI angeschlossene Einheiten
: Verwenden Sie diese Option, um SCSI-Einheiten zu konfigurieren, die mit einem SCSI-Adapter im Host verbunden sind.

Über Fibre Channel-SAN-angeschlossene Einheiten
: Verwenden Sie diese Option, um Einheiten zu konfigurieren, die mit einem Fibre Channel-Adapter (FC-Adapter) im Host verbunden sind. Wählen Sie eines der folgenden Attribute aus:

  Attribute einer erkannten Einheit auflisten
  : Listet Attribute einer Einheit auf, die der aktuellen ODM-Datenbank bekannt ist.

    - FC Port ID:

24-Bit FC Port ID(N(L)_Port oder F(L)_Port). Dies ist die Adress-ID, die innerhalb der zugeordneten Topologie, in der die Einheit verbunden ist, eindeutig ist. In den Switch- oder Fabric-Umgebungen kann sie durch den Switch anhand der oberen 2 Byte, die nicht null sind, bestimmt werden. In einer Private Arbitrated Loop ist dies die Arbitrated Loop Physical Address (AL_PA), wobei die oberen 2 Byte null sind. Wenden Sie sich an Ihren Fibre Channel-Hersteller, um zu bestimmen, wie wie eine AL_PA oder eine Port-ID zugeordnet wird.

- Mapped LUN ID:

  Ein FC-zu-SCSI-Brückenmodul (auch als Umsetzer, Router oder Gateway bezeichnet). Informationen zur Zuordnung von LUNs erhalten Sie von Ihrem Brückenhersteller. Zugeordnete LUN-IDs sollten nicht geändert werden.

- WW Name:

  Der weltweite Name (WWN) des Ports, an den die Einheit angeschlossen ist. Dies ist die eindeutige 64-Bit-Kennung, die von Herstellern von Fibre Channel-Komponenten wie Brücken oder nativen Fibre Channel-Einheiten zugeordnet wird. Wenden Sie sich an Ihren Fibre Channel-Hersteller, um den WWN eines Ports zu bestimmen.

- Product ID:

  Die Produkt-ID einer Einheit. Wenden Sie sich an Ihren Einheitenhersteller, um die Produkt-ID zu bestimmen.

Von IBM Spectrum Protect unterstützte Einheiten erkennen
: Mit dieser Option werden Einheiten in einem Fibre Channel-SAN, die von IBM Spectrum Protect unterstützt werden, erkannt und verfügbar gemacht. Wenn eine Einheit einer vorhandenen SAN-Umgebung hinzugefügt oder aus einer vorhandenen SAN-Umgebung entfernt wird, müssen Sie mithilfe dieser Option eine erneute Erkennung für die Einheiten ausführen. Einheiten müssen zunächst erkannt werden, damit aktuelle Werte der Einheitenattribute mit der Option Attribute einer erkannten Einheit auflisten angezeigt werden. Unterstützte Einheiten in einem Fibre Channel-SAN sind Bandlaufwerke und Datenträgerwechsler. Der IBM Spectrum Protect-Einheitentreiber ignoriert alle anderen Einheitentypen, wie beispielsweise Platte.

Alle definierten Einheiten entfernen
: Mit dieser Option werden alle an ein Fibre Channel-SAN angeschlossenen IBM Spectrum Protect-Einheiten mit dem Status `DEFINED` in der ODM-Datenbank entfernt. Falls erforderlich, müssen Sie für Einheiten eine erneute Erkennung ausführen, indem Sie die Option `Von IBM Spectrum Protect unterstützte Einheiten erkennen` auswählen, nachdem alle definierten Einheiten entfernt wurden.

Einheit entfernen
: Mit dieser Option wird eine einzelne an ein Fibre Channel-SAN angeschlossene IBM Spectrum Protect-Einheit mit dem Status `DEFINED` in der ODM-Datenbank entfernt. Falls erforderlich, müssen Sie für die Einheit eine erneute Erkennung ausführen, indem Sie die Option `Von IBM Spectrum Protect unterstützte Einheiten erkennen` auswählen, nachdem eine definierte Einheit entfernt wurde.

 AIX-Betriebssysteme

IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler konfigurieren

Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler für Speicherarchive anderer Hersteller zu konfigurieren.

Vorgehensweise

Führen Sie das Programm SMIT aus, um den Einheitentreiber für jeden Datenträgerwechsler oder Robotermechanismus zu konfigurieren:

1. Wählen Sie Devices aus.
2. Wählen Sie IBM Spectrum Protect Devices aus.
3. Wählen Sie Library/MediumChanger aus.
4. Wählen Sie Add a Library/MediumChanger aus.
5. Wählen Sie den IBM Spectrum Protect-SCSI-LB für jedes von IBM Spectrum Protect unterstützte Speicherarchiv aus.
6. Wählen Sie den übergeordneten Adapter aus, mit dem die Einheit verbunden wird. Diese Nummer wird im Format 00-0X aufgelistet; dabei gibt X die Steckplatznummer der SCSI-Adapterkarte an.
7. Geben Sie, wenn Sie dazu aufgefordert werden, die Verbindungsadresse der Einheit ein, die Sie installieren. Die Verbindungsadresse ist eine zweistellige Zahl. Die erste Ziffer ist die SCSI-ID (der Wert, der auf dem Arbeitsblatt notiert wurde). Die zweite Ziffer ist die Nummer der logischen SCSI-Einheit (LUN), die - sofern nicht anders angegeben - normalerweise null ist. Die SCSI-ID und die LUN müssen durch ein Komma (,) voneinander getrennt werden. Beispielsweise hat die Verbindungsadresse `4,0` eine SCSI-ID=4 und eine LUN=0.
8. Klicken Sie auf DO.

   Sie erhalten eine Nachricht (Name einer logischen Datei) in der Form `lbX Verfügbar`. Notieren Sie den Wert von X; dabei handelt es sich um eine Zahl, die automatisch vom System zugeordnet wird. Verwenden Sie diese Informationen, um das Feld Einheitenname auf Ihrem Arbeitsblatt auszufüllen.

   Wenn die Nachricht beispielsweise `lb0 Verfügbar` lautet, enthält das Feld Einheitenname auf dem Arbeitsblatt den Wert /dev/lb0. Verwenden Sie immer das Präfix /dev/ mit dem von SMIT zur Verfügung gestellten Namen.

 AIX-Betriebssysteme

IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke konfigurieren

Verwenden Sie die folgende Prozedur, um IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke für Speicherarchive anderer Hersteller zu konfigurieren.

Vorgehensweise

Wichtig: IBM Spectrum Protect kann *tar*- oder *dd*-Bänder nicht überschreiben, *tar* oder *dd* kann jedoch IBM Spectrum Protect-Bänder überschreiben.
Einschränkung: Bandlaufwerke können nur gemeinsam genutzt werden, wenn das Laufwerk nicht definiert oder der Server nicht gestartet ist. Der Befehl MKSYSB funktioniert nicht, wenn sowohl IBM Spectrum Protect als auch AIX dasselbe Laufwerk oder dieselben Laufwerke gemeinsam nutzen. Um den nativen Bandeinheitentreiber des Betriebssystems mit einem SCSI-Laufwerk verwenden zu können, muss die Einheit zuerst für AIX und dann für IBM Spectrum Protect konfiguriert werden. Ihre AIX-Dokumentation enthält Informationen zu diesen nativen Einheitentreibern.

Führen Sie das Programm SMIT aus, um den Einheitentreiber für jedes Laufwerk (einschließlich Laufwerke in Speicherarchiven) wie folgt zu konfigurieren:

1. Wählen Sie Devices aus.
2. Wählen Sie IBM Spectrum Protect Devices aus.
3. Wählen Sie Tape Drive aus.
4. Wählen Sie Add a Tape Drive aus.
5. Wählen Sie den IBM Spectrum Protect-SCSI-MT für jedes unterstützte Bandlaufwerk aus.
6. Wählen Sie den Adapter aus, mit dem die Einheit verbunden wird. Diese Nummer wird im Format 00-0X aufgelistet; dabei gibt X die Steckplatznummer der SCSI-Adapterkarte an.
7. Geben Sie, wenn Sie dazu aufgefordert werden, die Verbindungsadresse der Einheit ein, die Sie installieren. Die Verbindungsadresse ist eine zweistellige Zahl. Die erste Ziffer ist die SCSI-ID (der Wert, der auf dem Arbeitsblatt notiert wurde). Die zweite Ziffer ist die Nummer der logischen SCSI-Einheit (LUN), die - sofern nicht anders angegeben - normalerweise null ist. Die SCSI-ID und die LUN müssen durch ein Komma (,) voneinander getrennt werden. Beispielsweise hat die Verbindungsadresse `4,0` eine SCSI-ID=4 und eine LUN=0.
8. Klicken Sie auf DO. Sie erhalten eine Nachricht:

   Wenn Sie den Einheitentreiber für eine Bandeinheit (kein IBM® Bandlaufwerk) konfigurieren, erhalten Sie eine Nachricht (Name einer logischen Datei) in der Form `mtX Verfügbar`. Notieren Sie den Wert von X; dabei handelt es sich um eine Zahl, die automatisch vom System zugeordnet wird. Verwenden Sie diese Informationen, um das Feld Einheitenname auf dem Arbeitsblatt auszufüllen.

   Wenn die Nachricht beispielsweise `mt0 Verfügbar` lautet, enthält das Feld Einheitenname auf dem Arbeitsblatt den Wert /dev/mt0. Verwenden Sie immer das Präfix /dev/ mit dem von SMIT zur Verfügung gestellten Namen.

 AIX-Betriebssysteme

An ein Fibre Channel-SAN angeschlossene Einheiten konfigurieren

Um eine an ein Fibre Channel-SAN angeschlossene Einheit zu konfigurieren, führen Sie die Prozedur aus.

Vorgehensweise

1. Führen Sie das Programm SMIT aus.
2. Wählen Sie Devices aus.
3. Wählen Sie IBM Spectrum Protect Devices aus.
4. Wählen Sie Fibre Channel SAN Attached devices aus.
5. Wählen Sie Discover Devices Supported by IBM Spectrum Protect aus. Der Erkennungsprozess kann einige Zeit dauern.
6. Kehren Sie zum Menü Fibre Channel zurück und wählen Sie List Attributes of a Discovered Device aus.
7. Beachten Sie die aus drei Zeichen bestehende Einheiten-ID, die verwendet wird, wenn ein Pfad zu der Einheit für IBM Spectrum Protect definiert wird. Wenn ein Bandlaufwerk beispielsweise die ID `mt2` hat, geben Sie /dev/mt2 als den Einheitennamen an.

 Linux-Betriebssysteme

Bandeinheitentreiber auf Linux-Systemen konfigurieren

Lesen Sie die folgenden Abschnitte, wenn Sie Bandeinheitentreiber auf Linux-Systemen installieren und konfigurieren.

-  Linux-BetriebssystemeIBM Spectrum Protect-Durchgriffstreiber für Bandeinheiten und Speicherarchive konfigurieren
  Um den IBM Spectrum Protect-Durchgriffstreiber unter Linux verwenden zu können, müssen Sie die folgenden Schritte ausführen.
-  Linux-BetriebssystemezSeries LinuxFibre Channel-Adapter-Einheitentreiber (zfcp) installieren
  Der zSeries Linux Fibre Channel-Adapter-Einheitentreiber (zfcp) ist ein spezieller Adaptertreiber auf dem IBM® zSeries-System.
-  Linux-BetriebssystemeInformationen zu SCSI-Einheiten Ihres Systems
  Informationen zu den Einheiten, die von Ihrem System erkannt werden, befinden sich in der Datei */proc/scsi/scsi*. Diese Datei enthält eine Liste aller erkannten SCSI-Einheiten.

- Linux-BetriebssystemeÜberschreiben von Bandkennsätzen verhindern
  Der IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet den generischen Linux-SCSI-Einheitentreiber (sg), um Bandeinheiten, die an das System angeschlossen sind, zu steuern und zu betreiben. Wenn der generische Linux-SCSI-Bandeinheitentreiber (st) in den Kernel geladen wird und angeschlossene Bandeinheiten konfiguriert, können in Bezug auf die Art und Weise, wie eine Einheit verwaltet wird, Konflikte auftreten, da der generische sg-Treiber und der st-Treiber beide dieselbe Einheit steuern können.

Linux-Betriebssysteme

IBM Spectrum Protect-Durchgriffstreiber für Bandeinheiten und Speicherarchive konfigurieren

Um den IBM Spectrum Protect-Durchgriffstreiber unter Linux verwenden zu können, müssen Sie die folgenden Schritte ausführen.

Vorgehensweise

1. Stellen Sie sicher, dass die Einheit mit Ihrem System verbunden ist, eingeschaltet und aktiv ist.
2. Stellen Sie sicher, dass die Einheit von Ihrem System korrekt erkannt wird, indem Sie den folgenden Befehl ausgeben:

   ```
   cat /proc/scsi/scsi
   ```

3. Stellen Sie sicher, dass sowohl das IBM Spectrum Protect-Einheitentreiberpaket (tsmscsi) als auch das Speicherserverpaket installiert ist.
4. Im IBM Spectrum Protect-Einheitentreiberpaket stehen zwei Treiberkonfigurationsmethoden zur Verfügung: autoconf und tsmscsi. Mit beiden Methoden werden die folgenden Tasks ausgeführt:
   - Laden des generischen Linux-SCSI-Treibers (sg) in den Kernel
   - Erstellen der erforderlichen Gerätedateien für den Durchgriffstreiber
   - Erstellen der Einheitendatendateien für Bandeinheiten (/dev/tsmscsi/mtinfo) und Speicherarchive (/dev/tsmscsi/lbinfo)
5. Führen Sie die bevorzugte Konfigurationsmethode (autoconf oder tsmscsi) für den IBM Spectrum Protect-Durchgriffstreiber aus.
   - Um die Konfigurationsmethode autoconf auszuführen, geben Sie den folgenden Befehl aus:

     ```
     autoconf
     ```

   - Um die Konfigurationsmethode tsmscsi auszuführen, führen Sie die folgenden Schritte aus:
     a. Kopieren Sie die beiden Beispielkonfigurationsdateien, die sich im Installationsverzeichnis befinden, von *mt.conf.smp* und *lb.conf.smp* in *mt.conf* bzw. *lb.conf*.
     b. Editieren Sie die Dateien mt.conf und lb.conf. Fügen Sie (wie in dem Beispiel gezeigt am Anfang der Datei) eine Zeilengruppe für jede Kombination aus SCSI-Ziel, ID und LUN hinzu. Jede Kombination aus Einträgen für SCSI-Ziel, ID und LUN entspricht einem Bandlaufwerk oder einem Speicherarchiv, das konfiguriert werden soll. Stellen Sie sicher, dass die Dateien diese Voraussetzungen erfüllen:
        - Entfernen Sie das Beispiel, das sich am Anfang der Dateien befindet.
        - Zwischen jeder Zeilengruppe muss sich eine neue Zeile befinden.
        - Hinter der letzten Zeilengruppe muss sich eine neue Zeile befinden.
        - Stellen Sie sicher, dass keine der Dateien ein Nummernzeichen (#) enthält.
     c. Führen Sie im Installationsverzeichnis des Einheitentreibers das Script tsmscsi aus.
6. Prüfen Sie, ob die Einheit korrekt konfiguriert ist, indem Sie die Textdateien für Bandeinheiten (/dev/tsmscsi/mtinfo) und Speicherarchive (/dev/tsmscsi/lbinfo) anzeigen.
7. Bestimmen Sie die Gerätedateinamen für die Bandlaufwerke und Speicherarchive:
   - Um die Namen für Bandeinheiten zu bestimmen, geben Sie den folgenden Befehl aus:

     ```
     > ls  /dev/tsmscsi/mt*
     ```

   - Um die Namen für Speicherarchive zu bestimmen, geben Sie den folgenden Befehl aus:

     ```
     > ls  /dev/tsmscsi/lb*
     ```

   Mithilfe dieser Informationen können Sie ermitteln, welche der Gerätedateinamen /dev/tsmscsi/mtx und /dev/tsmscsi/lbx dem Server zur Verfügung gestellt werden müssen, wenn Sie einen Befehl DEFINE PATH ausgeben.

Nächste Schritte

Wenn Sie das Hostsystem erneut starten, müssen Sie das Script autoconf oder tsmscsi erneut ausführen, um IBM Spectrum Protect-Einheiten zu rekonfigurieren. Wenn Sie die IBM Spectrum Protect-Serverinstanz erneut starten, müssen Sie Einheiten nicht rekonfigurieren. Im Allgemeinen ist der generische Linux-SCSI-Treiber im Kernel vorinstalliert. Um zu prüfen, ob sich der Treiber im Kernel befindet, geben Sie den folgenden Befehl aus:

```
> lsmod | grep sg
```

Wenn sich der Treiber nicht im Kernel befindet, geben Sie den Befehl modprobe sg aus, um den sg-Treiber in den Kernel zu laden.
Linux-Betriebssysteme

zSeries LinuxFibre Channel-Adapter-Einheitentreiber (zfcp) installieren

Der zSeries Linux Fibre Channel-Adapter-Einheitentreiber (zfcp) ist ein spezieller Adaptertreiber auf dem IBM® zSeries-System.

Informationen zu diesem Vorgang

IBM Spectrum Protect und IBM Bandeinheitentreiber können auf zSeries-Plattformen mit Linux-Betriebssystemen in 64-Bit-Umgebungen ausgeführt werden. Sie unterstützen die meisten OEM-Bandeinheiten (OEM = Original-Equipment-Manufacturer) und IBM Bandeinheiten mit Fibre Channel-Schnittstellen.

Weitere Informationen zum Treiber zfcp finden Sie im IBM Redpaper, *Getting Started with zSeries Fibre Channel Protocol*, das unter IBM Redbooks verfügbar ist.

Vorgehensweise

1. Laden Sie das Modul qdio.
2. Installieren Sie den Treiber zfcp.
3. Ordnen Sie das Fibre Channel Protocol (FCP) zu und konfigurieren Sie den Treiber zfcp.
4. Installieren und konfigurieren Sie den IBM Bandeinheitentreiber.

Linux-Betriebssysteme

Informationen zu SCSI-Einheiten Ihres Systems

Informationen zu den Einheiten, die von Ihrem System erkannt werden, befinden sich in der Datei */proc/scsi/scsi*. Diese Datei enthält eine Liste aller erkannten SCSI-Einheiten.

Die folgenden Einheitendaten sind verfügbar: Hostnummer, Kanalnummer, SCSI-ID, Nummer der logischen Einheit, Anbieter, Firmwareversion, Einheitentyp und SCSI-Modus. Wenn ein System beispielsweise einige StorageTek- und IBM® Speicherarchive, ein SAN-Gateway und einige Quantum DLT-Laufwerke enthält, sieht die Datei */proc/scsi/scsi* ähnlich nachfolgend gezeigt aus:

```
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor:  STK    Model: 9738     Rev: 2003
  Type:  Medium Changer        ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor:  PATHLIGHT Model: SAN Gateway     Rev: 32aC
  Type: Unknown         ANSI SCSI revision: 03
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor:  QUANTUM  Model: DLT7000     Rev: 2560
  Type:  Sequential-Access         ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 04
  Vendor: IBM     Model: 7337     Rev: 1.63
  Type:  Medium Changer         ANSI SCSI revision: 02
```

Linux-Betriebssysteme

Überschreiben von Bandkennsätzen verhindern

Der IBM Spectrum Protect-Durchgriffseinheitentreiber verwendet den generischen Linux-SCSI-Einheitentreiber (sg), um Bandeinheiten, die an das System angeschlossen sind, zu steuern und zu betreiben. Wenn der generische Linux-SCSI-Bandeinheitentreiber (st) in den Kernel geladen wird und angeschlossene Bandeinheiten konfiguriert, können in Bezug auf die Art und Weise, wie eine Einheit verwaltet wird, Konflikte auftreten, da der generische sg-Treiber und der st-Treiber beide dieselbe Einheit steuern können.

Informationen zu diesem Vorgang

Wenn der st-Treiber Einheiten steuert, die von IBM Spectrum Protect verwendet werden, können interne IBM Spectrum Protect-Bandkennsätze überschrieben werden und Daten verloren gehen. Wenn eine Anwendung den st-Treiber zum Steuern von Einheiten verwendet und die Option, die angibt, dass Bänder nicht zurückgespult werden sollen, nicht definiert ist, werden Bänder automatisch nach Beendigung einer Operation zurückgespult. Mit der Operation zum automatischen Zurückspulen wird der Bandkennsatz wieder auf den Bandanfang positioniert. Wenn das Band im Laufwerk geladen bleibt, wird der IBM Spectrum Protect-Bandkennsatz bei der nächsten Schreiboperation, die keine IBM Spectrum Protect-Schreiboperation ist, überschrieben, da sich der Kennsatz am Anfang des Bands befindet.

Um zu verhindern, dass IBM Spectrum Protect-Kennsätze überschrieben werden, was zu einem Datenverlust führen kann, müssen Sie sicherstellen, dass nur der IBM Spectrum Protect-Durchgriffstreiber Einheiten steuert, die von IBM Spectrum Protect verwendet werden. Entfernen Sie den st-Treiber aus dem Kernel oder löschen Sie, wenn der Treiber von einigen Anwendungen auf dem System verwendet wird, die Gerätedateien, die den IBM Spectrum Protect-Einheiten entsprechen, sodass der st-Treiber diese nicht mehr steuern kann.

Wenn Sie den IBM Bandeinheitentreiber zum Steuern von Einheiten auf Ihrem System verwenden, können dieselben Probleme in Bezug auf Konflikte bei der Steuerung durch den Einheitentreiber auftreten. Bestimmen Sie anhand der Dokumentation zum IBM Bandeinheitentreiber, wie dieses Problem behoben und ein Datenverlust verhindert werden kann.

Entfernen Sie den st-Treiber.

Wenn keine anderen Anwendungen auf dem System st-Einheiten verwenden, entfernen Sie den st-Treiber aus dem Kernel. Geben Sie den folgenden Befehl aus, um den st-Treiber zu entladen:

```
rmmod st
```

Löschen Sie Gerätedateien für Einheiten, die IBM Spectrum Protect-Einheiten entsprechen.

Wenn Anwendungen vorhanden sind, die die Verwendung des st-Treibers erfordern, löschen Sie die Gerätedateien, die IBM Spectrum Protect-Einheiten entsprechen. Diese Gerätedateien werden vom st-Treiber generiert. Wenn diese Dateien gelöscht werden, kann der st-Treiber die entsprechenden IBM Spectrum Protect-Einheiten nicht mehr steuern. Gerätedateinamen für Bandlaufwerke werden im Verzeichnis /dev/ angezeigt. Ihre Namen haben das Format /dev/[n]st[0-1024][l][m][a].

Listen Sie die Gerätedateinamen für st-Laufwerke und die Gerätedateinamen für IBM Spectrum Protect-Einheiten mit dem Befehl ls auf. Abhängig von der Ausgabe der Einheitenfolgen können Sie Einheiten in der Liste der st-Einheiten finden, die mit Einheiten in der Liste der IBM Spectrum Protect-Einheiten übereinstimmen. Mithilfe des Befehls rm können Sie dann die st-Einheiten löschen.

Geben Sie die folgenden Befehle aus, um die st-Einheiten und die IBM Spectrum Protect-Einheiten aufzulisten:

```
ls -l /dev/*st*
ls -l /dev/tsmscsi/mt*
```

Löschen Sie die st-Einheiten mit dem Befehl `rm`:

```
rm /dev/*st*
```

Windows-Betriebssysteme

Bandeinheitentreiber auf Windows-Systemen konfigurieren

Lesen Sie die Anweisungen zum Installieren und Konfigurieren von Treibern für Bandeinheiten und Speicherarchive auf Windows-Systemen.

- WindowsBetriebssystemeVerwendung des IBM Spectrum Protect-Durchgriffstreibers für Bandeinheiten und Speicherarchive vorbereiten
  Um den IBM Spectrum Protect-Durchgriffseinheitentreiber unter Windows für Bandeinheiten und Speicherarchive verwenden zu können, müssen Sie die Treiber installieren und die Einheitennamen für den zu verwendenden Server abrufen.
- WindowsBetriebssystemeIBM Spectrum Protect-SCSI-Treiber für Bandeinheiten und Speicherarchive konfigurieren
  Wenn der Hersteller eines Bandlaufwerks oder Bandarchivs keinen SCSI-Einheitentreiber bereitstellt, müssen Sie den IBM Spectrum Protect-SCSI-Einheitentreiber installieren.

Windows-Betriebssysteme

Verwendung des IBM Spectrum Protect-Durchgriffstreibers für Bandeinheiten und Speicherarchive vorbereiten

Um den IBM Spectrum Protect-Durchgriffseinheitentreiber unter Windows für Bandeinheiten und Speicherarchive verwenden zu können, müssen Sie die Treiber installieren und die Einheitennamen für den zu verwendenden Server abrufen.

Vorbereitende Schritte

1. Stellen Sie fest, ob der Hersteller der Bandeinheit oder des Bandarchivs einen Einheitentreiber zur Verfügung stellt.
2. Wenn der Hersteller ein Einheitentreiberpaket bereitstellt, laden Sie das Paket herunter und installieren Sie es.
3. Konfigurieren Sie die SCSI-Einheitentreiber, indem Sie die Anweisungen des Herstellers ausführen.

Vorgehensweise

1. Installieren Sie den IBM Spectrum Protect-Durchgriffseinheitentreiber.
2. Rufen Sie die Einheitennamen ab, die der Server verwenden muss, indem Sie eine der folgenden Aktionen ausführen:
   - Führen Sie auf dem Server den Befehl QUERY SAN aus. In der Ausgabe werden alle Einheitennamen und ihre zugehörigen Einheitenseriennummern angezeigt.
   - Führen Sie im Serververzeichnis das Dienstprogramm tsmdlst.exe aus. In der Ausgabe werden alle Einheitennamen, ihre zugehörigen Einheitenseriennummern und die zugehörigen Einheitenpositionen angezeigt.
   - Führen Sie in der Windows-Eingabeaufforderung den Befehl regedit aus. Rufen Sie in der Ausgabe die Einheitendateinamen auf der Basis der Einheitenpositionen ab. Die Position besteht aus der Port-ID, der SCSI-Bus-ID, der LUN-ID und der SCSI-Ziel-ID. Der IBM Spectrum Protect-Einheitendateiname hat das Format mt*A.B.C.C* für Bandlaufwerke und lb*A.B.C.D* für Bandarchive; dabei gilt Folgendes:
     - *A* ist die SCSI-Ziel-ID.
     - *B* ist die LUN-ID.
     - *C* ist die SCSI-Bus-ID.
     - *D* ist die Port-ID.

Windows-Betriebssysteme

IBM Spectrum Protect-SCSI-Treiber für Bandeinheiten und Speicherarchive konfigurieren

Wenn der Hersteller eines Bandlaufwerks oder Bandarchivs keinen SCSI-Einheitentreiber bereitstellt, müssen Sie den IBM Spectrum Protect-SCSI-Einheitentreiber installieren.

Informationen zu diesem Vorgang

Der Name der Datei für den IBM Spectrum Protect-SCSI-Einheitentreiber ist tsmscsi64.sys.

Vorgehensweise

1. Lokalisieren Sie die Einheit in der Konsole des Geräte-Managers (devmgmt.msc) und wählen Sie sie aus. Bandlaufwerke sind unter Bandlaufwerke, Datenträgerwechsler unter Datenträgerwechsler aufgelistet.
2. Konfigurieren Sie die Einheit für die Verwendung durch den Einheitentreiber tsmscsi64.sys:
    a. Klicken Sie mit der rechten Maustaste auf die Einheit und klicken Sie auf Treibersoftware aktualisieren.
    b. Klicken Sie auf Auf dem Computer nach Treibersoftware suchen.
3. Klicken Sie auf Aus einer Liste von Gerätetreibern auf dem Computer auswählen.
4. Klicken Sie auf Weiter.
5. Wählen Sie die entsprechende Option aus:
    a. Wählen Sie für ein Bandlaufwerk IBM Spectrum Protect für Bandlaufwerke aus.
    b. Wählen Sie für einen Datenträgerwechsler IBM Spectrum Protect für Datenträgerwechsler aus.
6. Klicken Sie auf Weiter.
7. Klicken Sie auf Schließen.
8. Prüfen Sie, ob die Einheit korrekt für den Einheitentreiber tsmscsi64 konfiguriert wurde:
    a. Klicken Sie mit der rechten Maustaste auf die Einheit und klicken Sie auf Eigenschaften.
    b. Klicken Sie auf die Registerkarte Treiber und dann auf Treiberdetails. Im Fenster Treiberdetails wird der Einheitentreiber angezeigt, der die Einheit steuert.

Speicherarchive für die Verwendung durch einen Server konfigurieren

Um ein Speicherarchiv oder Speicherarchive für Speicher eines IBM Spectrum Protect-Servers verwenden zu können, müssen Sie zunächst die Einheiten auf dem Serversystem konfigurieren.

Vorbereitende Schritte

1. Schließen Sie Einheiten an die Server-Hardware an. Führen Sie die Anweisungen in Automatisierte Speicherarchiveinheit an das System anschließen aus.
2. Wählen Sie die Bandeinheitentreiber aus. Führen Sie die Anweisungen in Bandeinheitentreiber auswählen aus.
3. Installieren und konfigurieren Sie die Bandeinheitentreiber. Führen Sie die Anweisungen in Bandeinheitentreiber installieren und konfigurieren aus.
4. Bestimmen Sie die Einheitennamen, die zum Definieren des Speicherarchivs für den Server benötigt werden. Führen Sie die Anweisungen in Gerätedateinamen für Bandeinheiten aus.

Vorgehensweise

1. Definieren Sie das Speicherarchiv und den Pfad vom Server zum Speicherarchiv. Führen Sie die Anweisungen in Speicherarchive definieren aus.
2. Definieren Sie die Laufwerke im Speicherarchiv. Führen Sie die Anweisungen in Laufwerke definieren aus.

    Bei SCSI-Speicherarchiven und können Sie mithilfe des Befehls PERFORM LIBACTION Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt definieren, anstatt die beiden Schritte 2 und 3 auszuführen. Um den Befehl PERFORM LIBACTION zum Definieren von Laufwerken und Pfaden für ein Speicherarchiv verwenden zu können, muss die Option SANDISCOVERY unterstützt werden und aktiviert sein.

3. Definieren Sie mithilfe des Befehls DEFINE PATH einen Pfad vom Server zu jedem Laufwerk.
4. Definieren Sie eine Einheitenklasse. Führen Sie die Anweisungen in Bandeinheitenklassen definieren aus.

    Einheitenklassen geben die Aufzeichnungsformate für Laufwerke an und klassifizieren diese gemäß dem Typ. Verwenden Sie den Standardwert FORMAT=DRIVE nur dann als Aufzeichnungsformat, wenn alle Laufwerke, die der Einheitenklasse zugeordnet sind, Daten von allen Datenträgern lesen bzw. auf alle Datenträger schreiben können.

    Angenommen, es ist eine Kombination aus Ultrium-Laufwerken der Generation 3 und Ultrium-Laufwerken der Generation 4 vorhanden, es sind aber nur Ultrium-Datenträger der Generation 3 vorhanden. Sie können FORMAT=DRIVE angeben, da sowohl die Laufwerke der Generation 4 als auch die Laufwerke der Generation 3 Daten von Datenträgern der Generation 3 lesen bzw. auf Datenträger der Generation 3 schreiben können.
5. Definieren Sie einen Speicherpool mithilfe des Befehls DEFINE STGPOOL.

Beachten Sie beim Definieren von Speicherpools die folgenden wichtigsten Auswahlmöglichkeiten:

- Arbeitsdatenträger sind leere Datenträger, die für die Verwendung verfügbar sind. Wenn Sie für die maximale Anzahl Arbeitsdatenträger in dem Speicherpool einen Wert angeben, kann der Server aus den in dem Speicherarchiv verfügbaren Arbeitsdatenträgern eine Auswahl treffen.

  Wenn keine Arbeitsdatenträger zulässig sind, müssen Sie einen zusätzlichen Schritt ausführen, in dem Sie jeden im Speicherpool zu verwendenden Datenträger explizit definieren. Geben Sie außerdem den Parameter MAXSCRATCH=0 an, wenn Sie den Speicherpool definieren, damit keine Arbeitsdatenträger verwendet werden.

- Die Standardeinstellung für primäre Speicherpools ist die Kollokation nach Gruppe. Für Kopienspeicherpools und Pools für aktive Daten ist die Kollokation standardmäßig inaktiviert. Mithilfe der *Kollokation* speichert der Server alle Dateien, die zu einer Gruppe von Clientknoten, einem einzelnen Clientknoten, einem Clientdateibereich oder einer Gruppe von Clientdateibereichen gehören, auf möglichst wenigen Datenträgern. Wenn die Kollokation für einen Speicherpool inaktiviert ist und Clients mit dem Speichern von Daten beginnen, können Sie die Daten in dem Pool nicht einfach so ändern, dass sie kollokiert werden.

6. Stellen Sie Datenträger in das Speicherarchiv zurück und ordnen Sie ihnen Kennsätze zu. Führen Sie die Anweisungen in Datenträger in ein automatisiertes Speicherarchiv zurückstellen und Banddatenträgern Kennsätze zuordnen aus.

   Stellen Sie sicher, dass genügend Datenträger in dem Speicherarchiv für den Server verfügbar sind. Halten Sie genügend Datenträger mit Kennsätzen bereit, damit während einer Operation, wie beispielsweise einer Clientsicherung, keine Datenträger fehlen. Ordnen Sie zusätzlichen Arbeitsdatenträgern Kennsätze zu, damit später für mögliche Wiederherstellungsoperationen Arbeitsdatenträger verfügbar sind.

   Die Prozeduren für das Zurückstellen von Datenträgern und das Zuordnen von Kennsätzen sind, unabhängig davon, ob das Speicherarchiv Laufwerke mit einem einzigen Einheitentyp oder Laufwerke mit mehreren Einheitentypen enthält, identisch. Mit dem Befehl CHECKIN LIBVOLUME können Sie Datenträger, denen bereits ein Kennsatz zugeordnet wurde, zurückstellen. Wenn Datenträger gleichzeitig mit dem Zuordnen eines Kennsatzes zurückgestellt werden sollen, geben Sie den Befehl LABEL LIBVOLUME aus.

   Speicherarchive mit mehreren Einheitentypen: Wenn Ihr Speicherarchiv Laufwerke mit mehreren Einheitentypen enthält und Sie zwei Speicherarchive für den IBM Spectrum Protect-Server definiert hatten, stellen die beiden definierten Speicherarchive ein einziges physisches Speicherarchiv dar. Sie müssen Banddatenträger separat in jedes definierte Speicherarchiv zurückstellen. Stellen Sie sicher, dass die Datenträger in das korrekte IBM Spectrum Protect-Speicherarchiv zurückgestellt werden.

Nächste Schritte

Überprüfen Sie Ihre Einheitendefinitionen, um sicherzustellen, dass die gesamte Konfiguration korrekt ist. Mit dem Befehl QUERY können Sie Informationen zu jedem Speicherobjekt überprüfen.

Stellen Sie bei der Überprüfung der Ergebnisse des Befehls QUERY DRIVE sicher, dass der Einheitentyp für das Laufwerk wie erwartet lautet. Wenn ein Pfad nicht definiert ist, wird der Laufwerkeinheitentyp als UNKNOWN aufgelistet; wenn der falsche Pfad verwendet wird, wird GENERIC_TAPE oder ein anderer Einheitentyp angezeigt. Dieser Schritt ist insbesondere dann wichtig, wenn gemischte Datenträger verwendet werden.

Konfigurieren Sie wahlweise die gemeinsame Speicherarchivnutzung. Führen Sie die Anweisungen in Gemeinsame Speicherarchivnutzung konfigurieren aus.

- Bandeinheiten definieren
  Bevor Sie Daten sichern oder auf Band umlagern können, müssen Sie eine Bandeinheit für IBM Spectrum Protect definieren.
- Gemeinsame Speicherarchivnutzung konfigurieren
  Mehrere IBM Spectrum Protect-Server können Speichereinheiten unter Verwendung eines Speicherbereichsnetzes (SAN) gemeinsam nutzen. Ein Server wird als Speicherarchivmanager konfiguriert, die anderen Server werden als Speicherarchivclients konfiguriert.

Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Speicherarchiv definieren oder löschen)

Bandeinheiten definieren

Bevor Sie Daten sichern oder auf Band umlagern können, müssen Sie eine Bandeinheit für IBM Spectrum Protect definieren.

- Speicherarchive und Laufwerke definieren
  Ein Bandarchiv kann ein oder mehrere Bandlaufwerke enthalten. Nachfolgend ist beschrieben, wie Speicherarchive, Laufwerke und Pfade für den IBM Spectrum Protect-Server definiert werden.
- Bandeinheitenklassen definieren
  Eine Einheitenklasse definiert eine Reihe von Merkmalen, die von einer Gruppe von Datenträgern verwendet wird, die in einem Speicherpool erstellt werden kann. Sie müssen eine Einheitenklasse für eine Bandeinheit definieren, um sicherzustellen, dass der Server die Einheit verwenden kann.

Speicherarchive und Laufwerke definieren

Ein Bandarchiv kann ein oder mehrere Bandlaufwerke enthalten. Nachfolgend ist beschrieben, wie Speicherarchive, Laufwerke und Pfade für den IBM Spectrum Protect-Server definiert werden.

- Speicherarchive definieren
  Bevor ein Laufwerk verwendet werden kann, muss das Speicherarchiv, zu dem das Laufwerk gehört, definiert werden.
- Laufwerke definieren
  Um den Server über ein Laufwerk zu informieren, das für den Zugriff auf Speicherdatenträger verwendet werden kann, geben Sie den Befehl DEFINE DRIVE gefolgt vom Befehl DEFINE PATH aus.

Speicherarchive definieren

Bevor ein Laufwerk verwendet werden kann, muss das Speicherarchiv, zu dem das Laufwerk gehört, definiert werden.

Vorgehensweise

1. Definieren Sie das Speicherarchiv mit dem Befehl DEFINE LIBRARY.

   Beispielsweise können Sie bei einem Bandarchiv IBM TS3500 mithilfe des folgenden Befehls ein Speicherarchiv mit dem Namen ROBOTMOUNT definieren:

   ```
   define library robotmount libtype=scsi
   ```

   Wenn die gemeinsame Speicherarchivnutzung oder die LAN-unabhängige Datenversetzung erforderlich ist, lesen Sie die folgenden Informationen:
   - Gemeinsame Speicherarchivnutzung konfigurieren
   - LAN-unabhängige Datenversetzung konfigurieren
2. Definieren Sie mithilfe des Befehls DEFINE PATH einen Pfad vom Server zum Speicherarchiv. Wenn Sie den Parameter DEVICE angeben, geben Sie den Gerätedateinamen für die Einheit ein. Dieser Name wird vom Server für die Kommunikation mit Bandlaufwerken, Datenträgerwechslern, und Einheiten für austauschbare Datenträger benötigt. Weitere Informationen zu Gerätedateinamen für Einheiten finden Sie in Gerätedateinamen für Bandeinheiten.  AIX-Betriebssysteme

   ```
   define path server1 robotmount srctype=server desttype=library
    device=/dev/lb0
   ```

    Linux-Betriebssysteme

   ```
   define path server1 robotmount srctype=server desttype=library
    device=/dev/tsmscsi/lb0
   ```

    Windows-Betriebssysteme

   ```
   define path server1 robotmount srctype=server desttype=library
    device=lb0.0.1.0
   ```

- SCSI-Speicherarchive in einem SAN definieren
  Beim Speicherarchivtyp SCSI in einem SAN kann der Server die Seriennummer des Speicherarchivs verfolgen. Mit der Seriennummer kann der Server die Identität der Einheit bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

Zugehörige Verweise:
DEFINE LIBRARY (Speicherarchiv definieren)
DEFINE PATH (Pfad definieren)

Laufwerke definieren

Um den Server über ein Laufwerk zu informieren, das für den Zugriff auf Speicherdatenträger verwendet werden kann, geben Sie den Befehl DEFINE DRIVE gefolgt vom Befehl DEFINE PATH aus.

Vorbereitende Schritte

Ein *Laufwerkobjekt* stellt einen Laufwerkmechanismus in einem Speicherarchiv dar, das austauschbare Datenträger verwendet. Bei Einheiten mit mehreren Laufwerken, einschließlich automatisierter Speicherarchive, müssen Sie jedes Laufwerk separat definieren und einem Speicherarchiv zuordnen. Laufwerkdefinitionen können Informationen wie die Elementadresse für Laufwerke in SCSI-Speicherarchiven, die Anzahl Reinigungsvorgänge für ein Bandlaufwerk und die Angabe enthalten, ob das Laufwerk online ist.

IBM Spectrum Protect unterstützt Bandlaufwerke, bei denen es sich um Standalone-Bandlaufwerke handeln kann oder die Teil eines automatisierten Speicherarchivs sein können. Die bevorzugte Methode ist die Konfiguration der Bandspeicherlösung durch die Verwendung automatisierter Speicherarchive.

Informationen zu diesem Vorgang

Wenn Sie den Befehl DEFINE DRIVE ausgeben, müssen Sie einen Teil oder alle der folgenden Informationen zur Verfügung stellen:

Speicherarchivname
: Der Name des Speicherarchivs, in dem sich das Laufwerk befindet.

Laufwerkname
: Der Name, der dem Laufwerk zugeordnet ist.

Seriennummer
: Die Seriennummer des Laufwerks. Der Parameter für die Seriennummer gilt nur für Laufwerke in SCSI-Speicherarchiven. Mit der Seriennummer kann der Server die Identität der Einheit bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

  Falls gewünscht, können Sie die Seriennummer angeben. Standardmäßig kann der Server die Seriennummer vom Laufwerk selbst abrufen, wenn der Pfad definiert wird. Wenn Sie die Seriennummer angeben, bestätigt der Server, dass die Seriennummer korrekt ist, wenn Sie den Pfad zu dem Laufwerk definieren. Wenn Sie den Pfad definieren, können Sie den Parameter AUTODETECT=YES angeben, um dem Server die Korrektur der Seriennummer zu ermöglichen, wenn die von ihm erkannte Nummer nicht mit Ihrer Eingabe bei der Definition des Laufwerks übereinstimmt. Ein bewährtes Verfahren ist die Angabe des Parameters AUTODETECT=YES, damit die Seriennummer für das Laufwerk automatisch in der Datenbank aktualisiert wird, wenn der Pfad definiert wird.

  Abhängig vom Leistungsspektrum des Laufwerks kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet. Siehe Auswirkungen von Einheitenänderungen im SAN.

Elementadresse
: Die Elementadresse des Laufwerks. Der Parameter ELEMENT gilt nur für Laufwerke in SCSI-Speicherarchiven. Die Elementadresse ist eine Zahl, die die physische Position eines Laufwerks in einem automatisierten Speicherarchiv angibt. Der Server benötigt die Elementadresse, um die physische Position des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Der Server kann die Elementadresse vom Laufwerk abrufen, wenn Sie den Pfad definieren, oder Sie können die Elementadresse angeben, wenn Sie das Laufwerk definieren. Ein bewährtes Verfahren ist die Angabe des Parameters ELEMENT=AUTODETECT, damit der Server die Elementnummer automatisch erkennt, wenn der Pfad zu dem Laufwerk definiert wird.

  Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Elementadresse möglicherweise nicht automatisch erkennen. In diesem Fall müssen Sie die Elementadresse angeben, wenn Sie das Laufwerk definieren, falls das Speicherarchiv über mehrere Laufwerke verfügt. Um die Elementadresse abzurufen, rufen Sie das IBM® Support Portal for IBM Spectrum Protect auf.

Tipp: IBM Bandeinheitentreiber und Bandeinheitentreiber anderer Hersteller als IBM generieren unterschiedliche Einheitendateien und Formate:

- Bei IBM Bandeinheitentreibern beginnen Einheitennamen mit rmt, gefolgt von einer ganzen Zahl, beispielsweise /dev/rmt0.
- Bei IBM Spectrum Protect-Bandeinheitentreibern beginnen Bandeinheitennamen mit mt, gefolgt von einer ganzen Zahl, beispielsweise /dev/mt0.

Sie müssen die korrekte Einheitendatei verwenden, wenn Sie einen Pfad definieren.

Vorgehensweise

1. Ordnen Sie einem Speicherarchiv ein Laufwerk zu, indem Sie den Befehl DEFINE DRIVE ausgeben.
2. Damit der Server das Laufwerk verwenden kann, geben Sie den Befehl DEFINE PATH aus.

   Beispiele für die Konfiguration von Speicherarchiven, Pfaden und Laufwerken finden Sie in Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurieren und Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren.

Bandeinheitenklassen definieren

Eine Einheitenklasse definiert eine Reihe von Merkmalen, die von einer Gruppe von Datenträgern verwendet wird, die in einem Speicherpool erstellt werden kann. Sie müssen eine Einheitenklasse für eine Bandeinheit definieren, um sicherzustellen, dass der Server die Einheit verwenden kann.

Vorbereitende Schritte

Sie müssen Speicherarchive und Laufwerke für den Server definieren, bevor Sie Einheitenklassen definieren.

Informationen zu diesem Vorgang

Eine Liste der unterstützten Einheiten und gültigen Einheitenklassenformate finden Sie auf der Website mit den von IBM Spectrum Protect unterstützten Einheiten für Ihr Betriebssystem:

- AIX-Betriebssysteme Windows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Sie können mehrere Einheitenklassen für jeden Einheitentyp definieren. Beispielsweise möchten Sie möglicherweise unterschiedliche Attribute für unterschiedliche Speicherpools angeben, die denselben Typ von Bandlaufwerk verwenden. Unter Umständen sind Variationen erforderlich, die nicht einheitenspezifisch sind, sondern davon abhängig sind, wie die Einheit verwendet werden soll (zum Beispiel Mount-Aufbewahrungszeitraum oder Mountlimit).

Richtlinien:

- Eine einzelne Einheitenklasse kann mehreren Speicherpools zugeordnet werden, jeder Speicherpool ist jedoch nur einer einzigen Einheitenklasse zugeordnet.
- SCSI-Speicherarchive können Bandlaufwerke mehrerer Einheitentypen umfassen. Wenn Sie die Einheitenklasse in dieser Umgebung definieren, müssen Sie einen Wert für den Parameter FORMAT deklarieren.

  Weitere Informationen finden Sie in Gemischte Einheitentypen in Speicherarchiven.

Vorgehensweise

Um eine Einheitenklasse zu definieren, verwenden Sie den Befehl DEFINE DEVCLASS mit dem Parameter DEVTYPE, mit dem der Einheitenklasse ein Einheitentyp zugeordnet wird.

Ergebnisse

Wenn Sie die Option DEVCONFIG in die Datei dsmserv.opt einschließen, werden die über diese Option angegebenen Dateien automatisch mit den Ergebnissen der Befehle DEFINE DEVCLASS, UPDATE DEVCLASS und DELETE DEVCLASS aktualisiert.

- Einheitenklassen LTO definieren
  Um Probleme beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv zu vermeiden, beachten Sie die Einschränkungen. Beachten Sie außerdem die Einschränkungen für die LTO-Laufwerkverschlüsselung.
- Einheitenklassen 3592 definieren
  Einheitenklassendefinitionen für 3592-, TS1130-, TS1140-, TS1150-Einheiten und Einheiten späterer Generationen umfassen Parameter für höhere Datenträgerzugriffsgeschwindigkeiten und Laufwerkverschlüsselung. Um Probleme beim Mischen verschiedener Generationen von 3592- und TS1130-Laufwerken und Laufwerken späterer Generationen in einem Speicherarchiv zu verhindern, lesen Sie die Richtlinien.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
QUERY DEVCLASS (Informationen zu einer oder mehreren Einheitenklassen anzeigen)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Einheitenklassen LTO definieren

Um Probleme beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv zu vermeiden, beachten Sie die Einschränkungen. Beachten Sie außerdem die Einschränkungen für die LTO-Laufwerkverschlüsselung.

- LTO-Laufwerke und -Datenträger in einem Speicherarchiv mischen
  Beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern müssen Sie die Schreib-/Lesefunktionalität jeder Generation berücksichtigen. Die bevorzugte Methode ist die Konfiguration einer anderen Einheitenklasse für jede Generation von Datenträgern.
- Mountlimits in LTO-Umgebungen mit gemischten Datenträgern
  In einem Speicherarchiv mit gemischten Datenträgern, in dem mehrere Einheitenklassen auf dasselbe Speicherarchiv verweisen, werden kompatible Laufwerke von Speicherpools gemeinsam genutzt. Stellen Sie sicher, dass Sie für den Parameter MOUNTLIMIT in jeder der Einheitenklassen einen geeigneten Wert festlegen.
- Laufwerkverschlüsselung für LTO-Bandlaufwerke der Generation 4 oder späterer Generationen aktivieren und inaktivieren
  IBM Spectrum Protect unterstützt die drei Typen von Laufwerkverschlüsselung, die für LTO-Laufwerke der Generation 4 oder späterer Generationen verfügbar sind: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

LTO-Laufwerke und -Datenträger in einem Speicherarchiv mischen

Beim Mischen verschiedener Generationen von LTO-Laufwerken und -Datenträgern müssen Sie die Schreib-/Lesefunktionalität jeder Generation berücksichtigen. Die bevorzugte Methode ist die Konfiguration einer anderen Einheitenklasse für jede Generation von Datenträgern.

Informationen zu diesem Vorgang

Wenn Sie das Mischen verschiedener Generationen von LTO-Datenträgern und -Laufwerken in Betracht ziehen, beachten Sie die folgenden Einschränkungen:

Tabelle 1. Schreib-/Lesefunktionalität für verschiedene Generationen von LTO-Laufwerken

Laufwerke	Datenträger der Generation 1	Datenträger der Generation 2	Datenträger der Generation 3	Datenträger der Generation 4	Datenträger der Generation 5	Datenträger der Generation 6	Datenträger der Generation 7
Generation 1	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 2	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 3	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 4	nicht zutreffend	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 5	nicht zutreffend	nicht zutreffend	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend
Generation 6	nicht zutreffend	nicht zutreffend	nicht zutreffend	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend
Generation 7	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff

Beispiel

Wenn Sie verschiedene Typen von Laufwerken und Datenträgern mischen, konfigurieren Sie unterschiedliche Einheitenklassen: eine Einheitenklasse für jeden Datenträgertyp. Um den Datenträgertyp anzugeben, verwenden Sie den Parameter FORMAT in jeder der Einheitenklassendefinitionen. (Geben Sie nicht FORMAT=DRIVE an.) Wenn Sie beispielsweise Ultrium-Laufwerke der Generation 5 und Ultrium-Laufwerke der Generation 6 mischen, geben Sie FORMAT=ULTRIUM5C (oder ULTRIUM5) für die Ultrium-Einheitenklasse der Generation 5 und FORMAT=ULTRIUM6C (oder ULTRIUM6) für die Ultrium-Einheitenklasse der Generation 6 an.

In diesem Beispiel können beide Einheitenklassen auf dasselbe Speicherarchiv mit Ultrium-Laufwerken der Generation 5 und Ultrium-Laufwerken der Generation 6 verweisen. Die Laufwerke werden von den beiden Speicherpools gemeinsam genutzt. Ein Speicherpool verwendet ausschließlich die erste Einheitenklasse und Ultrium-Datenträger der Generation 5. Der andere Speicherpool verwendet ausschließlich die zweite Einheitenklasse und Ultrium-Datenträger der Generation 6. Da die beiden Speicherpools ein einzelnes Speicherarchiv gemeinsam nutzen, können Ultrium-Datenträger der Generation 5 in Ultrium-Laufwerken der Generation 6 bereitgestellt werden, sobald sie während der Mountpunktverarbeitung verfügbar werden.

Wenn Sie ältere Generationen von Datenträgern mit Lesezugriff mit neueren Generationen von Datenträgern mit Schreib-/Lesezugriff in einem einzelnen Speicherarchiv mischen, müssen Sie die Datenträger mit Lesezugriff als schreibgeschützt markieren und alle Arbeitsdatenträger mit Lesezugriff entnehmen. Wenn Sie beispielsweise Ultrium-Laufwerke und -Datenträger der Generation 4 und Ultrium-Laufwerke und -Datenträger der Generation 6 in einem einzelnen Speicherarchiv mischen, müssen Sie die Datenträger der Generation 4 als schreibgeschützt markieren. Außerdem müssen alle Arbeitsdatenträger der Generation 4 entnommen werden.

Mountlimits in LTO-Umgebungen mit gemischten Datenträgern

In einem Speicherarchiv mit gemischten Datenträgern, in dem mehrere Einheitenklassen auf dasselbe Speicherarchiv verweisen, werden kompatible Laufwerke von Speicherpools gemeinsam genutzt. Stellen Sie sicher, dass Sie für den Parameter MOUNTLIMIT in jeder der Einheitenklassen einen geeigneten Wert festlegen.

Beispielsweise können in einem Speicherarchiv mit gemischten Datenträgern, das Ultrium-Laufwerke und -Datenträger der Generation 1 und der Generation 2 enthält, Ultrium-Datenträger der Generation 1 in Ultrium-Laufwerken der Generation 2 bereitgestellt werden.

Betrachten Sie das Beispiel für ein Speicherarchiv mit gemischten Datenträgern, das die folgenden Laufwerke und Datenträger enthält:

- Vier LTO Ultrium-Laufwerke der Generation 1 und LTO Ultrium-Datenträger der Generation 1
- Vier LTO Ultrium-Laufwerke der Generation 2 und LTO Ultrium-Datenträger der Generation 2

Sie haben die folgenden Einheitenklassen erstellt:

- Einheitenklasse LTO1CLASS für LTO Ultrium Generation 1 mit der Angabe FORMAT=ULTRIUMC
- Einheitenklasse LTO2CLASS für LTO Ultrium Generation 2 mit der Angabe FORMAT=ULTRIUM2C

Außerdem haben Sie die folgenden Speicherpools erstellt:

- LTO Ultrium-Speicherpool LTO1POOL der Generation 1, der auf Einheitenklasse LTO1CLASS basiert
- LTO Ultrium-Speicherpool LTO2POOL der Generation 2, der auf Einheitenklasse LTO2CLASS basiert

Die Anzahl Mountpunkte, die von jedem Speicherpool verwendet werden können, wird mit dem Parameter MOUNTLIMIT in der Einheitenklasse angegeben. Der Parameter MOUNTLIMIT in der Einheitenklasse LTO2CLASS muss auf 4 gesetzt werden, damit er mit der Anzahl verfügbarer Laufwerke übereinstimmt, die nur LTO2-Datenträger bereitstellen können. Der Parameter MOUNTLIMIT in der Einheitenklasse LTO1CLASS muss

auf einen Wert gesetzt werden, der größer als die Anzahl verfügbarer Laufwerke (5 oder möglicherweise 6) ist, um der Tatsache Rechnung zu tragen, dass Ultrium-Datenträger der Generation 1 in Ultrium-Laufwerken der Generation 2 bereitgestellt werden können. Der optimale Wert für MOUNTLIMIT ist von der Workload und Speicherpoolzugriffsmustern abhängig.

Überwachen Sie die Einstellung für MOUNTLIMIT und passen Sie sie gemäß sich ändernden Workloads an. Wenn der Wert für MOUNTLIMIT für LTO1POOL zu hoch definiert wird, können Mountanforderungen für LTO2POOL verzögert werden oder fehlschlagen, da die Ultrium-Laufwerke der Generation 2 zur Ausführung von Mountanforderungen für Ultrium Generation 1 verwendet werden. Im Worst-Case-Szenario kann ein zu starkes Konkurrieren um Ultrium-Laufwerke der Generation 2 dazu führen, dass Mounts für Datenträger der Generation 2 mit der folgenden Nachricht fehlschlagen:

```
ANR8447E Gegenwärtig sind keine Laufwerke im Kassettenarchiv verfügbar.
```

Wenn der Wert für MOUNTLIMIT für LTO1POOL nicht hoch genug definiert wird, werden Mountanforderungen, die von LTO Ultrium-Laufwerken der Generation 2 ausgeführt werden könnten, verzögert.
Einschränkung: Aufgrund der Art und Weise, auf die Mountpunkte zugeordnet werden, gelten beim Kombinieren von Ultrium-Laufwerken der Generation 1 mit Ultrium-Laufwerken der Generation 2 oder der Generation 3 Einschränkungen. Prozesse, die mehrere Mountpunkte erfordern, die sowohl Ultrium-Datenträger der Generation 1 als auch Ultrium-Datenträger der Generation 2 einschließen, versuchen beispielsweise unter Umständen, nur Ultrium-Laufwerke der Generation 2 zu reservieren, selbst wenn ein einzelner Mount von einem verfügbaren Ultrium-Laufwerk der Generation 1 ausgeführt werden kann. Zu den Prozessen, die dieses Verhalten zeigen, gehören die Befehle MOVE DATA und BACKUP STGPOOL. Diese Prozesse warten, bis die erforderliche Anzahl Mountpunkte mit Ultrium-Laufwerken der Generation 2 erreicht werden kann.
Zugehörige Verweise:
BACKUP STGPOOL (Daten in primären Speicherpools in einem Kopienspeicherpool sichern)
DEFINE DEVCLASS (Einheitenklasse definieren)
MOVE DATA (Dateien auf einen Speicherpooldatenträger versetzen)

Laufwerkverschlüsselung für LTO-Bandlaufwerke der Generation 4 oder späterer Generationen aktivieren und inaktivieren

IBM Spectrum Protect unterstützt die drei Typen von Laufwerkverschlüsselung, die für LTO-Laufwerke der Generation 4 oder späterer Generationen verfügbar sind: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

Informationen zu diesem Vorgang

Der Parameter DRIVEENCRYPTION im Befehl DEFINE DEVCLASS gibt an, ob die Laufwerkverschlüsselung für IBM und HP LTO-Formate der Generation 4 oder späterer Generationen sowie für Ultrium 4- und Ultrium 4C-Formate zulässig ist. Mit diesem Parameter wird IBM Spectrum Protect-Kompatibilität mit Hardwareverschlüsselungseinstellungen für leere Datenträger sichergestellt. Sie können diesen Parameter nicht für Speicherpooldatenträger verwenden, die voll sind oder gefüllt werden.

IBM Spectrum Protect unterstützt das Anwendungsverschlüsselungsverfahren mit IBM und HP LTO-4-Laufwerken oder Laufwerken späterer Generationen. Die System- und Speicherarchivverfahren werden nur von IBM LTO-4 oder späteren Generationen unterstützt. Das Speicherarchivverschlüsselungsverfahren kann nur verwendet werden, wenn es von Ihrer Systemhardware (beispielsweise IBM TS3500) unterstützt wird.

Einschränkung: Sie können keine Laufwerkverschlüsselung für WORM-Datenträger (WORM = Write Once Read Many) verwenden.

Das Anwendungsverfahren wird über die Hardware definiert. Um das Anwendungsverfahren zu verwenden, bei dem IBM Spectrum Protect Verschlüsselungsschlüssel generiert und verwaltet, setzen Sie den Parameter DRIVEENCRYPTION auf ON. Mit dieser Aktion wird die Datenverschlüsselung für leere Datenträger aktiviert. Wenn der Parameter auf ON gesetzt wird und die Hardware für ein anderes Verschlüsselungsverfahren konfiguriert ist, schlagen Sicherungsoperationen fehl.

Vorgehensweise

Das folgende vereinfachte Beispiel zeigt die Schritte für die Aktivierung und die Inaktivierung der Datenverschlüsselung für leere Datenträger in einem Speicherpool:

1. Definieren Sie ein Speicherarchiv, indem Sie den Befehl DEFINE LIBRARY ausgeben:

   ```
   define library 3584 libtype=SCSI
   ```

2. Definieren Sie eine Einheitenklasse mit dem Namen LTO_ENCRYPT, indem Sie den Befehl DEFINE DEVCLASS unter Angabe von IBM Spectrum Protect als Schlüsselmanager ausgeben:

   ```
   define devclass lto_encrypt library=3584 devtype=lto driveencryption=on
   ```

3. Definieren Sie einen Speicherpool, indem Sie den Befehl DEFINE STGPOOL ausgeben:

   ```
   define stgpool lto_encrypt_pool lto_encrypt
   ```

4. Um die Verschlüsselung für neue Datenträger zu inaktivieren, setzen Sie den Parameter DRIVEENCRYPTION auf OFF. Der Standardwert ist ALLOW. Die Laufwerkverschlüsselung für leere Datenträger ist zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

Zugehörige Konzepte:
Verschlüsselungsverfahren für Bänder

Einheitenklassen 3592 definieren

Einheitenklassendefinitionen für 3592-, TS1130-, TS1140-, TS1150-Einheiten und Einheiten späterer Generationen umfassen Parameter für höhere Datenträgerzugriffsgeschwindigkeiten und Laufwerkverschlüsselung. Um Probleme beim Mischen verschiedener Generationen von 3592- und TS1130-Laufwerken und Laufwerken späterer Generationen in einem Speicherarchiv zu verhindern, lesen Sie die Richtlinien.

- Generationen von 3592-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen
  Um eine optimale Leistung zu erzielen, dürfen Sie keine Generationen von 3592-Datenträgern in einem einzelnen Speicherarchiv mischen. Es können Datenträgerprobleme auftreten, wenn verschiedene Laufwerkgenerationen gemischt werden. Beispielsweise kann IBM Spectrum Protect möglicherweise den Kennsatz eines Datenträgers nicht lesen.
- Datenzugriffsgeschwindigkeiten für 3592-Datenträger steuern
  Sie können die Speicherkapazität optimieren und Datenzugriffsgeschwindigkeiten verbessern, wenn Sie Datenträger erstellen. Indem Daten in Speicherpools mit Datenträgern partitioniert werden, können Sie die Skalierungskapazität in Prozent angeben, um maximale Speicherkapazität oder schnellen Zugriff auf den Datenträger bereitstellen zu können.
- Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen aktivieren und inaktivieren
  Bei IBM Spectrum Protect können Sie die folgenden Typen von Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen verwenden: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

Generationen von 3592-Laufwerken und -Datenträgern in einem einzelnen Speicherarchiv mischen

Um eine optimale Leistung zu erzielen, dürfen Sie keine Generationen von 3592-Datenträgern in einem einzelnen Speicherarchiv mischen. Es können Datenträgerprobleme auftreten, wenn verschiedene Laufwerkgenerationen gemischt werden. Beispielsweise kann IBM Spectrum Protect möglicherweise den Kennsatz eines Datenträgers nicht lesen.

Informationen zu diesem Vorgang

Die folgende Tabelle zeigt Schreib-/Leseinteroperabilität für Laufwerkgenerationen.

Laufwerke	Format der Generation 1	Format der Generation 2	Format der Generation 3	Format der Generation 4	Format der Generation 5
Generation 1	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 2	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 3	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend	nicht zutreffend
Generation 4	nicht zutreffend	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff	nicht zutreffend
Generation 5	nicht zutreffend	nicht zutreffend	Lesezugriff	Schreib-/Lesezugriff	Schreib-/Lesezugriff

Wenn Generationen von Laufwerken in einem Speicherarchiv gemischt werden müssen, schauen Sie sich das Beispiel und die Einschränkungen an, um Probleme zu vermeiden.

Tabelle 1. Generationen von Laufwerken mischen

Speicherarchivtyp	Beispiel und Einschränkungen

Speicherarchivtyp	Beispiel und Einschränkungen
SCSI	Definieren Sie einen neuen Speicherpool und eine neue Einheitenklasse für die neueste Laufwerkgeneration. Angenommen, Sie verfügen über einen Speicherpool und eine Einheitenklasse für 3592-2. Der Speicherpool enthält alle Datenträger, die im Format der Generation 2 geschrieben wurden. Angenommen, der Wert des Parameters FORMAT in der Einheitenklassendefinition ist auf 3952-2 (nicht DRIVE) gesetzt. Sie fügen dem Speicherarchiv Laufwerke der Generation 3 hinzu. Führen Sie die folgenden Schritte aus: 1. Setzen Sie in der neuen Einheitenklassendefinition für die Laufwerke der Generation 3 den Wert für den Parameter FORMAT auf 3592-3 oder 3592-3C. Geben Sie nicht DRIVE an. 2. Aktualisieren Sie in der Definition des Speicherpools, der Laufwerken der Generation 2 zugeordnet ist, den Parameter MAXSCRATCH mit 0, beispielsweise: `update stgpool genpool2 maxscratch=0` Diese Methode ermöglicht beiden Generationen die Verwendung ihres optimalen Formats und minimiert mögliche Datenträgerprobleme, die aus dem Mischen von Generationen resultieren können. Es werden jedoch nicht alle Datenträgerprobleme behoben. Beispielsweise könnten Konkurrenzsituationen bei Mountpunkten und Mountfehler die Folge sein. (Weitere Informationen zu Konkurrenzsituationen bei Mountpunkten im Kontext von 3592-Laufwerken und -Datenträgern finden Sie in Einheitenklassen 3592 definieren.) Einschränkung: In der folgenden Liste sind Einschränkungen beschrieben, die für Datenträger gelten: • CHECKIN LIBVOL: Das Problem liegt in der Verwendung der Option CHECKLABEL=YES. Wenn der Kennsatz in einem Format der Generation 3 oder einem späteren Format geschrieben ist und Sie die Option CHECKLABEL=YES angeben, schlägt die Verwendung dieses Befehls für Laufwerke früherer Generationen fehl. Um dieses Problem zu verhindern, geben Sie CHECKLABEL=BARCODE an. • LABEL LIBVOL: Wenn der Server versucht, Laufwerke einer früheren Generation zum Lesen des Kennsatzes zu verwenden, der in einem Format der Generation 3 oder einem späteren Format geschrieben ist, schlägt der Befehl LABEL LIBVOL fehl, es sei denn, OVERWRITE=YES wird angegeben. Stellen Sie sicher, dass Datenträger, denen unter Angabe von OVERWRITE=YES ein Kennsatz zugeordnet wird, keine aktiven Daten enthalten. • CHECKOUT LIBVOL: Wenn IBM Spectrum Protect feststellt, dass der Kennsatz (CHECKLABEL=YES) in einem Format der Generation 3 oder einem Format einer späteren Generation geschrieben ist, und Leseoperationen durch Laufwerke früherer Generationen erfolgen, schlägt der Befehl fehl. Um dieses Problem zu verhindern, geben Sie CHECKLABEL=NO an.

Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
UPDATE STGPOOL (Speicherpool aktualisieren)

Datenzugriffsgeschwindigkeiten für 3592-Datenträger steuern

Sie können die Speicherkapazität optimieren und Datenzugriffsgeschwindigkeiten verbessern, wenn Sie Datenträger erstellen. Indem Daten in Speicherpools mit Datenträgern partitioniert werden, können Sie die Skalierungskapazität in Prozent angeben, um maximale Speicherkapazität oder schnellen Zugriff auf den Datenträger bereitstellen zu können.

Informationen zu diesem Vorgang

Um die Datenträgerkapazität zu reduzieren, geben Sie den Parameter SCALECAPACITY an, wenn Sie die Einheitenklasse mit dem Befehl DEFINE DEVCLASS definieren oder wenn Sie die Einheitenklasse mit dem Befehl UPDATE DEVCLASS aktualisieren.

Geben Sie einen Prozentwert von 20, 90 oder 100 an. Mit einem Wert von 20 Prozent wird die schnellste Zugriffszeit und mit einem Wert von 100 Prozent die größte Speicherkapazität zur Verfügung gestellt. Wird beispielsweise eine Skalierungskapazität von 20 für eine Einheitenklasse 3592 ohne Komprimierung angegeben, würde ein 3592-Datenträger in dieser Einheitenklasse 20 Prozent seiner vollen Kapazität von 300 GB, d. h. ungefähr 60 GB, speichern.

Die Skalierungskapazität hat nur Auswirkungen, wenn Daten zum ersten Mal auf einen Datenträger geschrieben werden. Aktualisierungen an der Einheitenklasse für die Skalierungskapazität haben erst Auswirkungen auf einen Datenträger, auf den bereits Daten geschrieben wurden, wenn der Datenträger in den Arbeitsstatus zurückversetzt wird.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen aktivieren und inaktivieren

Bei IBM Spectrum Protect können Sie die folgenden Typen von Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen verwenden: Anwendung, System und Speicherarchiv. Diese Verfahren werden über die Hardware definiert.

Informationen zu diesem Vorgang

Der Parameter DRIVEENCRYPTION im Befehl DEFINE DEVCLASS gibt an, ob die Laufwerkverschlüsselung für 3592-Laufwerke der Generation 2 und späterer Generationen zulässig ist. Verwenden Sie diesen Parameter, um IBM Spectrum Protect-Kompatibilität mit Hardwareverschlüsselungseinstellungen für leere Datenträger sicherzustellen. Sie können diesen Parameter nicht für Speicherpooldatenträger verwenden, die voll sind oder gefüllt werden.

- Um das Anwendungsverfahren zu verwenden, bei dem IBM Spectrum Protect Verschlüsselungsschlüssel generiert und verwaltet, setzen Sie den Parameter DRIVEENCRYPTION auf ON. Damit wird die Verschlüsselung von Daten für leere Datenträger aktiviert. Wenn der Parameter auf ON gesetzt wird und die Hardware für ein anderes Verschlüsselungsverfahren konfiguriert ist, schlagen Sicherungsoperationen fehl.
- Um das Speicherarchiv- oder Systemverschlüsselungsverfahren zu verwenden, setzen Sie den Parameter auf ALLOW. Damit wird angegeben, dass IBM Spectrum Protect nicht der Schlüsselmanager für die Laufwerkverschlüsselung ist, der Hardware wird jedoch die Verschlüsselung der Daten des Datenträgers über eines der anderen Verfahren ermöglicht. Bei Angabe dieses Parameters werden Datenträger nicht automatisch verschlüsselt. Daten können nur verschlüsselt werden, wenn der Parameter ALLOW angegeben wird und die Hardware für die Verwendung eines dieser Verfahren konfiguriert wird.

Der Parameter DRIVEENCRYPTION ist optional. Gemäß dem Standardwert ist das Speicherarchiv- oder Systemverschlüsselungsverfahren zulässig.

Vorgehensweise

Das folgende vereinfachte Beispiel zeigt, wie Daten für leere Datenträger in einem Speicherpool unter Verwendung von IBM Spectrum Protect als Schlüsselmanager verschlüsselt werden können:

1. Definieren Sie ein Speicherarchiv, indem Sie den Befehl DEFINE LIBRARY ausgeben. Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   define library 3584 libtype=SCSI
   ```

2. Definieren Sie eine Einheitenklasse mit dem Namen 3592_ENCRYPT, indem Sie den Befehl DEFINE DEVCLASS unter Angabe des Werts ON für den DRIVEENCRYPTION Parameter ausgeben. Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   define devclass 3592_encrypt library=3584 devtype=3592 driveencryption=on
   ```

3. Definieren Sie einen Speicherpool. Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   define stgpool 3592_encrypt_pool 3592_encrypt
   ```

Nächste Schritte

Um eines des Verschlüsselungsverfahren für neue Datenträger zu inaktivieren, setzen Sie den Parameter DRIVEENCRYPTION auf OFF. Wenn die Hardware für die Verschlüsselung von Daten durch das Speicherarchiv- oder Systemverfahren konfiguriert ist und DRIVEENCRYPTION auf OFF gesetzt ist, schlagen Sicherungsoperationen fehl.

Gemeinsame Speicherarchivnutzung konfigurieren

Mehrere IBM Spectrum Protect-Server können Speichereinheiten unter Verwendung eines Speicherbereichsnetzes (SAN) gemeinsam nutzen. Ein Server wird als Speicherarchivmanager konfiguriert, die anderen Server werden als Speicherarchivclients konfiguriert.

Vorbereitende Schritte

Stellen Sie sicher, das Ihre Systeme die Lizenzierungsanforderungen für die gemeinsame Speicherarchivnutzung erfüllen. Ein Nutzungsrecht für IBM Spectrum Protect for SAN ist für jeden IBM Spectrum Protect-Server erforderlich, der als Speicherarchivclient oder Speicherarchivmanager in einer SAN-Umgebung konfiguriert wird.

Informationen zu diesem Vorgang

Bei der LAN-unabhängigen Datenversetzung können IBM Spectrum Protect-Clientsysteme direkt auf Speichereinheiten zugreifen, die für einen IBM Spectrum Protect-Server definiert sind. Speicheragenten werden auf den Clientsystemen zur Ausführung der Datenversetzung installiert und konfiguriert.

Um die gemeinsame Speicherarchivnutzung zu konfigurieren, müssen Sie einen einzelnen IBM Spectrum Protect-Server als den Speicherarchivmanager für die Konfiguration der gemeinsamen Speicherarchivnutzung definieren. Anschließend definieren Sie weitere IBM Spectrum Protect-Server als Speicherarchivclients, die mit dem Speicherarchivmanager kommunizieren und Speicherressourcen vom Speicherarchivmanager anfordern. Der Speicherarchivmanager-Server muss dieselbe Version oder eine höhere Version wie der Server oder die Server haben, die als Speicherarchivclients definiert sind.

Vorgehensweise

Um Speicherarchivressourcen in einem SAN zwischen mehreren IBM Spectrum Protect-Servern gemeinsam nutzen zu können, führen Sie die folgenden Schritte aus:

1. Konfigurieren Sie die Kommunikation zwischen Servern.

   Um eine Speichereinheit in einem SAN gemeinsam nutzen zu können, definieren Sie Server mithilfe der Überkreuzdefinitionsfunktion füreinander. Jeder Server muss einen eindeutigen Namen haben.

2. Definieren Sie ein gemeinsam genutztes Speicherarchiv und konfigurieren Sie Bandeinheiten auf den Serversystemen.

   Verwenden Sie die in Speicherarchive für die Verwendung durch einen Server konfigurieren beschriebene Prozedur zum Definieren eines Speicherarchivs für die Verwendung in einer Umgebung mit gemeinsamer Nutzung. Ändern Sie die Prozedur, um das Speicherarchiv als gemeinsam genutzt zu definieren, indem Sie den Parameter SHARED=YES für den Befehl DEFINE LIBRARY angeben.

3. Definieren Sie den Speicherarchivmanager-Server.
4. Definieren Sie das gemeinsam genutzte Speicherarchiv auf dem Server, der der Speicherarchivclient ist.
5. Definieren Sie auf dem Speicherarchivmanager-Server Pfade vom Speicherarchivclient zu jedem Laufwerk, auf das der Speicherarchivclient zugreifen kann. Der Einheitenname muss die Art und Weise widerspiegeln, auf die das Speicherarchivclientsystem die Bandeinheit erkennt. Vom Speicherarchivmanager muss ein Pfad zu jedem Laufwerk definiert werden, damit der Speicherarchivclient das Laufwerk verwenden kann.

   Um Probleme zu verhindern, stellen Sie sicher, dass alle Laufwerkpfaddefinitionen, die für den Speicherarchivmanager definiert werden, auch für jeden Speicherarchivclient definiert werden.

   Wenn beispielsweise der Speicherarchivmanager drei Bandlaufwerke definiert, muss auch der Speicherarchivclient drei Bandlaufwerke definieren. Um die Anzahl Bandlaufwerke, die ein Speicherarchivclient gleichzeitig nutzen kann, zu begrenzen, verwenden Sie den Parameter MOUNTLIMIT der Einheitenklasse auf dem Speicherarchivclient.
6. Definieren Sie Einheitenklassen für das gemeinsam genutzte Speicherarchiv.

   Die bevorzugte Methode ist, auf beiden Servern identische Einheitenklassennamen zu verwenden, um Unklarheiten zu vermeiden, wenn mehrere Einheitenklassen mit demselben Einheitentyp und denselben Speicherarchivparametern definiert werden. Bei einigen Operationen, wie beispielsweise der Datenbanksicherung, wird der Einheitenklassenname zur Identifikation der Daten für die Sicherung verwendet.

   Die Einheitenklassenparameter, die auf dem Speicherarchivmanager angegeben sind, überschreiben die für den Speicherarchivclient angegebenen Parameter. Wenn die Einheitenklassennamen unterschiedlich sind, verwendet der Speicherarchivmanager die Parameter, die in einer Einheitenklasse angegeben sind, die mit dem für den Speicherarchivclient angegebenen Einheitentyp übereinstimmt.

7. Definieren Sie einen Speicherpool für das gemeinsam genutzte Speicherarchiv.
8. Wiederholen Sie die Schritte, um einen anderen Server als Speicherarchivclient zu konfigurieren.

- AIX-BetriebssystemeLinux-BetriebssystemeBeispiel: Gemeinsame Speicherarchivnutzung für AIX- und Linux-Server
  Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für SCSI-Speicherarchive für Server, die auf AIX- oder Linux-Systemen ausgeführt werden, konfiguriert werden kann.
- Beispiel: Gemeinsame Speicherarchivnutzung für Windows-Server
  Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für Server, die auf Windows-Systemen ausgeführt werden, konfiguriert werden kann.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
DEFINE LIBRARY (Speicherarchiv definieren)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)
AIX-BetriebssystemeLinux-Betriebssysteme

Beispiel: Gemeinsame Speicherarchivnutzung für AIX- und Linux-Server

Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für SCSI-Speicherarchive für Server, die auf AIX- oder Linux-Systemen ausgeführt werden, konfiguriert werden kann.

Informationen zu diesem Vorgang

In diesem Beispiel werden ein Speicherarchivmanager-Server mit dem Namen ASTRO und ein Speicherarchivclient mit dem Namen JUDY konfiguriert. Um zu verdeutlichen, auf welchem Server der Schritt jeweils ausgeführt wird, steht vor dem jeweiligen Befehl der Name des Servers, auf dem der Befehl ausgegeben wird. Der größte Teil der Befehle wird auf dem Speicherarchivclient ausgegeben.

Definieren Sie für SCSI-Speicherarchive das Speicherarchiv unter Angabe des Parameters libtype=scsi.

Vorgehensweise

1. Um ASTRO als den Speicherarchivmanager-Server zu konfigurieren, definieren Sie ein gemeinsam genutztes SCSI-Speicherarchiv mit dem Namen SANGROUP. Beispiel:

   ```
   astro> define library sangroup libtype=scsi shared=yes
   ```

   Führen Sie dann die übrigen Schritte zum Konfigurieren des Speicherarchivs wie in Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurieren beschrieben aus.
   Tipp: Mithilfe des Befehls PERFORM LIBACTION können Sie Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt definieren.
2. Definieren Sie ASTRO als den Speicherarchivmanager-Server, indem Sie den Befehl DEFINE SERVER ausgeben.

   ```
   judy> define server astro serverpassword=secret hladdress=192.0.2.24
    lladdress=1777 crossdefine=yes
   ```

3. Definieren Sie das gemeinsam genutzte Speicherarchiv SANGROUP, indem Sie den Befehl DEFINE LIBRARY ausgeben. Sie müssen den im Parameter PRIMARYLIBMANAGER angegebenen Namen des Speicherarchivmanager-Servers und `LIBTYPE=SHARED` verwenden.

   ```
   judy> define library sangroup libtype=shared primarylibmanager=astro
   ```

   Stellen Sie sicher, dass der Speicherarchivname mit dem Speicherarchivnamen auf dem Speicherarchivmanager übereinstimmt.
4. Definieren Sie Pfade vom Speicherarchivmanager ASTRO zu zwei Laufwerken in dem gemeinsam genutzten Speicherarchiv, indem Sie den Befehl DEFINE PATH ausgeben.
   AIX-Betriebssysteme

   ```
   astro> define path judy drivea srctype=server desttype=drive
    library=sangroup device=/dev/rmt6
   astro> define path judy driveb srctype=server desttype=drive
    library=sangroup device=/dev/rmt7
   ```

   Linux-Betriebssysteme

   ```
   astro> define path judy drivea srctype=server desttype=drive
    library=sangroup device=/dev/IBMtape6
   astro> define path judy driveb srctype=server desttype=drive
    library=sangroup device=/dev/IBMtape7
   ```

5. Definieren Sie alle Einheitenklassen, die dem gemeinsam genutzten Speicherarchiv zugeordnet sind. AIX-Betriebssysteme

   ```
   judy> define devclass tape library=sangroup devtype=lto
   ```

   Linux-Betriebssysteme

   ```
   judy> define devclass tape library=sangroup devtype=lto
   ```

   Die folgenden Parameter für die Einheitenklassendefinition müssen auf dem Speicherarchivclient und dem Speicherarchivmanager übereinstimmen:
   - LIBRARY
   - DRIVEENCRYPTION
   - WORM
   - FORMAT
6. Definieren Sie einen Speicherpool mit dem Namen BACKTAPE für die Verwendung durch das gemeinsam genutzte Speicherarchiv. Geben Sie den Befehl DEFINE STGPOOL aus.

   ```
   judy> define stgpool backtape tape maxscratch=50
   ```

Nächste Schritte

Wiederholen Sie die Prozedur, um weitere Speicherarchivclients für Ihren Speicherarchivmanager zu definieren.
Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
DEFINE DRIVE (Laufwerk für ein Speicherarchiv definieren)
DEFINE LIBRARY (Speicherarchiv definieren)
DEFINE PATH (Pfad definieren)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)
Windows-Betriebssysteme

Beispiel: Gemeinsame Speicherarchivnutzung für Windows-Server

Die Beispielprozedur zeigt, wie eine Umgebung mit gemeinsamer Speicherarchivnutzung für Server, die auf Windows-Systemen ausgeführt werden, konfiguriert werden kann.

Informationen zu diesem Vorgang

In diesem Beispiel werden ein Speicherarchivmanager-Server mit dem Namen ASTRO und ein Speicherarchivclient mit dem Namen JUDY konfiguriert.

Definieren Sie für SCSI-Speicherarchive das Speicherarchiv unter Angabe des Parameters libtype=scsi.

- Windows-BetriebssystemeSpeicherarchivmanager-Server konfigurieren
  Sie müssen den Speicherarchivmanager-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.
- Windows-BetriebssystemeSpeicherarchivclient-Server konfigurieren
  Sie müssen einen oder mehrere Speicherarchivclient-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.

Windows-Betriebssysteme

Speicherarchivmanager-Server konfigurieren

Sie müssen den Speicherarchivmanager-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.

Vorgehensweise

Die folgende Beispielprozedur zeigt, wie ein IBM Spectrum Protect-Server mit dem Namen ASTRO als Speicherarchivmanager konfiguriert wird:

1. Stellen Sie sicher, dass der Speicherarchivmanager-Server aktiv ist:
   a. Starten Sie die Windows-Diensteverwaltungskonsole (services.msc).
   b. Wählen Sie den Dienst aus, beispielsweise `TSM Server1`.
   c. Wenn der Dienst nicht aktiv ist, klicken Sie mit der rechten Maustaste auf den Namen des Dienstes und wählen Sie Starten aus.
2. Rufen Sie die Speicherarchiv- und Laufwerkdaten für die gemeinsam genutzte Speicherarchiveinheit ab:
   a. Führen Sie das Dienstprogramm `tsmdlst.exe` aus. Das Dienstprogramm befindet sich im Verzeichnis \Programme\Tivoli\TSM\server.
3. Definieren Sie ein Speicherarchiv mit dem Speicherarchivtyp SCSI. Beispiel:

   ```
   define library sangroup libtype=scsi shared=yes
   ```

   In diesem Beispiel wird die Standardeinstellung für die Seriennummer des Speicherarchivs verwendet, gemäß der der Server die Seriennummer vom Speicherarchiv selbst abruft, wenn der Pfad definiert wird. Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

4. Definieren Sie den Pfad vom Server zum Speicherarchiv.

   ```
   define path astro sangroup srctype=server desttype=library
    device=lb0.0.0.2
   ```

   Wenn die Seriennummer beim Definieren des Speicherarchivs nicht eingeschlossen wurde, fragt der Server das Speicherarchiv jetzt ab, um diese Informationen abzurufen. Wenn die Seriennummer beim Definieren des Speicherarchivs eingeschlossen wurde, überprüft der Server die Definition und gibt eine Nachricht aus, wenn eine Übereinstimmung vorliegt.

5. Definieren Sie die Laufwerke im Speicherarchiv.

   ```
   define drive sangroup drivea
   define drive sangroup driveb
   ```

   In diesem Beispiel wird die Standardeinstellung für die Seriennummer des Laufwerks verwendet, gemäß der der Server die Seriennummer vom Laufwerk selbst abruft, wenn der Pfad definiert wird. Abhängig vom Leistungsspektrum des Laufwerks kann der Server die Seriennummer möglicherweise nicht automatisch erkennen. In diesem Fall zeichnet der Server keine Seriennummer für die Einheit auf und kann die Identität der Einheit nicht bestätigen, wenn Sie den Pfad definieren oder wenn der Server die Einheit verwendet.

   In diesem Beispiel wird auch die Standardeinstellung für die Elementadresse des Laufwerks verwendet, gemäß der der Server die Elementnummer vom Laufwerk selbst abruft, wenn der Pfad definiert wird.

   Die Elementadresse ist eine Zahl, die die physische Position eines Laufwerks in einem automatisierten Speicherarchiv angibt. Der Server benötigt die Elementadresse, um die physische Position des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Der Server kann

die Elementnummer vom Laufwerk selbst abrufen, wenn der Pfad definiert wird, oder Sie können die Elementnummer angeben, wenn Sie das Laufwerk definieren.

Abhängig vom Leistungsspektrum des Speicherarchivs kann der Server die Elementadresse möglicherweise nicht automatisch erkennen. In diesem Fall müssen Sie die Elementadresse angeben, wenn Sie das Laufwerk definieren. Elementnummern für viele Speicherarchive sind unter IBM® Support Portal for IBM Spectrum Protect verfügbar.

6. Definieren Sie den Pfad vom Server zu jedem der Laufwerke.

```
define path astro drivea srctype=server desttype=drive library=sangroup
 device=mt0.1.0.2
define path astro driveb srctype=server desttype=drive library=sangroup
 device=mt0.2.0.2
```

Wenn die Seriennummer oder Elementadresse beim Definieren des Laufwerks nicht eingeschlossen wurde, fragt der Server das Laufwerk oder Speicherarchiv jetzt ab, um diese Informationen abzurufen.

7. Definieren Sie mindestens eine Einheitenklasse.

```
define devclass tape devtype=dlt library=sangroup
```

8. Stellen Sie den Speicherarchivbestand zurück. Bei dem folgenden Beispiel werden alle Datenträger als Arbeitsdatenträger in den Speicherarchivbestand zurückgestellt. Der Server verwendet den Namen auf dem Barcodeetikett als den Datenträgernamen.

```
checkin libvolume sangroup search=yes status=scratch
 checklabel=barcode
```

9. Konfigurieren Sie einen Speicherpool mit maximal 50 Arbeitsdatenträgern für das gemeinsam genutzte Speicherarchiv.

```
define stgpool backtape tape
 description='Speicherpool für gemeinsam genutztes Speicherarchiv sangroup' maxscratch=50
```

Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
DEFINE DEVCLASS (Einheitenklasse definieren)
DEFINE DRIVE (Laufwerk für ein Speicherarchiv definieren)
DEFINE LIBRARY (Speicherarchiv definieren)
DEFINE PATH (Pfad definieren)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)
Windows-Betriebssysteme

Speicherarchivclient-Server konfigurieren

Sie müssen einen oder mehrere Speicherarchivclient-Server konfigurieren, um die IBM Spectrum Protect-Server für die gemeinsame Nutzung von Einheiten, die über ein SAN verbunden sind, konfigurieren zu können.

Vorbereitende Schritte

Stellen Sie sicher, dass ein Speicherarchivmanager-Server definiert ist.

Informationen zu diesem Vorgang

Sie müssen den Speicherarchivmanager-Server definieren. Die folgende Beispielprozedur zeigt, wie ein IBM Spectrum Protect-Server mit dem Namen JUDY als Speicherarchivclient konfiguriert wird.

Vorgehensweise

1. Stellen Sie sicher, dass der Speicherarchivmanager-Server aktiv ist:
   a. Starten Sie die Windows-Diensteverwaltungskonsole (services.msc).
   b. Wählen Sie den Dienst aus, beispielsweise `TSM Server1`.
   c. Wenn der Dienst nicht aktiv ist, klicken Sie mit der rechten Maustaste und wählen Sie Starten aus.
2. Rufen Sie die Speicherarchiv- und Laufwerkdaten für die gemeinsam genutzte Speicherarchiveinheit ab:
   a. Führen Sie das Dienstprogramm `tsmdlst.exe` aus. Das Dienstprogramm befindet sich im Verzeichnis \Programme\Tivoli\TSM\server.
3. Definieren Sie das gemeinsam genutzte Speicherarchiv SANGROUP und geben Sie den Speicherarchivmanager an. Stellen Sie sicher, dass der Speicherarchivname mit dem Speicherarchivnamen auf dem Speicherarchivmanager übereinstimmt.

```
define library sangroup libtype=shared primarylibmanager=astro
```

4. Definieren Sie die Pfade vom Speicherarchivclient-Server zu jedem der Laufwerke, indem Sie Befehle auf dem Verwaltungsclient ausgeben:

```
define path judy drivea srctype=server desttype=drive library=sangroup
 device=mt0.1.0.3
 define path judy driveb srctype=server desttype=drive library=sangroup
 device=mt0.2.0.3
```

5. Definieren Sie mindestens eine Einheitenklasse, indem Sie Befehle auf dem Speicherarchivclient ausgeben:

   ```
   define devclass tape devtype=dlt mountretention=1 mountwait=10
   library=sangroup
   ```

   Definieren Sie die Parameter für die Einheitenklasse auf dem Speicherarchivclient mit denselben Werten wie auf dem Speicherarchivmanager. Es ist zwar sinnvoll, auf beiden Servern identische Einheitenklassennamen zu verwenden, dies ist jedoch nicht erforderlich.

   Die Einheitenklassenparameter, die auf dem Speicherarchivmanager-Server angegeben sind, überschreiben die für den Speicherarchivclient angegebenen Parameter. Dies gilt unabhängig davon, ob die Einheitenklassennamen auf beiden Servern identisch sind. Wenn die Einheitenklassennamen unterschiedlich sind, verwendet der Speicherarchivmanager die Parameter, die in einer Einheitenklasse angegeben sind, die mit dem für den Speicherarchivclient angegebenen Einheitentyp übereinstimmt.

   Wenn ein Speicherarchivclient eine andere Einstellung als die in der Einheitenklasse des Speicherarchivmanagers angegebene Einstellung (beispielsweise ein anderes Mountlimit) erfordert, führen Sie die folgenden Schritte aus:

   a. Erstellen Sie auf dem Speicherarchivmanager-Server eine zusätzliche Einheitenklasse. Geben Sie die Parametereinstellungen an, die der Speicherarchivclient verwenden soll.
   b. Erstellen Sie auf dem Speicherarchivclient eine Einheitenklasse mit demselben Namen und Einheitentyp wie die neue Einheitenklasse, die Sie auf dem Speicherarchivserver erstellt haben.

6. Definieren Sie den Speicherpool BACKTAPE, der das gemeinsam genutzte Speicherarchiv verwenden wird:

   ```
   define stgpool backtape tape
   description='Speicherpool für gemeinsam genutztes Speicherarchiv sangroup' maxscratch=50
   ```

7. Wiederholen Sie diese Prozedur, um weitere Server als Speicherarchivclients zu definieren.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
DEFINE LIBRARY (Speicherarchiv definieren)
DEFINE PATH (Pfad definieren)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Speicherpoolhierarchie konfigurieren

Im Rahmen des Implementierungsprozesses müssen Sie eine Speicherpoolhierarchie konfigurieren. Konfigurieren Sie mindestens einen primären Speicherpool auf Platte und einen primären Speicherpool auf Band. Stellen Sie sicher, dass Daten täglich von Platte auf Band umgelagert werden.

Vorbereitende Schritte

1. Stellen Sie sicher, dass Sie die Informationen in Planung der Speicherpoolhierarchie gelesen haben.
2. Stellen Sie sicher, dass die entsprechenden Regeln, die auch als *Maßnahmen* bezeichnet werden, zum Sichern von Clientdaten angegeben sind. Führen Sie die Anweisungen in Regeln zum Sichern und Archivieren von Clientdaten angeben aus.
3. Stellen Sie sicher, dass jedem Knoten eine Maßnahme zugeordnet ist. Anweisungen zum Zuordnen einer Maßnahme beim Registrieren eines Knotens finden Sie in Clients registrieren.

Vorgehensweise

Um eine Speicherpoolhierarchie zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Definieren Sie einen primären Speicherpool für die Bandeinheit, indem Sie den Befehl DEFINE STGPOOL ausgeben.

   Definieren Sie beispielsweise einen primären Speicherpool mit dem Namen TAPE1 mit der Einheitenklasse LTO und aktivieren Sie die Grupppenkollokation. Legen Sie die maximale Anzahl Arbeitsdatenträger, die der Server für diesen Speicherpool anfordern kann, mit 999 fest. Geben Sie den folgenden Befehl aus:

   ```
   define stgpool tape1 lto pooltype=primary collocate=group
   maxscratch=999
   ```

2. Definieren Sie die Laufwerke, Pfade, und Speicherarchive für den primären Speicherpool auf Band. Führen Sie die Anweisungen in Bandeinheiten definieren aus.
3. Definieren Sie einen primären Speicherpool für die Platteneinheit, indem Sie den Befehl DEFINE STGPOOL ausgeben.

   Definieren Sie beispielsweise einen Speicherpool mit dem Namen DISK1 mit der Einheitenklasse FILE. Stellen Sie sicher, dass Daten in den Bandspeicherpool TAPE1 umgelagert werden können, verhindern Sie jedoch die automatische Umlagerung, indem Sie 100 für den

Parameter HIGHMIG und 0 für den Parameter LOWMIG angeben. Verhindern Sie die Konsolidierung, indem Sie 100 für den Parameter RECLAIM angeben. Aktivieren Sie die Knotenkollokation. Legen Sie die maximale Anzahl Arbeitsdatenträger, die der Server für diesen Speicherpool anfordern kann, mit 9999 fest. Geben Sie mithilfe des Parameters MIGPROCESS die Anzahl Umlagerungsprozesse an. Der Wert des Parameters MIGPROCESS sollte der Anzahl Laufwerke in dem Speicherarchiv minus der Anzahl Laufwerke, die für Zurückschreibungsoperationen reserviert sind, entsprechen. Geben Sie den folgenden Befehl aus:

```
define stgpool disk1 file pooltype=primary nextstgpool=tape1
highmig=100 lowmig=0 reclaim=100 collocate=node maxscratch=9999 migprocess=5
```

Weitere Informationen zum Konfigurieren der Umlagerung von Platte auf Band finden Sie in Plattenspeicherpools umlagern.

Nächste Schritte

Eine Speicherpoolhierarchie umfasst nur primäre Speicherpools. Nachdem Sie die Speicherpoolhierarchie konfiguriert haben, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Kopienspeicherpool auf einer Bandeinheit. Anweisungen finden Sie in DEFINE STGPOOL (Kopienspeicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet ist).
2. Sichern Sie den bandbasierten primären Speicherpool im Kopienspeicherpool mithilfe des Befehls BACKUP STGPOOL. Anweisungen finden Sie in BACKUP STGPOOL (Daten in primären Speicherpools in einem Kopienspeicherpool sichern).
3. Um sicherzustellen, dass Daten in einem Katastrophenfall wiederhergestellt werden können, definieren Sie eine Prozedur zum Versetzen von Banddatenträgern aus dem Kopienspeicherpool an einen anderen Standort. Anweisungen finden Sie in Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM.

Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Anwendungen, virtuelle Maschinen und Systeme schützen

Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können.

- Clients hinzufügen
  Installieren und konfigurieren Sie im Anschluss an die erfolgreiche Konfiguration Ihres IBM Spectrum Protect-Servers die Client-Software, um mit dem Sichern von Daten beginnen zu können.

LAN-unabhängige Datenversetzung konfigurieren

Sie können den IBM Spectrum Protect-Client und -Server so konfigurieren, dass der Client seine Daten über einen Speicheragenten direkt in Speicher in einem SAN versetzen kann. Diese Funktion, die als LAN-unabhängige Datenversetzung bezeichnet wird, wird vom Produkt IBM Spectrum Protect for SAN bereitgestellt.

Vorgehensweise

Um die LAN-unabhängige Datenversetzung zu konfigurieren, führen Sie die folgenden Schritte aus. Ausführliche Informationen finden Sie in der Dokumentation für IBM Spectrum Protect for SAN.

1. Überprüfen Sie die Netzverbindung.
2. Richten Sie die Kommunikation zwischen dem Client, dem Speicheragenten und dem Server ein.
3. Installieren und konfigurieren Sie die Software auf Clientsystemen.
4. Konfigurieren Sie Einheiten auf dem Server für den Zugriff durch den Speicheragenten.
5. Konfigurieren Sie IBM Spectrum Protect-Maßnahmen für die LAN-unabhängige Datenversetzung für den Client.
6. Wenn Sie gemeinsam genutzten Speicher des Typs FILE verwenden, installieren und konfigurieren Sie IBM® TotalStorage SAN File System oder IBM Spectrum Scale.
   Windows-BetriebssystemeEinschränkung: Wenn ein IBM Spectrum Scale-Datenträger von einem AIX-Server formatiert wird, verwendet das Windows-System TCP/IP und nicht das Speicherbereichsnetz für die Übertragung von Daten.
7. Definieren Sie Pfade vom Speicheragenten zu Laufwerken.
8. Starten Sie den Speicheragenten und überprüfen Sie die LAN-unabhängige Konfiguration.

Nächste Schritte

Zur Optimierung Ihrer LAN- und SAN-Ressourcennutzung können Sie den Pfad steuern, über den Datenübertragungen für Clients mit der Fähigkeit zur LAN-unabhängigen Datenversetzung erfolgen. Steuern Sie den Pfad mithilfe des Befehls UPDATE NODE. Für jeden Client können Sie für Lese- und Schreiboperationen für Daten eine der folgenden Einstellungen auswählen. Geben Sie Operationen zum Lesen von Daten mit dem Parameter DATAREADPATH und Operationen zum Schreiben von Daten mit dem Parameter DATAWRITEPATH an. Der Parameter ist optional. Der Standardwert ist ANY.

LAN (nur LAN-Pfad)
Geben Sie den Wert LAN an, wenn eine der folgenden Bedingungen erfüllt ist:

- Es soll ein kleines Datenvolumen gesichert oder zurückgeschrieben werden.
- Der Client verfügt nicht über SAN-Konnektivität.

LANFREE (nur LAN-unabhängiger Pfad)
: Geben Sie den Wert LANFREE an, wenn sich der Client und der Server in demselben SAN befinden und eine der folgenden Bedingungen erfüllt ist

  - Es soll ein großes Datenvolumen gesichert oder zurückgeschrieben werden.
  - Die Serververarbeitungslast soll auf den Client verlagert werden.
  - Das LAN soll entlastet werden.

ANY (jeder beliebige verfügbare Pfad)
: Ein LAN-unabhängiger Pfad wird verwendet, sofern ein derartiger Pfad verfügbar ist. Wenn kein LAN-unabhängiger Pfad verfügbar ist, werden die Daten über das LAN übertragen.

- LAN-unabhängige Konfiguration prüfen
  Nach der Konfiguration eines IBM Spectrum Protect-Clients für die LAN-unabhängige Datenversetzung können Sie die Konfiguration und die Serverdefinitionen mithilfe des Befehls VALIDATE LANFREE prüfen.

Verschlüsselungsverfahren für Bänder

Die Entscheidung über das zu verwendende Verschlüsselungsverfahren ist davon abhängig, wie Ihre Daten verwaltet werden sollen.

Es ist wichtig, Clientdaten zu schützen, insbesondere dann, wenn diese Daten sensibel sind. Mithilfe von IBM Bandverschlüsselungstechnologie kann sichergestellt werden, dass Daten auf Datenträgern vor Ort und an einem anderen Standort geschützt sind.

IBM Bandtechnologie unterstützt verschiedene Verfahren der Laufwerkverschlüsselung für die folgenden Einheiten:

- IBM 3592 Generation 2 und Generation 3
- IBM Linear Tape-Open (LTO) Generation 4 und Generation 5

Die Verfahren der Laufwerkverschlüsselung, die Sie mit IBM Spectrum Protect verwenden können, werden auf der Hardwareebene konfiguriert. IBM Spectrum Protect kann nicht steuern oder ändern, welches Verschlüsselungsverfahren in der Hardwarekonfiguration verwendet wird. Wenn die Hardware für das Anwendungsverfahren konfiguriert ist, kann IBM Spectrum Protect die Verschlüsselung abhängig vom Wert für DRIVEENCRYPTION für die Einheitenklasse aktivieren oder inaktivieren.

Um alle Daten in einem bestimmten logischen Speicherarchiv zu verschlüsseln oder Daten auf mehr als nur Speicherpooldatenträgern zu verschlüsseln, verwenden Sie die das Speicherarchiv- oder Systemverfahren. Wenn der Verschlüsselungsschlüsselmanager für die gemeinsame Nutzung von Schlüsseln konfiguriert ist, können die Speicherarchiv- und Systemverfahren den Verschlüsselungsschlüssel gemeinsam nutzen, was den gegenseitigen Austausch der beiden Verfahren ermöglicht. IBM Spectrum Protect kann Verschlüsselungsschlüssel zwischen dem Anwendungsverfahren und dem Speicherarchiv- oder dem Systemverschlüsselungsverfahren nicht gemeinsam nutzen oder verwenden.

Tabelle 1. Verschlüsselungsverfahren

Verschlüsselungsverfahren	Beschreibung

Verschlüsselungsverfahren	Beschreibung
Anwendungsverschlüsselung	Bei der anwendungsverwalteten Verschlüsselung, können Sie dedizierte Speicherpools erstellen, die nur verschlüsselte Datenträger enthalten. Auf diese Weise können Sie Speicherpoolhierarchien und Maßnahmen verwenden, um zu steuern, wie die Daten verschlüsselt werden. Verschlüsselungsschlüssel werden von der Anwendung verwaltet, in diesem Fall von IBM Spectrum Protect. IBM Spectrum Protect generiert und speichert die Schlüssel in der Serverdatenbank. Daten werden während der Ausführung von Schreiboperationen verschlüsselt, wenn der Verschlüsselungsschlüssel vom Server an das Laufwerk übergeben wird. Daten werden für Leseoperation entschlüsselt. Um Speicherpooldatenträger zu verschlüsseln und einen Teil der Verschlüsselungsverarbeitung auf Ihrem System zu eliminieren, aktivieren Sie das Anwendungsverfahren. Verwenden Sie die anwendungsverwaltete Verschlüsselung nur für Speicherpooldatenträger. Andere Datenträger, wie beispielsweise Bänder mit Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger, werden nicht mithilfe des Anwendungsverfahrens verschlüsselt. Voraussetzung: Wenn die Anwendungsverschlüsselung aktiviert ist, müssen Sie beim Schützen von Datenbanksicherungen besonders vorsichtig vorgehen, da die Verschlüsselungsschlüssel zum Verschlüsseln und Entschlüsseln von Daten in der Serverdatenbank gespeichert sind. Um Ihre Daten zurückschreiben zu können, müssen Sie über die korrekte Datenbanksicherung und die zugehörigen Verschlüsselungsschlüssel verfügen, um auf Ihre Informationen zugreifen zu können. Stellen Sie sicher, dass die Datenbank häufig gesichert wird, und schützen Sie die Sicherungen, um Datenverlust oder Diebstahl zu verhindern. Jeder, der sowohl Zugriff auf die Datenbanksicherung als auch auf die Verschlüsselungsschlüssel hat, hat Zugriff auf Ihre Daten.
Speicherarchivverschlüsselung	Bei der speicherarchivverwalteten Verschlüsselung können Sie steuern, welche Datenträger unter Verwendung ihrer Seriennummern verschlüsselt werden. Sie können einen Bereich oder eine Gruppe von Datenträgern angeben, die verschlüsselt werden sollen. Verschlüsselungsschlüssel werden vom Speicherarchiv verwaltet. Schlüssel sind in einem Verschlüsselungsschlüsselmanager gespeichert und werden dem Laufwerk zur Verfügung gestellt. Wenn Sie die Hardware für die Verwendung der speicherarchivverwalteten Verschlüsselung konfigurieren, können Sie dieses Verfahren verwenden, indem Sie den Befehl DEFINE DEVCLASS unter Angabe des Parameters DRIVEENCRYPTION=ALLOW ausgeben. Einschränkung: Die Verschlüsselung mit IBM LTO-4 und späteren Generationen wird nur von bestimmten IBM Speicherarchiven unterstützt. Ausführliche Informationen finden Sie in Bandlaufwerkverschlüsselung konfigurieren.
Systemverschlüsselung	Die systemverwaltete Verschlüsselung ist nur unter dem Betriebssystem AIX® verfügbar. Verschlüsselungsschlüssel, die dem Laufwerk zur Verfügung gestellt werden, werden vom Einheitentreiber oder Betriebssystem verwaltet und in einem Verschlüsselungsschlüsselmanager gespeichert. Wenn die Hardware für die Verwendung der Systemverschlüsselung konfiguriert ist, können Sie dieses Verfahren verwenden, indem Sie den Befehl DEFINE DEVCLASS unter Angabe des Parameters DRIVEENCRYPTION=ALLOW ausgeben.

Um festzustellen, ob ein Datenträger verschlüsselt ist und welches Verfahren verwendet wurde, geben Sie den Befehl QUERY VOLUME unter Angabe des Parameters FORMAT=DETAILED aus.

- Bandlaufwerkverschlüsselung konfigurieren
  Mithilfe der Laufwerkverschlüsselung können Sie Bänder schützen, die kritische oder sensible Daten enthalten, wie beispielsweise Bänder

mit vertraulichen Finanzdaten. Die Laufwerkverschlüsselung kann hilfreich sein, wenn Sie Bänder aus der IBM Spectrum Protect-Serverumgebung an einen Standort vor Ort oder an einen anderen Standort versetzen.

Bandspeicheroperationen steuern

Einheitenklassendefinitionen für Bänder umfassen Parameter, die Ihnen die Steuerung von Speicheroperationen ermöglichen.

- Wie Datenträger von IBM Spectrum Protect gefüllt werden
  Der Befehl DEFINE DEVCLASS hat einen optionalen Parameter ESTCAPACITY, der die geschätzte Kapazität sequenzieller Datenträger angibt, die der Einheitenklasse zugeordnet sind. IBM Spectrum Protect bestimmt mithilfe der geschätzten Kapazität von Datenträgern die geschätzte Kapazität eines Speicherpools sowie die geschätzte Auslastung in Prozent.
- Geschätzte Kapazität von Banddatenträgern angeben
  IBM Spectrum Protect bestimmt anhand der geschätzten Kapazität außerdem, wann die Konsolidierung von Speicherpooldatenträgern beginnen soll.
- Aufzeichnungsformate für Banddatenträger angeben
  Sie können das Aufzeichnungsformat angeben, das von IBM Spectrum Protect zum Schreiben von Daten auf Banddatenträger verwendet wird. Wenn Sie planen, Generationen von Laufwerken oder unterschiedliche Laufwerktypen in einem Speicherarchiv zu mischen, müssen Sie für jede Laufwerkgeneration und jeden Laufwerktyp ein Aufzeichnungsformat angeben. Auf diese Weise kann der Server zwischen den einzelnen Laufwerkgenerationen und Laufwerktypen unterscheiden.
- Speicherarchivobjekte Einheitenklassen zuordnen
  Ein Speicherarchiv enthält die Laufwerke, die zum Bereitstellen des Datenträgers verwendet werden können. Einer Einheitenklasse kann nur ein einziges Speicherarchiv zugeordnet werden. Mehrere Einheitenklassen können jedoch dasselbe Speicherarchiv referenzieren.
- Datenträgermountoperationen für Bandeinheiten steuern
  Mithilfe von Einheitenklassendefinitionen können Sie die Anzahl bereitgestellter Datenträger, die Zeit, die ein Datenträger bereitgestellt bleibt, und die Zeit, die der IBM Spectrum Protect-Server auf ein verfügbares Laufwerk wartet, steuern.
- Operationen zurückstellen
  Der Server kann Server- oder Clientoperationen für eine Operation mit höherer Priorität zurückstellen, wenn ein Mountpunkt im Gebrauch ist und keine anderen Mountpunkte verfügbar sind oder der Zugriff auf einen bestimmten Datenträger erforderlich ist. Wenn eine Operation zurückgestellt wird, wird sie abgebrochen.
- Auswirkungen von Einheitenänderungen im SAN
  Die SAN-Umgebung kann sich aufgrund von Änderungen an den Einheiten oder an der Verkabelung dramatisch ändern. Aufgrund der dynamischen Natur des SAN können statische Definitionen fehlschlagen oder unvorhersehbar werden.
- Windows-BetriebssystemeEinheitendaten anzeigen
  Mithilfe des Dienstprogramms für Einheitendaten (tsmdlst) können Sie Informationen zu Einheiten anzeigen, die mit dem Server verbunden sind.
- WORM-Banddatenträger
  WORM-Datenträger können als Schutz vor dem versehentlichen oder absichtlichen Löschen kritischer Daten verwendet werden. In IBM Spectrum Protect gibt es jedoch bestimmte Einschränkungen und Richtlinien, die bei der Verwendung von WORM-Datenträgern zu beachten sind.
- Windows-BetriebssystemeEinheitenfehler beheben
  Sie können Fehler beheben, die bei der Konfiguration oder Verwendung von Einheiten mit IBM Spectrum Protect auftreten.

Wie Datenträger von IBM Spectrum Protect gefüllt werden

Der Befehl DEFINE DEVCLASS hat einen optionalen Parameter ESTCAPACITY, der die geschätzte Kapazität sequenzieller Datenträger angibt, die der Einheitenklasse zugeordnet sind. IBM Spectrum Protect bestimmt mithilfe der geschätzten Kapazität von Datenträgern die geschätzte Kapazität eines Speicherpools sowie die geschätzte Auslastung in Prozent.

Wenn der Parameter ESTCAPACITY nicht angegeben wird, verwendet IBM Spectrum Protect einen Standardwert, der auf dem Aufzeichnungsformat basiert, das für die Einheitenklasse unter Verwendung des Parameters FORMAT angegeben wird.

Wenn Sie eine geschätzte Kapazität angeben, die die tatsächliche Kapazität des Datenträgers in der Einheitenklasse überschreitet, aktualisiert IBM Spectrum Protect die geschätzte Kapazität des Datenträgers, wenn der Datenträger voll wird. Wenn IBM Spectrum Protect das Ende des Datenträgers erreicht, wird die Kapazität in Übereinstimmung mit dem Datenvolumen, das auf den Datenträger geschrieben wurde, aktualisiert.

Sie können den Standardwert für die geschätzte Kapazität für die Einheitenklasse akzeptieren oder explizit eine geschätzte Kapazität angeben. Ein genauer Wert für die geschätzte Kapazität ist nicht erforderlich, aber nützlich. IBM Spectrum Protect bestimmt mithilfe der geschätzten Kapazität von Datenträgern die geschätzte Kapazität eines Speicherpools sowie die geschätzte Auslastung in Prozent. Unter Umständen möchten Sie die geschätzte Kapazität ändern, wenn eine oder beide der folgenden Bedingungen erfüllt sind:

- Der Standardwert für die geschätzte Kapazität ist aufgrund der Datenkomprimierung ungenau.
- Es sind Datenträger vorhanden, deren Größe vom Standard abweicht.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Geschätzte Kapazität von Banddatenträgern angeben

IBM Spectrum Protect bestimmt anhand der geschätzten Kapazität außerdem, wann die Konsolidierung von Speicherpooldatenträgern beginnen soll.

Informationen zu diesem Vorgang

Bei Bandeinheitenklassen sind die vom Server ausgewählten Standardwerte von dem Aufzeichnungsformat abhängig, mit dem Daten auf den Datenträger geschrieben werden. Sie können entweder den Standardwert für einen Einheitentyp akzeptieren oder einen Wert angeben.

Um die geschätzte Kapazität für Banddatenträger anzugeben, verwenden Sie den Parameter ESTCAPACITY, wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Aufzeichnungsformate für Banddatenträger angeben

Sie können das Aufzeichnungsformat angeben, das von IBM Spectrum Protect zum Schreiben von Daten auf Banddatenträger verwendet wird. Wenn Sie planen, Generationen von Laufwerken oder unterschiedliche Laufwerktypen in einem Speicherarchiv zu mischen, müssen Sie für jede Laufwerkgeneration und jeden Laufwerktyp ein Aufzeichnungsformat angeben. Auf diese Weise kann der Server zwischen den einzelnen Laufwerkgenerationen und Laufwerktypen unterscheiden.

Informationen zu diesem Vorgang

Um ein Aufzeichnungsformat anzugeben, verwenden Sie den Parameter FORMAT, wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren.

Wenn alle Laufwerke, die dieser Einheitenklasse zugeordnet sind, identisch sind, geben Sie FORMAT=DRIVE an. Der Server wählt das höchste Format aus, das von dem Laufwerk unterstützt wird, in dem ein Datenträger bereitgestellt wird.

Wenn einige der Laufwerke, die der Einheitenklasse zugeordnet sind, ein Format mit höherer Speicherdichte als andere unterstützen, geben Sie ein Format an, das mit allen Laufwerken kompatibel ist.

Wenn Laufwerke in einem einzelnen SCSI-Speicherarchiv verschiedene Bandtechnologien (beispielsweise DLT und LTO Ultrium) verwenden, geben Sie einen eindeutigen Wert für den Parameter FORMAT in jeder Einheitenklassendefinition an.

Ein Konfigurationsbeispiel befindet sich in Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren.

Das Aufzeichnungsformat, das der Server für einen Datenträger verwendet, wird ausgewählt, wenn zum ersten Mal Daten auf den Datenträger geschrieben werden. Eine Aktualisierung des Parameters FORMAT wirkt sich auf Datenträger, die bereits Daten enthalten, erst dann aus, wenn diese Datenträger ab dem Anfang neu beschrieben werden. Dies kann nach dem Konsolidieren oder Löschen eines Datenträgers oder nach dem Verfall aller Daten auf dem Datenträger der Fall sein.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Speicherarchivobjekte Einheitenklassen zuordnen

Ein Speicherarchiv enthält die Laufwerke, die zum Bereitstellen des Datenträgers verwendet werden können. Einer Einheitenklasse kann nur ein einziges Speicherarchiv zugeordnet werden. Mehrere Einheitenklassen können jedoch dasselbe Speicherarchiv referenzieren.

Informationen zu diesem Vorgang

Um eine Einheitenklasse einem Speicherarchiv zuzuordnen, verwenden Sie den Parameter LIBRARY wenn Sie eine Einheitenklasse definieren oder ihre Definition aktualisieren.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Datenträgermountoperationen für Bandeinheiten steuern

Mithilfe von Einheitenklassendefinitionen können Sie die Anzahl bereitgestellter Datenträger, die Zeit, die ein Datenträger bereitgestellt bleibt, und die Zeit, die der IBM Spectrum Protect-Server auf ein verfügbares Laufwerk wartet, steuern.

- Anzahl gleichzeitig bereitgestellter Datenträger steuern
  Wenn Sie ein Mountlimit für eine Einheitenklasse festlegen, müssen Sie die Anzahl Speichereinheiten berücksichtigen, die mit Ihrem System verbunden sind. Außerdem müssen Sie berücksichtigen, ob die Funktion für gleichzeitiges Schreiben verwendet wird und ob mehrere Einheitenklassen einem einzelnen Speicherarchiv zugeordnet werden; darüber hinaus müssen Sie die Anzahl Prozesse berücksichtigen, die gleichzeitig ausgeführt werden.
- Steuern, wie lange ein Datenträger bereitgestellt bleibt
  Sie können steuern, wie lange ein bereitgestellter Datenträger nach seiner letzten E/A-Aktivität bereitgestellt bleiben soll. Wenn ein Datenträger häufig verwendet wird, können Sie die Leistung verbessern, indem Sie einen längeren Mount-Aufbewahrungszeitraum definieren, um unnötige Operationen zum Bereitstellen und Aufheben der Bereitstellung zu vermeiden.
- Zeit steuern, die der Server auf ein Laufwerk wartet
  Sie können die Höchstdauer in Minuten angeben, die der IBM Spectrum Protect-Server für die aktuelle Mountanforderung auf ein verfügbares Laufwerk wartet.

Anzahl gleichzeitig bereitgestellter Datenträger steuern

Wenn Sie ein Mountlimit für eine Einheitenklasse festlegen, müssen Sie die Anzahl Speichereinheiten berücksichtigen, die mit Ihrem System verbunden sind. Außerdem müssen Sie berücksichtigen, ob die Funktion für gleichzeitiges Schreiben verwendet wird und ob mehrere Einheitenklassen einem einzelnen Speicherarchiv zugeordnet werden; darüber hinaus müssen Sie die Anzahl Prozesse berücksichtigen, die gleichzeitig ausgeführt werden.

Informationen zu diesem Vorgang

Wenn Sie ein Mountlimit für eine Einheitenklasse auswählen, müssen Sie Folgendes berücksichtigen:

- Wie viele Speichereinheiten sind an Ihr System angeschlossen?

  Geben Sie keinen Wert für das Mountlimit an, der größer als die Anzahl zugeordneter, verfügbarer Laufwerke in Ihrer Installation ist. Wenn der Server versucht, die durch das Mountlimit angegebene Anzahl Datenträger bereitzustellen und keine Laufwerke für den erforderlichen Datenträger verfügbar sind, tritt ein Fehler auf und Clientsitzungen werden möglicherweise beendet. (Diese Einschränkung gilt nicht, wenn der Parameter DRIVES angegeben wird.)

  Wenn Speicherarchivressourcen in einem SAN von IBM Spectrum Protect-Servern gemeinsam genutzt werden, müssen Sie die Anzahl Bandlaufwerke, die ein Speicherarchivclient gleichzeitig nutzen kann, begrenzen. Um mehreren Speicherarchivclient-Servern die gleichzeitige Verwendung eines Speicherarchivs zu ermöglichen, geben Sie den Parameter MOUNTLIMIT an, wenn Sie die Einheitenklasse auf dem Speicherarchivclient definieren oder aktualisieren. Weitere Informationen zum Konfigurieren der gemeinsamen Speicherarchivnutzung finden Sie in Gemeinsame Speicherarchivnutzung konfigurieren.

- Verwenden Sie die Funktion für gleichzeitiges Schreiben für primäre Speicherpools, Kopienspeicherpools und Pools für aktive Daten?

  Geben Sie einen Wert für das Mountlimit an, mit dem genügend Mountpunkte bereitstellt werden, um das gleichzeitige Schreiben von Daten in den primären Speicherpool und in alle zugehörigen Kopienspeicherpools und Pools für aktive Daten zu unterstützen.

- Ordnen Sie mehrere Einheitenklassen einem einzigen Speicherarchiv zu?

  Eine Einheitenklasse, die einem Speicherarchiv zugeordnet ist, kann jedes Laufwerk in dem Speicherarchiv verwenden, das mit dem Einheitentyp der Einheitenklasse kompatibel ist. Da Sie einem Speicherarchiv mehrere Einheitenklassen zuordnen können, kann ein einzelnes Laufwerk im Speicherarchiv von mehreren Einheitenklassen verwendet werden. IBM Spectrum Protect stellt sicher, dass zwei Operationen nicht gleichzeitig dasselbe Laufwerk mit zwei unterschiedliche Einheitenklassen verwenden können.

- Wie viele IBM Spectrum Protect-Prozesse sollen unter Verwendung der Einheiten in dieser Einheitenklasse gleichzeitig ausgeführt werden?

  IBM Spectrum Protect bricht einige Prozesse automatisch ab, um andere Prozesse mit höherer Priorität auszuführen. Wenn der Server alle verfügbaren Laufwerke in einer Einheitenklasse zur Ausführung von Prozessen mit höherer Priorität verwendet, müssen Prozesse mit niedriger Priorität warten, bis ein Laufwerk verfügbar wird. IBM Spectrum Protect bricht beispielsweise den Prozess für einen Client ab, der Daten direkt auf Band sichert, wenn das Laufwerk für einen Servermigrations- oder Bandkonsolidierungsprozess benötigt wird. IBM Spectrum Protect bricht einen Bandkonsolidierungsprozess ab, wenn das Laufwerk für eine Clientzurückschreibungsoperation benötigt wird. Weitere Informationen finden Sie in Operationen zurückstellen.

  Wenn Prozesse häufig durch andere Prozesse abgebrochen werden, überlegen Sie, ob IBM Spectrum Protect mehr Laufwerke zur Verfügung gestellt werden können. Überprüfen Sie andernfalls die Planung von Operationen, um Laufwerkkonflikte zu reduzieren.

  Diese Überlegungen gelten auch für die Funktion für gleichzeitiges Schreiben. Es müssen genügend Laufwerke verfügbar sein, um eine Operation für gleichzeitiges Schreiben erfolgreich ausführen zu können.

  Um die maximale Anzahl Datenträger anzugeben, die gleichzeitig bereitgestellt werden können, verwenden Sie den Parameter MOUNTLIMIT wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Steuern, wie lange ein Datenträger bereitgestellt bleibt

Sie können steuern, wie lange ein bereitgestellter Datenträger nach seiner letzten E/A-Aktivität bereitgestellt bleiben soll. Wenn ein Datenträger häufig verwendet wird, können Sie die Leistung verbessern, indem Sie einen längeren Mount-Aufbewahrungszeitraum definieren, um unnötige Operationen zum Bereitstellen und Aufheben der Bereitstellung zu vermeiden.

Informationen zu diesem Vorgang

Wenn Mountoperationen durch manuelle Bedieneraktivitäten ausgeführt werden, möchten Sie möglicherweise einen langen Mount-Aufbewahrungszeitraum angeben. Wenn beispielsweise der gesamte Betrieb an einem Wochenende durch nur einen einzigen Bediener unterstützt wird, definieren Sie einen langen Mount-Aufbewahrungszeitraum, damit der Bediener nicht ständig zur Bereitstellung von Datenträgern aufgefordert wird.

Um zu steuern, wie lange ein bereitgestellter Datenträger bereitgestellt bleiben soll, verwenden Sie den Parameter MOUNTRETENTION, wenn Sie die Einheitenklasse definieren oder ihre Definition aktualisieren. Wenn der Wert für den Mount-Aufbewahrungszeitraum beispielsweise 60 ist und ein bereitgestellter Datenträger 60 Minuten lang inaktiv ist, wird seine Bereitstellung vom Server aufgehoben.

Solange ein Datenträger für IBM Spectrum Protect bereitgestellt ist, ist das Laufwerk IBM Spectrum Protect zugeordnet und kann nicht anderweitig verwendet werden. Wenn das Laufwerk für andere Verwendungszwecke freigegeben werden muss, können Sie IBM Spectrum Protect-Operationen, die das Laufwerk verwenden, abbrechen und dann die Bereitstellung des Datenträgers aufheben. Sie können beispielsweise Servermigrations- oder -sicherungsoperationen abbrechen. Informationen zum Abbrechen von Prozessen und zum Aufheben der Bereitstellung von Datenträgern finden Sie in Serveranforderungen für Datenträger verwalten.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Zeit steuern, die der Server auf ein Laufwerk wartet

Sie können die Höchstdauer in Minuten angeben, die der IBM Spectrum Protect-Server für die aktuelle Mountanforderung auf ein verfügbares Laufwerk wartet.

Informationen zu diesem Vorgang

Um zu steuern, wie lange gewartet werden soll, bis ein Laufwerk für eine Mountanforderung verfügbar wird, verwenden Sie den Parameter MOUNTWAIT, wenn Sie eine Einheitenklasse definieren oder aktualisieren.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Operationen zurückstellen

Der Server kann Server- oder Clientoperationen für eine Operation mit höherer Priorität zurückstellen, wenn ein Mountpunkt im Gebrauch ist und keine anderen Mountpunkte verfügbar sind oder der Zugriff auf einen bestimmten Datenträger erforderlich ist. Wenn eine Operation zurückgestellt wird, wird sie abgebrochen.

Mit dem Befehl QUERY MOUNT können Sie den Status des Datenträgers für den Mountpunkt anzeigen.

Standardmäßig ist die Zurückstellung auf dem Server aktiviert. Um die Zurückstellung zu inaktivieren, geben Sie NOPREEMPT in der Serveroptionsdatei an. Wenn Sie diese Option angeben, sind der Befehl BACKUP DB und die Export- und Importbefehle die einzigen Operationen, durch die andere Operationen zurückgestellt werden können.

- Zurückstellung von Operationen für einen Mountpunkt
  Wenn eine Operation mit hoher Priorität einen Mountpunkt in einer bestimmten Einheitenklasse erfordert und alle Mountpunkte in der Einheitenklasse im Gebrauch sind, kann ein Mountpunkt einer Operation mit niedrigerer Priorität durch die Operation mit hoher Priorität zurückgestellt werden.
- Zurückstellung des Datenträgerzugriffs
  Wenn eine Operation mit hoher Priorität Zugriff auf einen bestimmten Datenträger erfordert und dieser Datenträger im Gebrauch ist, kann die Operation mit niedrigerer Priorität für diesen Datenträger durch die Operation mit hoher Priorität zurückgestellt werden.

Zugehörige Verweise:
BACKUP DB (Datenbank sichern)
QUERY MOUNT (Informationen zu bereitgestellten Datenträgern mit sequenziellem Zugriff anzeigen)

Zurückstellung von Operationen für einen Mountpunkt

Wenn eine Operation mit hoher Priorität einen Mountpunkt in einer bestimmten Einheitenklasse erfordert und alle Mountpunkte in der Einheitenklasse im Gebrauch sind, kann ein Mountpunkt einer Operation mit niedrigerer Priorität durch die Operation mit hoher Priorität zurückgestellt werden.

Mountpunkte können nur zurückgestellt werden, wenn die Einheitenklasse der Operation, die die Zurückstellung ausführt, mit der Einheitenklasse der Operation, die zurückgestellt wird, übereinstimmt.

Die folgenden Operationen mit hoher Priorität können eine Zurückstellung anderer Operationen für einen Mountpunkt bewirken.

- Datenbanksicherungsoperationen
- Abruf-, Zurückschreibungs- oder HSM-Rückrufoperationen, die von Clients eingeleitet werden
- Zurückschreibungsoperationen mithilfe einer fernen Einheit zum Versetzen von Daten
- Exportoperationen
- Importoperationen
- Operationen zum Generieren von Sicherungsgruppen

Die folgenden Serveroperationen können keine Zurückstellung anderer Operationen bewirken bzw. nicht durch andere Operationen zurückgestellt werden:

- Prüfen eines Datenträgers
- Zurückschreiben von Daten aus einem Kopienspeicherpool oder einem Pool für aktive Daten
- Vorbereiten einer Wiederherstellungsplandatei
- Speichern von Daten mithilfe einer fernen Einheit zum Versetzen von Daten

Die folgenden Operationen können zurückgestellt werden und sind in der Reihenfolge von der höchsten zur niedrigsten Priorität aufgelistet. Der Server wählt die Operation mit der niedrigsten Priorität, beispielsweise die Identifikation doppelter Daten, für die Zurückstellung aus.

- Replizieren von Knoten
- Sichern von Daten in einem Kopienspeicherpool
- Kopieren aktiver Daten in einen Pool für aktive Daten
- Versetzen von Daten auf einen Speicherpooldatenträger
- Umlagern von Daten von Platte auf sequenzielle Datenträger
- Umlagern von Daten von sequenziellen Datenträgern auf sequenzielle Datenträger
- Sicherungs-, Archivierungs- oder HSM-Umlagerungsoperationen, die von Clients eingeleitet werden
- Konsolidieren von Datenträgern in einem Speicherpool mit sequenziellem Zugriff
- Identifizieren doppelter Daten

Zurückstellung des Datenträgerzugriffs

Wenn eine Operation mit hoher Priorität Zugriff auf einen bestimmten Datenträger erfordert und dieser Datenträger im Gebrauch ist, kann die Operation mit niedrigerer Priorität für diesen Datenträger durch die Operation mit hoher Priorität zurückgestellt werden.

Wenn beispielsweise eine Zurückschreibungsanforderung Zugriff auf einen Datenträger erfordert, der von einer Konsolidierungsoperation verwendet wird, und ein Laufwerk verfügbar ist, wird die Konsolidierungsoperation abgebrochen.

Die folgenden Operationen mit hoher Priorität können eine Zurückstellung von Operationen für den Zugriff auf einen bestimmten Datenträger bewirken:

- Datenbanksicherungsoperationen
- Abruf-, Zurückschreibungs- oder HSM-Rückrufoperationen, die von Clients eingeleitet werden
- Zurückschreibungsoperationen mithilfe einer fernen Einheit zum Versetzen von Daten
- Exportoperationen
- Importoperationen
- Operationen zum Generieren von Sicherungsgruppen

Die folgenden Operationen können keine Zurückstellung anderer Operationen bewirken bzw. nicht durch andere Operationen zurückgestellt werden:

- Prüfen eines Datenträgers
- Zurückschreiben von Daten aus einem Kopienspeicherpool oder einem Pool für aktive Daten
- Vorbereiten eines Wiederherstellungsplans
- Speichern von Daten mithilfe einer fernen Einheit zum Versetzen von Daten

Die folgenden Operationen können zurückgestellt werden und sind in der Reihenfolge von der höchsten zur niedrigsten Priorität aufgelistet. Der Server wählt die Operation mit der niedrigsten Priorität, beispielsweise die Identifikation doppelter Daten, für die Zurückstellung aus.

- Replizieren von Knoten
- Sichern von Daten in einem Kopienspeicherpool
- Kopieren aktiver Daten in einen Pool für aktive Daten
- Versetzen von Daten auf einen Speicherpooldatenträger
- Umlagern von Daten von Platte auf sequenzielle Datenträger

- Umlagern von Daten von sequenziellen Datenträgern auf sequenzielle Datenträger
- Sicherungs-, Archivierungs- oder HSM-Umlagerungsoperationen, die vom Client eingeleitet werden
- Konsolidieren von Datenträgern in einem Speicherpool mit sequenziellem Zugriff
- Identifizieren doppelter Daten

Auswirkungen von Einheitenänderungen im SAN

Die SAN-Umgebung kann sich aufgrund von Änderungen an den Einheiten oder an der Verkabelung dramatisch ändern. Aufgrund der dynamischen Natur des SAN können statische Definitionen fehlschlagen oder unvorhersehbar werden.

Einheiten-IDs, die vom SAN zugeordnet werden und dem Server oder Speicheragenten bekannt sind, können sich aufgrund von Buszurücksetzungen oder aufgrund anderer Umgebungsänderungen ändern. Beispielsweise kann dem Server eine Einheit X auf der Basis der ursprünglichen Pfadspezifikation für den Server und der ursprünglichen Konfiguration des LAN als *rmt0* (unter AIX) bekannt sein. Ein Ereignis im SAN, beispielsweise das Hinzufügen der neuen Einheit Y, führt jedoch dazu, dass der Einheit X die ID *rmt1* zugeordnet wird. Wenn der Server versucht, auf Einheit X unter Verwendung von *rmt0* zuzugreifen, schlägt der Zugriff fehl oder der Zugriff erfolgt auf die falsche Zieleinheit. Der Server versucht, die Wiederherstellung nach Änderungen an Einheiten im SAN durch Verwendung von Seriennummern auszuführen, um die Identität der Einheiten, auf die er zugreift, zu bestätigen.

Wenn Sie ein Laufwerk oder Speicherarchiv definieren, können Sie wahlweise die Seriennummer für diese Einheit angeben. Wenn Sie die Seriennummer bei der Definition der Einheiten nicht angeben, ruft der Server die Seriennummer ab, wenn Sie den Pfad für die Einheit definieren. In beiden Fällen wird die Einheitenseriennummer in der Datenbank des Servers gespeichert und kann zum Bestätigen der Identität einer Einheit für Operationen verwendet werden.

Wenn der Server Laufwerke und Speicherarchive in einem SAN verwendet, versucht der Server zu überprüfen, ob die korrekte Einheit verwendet wird. Der Server kontaktiert die Einheit unter Verwendung des Einheitennamens in dem von Ihnen für die Einheit definierten Pfad. Anschließend fordert der Server die Seriennummer von der Einheit an und vergleicht diese Seriennummer mit der Seriennummer, die für diese Einheit in der Serverdatenbank gespeichert ist.

Wenn die Seriennummern nicht übereinstimmen, startet der Server den Erkennungsprozess im SAN und versucht, die Einheit mit der übereinstimmenden Seriennummer zu finden. Wenn der Server die Einheit mit der übereinstimmenden Seriennummer findet, korrigiert er die Definition des Pfads in der Serverdatenbank, indem er den Einheitennamen in diesem Pfad aktualisiert. Der Server gibt eine Nachricht mit Informationen zu der an der Einheit durchgeführten Änderung aus. Anschließend wird die Einheit vom Server verwendet.

Um festzustellen, wann sich Einheitenänderungen im SAN auf den IBM Spectrum Protect-Server auswirken, können Sie das Aktivitätenprotokoll auf Nachrichten überwachen. Die folgenden Nachrichten betreffen Seriennummern:

- ANR8952 bis ANR8958
- ANR8961 bis ANR8968
- ANR8974 bis ANR8975

Einschränkung: Einige Einheiten können ihre Seriennummern nicht an Anwendungen wie den IBM Spectrum Protect-Server melden. Wenn der Server die Seriennummer einer Einheit nicht abrufen kann, kann der Server das System nicht bei der Wiederherstellung nach der Änderung einer Einheitenposition im SAN unterstützen.
Windows-Betriebssysteme

Einheitendaten anzeigen

Mithilfe des Dienstprogramms für Einheitendaten (tsmdlst) können Sie Informationen zu Einheiten anzeigen, die mit dem Server verbunden sind.

Vorbereitende Schritte

- Stellen Sie sicher, dass die HBA-API installiert ist. Die HBA-API ist erforderlich, um das Dienstprogramm für Einheitendaten auszuführen.
- Stellen Sie sicher, dass der Bandeinheitentreiber installiert und konfiguriert ist.

Vorgehensweise

1. Wechseln Sie über eine Eingabeaufforderung in das Unterverzeichnis `server` im Serverinstallationsverzeichnis, beispielsweise C:\Programme\Tivoli\TSM\server.
2. Führen Sie die ausführbare Datei tsmdlst.exe aus.

Zugehörige Verweise:
QUERY SAN (Einheiten im SAN abfragen)
tsmdlst (Informationen zu Einheiten anzeigen)

WORM-Banddatenträger

WORM-Datenträger können als Schutz vor dem versehentlichen oder absichtlichen Löschen kritischer Daten verwendet werden. In IBM Spectrum Protect gibt es jedoch bestimmte Einschränkungen und Richtlinien, die bei der Verwendung von WORM-Datenträgern zu beachten sind.

Die folgenden Typen von WORM-Datenträgern können mit IBM Spectrum Protect verwendet werden:

- IBM® 3592, alle unterstützten Generationen
- IBM LTO-3 und alle unterstützten Generationen
- HP LTO-3 und alle unterstützten Generationen
- Quantum LTO-3 und alle unterstützten Generationen
- Quantum SDLT 600, Quantum DLT V4 und Quantum DLT S4
- StorageTek VolSafe
- Sony AIT50 und AIT100

Tipps:

- Ein Speicherpool kann entweder aus WORM-Datenträgern oder aus RW-Datenträgern bestehen, aber nicht aus Datenträgern beider Typen.
- Um die Verschwendung von Bändern nach einer Zurückschreibungs- oder Importoperation zu verhindern, verwenden Sie keine WORM-Bänder für Datenbanksicherungs- oder Exportoperationen.

- WORM-fähige Laufwerke
  Um WORM-Datenträger in einem Speicherarchiv verwenden zu können, müssen alle Laufwerke in dem Speicherarchiv WORM-fähig sein. Ein Mount schlägt fehl, wenn eine WORM-Kassette in einem Laufwerk mit Schreib-/Lesezugriff (RW-Laufwerk) bereitgestellt wird.
- WORM-Datenträger zurückstellen
  Der Typ des WORM-Datenträgers legt fest, ob der Datenträgerkennsatz beim Zurückstellen gelesen werden muss.
- Einschränkungen für WORM-Datenträger
  Sie können keine WORM-Datenträger, denen vorab Kennsätze zugeordnet wurden, mit der Einheitenklasse LTO oder ECARTRIDGE verwenden.
- Mountfehler bei WORM-Datenträgern
  Wenn WORM-Banddatenträger für einen Mount mit einer Einheitenklasse mit Schreib-/Lesezugriff (RW) in ein Laufwerk geladen werden, hat dies einen Mountfehler zur Folge. Dementsprechend hat, wenn RW-Banddatenträger für einen Mount mit einer Einheitenklasse WORM in ein Laufwerk geladen werden, dies ebenfalls das Fehlschlagen des Mounts zur Folge.
- WORM-Datenträgern neue Kennsätze zuordnen
  Einer WORM-Kassette kann kein neuer Kennsatz zugeordnet werden, wenn sie Daten enthält. Dies gilt für Sony AIT WORM-, LTO WORM-, SDLT WORM-, DLT WORM- und IBM 3592-Kassetten. Der Kennsatz auf einem VolSafe-Datenträger sollte nur einmal überschrieben werden und sollte nur überschrieben werden, wenn der Datenträger keine verwendbaren, gelöschten oder verfallenen Daten enthält.
- Private WORM-Datenträger aus einem Speicherarchiv entfernen
  Wenn Sie eine Aktion für einen WORM-Datenträger ausführen (wenn Sie beispielsweise Dateibereiche löschen) und der Server den Datenträger nicht als voll markiert, wird der Datenträger in den Arbeitsstatus zurückversetzt. Wenn ein WORM-Datenträger nicht als voll markiert wird und aus einem Speicherpool gelöscht wird, bleibt der Datenträger ein privater Datenträger. Um einen privaten WORM-Datenträger aus einem Speicherarchiv zu entfernen, müssen Sie den Befehl CHECKOUT LIBVOLUME ausgeben.
- Erstellung von DLT WORM-Datenträgern
  DLT WORM-Datenträger können aus Datenträgern mit Schreib-/Lesezugriff (RW-Datenträgern) erstellt werden, indem sie konvertiert werden.
- Unterstützung für kurze und normale 3592 WORM-Bänder
  IBM Spectrum Protect unterstützt sowohl kurze als auch normale 3592 WORM-Bänder. Die besten Ergebnisse werden erzielt, wenn Sie die Bänder in separaten Speicherpools definieren.
- Einheitenklasse nach der Einstellung des Parameters WORM abfragen
  Sie können die Einstellung des Parameters WORM für eine Einheitenklasse mithilfe des Befehls QUERY DEVCLASS bestimmen. Die Ausgabe enthält ein Feld mit der Bezeichnung WORM und einen Wert (YES oder NO).

WORM-fähige Laufwerke

Um WORM-Datenträger in einem Speicherarchiv verwenden zu können, müssen alle Laufwerke in dem Speicherarchiv WORM-fähig sein. Ein Mount schlägt fehl, wenn eine WORM-Kassette in einem Laufwerk mit Schreib-/Lesezugriff (RW-Laufwerk) bereitgestellt wird.

Ein WORM-fähiges Laufwerk kann jedoch als RW-Laufwerk verwendet werden, wenn der Parameter WORM in der Einheitenklasse auf NO gesetzt wird. Jeder Typ von Speicherarchiv kann sowohl über WORM- als auch über RW-Datenträger verfügen, wenn *alle* Laufwerke für WORM aktiviert sind. Die einzige Ausnahme von dieser Regel sind NAS-Speicherarchive, in denen WORM-Banddatenträger nicht verwendet werden können.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

WORM-Datenträger zurückstellen

Der Typ des WORM-Datenträgers legt fest, ob der Datenträgerkennsatz beim Zurückstellen gelesen werden muss.

Speicherarchivwechsler können nicht zwischen standardmäßigen Banddatenträgern mit Schreib-/Lesezugriff (RW-Banddatenträgern) und den folgenden Typen von WORM-Banddatenträgern unterscheiden:

- VolSafe
- Sony AIT

- LTO
- SDLT
- DLT

Um den Typ des WORM-Datenträgers zu bestimmen, der verwendet wird, muss ein Datenträger in ein Laufwerk geladen werden. Daher müssen Sie beim Zurückstellen einer dieser Typen von WORM-Datenträgern die Option CHECKLABEL=YES im Befehl CHECKIN LIBVOLUME verwenden.

Wenn Speicherarchivwechsler IBM® 3592 Unterstützung für WORM-Datenträger zur Verfügung stellen, können diese Speicherarchivwechsler feststellen, ob ein Datenträger ein WORM-Datenträger ist, ohne den Datenträger in ein Laufwerk laden zu müssen. Die Angabe von CHECKLABEL=YES ist nicht erforderlich. Prüfen Sie mit Ihren Hardwareanbietern, ob Ihre 3592-Laufwerke und -Speicherarchive die erforderliche Unterstützung zur Verfügung stellen.

Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Einschränkungen für WORM-Datenträger

Sie können keine WORM-Datenträger, denen vorab Kennsätze zugeordnet wurden, mit der Einheitenklasse LTO oder ECARTRIDGE verwenden.

Wenn IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung angegeben ist, können Sie für die folgenden Laufwerke keine WORM-Datenträger verwenden:

- IBM® LTO-5, LTO-6 und später
- HP LTO-5, LTO-6 und später
- Oracle StorageTek T10000B
- Oracle StorageTek T10000C
- Oracle StorageTek T10000D

Mountfehler bei WORM-Datenträgern

Wenn WORM-Banddatenträger für einen Mount mit einer Einheitenklasse mit Schreib-/Lesezugriff (RW) in ein Laufwerk geladen werden, hat dies einen Mountfehler zur Folge. Dementsprechend hat, wenn RW-Banddatenträger für einen Mount mit einer Einheitenklasse WORM in ein Laufwerk geladen werden, dies ebenfalls das Fehlschlagen des Mounts zur Folge.

WORM-Datenträgern neue Kennsätze zuordnen

Einer WORM-Kassette kann kein neuer Kennsatz zugeordnet werden, wenn sie Daten enthält. Dies gilt für Sony AIT WORM-, LTO WORM-, SDLT WORM-, DLT WORM- und IBM® 3592-Kassetten. Der Kennsatz auf einem VolSafe-Datenträger sollte nur einmal überschrieben werden und sollte nur überschrieben werden, wenn der Datenträger keine verwendbaren, gelöschten oder verfallenen Daten enthält.

Geben Sie den Befehl LABEL LIBVOLUME nur einmal für VolSafe-Datenträger aus. Um zu verhindern, dass der Kennsatz überschrieben wird, können Sie die Option OVERWRITE=NO im Befehl LABEL LIBVOLUME verwenden.

Zugehörige Verweise:
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

Private WORM-Datenträger aus einem Speicherarchiv entfernen

Wenn Sie eine Aktion für einen WORM-Datenträger ausführen (wenn Sie beispielsweise Dateibereiche löschen) und der Server den Datenträger nicht als voll markiert, wird der Datenträger in den Arbeitsstatus zurückversetzt. Wenn ein WORM-Datenträger nicht als voll markiert wird und aus einem Speicherpool gelöscht wird, bleibt der Datenträger ein privater Datenträger. Um einen privaten WORM-Datenträger aus einem Speicherarchiv zu entfernen, müssen Sie den Befehl CHECKOUT LIBVOLUME ausgeben.

Zugehörige Verweise:
CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)

Erstellung von DLT WORM-Datenträgern

DLT WORM-Datenträger können aus Datenträgern mit Schreib-/Lesezugriff (RW-Datenträgern) erstellt werden, indem sie konvertiert werden.

Wenn SDLT-600-, DLT-V4- oder DLT-S4-Laufwerke vorhanden sind und diese für WORM-Datenträger aktiviert werden sollen, führen Sie für die Laufwerke unter Verwendung von V30 oder einer späteren Firmware, die von Quantum verfügbar ist, ein Upgrade durch. Sie können auch DLTIce-Software verwenden, um unformatierte RW-Datenträger oder leere Datenträger in WORM-Datenträger zu konvertieren.

In SCSI-Speicherarchiven erstellt der IBM Spectrum Protect-Server automatisch DLT WORM-Arbeitsdatenträger, wenn der Server keine WORM-Arbeitsdatenträger im Bestand eines Speicherarchivs finden kann. Der Server konvertiert verfügbare unformatierte oder leere RW-

Arbeitsdatenträger oder leere private RW-Datenträger in WORM-Arbeitsdatenträger. Der Server schreibt auch die Kennsätze auf neu erstellten WORM-Datenträgern neu, indem die Kennsatzinformationen auf den vorhandenen RW-Datenträgern verwendet werden.

Unterstützung für kurze und normale 3592 WORM-Bänder

IBM Spectrum Protect unterstützt sowohl kurze als auch normale 3592 WORM-Bänder. Die besten Ergebnisse werden erzielt, wenn Sie die Bänder in separaten Speicherpools definieren.

Einheitenklasse nach der Einstellung des Parameters WORM abfragen

Sie können die Einstellung des Parameters WORM für eine Einheitenklasse mithilfe des Befehls QUERY DEVCLASS bestimmen. Die Ausgabe enthält ein Feld mit der Bezeichnung WORM und einen Wert (YES oder NO).

Zugehörige Verweise:
QUERY DEVCLASS (Informationen zu einer oder mehreren Einheitenklassen anzeigen)
Windows-Betriebssysteme

Einheitenfehler beheben

Sie können Fehler beheben, die bei der Konfiguration oder Verwendung von Einheiten mit IBM Spectrum Protect auftreten.

Informationen zu diesem Vorgang

Verwenden Sie Tabelle 1, um eine Lösung für den einheitenbezogenen Fehler zu finden.

Tabelle 1. Behebung von Einheitenfehlern

Symptom	Problem	Lösung
Konflikte mit anderen Anwendungen	IBM Spectrum Protect erfordert für die gemeinsame Nutzung von Einheiten ein Speicherbereichsnetz.	Konfigurieren Sie ein Speicherbereichsnetz. Achtung: Wenn mehrere IBM Spectrum Protect-Server dieselbe Einheit verwenden, kann dies zu einem Datenverlust führen. Definieren oder verwenden Sie eine Einheit nur für einen einzigen IBM Spectrum Protect-Server. AIX-Betriebssysteme Linux-BetriebssystemeAndere Anwendungen können auf IBM Spectrum Protect-Einheiten unter Verwendung eines SCSI-Bandtreibers zugreifen.
Fehlschlagen der Zuordnung von Kennsätzen	Eine Einheit kann nicht zum Zuordnen von Kennsätzen zu Datenträgern verwendet werden, wenn der Server die Einheit gleichzeitig für andere Prozesse verwendet.	Sie können vorhandene Datenträger in einem Speicherpool nicht überschreiben. Sie müssen alle Hardwareprobleme lösen, bevor Sie einem Datenträger einen Kennsatz zuordnen können.
	Falsche oder unvollständige Lizenzregistrierung	Registrieren Sie die Lizenz für die gekaufte Einheitenunterstützung.
Konflikte zwischen Einheitentreibern	IBM Spectrum Protect gibt Nachrichten zu E/A-Fehlern aus, wenn Sie eine Einheit mit sequenziellem Zugriff definieren oder verwenden.	Bei Windows-Einheitentreibern und von anderen Anwendungen bereitgestellten Treibern können Konflikte mit dem IBM Spectrum Protect-Einheitentreiber auftreten, wenn der IBM Spectrum Protect-Treiber nicht zuerst gestartet wird. Um die Reihenfolge zu überprüfen, in der die Einheitentreiber vom System gestartet werden, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf Systemsteuerung. 2. Klicken Sie auf Geräte. Einheitentreiber und ihre Starttypen werden aufgelistet.

Symptom	Problem	Lösung
E/A-Fehler	Wenn Sie versuchen, eine Bandeinheit zu definieren oder zu verwenden, können Konflikte mit Einheitentreibern auftreten. Bei Windows-Einheitentreibern und von anderen Anwendungen bereitgestellten Treibern können Konflikte mit dem IBM Spectrum Protect-Einheitentreiber auftreten, wenn dieser nicht zuerst gestartet wird.	

Implementierung abschließen

Nachdem die IBM Spectrum Protect- Lösung konfiguriert wurde und aktiv ist, testen Sie Sicherungsoperationen und konfigurieren Sie die Überwachung, um sicherzustellen, dass alles ordnungsgemäß funktioniert.

Vorgehensweise

1. Testen Sie Sicherungsoperationen, um sicherzustellen, dass Ihre Daten wie erwartet geschützt werden.
    a. Wählen Sie auf der Seite Clients im Operations Center die Clients aus, die gesichert werden sollen, und klicken Sie auf Sichern.
    b. Wählen Sie auf der Seite Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Datenbank sichern aus.
    c. Überprüfen Sie, ob die Sicherungsoperationen erfolgreich ohne Warnungen oder Fehlernachrichten ausgeführt wurden.
    Tipp: Sie können auch stattdessen die GUI des Clients für Sichern/Archivieren zum Sichern von Clientdaten verwenden und die Serverdatenbank sichern, indem Sie den Befehl BACKUP DB in einer Verwaltungsbefehlszeile ausgeben.
2. Konfigurieren Sie die Überwachung für Ihre Lösung, indem Sie die Anweisungen in Bandspeicherlösung überwachen ausführen.

Bandspeicherlösung überwachen

Überwachen Sie nach der Implementierung einer bandbasierten Lösung in IBM Spectrum Protect die Lösung, um ihre korrekte Funktionsweise sicherzustellen. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.

Informationen zu diesem Vorgang

Die Überwachung einer Lösung erfolgt bevorzugt über die Verwendung des Operations Center, das den Gesamtsystemstatus und den detaillierten Systemstatus in einer grafischen Benutzerschnittstelle bereitstellt. Darüber hinaus können Sie das Operations Center zum Generieren von E-Mail-Berichten zur Zusammenfassung des Systemstatus konfigurieren.

Vorgehensweise

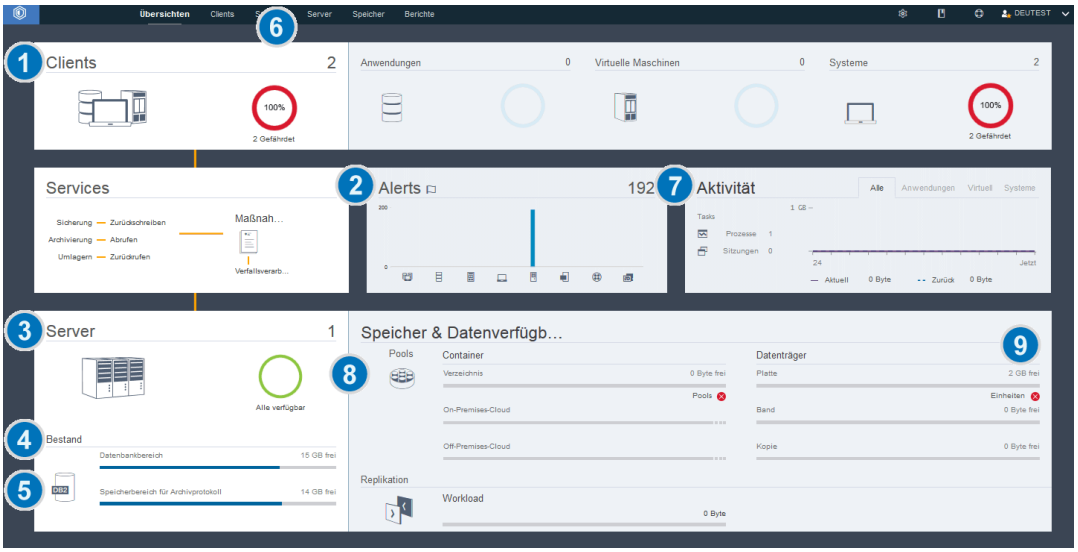
1. Führen Sie tägliche Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für tägliche Überwachungstasks.
2. Führen Sie regelmäßige Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für regelmäßige Überwachungstasks.
3. Überprüfen Sie, ob Ihr System die Lizenzierungsanforderungen erfüllt. Anweisungen finden Sie in Lizenzeinhaltung überprüfen.
4. Optional: Konfigurieren Sie E-Mail-Berichte des Systemstatus. Anweisungen finden Sie in Systemstatus mithilfe von E-Mail-Berichten verfolgen.

Prüfliste für tägliche Überwachungstasks

Um sicherzustellen, dass die täglichen Überwachungstasks für Ihre IBM Spectrum Protect-Lösung ausgeführt werden, überprüfen Sie die Prüfliste für tägliche Überwachungstasks.

Führen Sie die täglichen Überwachungstasks über die Seite Übersicht im Operations Center aus. Sie können auf die Seite Übersicht zugreifen, indem Sie das Operations Center öffnen und auf Übersichten klicken.

Die folgende Abbildung zeigt die Position zur Ausführung der jeweiligen Task.



Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder.

In der folgenden Tabelle sind die täglichen Überwachungstasks sowie Anweisungen zur Ausführung jeder Task aufgeführt.

Tabelle 1. Tägliche Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
1 Bestimmen Sie, ob Clients vorhanden sind, bei denen die Gefahr besteht, dass sie aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen ungeschützt sind.	Um zu überprüfen, ob Clients gefährdet sind, suchen Sie nach einem Hinweis Gefährdet. Um Details anzuzeigen, klicken Sie auf den Bereich 'Clients'. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie die Clientfehler- und -planungsprotokolle anzeigen, indem Sie die folgenden Schritte ausführen: 1. Wählen Sie in der Tabelle 'Clients' den Client aus und klicken Sie auf Details. 2. Um ein Problem zu diagnostizieren, klicken Sie auf Diagnose.	Greifen Sie bei Clients, für die der Clientverwaltungsservice nicht installiert ist, auf das Clientsystem zu, um die Clientfehlerprotokolle zu überprüfen.
2 Bestimmen Sie, ob clientbezogene oder serverbezogene Fehler einen Bedienereingriff erfordern.	Um die Bewertung jedes zurückgemeldeten Alerts zu bestimmen, bewegen Sie den Mauszeiger im Bereich 'Alerts' über die Spalten.	Um zusätzliche Informationen zu Alerts anzuzeigen, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Alerts'. 2. Wählen Sie in der Tabelle 'Alerts' einen Alert aus. 3. Überprüfen Sie die Nachrichten im Fenster 'Aktivitätenprotokoll'. In dem Fenster werden zugehörige Nachrichten angezeigt, die vor und nach dem Auftreten des ausgewählten Alerts ausgegeben wurden.
3 Bestimmen Sie, ob die vom Operations Center verwalteten Server verfügbar sind, um Datenschutzservices für Clients bereitzustellen.	1. Um zu überprüfen, ob Server gefährdet sind, suchen Sie im Bereich 'Server' nach einem Hinweis Nicht verfügbar. 2. Um zusätzliche Informationen anzuzeigen, klicken Sie auf den Bereich 'Server'. 3. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.	Tipp: Wenn Sie ein Problem erkennen, das sich auf die Servermerkmale bezieht, aktualisieren Sie die Servermerkmale: 1. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details. 2. Um die Servermerkmale zu aktualisieren, klicken Sie auf Merkmale.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
4 Bestimmen Sie, ob für den Serverbestand, der aus der Serverdatenbank, der aktiven Protokolldatei und dem Archivprotokoll besteht, genügend Speicherbereich verfügbar ist.	1. Klicken Sie auf den Bereich 'Server'. 2. Zeigen Sie in der Spalte 'Status' der Tabelle den Status des Servers an und beheben Sie alle Probleme: ○ Normal Für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll ist genügend Speicherbereich verfügbar. ○ Kritisch Für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll ist nicht genügend Speicherbereich verfügbar. Sie müssen unverzüglich Speicherbereich hinzufügen; andernfalls werden die vom Server bereitgestellten Datenschutzservices unterbrochen. ○ Warnung Der Der Speicherbereich für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll wird knapp. Wenn diese Bedingung bestehen bleibt, müssen Sie Speicherbereich hinzufügen. ○ Nicht verfügbar Der Status kann nicht abgerufen werden. Stellen Sie sicher, dass der Server aktiv ist und keine Netzprobleme vorliegen. Dieser Status wird auch angezeigt, wenn die Überwachungsadministrator-ID gesperrt ist oder aus anderen Gründen auf dem Server nicht verfügbar ist. Diese ID hat den Namen IBM-OC-Name_des_Hub-Servers. ○ Nicht überwacht Nicht überwachte Server sind für den Hub-Server definiert, aber nicht für die Verwaltung durch das Operations Center konfiguriert. Um einen nicht überwachten Server zu konfigurieren, wählen Sie den Server aus und klicken Sie auf Peripherieserver überwachen.	Sie können auch auf der Seite Alerts nach zugehörigen Alerts suchen. Weitere Anweisungen zur Fehlerbehebung finden Sie in Serverprobleme beheben.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
5 Überprüfen Sie Operationen zur Sicherung der Serverdatenbank.	Um zu bestimmen, ob ein Server kürzlich gesichert wurde, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Server'. 2. Überprüfen Sie in der Tabelle 'Server' die Spalte 'Letzte Datenbanksicherung'.	Um detaillierte Informationen zu Sicherungsoperationen abzurufen, führen Sie die folgenden Schritte aus: 1. Wählen Sie in der Tabelle 'Server' eine Zeile aus und klicken Sie auf Details. 2. Bewegen Sie im Bereich 'Datenbanksicherung' den Mauszeiger über die Häkchen, um Informationen zu Sicherungsoperation zu überprüfen. Wenn eine Datenbank nicht kürzlich (beispielsweise innerhalb der letzten 24 Stunden) gesichert wurde, können Sie eine Sicherungsoperation starten: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Server'. 2. Wählen Sie in der Tabelle einen Server aus und klicken Sie auf Sichern. Um zu bestimmen, ob die Serverdatenbank für automatische Sicherungsoperationen konfiguriert ist, führen Sie die folgenden Schritte aus: 1. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Geben Sie den Befehl QUERY DB aus: `query db f=d` 3. Überprüfen Sie in der Ausgabe das Feld `Einheitenklassenname für Gesamtsicherungen`. Wenn eine Einheitenklasse angegeben ist, ist der Server für automatische Datenbanksicherungen konfiguriert.
6 Überwachen Sie andere Serververwaltungstasks. Serververwaltungstasks können die Ausführung von Zeitplänen für Verwaltungsbefehle, Verwaltungsscripts und zugehörigen Befehlen umfassen.	Um nach Informationen zu Prozessen zu suchen, die aufgrund von Serverproblemen fehlgeschlagen sind, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf Server > Verwaltung. 2. Um das zwei Wochen umfassende Verlaufsprotokoll eines Prozesses abzurufen, zeigen Sie Spalte 'History' an. 3. Um weitere Informationen zu einem geplanten Prozess abzurufen, bewegen Sie den Mauszeiger über das Kontrollkästchen, das dem Prozess zugeordnet ist.	Weitere Informationen zum Überwachen von Prozessen und Beheben von Problemen, finden Sie in der Onlinehilfe des Operations Center.
7 Überprüfen Sie, ob das Datenvolumen, das kürzlich an Server bzw. von Servern gesendet wurde, innerhalb des erwarteten Bereichs liegt.	• Um eine Übersicht über die Aktivität der letzten 24 Stunden abzurufen, zeigen Sie den Bereich 'Aktivität' an. • Um die Aktivität der letzten 24 Stunden mit der Aktivität der vorherigen 24 Stunden zu vergleichen, studieren Sie die Zahlen in den Bereichen 'Aktuell' und 'Vorherig'.	• Wenn mehr Daten als erwartet an den Server gesendet wurden, bestimmen Sie die Clients, die mehr Daten sichern und ermitteln Sie die Ursache. Möglicherweise funktioniert die clientseitige Datendeduplizierung nicht ordnungsgemäß. • Wenn weniger Daten als erwartet an den Server gesendet wurden, überprüfen Sie, ob Clientsicherungsoperationen gemäß Zeitplan ausgeführt werden.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
8 Stellen Sie sicher, dass Speicherpools zum Sichern von Clientdaten verfügbar sind.	1. Wenn im Bereich 'Speicher & Datenverfügbarkeit' Probleme angezeigt werden, klicken Sie auf Pools, um die Details anzuzeigen: ○ Wenn der Status Kritisch angezeigt wird, ist in dem Speicherpool nicht genügend Speicherbereich verfügbar oder der Speicherpool hat den Zugriffsstatus UNAVAILABLE (Nicht verfügbar). ○ Wenn der Status Warnung angezeigt wird, wird der Speicherbereich für den Speicherpool knapp oder der Speicherpool hat den Zugriffsstatus READONLY (Lesezugriff). 2. Um den verwendeten Speicherbereich, den freien Speicherbereich und den Gesamtspeicherbereich für Ihren ausgewählten Speicherpool anzuzeigen, bewegen Sie den Mauszeiger über die Einträge in der Spalte 'Verwendete Kapazität'.	Um die Speicherpoolkapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie eine Zeile in der Tabelle 'Speicherpools' aus und klicken Sie auf Details.
9 Stellen Sie sicher, dass Speichereinheiten für Sicherungsoperationen verfügbar sind.	Überprüfen Sie im Bereich 'Speicher & Datenverfügbarkeit' im Abschnitt 'Datenträger' unterhalb der Balken für die Kapazität den Status, der neben Einheiten angegeben ist. Wenn der Status Kritisch oder Warnung für eine Einheit angezeigt wird, müssen Sie das Problem untersuchen. Um Details anzuzeigen, klicken Sie auf Einheiten.	Bandeinheiten können den Status 'Warnung' oder 'Kritisch' haben, wenn Laufwerke nicht verfügbar sind. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. Eine Bandeinheit kann auch den Status 'Kritisch' haben, wenn das Speicherarchiv offline ist. In anderen Spalten der Tabelle 'Bandeinheiten' wird der Status der automatischen Einheiten im Speicherarchivs, der Laufwerke und der Pfade angezeigt. Um Probleme mit Bandlaufwerken zu beheben, die einen kritischen Status haben, können Sie das Laufwerk offline schalten, wenn es für eine andere Aktivität, wie beispielsweise Wartung, verwendet werden muss. Um ein Laufwerk offline zu schalten, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite Speicher im Operations Center Bandeinheiten aus. 2. Um weitere Informationen zu einem Bandarchiv anzuzeigen, wählen Sie eine Zeile aus und klicken Sie auf Details. 3. Um ein Laufwerk offline zu schalten, wählen Sie das Bandlaufwerk aus und klicken Sie auf Offline. Stellen Sie bei Bandsicherungsoperationen sicher, dass genügend Arbeitsbänder verfügbar sind. Wenn Sie sich nicht sicher sind, ob die Anzahl verfügbarer Arbeitsbänder ausreichend ist, öffnen Sie das Notizbuch 'Details', um die Bandnutzung sowie eine Schätzung der Verfügbarkeit von Arbeitsbändern anzuzeigen. Um das Notizbuch 'Details' zu öffnen, wählen Sie in der Tabelle ein Speicherarchiv aus und klicken Sie auf 'Details'.

Prüfliste für regelmäßige Überwachungstasks

Um sicherzustellen, dass Operationen korrekt ausgeführt werden, führen Sie die Tasks in der Prüfliste für regelmäßige Überwachungstasks aus. Planen Sie regelmäßige Tasks häufig genug, sodass Sie potenzielle Probleme erkennen können, bevor diese wirklich problematisch werden.

Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen,

rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder.

Tabelle 1. Regelmäßige Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie die Systemleistung.	Bestimmen Sie den für Clientsicherungsoperationen erforderlichen Zeitraum: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Suchen Sie den Server, der dem Client zugeordnet ist. 2. Klicken Sie auf Server. Wählen Sie den Server aus und klicken Sie auf Details. 3. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die in den letzten 24 Stunden abgeschlossenen wurden, klicken Sie auf Abgeschlossene Tasks. 4. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die vor mehr als 24 Stunden abgeschlossen wurden, verwenden Sie den Befehl QUERY ACTLOG. Informationen zu diesem Befehl finden Sie in QUERY ACTLOG (Aktivitätenprotokoll abfragen). 5. Wenn die Dauer von Clientsicherungsoperationen zunimmt, ohne dass ein offensichtlicher Grund erkennbar ist, überprüfen Sie Ursache. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie Leistungsprobleme für den Client für Sichern/Archivieren diagnostizieren, indem Sie die folgenden Schritte ausführen: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. 2. Wählen Sie einen Client für Sichern/Archivieren aus und klicken Sie auf Details. 3. Um Clientprotokolle abzurufen, klicken Sie auf Diagnose.	Begrenzen Sie die Zeit für Clientsicherungsoperationen auf 8 bis 12 Stunden. Stellen Sie sicher, dass sich Clientzeitpläne nicht mit Serververwaltungstasks überschneiden. Anweisungen zur Reduzierung der Zeit, die der Client zum Sichern von Daten auf dem Server benötigt, finden Sie in Häufig auftretende Clientleistungsprobleme lösen. Suchen Sie nach Leistungsengpässen. Anweisungen finden Sie in Leistungsengpässe identifizieren. Informationen zur Identifikation und Behebung anderer Leistungsprobleme finden Sie in Leistung.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Stellen Sie sicher, dass aktuelle Sicherungsdateien für Einheitenkonfigurations- und Datenträgerprotokolldaten gesichert werden.	Greifen Sie auf Ihre Speicherpositionen zu, um sicherzustellen, dass die Dateien verfügbar sind. Die bevorzugte Methode ist die Sicherung der Dateien an zwei Positionen.
	Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, führen Sie die folgenden Schritte aus:
	1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder.
	2. Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, geben Sie die folgenden Befehle aus:
	`query option volhistory`
	`query option devconfig`
	3. Überprüfen Sie in der Ausgabe die Spalte 'Optionseinstellung', um die Dateipositionen zu finden.
	Wenn ein Katastrophenfall eintritt, sind sowohl die Protokolldatei für Datenträger als auch die Einheitenkonfigurationsdatei für die Zurückschreibung der Serverdatenbank erforderlich.	

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Bestimmen Sie, ob im Verzeichnis für die Serverinstanz genügend Speicherbereich verfügbar ist.	Stellen Sie sicher, dass im Verzeichnis für die Serverinstanz mindestens 50 GB freier Speicherbereich verfügbar ist. Führen Sie die für Ihr Betriebssystem zutreffende Aktion aus:
	• AIX-BetriebssystemeUm den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -g Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Linux-BetriebssystemeUm den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -h Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Windows-BetriebssystemeKlicken Sie in Windows Explorer mit der rechten Maustaste auf das Dateisystem und klicken Sie auf Eigenschaften. Zeigen Sie die Kapazitätsdaten an.
	Die bevorzugte Position des Instanzverzeichnisses ist von dem Betriebssystem abhängig, unter dem der Server installiert ist:
	• AIX-Betriebssysteme Linux-Betriebssysteme /home/tsminst1/tsminst1
	• Windows-Betriebssysteme C:\tsminst1
	Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.	

Ermitteln Sie nicht erwartete Clientaktivität.	Um im Rahmen der Überwachung der Clientaktivität zu bestimmen, ob das Datenvolumen das erwartete Volumen überschreitet, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Clients'. 2. Um die Aktivität der vergangen zwei Wochen anzuzeigen, doppelklicken Sie auf einen beliebigen Client. 3. Um die Anzahl Byte anzuzeigen, die an den Client gesendet wurden, klicken Sie auf die Registerkarte Merkmale. 4. Zeigen Sie im Bereich 'Letzte Sitzung' die Zeile 'An Client gesendet' an.	Wenn Sie auf einen Client in der Tabelle 'Clients' doppelklicken, wird im Bereich Aktivität im Lauf von 2 Wochen das Datenvolumen angezeigt, das vom Client jeden Tag an den Server gesendet wurde.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie das Speicherpoolwachstum im Laufe der Zeit.	1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Pools'. 2. Um die Kapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie einen Pool aus und klicken Sie auf Details.	Tipps: • Um die Zeit anzugeben, die verstreichen muss, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool oder einem Cloud-Containerspeicherpool entfernt werden, nachdem sie nicht mehr vom Bestand referenziert werden, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus. 2. Klicken Sie auf Details > Merkmale. 3. Geben Sie im Feld `Verzögerungszeitraum für Containerwiederverwendung` den Zeitraum an. • Bestimmen Sie die Datendeduplizierungsleistung für Verzeichniscontainer- und Cloud-Containerspeicherpools mithilfe des Befehls GENERATE DEDUPSTATS. • Um Deduplizierungsstatistikdaten für einen Speicherpool anzuzeigen, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus. 2. Klicken Sie auf Details > Merkmale. Verwenden Sie dementsprechend den Befehl QUERY EXTENTUPDATES, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainer- oder Cloud-Containerspeicherpools anzuzeigen. Anhand der Befehlsausgabe können Sie die Datenbereiche bestimmen, die nicht mehr referenziert werden, sowie die Datenbereiche, die zum Löschen vom System auswählbar sind. Überwachen Sie in der Ausgabe die Anzahl Datenbereiche, die zum Löschen vom System auswählbar sind. Diese Messgröße steht in direkten Zusammenhang mit dem Umfang des freien Speicherbereichs, der im Containerspeicherpool verfügbar ist. • Um den Umfang des physischen Speicherbereichs anzuzeigen, der von einem Dateibereich nach dem Entfernen der Datendeduplizierungseinsparungen belegt wird, verwenden Sie den Befehl select * from occupancy. Die Befehlsausgabe umfasst den Wert für LOGICAL_MB. LOGICAL_MB gibt an, wie viel Speicherbereich von diesem Dateibereich belegt wird.
Überwachen und verwalten Sie Bandeinheiten.	Überwachen Sie Ihre Umgebung auf Hardwarefehler auf Bandlaufwerken und in Bandarchiven. Anweisungen finden Sie in Bandalertnachrichten auf Hardwarefehler überwachen. Überwachen Sie die Datenträgerkompatibilität, um Fehler auf Bandlaufwerken zu verhindern. Anweisungen finden Sie in Durch Datenträgerinkompatibilität verursachte Fehler verhindern. Überwachen Sie Reinigungsnachrichten für Bandlaufwerke. Anweisungen finden Sie in Operationen mit Reinigungskassetten.	

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass sich die Start- und Endzeiten von Clientzeitplänen nicht mit denen von Serververwaltungstasks überschneiden. Begrenzen Sie die Zeit für Clientsicherungsoperationen auf 8 bis 12 Stunden.	Klicken Sie auf der Seite Übersicht im Operations Center auf Clients > Zeitpläne. In der Tabelle 'Zeitpläne' wird in der Spalte 'Start' die konfigurierte Startzeit für die geplante Operation angezeigt. Um anzuzeigen, wann die letzte Operation gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	Tipp: Wenn die Ausführung einer Clientoperation länger als erwartet dauert, empfangen Sie unter Umständen eine Warnung. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite 'Übersicht' im Operations Center den Mauszeiger über Clients und klicken Sie auf Zeitpläne. 2. Wählen Sie einen Zeitplan aus und klicken Sie auf Details. 3. Zeigen Sie die Details eines Zeitplans an, indem Sie auf den blauen Pfeil neben der Zeile klicken. 4. Geben Sie im Feld Ausführungszeitalert die Uhrzeit an, zu der eine Warnung ausgegeben wird, wenn die geplante Operation nicht ausgeführt wird. 5. Klicken Sie auf Sichern.
Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass sich die Start- und Endzeiten von Verwaltungstasks nicht mit denen von Clientzeitplänen überschneiden.	Klicken Sie auf der Seite Übersicht im Operations Center auf Server > Verwaltung. Überprüfen Sie in der Tabelle 'Verwaltung' die Informationen in der Spalte 'Letzte Ausführungsdauer'. Um anzuzeigen, wann die letzte Verwaltungstask gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	Bei der bevorzugten Methode wird sichergestellt, dass jede Verwaltungstask bis zum Abschluss ausgeführt wird, bevor die nächste Verwaltungstask gestartet wird. Beispiele für Verwaltungstasks umfassen Bestandsverfall, Kopieren von Speicherpools, Speicherbereichskonsolidierung und Datenbanksicherung. Tipp: Wenn die Ausführung einer Verwaltungstask zu lange dauert, ändern Sie die Startzeit oder die maximale Ausführungszeit. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Um die Startzeit oder die maximale Ausführungszeit für eine Task zu ändern, geben Sie den Befehl UPDATE SCHEDULE aus. Informationen zu diesem Befehl finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).

- Bandalertnachrichten auf Hardwarefehler überwachen
  Bandalertnachrichten werden von Band- und Speicherarchiveinheiten generiert, um Hardwarefehler zurückzumelden. Diese Nachrichten unterstützen Sie bei der Bestimmung von Fehlern, die sich nicht auf den IBM Spectrum Protect-Server beziehen.
- Durch Datenträgerinkompatibilität verursachte Fehler verhindern
  Indem Datenträgerkompatibilitätsprobleme überwacht und behoben werden, können Sie Fehler in einer bandbasierten Lösung in IBM Spectrum Protect verhindern. Ein neues Laufwerk hat möglicherweise nur eingeschränkt die Fähigkeit zur Verwendung der von einer vorherigen Version des Laufwerks unterstützten Datenträgerformate. Häufig kann ein neues Laufwerk Daten mit dem vorherigen Datenträgerformat lesen, aber nicht schreiben.
- Operationen mit Reinigungskassetten
  Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

Bandalertnachrichten auf Hardwarefehler überwachen

Bandalertnachrichten werden von Band- und Speicherarchiveinheiten generiert, um Hardwarefehler zurückzumelden. Diese Nachrichten unterstützen Sie bei der Bestimmung von Fehlern, die sich nicht auf den IBM Spectrum Protect-Server beziehen.

Informationen zu diesem Vorgang

Es wird eine Protokollseite erstellt, die jederzeit oder zu einem bestimmten Zeitpunkt, beispielsweise wenn ein Laufwerk abgehängt wird, abgerufen werden kann.

Eine Bandalertnachricht kann eine der folgenden Bewertungsstufen haben:

- Information (beispielsweise wird versucht, einen nicht unterstützten Kassettentyp einzulegen)
- Warnung (beispielsweise wird ein Hardwarefehler vorhergesagt)
- Kritisch (beispielsweise liegt ein Bandfehler vor und Ihre Daten sind gefährdet)

Bandalertnachrichten sind standardmäßig inaktiviert.

Vorgehensweise

- Um Bandalertnachrichten zu aktivieren, geben Sie den Befehl SET TAPEALERTMSG unter Angabe des Werts ON aus: `set tapealertmsg on`
- Um zu überprüfen, ob Bandalertnachrichten aktiviert sind, geben Sie den Befehl QUERY TAPEALERTMSG aus: `query tapealertmsg`

Durch Datenträgerinkompatibilität verursachte Fehler verhindern

Indem Datenträgerkompatibilitätsprobleme überwacht und behoben werden, können Sie Fehler in einer bandbasierten Lösung in IBM Spectrum Protect verhindern. Ein neues Laufwerk hat möglicherweise nur eingeschränkt die Fähigkeit zur Verwendung der von einer vorherigen Version des Laufwerks unterstützten Datenträgerformate. Häufig kann ein neues Laufwerk Daten mit dem vorherigen Datenträgerformat lesen, aber nicht schreiben.

Informationen zu diesem Vorgang

Standardmäßig verbleiben vorhandene Datenträger mit dem Status `FILLING` nach einem Laufwerkupgrade in diesem Status. In einigen Fällen möchten Sie vielleicht ein älteres Laufwerk weiterhin nutzen, um diese Datenträger mit Daten zu füllen. Dadurch bleibt die Schreib-/Lesefunktionalität für die vorhandenen Datenträger erhalten, bis sie konsolidiert werden. Wenn für alle Laufwerke in einem Speicherarchiv ein Upgrade durchgeführt werden soll, stellen Sie sicher, dass die Datenträgerformate von der neuen Hardware unterstützt werden. Wenn nicht ausschließlich die neuesten Datenträger mit dem neuen Laufwerk verwendet werden sollen, müssen Sie sich aller Kompatibilitätsprobleme bewusst sein. Anweisungen zum Umlagern von Daten finden Sie in Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde.

Um ein neues Laufwerk mit Datenträgern zu verwenden, von denen Daten gelesen, auf die aber keine Daten geschrieben werden können, geben Sie den Befehl UPDATE VOLUME aus, um Lesezugriff für diese Datenträger festzulegen. Damit wird verhindert, dass durch Schreib-/Leseinkompatibilität Fehler auftreten. Beispielsweise kann ein neues Laufwerk unter Umständen Datenträger, auf die Daten in einem von dem Laufwerk nicht unterstützten Format geschrieben wurden, ausgeben, sobald die Datenträger in das Laufwerk geladen werden. Es kann auch vorkommen, dass ein neues Laufwerk den ersten Schreibbefehl nicht für einen Datenträger ausführt, der teilweise in einem Format beschrieben ist, das von dem Laufwerk nicht unterstützt wird.

Wenn Daten auf dem Datenträger mit Lesezugriff verfallen und der Datenträger konsolidiert wird, ersetzen Sie ihn durch einen Datenträger, der mit dem neuen Laufwerk vollständig kompatibel ist. Fehler können generiert werden, wenn ein neues Laufwerk einen in einem älteren Format beschriebenen Datenträger nicht korrekt kalibrieren kann. Um dieses Problem zu verhindern, stellen Sie sicher, dass das ursprüngliche Laufwerk voll funktionsfähig ist und über aktuelle Mikrocodeversionen verfügt.

Operationen mit Reinigungskassetten

Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

Reinigungsprozess überwachen
: Wenn eine Reinigungskassette in ein Speicherarchiv zurückgestellt wird und ein Laufwerk gereinigt werden muss, hebt der Server die Bereitstellung des Datenträgers auf und führt die Reinigungsoperation aus. Wenn die Reinigungsoperation fehlschlägt oder wenn sie abgebrochen wird oder wenn keine Reinigungskassette verfügbar ist, sind Sie sich der Tatsache, dass das Laufwerk gereinigt werden muss, möglicherweise nicht bewusst. Überwachen Sie Reinigungsnachrichten auf diese Probleme, um sicherzustellen, dass Laufwerke wie erforderlich gereinigt werden. Geben Sie, falls erforderlich, den Befehl CLEAN DRIVE aus, damit der Server den Reinigungsversuch wiederholt, oder laden Sie manuell eine Reinigungskassette in das Laufwerk.

Mehrere Reinigungskassetten verwenden
: Der Server verwendet eine Reinigungskassette für die Anzahl Reinigungen, die Sie beim Zurückstellen der Reinigungskassette angeben. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen, verwendet der Server nur eine der Kassetten, bis die angegebene Anzahl Reinigungen für diese Kassette erreicht ist. Dann verwendet der Server die nächste Reinigungskassette. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen und zwei oder mehr Befehle CLEAN DRIVE gleichzeitig ausgegeben, verwendet der Server mehrere Kassetten gleichzeitig und verringert die verbleibenden Reinigungen auf jeder Kassette.

Zugehörige Verweise:

- AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)
- CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
- CLEAN DRIVE (Laufwerk reinigen)
- LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
- QUERY LIBVOLUME (Datenträger im Speicherarchiv abfragen)

Lizenzeinhaltung überprüfen

Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen. Planen Sie anhand dieser Informationen den weiteren Kauf von Lizenzen.

Informationen zu diesem Vorgang

Die Methode zur Überprüfung der Einhaltung der Lizenzbedingungen durch Ihre Lösung variiert abhängig von den Bedingungen Ihrer IBM Spectrum Protect-Lizenzvereinbarung.

Front-End-Kapazitätslizenzierung
: Das Front-End-Modell bestimmt die Lizenzvoraussetzungen auf der Basis des zurückgemeldeten Volumens an primären Daten, das von Clients gesichert wird. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme.

Back-End-Kapazitätslizenzierung
: Das Back-End-Modell bestimmt Lizenzvoraussetzungen auf der Basis der Terabyte Daten, die in primären Speicherpools und Repositorys gespeichert werden.
Tipps:

- Um die Genauigkeit von Schätzungen der Front-End- und Back-End-Kapazität zu gewährleisten, installieren Sie die neueste Version der Client-Software auf jedem Clientknoten.
- Die Informationen zur Front-End- und Back-End-Kapazität im Operations Center dienen zum Zweck der Planung und Schätzung.

PVU-Lizenzierung
: Das PVU-Modell basiert auf der Nutzung von PVUs durch Servereinheiten.
Wichtig: Die von IBM Spectrum Protect bereitgestellten PVU-Berechnungen werden als Schätzungen betrachtet und sind nicht rechtsverbindlich. Die von IBM Spectrum Protect zurückgemeldeten PVU-Lizenzinformationen werden nicht als zulässiger Ersatz für das IBM® License Metric Tool angesehen.

Die neuesten Informationen zu Lizenzierungsmodellen finden Sie in den Informationen zu Produktdetails und Lizenzen auf der Website der IBM Spectrum Protect-Produktfamilie. Wenden Sie sich bei Fragen oder Problemstellungen zu Lizenzierungsanforderungen an Ihren IBM Spectrum Protect-Software-Provider.

Vorgehensweise

Führen Sie zur Überwachung der Lizenzeinhaltung die Schritte aus, die den Bedingungen Ihrer Lizenzvereinbarung entsprechen.
Tipp: Das Operations Center stellt einen E-Mail-Bericht bereit, in dem die Front-End- und Back-End-Kapazitätsnutzung zusammengefasst sind. Berichte können automatisch regelmäßig an einen oder mehrere Empfänger gesendet werden. Klicken Sie für die Konfiguration und Verwaltung von E-Mail-Berichten in der Menüleiste des Operations Center auf Berichte.

Option	Bezeichnung
Front-End-Modell	a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen und klicken Sie auf Lizenzierung. Die Schätzung der Front-End-Kapazität wird auf der Seite 'Front-End-Nutzung' angezeigt. b. Wenn in der Spalte 'Keine Zurückmeldung' ein Wert angezeigt wird, klicken Sie auf die Zahl, um Clients zu identifizieren, von denen keine Kapazitätsnutzung zurückgemeldet wurde. c. Um die Kapazität für Clients zu schätzen, für die keine Kapazitätsnutzung zurückgemeldet wurde, rufen Sie die folgende FTP-Site auf, auf der Tools und Anweisungen zum Messen der Kapazität bereitgestellt werden: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Um die Front-End-Kapazität mithilfe eines Scripts zu messen, führen Sie die Anweisungen im aktuellen Lizenzierungshandbuch aus. d. Addieren Sie den Operations Center-Schätzwert und alle Schätzwerte, die Sie mithilfe eines Scripts ermittelt haben. e. Überprüfen Sie, ob die geschätzte Kapazität die Bedingungen Ihrer Lizenzvereinbarung einhält.
Back-End-Modell	Einschränkung: Wenn der Quellen- und der Zielreplikationsserver nicht dieselben Maßnahmeneinstellungen verwenden, können Sie das Operations Center nicht zur Überwachung der Back-End-Kapazitätsnutzung für replizierte Clients verwenden. Informationen zur Schätzung der Kapazitätsnutzung für diese Clients finden Sie in Technote 1656476. a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen und klicken Sie auf Lizenzierung. b. Klicken Sie auf die Registerkarte Back-End. c. Überprüfen Sie, ob das geschätzte Datenvolumen die Bedingungen Ihrer Lizenzvereinbarung einhält.
PVU-Modell	Informationen zur Vorgehensweise beim Prüfen der Einhaltung der PVU-Lizenzbedingungen finden Sie in Einhaltung des PVU-Lizenzierungsmodells prüfen.

Systemstatus mithilfe von E-Mail-Berichten verfolgen

Konfigurieren Sie das Operations Center für die Generierung von E-Mail-Berichten zur Zusammenfassung des Systemstatus. Sie können eine Mail-Server-Verbindung konfigurieren, Berichtseinstellungen ändern und wahlweise angepasste SQL-Berichte erstellen.

Vorbereitende Schritte

Bevor Sie E-Mail-Berichte konfigurieren, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Es ist ein SMTP-Host-Server (SMTP = Simple Mail Transfer Protocol) verfügbar, um Berichte als E-Mail senden und empfangen zu können. Der SMTP-Server muss als offenes Mail-Relay konfiguriert sein. Außerdem müssen Sie sicherstellen, dass der IBM Spectrum Protect-Server, der E-Mail-Nachrichten sendet, Zugriff auf den SMTP-Server hat. Wenn das Operations Center auf einem anderen Computer installiert ist, ist für diesen Computer kein Zugriff auf den SMTP-Server erforderlich.
- Um E-Mail-Berichte konfigurieren zu können, müssen Sie über Systemberechtigung für den Server verfügen.
- Um die Empfänger anzugeben, können Sie eine oder mehrere E-Mail-Adressen oder Administrator-IDs eingeben. Wenn eine Administrator-ID eingegeben werden soll, muss die ID auf dem Hub-Server registriert sein und der ID muss eine E-Mail-Adresse zugeordnet sein. Eine E-Mail-Adresse für einen Administrator können Sie mithilfe des Parameters EMAILADDRESS im Befehl UPDATE ADMIN angeben.

Informationen zu diesem Vorgang

Sie können das Operations Center zum Senden eines Berichts über allgemeine Operationen, eines Lizenzeinhaltungsberichts und eines oder mehrerer angepasster Berichte, die SQL-Anweisungen SELECT zum Abfragen verwalteter Server verwenden, konfigurieren.

Vorgehensweise

Um E-Mail-Berichte zu konfigurieren und zu verwalten, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Berichte.
2. Wenn noch keine E-Mail-Server-Verbindung konfiguriert ist, klicken Sie auf Mail-Server konfigurieren und füllen Sie die Felder aus. Nach der Konfiguration des Mail-Servers sind der Bericht über allgemeine Operationen und der Lizenzeinhaltungsbericht aktiviert.
3. Um Berichtseinstellungen zu ändern, wählen Sie einen Bericht aus, klicken Sie auf Details und aktualisieren Sie das Formular.
4. Optional: Um einen angepassten SQL-Bericht hinzuzufügen, klicken Sie auf + Bericht und füllen Sie die Felder aus.
   Tipp: Um einen Bericht sofort auszuführen und zu senden, wählen Sie den Bericht aus und klicken Sie auf Senden.

Ergebnisse

Aktivierte Berichte werden gemäß den angegebenen Einstellungen gesendet.

Nächste Schritte

Der Bericht über allgemeine Operationen umfasst eine Anlage. Um detaillierte Informationen anzuzeigen, erweitern Sie die Abschnitte in der Anlage.

Wenn Sie das Image in einem Bericht nicht anzeigen können, verwenden Sie möglicherweise einen E-Mail-Client, der HTML in ein anderes Format konvertiert. Informationen zu Einschränkungen finden Sie in der Onlinehilfe des Operations Center.

Operationen für eine Bandspeicherlösung verwalten

Verwenden Sie diese Informationen, um Operationen für eine Bandspeicherimplementierung für einen IBM Spectrum Protect-Server zu verwalten.

- Operations Center verwalten
  Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit.
- Clientoperationen verwalten
  Sie können Clientfehler beheben, Client-Upgrades verwalten und Clientknoten, die nicht mehr erforderlich sind, stilllegen. Um Speicherbereich auf dem Server freizugeben, können Sie veraltete Daten, die von Anwendungsclients gespeichert werden, inaktivieren.
- Datenspeicher verwalten
  Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.
- Bandeinheiten verwalten
  Routinemäßige Bandoperationen umfassen die Vorbereitung von Banddatenträgern für die Verwendung, die Steuerung, wie und wann Datenträger wiederverwendet werden, und die Sicherstellung, dass genügend Datenträger verfügbar sind. Außerdem müssen Sie auf Bedieneranforderungen antworten und Speicherarchive, Laufwerke, Pfade und Einheiten zum Versetzen von Daten verwalten.
- Bandlaufwerke verwalten
  Sie können Bandlaufwerke abfragen, aktualisieren und löschen. Außerdem können Sie Bandlaufwerke reinigen und Bandlaufwerkverschlüsselung und Datenprüfung konfigurieren.
- IBM Spectrum Protect-Server schützen
  Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

- Server stoppen und starten
  Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.
- Durchführung eines Upgrades für den Server planen
  Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.
- Vorbereitungen für einen Ausfall oder eine Systemaktualisierung
  Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.
- Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM
  IBM Spectrum Protect stellt die Funktion Disaster Recovery Manager (DRM) für die Wiederherstellung Ihrer Server- und Clientdaten bei einem Katastrophenfall zur Verfügung.

Operations Center verwalten

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit.

Informationen zu diesem Vorgang

Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt. Weitere Informationen zur Verwaltung des Operations Center finden Sie in Operations Center verwalten.

Clientoperationen verwalten

Sie können Clientfehler beheben, Client-Upgrades verwalten und Clientknoten, die nicht mehr erforderlich sind, stilllegen. Um Speicherbereich auf dem Server freizugeben, können Sie veraltete Daten, die von Anwendungsclients gespeichert werden, inaktivieren.

Informationen zu diesem Vorgang

In einigen Fällen können Clientfehler behoben werden, indem der Clientakzeptor gestoppt und gestartet wird. Wenn Clientknoten oder Administrator-IDs gesperrt sind, können Sie das Problem beheben, indem Sie den Clientknoten bzw. die Administrator-ID entsperren und dann das Kennwort zurücksetzen.

Ausführliche Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in Clientprobleme lösen.

Anweisungen zum Hinzufügen von Clients finden Sie in Anwendungen, virtuelle Maschinen und Systeme schützen.

- Fehler in Clientfehlerprotokollen auswerten
  Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.
- Clientakzeptor stoppen und erneut starten
  Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.
- Kennwörter zurücksetzen
  Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.
- Client-Upgrades verwalten
  Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.
- Clientknoten stilllegen
  Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.
- Daten zum Freigeben von Speicherbereich inaktivieren
  In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegeben Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

Fehler in Clientfehlerprotokollen auswerten

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

Vorbereitende Schritte

(Optional) Um Fehler in einem Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem zu beheben, stellen Sie sicher, dass der Clientverwaltungsservice installiert und gestartet wurde. Installationsanweisungen finden Sie in Clientverwaltungsservice installieren.

Vorgehensweise

Um Clientfehler zu diagnostizieren und zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn der Clientverwaltungsservice auf dem Clientknoten installiert ist, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Details.
  3. Klicken Sie auf der Seite 'Zusammenfassung' auf die Registerkarte Diagnose.
  4. Überprüfen Sie die abgerufenen Protokollnachrichten.
     Tipps:
     - Um das Fenster 'Clientprotokolle' ein- oder auszublenden, doppelklicken Sie auf den Rahmen des Fensters 'Clientprotokolle'.
     - Um die Größe des Fensters 'Clientprotokolle' zu ändern, klicken Sie auf den Rahmen des Fensters 'Clientprotokolle' und ziehen Sie den Rahmen.

     Wenn auf der Seite 'Diagnose' Vorschläge angezeigt werden, wählen Sie einen Vorschlag aus. Im Fenster 'Clientprotokolle' sind die Clientprotokollnachrichten, auf die sich der Vorschlag bezieht, hervorgehoben.
  5. Lösen Sie die in den Fehlernachrichten angegebenen Probleme mithilfe der Vorschläge.
     Tipp: Vorschläge werden nur für einen Teil der Clientnachrichten bereitgestellt.
- Wenn der Clientverwaltungsservice nicht auf dem Clientknoten installiert ist, überprüfen Sie die Fehlerprotokolle für den installierten Client.

Clientakzeptor stoppen und erneut starten

Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.

Informationen zu diesem Vorgang

In einigen Fällen können Clientzeitplanungsprobleme behoben werden, indem der Clientakzeptor gestoppt und erneut gestartet wird. Der Clientakzeptor muss aktiv sein, um sicherzustellen, dass geplante Operationen auf dem Client ausgeführt werden können. Wenn Sie beispielsweise die IP-Adresse oder den Domänennamen des Servers ändern, müssen Sie den Clientakzeptor erneut starten.

Vorgehensweise

Führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

- Um den Clientakzeptor zu stoppen, führen Sie die folgenden Schritte aus:
  a. Bestimmen Sie die Prozess-ID für den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

     ```
     ps -ef | grep dsmcad
     ```

     Überprüfen Sie die Ausgabe. In der folgenden Beispielausgabe lautet die Prozess-ID für den Clientakzeptor 6764:

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```

  b. Geben Sie in der Befehlszeile den folgenden Befehl aus:

     ```
     kill -9 PID
     ```

     Dabei gibt *PID* die Prozess-ID für den Clientakzeptor an.
- Um den Clientakzeptor zu starten, geben Sie in der Befehlszeile den folgenden Befehl aus:

  ```
  /usr/bin/dsmcad
  ```

Linux

- Um den Clientakzeptor zu stoppen, ohne ihn erneut zu starten, geben Sie den folgenden Befehl aus:

  ```
  # service dsmcad stop
  ```
- Um den Clientakzeptor zu stoppen und erneut zu starten, geben Sie den folgenden Befehl aus:

  ```
  # service dsmcad restart
  ```

MAC OS X

Klicken Sie auf Applications > Utilities > Terminal.

- Um den Clientakzeptor zu stoppen, geben Sie den folgenden Befehl aus:

  ```
  /bin/launchctl unload -w com.ibm.tivoli.dsmcad
  ```

- Um den Clientakzeptor zu starten, geben Sie den folgenden Befehl aus:

  ```
  /bin/launchctl load -w com.ibm.tivoli.dsmcad
  ```

Windows

- Um den Clientakzeptorservice zu stoppen, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf Start > Verwaltung > Dienste.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf Beenden und OK.
- Um den Clientakzeptorservice erneut zu starten, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf Start > Verwaltung > Dienste.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf Starten und OK.

Zugehörige Verweise:
Fehler für Clientzeitplanung beheben

Kennwörter zurücksetzen

Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.

Vorgehensweise

Um Kennwortprobleme zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn ein Client für Sichern/Archivieren auf einem Clientknoten installiert ist und das Kennwort verloren gegangen ist oder Sie das Kennwort vergessen haben, führen Sie die folgenden Schritte aus:
  1. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Knotenname* den Clientknoten und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
  2. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.
     Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf `generate` gesetzt haben.
- Wenn ein Administrator aufgrund von Kennwortproblemen ausgesperrt ist, führen Sie die folgenden Schritte aus:
  1. Um dem Administrator den Zugriff auf den Server zu ermöglichen, geben Sie den Befehl UNLOCK ADMIN aus. Anweisungen finden Sie in UNLOCK ADMIN (Administrator entsperren).
  2. Legen Sie mit dem Befehl UPDATE ADMIN ein neues Kennwort fest:

     ```
     update admin Administratorname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Administratorname* den Namen des Administrators und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
- Wenn ein Clientknoten gesperrt ist, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, warum der Clientknoten gesperrt ist und ob er entsperrt werden muss. Wenn beispielsweise der Clientknoten stillgelegt ist, wird der Clientknoten aus der Produktionsumgebung entfernt. Sie können die Stilllegungsoperation nicht zurücknehmen und der Clientknoten bleibt gesperrt. Ein Clientknoten kann auch gesperrt sein, wenn die Clientdaten Gegenstand einer rechtlichen Untersuchung sind.
  2. Verwenden Sie zum Entsperren eines Clientknotens den Befehl UNLOCK NODE. Anweisungen finden Sie in UNLOCK NODE (Clientknoten entsperren).
  3. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Knotenname* den Namen des Knotens und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
  4. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.

Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf `generate` gesetzt haben.

Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

Vorbereitende Schritte

1. Überprüfen Sie die Voraussetzungen für die Client/Server-Kompatibilität in Technote 1053218. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden.
2. Überprüfen Sie die Systemvoraussetzungen für den Client in IBM Spectrum Protect Supported Operating Systems.
3. Wenn die Lösung Speicheragenten oder Speicherarchivclients umfasst, überprüfen Sie die Informationen zur Kompatibilität von Speicheragenten bzw. Speicherarchivclients mit Servern, die als Speicherarchivmanager konfiguriert sind. Siehe Technote 1302789.

   Wenn Sie planen, ein Upgrade für einen Speicherarchivmanager und einen Speicherarchivclient durchzuführen, müssen Sie zuerst das Upgrade für den Speicherarchivmanager durchführen.

Vorgehensweise

Um ein Software-Upgrade durchzuführen, führen Sie die in der folgenden Tabelle aufgelisteten Anweisungen aus.

Software	Link zu Anweisungen
IBM Spectrum Protect-Client für Sichern/Archivieren	• Upgrade des Clients für Sichern/Archivieren durchführen
IBM Spectrum Protect Snapshot	• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
IBM Spectrum Protect for Databases	• Upgrade für Data Protection for SQL Server durchführen • Installation von Data Protection for Oracle • Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 durchführen • Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle durchführen
IBM Spectrum Protect for Mail	• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) • Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0) • Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Virtual Environments	• Installation und Upgrade für Data Protection for VMware durchführen • Data Protection for Microsoft Hyper-V installieren

Clientknoten stilllegen

Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.

Informationen zu diesem Vorgang

Wenn Sie den Stilllegungsprozess starten, sperrt der Server den Clientknoten, um zu verhindern, dass dieser auf den Server zugreift. Dateien, die zu dem Clientknoten gehören, werden nacheinander gelöscht; anschließend wird der Clientknoten gelöscht. Sie können die folgenden Typen von

Clientknoten stilllegen:

Anwendungsclientknoten
: Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Systemclientknoten
: Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

VM-Clientknoten
: Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Die einfachste Methode zur Stilllegung eines Clientknotens ist die Verwendung des Operations Center. Der Stilllegungsprozess wird im Hintergrund ausgeführt. Wenn der Client für die Replikation von Clientdaten konfiguriert ist, entfernt das Operations Center den Client automatisch aus der Replikation auf dem Quellen- und dem Zielreplikationsserver, bevor es den Client stilllegt.
Tipp: Sie können einen Clientknoten auch stilllegen, indem Sie den Befehl DECOMMISSION NODE oder DECOMMISSION VM ausgeben. Diese Methode kann beispielsweise in den folgenden Fällen verwendet werden:

- Um den Stilllegungsprozess für einen späteren Zeitpunkt zu planen oder eine Serie von Befehlen unter Verwendung eines Scripts auszuführen, geben Sie die Ausführung des Stilllegungsprozesses im Hintergrund an.
- Um den Stilllegungsprozess zu Zwecken der Fehlerbehebung zu überwachen, geben Sie die Ausführung des Stilllegungsprozesses im Vordergrund an. Wenn Sie den Prozess im Vordergrund ausführen, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor Sie die Arbeit mit anderen Tasks fortsetzen können.

Vorgehensweise

Führen Sie eine der folgenden Aktionen aus:

- Um einen Client mithilfe des Operations Center im Hintergrund stillzulegen, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Weitere > Stilllegen.
- Um einen Clientknoten mithilfe eines Verwaltungsbefehls stillzulegen, führen Sie eine der folgenden Aktionen aus:
  - Um einen Anwendungs- oder Systemclientknoten im Hintergrund stillzulegen, geben Sie den Befehl DECOMMISSION NODE aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

    ```
    decommission node austin
    ```

  - Um einen Anwendungs- oder Systemclientknoten im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION NODE unter Angabe des Parameters `wait=yes` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

    ```
    decommission node austin wait=yes
    ```

  - Um eine virtuelle Maschine im Hintergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM aus. Wenn beispielsweise die virtuelle Maschine den Namen AUSTIN hat, der Dateibereich 7 ist und der Dateibereichsname über die Dateibereichs-ID angegeben wird, geben Sie den folgenden Befehl aus:

    ```
    decommission vm austin 7 nametype=fsid
    ```

    Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

    ```
    decommission vm "austin 2" 7 nametype=fsid
    ```

  - Um eine virtuelle Maschine im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM unter Angabe des Parameters `wait=yes` aus. Geben Sie beispielsweise den folgenden Befehl aus:

    ```
    decommission vm austin 7 nametype=fsid wait=yes
    ```

    Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

    ```
    decommission vm "austin 2" 7 nametype=fsid wait=yes
    ```

Nächste Schritte

Achten Sie auf Fehlernachrichten, die unter Umständen in der Benutzerschnittstelle oder in der Befehlsausgabe unmittelbar nach der Ausführung des Prozesses angezeigt werden.

Um zu überprüfen, ob der Clientknoten stillgelegt wurde, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
2. Überprüfen Sie in der Tabelle 'Clients' in der Spalte 'Gefährdet' den Status:
   - Der Status 'Stillgelegt' (DECOMMISSIONED) gibt an, dass der Knoten stillgelegt wurde.
   - Ein Nullwert gibt an, dass der Knoten nicht stillgelegt wurde.
   - Der Status 'Anstehend' (PENDING) gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

   Tipp: Wenn der Status eines anstehenden Stilllegungsprozesses bestimmt werden soll, geben Sie den folgenden Befehl aus:

   ```
   query process
   ```

3. Überprüfen Sie die Befehlsausgabe:
   - Wenn für den Stilllegungsprozess ein Status angegeben ist, ist der Prozess in Bearbeitung. Beispiel:

     ```
     query process
      Prozess-     Prozessbeschreibung           Prozessstatus
      nummer
     ---------     --------------------     -----------------------------------------
             3     DECOMMISSION NODE        Anzahl der für Knoten NODE1 inaktivierten
                                            Sicherungsobjekte: 8 Objekte inaktiviert.
     ```

   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie keine Fehlernachricht empfangen haben, ist der Prozess unvollständig. Ein Prozess kann unvollständig sein, wenn Dateien, die dem Knoten zugeordnet sind, noch nicht inaktiviert wurden. Führen Sie nach der Inaktivierung der Dateien den Stilllegungsprozess erneut aus.
   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie eine Fehlernachricht empfangen, ist der Prozess fehlgeschlagen. Führen Sie den Stilllegungsprozess erneut aus.

Zugehörige Verweise:
DECOMMISSION NODE (Clientknoten stilllegen)
DECOMMISSION VM (Virtuelle Maschine stilllegen)

Daten zum Freigeben von Speicherbereich inaktivieren

In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegeben Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

Informationen zu diesem Vorgang

Einige Anwendungsclients sichern Daten immer als aktive Sicherungsdaten auf dem Server. Da aktive Sicherungsdaten nicht durch die Bestandsverfallsmaßnahmen verwaltet werden, werden die Daten nicht automatisch gelöscht und belegen unbegrenzt Serverspeicher. Um den Speicherbereich freizugeben, der von veralteten Daten belegt wird, können Sie die Daten inaktivieren.

Wenn Sie den Inaktivierungsprozess ausführen, werden alle aktiven Sicherungsdaten, die vor dem angegeben Datum gespeichert wurden, inaktiv. Die Daten werden gelöscht, sobald sie verfallen, und können nicht zurückgeschrieben werden. Die Inaktivierungsfunktion gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

Vorgehensweise

1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients.
2. Wählen Sie in der Tabelle 'Clients' einen oder mehrere Clients aus und klicken Sie auf Weitere > Bereinigen.
   Befehlszeilenmethode: Inaktivieren Sie Daten mit dem Befehl DEACTIVATE DATA.

Zugehörige Verweise:
DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)

Datenspeicher verwalten

Verwalten Sie Ihre Daten effizient und fügen Sie dem Server unterstützte Einheiten und Datenträger zum Speichern von Clientdaten hinzu.

- Bestandskapazität verwalten
  Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.
- Geplante Aktivitäten optimieren
  Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.
- Operationen durch Aktivierung der Kollokation von Clientdateien optimieren
  Die Kollokation von Clientdateien reduziert die Anzahl Datenträgermounts, die erforderlich sind, wenn Benutzer viele Dateien aus einem Speicherpool zurückschreiben, abrufen oder zurückrufen. Die Kollokation reduziert somit die Zeit, die für diese Operationen erforderlich ist.

Zugehörige Verweise:
Speicherpooltypen

Bestandskapazität verwalten

Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.

Vorbereitende Schritte

Die aktive Protokolldatei und das Archivprotokoll haben die folgenden Merkmale:

- Die Größe der aktiven Protokolldatei kann maximal 512 GB betragen. Weitere Informationen zum Festlegen der Größe der aktiven Protokolldatei für Ihr System finden Sie in Planung der Speicherarrays.
- Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist. Die Größe des Archivprotokolls ist im Gegensatz zur Größe der aktiven Protokolldatei nicht auf eine vordefinierte Größe festgelegt. Archivprotokolldateien werden automatisch gelöscht, wenn sie nicht mehr benötigt werden.

Als Best Practice können Sie wahlweise ein Archivübernahmeprotokoll erstellen, in dem Archivprotokolldateien gespeichert werden, wenn das Archivprotokollverzeichnis voll ist.

Bestimmen Sie über das Operations Center, welche Komponente des Bestands voll ist. Stellen Sie sicher, dass der Server gestoppt wird, bevor Sie eine der Bestandskomponenten vergrößern.

Vorgehensweise

- Um den Plattenspeicherplatz für die Datenbank zu vergrößern, führen Sie die folgenden Schritte aus:
  - Erstellen Sie in unterschiedlichen Laufwerken oder Dateisystemen ein oder mehrere Verzeichnisse für die Datenbank.
  - Geben Sie den Befehl EXTEND DBSPACE aus, um der Datenbank das Verzeichnis oder die Verzeichnisse hinzuzufügen. Die Instanzbenutzer-ID des Datenbankmanagers muss Zugriff auf die Verzeichnisse haben. Standardmäßig erfolgt eine Neuverteilung der Daten auf alle Datenbankverzeichnisse und eine Konsolidierung des Speicherbereichs.
    Tipps:
    - Die Zeit, die für die vollständige Neuverteilung von Daten und die Konsolidierung von Speicherbereich erforderlich ist, variiert abhängig von der Größe Ihrer Datenbank. Stellen Sie sicher, dass Sie dies bei der Planung berücksichtigen.
    - Stellen Sie sicher, dass die Verzeichnisse, die Sie angeben, dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.
  - Stoppen Sie den Server und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig nutzen zu können.
  - Reorganisieren Sie die Datenbank, falls erforderlich. Die Index- und Tabellenreorganisation für die Serverdatenbank kann dazu beitragen, unerwartetes Datenbankwachstum und Leistungsprobleme zu verhindern. Weitere Informationen zur Reorganisation der Datenbank finden Sie in Technote 1683633.
- Informationen zur Verringerung der Größe der Datenbank für Server der Version 7.1 und höher finden Sie in Technote 1683633. Einschränkung: Die Befehle können die E/A-Aktivität erhöhen und sich unter Umständen auf die Serverleistung auswirken. Um Leistungsprobleme auf ein Mindestmaß zu reduzieren, warten Sie, bis ein Befehl abgeschlossen ist, bevor Sie den nächsten Befehl ausgeben. Die DB2-Befehle können ausgegeben werden, wenn der Server aktiv ist.
- Um die aktive Protokolldatei zu vergrößern oder zu verkleinern, führen Sie die folgenden Schritte aus:
  1. Stellen Sie sicher, dass die Position für die aktive Protokolldatei über genügend Speicherbereich für die erhöhte Protokollgröße verfügt.
  2. Stoppen Sie den Server.
  3. Aktualisieren Sie in der Datei dsmserv.opt die Option ACTIVELOGSIZE mit der neuen Größe der aktiven Protokolldatei (angegeben in Megabyte).
     Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Die folgende Tabelle enthält Richtlinien für den Speicherbedarf:

     Tabelle 1. Schätzen des Speicherbedarfs für Datenträger und Dateibereiche

Wert für die Option ACTIVELOGSize	Größe des im Verzeichnis für aktive Protokolldateien zu reservierender freier Speicherbereich zusätzlich zum Speicherbereich für ACTIVELOGSize
16 GB bis 128 GB	5120 MB
129 GB bis 256 GB	10240 MB
257 GB bis 512 GB	20480 MB

     Um die Größe der aktiven Protokolldatei in die maximale Größe von 512 GB zu ändern, geben Sie die folgende Serveroption ein:

     ```
     activelogsize 524288
     ```

  4. Wenn Sie planen, ein neues Verzeichnis für aktive Protokolldateien zu verwenden, aktualisieren Sie den in der Serveroption ACTIVELOGDIRECTORY angegebenen Verzeichnisnamen. Das neue Verzeichnis muss leer sein und die Benutzer-ID des Datenbankmanagers muss Zugriff auf dieses Verzeichnis haben.

5. Starten Sie den Server erneut.

- Komprimieren Sie die Archivprotokolle, um die Größe des Speicherbereichs, der zum Speichern benötigt wird, zu reduzieren. Aktivieren Sie die dynamische Komprimierung für das Archivprotokoll, indem Sie den folgenden Befehl ausgeben:

  ```
  setopt archlogcompress yes
  ```

  Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hohen Workloads aktivieren. Ein Aktivieren dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Dateisystem für Archivprotokolle haben. Diese Verzögerung kann zur Folge haben, dass der Speicherbereich im Dateisystem für aktive Protokolldateien knapp wird. Sie müssen den verfügbaren Speicherbereich im Dateisystem für aktive Protokolldateien überwachen, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn für das Dateisystem für das Verzeichnis für aktive Protokolldateien fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT können Sie die Komprimierung für das Archivprotokoll sofort inaktivieren, ohne den Server stoppen zu müssen.

Zugehörige Verweise:
Serveroption ACTIVELOGSIZE
EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)
SETOPT (Serveroption für dynamische Aktualisierung definieren)

Geplante Aktivitäten optimieren

Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

Vorgehensweise

1. Überwachen Sie die Systemleistung regelmäßig, um sicherzustellen, dass Sicherungs- und Verwaltungstasks erfolgreich ausgeführt werden. Weitere Informationen zur Überwachung finden Sie in Bandspeicherlösung überwachen.
2. Wenn die Überwachungsdaten anzeigen, dass sich die Server-Workload erhöht hat, müssen Sie die Planungsinformationen gegebenenfalls überprüfen. Überprüfen Sie, ob die Kapazität des Systems in den folgenden Fällen ausreichend ist:
   - Erhöhung der Anzahl Clients
   - Zunahme des Datenvolumens, das gesichert wird
   - Änderung des Zeitraums, der für Sicherungen verfügbar ist
3. Bestimmen Sie, ob für Ihre Lösung Leistungsprobleme vorliegen. Überprüfen Sie die Clientzeitpläne dahingehend, ob Tasks innerhalb des geplanten Zeitrahmens ausgeführt werden:
   a. Wählen Sie auf der Seite Clients im Operations Center den Client aus.
   b. Klicken Sie auf Details.
   c. Überprüfen Sie auf der Seite Zusammenfassung des Clients die für Gesichert und Repliziert angegebene Aktivität, um alle Risiken zu ermitteln.

   Passen Sie, falls erforderlich, den Zeitpunkt und die Häufigkeit für die Ausführung von Clientsicherungsoperationen an.
4. Planen Sie ausreichend Zeit ein, um die folgenden Verwaltungstasks innerhalb von 24 Stunden erfolgreich ausführen zu können:
   a. Sichern der Datenbank
   b. Ausführen der Verfallsverarbeitung, um Clientsicherungen und Archivierungsdateikopien aus dem Serverspeicher zu entfernen

Zugehörige Konzepte:
Leistung
Zugehörige Tasks:
Daten deduplizieren (Version 7.1.1)

Operationen durch Aktivierung der Kollokation von Clientdateien optimieren

Die Kollokation von Clientdateien reduziert die Anzahl Datenträgermounts, die erforderlich sind, wenn Benutzer viele Dateien aus einem Speicherpool zurückschreiben, abrufen oder zurückrufen. Die Kollokation reduziert somit die Zeit, die für diese Operationen erforderlich ist.

Informationen zu diesem Vorgang

Bei aktivierter Kollokation versucht der Server, Dateien auf möglichst wenigen Speicherdatenträgern mit sequenziellem Zugriff zu speichern. Die Dateien können zu einem einzelnen Clientknoten, einer Gruppe von Clientknoten, einem Clientdateibereich oder einer Gruppe von Dateibereichen gehören. Sie können die Kollokation für jeden Speicherpool mit sequenziellem Zugriff festlegen, wenn Sie den Pool definieren oder aktualisieren.

Abbildung 1 zeigt ein Beispiel für die Kollokation nach Clientknoten mit drei Clients, von denen jeder über einen separaten Datenträger verfügt, der Daten dieses Clients enthält.

Abbildung 1. Beispiel für die aktivierte Kollokation nach Knoten

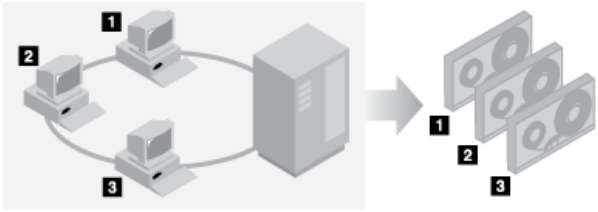


Abbildung 2 zeigt ein Beispiel für die Kollokation nach Clientknotengruppe. Es sind drei Gruppen definiert und die Daten jeder Gruppe werden auf separaten Datenträgern gespeichert.

Abbildung 2. Beispiel für die aktivierte Kollokation nach Knotenkollokationsgruppe

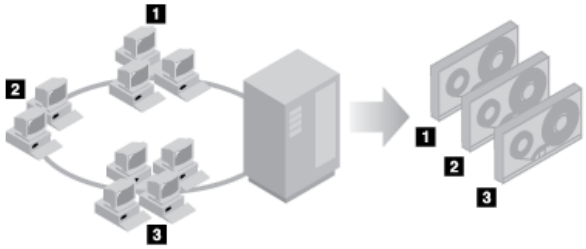
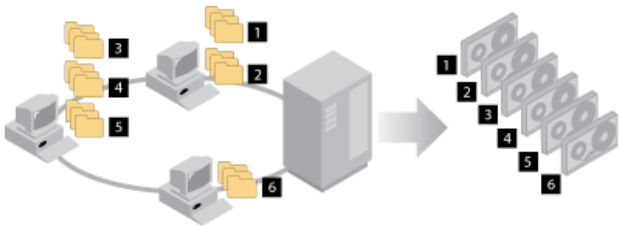


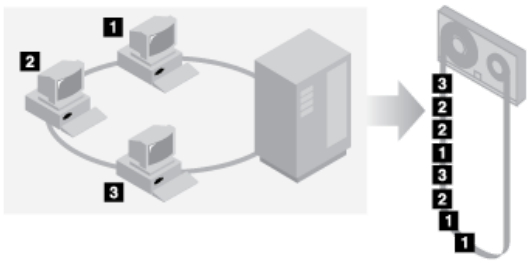
Abbildung 3 zeigt ein Beispiel für die Kollokation nach Dateibereichsgruppe. Es sind sechs Gruppen definiert. Jede Gruppe enthält Daten aus Dateibereichen, die zu einem einzelnen Knoten gehören. Die Daten jeder Gruppe werden auf einem separaten Datenträger gespeichert.

Abbildung 3. Beispiel für die aktivierte Kollokation nach Dateibereichskollokationsgruppe



Bei inaktivierter Kollokation versucht der Server, den gesamten verfügbaren Speicherbereich auf jedem Datenträger zu nutzen, bevor er einen neuen Datenträger auswählt. Dieser Prozess ermöglicht zwar eine bessere Nutzung einzelner Datenträger, Benutzerdateien können jedoch über viele Datenträger verstreut werden. Abbildung 4 zeigt ein Beispiel für die inaktivierte Kollokation mit drei Clients, die Speicherbereich auf einem einzelnen Datenträger gemeinsam nutzen.

Abbildung 4. Beispiel für die inaktivierte Kollokation



Bei inaktivierter Kollokation sind unter Umständen mehr Datenträgermountoperationen zum Bereitstellen von Datenträgern erforderlich, wenn Benutzer viele Dateien zurückschreiben, abrufen oder zurückrufen.

Die Kollokation nach Gruppe ist der IBM Spectrum Protect-Systemstandardwert für primäre Speicherpools mit sequenziellem Zugriff. Für Kopienspeicherpools erfolgt standardmäßig keine Kollokation.

- Auswirkungen der Kollokation auf Operationen
  Die Auswirkungen der Kollokation auf Ressourcen und die Systemleistung sind vom Typ der Operation abhängig, die ausgeführt wird.
- Datenträger bei aktivierter Kollokation auswählen
  Die Auswahl der Datenträger ist davon abhängig, ob die Kollokation nach Gruppe, nach Knoten oder nach Dateibereich erfolgt.

- Datenträger bei inaktivierter Kollokation auswählen
  Bei inaktivierter Kollokation versucht der Server, den gesamten verfügbaren Speicherbereich in einem Speicherdatenträger zu nutzen, bevor er auf einen neuen Datenträger zugreift.
- Kollokationseinstellungen
  Nach der Definition eines Speicherpools können Sie die Kollokationseinstellung durch Aktualisieren des Speicherpools ändern. Die Änderung der Kollokation für den Pool hat keine Auswirkungen auf Dateien, die bereits in dem Pool gespeichert sind.
- Kollokation von Kopienspeicherpools
  Bei der Verwendung der Kollokation für Kopienspeicherpools müssen bestimmte Hinweise beachtet werden. Die Kollokation von Kopienspeicherpools, insbesondere die Kollokation nach Knoten oder Dateibereich, hat mehr teilweise gefüllte Datenträger und möglicherweise unnötige Konsolidierungsaktivität für ausgelagerte Datenträger zur Folge.
- Kollokation planen und aktivieren
  Zu wissen, welche Auswirkungen die Kollokation hat, kann hilfreich sein, um die Anzahl der Datenträgermounts zu reduzieren, den Speicherbereich auf sequenziellen Datenträgern besser zu nutzen und die Effizienz von Serveroperationen zu verbessern.

Auswirkungen der Kollokation auf Operationen

Die Auswirkungen der Kollokation auf Ressourcen und die Systemleistung sind vom Typ der Operation abhängig, die ausgeführt wird.

In Tabelle 1 sind die Auswirkungen der Kollokation auf Operationen zusammengefasst.

Tabelle 1. Auswirkungen der Kollokation auf Operationen

Operation	**Kollokation aktiviert**	**Kollokation inaktiviert**
Sichern, Archivieren oder Umlagern von Clientdateien	Mehr Datenträgermounts zum Kollokieren von Dateien.	Es sind weniger Datenträgermounts erforderlich.
Zurückschreiben, Abrufen oder Rückrufen von Clientdateien	Eine große Anzahl Dateien kann schneller zurückgeschrieben, abgerufen oder zurückgerufen werden, da sich die Dateien auf weniger Datenträgern befinden.	Möglicherweise sind mehrere Datenträgermounts für einen einzelnen Benutzer erforderlich, da Dateien auf mehrere Datenträger verteilt sein können. Die Dateien mehrerer Benutzer können auf demselben Speicherdatenträger mit sequenziellem Zugriff gespeichert sein. Wenn beispielsweise zwei Benutzer versuchen, eine Datei wiederherzustellen, die sich auf demselben Datenträger befindet, muss ein Benutzer warten, bis der andere Benutzer seine Dateien wiederhergestellt hat.
Speichern von Daten auf Band	Der Server versucht, alle verfügbaren Banddatenträger zum Trennen von Benutzerdateien zu verwenden, bevor der gesamte verfügbare Speicherbereich auf jedem Banddatenträger genutzt wird.	Der Server versucht, den gesamten verfügbaren Speicherbereich auf jedem einzelnen Banddatenträger zu nutzen, bevor ein anderer Banddatenträger verwendet wird.
Datenträgermountoperationen	Es sind mehr Mountoperationen erforderlich, wenn Benutzerdateien von Clientknoten direkt auf Datenträger mit sequenziellem Zugriff gesichert, archiviert oder umgelagert werden. Während der Konsolidierung und Speicherpoolumlagerung sind mehr Mountoperationen erforderlich. Es werden mehr Datenträger verwaltet werden, da Datenträger nicht vollständig genutzt werden.	Während der Zurückschreibung, des Abrufs und des Rückrufs von Clientdateien sind mehr Mountoperationen erforderlich.
Generieren von Sicherungsgruppen	Es wird weniger Zeit für die Suche nach Datenbankeinträgen benötigt und es sind weniger Mountoperationen erforderlich.	Es wird mehr Zeit für die Suche nach Datenbankeinträgen benötigt und es sind weniger Mountoperationen erforderlich.

Wenn die Kollokation für eine Gruppe, einen einzelnen Clientknoten oder einen einzelnen Dateibereich aktiviert ist, werden alle Daten, die zu der Gruppe, dem Knoten oder dem Dateibereich gehören, durch einen einzigen Serverprozess versetzt oder kopiert. Wenn beispielsweise Daten nach Gruppe kollokiert werden, werden alle Daten für alle Knoten, die zu derselben Kollokationsgruppe gehören, durch denselben Prozess umgelagert.

Bei der Kollokation von Daten versucht der IBM Spectrum Protect-Server, Dateien auf möglichst wenigen Speicherdatenträgern mit sequenziellem Zugriff zu speichern. Wenn der Server Daten auf Datenträgern in einem Speicherpool mit sequenziellem Zugriff sichert, hat der Sicherungsprozess jedoch Priorität vor den Kollokationseinstellungen. Demzufolge führt der Server die Sicherungsoperation aus, kann aber die Daten möglicherweise nicht kollokieren.

Angenommen, die Kollokation erfolgt nach Knoten und Sie geben an, dass ein Knoten zwei Mountpunkte auf dem Server verwenden kann. Weiterhin sei angenommen, dass die Daten, die von dem Knoten gesichert werden, problemlos auf einen einzigen Banddatenträger passen. Während der Sicherung stellt der Server möglicherweise zwei Banddatenträger bereit und die Daten des Knotens werden möglicherweise auf zwei Bänder verteilt und nicht auf einem einzigen Band gespeichert. Wenn Sie die Kollokation aktivieren, verwenden die folgenden Serveroperationen einen einzigen Serverprozess:

- Versetzen von Daten von Datenträgern mit wahlfreiem Zugriff und sequenziellem Zugriff
- Versetzen von Knotendaten von Datenträgern mit sequenziellem Zugriff
- Sichern eines Speicherpools mit wahlfreiem Zugriff oder sequenziellem Zugriff
- Zurückschreiben eines Speicherpools mit sequenziellem Zugriff
- Konsolidierung von Speicherbereich in einem Speicherpool mit sequenziellem Zugriff oder auf ausgelagerten Datenträgern
- Umlagerung von Daten aus einem Speicherpool mit wahlfreiem Zugriff

Wenn die Umlagerung von Daten aus einem Plattenspeicherpool mit wahlfreiem Zugriff in einen Speicherpool mit sequenziellem Zugriff erfolgt und die Kollokation nach Knoten oder Dateibereich erfolgt, werden Knoten oder Dateibereiche automatisch für die Umlagerung auf der Basis des umzulagernden Datenvolumens ausgewählt. Der Knoten oder Dateibereich mit den meisten Daten wird zuerst umgelagert. Wenn die Kollokation nach Gruppe erfolgt, werden alle Knoten in dem Speicherpool ausgewertet, um den Knoten mit den meisten Daten zu bestimmen. Der Knoten mit den meisten Daten wird zusammen mit allen Daten für alle Knoten, die zu dieser Kollokationsgruppe gehören, zuerst umgelagert. Dieser Prozess erfolgt unabhängig von dem Datenvolumen, das in den Dateibereichen der Knoten gespeichert ist, und unabhängig davon, ob der untere Umlagerungsschwellenwert erreicht wurde.

Wenn jedoch kollokierte Daten aus einem Speicherpool mit sequenziellem Zugriff in einen anderen Speicherpool mit sequenziellem Zugriff umgelagert werden, ordnet der Server die Datenträger gemäß dem Datum, an dem zuletzt auf den Datenträger zugegriffen wurde. Der Datenträger mit dem frühesten Zugriffsdatum wird zuerst umgelagert und der Datenträger mit dem neuesten Zugriffsdatum wird zuletzt umgelagert.

Ein Grund für die Kollokation nach Gruppe besteht darin, dass einzelne Clientknoten oft nicht über ausreichend Daten verfügen, um Banddatenträger mit hoher Speicherkapazität zu füllen. Durch die Kollokation von Daten nach Gruppen von Knoten kann die nicht verwendete Bandkapazität reduziert werden, indem mehr kollokierte Daten auf einzelnen Bändern gespeichert werden. Durch die Kollokation von Daten nach Gruppen von Dateibereichen wird die nicht verwendete Bandkapazität noch stärker reduziert.

Die Daten, die zu allen Knoten in derselben Kollokationsgruppe gehören, werden durch denselben Prozess umgelagert. Demzufolge kann durch die Kollokation nach Gruppe die Häufigkeit der erforderlichen Mounts für einen Datenträger, der umgelagert werden soll, reduziert werden. Die Kollokation nach Gruppe kann auch das Durchsuchen der Datenbank minimieren und Bandübergaben während der Übertragung von Daten von einem Speicherpool mit sequenziellem Zugriff in einen anderen reduzieren.

Datenträger bei aktivierter Kollokation auswählen

Die Auswahl der Datenträger ist davon abhängig, ob die Kollokation nach Gruppe, nach Knoten oder nach Dateibereich erfolgt.

Tabelle 1 zeigt, wie der IBM Spectrum Protect-Server den ersten Datenträger auswählt, wenn die Kollokation für einen Speicherpool auf Clientknoten-, Kollokationsgruppen- und Dateibereichsebene aktiviert ist.

Tabelle 1. Wie der Server Datenträger bei aktivierter Kollokation auswählt

Reihenfolge bei der Auswahl der Datenträger	Bei Kollokation nach Gruppe	Bei Kollokation nach Knoten	Bei Kollokation nach Dateibereich
1	Ein Datenträger, der bereits Dateien aus der Kollokationsgruppe enthält, zu der der Client gehört	Ein Datenträger, der bereits Dateien desselben Clientknotens enthält	Ein Datenträger, der bereits Dateien aus demselben Dateibereich dieses Clientknotens enthält
2	Ein leerer vordefinierter Datenträger	Ein leerer vordefinierter Datenträger	Ein leerer vordefinierter Datenträger
3	Ein leerer Arbeitsdatenträger	Ein leerer Arbeitsdatenträger	Ein leerer Arbeitsdatenträger
4	Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich	Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich	Ein Datenträger, der Daten desselben Clientknotens enthält
5	Nicht zutreffend	Nicht zutreffend	Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich

Wenn der Server das Speichern der Daten auf einem zweiten Datenträger fortsetzen muss, fordert er weiteren Speicherbereich in der folgenden Auswahlreihenfolge an:

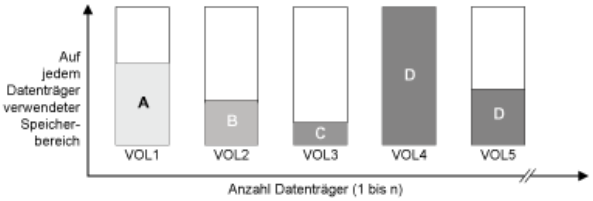
1. Ein leerer vordefinierter Datenträger
2. Ein leerer Arbeitsdatenträger
3. Bei Datenträgern, die bereits Daten enthalten, ein Datenträger mit dem meisten verfügbaren freien Speicherbereich

4. Ein beliebiger verfügbarer Datenträger im Speicherpool

Wenn die Kollokation nach Clientknoten oder Dateibereich erfolgt, versucht der Server, die beste Nutzung einzelner Datenträger zu ermöglichen, und minimiert das Mischen von Dateien von unterschiedlichen Clients oder aus unterschiedlichen Dateibereichen auf Datenträgern. Diese Konfiguration ist in Abbildung 1 dargestellt. Die Abbildung zeigt, dass die Datenträgerauswahl *horizontal* erfolgt, wobei alle verfügbaren Datenträger verwendet werden, bevor der gesamte verfügbare Speicherbereich auf jedem einzelnen Datenträger genutzt wird. A, B, C und D stellen Dateien aus vier verschiedenen Clientknoten dar.
Tipps:

1. Wenn die Kollokation nach Knoten erfolgt und der Knoten mehrere Dateibereiche hat, versucht der Server nicht, diese Dateibereiche zu kollokieren.
2. Wenn die Kollokation nach Dateibereich erfolgt und ein Knoten mehrere Dateibereiche hat, versucht der Server, Daten für verschiedene Dateibereiche auf unterschiedlichen Datenträgern zu speichern.

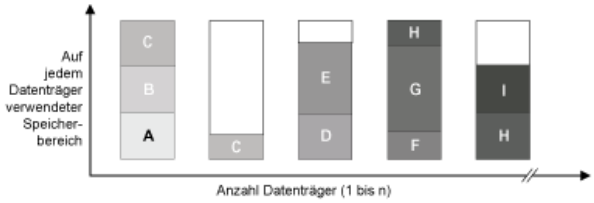
Abbildung 1. Verwendung aller verfügbaren Speicherdatenträger mit sequenziellem Zugriff bei aktivierter Kollokation auf Knoten- oder Dateibereichsebene



Die Kollokation kann nach Dateibereichsgruppe oder Knotengruppe erfolgen. Wenn die Kollokation nach Knotengruppe (Knotenkollokationsgruppe) erfolgt, versucht der Server, Daten von Knoten, die zu derselben Kollokationsgruppe gehören, zu kollokieren. Eine Dateibereichskollokationsgruppe verwendet dieselben Methoden wie eine Knotenkollokationsgruppe, kann jedoch aufgrund der Granularität der Dateibereichsgrößen mehr Speicherbereich verwenden. Wie in Abbildung 2 gezeigt wurden Daten für die folgenden Gruppen von Knoten kollokiert:

- Gruppe 1 besteht aus Knoten A, B und C.
- Gruppe 2 besteht aus Knoten D und E.
- Gruppe 3 besteht aus Knoten F, G, H und I.

Wenn möglich, kollokiert der IBM Spectrum Protect-Server Daten, die zu einer Gruppe von Knoten gehören, auf einem einzigen Band. Dies ist in der Abbildung durch Gruppe 2 dargestellt. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind (Gruppe 1 und 2). Wenn die Knoten in der Kollokationsgruppe mehrere Dateibereiche haben, versucht der Server nicht, diese Dateibereiche zu kollokieren.
Abbildung 2. Verwendung aller verfügbaren Speicherdatenträger mit sequenziellem Zugriff bei aktivierter Kollokation auf Gruppenebene



Normalerweise schreibt der IBM Spectrum Protect-Server Daten für die aktive Operation immer auf den Datenträger, der gerade gefüllt wird. Gelegentlich kann es jedoch vorkommen, dass sich mehr als ein Datenträger, der mit Daten gefüllt wird, in einem kollokierten Speicherpool befindet. Es kann vorkommen, dass sich mehrere Datenträger, die mit Daten gefüllt werden, in einem kollokierten Speicherpool befinden, wenn verschiedene Serverprozesse oder Clientsitzungen versuchen, Daten gleichzeitig in dem kollokierten Pool zu speichern. In dieser Situation ordnet IBM Spectrum Protect einen Datenträger für jeden Prozess oder jede Sitzung zu, der bzw. die einen Datenträger benötigt, sodass beide Operationen so schnell wie möglich ausgeführt werden.

Datenträger bei inaktivierter Kollokation auswählen

Bei inaktivierter Kollokation versucht der Server, den gesamten verfügbaren Speicherbereich in einem Speicherdatenträger zu nutzen, bevor er auf einen neuen Datenträger zugreift.

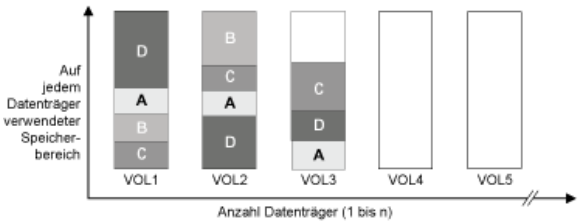
Wenn Sie Clientdateien in einem Speicherpool mit sequenziellem Zugriff speichern, für den die Kollokation inaktiviert ist, erfolgt die Auswahl eines Datenträgers durch den Server in der folgenden Reihenfolge:

1. Ein zuvor verwendeter sequenzieller Datenträger mit verfügbarem Speicherbereich (ein Datenträger mit dem größten Datenvolumen wird zuerst ausgewählt)
2. Ein leerer Datenträger

Wenn der Server das Speichern der Daten auf einem zweiten Datenträger fortsetzen muss, versucht er, einen leeren Datenträger auszuwählen. Wenn kein leerer Datenträger vorhanden ist, versucht der Server, einen der übrigen verfügbaren Datenträger im Speicherpool auszuwählen.

Abbildung 1 zeigt dass die Datenträgerverwendung vertikal erfolgt, wenn die Kollokation inaktiviert ist. In diesem Beispiel werden weniger Datenträger verwendet, da der Server versucht, den gesamten verfügbaren Speicherbereich durch Mischen von Clientdateien auf einzelnen Datenträgern zu nutzen. A, B, C und D stellen Dateien aus vier verschiedenen Clientknoten dar.

Abbildung 1. Verwendung des gesamten verfügbaren Speicherbereichs auf Datenträgern mit sequenziellem Zugriff bei inaktivierter Kollokation



Kollokationseinstellungen

Nach der Definition eines Speicherpools können Sie die Kollokationseinstellung durch Aktualisieren des Speicherpools ändern. Die Änderung der Kollokation für den Pool hat keine Auswirkungen auf Dateien, die bereits in dem Pool gespeichert sind.

Wenn beispielsweise die Kollokation für einen Speicherpool inaktiviert ist und jetzt aktiviert wird, werden ab diesem Zeitpunkt Clientdateien, die in dem Pool gespeichert werden, kollokiert. Dateien, die zuvor in dem Speicherpool gespeichert wurden, werden nicht versetzt, um kollokiert zu werden. Wenn Datenträger konsolidiert werden, werden die Daten in dem Pool im Laufe der Zeit immer stärker kollokiert. Sie können auch den Befehl MOVE DATA oder MOVE NODEDATA verwenden, um Daten auf neue Datenträger zu versetzen, um die Kollokation zu erhöhen. Das Versetzen von Daten auf neue Datenträger führt jedoch zu einer Verlängerung der Verarbeitungszeit und zu einer Erhöhung der Datenträgermountaktivität.
Tipp: Wenn die Kollokation nach Dateibereich aktiviert ist und ein Knoten über einen Datenträger mit mehreren Dateibereichen verfügt, kann eine Mountwartezeit auftreten oder der Mount länger als üblich dauern. Wenn ein Datenträger für den Datenempfang auswählbar ist, wartet IBM Spectrum Protect auf diesen Datenträger.

Kollokation von Kopienspeicherpools

Bei der Verwendung der Kollokation für Kopienspeicherpools müssen bestimmte Hinweise beachtet werden. Die Kollokation von Kopienspeicherpools, insbesondere die Kollokation nach Knoten oder Dateibereich, hat mehr teilweise gefüllte Datenträger und möglicherweise unnötige Konsolidierungsaktivität für ausgelagerte Datenträger zur Folge.

Primäre Speicherpools spielen bei der Wiederherstellung eine andere Rolle als Kopienspeicherpools. Normalerweise werden primäre Speicherpools verwendet, um Daten direkt auf Clients wiederherzustellen. Wenn in einem Katastrophenfall sowohl Clients als auch der Server verloren gehen, können Sie ausgelagerte Kopienspeicherpooldatenträger verwenden, um die primären Speicherpools wiederherzustellen. Mithilfe der Typen von Wiederherstellungsszenarios können Sie bestimmen, ob die Kollokation für Ihre Kopienspeicherpools verwendet werden sollte.

Die Kollokation hat in der Regel teilweise gefüllte Datenträger zur Folge, wenn die Kollokation nach Knoten oder Dateibereich erfolgt. Teilweise gefüllte Datenträger sind jedoch seltener vorhanden, wenn die Kollokation nach Gruppe erfolgt. Teilweise gefüllte Datenträger können für primäre Speicherpools akzeptabel sein, da die Datenträger verfügbar bleiben und während des nächsten Umlagerungsprozesses gefüllt werden können. Teilweise gefüllte Datenträger können jedoch für Kopienspeicherpools, deren Speicherpooldatenträger sofort ausgelagert werden, inakzeptabel sein. Wenn Sie die Kollokation für Kopienspeicherpools verwenden, müssen Sie die folgenden Entscheidungen treffen:

- Auslagerung einer größeren Anzahl teilweise gefüllter Datenträger, wodurch sich die Konsolidierungsaktivität erhöht, wenn der Konsolidierungsschwellenwert verringert oder erreicht wird.
- Verbleib dieser teilweise gefüllten Datenträger vor Ort, bis sie voll sind, wobei das Risiko besteht, dass keine ausgelagerte Kopie der Daten auf diesen Datenträgern vorhanden ist.
- Angabe, ob die Kollokation nach Gruppe erfolgen soll, um möglichst viel Bandkapazität zu nutzen.

Wenn die Kollokation für einen Kopienspeicherpool inaktiviert ist, sind nach dem Sichern von Daten im Kopienspeicherpool normalerweise nur einige wenige teilweise gefüllte Datenträger vorhanden.

Überprüfen Sie Ihre Optionen sorgfältig, bevor Sie die Kollokation für Kopienspeicherpools verwenden, und wägen Sie ab, ob gleichzeitiges Schreiben verwendet werden soll. Wenn bei Verwendung der Kollokation für Ihre primären Speicherpools kein gleichzeitiges Schreiben verwendet wird, können Sie die Kollokation für Kopienspeicherpools gegebenenfalls inaktivieren. Die Kollokation für Kopienspeicherpools kann sinnvoll sein, wenn nur wenige Clients vorhanden sind und für jeden dieser Clients täglich sehr viele Teilsicherungsdaten anfallen. Wenn die Kollokation zusammen mit gleichzeitigem Schreiben verwendet wird, müssen Sie sicherstellen, dass die Kollokationseinstellungen für die primären Speicherpools und die Kopienspeicherpools identisch sind.

Kollokation planen und aktivieren

Zu wissen, welche Auswirkungen die Kollokation hat, kann hilfreich sein, um die Anzahl der Datenträgermounts zu reduzieren, den Speicherbereich auf sequenziellen Datenträgern besser zu nutzen und die Effizienz von Serveroperationen zu verbessern.

Informationen zu diesem Vorgang

In Tabelle 1 sind die vier Kollokationsoptionen aufgeführt, die Sie in den Befehlen DEFINE STGPOOL und UPDATE STGPOOL angeben können. Die Tabelle zeigt auch die Auswirkungen der Kollokation auf Daten, die zu Knoten gehören, die Mitglieder einer Kollokationsgruppe sind, bzw. die zu Knoten gehören, die keine Mitglieder einer Kollokationsgruppe sind.

Tabelle 1. Kollokationsoptionen und Auswirkungen auf Knotendaten

Kollokationsoption	Wenn ein Knoten nicht als Mitglied einer Kollokationsgruppe definiert ist	Wenn ein Knoten als Mitglied einer Kollokationsgruppe definiert ist
Keine	Die Daten für den Knoten werden nicht kollokiert.	Die Daten für den Knoten werden nicht kollokiert.
Gruppe	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern im Speicherpool.	Der Server speichert die Daten für den Knoten und für andere Knoten, die zu derselben Kollokationsgruppe gehören, auf möglichst wenigen Datenträgern.
Knoten	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.
Dateibereich	Der Server speichert die Daten für den Dateibereich des Knotens auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool.	Der Server speichert die Daten für den Dateibereich des Knotens auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool.

Tabelle 2. Kollokationsgruppenoptionen und Auswirkungen auf Dateibereichsdaten

Kollokationsoption	Wenn ein Dateibereich nicht als Mitglied einer Kollokationsgruppe definiert ist	Wenn ein Dateibereich als Mitglied einer Kollokationsgruppe definiert ist
Keine	Die Daten für den Dateibereich werden nicht kollokiert.	Die Daten für den Dateibereich werden nicht kollokiert.
Gruppe	Der Server speichert die Daten für den Dateibereich auf möglichst wenigen Datenträgern im Speicherpool.	Der Server speichert die Daten für den Dateibereich und für andere Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf möglichst wenigen Datenträgern.
Knoten	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.	Der Server speichert die Daten für den Knoten auf möglichst wenigen Datenträgern.
Dateibereich	Der Server speichert die Daten für den Dateibereich des Knotens auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool.	Der Server speichert die Daten für die Dateibereiche auf möglichst wenigen Datenträgern. Wenn ein Knoten mehrere Dateibereiche hat, speichert der Server die Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern im Speicherpool.

Vorgehensweise

Um festzulegen, ob und wie Daten kollokiert werden, führen Sie die folgenden Schritte aus:

1. Legen Sie fest, wie Daten zusammengefasst werden sollen, ob nach Clientknoten, nach Clientknotengruppe oder nach Dateibereich. Bei der Kollokation nach Gruppe müssen Sie entscheiden, wie Knoten in Gruppen zusammengefasst werden sollen:
   - Wenn das Einsparen von Speicherbereich das Ziel ist, möchten Sie möglicherweise kleine Knoten in einer Gruppe zusammenfassen, um Bänder besser zu nutzen.
   - Wenn schnellere Clientzurückschreibungen das Ziel sind, gruppieren Sie Knoten so, dass sie möglichst viele Bänder füllen. Indem Knoten in Gruppen zusammengefasst werden, werden die Daten der einzelnen Knoten auf zwei oder mehr Bänder verteilt und es können mehr Bänder während einer Mehrfachsitzung für eine Zurückschreibungsoperation ohne Abfrage gleichzeitig bereitgestellt werden.
   - Wenn die Aufteilung der Daten nach Abteilung das Ziel ist, können Sie Knoten nach Abteilung gruppieren.
2. Um Gruppen zu kollokieren, führen Sie die folgenden Schritte aus:
   a. Definieren Sie Kollokationsgruppen mit dem Befehl DEFINE COLLOCGROUP.
   b. Fügen Sie den Kollokationsgruppen mit dem Befehl DEFINE COLLOCMEMBER Clientknoten hinzu.

   Die folgenden Abfragebefehle sind zum Kollokieren von Gruppen verfügbar:

   QUERY COLLOCGROUP
   : Zeigt die Kollokationsgruppen an, die auf dem Server definiert sind.

   QUERY NODE
   : Zeigt die Kollokationsgruppe an (falls vorhanden), zu der ein Knoten gehört.

   QUERY NODEDATA
   : Zeigt Informationen zu den Daten für einen oder mehrere Knoten in einem Speicherpool mit sequenziellem Zugriff an.

   QUERY STGPOOL

Zeigt Informationen zur Position von Clientdaten in einem Speicherpool mit sequenziellem Zugriff und zum Umfang des Speicherbereichs an, den ein Knoten auf einem Datenträger belegt.

Sie können auch IBM Spectrum Protect-Server-Scripts oder PERL-Scripts verwenden, um Informationen anzuzeigen, die beim Definieren von Kollokationsgruppen hilfreich sein können.

3. Geben Sie an, wie Daten in einem Speicherpool kollokiert werden müssen, indem Sie den Befehl DEFINE STGPOOL oder UPDATE STGPOOL unter Angabe des Parameters COLLOCATE ausgeben.

Nächste Schritte

Tipp: Um die Anzahl Datenträgermounts zu reduzieren, Speicherbereich auf sequenziellen Datenträgern effizienter zu verwenden und die Kollokation zu aktivieren, führen Sie die folgenden Schritte aus:

- Definieren Sie eine Speicherpoolhierarchie und eine Maßnahme, die erfordert, dass gesicherte, archivierte oder speicherverwaltete Dateien anfänglich in Plattenspeicherpools gespeichert werden.

  Wenn Dateien aus einem Plattenspeicherpool umgelagert werden, versucht der Server, alle Dateien umzulagern, die zu dem Clientknoten oder zu der Kollokationsgruppe gehören, der bzw. die den meisten Plattenspeicherplatz in dem Speicherpool belegt. Dieser Prozess funktioniert gut mit der Kollokationsoption, da der Server versucht, alle Dateien eines bestimmten Clients auf demselben Speicherdatenträger mit sequenziellem Zugriff zu speichern.

- Verwenden Sie Arbeitsdatenträger für Speicherpools mit sequenziellem Zugriff, damit der Server neue Datenträger für die Kollokation auswählen kann.
- Geben Sie die Clientoption COLLOCATEBYFILESPEC an, um die Anzahl Bänder zu begrenzen, auf die Objekte, die einer einzelnen Dateispezifikation zugeordnet sind, geschrieben werden. Diese Kollokationsoption hat eine effizientere Kollokation durch den Server zur Folge; diese Kollokationsoption überschreibt nicht die Kollokation nach Dateibereich oder die Kollokation nach Knoten.

Bandeinheiten verwalten

Routinemäßige Bandoperationen umfassen die Vorbereitung von Banddatenträgern für die Verwendung, die Steuerung, wie und wann Datenträger wiederverwendet werden, und die Sicherstellung, dass genügend Datenträger verfügbar sind. Außerdem müssen Sie auf Bedieneranforderungen antworten und Speicherarchive, Laufwerke, Pfade und Einheiten zum Versetzen von Daten verwalten.

- Austauschbare Datenträger vorbereiten
  Sie müssen austauschbare Datenträger vorbereiten, bevor sie zum Speichern von Daten verwendet werden können. Typische Vorbereitungstasks umfassen das Zuordnen von Kennsätzen und das Zurückstellen von Datenträgern.
- Datenträgerbestand verwalten
  Sie können den Datenträgerbestand verwalten, indem Sie den Zugriff des Servers auf Datenträger steuern, Bänder wiederverwenden und Datenträger wiederverwenden, die für Datenbanksicherungs- und Exportoperationen verwendet werden. Sie können den Bestand auch verwalten, indem Sie einen Vorrat an Arbeitsdatenträgern bereithalten.
- Teilweise beschriebene Datenträger
  Teilweise beschriebene Datenträger sind immer private Datenträger; dies ist auch dann der Fall, wenn ihr Status vor dem Bereitstellen durch den Server PRIVATE lautete. Der Server protokolliert den ursprünglichen Status von Arbeitsdatenträgern und versetzt diese wieder in den Arbeitsstatus, wenn sie leer sind.
- Operationen für gemeinsam genutzte Speicherarchive
  Gemeinsam genutzte Speicherarchive sind logische Speicherarchive, die physisch durch SCSI-Speicherarchive dargestellt werden. Das physische Speicherarchiv wird durch den IBM Spectrum Protect-Server gesteuert, der als Speicherarchivmanager konfiguriert ist. IBM Spectrum Protect-Server, die den Speicherarchivtyp SHARED verwenden, sind Speicherarchivclients für den IBM Spectrum Protect-Speicherarchivmanager-Server.
- Serveranforderungen für Datenträger verwalten
  IBM Spectrum Protect zeigt allen Verwaltungsbefehlszeilenclients, die im Konsolenmodus gestartet werden, Anforderungen und Statusnachrichten an. Für diese Anforderungsnachrichten ist häufig ein Zeitlimit festgelegt. Erfolgreiche Serveroperationen müssen innerhalb des angegebenen Zeitlimits abgeschlossen werden; andernfalls tritt für die Operation eine Zeitlimitüberschreitung auf.

Austauschbare Datenträger vorbereiten

Sie müssen austauschbare Datenträger vorbereiten, bevor sie zum Speichern von Daten verwendet werden können. Typische Vorbereitungstasks umfassen das Zuordnen von Kennsätzen und das Zurückstellen von Datenträgern.

Informationen zu diesem Vorgang

Wenn IBM Spectrum Protect auf einen austauschbaren Datenträger zugreift, wird der Datenträgername im Kennsatzheader geprüft, um sicherzustellen, dass auf den korrekten Datenträger zugegriffen wird.

Banddatenträgern müssen Kennsätze zugeordnet werden, bevor sie vom Server verwendet werden können.

Vorgehensweise

Um einen Datenträger für die Verwendung vorzubereiten, führen Sie die folgenden Schritte aus:

1. Ordnen Sie dem Datenträger einen Kennsatz zu, indem Sie den Befehl LABEL LIBVOLUME ausgeben.
2. Stellen Sie bei automatisierten Speicherarchiven den Datenträger in das Speicherarchiv zurück. Anweisungen finden Sie in Datenträger in ein automatisiertes Speicherarchiv zurückstellen.
   Tipp: Wenn Sie den Befehl LABEL LIBVOLUME für Laufwerke in einem automatisierten Speicherarchiv verwenden, ist es mit einem einzigen Befehl möglich, den Datenträgern Kennsätze zuzuordnen und die Datenträger zurückzustellen.
3. Wenn der Speicherpool keine Arbeitsdatenträger enthalten kann (`MAXSCRATCH=0`), identifizieren Sie den Datenträger in IBM Spectrum Protect anhand des Namens, damit später auf den Datenträger zugegriffen werden kann.

   Wenn der Speicherpool Arbeitsdatenträger enthalten kann (MAXSCRATCH ist auf einen Wert ungleich null gesetzt), überspringen Sie diesen Schritt.

- Banddatenträgern Kennsätze zuordnen
  Sie müssen Banddatenträgern Kennsätze zuordnen, bevor diese vom Server verwendet werden können.
- Datenträger in ein automatisiertes Speicherarchiv zurückstellen
  Sie können einen Datenträger mithilfe des Befehls CHECKIN LIBVOLUME in ein automatisiertes Speicherarchiv zurückstellen.

Banddatenträgern Kennsätze zuordnen

Sie müssen Banddatenträgern Kennsätze zuordnen, bevor diese vom Server verwendet werden können.

Informationen zu diesem Vorgang

Bei automatisierten Speicherarchiven werden Sie zum Einlegen des Datenträgers in den Eingangs-/Ausgangsschacht des Speicherarchivs aufgefordert. Wenn keine Serviceein-/-ausgabestation verfügbar ist, legen Sie den Datenträger in einen leeren Schacht ein. Sie können den Datenträgern Kennsätze zuordnen, wenn Sie die Datenträger zurückstellen oder bevor Sie die Datenträger zurückstellen.

Vorgehensweise

Um Banddatenträgern Kennsätze zuzuordnen, bevor sie zurückgestellt werden, führen Sie die folgenden Schritte aus:

1. Ordnen Sie Banddatenträgern Kennsätze zu, indem Sie den Befehl LABEL LIBVOLUME ausgeben. Um beispielsweise einem Datenträger in einem Speicherarchiv mit dem Namen LIBRARY1 den Namen VOLUME1 zuzuordnen, geben Sie den folgenden Befehl aus:

   ```
   label libvolume library1 volume1
   ```

   Voraussetzung: Es muss mindestens ein Laufwerk verfügbar sein. Das Laufwerk darf nicht von einem anderen IBM Spectrum Protect-Prozess verwendet werden. Wenn ein Laufwerk inaktiv ist, wird das Laufwerk als nicht verfügbar betrachtet.
2. Um einen vorhandenen Kennsatz zu überschreiben, geben Sie den Parameter `OVERWRITE=YES` an. Standardmäßig wird ein vorhandener Kennsatz mit dem Befehl LABEL LIBVOLUME nicht überschrieben.

- Datenträgern in einem SCSI-Speicherarchiv Kennsätze zuordnenSpeicherarchiv
  Sie können Datenträgern einzeln einen Kennsatz zuordnen oder das Speicherarchiv mithilfe von IBM Spectrum Protect durchsuchen und den gefundenen Datenträgern Kennsätze zuordnen.

Zugehörige Tasks:
Neuen Datenträgern mit AUTOLABEL Kennsätze zuordnen
Zugehörige Verweise:
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

Datenträger in ein automatisiertes Speicherarchiv zurückstellen

Sie können einen Datenträger mithilfe des Befehls CHECKIN LIBVOLUME in ein automatisiertes Speicherarchiv zurückstellen.

Vorbereitende Schritte

Um Bändern automatisch Kennsätze zuzuordnen, bevor sie zurückgestellt werden, geben Sie den Befehl DEFINE LIBRARY unter Angabe des Parameters AUTOLABEL=YES aus. Wenn der Parameter AUTOLABEL verwendet wird, entfällt die Notwendigkeit, einer Gruppe von Bändern vorab Kennsätze zuordnen zu müssen.

Informationen zu diesem Vorgang

Jeder Datenträger, der von einem Server für einen beliebigen Zweck verwendet wird, muss einen eindeutigen Namen haben. Diese Voraussetzung gilt für alle Datenträger, unabhängig davon, ob die Datenträger für Speicherpools oder für Operationen wie beispielsweise Datenbanksicherung oder Export verwendet werden. Die Voraussetzung gilt auch für Datenträger, die sich in unterschiedlichen Speicherarchiven befinden, aber von demselben Server verwendet werden.

Tipps:

- Verwenden Sie nicht ein einzelnes Speicherarchiv für Datenträger mit Barcodeetiketten und Datenträger ohne Barcodeetiketten. Das Scannen von Barcodes kann bei Datenträgern ohne Kennsatz lange dauern.
- Der Server akzeptiert nur Bänder, denen IBM® Standardkennsätze zugeordnet wurden.
- Jeder Datenträger mit einem Barcode, der mit `CLN` beginnt, wird als Reinigungsband betrachtet.
- Wenn für einen Datenträger ein Eintrag im Datenträgerprotokoll vorhanden ist, kann der Datenträger nicht als Arbeitsdatenträger zurückgestellt werden.

Vorgehensweise

1. Um einen Speicherdatenträger in ein Speicherarchiv zurückzustellen, geben Sie den Befehl CHECKIN LIBVOLUME aus.
   Tipp: Der Befehl wird immer als Hintergrundprozess ausgeführt. Warten Sie, bis die Verarbeitung des Prozesses CHECKIN LIBVOLUME abgeschlossen ist, bevor Sie Datenträger definieren; andernfalls schlägt der Definitionsprozess fehl. Sie können Zeit sparen, indem Sie Datenträger im Rahmen der Operation zum Zuordnen von Kennsätzen zurückstellen.
2. Geben Sie den Namen des Speicherarchivs an und geben Sie an, ob es sich bei dem Datenträger um einen privaten Datenträger oder einen Arbeitsdatenträger handelt. Führen Sie abhängig davon, ob Sie Arbeitsdatenträger oder private Datenträger verwenden, einen der folgenden Schritte aus:
   - Wenn Sie nur Arbeitsdatenträger verwenden, stellen Sie sicher, dass genügend Arbeitsdatenträger verfügbar sind. Beispielsweise müssen Sie gegebenenfalls weiteren Datenträgern Kennsätze zuordnen. In dem Maße, wie Datenträger verwendet werden, müssen Sie unter Umständen auch die Anzahl zulässiger Arbeitsdatenträger in dem Speicherpool erhöhen, der für dieses Speicherarchiv definiert wurde.
   - Wenn private Datenträger zusätzlich zu oder anstelle von Arbeitsdatenträgern in dem Speicherarchiv verwendet werden sollen, definieren Sie Datenträger für den Speicherpool mithilfe des Befehls DEFINE VOLUME. Sie müssen den Datenträgern, die Sie definieren, Kennsätze zuordnen und die Datenträger zurückstellen.

- Einzelnen Datenträger in ein SCSI-Speicherarchiv zurückstellen
  Sie können einen einzelnen Datenträger zurückstellen, indem Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SEARCH=NO ausgeben. IBM Spectrum Protect fordert den Bediener, der den Mount durchführt, dazu auf, den Datenträger in den Eingangs-/Ausgangsport des Speicherarchivs zu laden.
- Datenträger aus Speicherarchivspeicherschächten zurückstellen
  Wenn viele Datenträger zurückgestellt werden müssen und verhindert werden soll, dass für jeden Datenträger ein Befehl CHECKIN LIBVOLUME ausgegeben werden muss, können Sie Speicherschächte nach neuen Datenträgern durchsuchen. Der Server findet Datenträger, die dem Datenträgerbestand noch nicht hinzugefügt wurden.
- Datenträger aus Eingangs-/Ausgangsports eines Speicherarchivs zurückstellen
  Sie können alle Schächte von Masseneingangs-/-ausgangsports nach Datenträgern mit Kennsätzen durchsuchen und der Server kann diese automatisch zurückstellen.
- Datenträger mithilfe von Barcodelesern in Speicherarchiven zurückstellen
  Sie können Zeit sparen, wenn Sie Datenträger in Speicherarchive mit Barcodelesern zurückstellen, indem Sie die Zeichen auf den Barcodeetiketten als Namen für die Datenträger verwenden.
- Datenträger mithilfe eines Barcodelesers zurückstellen
  Sie können Zeit sparen, wenn Sie Datenträger mithilfe eines Barcodelesers zurückstellen, vorausgesetzt, Ihr Speicherarchiv verfügt über einen Barcodeleser.
- Datenträger mit der Auslagerungsfunktion in ein volles Speicherarchiv zurückstellen
  Wenn beim Zurückstellen von Datenträgern keine leeren Schächte in dem Speicherarchiv verfügbar sind, schlägt die Zurückstelloperation fehl, es sei denn, Sie aktivieren die *Auslagerungsfunktion*. Wenn Sie die Auslagerungsfunktion aktivieren und das Speicherarchiv voll ist, wählt der Server einen Datenträger zum Ausgeben aus und stellt dann den angeforderten Datenträger zurück.
- Windows-BetriebssystemePrivate Datenträger und Arbeitsdatenträger
  Lesen Sie zur Optimierung von Bandspeicher die Informationen zu privaten Datenträgern und Arbeitsdatenträgern. Verwenden Sie private Datenträger und Arbeitsdatenträger dementsprechend.
- Windows-BetriebssystemeElementadressen für Speicherarchivspeicherschächte
  Eine Elementadresse ist eine Zahl, die die physische Position eines Speicherschachts oder Laufwerks in einem automatisierten Speicherarchiv angibt.

Zugehörige Tasks:
Banddatenträgern Kennsätze zuordnen

Einzelnen Datenträger in ein SCSI-Speicherarchiv zurückstellen

Sie können einen einzelnen Datenträger zurückstellen, indem Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SEARCH=NO ausgeben. IBM Spectrum Protect fordert den Bediener, der den Mount durchführt, dazu auf, den Datenträger in den Eingangs-/Ausgangsport des Speicherarchivs zu laden.

Vorgehensweise

1. Geben Sie den Befehl CHECKIN LIBVOLUME aus.

   Um beispielsweise den Datenträger VOL001 zurückzustellen, geben Sie den folgenden Befehl ein:

   ```
   checkin libvolume tapelib vol001 search=no status=scratch
   ```

2. Antworten Sie auf die Eingabeaufforderung des Servers.
   - Wenn das Speicherarchiv über einen Eingangs-/Ausgangsport verfügt, werden Sie zum Einlegen eines Bands in den Eingangs-/Ausgangsport aufgefordert.
   - Wenn das Speicherarchiv über keinen Eingangs-/Ausgangsport verfügt, werden Sie zum Einlegen eines Bands in einen der Schächte im Speicherarchiv aufgefordert. Diese Schächte werden durch Elementadressen angegeben. Wenn der Server beispielsweise erkennt, dass der erste leere Schacht die Elementadresse 5 hat, wird die folgende Nachricht zurückgegeben:

     ```
     ANR8306I 001: 8MM-Datenträger VOL001 R/W innerhalb von 60 Minuten
     in Schacht mit Elementnummer 5 in Kassettenarchiv TAPELIB einlegen;
     wenn bereit, 'REPLY' zusammen mit der Anforderungs-ID ausgeben.
     ```

     Wenn Sie die Position von Elementadresse 5 in dem Speicherarchiv nicht kennen, überprüfen Sie das Arbeitsblatt auf die Einheit. Angaben zur Lokalisation des Arbeitsblattes enthält die Dokumentation zu Ihrem Speicherarchiv. Nachdem Sie den Datenträger wie angefordert eingelegt haben, antworten Sie auf die Nachricht von einem IBM Spectrum Protect-Verwaltungsclient. Geben Sie den Befehl REPLY gefolgt von der Anforderungsnummer (die Nummer am Anfang der Mountanforderung) aus, beispielsweise:

     ```
     reply 1
     ```

     Tipp: Elementadressen beginnen nicht notwendigerweise mit der Zahl 1. Überprüfen Sie das Arbeitsblatt dahingehend. Wenn für Ihre Einheit im IBM® Support Portal for IBM Spectrum Protect kein Arbeitsblatt aufgelistet ist, ziehen Sie die Dokumentation zu Ihrem Speicherarchiv zu Rate.

Wenn Sie über den optionalen Parameter WAITTIME im Befehl CHECKIN LIBVOLUME eine Wartezeit von 0 angeben, ist kein Befehl REPLY erforderlich. Die Standardwartezeit beträgt 60 Minuten.

Datenträger aus Speicherarchivspeicherschächten zurückstellen

Wenn viele Datenträger zurückgestellt werden müssen und verhindert werden soll, dass für jeden Datenträger ein Befehl CHECKIN LIBVOLUME ausgegeben werden muss, können Sie Speicherschächte nach neuen Datenträgern durchsuchen. Der Server findet Datenträger, die dem Datenträgerbestand noch nicht hinzugefügt wurden.

Vorgehensweise

1. Öffnen Sie das Speicherarchiv und legen Sie die neuen Datenträger in freie Schächte ein. Öffnen Sie beispielsweise bei einer SCSI-Einheit die Zugangstür des Speicherarchivs, legen Sie alle neuen Datenträger in freie Schächte ein und schließen Sie die Zugangstür.
2. Wenn den Datenträgern kein Kennsatz zugeordnet ist, ordnen Sie dem Datenträger mit dem Befehl LABEL LIBVOLUME einen Kennsatz zu.
3. Geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SEARCH=YES aus.

Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Datenträger aus Eingangs-/Ausgangsports eines Speicherarchivs zurückstellen

Sie können alle Schächte von Masseneingangs-/-ausgangsports nach Datenträgern mit Kennsätzen durchsuchen und der Server kann diese automatisch zurückstellen.

Vorbereitende Schritte

Geben Sie den Befehl LABEL LIBVOLUME aus, um allen Datenträgern ohne Kennsatz einen Kennsatz zuzuordnen.

Informationen zu diesem Vorgang

Bei SCSI-Speicherarchiven durchsucht der Server alle Eingangs-/Ausgangsports in dem Speicherarchiv nach Datenträgern. Wenn ein Datenträger gefunden wird, der einen gültigen Datenträgerkennsatz enthält, wird der Datenträger automatisch zurückgestellt.

Vorgehensweise

Geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SEARCH=BULK aus.

- Um ein Band in ein Laufwerk zu laden und den Kennsatz zu lesen, geben Sie den Parameter CHECKLABEL=YES an. Nachdem der Kennsatz vom Server gelesen wurde, versetzt der Server das Band aus dem Laufwerk in einen Speicherschacht.
- Damit der Server den Barcodeleser zur Überprüfung externer Kennsätze auf Bändern verwendet, geben Sie den Parameter CHECKLABEL=BARCODE an. Wenn das Lesen von Barcodes aktiviert ist, liest der Server den Kennsatz und versetzt das Band aus dem Eingangs-/Ausgangsport in einen Speicherschacht.

Datenträger mithilfe von Barcodelesern in Speicherarchiven zurückstellen

Sie können Zeit sparen, wenn Sie Datenträger in Speicherarchive mit Barcodelesern zurückstellen, indem Sie die Zeichen auf den Barcodeetiketten als Namen für die Datenträger verwenden.

Informationen zu diesem Vorgang

Der Server liest die Barcodeetiketten und verwendet die Informationen zum Schreiben der internen Datenträgerkennsätze. Bei Datenträgern ohne Barcodeetiketten stellt der Server die Datenträger in einem Laufwerk bereit und versucht, den internen aufgezeichneten Kennsatz zu lesen.

Vorgehensweise

Geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters CHECKLABEL=BARCODE aus. Um beispielsweise mithilfe eines Barcodelesers ein Speicherarchiv mit dem Namen TAPELIB zu durchsuchen und ein Arbeitsband zurückzustellen, geben Sie den folgenden Befehl aus:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Datenträger mithilfe eines Barcodelesers zurückstellen

Sie können Zeit sparen, wenn Sie Datenträger mithilfe eines Barcodelesers zurückstellen, vorausgesetzt, Ihr Speicherarchiv verfügt über einen Barcodeleser.

Informationen zu diesem Vorgang

Wenn Sie einen Datenträger zurückstellen, können Sie angeben, ob die Datenträgerkennsätze während der Zurückstellungsverarbeitung gelesen werden sollen. Wenn die Kennsatzprüfung aktiviert ist, stellt IBM Spectrum Protect jeden Datenträger bereit, um den internen Kennsatz zu lesen, und stellt einen Datenträger nur dann zurück, wenn der Kennsatz korrekt ist. Mithilfe der Kennsatzprüfung können zukünftige Fehler verhindert werden, wenn Datenträger in Speicherpools verwendet werden; dadurch verlängert sich jedoch die Verarbeitungszeit beim Zurückstellen.

Wenn ein Datenträger kein Barcodeetikett hat, stellt IBM Spectrum Protect die Datenträger in einem Laufwerk bereit und versucht, den aufgezeichneten Kennsatz zu lesen.

Vorgehensweise

Um Datenträger mithilfe eines Barcodelesers zurückzustellen, geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe von CHECKLABEL=BARCODE aus. Um beispielsweise mithilfe des Barcodelesers alle Datenträger als Arbeitsdatenträger in ein Speicherarchiv mit dem Namen TAPELIB zurückzustellen, geben Sie den folgenden Befehl aus:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

Zugehörige Tasks:
Austauschbare Datenträger vorbereiten
Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Datenträger mit der Auslagerungsfunktion in ein volles Speicherarchiv zurückstellen

Wenn beim Zurückstellen von Datenträgern keine leeren Schächte in dem Speicherarchiv verfügbar sind, schlägt die Zurückstelloperation fehl, es sei denn, Sie aktivieren die *Auslagerungsfunktion*. Wenn Sie die Auslagerungsfunktion aktivieren und das Speicherarchiv voll ist, wählt der Server einen Datenträger zum Ausgeben aus und stellt dann den angeforderten Datenträger zurück.

Informationen zu diesem Vorgang

Bei der Auswahl des auszugebenden Datenträgers prüft der Server zunächst, ob ein verfügbarer Arbeitsdatenträger vorhanden ist und sucht dann nach dem Datenträger mit der geringsten Anzahl Mounts. Der Server gibt den für die Auslagerungsoperation ausgewählten Datenträger aus dem Speicherarchiv aus und ersetzt ihn durch den Datenträger, der zurückgestellt wird.

Vorgehensweise

Um Datenträger auszulagern, wenn kein leerer Speicherarchivschacht zum Zurückstellen eines Datenträgers verfügbar ist, geben Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters SWAP=YES aus. Um beispielsweise einen Datenträger mit dem Namen `VOL1` in ein Speicherarchiv mit dem Namen AUTO zurückzustellen und die Auslagerungsfunktion zu aktivieren, geben Sie den folgenden Befehl aus:

```
checkin libvolume auto vol1 swap=yes
```

Zugehörige Tasks:
Volles Speicherarchiv mit einer Überlaufposition verwalten
Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Private Datenträger und Arbeitsdatenträger

Lesen Sie zur Optimierung von Bandspeicher die Informationen zu privaten Datenträgern und Arbeitsdatenträgern. Verwenden Sie private Datenträger und Arbeitsdatenträger dementsprechend.

Private Datenträger können nicht überschrieben werden, wenn die Bereitstellung eines Arbeitsdatenträgers angefordert wird. Sie können einen Datenträger im Arbeitsstatus nicht zurückstellen, wenn dieser Datenträger von einem Speicherpool verwendet wird, um Daten zu exportieren, eine Datenbank zu sichern oder einen Sicherungsgruppendatenträger zu sichern.

Teilweise beschriebene Datenträger sind immer private Datenträger. Datenträger haben entweder den Status SCRATCH (Arbeitsdatenträger) oder PRIVATE (privater Datenträger); wenn IBM Spectrum Protect jedoch Daten auf ihnen speichert, wird ihnen der Status PRIVATE zugeordnet.

Tabelle 1. Verwendung privater Datenträger und Arbeitsdatenträger

Datenträgertyp	Verwendung
Private Datenträger	Verwenden Sie private Datenträger, um die von einzelnen Speicherpools verwendeten Datenträger festzulegen und die Datenträger manuell zu steuern. Geben Sie zum Definieren privater Datenträger den Befehl DEFINE VOLUME aus. Bei Zurückschreibungen, Hauptspeicherauszügen oder Ladevorgängen für Datenbanken oder bei Serverimportoperationen müssen Sie private Datenträger angeben.
Arbeitsdatenträger	In einigen Fällen können Sie die Datenträgerverwaltung durch Verwendung von Arbeitsdatenträgern vereinfachen. Arbeitsdatenträger können unter den folgenden Bedingungen verwendet werden: • Es ist nicht erforderlich, jeden einzelnen Speicherpooldatenträger zu definieren. • Die Vorteile der Automatisierung automatischer Einheiten sollen genutzt werden. • Verschiedene Speicherpools nutzen ein automatisiertes Speicherarchiv gemeinsam und die Speicherpools können Datenträger dynamisch von den Arbeitsdatenträgern in dem Speicherarchiv anfordern. Die Datenträger müssen den Speicherpools nicht vorab zugeordnet werden.

Zugehörige Tasks:
Status eines Datenträgers in einem automatisierten Speicherarchiv ändern
Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
DELETE VOLUME (Speicherpooldatenträger löschen)

Elementadressen für Speicherarchivspeicherschächte

Eine Elementadresse ist eine Zahl, die die physische Position eines Speicherschachts oder Laufwerks in einem automatisierten Speicherarchiv angibt.

Wenn ein Speicherarchiv über Eingangs-/Ausgangsports verfügt, können Sie Datenträger unter Verwendung der Ports hinzufügen und entfernen. Wenn keine Eingangs-/Ausgangsports vorhanden sind, müssen Sie Bänder in Speicherschächte laden.

Wenn Sie Bänder in Speicherschächte laden, müssen Sie auf Mountanforderungen antworten, die Speicherschächte mit Elementadressen angeben. Wenn Sie im Befehl CHECKIN LIBVOLUME oder im Befehl LABEL LIBVOLUME eine Wartezeit von 0 angeben, müssen Sie nicht auf eine Mountanforderung antworten.

Informationen zu Elementadressen finden Sie in der Dokumentation des Einheitenherstellers oder bei der Suche nach Elementadressen im IBM® Support Portal for IBM Spectrum Protect.

Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)

Datenträgerbestand verwalten

Sie können den Datenträgerbestand verwalten, indem Sie den Zugriff des Servers auf Datenträger steuern, Bänder wiederverwenden und Datenträger wiederverwenden, die für Datenbanksicherungs- und Exportoperationen verwendet werden. Sie können den Bestand auch verwalten, indem Sie einen Vorrat an Arbeitsdatenträgern bereithalten.

Informationen zu diesem Vorgang

Jeder Datenträger, der von einem Server verwendet wird, muss - unabhängig davon, ob die Datenträger für Speicherpools oder für Operationen wie beispielsweise Datenbanksicherung oder Export verwendet werden - einen eindeutigen Namen haben. Auch Datenträger, die sich in unterschiedlichen Speicherarchiven befinden, aber von demselben Server verwendet werden, müssen einen eindeutigen Namen haben.

- Zugriff auf Datenträger steuern
  Sie können verschiedene Methoden verwenden, um den Zugriff auf Datenträger zu steuern.
- Bänder wiederverwenden
  Um sicherzustellen, dass immer ein ausreichender Vorrat an Bändern verfügbar ist, können Sie alte Dateien verfallen lassen, Datenträger konsolidieren und Datenträger, die das Ende des Lebenszyklus erreicht haben, löschen. Sie können auch einen Vorrat an Arbeitsdatenträgern bereithalten.
- Vorrat an Arbeitsdatenträgern bereithalten
  Sie müssen die die maximale Anzahl Arbeitsdatenträger für einen Speicherpool auf einen entsprechend hohen Wert setzen, um dem erwarteten Bedarf gerecht zu werden.
- AIX-BetriebssystemeLinux-BetriebssystemeVorrat an Datenträgern in einem Speicherarchiv mit WORM-Datenträgern bereithalten
  Bei Speicherarchiven, die WORM-Datenträger (WORM = Write Once Read Many) enthalten, können Sie den Abbruch von Datenspeicherungstransaktionen verhindern, indem Sie einen Vorrat an Arbeitsdatenträgern oder neuen privaten Datenträgern in dem Speicherarchiv bereithalten. Abgebrochene Transaktionen können zur Folge haben, dass WORM-Datenträger verschwendet werden.
- Datenträgerbestand in automatisierten Speicherarchiven verwalten
  Der IBM Spectrum Protect-Server verwendet den Datenträgerbestand eines Speicherarchivs, um Arbeitsdatenträger und private Datenträger, die in einem automatisierten Speicherarchiv verfügbar sind, zu verfolgen. Sie müssen sicherstellen, dass der Bestand mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind.

Zugriff auf Datenträger steuern

Sie können verschiedene Methoden verwenden, um den Zugriff auf Datenträger zu steuern.

Vorgehensweise

Um den Zugriff auf Datenträger zu steuern, führen Sie eine der folgenden Aktionen aus:

- Um zu verhindern, dass der Server einen Datenträger bereitstellt, geben Sie den Befehl UPDATE VOLUME unter Angabe des Parameters ACCESS=UNAVAILABLE aus.
- Um Datenträger nicht verfügbar zu machen und zum Schutz an einen anderen Standort zu senden, verwenden Sie einen Kopienspeicherpool oder einen Speicherpool für aktive Daten.
- Sie können primäre Speicherpools in einem Kopienspeicherpool sichern und dann die Kopienspeicherpooldatenträger auslagern.
- Sie können aktive Versionen von Clientsicherungsdaten in Speicherpools für aktive Daten kopieren und dann die Datenträger auslagern.
- Sie können Kopienspeicherpooldatenträger und Datenträger in Pools für aktive Daten verfolgen, indem Sie ihren Zugriffsmodus in OFFSITE ändern und das Datenträgerprotokoll aktualisieren, um ihren Standort zu identifizieren.

Zugehörige Verweise:
UPDATE VOLUME (Speicherpooldatenträger aktualisieren)

Bänder wiederverwenden

Um sicherzustellen, dass immer ein ausreichender Vorrat an Bändern verfügbar ist, können Sie alte Dateien verfallen lassen, Datenträger konsolidieren und Datenträger, die das Ende des Lebenszyklus erreicht haben, löschen. Sie können auch einen Vorrat an Arbeitsdatenträgern bereithalten.

Informationen zu diesem Vorgang

Im Laufe der Zeit altern Datenträger und ein Teil der auf den Datenträgern gespeicherten Sicherungsdaten wird unter Umständen nicht mehr benötigt. Sie können Servermaßnahmen definieren, um festzulegen, wie viele Sicherungsversionen und wie lange Sicherungsversionen aufbewahrt werden sollen. Mithilfe der Verfallsverarbeitung können Dateien, die nicht mehr erforderlich sind, gelöscht werden. Sie können die erforderlichen Daten auf den Datenträgern beibehalten. Wenn die Daten nicht mehr benötigt werden, können Sie die Datenträger konsolidieren und wiederverwenden.

Vorgehensweise

1. Löschen Sie nicht benötigte Clientdaten durch regelmäßige Ausführung der Verfallsverarbeitung. Bei der Verfallsverarbeitung werden Daten gelöscht, die nicht mehr gültig sind, da sie den in der Maßnahme angegebenen Aufbewahrungszeitraum überschreiten oder da Benutzer oder Administratoren die aktiven Versionen der Daten gelöscht haben.
2. Verwenden Sie Datenträger in Speicherpools wieder, indem Sie die Konsolidierungsverarbeitung ausführen.

   Bei der Konsolidierungsverarbeitung werden alle nicht verfallenen Daten konsolidiert, indem sie von mehreren Datenträgern auf eine geringere Anzahl Datenträger versetzt werden. Die Datenträger können dann wieder in den Speicherpool gestellt und wiederverwendet werden.

3. Verwenden Sie Datenträger wieder, die veraltete Datenbanksicherungen oder exportierte Daten enthalten, die nicht mehr erforderlich sind, indem Sie das Datenträgerprotokoll löschen.

   Bevor der Server Datenträger wiederverwenden kann, die im Datenträgerprotokoll protokolliert sind, müssen Sie die Datenträgerinformationen durch Ausgabe des Befehls DELETE VOLHISTORY aus der Protokolldatei für Datenträger löschen.

   Tipp: Wenn Ihr Server die Funktion Disaster Recovery Manager (DRM) verwendet, werden die Datenträgerinformationen automatisch während der Verarbeitung des Befehls MOVE DRMEDIA gelöscht.
4. Legen Sie fest, wann Banddatenträger das Ende des Lebenszyklus erreichen. Mithilfe des Servers können Sie Statistikdaten zu Datenträgern anzeigen, die die Anzahl Schreiboperationen für die Datenträger und die Anzahl Schreibfehler umfassen. Für private Datenträger und Arbeitsdatenträger werden die folgenden statistischen Daten angezeigt:

   Private Datenträger
   : Bei Datenträgern, die anfänglich als private Datenträger definiert wurden, werden diese statistischen Daten vom Server selbst dann beibehalten, wenn der Datenträger konsolidiert wird. Sie können die Informationen mit der vom Hersteller empfohlenen Anzahl Schreiboperationen und Schreibfehler vergleichen.

   Arbeitsdatenträger
   : Bei Datenträgern, die anfänglich als Arbeitsdatenträger definiert wurden, überschreibt der Server diese statistischen Daten bei jeder Konsolidierung der Datenträger.

5. Konsolidieren Sie alle gültigen Daten von Datenträgern, die das Ende des Lebenszyklus erreicht haben. Wenn sich die Datenträger in automatisierten Speicherarchiven befinden, entnehmen Sie diese aus dem Datenträgerbestand. Löschen Sie private Datenträger mit dem Befehl DELETE VOLUME aus der Datenbank.
6. Stellen Sie sicher, dass Datenträger für die Bandrotation verfügbar sind, damit der Speicherbereich im Speicherpool nicht knapp wird. Mithilfe des Operations Center können Sie die Verfügbarkeit von Arbeitsdatenträgern überwachen. Stellen Sie sicher, dass die Anzahl Arbeitsdatenträger hoch genug ist, um den Bedarf zu decken. Weitere Informationen finden Sie in Vorrat an Datenträgern in einem Speicherarchiv mit WORM-Datenträgern bereithalten.
   WORM-Datenträger: WORM-Laufwerke (WORM = Write Once Read Many) können zur Datenträgerverschwendung führen, wenn der Server Transaktionen abbricht, da keine Datenträger zur Ausführung der Sicherungsoperation zur Verfügung stehen. Nachdem Daten vom Server auf WORM-Datenträger geschrieben wurden, kann der Speicherbereich auf den Datenträgern selbst dann nicht wiederverwendet werden, wenn die Transaktionen abgebrochen werden (beispielsweise wenn eine Sicherung wegen Datenträgerknappheit in der Einheit abgebrochen wird). Um die Verschwendung von WORM-Datenträgern zu minimieren, führen Sie die folgenden Aktionen aus:
   a. Stellen Sie sicher, dass die maximale Anzahl Arbeitsdatenträger für den Speicherpool der Einheit mindestens der Anzahl Speicherschächte in dem Speicherarchiv entspricht.
   b. Stellen Sie genügend Datenträger in den Datenträgerbestand der Einheit zurück, um dem erwarteten Bedarf gerecht zu werden.

   Wenn die meisten Sicherungsoperationen kleine Dateien betreffen, kann sich die Steuerung der Transaktionsgröße auf die Verwendung von WORM-Platten auswirken. Kleinere Transaktionen bedeuten, dass weniger Speicherbereich verschwendet wird, wenn eine Transaktion, wie beispielsweise eine Sicherungsoperation, abgebrochen werden muss. Die Transaktionsgröße wird durch die Serveroption TXNGROUPMAX und die Clientoption TXNBYTELIMIT gesteuert.

Zugehörige Tasks:
Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde
Serveranforderungen für Datenträger verwalten
Zugehörige Verweise:
DELETE VOLHISTORY (Protokolldaten sequenzieller Datenträger löschen)
DELETE VOLUME (Speicherpooldatenträger löschen)
EXPIRE INVENTORY (Bestandsverfallsverarbeitung manuell starten)
Option 'txnbytelimit'
Serveroption TXNGROUPMAX

Vorrat an Arbeitsdatenträgern bereithalten

Sie müssen die die maximale Anzahl Arbeitsdatenträger für einen Speicherpool auf einen entsprechend hohen Wert setzen, um dem erwarteten Bedarf gerecht zu werden.

Informationen zu diesem Vorgang

Wenn Sie einen Speicherpool definieren, müssen Sie die maximale Anzahl Arbeitsdatenträger angeben, die der Speicherpool verwenden kann. Der Server fordert bei Bedarf automatisch einen Arbeitsdatenträger an. Wenn die Anzahl Arbeitsdatenträger, die der Server für den Speicherpool verwendet, den angegebenen maximalen Wert überschreitet, kann der Speicherbereich im Speicherpool knapp werden.

Vorgehensweise

Wenn für einen Speicherpool mehr als die maximale Anzahl Arbeitsdatenträger erforderlich ist, können Sie eine oder beide der folgenden Aktionen ausführen:

1. Erhöhen Sie die maximale Anzahl Arbeitsdatenträger, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters MAXSCRATCH ausgeben.

2. Machen Sie Datenträger für die Wiederverwendung verfügbar, indem Sie die Verfallsverarbeitung und die Konsolidierung ausführen, um Daten auf weniger Datenträgern zu konsolidieren.
    a. Geben Sie den Befehl EXPIRE INVENTORY aus, um die Verfallsverarbeitung auszuführen.
    Tipp: Standardmäßig wird dieser Prozess täglich ausgeführt. Sie können auch die Serveroption EXPINTERVAL in der Serveroptionsdatei dsmserv.opt angeben, um die Verfallsverarbeitung automatisch auszuführen. Der Wert 0 gibt an, dass der Befehl EXPIRE INVENTORY zur Ausführung der Verfallsverarbeitung verwendet werden muss.
    b. Geben Sie den Befehl RECLAIM STGPOOL aus, um die Konsolidierungsverarbeitung auszuführen.
    Tipp: Sie können auch Konsolidierungsschwellenwerte angeben, wenn Sie den Speicherpool definieren, indem Sie den Befehl DEFINE STGPOOL verwenden und den Parameter RECLAIMPROCESS angeben.

Nächste Schritte

Wenn weitere Datenträger für zukünftige Sicherungsoperationen benötigt werden, ordnen Sie weiteren Arbeitsdatenträgern mit dem Befehl LABEL LIBVOLUME Kennsätze zu.

Zugehörige Tasks:
Vorrat an Arbeitsdatenträgern in einem automatisierten Speicherarchiv bereithalten

Zugehörige Verweise:
EXPIRE INVENTORY (Bestandsverfallsverarbeitung manuell starten)
LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
RECLAIM STGPOOL (Datenträger in einem Speicherpool mit sequenziellem Zugriff konsolidieren)
UPDATE STGPOOL (Speicherpool aktualisieren)

Vorrat an Datenträgern in einem Speicherarchiv mit WORM-Datenträgern bereithalten

Bei Speicherarchiven, die WORM-Datenträger (WORM = Write Once Read Many) enthalten, können Sie den Abbruch von Datenspeicherungstransaktionen verhindern, indem Sie einen Vorrat an Arbeitsdatenträgern oder neuen privaten Datenträgern in dem Speicherarchiv bereithalten. Abgebrochene Transaktionen können zur Folge haben, dass WORM-Datenträger verschwendet werden.

Informationen zu diesem Vorgang

IBM Spectrum Protect bricht eine Transaktion ab, wenn keine Datenträger (private Datenträger oder Arbeitsdatenträger) verfügbar sind, um die Datenspeicherungsoperation auszuführen. Nachdem IBM Spectrum Protect eine Transaktion startet, indem Daten auf einen WORM-Datenträger geschrieben werden, kann der beschriebene Bereich auf dem Datenträger selbst dann nicht wiederverwendet werden, wenn die Transaktion abgebrochen wird.

Angenommen, es sind WORM-Datenträger mit einer Speicherkapazität von jeweils 2,6 GB vorhanden und ein Client beginnt mit der Sicherung einer 12-GB-Datei. Wenn IBM Spectrum Protect keinen fünften Arbeitsdatenträger anfordern kann, nachdem vier Datenträger gefüllt wurden, bricht IBM Spectrum Protect die Sicherungsoperation ab. Die vier Datenträger, die IBM Spectrum Protect bereits mit Daten gefüllt hat, können nicht wiederverwendet werden.

Um das Abbrechen von Transaktionen auf ein Mindestmaß zu reduzieren, müssen genügend Datenträger in dem Speicherarchiv verfügbar sein, um die erwarteten Clientoperationen, wie beispielsweise Sicherungen, ausführen zu können.

Vorgehensweise

1. Stellen Sie sicher, dass der Speicherpool, der dem Speicherarchiv zugeordnet ist, über genügend Arbeitsdatenträger verfügt. Geben Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters MAXSCRATCH aus.
2. Um dem erwarteten Bedarf gerecht zu werden, stellen Sie eine ausreichende Anzahl Arbeitsdatenträger oder private Datenträger in das Speicherarchiv zurück, indem Sie den Befehl CHECKIN LIBVOLUME ausgeben.
3. Um die Transaktionsgröße zu steuern, geben Sie die Serveroption TXNGROUPMAX und die Clientoption TXNBYTELIMIT an. Wenn Ihre Clients hauptsächlich kleine Dateien speichern, kann eine Steuerung der Transaktionsgröße die Verwendung von WORM-Datenträgern beeinflussen. Bei kleineren Transaktionen wird weniger Speicherbereich verschwendet, wenn eine Transaktion, wie beispielsweise eine Sicherung, abgebrochen werden muss.

Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
UPDATE STGPOOL (Speicherpool aktualisieren)
Option 'txnbytelimit'
Serveroption TXNGROUPMAX

Datenträgerbestand in automatisierten Speicherarchiven verwalten

Der IBM Spectrum Protect-Server verwendet den Datenträgerbestand eines Speicherarchivs, um Arbeitsdatenträger und private Datenträger, die in einem automatisierten Speicherarchiv verfügbar sind, zu verfolgen. Sie müssen sicherstellen, dass der Bestand mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind.

Der Datenträgerbestand des Speicherarchivs entspricht nicht dem Datenträgerbestand jedes Speicherpools. Um dem Datenträgerbestand des Speicherarchivs einen Datenträger hinzuzufügen, stellen Sie einen Datenträger in dieses IBM Spectrum Protect-Speicherarchiv zurück.

Eine Liste der Datenträger im Datenträgerbestand des Speicherarchivs ist möglicherweise nicht mit einer Liste der Datenträger im Datenträgerbestand des Speicherpools für die Einheit identisch. Sie können beispielsweise Arbeitsdatenträger in das Speicherarchiv zurückstellen, diese aber nicht für einen Speicherpool definieren. Wenn Arbeitsdatenträger nicht für Sicherungsoperationen ausgewählt werden, können Sie private Datenträger für einen Speicherpool definieren, diese aber nicht in den Datenträgerbestand für die Einheit zurückstellen.

Um sicherzustellen, dass der Datenträgerbestand für das Serverspeicherarchiv immer korrekt ist, entnehmen Sie Datenträger, um die Datenträger physisch aus einem SCSI--Speicherarchiv zu entfernen. Wenn Sie einen Datenträger entnehmen, der von einem Speicherpool verwendet wird, verbleibt der Datenträger in dem Speicherpool. Wenn Sie den Datenträger bereitstellen müssen, während dieser entnommen ist, wird an der Konsole des Bedieners, der den Mount durchführt, eine Nachricht mit der Aufforderung, den Datenträger zurückzustellen, angezeigt. Wenn die Zurückstelloperation nicht erfolgreich ist, markiert der Server den Datenträger als nicht verfügbar.

Wenn sich ein Datenträger im Datenträgerbestand des Speicherarchivs befindet, können Sie den Status des Datenträgers von SCRATCH (Arbeitsdatenträger) in PRIVATE (privater Datenträger) ändern.

Um zu überprüfen, ob der Datenträgerbestand für das Serverspeicherarchiv mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind, können Sie das Speicherarchiv prüfen. Der Bestand kann inkonsistent werden, wenn Datenträger in das Speicherarchiv gestellt bzw. aus dem Speicherarchiv entfernt werden, ohne dass der Server über Entnahme- oder Zurückstelloperationen für Datenträger informiert wird.

- Status eines Datenträgers in einem automatisierten Speicherarchiv ändern
  Sie können den Status eines Datenträgers von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) oder umgekehrt ändern.
- Datenträger aus einem automatisierten Speicherarchiv entfernen
  Datenträger können aus einem automatisierten Speicherarchiv entfernt werden, wenn Daten auf einen Datenträger exportiert wurden und die Daten in ein anderes System importiert werden sollen. Möglicherweise sollen auch Datenträger entfernt werden, um Speicherbereich für neue Datenträger zu erstellen.
- Vorrat an Arbeitsdatenträgern in einem automatisierten Speicherarchiv bereithalten
  Wenn Sie einen Speicherpool definieren, der einem automatisierten Speicherarchiv zugeordnet ist, können Sie eine maximale Anzahl Arbeitsdatenträger angeben, die der physischen Kapazität des Speicherarchivs entspricht. Wenn der Server eine größere Anzahl Arbeitsdatenträger für den Speicherpool verwendet, müssen Sie sicherstellen, dass genügend Datenträger verfügbar sind.
- Volles Speicherarchiv mit einer Überlaufposition verwalten
  Mit zunehmendem Speicherbedarf überschreitet die Anzahl Datenträger, die für einen Speicherpool erforderlich sind, unter Umständen die physische Kapazität eines automatisierten Speicherarchivs. Um Speicherbereich für neue Datenträger verfügbar zu machen und vorhandene Datenträger zu überwachen, können Sie eine Überlaufposition für einen Speicherpool definieren.
- Datenträgerbestand in einem Speicherarchiv prüfen
  Sie können ein automatisiertes Speicherarchiv prüfen, um sicherzustellen, dass der Datenträgerbestand des Speicherarchivs mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind. Die Prüfung eines Speicherarchivs bietet sich an, wenn der Datenträgerbestand des Speicherarchivs aufgrund manueller Versetzungen der Datenträger in dem Speicherarchiv oder aufgrund von Datenbankproblemen nicht mehr korrekt ist.

Zugehörige Tasks:
Datenträger in ein automatisiertes Speicherarchiv zurückstellen
Zugehörige Verweise:
AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)

Status eines Datenträgers in einem automatisierten Speicherarchiv ändern

Sie können den Status eines Datenträgers von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) oder umgekehrt ändern.

Vorgehensweise

Um den Status eines Datenträgers zu ändern, geben Sie den Befehl UPDATE LIBVOLUME aus. Um beispielsweise den Status eines Datenträgers mit dem Namen VOL1 in PRIVATE (privater Datenträger) zu ändern, geben Sie den folgenden Befehl aus:

```
update libvolume lib1 vol1 status=private
```

Einschränkungen:

- Sie können den Status eines Datenträgers nicht von PRIVATE (privater Datenträger) in SCRATCH (Arbeitsdatenträger) ändern, wenn der Datenträger zu einem Speicherpool gehört oder in der Protokolldatei für Datenträger definiert ist.
- Private Datenträger müssen vom Administrator definierte Datenträger ohne Daten oder mit ungültigen Daten sein. Sie dürfen keine teilweise beschriebenen Datenträger sein, die aktive Daten enthalten. Die Datenträgerstatistik geht verloren, wenn der Datenträgerstatus geändert wird.

Datenträger aus einem automatisierten Speicherarchiv entfernen

Datenträger können aus einem automatisierten Speicherarchiv entfernt werden, wenn Daten auf einen Datenträger exportiert wurden und die Daten in ein anderes System importiert werden sollen. Möglicherweise sollen auch Datenträger entfernt werden, um Speicherbereich für neue Datenträger zu erstellen.

Informationen zu diesem Vorgang

Standardmäßig wird der Datenträger, der entnommen werden soll, vom Server bereitgestellt und der interne Kennsatz überprüft. Nach der Überprüfung des Kennsatzes entfernt der Server den Datenträger aus dem Datenträgerbestand des Speicherarchivs und versetzt ihn dann in den Eingangs-/Ausgangsport oder die Serviceein-/-ausgabestation des Speicherarchivs. Wenn das Speicherarchiv über keinen Eingangs-/Ausgangsport verfügt, fordert der Server den Bediener, der den Mount durchführt, dazu auf, den Datenträger aus einem Schacht oder einer Einheit in dem Speicherarchiv zu entfernen.

Vorgehensweise

- Um einen Datenträger aus einem automatisierten Speicherarchiv zu entfernen, geben Sie den Befehl CHECKOUT LIBVOLUME aus.
- Geben Sie bei automatisierten Speicherarchiven mit mehreren Eingangs-/Ausgangsports den Befehl CHECKOUT LIBVOLUME unter Angabe des Parameters REMOVE=BULK aus. Der Server gibt den Datenträger am nächsten verfügbaren Eingangs-/Ausgangsport aus.

Nächste Schritte

Wenn Sie einen Datenträger entnehmen, der in einem Speicherpool definiert ist, und der Server später auf den Datenträger zugreifen muss, fordert der Server das Zurückstellen des Datenträgers an. Um Datenträger in ein Speicherarchiv zurückzustellen, geben Sie den Befehl CHECKIN LIBVOLUME aus.

Zugehörige Verweise:

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)

Vorrat an Arbeitsdatenträgern in einem automatisierten Speicherarchiv bereithalten

Wenn Sie einen Speicherpool definieren, der einem automatisierten Speicherarchiv zugeordnet ist, können Sie eine maximale Anzahl Arbeitsdatenträger angeben, die der physischen Kapazität des Speicherarchivs entspricht. Wenn der Server eine größere Anzahl Arbeitsdatenträger für den Speicherpool verwendet, müssen Sie sicherstellen, dass genügend Datenträger verfügbar sind.

Vorgehensweise

Wenn die Anzahl Arbeitsdatenträger, die der Server für den Speicherpool verwendet, die in der Speicherpooldefinition angegebene Anzahl überschreitet, führen Sie die folgenden Schritte aus:

1. Fügen Sie dem Speicherarchiv Arbeitsdatenträger hinzu, indem Sie den Befehl CHECKIN LIBVOLUME ausgeben.
   Tipp: Möglicherweise müssen Sie eine Überlaufposition verwenden, um Datenträger aus dem Speicherarchiv zu entfernen, um Platz für diese Arbeitsdatenträger zu schaffen. Weitere Informationen finden Sie in Volles Speicherarchiv mit einer Überlaufposition verwalten.
2. Erhöhen Sie die maximale Anzahl Arbeitsdatenträger, die einem Speicherpool hinzugefügt werden können, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters MAXSCRATCH ausgeben.

Nächste Schritte

Da unter Umständen weitere Datenträger für zukünftige Wiederherstellungsoperationen erforderlich sind, ordnen Sie gegebenenfalls zusätzlichen Arbeitsdatenträgern Kennsätze zu und halten Sie diese Datenträger als Vorrat bereit.

Zugehörige Tasks:

Vorrat an Arbeitsdatenträgern bereithalten

Volles Speicherarchiv mit einer Überlaufposition verwalten

Mit zunehmendem Speicherbedarf überschreitet die Anzahl Datenträger, die für einen Speicherpool erforderlich sind, unter Umständen die physische Kapazität eines automatisierten Speicherarchivs. Um Speicherbereich für neue Datenträger verfügbar zu machen und vorhandene Datenträger zu überwachen, können Sie eine Überlaufposition für einen Speicherpool definieren.

Informationen zu diesem Vorgang

Der Server überwacht die Datenträger, die in den Überlaufbereich versetzt werden, und macht Speicherschächte für neue Datenträger verfügbar.

Vorgehensweise

1. Erstellen Sie eine Überlaufposition für Datenträger. Definieren oder aktualisieren Sie den Speicherpool, der dem automatisierten Speicherarchiv zugeordnet ist, indem Sie den Befehl DEFINE STGPOOL bzw. UPDATE STGPOOL unter Angabe des Parameters OVFLOCATION ausgeben. Um beispielsweise eine Überlaufposition mit dem Namen `ROOM2948` für einen Speicherpool mit dem Namen `ARCHIVEPOOL` zu erstellen, geben Sie den folgenden Befehl aus:

   ```
   update stgpool archivepool ovflocation=Room2948
   ```

2. Wenn in dem Speicherarchiv Speicherbereich für Arbeitsdatenträger erstellt werden muss, versetzen Sie volle Datenträger an die Überlaufposition, indem Sie den Befehl MOVE MEDIA ausgeben. Um beispielsweise alle vollen Datenträger in dem angegebenen Speicherpool aus dem Speicherarchiv zu versetzen, geben Sie den folgenden Befehl aus:

   ```
   move media * stgpool=archivepool
   ```

3. Stellen Sie Arbeitsdatenträger nach Bedarf zurück.
   Einschränkung: Wenn für einen Datenträger ein Eintrag in der Protokolldatei für Datenträger vorhanden ist, kann der Datenträger nicht als Arbeitsdatenträger zurückgestellt werden. Weitere Informationen finden Sie in Datenträger in ein automatisiertes Speicherarchiv zurückstellen.
4. Identifizieren Sie die leeren Arbeitsbänder an der Überlaufposition, indem Sie den Befehl QUERY MEDIA ausgeben. Geben Sie beispielsweise den folgenden Befehl aus:

   ```
   query media * stg=* whereovflocation=Room2948 wherestatus=empty
   ```

5. Wenn der Server weitere Datenträger anfordert, lokalisieren Sie Datenträger und stellen Sie diese von der Überlaufposition zurück.

   Um Datenträger an einer Überlaufposition zu finden, geben Sie den Befehl QUERY MEDIA aus. Sie können den Befehl QUERY MEDIA auch verwenden, um Befehle zum Zurückstellen von Datenträgern zu generieren.

   Um beispielsweise die Datenträger an der Überlaufposition aufzulisten und gleichzeitig die Befehle zum Zurückstellen dieser Datenträger in das Speicherarchiv zu generieren, geben Sie einen ähnlichen Befehl wie in dem folgenden Beispiel aus:

   ```
   query media format=cmd stgpool=archivepool whereovflocation=Room2948
   cmd="checkin libvol autolib &vol status=private"
   cmdfilename="\storage\move\media\checkin.vols"
   ```

   Tipps:
   - Mountanforderungen vom Server umfassen den Standort der Datenträger.
   - Um die Anzahl Tage anzugeben, die verstreichen müssen, bevor die Datenträger für die Verarbeitung auswählbar sind, geben Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters REUSEDELAY aus.
   - Die Datei, die die generierten Befehle enthält, kann mit dem IBM Spectrum Protect-Befehl MACRO ausgeführt werden.

Zugehörige Verweise:
MOVE MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff versetzen)
QUERY MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff abfragen)
UPDATE STGPOOL (Speicherpool aktualisieren)

Datenträgerbestand in einem Speicherarchiv prüfen

Sie können ein automatisiertes Speicherarchiv prüfen, um sicherzustellen, dass der Datenträgerbestand des Speicherarchivs mit den Datenträgern konsistent ist, die physisch in dem Speicherarchiv vorhanden sind. Die Prüfung eines Speicherarchivs bietet sich an, wenn der Datenträgerbestand des Speicherarchivs aufgrund manueller Versetzungen der Datenträger in dem Speicherarchiv oder aufgrund von Datenbankproblemen nicht mehr korrekt ist.

Vorgehensweise

1. Stellen Sie sicher, dass keine Datenträger in den Speicherarchivlaufwerken bereitgestellt sind. Wenn Datenträger im Status IDLE (Inaktiv) bereitgestellt sind, geben Sie den Befehl DISMOUNT VOLUME aus, um die Bereitstellung dieser Datenträger aufzuheben.
2. Prüfen Sie den Datenträgerbestand, indem Sie den Befehl AUDIT LIBRARY ausgeben. Führen Sie eine der folgenden Aktionen aus:
   - Wenn das Speicherarchiv über einen Barcodeleser verfügt, können Sie Zeit sparen, indem Sie Datenträger mithilfe des Barcodelesers identifizieren. Um beispielsweise das Speicherarchiv TAPELIB mithilfe seines Barcodelesers zu prüfen, geben Sie den folgenden Befehl aus:

     ```
     audit library tapelib checklabel=barcode
     ```

   - Wenn das Speicherarchiv über keinen Barcodeleser verfügt, geben Sie den Befehl AUDIT LIBRARY ohne Angabe von CHECKLABEL=BARCODE aus. Jeder Datenträger wird vom Server zur Überprüfung seines Kennsatzes bereitgestellt. Nachdem der Kennsatz überprüft wurde, führt der Server die Überprüfung für alle verbleibenden Datenträger aus.

Ergebnisse

Der Server löscht fehlende Datenträger aus dem Bestand und aktualisiert die Positionen von Datenträgern, die seit der letzten Prüfung versetzt wurden.

Einschränkung: Während einer Prüfoperation kann der Server dem Bestand keine neuen Datenträger hinzufügen.
Zugehörige Tasks:
Banddatenträgern Kennsätze zuordnen
Zugehörige Verweise:
AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)
DISMOUNT VOLUME (Datenträger nach Datenträgername abhängen)

Teilweise beschriebene Datenträger

Teilweise beschriebene Datenträger sind immer private Datenträger; dies ist auch dann der Fall, wenn ihr Status vor dem Bereitstellen durch den Server PRIVATE lautete. Der Server protokolliert den ursprünglichen Status von Arbeitsdatenträgern und versetzt diese wieder in den Arbeitsstatus, wenn sie leer sind.

Mit Ausnahme von Datenträgern in automatisierten Speicherarchiven erkennt der Server einen Arbeitsdatenträger erst nach dessen Bereitstellung. Der Datenträgerstatus ändert sich dann in PRIVATE und der Datenträger wird automatisch als Teil des Speicherpools definiert, für den die Mountanforderung erfolgte.

Zugehörige Tasks:
Status eines Datenträgers in einem automatisierten Speicherarchiv ändern

Operationen für gemeinsam genutzte Speicherarchive

Gemeinsam genutzte Speicherarchive sind logische Speicherarchive, die physisch durch SCSI-Speicherarchive dargestellt werden. Das physische Speicherarchiv wird durch den IBM Spectrum Protect-Server gesteuert, der als Speicherarchivmanager konfiguriert ist. IBM Spectrum Protect-Server, die den Speicherarchivtyp SHARED verwenden, sind Speicherarchivclients für den IBM Spectrum Protect-Speicherarchivmanager-Server.

Der Speicherarchivclient kontaktiert den Speicherarchivmanager, wenn der Speicherarchivmanager startet und die Speichereinheit initialisiert wird oder nachdem ein Speicherarchivmanager für einen Speicherarchivclient definiert wurde. Der Speicherarchivclient bestätigt, dass der kontaktierte Server der Speicherarchivmanager für die angegebene Speicherarchiveinheit ist. Der Speicherarchivclient vergleicht außerdem die Laufwerkdefinitionen mit dem Speicherarchivmanager auf Konsistenz. Der Speicherarchivclient kontaktiert den Speicherarchivmanager für jede der folgenden Operationen:

Datenträgermount
: Ein Speicherarchivclient sendet eine Zugriffsanforderung für einen bestimmten Datenträger in der gemeinsam genutzten Speicherarchiveinheit an den Speicherarchivmanager. Bei einem Arbeitsdatenträger gibt der Speicherarchivclient keinen Datenträgernamen an. Wenn der Speicherarchivmanager nicht auf den angeforderten Datenträger zugreifen kann oder wenn keine Arbeitsdatenträger verfügbar sind, weist der Speicherarchivmanager die Mountanforderung zurück. Wenn der Mount erfolgreich ist, gibt der Speicherarchivmanager den Namen des Laufwerks zurück, in dem der Datenträger bereitgestellt ist.

Datenträgerfreigabe
: Wenn ein Speicherarchivclient nicht mehr auf einen Datenträger zugreifen muss, teilt er dem Speicherarchivmanager mit, dass der Datenträger wieder als Arbeitsdatenträger verwendet werden kann. Die Datenbank des Speicherarchivmanagers wird mit der neuen Position des Datenträgers, der sich jetzt im Bestand des Speicherarchivservers befindet, aktualisiert. Der Datenträger wird aus dem Datenträgerbestand des Speicherarchivclients gelöscht.

Tabelle 1 zeigt die Interaktion zwischen Speicherarchivclients und dem Speicherarchivmanager bei der Verarbeitung von IBM Spectrum Protect-Operationen.

Tabelle 1. Wie SAN-fähige Server IBM Spectrum Protect-Operationen verarbeiten

Operation **(Befehl)**	**Speicherarchivmanager**	**Speicherarchivclient**
Datenträger im Speicherarchiv abfragen (QUERY LIBVOLUME)	Zeigt die in das Speicherarchiv zurückgestellten Datenträger an. Bei privaten Datenträgern wird außerdem der Eignerserver angezeigt.	Nicht zutreffend
Speicherarchivdatenträger zurückstellen und entnehmen (CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME)	Sendet die Befehle an die Speicherarchiveinheit.	Nicht zutreffend Wenn eine Zurückstelloperation aufgrund einer Clientzurückschreibungsoperation erforderlich ist, wird eine Anforderung an den Speicherarchivmanager-Server gesendet.

Operation (Befehl)	Speicherarchivmanager	Speicherarchivclient
Datenträger und DRM-Datenträger versetzen (MOVE MEDIA, MOVE DRMEDIA)	Nur gültig für Datenträger, die vom Speicherarchivmanager-Server verwendet werden.	Fordert die Ausführung der Operationen vom Speicherarchivmanager-Server an. Generiert einen Entnahmeprozess auf dem Speicherarchivmanager-Server.
Speicherarchivbestand prüfen (AUDIT LIBRARY)	Synchronisiert den Bestand mit der Speicherarchiveinheit.	Synchronisiert den Bestand mit dem Speicherarchivmanager-Server.
Datenträger im Speicherarchiv einen Kennsatz zuordnen (LABEL LIBVOLUME)	Ordnet Datenträgern Kennsätze zu und stellt Datenträger zurück.	Nicht zutreffend
Bereitstellung eines Datenträgers aufheben (DISMOUNT VOLUME)	Sendet die Anforderung an die Speicherarchiveinheit.	Fordert die Ausführung der Operationen vom Speicherarchivmanager-Server an.
Datenträger abfragen (QUERY VOLUME)	Prüft, ob der anfordernde Speicherarchivclient Eigner des Datenträgers ist und ob sich der Datenträger in der Speicherarchiveinheit befindet.	Fordert die Ausführung der Operationen vom Speicherarchivmanager-Server an.

Serveranforderungen für Datenträger verwalten

IBM Spectrum Protect zeigt allen Verwaltungsbefehlszeilenclients, die im Konsolenmodus gestartet werden, Anforderungen und Statusnachrichten an. Für diese Anforderungsnachrichten ist häufig ein Zeitlimit festgelegt. Erfolgreiche Serveroperationen müssen innerhalb des angegebenen Zeitlimits abgeschlossen werden; andernfalls tritt für die Operation eine Zeitlimitüberschreitung auf.

Informationen zu diesem Vorgang

Verwenden Sie bei automatisierten Speicherarchiven die Befehle CHECKIN LIBVOLUME und LABEL LIBVOLUME, um Kassetten in Schächte einzulegen. Wenn Sie einen Wert für den Parameter WAITTIME angeben, wird eine Antwortnachricht angezeigt. Wenn der Wert des Parameters 0 ist, ist keine Antwort erforderlich. Wenn Sie den Befehl CHECKOUT LIBVOLUME ausgeben, müssen Sie Kassetten in Schächte einlegen und es wird in jedem Fall eine Antwortnachricht angezeigt.

Vorgehensweise

Die folgende Tabelle enthält Informationen zur Handhabung verschiedener Serverdatenträgertasks.

Task	Details
Verwaltungsclient für Mountnachrichten verwenden	Der Server sendet Statusnachrichten für Mountanforderungen an die Serverkonsole und an alle Verwaltungsbefehlszeilenclients im Mountmodus oder Konsolenmodus. Um einen Verwaltungsbefehlszeilenclient im Mountmodus zu starten, geben Sie im Verwaltungsbefehlszeilenclient den Befehl dsmadmc -mountmode aus.
Nachrichten zu automatisierten Speicherarchiven empfangen	Sie können Mountnachrichten und Fehlernachrichten zu automatisierten Speicherarchiven auf Verwaltungsbefehlszeilenclients im Mountmodus oder Konsolenmodus anzeigen. Mountnachrichten werden an das Speicherarchiv und nicht an einen Bediener gesendet. Nachrichten zu Problemen mit dem Speicherarchiv werden an die Mountnachrichtenwarteschlange gesendet.
Informationen zu anstehenden Bedieneranforderungen abrufen	Um Informationen zu anstehenden Bedieneranforderungen abzurufen, geben Sie den Befehl QUERY REQUEST aus oder zeigen Sie die Mountnachrichtenwarteschlange auf einem Verwaltungsbefehlszeilenclient an, der im Mountmodus gestartet wurde. Wenn Sie den Befehl QUERY REQUEST ausgeben, zeigt der Server angeforderte Aktionen und die verbleibende Zeit, bevor das Zeitlimit für die Anforderungen überschritten wird.

Task	Details
Bedieneranforderungen beantworten	Wenn der Server eine explizite Antwort auf eine abgeschlossene Mountanforderung erfordert, verwenden Sie den Befehl REPLY. Der Parameter *Anforderungsnummer* gibt die Anforderungsidentifikationsnummer an, die dem Server anzeigt, welche anstehende Bedieneranforderung abgeschlossen ist. Diese dreistellige Zahl wird immer in der Anforderungsnachricht angezeigt.
Bedieneranforderung abbrechen	Um eine Mountanforderung für ein Speicherarchiv abzubrechen, geben Sie den Befehl CANCEL REQUEST aus. Bei den meisten Anforderungen, die automatisierten SCSI-Speicherarchiven zugeordnet sind, muss ein Bediener eine Hardware- oder Systemaktion ausführen, um den angeforderten Mount abzubrechen. Bei derartigen Anforderungen wird der Befehl CANCEL REQUEST nicht vom Server akzeptiert. Der Befehl CANCEL REQUEST muss die Anforderungsidentifikationsnummer enthalten. Diese Nummer ist in die Anforderungsnachricht eingeschlossen. Wenn der angeforderte Datenträger als UNAVAILABLE markiert werden soll, geben Sie den Befehl CANCEL REQUEST unter Angabe des Parameters PERMANENT aus. Wenn Sie den Parameter PERMANENT angeben, versucht der Server nicht, den angeforderten Datenträger erneut bereitzustellen. Dies ist beispielsweise hilfreich, wenn sich der Datenträger an einem fernen Standort befindet oder aus einem anderen Grund nicht verfügbar ist.
Anforderung zum Zurückstellen eines Datenträgers beantworten	Wenn der Server einen bestimmten Datenträger, der in einem automatisierten Speicherarchiv bereitgestellt werden soll, nicht finden kann, fordert der Server den Bediener zum Zurückstellen des Datenträgers auf. Wenn der angeforderte Datenträger verfügbar ist, legen Sie den Datenträger in das Speicherarchiv ein und stellen Sie ihn zurück. Weitere Informationen finden Sie in Datenträger in ein automatisiertes Speicherarchiv zurückstellen. Wenn der angeforderte Datenträger nicht verfügbar ist, aktualisieren Sie den Zugriffsmodus des Datenträgers, indem Sie den Befehl UPDATE VOLUME unter Angabe des Parameters ACCESS=UNAVAILABLE ausgeben. Brechen Sie dann die Zurückstellanforderung mit dem Befehl CANCEL REQUEST ab. Brechen Sie nicht den Clientprozess ab, der die Anforderung zur Folge hatte! Rufen Sie mithilfe des Befehls QUERY REQUEST die ID der Anforderung ab, die abgebrochen werden soll. Wenn Sie nicht innerhalb der für die Einheitenklasse des Speicherpools angegebene Mountwartezeit auf die Zurückstellanforderung des Servers antworten, markiert der Server den Datenträger als nicht verfügbar.
Bereitgestellte Datenträger bestimmen	Um einen Bericht zu allen Datenträgern anzufordern, die momentan für die Verwendung durch den Server bereitgestellt sind, geben Sie den Befehl QUERY MOUNT aus. Der Bericht zeigt, welche Datenträger bereitgestellt sind, welche Laufwerke auf die Datenträger zugegriffen haben und ob die Datenträger im Gebrauch sind.
Bereitstellung inaktiver Datenträger aufheben	Wenn ein Datenträger inaktiv ist, hebt der Server die Bereitstellung des Datenträgers nicht sofort auf; der Datenträger bleibt vielmehr so lange bereitgestellt, wie im Parameter für den Mount-Aufbewahrungszeitraum für die Einheitenklasse angegeben ist. Durch die Verwendung eines Mount-Aufbewahrungszeitraums kann die Zugriffszeit reduziert werden, wenn Datenträger wiederholt verwendet werden. Um die Bereitstellung eines inaktiven Datenträgers für das Laufwerk aufzuheben, in dem er bereitgestellt ist, geben Sie den Befehl DISMOUNT VOLUME aus. Informationen zum Festlegen des Mount-Aufbewahrungszeitraums finden Sie in Steuern, wie lange ein Datenträger bereitgestellt bleibt.

Zugehörige Verweise:
QUERY REQUEST (Eine oder mehrere anstehende Mountanforderungen abfragen)

Bandlaufwerke verwalten

Sie können Bandlaufwerke abfragen, aktualisieren und löschen. Außerdem können Sie Bandlaufwerke reinigen und Bandlaufwerkverschlüsselung und Datenprüfung konfigurieren.

- Laufwerke aktualisieren
  Sie können die Attribute einer Laufwerkdefinition ändern, um ein Laufwerk offline zu schalten oder ein Laufwerk zu rekonfigurieren.
- Datenprüfung während Schreib-/Leseoperationen auf Band
  Um Daten zu prüfen und beschädigte Daten zu identifizieren, können Sie eine Funktion verwenden, die als 'Schutz logischer Blöcke'

bezeichnet wird. Wenn Sie den Schutz logischer Blöcke verwenden, fügt IBM Spectrum Protect einen Wert für zyklische Blockprüfung (CRC = Cyclic Redundancy Check) am Ende jedes logischen Blocks mit Daten ein, während die Daten auf Band geschrieben werden.

- Bandlaufwerke reinigen
  Die Steuerung der Bandlaufwerkreinigung kann durch den Server erfolgen. Der Server kann steuern, wie Bandlaufwerke in SCSI-Speicherarchiven gereinigt werden.
- Bandlaufwerke ersetzen
  Wenn Sie ein Laufwerk in einem Bandarchiv ersetzen, das für IBM Spectrum Protect definiert ist, müssen Sie die Laufwerk- und Pfaddefinitionen für das alte Laufwerk löschen und das neue Laufwerk samt Pfad definieren.

Laufwerke aktualisieren

Sie können die Attribute einer Laufwerkdefinition ändern, um ein Laufwerk offline zu schalten oder ein Laufwerk zu rekonfigurieren.

Informationen zu diesem Vorgang

Sie können die folgenden Attribute eines Laufwerks ändern:

- Die Elementadresse, wenn sich das Laufwerk in einem SCSI-Speicherarchiv befindet
- Die Reinigungshäufigkeit
- Den Laufwerkstatus: ONLINE oder OFFLINE

Einschränkung: Wenn ein Laufwerk im Gebrauch ist, können Sie die Elementnummer oder den Einheitennamen nicht ändern. Anweisungen zum Offlineschalten von Laufwerken finden Sie in Bandlaufwerke offline schalten.
Wenn ein Datenträger im Laufwerk bereitgestellt, aber inaktiv ist, kann seine Bereitstellung explizit aufgehoben werden. Anweisungen zum Aufheben der Bereitstellung inaktiver Datenträger finden Sie in Serveranforderungen für Datenträger verwalten.

Vorgehensweise

- Ändern Sie die Elementadresse eines Laufwerks, indem Sie den Befehl UPDATE DRIVE ausgeben. Ändern Sie beispielsweise in einem Speicherarchiv mit dem Namen AUTO die Elementadresse von DRIVE3 in 119, indem Sie den folgenden Befehl ausgeben:

  ```
  update drive auto drive3 element=119
  ```

- Ändern Sie den Einheitennamen eines Laufwerks, indem Sie den Befehl UPDATE PATH ausgeben. Um beispielsweise den Einheitennamen eines Laufwerks mit dem Namen DRIVE3 zu ändern, geben Sie den folgenden Befehl aus:  AIX-Betriebssysteme

  ```
  update path server1 drive3 srctype=server desttype=drive library=scsilib
   device=/dev/rmt0
  ```

   Linux-Betriebssysteme

  ```
  update path server1 drive3 srctype=server desttype=drive library=scsilib
   device=/dev/IBMtape0
  ```

   Windows-Betriebssysteme

  ```
  update path server1 drive3 srctype=server desttype=drive library=scsilib
     device=mt3.0.0.0
  ```

- Bandlaufwerke offline schalten
  Sie können ein Bandlaufwerk offline schalten, während es im Gebrauch ist. Sie können ein Laufwerk beispielsweise zur Ausführung der Wartung offline schalten.

Zugehörige Verweise:
UPDATE DRIVE (Laufwerk aktualisieren)
UPDATE PATH (Pfad ändern)

Datenprüfung während Schreib-/Leseoperationen auf Band

Um Daten zu prüfen und beschädigte Daten zu identifizieren, können Sie eine Funktion verwenden, die als 'Schutz logischer Blöcke' bezeichnet wird. Wenn Sie den Schutz logischer Blöcke verwenden, fügt IBM Spectrum Protect einen Wert für zyklische Blockprüfung (CRC = Cyclic Redundancy Check) am Ende jedes logischen Blocks mit Daten ein, während die Daten auf Band geschrieben werden.

Der Schutz logischer Blöcke ermöglicht es Ihnen, Fehler zu identifizieren, die auftreten, während Daten auf Band geschrieben werden und während Daten über das Speicherbereichsnetz vom Bandlaufwerk an IBM Spectrum Protect übertragen werden. Laufwerke, die den Schutz logischer Blöcke unterstützen, prüfen Daten während Lese- und Schreiboperationen. Der IBM Spectrum Protect-Server prüft Daten während Leseoperationen.

Wenn die Prüfung durch das Laufwerk während Schreiboperationen fehlschlägt, kann dies darauf hinweisen, dass Daten während der Übertragung auf Band beschädigt wurden. In diesem Fall schlägt die Schreiboperation für den IBM Spectrum Protect-Server fehl. Sie müssen die Operation erneut starten, um fortfahren zu können. Wenn die Prüfung durch das Laufwerk während Leseoperationen fehlschlägt, kann dies

darauf hinweisen, dass die Banddatenträger beschädigt sind. Wenn die Prüfung durch den IBM Spectrum Protect-Server während Leseoperationen fehlschlägt, kann dies darauf hinweisen, dass die Daten während der Übertragung vom Bandlaufwerk beschädigt wurden; der Server versucht, die Operation erneut auszuführen. Wenn die Prüfung durchgängig fehlschlägt, gibt der IBM Spectrum Protect-Server eine Fehlernachricht aus, die auf Hardwarefehler oder Verbindungsprobleme hinweist.

Wenn der Schutz logischer Blöcke auf einem Bandlaufwerk inaktiviert ist oder das Laufwerk den Schutz logischer Blöcke nicht unterstützt, kann der IBM Spectrum Protect-Server geschützte Daten nur lesen. Die Daten werden jedoch nicht geprüft.

Der Schutz logischer Blöcke hat eine höhere Priorität als die zyklische Blockprüfung, die Sie beim Definieren oder Aktualisieren einer Speicherpooldefinition angeben können. Wenn Sie die zyklische Blockprüfung für einen Speicherpool angeben, werden Daten nur während Datenträgerprüfoperationen geprüft. Fehler werden identifiziert, nachdem die Daten auf Band geschrieben wurden.

Einschränkungen:

- Sie können den Schutz logischer Blöcke nicht für sequenzielle Daten wie Sicherungsgruppen und Datenbanksicherungen verwenden.
- Die CRC-Prüfung hat Auswirkungen auf die Leistung, da mehr Prozessorauslastung auf dem Client und dem Server erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen.
- Ändern Sie bei einem Arbeitsdatenträger, wenn Sie den Schutz logischer Blöcke für Schreib-/Leseoperationen (LBPROTECT=READWRITE) angeben, den Parameterwert nicht, nachdem Daten auf den Datenträger geschrieben wurden. Das Ändern des Parameterwerts während des Lebenszyklus des Datenträgers auf dem IBM Spectrum Protect-Server wird nicht unterstützt.

- Laufwerke, die den Schutz logischer Blöcke unterstützen
  Der Schutz logischer Blöcke ist nur für die Einheitentypen 3592, LTO und ECARTRIDGE verfügbar. 3592-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM TS1130, TS1140 und spätere Generationen. LTO-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM LTO-5-Laufwerke und unterstützte LTO-6-Laufwerke. Oracle StorageTek-Laufwerke, die diese Art von Schutz bereitstellen, umfassen Laufwerke mit dem T10000C-Format und dem T10000D-Format.
- Schutz logischer Blöcke aktivieren und inaktivieren
  Sie können den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben. Es ist auch möglich, den Schutz logischer Blöcke zu inaktivieren. Standardmäßig ist der Schutz logischer Blöcke wegen der Auswirkungen, die die zyklische Blockprüfung auf dem Server und dem Bandlaufwerk auf die Leistung hat, inaktiviert.
- Schreib-/Leseoperationen für Datenträger mit Schutz logischer Blöcke
  Schreib-/Leseoperationen für leere Datenträger oder Datenträger, die mit Daten gefüllt werden, sind davon abhängig, ob für die Datenträger der Schutz logischer Blöcke definiert ist. Geschützte und ungeschützte Datenblöcke können nicht auf demselben Datenträger gemischt werden.
- Speicherpoolverwaltung in einem Bandarchiv
  Um geschützte und ungeschützte Daten in einem Speicherarchiv zu mischen, müssen Sie unterschiedliche Einheitenklassen und unterschiedliche Speicherpools erstellen, um die Daten voneinander zu trennen. Wenn eine Einheitenklasse geschützten Daten zugeordnet ist, können Sie den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben.

Laufwerke, die den Schutz logischer Blöcke unterstützen

Der Schutz logischer Blöcke ist nur für die Einheitentypen 3592, LTO und ECARTRIDGE verfügbar. 3592-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM TS1130, TS1140 und spätere Generationen. LTO-Laufwerke, die diese Art von Schutz bereitstellen, umfassen IBM LTO-5-Laufwerke und unterstützte LTO-6-Laufwerke. Oracle StorageTek-Laufwerke, die diese Art von Schutz bereitstellen, umfassen Laufwerke mit dem T10000C-Format und dem T10000D-Format.

In der folgenden Tabelle sind die Datenträger und Formate aufgeführt, die Sie zusammen mit Laufwerken verwenden können, die den Schutz logischer Blöcke unterstützen.

Laufwerk	Banddatenträger	Laufwerkformate
IBM TS1130	3592 Generation 2	3592-3 und 3592-3C
IBM TS1140	3592 Generation 2 3592 Generation 3	Generation 2: 3592-3 und 3592-3C Generation 3: 3592-4 und 3592-4C
IBM TS1150	3592 Generation 3 3592 Generation 4	Generation 4: 3592-5 und 3592-5C
IBM LTO-5	LTO-5	Ultrium 5 und Ultrium 5C
IBM LTO-6	LTO-6 LTO-5	Ultrium 6 und Ultrium 6C Ultrium 5 und Ultrium 5C
IBM LTO-7	LTO-7 LTO-6	Ultrium 7 und Ultrium 7C Ultrium 6 und Ultrium 6C

Laufwerk	Banddatenträger	Laufwerkformate
Oracle T10000C	Oracle StorageTek T10000 T2	T10000C und T10000C-C
Oracle T10000D	Oracle StorageTek T10000 T2	T10000D und T10000D-C

Tipps:

- Um den Schutz logischer Blöcke für einen Banddatenträger zu aktivieren und den Datenträger dann zum Sichern von Daten wiederzuverwenden, müssen Sie den Schutz logischer Blöcke für die Einheitenklasse und das Laufwerk aktivieren.
- Bei einem 3592-, LTO- oder Oracle StorageTek-Laufwerk, das keinen Schutz logischer Blöcke bereitstellen kann, können Sie für das Laufwerk ein Upgrade mit Firmware durchführen, die Schutz logischer Blöcke bereitstellt.

Der Schutz logischer Blöcke ist für Laufwerke in Speicherarchiven des Typs SCSI verfügbar. Aktuelle Informationen zur Unterstützung für den Schutz logischer Blöcke finden Sie in Technote 1568108.

Um den Schutz logischer Blöcke für Schreiboperationen verwenden zu können, müssen alle Laufwerke in einem Speicherarchiv den Schutz logischer Blöcke unterstützen. Wenn ein Laufwerk keinen Schutz logischer Blöcke bereitstellen kann, werden Datenträger mit Schreib-/Lesezugriff nicht bereitgestellt. Der Server kann jedoch mithilfe des Laufwerks Datenträger mit Lesezugriff bereitstellen. Die geschützten Daten werden vom IBM Spectrum Protect-Server gelesen und geprüft, wenn der Schutz logischer Blöcke für Schreib-/Leseoperationen aktiviert ist.

Schutz logischer Blöcke aktivieren und inaktivieren

Sie können den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben. Es ist auch möglich, den Schutz logischer Blöcke zu inaktivieren. Standardmäßig ist der Schutz logischer Blöcke wegen der Auswirkungen, die die zyklische Blockprüfung auf dem Server und dem Bandlaufwerk auf die Leistung hat, inaktiviert.

Informationen zu diesem Vorgang

Schreib-/Leseoperationen für leere Datenträger oder Datenträger, die mit Daten gefüllt werden, sind davon abhängig, ob für die Datenträger der Schutz logischer Blöcke definiert ist. Geschützte und ungeschützte Datenblöcke können nicht auf demselben Datenträger gemischt werden. Wenn Sie die Einstellung für den Schutz logischer Blöcke ändern, gilt die Änderung nur für leere Datenträger. Datenträger, die mit Daten gefüllt werden, und volle Datenträger behalten ihren Status für den Schutz logischer Blöcke bei, bis sie leer und zum erneuten Füllen bereit sind. Wenn Sie beispielsweise den Schutz logischer Blöcke inaktivieren und der Server einen Datenträger auswählt, der einer Einheitenklasse zugeordnet ist, für die der Schutz logischer Blöcke definiert ist, schreibt der Server weiterhin geschützte Daten auf den Datenträger.
Einschränkung: Der Schutz logischer Blöcke ist nur für bestimmte Einheitentypen verfügbar. Weitere Informationen finden Sie in Laufwerke, die den Schutz logischer Blöcke unterstützen.

Vorgehensweise

1. Um den Schutz logischer Blöcke für die Einheitentypen 3592, LTO und ECARTRIDGE zu aktivieren, geben Sie den Befehl DEFINE DEVCLASS oder den Befehl UPDATE DEVCLASS unter Angabe des Parameters LBPROTECT aus. Um beispielsweise den Schutz logischer Blöcke während Lese- und Schreiboperationen für eine Einheitenklasse 3592 mit dem Namen 3592_lbprotect anzugeben, geben Sie den folgenden Befehl aus:

   ```
   define devclass 3592_lbprotect library=3594 lbprotect=readwrite
   ```

   Tipps:
   - Wenn Sie den Wert des Parameters LBPROTECT von NO in READWRITE oder WRITEONLY ändern und der Server einen Datenträger auswählt, der mit Daten gefüllt wird und für den kein Schutz logischer Blöcke für Schreiboperationen definiert ist, gibt der Server jedes Mal eine Nachricht aus, wenn der Datenträger bereitgestellt wird. Die Nachricht gibt an, dass Daten auf den Datenträger ohne Schutz logischer Blöcke geschrieben werden. Soll die Anzeige dieser Nachricht verhindert werden oder soll IBM Spectrum Protect nur Daten mit Schutz logischer Blöcke auf den Datenträger schreiben, ändern Sie den Zugriff für Datenträger ohne Schutz logischer Blöcke, die mit Daten gefüllt werden, in Lesezugriff.
   - Um die Leistung zu verbessern, geben Sie den Parameter CRCDATA nicht im Befehl DEFINE STGPOOL oder UPDATE STGPOOL an.
   - Wenn Daten während Leseoperationen sowohl vom Laufwerk als auch vom IBM Spectrum Protect-Server geprüft werden, kann dies die Serverleistung während Zurückschreibungs- und Abrufoperationen verschlechtern. Um die für Zurückschreibungs- und Abrufoperationen erforderliche Zeit zu verringern, ändern Sie die Einstellung des Parameters LBPROTECT von READWRITE in WRITEONLY. Nachdem die Daten zurückgeschrieben oder abgerufen wurden, können Sie den Parameter LBPROTECT auf READWRITE zurücksetzen.
2. Um den Schutz logischer Blöcke zu inaktivieren, geben Sie den Befehl DEFINE DEVCLASS oder den Befehl UPDATE DEVCLASS unter Angabe des Parameters LBPROTECT=NO aus.
   Einschränkung: Wenn der Schutz logischer Blöcke inaktiviert ist, schreibt der Server keine Daten auf ein leeres Band, für das der Schutz logischer Blöcke definiert ist. Wenn jedoch ein Datenträger, der mit Daten gefüllt wird und für den der Schutz logischer Blöcke definiert ist, ausgewählt wird, schreibt der Server weiterhin Daten auf den Datenträger, für den der Schutz logischer Blöcke definiert ist. Um zu verhindern, dass der Server Daten auf Bänder mit Schutz logischer Blöcke schreibt, ändern Sie den Zugriff für Datenträger, die mit Daten gefüllt werden und für die der Schutz logischer Blöcke definiert ist, in Lesezugriff. Wenn Daten gelesen werden, werden die Ergebnisse der zyklischen Blockprüfung nicht vom Laufwerk oder Server geprüft.

Wenn in einem Katastrophenfall der Standort zur Wiederherstellung über keine Laufwerke verfügt, die den Schutz logischer Blöcke unterstützen, müssen Sie den Parameter LBPROTECT=NO angeben. Wenn die Bandlaufwerke für Schreiboperationen verwendet werden, müssen Sie den Datenträgerzugriff für Datenträger mit geschützten Daten in Lesezugriff ändern, um eine Verwendung der Datenträger durch den Server zu verhindern.

Wenn der Server den Schutz logischer Blöcke aktivieren muss, gibt der Server eine Fehlernachricht aus, die angibt, dass das Laufwerk den Schutz logischer Blöcke nicht unterstützt.

Nächste Schritte

Um festzustellen, ob für einen Datenträger der Schutz logischer Blöcke definiert ist, geben Sie den Befehl QUERY VOLUME aus und prüfen Sie den Wert im Feld `Schutz logischer Blöcke`.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)
QUERY VOLUME (Speicherpooldatenträger abfragen)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)
UPDATE STGPOOL (Speicherpool aktualisieren)

Schreib-/Leseoperationen für Datenträger mit Schutz logischer Blöcke

Schreib-/Leseoperationen für leere Datenträger oder Datenträger, die mit Daten gefüllt werden, sind davon abhängig, ob für die Datenträger der Schutz logischer Blöcke definiert ist. Geschützte und ungeschützte Datenblöcke können nicht auf demselben Datenträger gemischt werden.

Wenn Sie mit dem Befehl UPDATE DEVCLASS die Einstellung für den Schutz logischer Blöcke ändern, gilt die Änderung nur für leere Datenträger. Datenträger, die mit Daten gefüllt werden, und volle Datenträger behalten ihren Status für den Schutz logischer Blöcke bei, bis sie leer und zum erneuten Füllen bereit sind.

Angenommen, Sie ändern den Wert des Parameters LBPROTECT von READWRITE in NO. Wenn der Server einen Datenträger auswählt, der der Einheitenklasse zugeordnet ist und über Schutz logischer Blöcke verfügt, schreibt der Server weiterhin geschützte Daten auf den Datenträger.

Tipps:

- Wenn ein Laufwerk den Schutz logischer Blöcke nicht unterstützt, können Datenträger mit Schutz logischer Blöcke für Schreiboperationen nicht bereitgestellt werden. Um zu verhindern, dass der Server den geschützten Datenträger für Schreiboperationen bereitstellt, ändern Sie den Datenträgerzugriff in Lesezugriff. Inaktivieren Sie außerdem den Schutz logischer Blöcke, um zu verhindern, dass der Server die Funktion auf dem Bandlaufwerk aktiviert.
- Wenn ein Laufwerk den Schutz logischer Blöcke nicht unterstützt und der Schutz logischer Blöcke inaktiviert ist, liest der Server Daten von geschützten Datenträgern. Die Daten werden jedoch nicht vom Server und dem Bandlaufwerk geprüft.

Zugehörige Verweise:
QUERY VOLUME (Speicherpooldatenträger abfragen)
UPDATE DEVCLASS (Einheitenklasse aktualisieren)

Speicherpoolverwaltung in einem Bandarchiv

Um geschützte und ungeschützte Daten in einem Speicherarchiv zu mischen, müssen Sie unterschiedliche Einheitenklassen und unterschiedliche Speicherpools erstellen, um die Daten voneinander zu trennen. Wenn eine Einheitenklasse geschützten Daten zugeordnet ist, können Sie den Schutz logischer Blöcke für Lese- und Schreiboperationen oder ausschließlich für Schreiboperationen angeben.

Um Einheitenklassen und Speicherpools für ein TS3500-Speicherarchiv mit LTO-5-Laufwerken für geschützte und ungeschützte Daten zu definieren, können Sie eine Folge von Befehlen ausgeben wie in dem folgenden Beispiel gezeigt:

```
define library 3584 libtype=scsi
define devclass lbprotect library=3584 devicetype=lto lbprotect=readwrite
define devclass normal library=3584 devicetype=lto lbprotect=no
define stgpool lbprotect_pool lbprotect maxscratch=10
define stgpool normal_pool normal maxscratch=10
```

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
DEFINE LIBRARY (Speicherarchiv definieren)
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)

Bandlaufwerke reinigen

Die Steuerung der Bandlaufwerkreinigung kann durch den Server erfolgen. Der Server kann steuern, wie Bandlaufwerke in SCSI-Speicherarchiven gereinigt werden.

Informationen zu diesem Vorgang

Um Bandlaufwerke reinigen zu können, müssen Sie über Systemberechtigung oder uneingeschränkte Speicherberechtigung verfügen. Bei automatisierten Speicherarchiven können Sie die Reinigung automatisieren, indem Sie die Häufigkeit der Reinigungsoperationen angeben und eine Reinigungskassette in den Datenträgerbestand des Speicherarchivs zurückstellen. IBM Spectrum Protect stellt die Reinigungskassette wie angegeben bereit. Wenn Sie planen, bei einem SCSI-Speicherarchiv, das in seiner Einheitenhardware die Unterstützung für die automatische Laufwerkreinigung bereitstellt, die servergesteuerte Laufwerkreinigung zu verwenden, sind spezielle Hinweise zu berücksichtigen.

Tipp: Wenn ein automatisiertes Bandarchiv die Speicherarchivlaufwerkreinigung unterstützt, stellen Sie sicher, dass die Funktion aktiviert ist.

Sie können die vorzeitige Abnutzung der Schreib-/Leseköpfe von Laufwerken verhindern, indem Sie die Speicherarchivreinigungsfunktionen Ihres Einheitenherstellers verwenden.

Bei Laufwerken und Speicherarchiven unterschiedlicher Hersteller bestehen Unterschiede in der Handhabung von Reinigungskassetten und in der Art und Weise, wie das Vorhandensein einer Reinigungskassette in einem Laufwerk zurückgemeldet wird. Möglicherweise kann ein Laufwerk, das eine Reinigungskassette enthält, vom Einheitentreiber nicht geöffnet werden. Die von Einheiten ausgegebenen Prüfcodes und Fehlercodes für die Laufwerkreinigung sind unterschiedlich. Die Speicherarchivlaufwerkreinigung ist normalerweise Anwendungen nicht bekannt. Daher kann IBM Spectrum Protect möglicherweise die Reinigungskassetten in Laufwerken nicht immer erkennen und unter Umständen nicht bestimmen, wann die Reinigung beginnt.

Einige Einheiten erfordern eine kurze Leerlaufzeit zwischen Mountanforderungen, um die Laufwerkreinigung starten zu können. IBM Spectrum Protect versucht jedoch, die Leerlaufzeit für ein Laufwerk zu minimieren. Dies kann dazu führen, dass die Speicherarchivlaufwerkreinigung nicht effektiv funktioniert. Verwenden Sie in diesem Fall IBM Spectrum Protect zur Steuerung der Laufwerkreinigung. Sie können die Häufigkeit so festlegen, dass sie mit den Reinigungsempfehlungen des Herstellers übereinstimmt.

- Methoden zum Reinigen von Bandlaufwerken
  Im Laufe der Zeit können die Leseköpfe für Bänder verschmutzen, was zum Fehlschlagen von Lese- und Schreiboperationen führen kann. Aktivieren Sie die Bandreinigung, um diese Probleme zu verhindern. Sie können die Bandreinigung über das Laufwerk oder IBM Spectrum Protect aktivieren.
- Server für die Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren
  Wenn Sie die servergesteuerte Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren, können Sie angeben, wie oft die Laufwerke gereinigt werden sollen.
- Fehler bei der Laufwerkreinigung beheben
  Während Kassetten in einem Speicherarchiv versetzt werden, wird eine Datenkassette möglicherweise an eine Stelle versetzt, an der sich eine Reinigungskassette befinden sollte. Überprüfen Sie den Prozess, den der Server ausführt, und die Nachrichten, die ausgegeben werden, sodass Sie das Problem beheben können.

Methoden zum Reinigen von Bandlaufwerken

Im Laufe der Zeit können die Leseköpfe für Bänder verschmutzen, was zum Fehlschlagen von Lese- und Schreiboperationen führen kann. Aktivieren Sie die Bandreinigung, um diese Probleme zu verhindern. Sie können die Bandreinigung über das Laufwerk oder IBM Spectrum Protect aktivieren.

Sie können entweder die Speicherarchivlaufwerkreinigungsmethode oder die IBM Spectrum Protect-Laufwerkreinigungsmethode verwenden, aber nicht beide Methoden gleichzeitig. Einige SCSI-Speicherarchive stellen eine automatische Laufwerkreinigung zur Verfügung. Wählen Sie die Speicherarchivlaufwerkreinigungsmethode aus, sofern diese verfügbar ist. Ist sie nicht verfügbar oder hat sie Probleme zur Folge, verwenden Sie IBM Spectrum Protect zur Steuerung der Speicherarchivlaufwerkreinigung.

Speicherarchivlaufwerkreinigungsmethode
: Die Speicherarchivlaufwerkreinigungsmethode bietet für automatisierte Bandarchive, die diese Funktion verwenden, eine Reihe von Vorteilen:

  - Sie verringert den Aufwand, den der IBM Spectrum Protect-Administrator hat, um die Reinigung mithilfe von Kassetten physisch zu handhaben.
  - Sie verbessert die Verwendungsraten von Reinigungskassetten. Bei den meisten Bandarchiven wird die Häufigkeit, mit der Laufwerke gereinigt werden können, auf der Basis von Hardwareanzeigern verfolgt. IBM Spectrum Protect verwendet eine Rohzählung.
  - Sie reduziert die Häufigkeit unnötiger Reinigungen. Moderne Bandlaufwerke müssen nicht in festen Intervallen gereinigt werden; sie können erkennen, wann eine Reinigung erforderlich ist, und diese dann anfordern.

  Hersteller, die eine Speicherarchivlaufwerkreinigungsmethode zur Verfügung stellen, empfehlen die Verwendung dieser Funktion, um eine vorzeitige Abnutzung der Schreib-/Leseköpfe der Laufwerke zu verhindern. Bei Laufwerken und Speicherarchiven unterschiedlicher Hersteller bestehen Unterschiede in der Handhabung von Reinigungskassetten und in der Art und Weise, wie das Vorhandensein einer Reinigungskassette in einem Laufwerk zurückgemeldet wird. Möglicherweise kann ein Laufwerk, das eine Reinigungskassette enthält, vom Einheitentreiber nicht geöffnet werden. Die von Einheiten ausgegebenen Prüfcodes und Fehlercodes für die Laufwerkreinigung sind unterschiedlich. Die Speicherarchivlaufwerkreinigung ist normalerweise für alle Anwendungen transparent. IBM Spectrum Protect kann

jedoch möglicherweise Reinigungskassetten in Laufwerken nicht immer erkennen und unter Umständen nicht bestimmen, wann die Reinigung beginnt.

IBM Spectrum Protect-Laufwerkreinigungsmethode

Einige Einheiten erfordern eine kurze Leerlaufzeit zwischen Mountanforderungen, um die Laufwerkreinigung starten zu können. IBM Spectrum Protect versucht jedoch, die Leerlaufzeit für ein Laufwerk zu minimieren. Dies kann dazu führen, dass die Speicherarchivlaufwerkreinigung nicht effektiv funktioniert. Versuchen Sie in diesem Fall, IBM Spectrum Protect zur Steuerung der Laufwerkreinigung zu verwenden. Legen Sie die Häufigkeit so fest, dass sie mit den Reinigungsempfehlungen des Herstellers übereinstimmt.

Wenn der Laufwerkreinigungsprozess durch IBM Spectrum Protect gesteuert wird, inaktivieren Sie die Speicherarchivlaufwerkreinigungsfunktion, um Probleme zu verhindern. Wenn die Speicherarchivlaufwerkreinigungsfunktion aktiviert ist, versetzen einige Einheiten automatisch alle Reinigungskassetten, die im Speicherarchiv gefunden werden, in die Schächte des Speicherarchivs, die für Reinigungskassetten vorgesehen sind. Sie können eine Reinigungskassette erst nach der Inaktivierung der Speicherarchivlaufwerkreinigungsfunktion in den IBM Spectrum Protect-Speicherarchivbestand zurückstellen.

Um die Reinigung über das Laufwerk zu aktivieren, führen Sie die Anweisungen des Laufwerkherstellers aus. Informationen zum Aktivieren der Bereinigung mithilfe von IBM Spectrum Protect finden Sie in Server für die Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren.

Server für die Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren

Wenn Sie die servergesteuerte Laufwerkreinigung in einem automatisierten Speicherarchiv konfigurieren, können Sie angeben, wie oft die Laufwerke gereinigt werden sollen.

Vorbereitende Schritte

Bestimmen Sie, wie oft das Laufwerk gereinigt werden muss. Dieser Schritt ist erforderlich, damit Sie einen geeigneten Wert für den Parameter CLEANFREQUENCY im Befehl DEFINE DRIVE oder UPDATE DRIVE angeben können. Um beispielsweise ein Laufwerk zu reinigen, nachdem 100 GB Daten in dem Laufwerk verarbeitet wurden, würden Sie CLEANFREQUENCY=100 angeben.

Richtlinien zur Reinigungshäufigkeit enthält die Dokumentation des Laufwerkherstellers. Wenn die Dokumentation Richtlinien zur Reinigungshäufigkeit in Nutzungsstunden angibt, rechnen Sie den Wert in einen Gigabytewert um, indem Sie die folgenden Schritte ausführen:

1. Verwenden Sie den Wert für Byte pro Sekunde des Laufwerks, um einen Wert für Gigabyte pro Stunde zu ermitteln.
2. Multiplizieren Sie den Wert für Gigabyte pro Stunde mit der empfohlenen Anzahl Nutzungsstunden zwischen Reinigungen.
3. Verwenden Sie das Ergebnis als Wert für die Reinigungshäufigkeit.

Sie können entweder einen Wert für den Parameter CLEANFREQUENCY angeben oder ASNEEDED angeben, um das Laufwerk nach Bedarf zu reinigen.
Einschränkungen:

1. Bei Laufwerken IBM® 3592 müssen Sie einen numerischen Wert für den Parameter CLEANFREQUENCY angeben. Bei Einhaltung der in der Produktinformation aufgelisteten Reinigungshäufigkeit werden die Laufwerke nicht übermäßig gereinigt.
2. Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht für alle Bandlaufwerke. Die Informationen für Ihr Betriebssystem geben Auskunft darüber, ob ein Laufwerk diese Funktion unterstützt:
   - AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
   - Linux-BetriebssystemeSupported devices for Linux

   Klicken Sie in der Technote auf den Laufwerknamen, um detaillierte Informationen anzuzeigen. Wenn der Wert ASNEEDED nicht unterstützt wird, geben Sie die Anzahl Gigabyte an.

Vorgehensweise

Um die servergesteuerte Laufwerkreinigung in einem automatisierten Speicherarchiv zu konfigurieren, führen Sie die folgenden Schritte aus:

Definieren oder aktualisieren Sie die Laufwerke in dem Speicherarchiv unter Angabe des Parameters CLEANFREQUENCY im Befehl DEFINE DRIVE oder UPDATE DRIVE. Um beispielsweise ein Laufwerk mit dem Namen DRIVE1 nach der Verarbeitung von 100 GB Daten zu reinigen, geben Sie den folgenden Befehl aus:

```
update drive autolib1 drive1 cleanfrequency=100
```

Ergebnisse

Nachdem die Reinigungskassette zurückgestellt wurde, wird sie vom Server in ein Laufwerk geladen, wenn dieses gereinigt werden muss. Der Server verwendet diese Reinigungskassette gemäß den Angaben für die Reinigungsanzahl. Weitere Informationen finden Sie in Operationen mit Reinigungskassetten.

Nächste Schritte

Stellen Sie die Reinigungskassette in den Datenträgerbestand im Speicherarchiv zurück, indem Sie die Anweisungen in Reinigungskassette in ein Speicherarchiv zurückstellen ausführen.

- Reinigungskassette in ein Speicherarchiv zurückstellen
  Um die automatische Bandlaufwerkreinigung zu ermöglichen, müssen Sie eine Reinigungskassette in den Datenträgerbestand des automatisierten Speicherarchivs zurückstellen.
- Operationen mit Reinigungskassetten
  Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

Zugehörige Verweise:
DEFINE DRIVE (Laufwerk für ein Speicherarchiv definieren)
UPDATE DRIVE (Laufwerk aktualisieren)

Reinigungskassette in ein Speicherarchiv zurückstellen

Um die automatische Bandlaufwerkreinigung zu ermöglichen, müssen Sie eine Reinigungskassette in den Datenträgerbestand des automatisierten Speicherarchivs zurückstellen.

Informationen zu diesem Vorgang

Wenn Sie eine Reinigungskassette in ein Speicherarchiv zurückstellen, stellen Sie sicher, dass sie vom Server korrekt als Reinigungskassette erkannt wird. Stellen Sie sicher, dass sich keine Reinigungskassette in einem Schacht befindet, der beim Suchvorgang erkannt wird. Fehler und Verzögerungen von mindestens 15 Minuten können anzeigen, dass eine Reinigungskassette falsch platziert wurde.

Bei der bevorzugten Methode werden Reinigungskassetten einzeln zurückgestellt. Wenn Sie sowohl Datenkassetten als auch Reinigungskassetten zurückstellen müssen, stellen Sie zuerst die Datenkassetten in das Speicherarchiv zurück. Stellen Sie anschließend die Reinigungskassetten in das Speicherarchiv zurück.

Vorgehensweise

Um eine Reinigungskassette in ein Speicherarchiv zurückzustellen, geben Sie den Befehl CHECKIN LIBVOLUME aus. Um beispielsweise eine Reinigungskassette mit dem Namen AUTOLIB1 zurückzustellen, geben Sie den folgenden Befehl aus:

```
checkin libvolume autolib1 cleanv status=cleaner cleanings=10
 checklabel=no
```

Der Server gibt die Anforderung aus, die Kassette in den Eingangs-/Ausgangsport oder in einen bestimmten Schacht einzulegen.

Zugehörige Verweise:
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Operationen mit Reinigungskassetten

Um sicherzustellen, dass Bandlaufwerke wie erforderlich gereinigt werden, und um Probleme mit Bandspeicher zu verhindern, müssen Sie die Richtlinien beachten.

Reinigungsprozess überwachen
: Wenn eine Reinigungskassette in ein Speicherarchiv zurückgestellt wird und ein Laufwerk gereinigt werden muss, hebt der Server die Bereitstellung des Datenträgers auf und führt die Reinigungsoperation aus. Wenn die Reinigungsoperation fehlschlägt oder wenn sie abgebrochen wird oder wenn keine Reinigungskassette verfügbar ist, sind Sie sich der Tatsache, dass das Laufwerk gereinigt werden muss, möglicherweise nicht bewusst. Überwachen Sie Reinigungsnachrichten auf diese Probleme, um sicherzustellen, dass Laufwerke wie erforderlich gereinigt werden. Geben Sie, falls erforderlich, den Befehl CLEAN DRIVE aus, damit der Server den Reinigungsversuch wiederholt, oder laden Sie manuell eine Reinigungskassette in das Laufwerk.

Mehrere Reinigungskassetten verwenden
: Der Server verwendet eine Reinigungskassette für die Anzahl Reinigungen, die Sie beim Zurückstellen der Reinigungskassette angeben. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen, verwendet der Server nur eine der Kassetten, bis die angegebene Anzahl Reinigungen für diese Kassette erreicht ist. Dann verwendet der Server die nächste Reinigungskassette. Wenn Sie zwei oder mehr Reinigungskassetten zurückstellen und zwei oder mehr Befehle CLEAN DRIVE gleichzeitig ausgegeben, verwendet der Server mehrere Kassetten gleichzeitig und verringert die verbleibenden Reinigungen auf jeder Kassette.

Zugehörige Verweise:
AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Speicherarchiv prüfen)
CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
CLEAN DRIVE (Laufwerk reinigen)

LABEL LIBVOLUME (Datenträger im Speicherarchiv einen Kennsatz zuordnen)
QUERY LIBVOLUME (Datenträger im Speicherarchiv abfragen)

Fehler bei der Laufwerkreinigung beheben

Während Kassetten in einem Speicherarchiv versetzt werden, wird eine Datenkassette möglicherweise an eine Stelle versetzt, an der sich eine Reinigungskassette befinden sollte. Überprüfen Sie den Prozess, den der Server ausführt, und die Nachrichten, die ausgegeben werden, sodass Sie das Problem beheben können.

Wenn ein Laufwerk gereinigt werden muss, lädt der Server das, was laut Datenbank eine Reinigungskassette sein müsste, in das Laufwerk. Das Laufwerk wird dann in den Bereitstatus (READY) versetzt und IBM Spectrum Protect erkennt, dass es sich bei der Kassette um eine Datenkassette handelt. Der Server führt die folgenden Schritte aus:

1. Der Server versucht, den internen Bandkennsatz der Datenkassette zu lesen.
2. Der Server gibt die Kassette aus dem Laufwerk aus und stellt sie innerhalb des Speicherarchivs in den Ausgangsspeicherschacht der Reinigungskassette zurück. Wenn die Ausgabeoperation fehlschlägt, markiert der Server das Laufwerk als offline und gibt eine Nachricht aus, die besagt, dass sich die Kassette noch im Laufwerk befindet.
3. Der Server entnimmt die Reinigungskassette, um zu verhindern, dass sie für eine weitere Laufwerkreinigungsanforderung ausgewählt wird. Die Reinigungskassette verbleibt im Speicherarchiv, erscheint jedoch nicht mehr im IBM Spectrum Protect-Speicherarchivbestand.
4. Unter Verwendung des internen Bandkennsatzes gleicht der Server den Datenträgernamen mit dem aktuellen Speicherarchivbestand, mit den Speicherpooldatenträgern und mit der Protokolldatei für Datenträger ab.
    - Wenn der Datenträgername im Speicherarchivbestand nicht gefunden wird, wird unter Umständen fälschlicherweise eine Datenkassette als Reinigungskassette zurückgestellt. Wenn der Datenträger entnommen wird, müssen Sie keine weitere Aktion ausführen.
    - Wenn der Datenträgername im Speicherarchivbestand gefunden wird, gibt der Server Nachrichten aus, dass ein manueller Eingriff und eine Speicherarchivprüfung erforderlich sind. Um das Problem zu beheben, führen Sie die Anweisungen in Datenträgerbestand in einem Speicherarchiv prüfen aus.

Bandlaufwerke ersetzen

Wenn Sie ein Laufwerk in einem Bandarchiv ersetzen, das für IBM Spectrum Protect definiert ist, müssen Sie die Laufwerk- und Pfaddefinitionen für das alte Laufwerk löschen und das neue Laufwerk samt Pfad definieren.

Das Ersetzen von Laufwerk- und Pfaddefinitionen ist selbst dann erforderlich, wenn Sie ein Laufwerk durch ein anderes Laufwerk desselben Typs mit derselben logischen Adresse, derselben physischen Adresse, derselben SCSI-ID und derselben Portnummer austauschen. Die Aliasnamen der Einheiten können sich ändern, wenn Sie Ihre Laufwerkverbindungen ändern.

Wenn es sich bei dem neuen Laufwerk um ein Upgrade handelt, das ein neues Datenträgerformat unterstützt, müssen Sie unter Umständen auch ein neues logisches Speicherarchiv, eine neue Einheitenklasse und einen neuen Speicherpool definieren. Die Prozeduren für das Konfigurieren einer Maßnahme für ein neues Laufwerk in einem Speicherarchiv mit mehreren Laufwerken sind je nach Laufwerktyp und Datenträgertyp in dem Speicherarchiv unterschiedlich.

- Bandlaufwerke löschen
  Sie können Bandlaufwerke aus einem Speicherarchiv löschen. Beispielsweise können Sie ein Laufwerk, das nicht mehr verwendet wird oder das ersetzt werden soll, löschen.
- Laufwerke durch andere Laufwerke desselben Typs ersetzen
  Um ein Laufwerk hinzuzufügen, das dieselben Datenträgerformate wie das zu ersetzende Laufwerk unterstützt, müssen Sie ein neues Laufwerk und einen neuen Pfad definieren.
- Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde
  Wenn Sie ein Upgrade für alle Bandlaufwerke in einem Speicherarchiv durchführen, können Sie Ihre vorhandenen Maßnahmendefinitionen für die Umlagerung und den Verfall bestehender Daten beibehalten, während Sie die neuen Laufwerke zum Speichern neuer Daten verwenden können.

Bandlaufwerke löschen

Sie können Bandlaufwerke aus einem Speicherarchiv löschen. Beispielsweise können Sie ein Laufwerk, das nicht mehr verwendet wird oder das ersetzt werden soll, löschen.

Vorgehensweise

1. Stoppen Sie den IBM Spectrum Protect-Server und fahren Sie das Betriebssystem herunter.
2. Entfernen Sie das alte Laufwerk und befolgen Sie zum Installieren des neuen Laufwerks die Anweisungen des Herstellers.
3. Starten Sie das Betriebssystem und den IBM Spectrum Protect-Server erneut.
4. Löschen Sie den Pfad vom Server zum Laufwerk. Um beispielsweise einen Pfad von SERVER1 zu LIB1 zu löschen, geben Sie den folgenden Befehl aus:

```
delete path server1 lib1 srctype=server desttype=drive
```

5. Löschen Sie die Laufwerkdefinition. Geben Sie beispielsweise den folgenden Befehl aus, um ein Laufwerk mit dem Namen DLT1 aus einem Speicherarchiv mit dem Namen LIB1 zu löschen:

```
delete drive lib1 dlt1
```

Zugehörige Verweise:
DELETE DRIVE (Laufwerk aus einem Speicherarchiv löschen)
DELETE PATH (Pfad löschen)

Laufwerke durch andere Laufwerke desselben Typs ersetzen

Um ein Laufwerk hinzuzufügen, das dieselben Datenträgerformate wie das zu ersetzende Laufwerk unterstützt, müssen Sie ein neues Laufwerk und einen neuen Pfad definieren.

Informationen zu diesem Vorgang

Wenn ein Speicherarchiv nur ein einziges Laufwerkmodell enthält und ein Laufwerk ersetzt werden soll, müssen Sie das Laufwerk durch ein Laufwerk desselben Modells ersetzen. Wenn ein Speicherarchiv unterschiedliche Laufwerkmodelle enthält und ein Laufwerk ersetzt werden soll, können Sie das Laufwerk durch ein Laufwerk eines beliebigen Modells, das im Speicherarchiv vorhanden ist, ersetzen.

Vorgehensweise

1. Löschen Sie die Pfad- und Laufwerkdefinitionen für das alte Laufwerk. Um beispielsweise ein Laufwerk mit dem Namen DRIVE1 aus einem Speicherarchiv mit dem Namen LIB1 zu löschen, geben Sie den folgenden Befehl ein:

```
delete path server2 drive1 srctype=server desttype=drive library=lib1
delete drive lib1 drive1
```

2. Schalten Sie das Speicherarchiv aus, entfernen Sie das ursprüngliche Laufwerk, ersetzen Sie es durch das neue Laufwerk und schalten Sie das Speicherarchiv ein.
3. Aktualisieren Sie das Hostsystem, um sicherzustellen, dass das System das neue Laufwerk erkennt.
4. Definieren Sie das neue Laufwerk und den neuen Pfad. Um beispielsweise ein neues Laufwerk mit dem Namen DRIVE2 und einen Pfad von SERVER2 zu diesem Laufwerk zu definieren, wenn der IBM Spectrum Protect-Einheitentreiber verwendet wird, geben Sie die folgenden Befehle ein:

   AIX-Betriebssysteme

```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
   device=/dev/mt0
```

   Linux-Betriebssysteme

```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
   device=/dev/tsmscsi/mt0
```

   Windows-Betriebssysteme

```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
   device=mt3.0.0.1
```

   Tipp: Sie können Ihre vorhandenen Speicherarchiv-, Einheitenklassen- und Speicherpooldefinitionen verwenden.

Zugehörige Verweise:
DELETE DRIVE (Laufwerk aus einem Speicherarchiv löschen)
DELETE PATH (Pfad löschen)

Daten in Laufwerke umlagern, für die ein Upgrade durchgeführt wurde

Wenn Sie ein Upgrade für alle Bandlaufwerke in einem Speicherarchiv durchführen, können Sie Ihre vorhandenen Maßnahmendefinitionen für die Umlagerung und den Verfall bestehender Daten beibehalten, während Sie die neuen Laufwerke zum Speichern neuer Daten verwenden können.

Vorbereitende Schritte

Bei dem folgenden Szenario wird vorausgesetzt, dass bereits ein primärer Speicherpool mit dem Namen POOL1 für eine Einheitenklasse DISK vorhanden ist.

Vorgehensweise

1. Um Daten in einen Speicherpool umzulagern, der für die neuen Laufwerke erstellt wird, geben Sie den Parameter NEXTSTGPOOL an. Um beispielsweise Daten aus einem vorhandenen Speicherpool mit dem Namen POOL1 in den neuen Speicherpool mit dem Namen POOL2 umzulagern, geben Sie den folgenden Befehl aus:

   ```
   update stgpool pool1 nextstgpool=pool2
   ```

2. Aktualisieren Sie die Verwaltungsklassendefinitionen, um Daten mithilfe des Befehls UPDATE MGMTCLASS in dem neuen DISK-Speicherpool zu speichern.

Zugehörige Verweise:
DEFINE STGPOOL (Datenträger in einem Speicherpool definieren)
UPDATE MGMTCLASS (Verwaltungsklasse aktualisieren)
UPDATE STGPOOL (Speicherpool aktualisieren)

IBM Spectrum Protect-Server schützen

Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

- Administratoren verwalten
  Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.
- Kennwortanforderungen ändern
  Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.
- Server auf dem System schützen
  Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

Administratoren verwalten

Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Administratoreinstellungen zu ändern.

Task	Prozedur

Administrator hinzufügen	Um einen Administrator, ADMIN1, mit Systemberechtigung hinzuzufügen und ein Kennwort anzugeben, führen Sie die folgenden Schritte aus:
	a. Registrieren Sie den Administrator und geben Sie Pa$#$twO als Kennwort an, indem Sie den folgenden Befehl ausgeben:
	`register admin admin1 Pa$#$twO`
	b. Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`

Administratorberechtigung ändern	Ändern Sie die Berechtigungsstufe für einen Administrator, ADMIN1.
	• Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`
	• Entziehen Sie dem Administrator die Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`revoke authority admin1 classes=system`

Task	Prozedur
Administratoren entfernen	Entfernen Sie einen Administrator, ADMIN1, sodass er nicht mehr auf den IBM Spectrum Protect-Server zuzugreifen kann, indem Sie den folgenden Befehl ausgeben: `remove admin admin1`
Zugriff auf den Server vorübergehend verhindern	Sperren oder entsperren Sie einen Administrator, indem Sie den Befehl LOCK ADMIN bzw. UNLOCK ADMIN verwenden.

Zugehörige Konzepte:
Planung für Administratorrollen

Kennwortanforderungen ändern

Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.

Informationen zu diesem Vorgang

Indem Sie die Kennwortauthentifizierung durchsetzen und Kennworteinschränkungen verwalten, können Sie Ihre Daten und Ihre Server vor möglichen Sicherheitsrisiken schützen.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Kennwortanforderungen für IBM Spectrum Protect-Server zu ändern.

Tabelle 1. Authentifizierungstasks für IBM Spectrum Protect-Server

Task	Prozedur
Grenzwert für ungültige Kennworteingabeversuche festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl ungültiger Versuche im Feld Grenzwert für ungültige Anmeldeversuche an. Der Standardwert bei der Installation ist 0.
Mindestlänge für Kennwörter festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl Zeichen im Feld Mindestlänge für Kennwort an.
Ablaufzeitraum für Kennwörter festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl Tage im Feld Allgemeine Kennwortablaufdauer an.
Kennwortauthentifizierung inaktivieren	Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer ein Kennwort eingeben, um auf den Server zugreifen zu können. Sie können die Kennwortauthentifizierung nur für Kennwörter inaktivieren, die mit dem Server (LOCAL) authentifiziert werden. Durch das Inaktivieren der Kennwortauthentifizierung erhöht sich das Sicherheitsrisiko für den Server.

Task	Prozedur

Standardauthentifizierungsmethode festlegen	Geben Sie den Befehl SET DEFAULTAUTHENTICATION aus. Um beispielsweise den Server als die Standardauthentifizierungsmethode zu verwenden, geben Sie den folgenden Befehl aus:
	`set defaultauthentication local`
	Um einen Clientknoten für die Authentifizierung mit dem Server zu aktualisieren, schließen Sie `AUTHENTICATION=LOCAL` in den Befehl UPDATE NODE ein:
	`update node authentication=local`

Server auf dem System schützen

Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

Vorgehensweise

Stellen Sie sicher, dass nicht berechtigte Benutzer nicht auf die Verzeichnisse für die Serverdatenbank und die Serverinstanz zugreifen können. Behalten Sie die Zugriffseinstellungen für diese Verzeichnisse bei, die Sie während der Implementierung konfiguriert haben.

- Benutzerzugriff auf den Server einschränken
  Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Server stoppen und starten

Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.

Vorbereitende Schritte

Um den IBM Spectrum Protect-Server stoppen und starten zu können, müssen Sie über System- oder Bedienerberechtigung verfügen.

- Server stoppen
  Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.
- Server für Verwaltungs- oder Rekonfigurationstasks starten
  Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

Server stoppen

Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

Informationen zu diesem Vorgang

Wenn Sie den Befehl HALT zum Stoppen des Servers ausgeben, werden die folgenden Aktionen ausgeführt:

- Alle Prozesse und Clientknotensitzungen werden abgebrochen.
- Alle aktuellen Transaktionen werden gestoppt. (Die Transaktionen werden rückgängig gemacht, wenn der Server erneut gestartet wird.)

Vorgehensweise

Um das System vorzubereiten und den Server zu stoppen, führen Sie die folgenden Schritte aus:

1. Verhindern Sie, dass neue Clientknotensitzungen gestartet werden, indem Sie den Befehl DISABLE SESSIONS ausgeben:

   ```
   disable sessions all
   ```

2. Bestimmen Sie, ob Clientknotensitzungen oder -prozesse aktiv sind, indem Sie die folgenden Schritte ausführen:

a. Rufen Sie die Seite Übersicht im Operations Center auf, auf der im Bereich Aktivität die Gesamtzahl Prozesse und Sitzungen angezeigt wird, die derzeit aktiv sind. Wenn die Zahlen erheblich von den Zahlen abweichen, die normalerweise während Ihrer täglichen Speicherverwaltungsroutine angezeigt werden, überprüfen Sie mithilfe weiterer Statusanzeiger im Operations Center, ob ein Problem vorliegt.
b. Zeigen Sie das Diagramm im Bereich Aktivität an, um den Umfang des Datenaustauschs im Netz für die folgenden Perioden zu vergleichen:
   - Die laufende Periode, d. h. die letzte 24-Stunden-Periode
   - Die vorherige Periode, d. h. die 24 Stunden vor der laufenden Periode

   Wenn das Diagramm für die vorherige Periode den erwarteten Umfang des Datenaustauschs darstellt, können deutliche Abweichungen in dem Diagramm für die laufende Periode auf ein Problem hindeuten.
c. Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details. Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, rufen Sie mithilfe von Verwaltungsbefehlen Informationen zu Prozessen ab. Geben Sie den Befehl QUERY PROCESS aus, um Prozesse abzufragen; geben Sie den Befehl QUERY SESSION aus, um Informationen zu Sitzungen abzurufen.

3. Warten Sie, bis die Clientknotensitzungen abgeschlossen sind oder brechen Sie diese ab. Um Prozesse und Sitzungen abzubrechen, führen Sie die folgenden Schritte aus:
   - Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
   - Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
   - Klicken Sie auf Abbrechen.
   - Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, brechen Sie Sitzungen mithilfe von Verwaltungsbefehlen ab. Geben Sie den Befehl CANCEL SESSION aus, um eine Sitzung abzubrechen; geben Sie den Befehl CANCEL PROCESS aus, um Prozesse abzubrechen.
     Tipp: Wenn der Prozess, der abgebrochen werden soll, auf die Bereitstellung eines Banddatenträgers wartet, wird die Mountanforderung abgebrochen. Wenn Sie beispielsweise einen Befehl EXPORT, IMPORT oder MOVE DATA ausgeben, leitet der Befehl möglicherweise einen Prozess ein, der die Bereitstellung eines Banddatenträgers erfordert. Wenn jedoch ein Banddatenträger durch ein automatisiertes Speicherarchiv bereitgestellt wird, wird die Abbruchoperation unter Umständen erst wirksam, wenn der Bereitstellungsprozess abgeschlossen ist. Abhängig von Ihrer Systemumgebung kann dies mehrere Minuten dauern.

4. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

```
halt
```

Server für Verwaltungs- oder Rekonfigurationstasks starten

Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

Informationen zu diesem Vorgang

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm DSMSERV mit dem Parameter MAINTENANCE ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.
Tipps:

- Sie müssen die Serveroptionsdatei, dsmserv.opt, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung, den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

Vorgehensweise

Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

```
dsmserv maintenance
```

Tipp: Informationen zum Anzeigen eines Ein Video zum Starten des Servers im Verwaltungsmodus kann über Server im Verwaltungsmodus starten angezeigt werden.

Nächste Schritte

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl HALT ausgeben:

   ```
   halt
   ```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden. Führen Sie die Anweisungen für Ihr Betriebssystem aus:
   - AIX-BetriebssystemeServerinstanz starten
   - Linux-BetriebssystemeServerinstanz starten
   - Windows-BetriebssystemeServerinstanz starten

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

Durchführung eines Upgrades für den Server planen

Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.

Informationen zu diesem Vorgang

Beachten Sie diese Richtlinien:

- Bei der bevorzugten Methode erfolgt das Upgrade für den Server mithilfe des Installationsassistenten. Nachdem Sie den Assistenten gestartet haben, klicken Sie im Fenster IBM Installation Manager auf das Symbol zum Aktualisieren; klicken Sie nicht auf das Symbol zum Installieren oder Ändern!
- Wenn sowohl für die Serverkomponente als auch für die Operations Center-Komponente Upgrades verfügbar sind, wählen Sie die Kontrollkästchen aus, um das Upgrade für beide Komponenten durchzuführen.

Vorgehensweise

1. Überprüfen Sie die Liste der Fixpacks und vorläufigen Fixes. Siehe Technote 1239415.
2. Studieren Sie die Produktverbesserungen, die in der Readme-Datei beschrieben sind.
   Tipp: Wenn Sie die Installationspaketdatei von der IBM Spectrum Protect-Unterstützungssite abrufen, können Sie auch auf die Readme-Datei zugreifen.
3. Stellen Sie sicher, dass die Version, auf die das Upgrade für Ihren Server durchgeführt wird, mit anderen Komponenten, wie beispielsweise Speicheragenten und Speicherarchivclients, kompatibel ist. Siehe Technote 1302789.
4. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden. Siehe Technote 1053218.
5. Lesen Sie die Upgradeanweisungen. Stellen Sie sicher, dass Sie die Serverdatenbank, die Einheitenkonfigurationsinformationen und die Protokolldatei für Datenträger sichern.

Nächste Schritte

Um ein Fixpack oder einen vorläufigen Fix zu installieren, führen Sie die Anweisungen für Ihr Betriebssystem aus:

- AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
- Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
- Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren

Zugehörige Informationen:
Upgrade- und Umlagerungsprozess - Häufig gestellte Fragen

Vorbereitungen für einen Ausfall oder eine Systemaktualisierung

Treffen Sie Vorbereitungen in IBM Spectrum Protect, damit Ihr System während eines geplanten Stromausfalls oder einer geplanten Systemaktualisierung in einem konsistenten Zustand verbleibt.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass Sie die regelmäßige Ausführung von Aktivitäten planen, um den Server zu verwalten und zu schützen. Informationen zum Planen von Aktivitäten wie beispielsweise Sichern der Datenbank, Sichern der Einheitenkonfigurationsdatei und Sichern des Datenträgerprotokolls finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren.

Vorgehensweise

1. Brechen Sie Prozesse und Sitzungen, die aktiv sind, ab, indem Sie die folgenden Schritte ausführen:

a. Wählen Sie im Operations Center auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
b. Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
c. Klicken Sie auf Abbrechen.

2. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

```
halt
```

Tipp: Sie können den Befehl HALT im Operations Center ausgeben, indem Sie den Mauszeiger über das Symbol für Einstellungen bewegen und auf Command Builder klicken. Wählen Sie dann den Server aus, geben Sie `halt` ein und drücken Sie die Eingabetaste.

Zugehörige Verweise:
HALT (Server herunterfahren)

Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM

IBM Spectrum Protect stellt die Funktion Disaster Recovery Manager (DRM) für die Wiederherstellung Ihrer Server- und Clientdaten bei einem Katastrophenfall zur Verfügung.

DRM verfolgt die Versetzung ausgelagerter Datenträger und registriert diese Informationen in der IBM Spectrum Protect-Datenbank. DRM konsolidiert Pläne, Scripts und andere Informationen in einer Plandatei, die im Katastrophenfall oder bei einer ungeplanten Betriebsunterbrechung zum Wiederherstellen des IBM Spectrum Protect-Servers erforderlich ist.
Einschränkung: DRM ist nur im Produkt IBM Spectrum Protect Extended Edition verfügbar.

- Plandatei zur Wiederherstellung nach einem Katastrophenfall
  Die Plandatei zur Wiederherstellung nach einem Katastrophenfall, die auch als Wiederherstellungsplandatei bezeichnet wird, enthält die Informationen, die zum Wiederherstellen eines IBM Spectrum Protect-Servers mit dem Stand des Zeitpunkts der letzten Datenbanksicherungsoperation, die vor der Erstellung des Plans abgeschlossen wurde, erforderlich sind.
- Server und Clientdaten mithilfe von DRM wiederherstellen
  Verwenden Sie die Funktion 'Disaster Recovery Manager' (DRM), um den IBM Spectrum Protect-Server und Clientdaten im Katastrophenfall wiederherzustellen.
- Drilloperation für die Wiederherstellung nach einem Katastrophenfall ausführen
  Planen Sie Drilloperationen für die Wiederherstellung nach einem Katastrophenfall als Vorbereitung für Prüfungen, mit denen die Wiederherstellbarkeit des IBM Spectrum Protect-Servers bestätigt wird, und um sicherzustellen, dass nach einem Ausfall Daten zurückgeschrieben und Operationen wiederaufgenommen werden können. Mithilfe einer Drilloperation können Sie außerdem vor dem Eintreten einer kritischen Situation sicherstellen, dass alle Daten zurückgeschrieben und Operationen wiederaufgenommen werden können.
- Datenbank zurückschreiben
  Wenn die Funktion 'Disaster Recovery Manager' (DRM) aktiviert ist und Sie die Prozedur zur Vorbereitung auf einen Katastrophenfall ausgeführt haben, können Sie die Datenbank nach einem Katastrophenfall zurückschreiben. Wenn DRM nicht konfiguriert ist, können Sie die Datenbank dennoch zurückschreiben, vorausgesetzt, Sie verfügen über die erforderlichen Sicherungsdateien.

Plandatei zur Wiederherstellung nach einem Katastrophenfall

Die Plandatei zur Wiederherstellung nach einem Katastrophenfall, die auch als Wiederherstellungsplandatei bezeichnet wird, enthält die Informationen, die zum Wiederherstellen eines IBM Spectrum Protect-Servers mit dem Stand des Zeitpunkts der letzten Datenbanksicherungsoperation, die vor der Erstellung des Plans abgeschlossen wurde, erforderlich sind.

Der Plan besteht aus Zeilengruppen, die Sie in mehrere Dateien aufteilen können. Jede Zeilengruppe verfügt über eine Anfangsanweisung (begin) und eine Endanweisung (end).

Tabelle 1. Zeilengruppen in der Wiederherstellungsplandatei

Zeilengruppe	Informationen in der Zeilengruppe
SERVER.REQUIREMENTS	Gibt den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll für den Server an.
RECOVERY.INSTRUCTIONS.GENERAL	Gibt standortspezifische Anweisungen an, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.GENERAL angegebene Datei eingibt. Die Anweisungen umfassen die Wiederherstellungsstrategie, die Namen der wichtigsten Ansprechpartner, eine Übersicht über die wichtigsten Anwendungen, die von diesem Server gesichert werden, und andere relevante Wiederherstellungsanweisungen.

Zeilengruppe	Informationen in der Zeilengruppe
RECOVERY.INSTRUCTIONS.OFFSITE	Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.OFFSITE angegebene Datei eingibt. Die Anweisungen umfassen den Namen und den Standort der Vault an einem anderen Standort sowie Informationen dazu, wie Kontakt zum Vaultadministrator aufgenommen werden kann (beispielsweise ein Name und eine Telefonnummer).
RECOVERY.INSTRUCTIONS.INSTALL	Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.INSTALL angegebene Datei eingibt. Die Anweisungen umfassen Informationen, die angeben, wie der Basisserver wiederhergestellt wird, und den Aufbewahrungsort der Sicherungskopien des Systemimage.
RECOVERY.INSTRUCTIONS.DATABASE	Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.DATABASE angegebene Datei eingibt. Die Anweisungen umfassen Informationen, die angeben, wie die Datenbankwiederherstellung vorbereitet wird. Sie können beispielsweise Anweisungen eingeben, die angeben, wie die Sicherungsdatenträger für ein automatisiertes Speicherarchiv initialisiert oder geladen werden sollen. Für diese Zeilengruppe wird kein Beispiel bereitgestellt.
RECOVERY.INSTRUCTIONS.STGPOOL	Enthält Anweisungen, die der Administrator in die durch das Präfix RECOVERY.INSTRUCTIONS.STGPOOL angegebene Datei eingibt. Die Anweisungen umfassen die Namen Ihrer Softwareanwendungen und der Kopienspeicherpools, die die Sicherung dieser Anwendungen enthalten. Für diese Zeilengruppe wird kein Beispiel bereitgestellt.
RECOVERY.VOLUMES.REQUIRED	Stellt eine Liste der Datenbanksicherungs- und Kopienspeicherpooldatenträger bereit, die zum Wiederherstellen des Servers erforderlich sind. Ein Datenbanksicherungsdatenträger wird eingeschlossen, wenn er Bestandteil der jüngsten Datenbanksicherungsserie ist. Ein Kopienspeicherpooldatenträger wird eingeschlossen, wenn er nicht leer und nicht als dauerhaft beschädigt markiert ist.
RECOVERY.DEVICES.REQUIRED	Stellt Details zu den Einheiten bereit, die zum Lesen der Sicherungsdatenträger erforderlich sind.
RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE	Enthält ein Script mit den Befehlen, die zum Wiederherstellen des Servers erforderlich sind.
RECOVERY.SCRIPT.NORMAL.MODE	Enthält ein Script mit den Befehlen, die zum Zurückschreiben der primären Speicherpools des Servers erforderlich sind.
DB.STORAGEPATHS	Gibt die Verzeichnisse für die IBM Spectrum Protect-Datenbank an.
LICENSE.REGISTRATION	Enthält ein Makro zum Registrieren Ihrer Serverlizenzen.
COPYSTGPOOL.VOLUMES.AVAILABLE	Enthält ein Makro zum Markieren von Kopienspeicherpooldatenträgern, die an einen anderen Standort transportiert wurden und anschließend wieder vor Ort transportiert wurden. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle ausgeben. Es ist auch möglich, das Makro in eine Datei zu kopieren, zu ändern und auszuführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.
COPYSTGPOOL.VOLUMES.DESTROYED	Enthält ein Makro, mit dem Kopienspeicherpooldatenträger als nicht verfügbar markiert werden können, wenn sich die Datenträger zum Zeitpunkt der Katastrophe vor Ort befanden. Diese Datenträger werden als ausgelagert betrachtet und wurden bei einem Katastrophenfall nicht dauerhaft beschädigt. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausgeben oder Sie können das Makro in eine Datei kopieren, ändern und ausführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.

Zeilengruppe	Informationen in der Zeilengruppe
PRIMARY.VOLUMES.DESTROYED	Enthält ein Makro, mit dem Datenträger für primäre Speicherpools als dauerhaft beschädigt markiert werden können, wenn sich die Datenträger zum Zeitpunkt der Katastrophe vor Ort befanden. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausführen oder Sie können das Makro in eine Datei kopieren, ändern und ausführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.
PRIMARY.VOLUMES.REPLACEMENT	Enthält ein Makro zum Ermitteln der Ersatzdatenträger für primäre Speicherpools. Sie können die Informationen als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausführen oder Sie können das Makro in eine Datei kopieren, ändern und ausführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE gestartet.
STGPOOLS.RESTORE	Enthält ein Makro zum Zurückschreiben der primären Speicherpools. Sie können die Zeilengruppe als Leitfaden verwenden und die Verwaltungsbefehle über eine Befehlszeile ausführen. Es ist auch möglich, das Makro in eine Datei zu kopieren, zu ändern und auszuführen. Dieses Makro wird vom Script RECOVERY.SCRIPT.NORMAL.MODE gestartet.
VOLUME.HISTORY.FILE	Enthält eine Kopie der Datenträgerprotokolldaten zum Erstellungszeitpunkt des Wiederherstellungsplans. Das Dienstprogramm DSMSERV RESTORE DB bestimmt mithilfe der Protokolldatei für Datenträger, welche Datenträger zum Zurückschreiben der Datenbank erforderlich sind. Die Protokolldatei für Datenträger wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE verwendet.
DEVICE.CONFIGURATION.FILE	Enthält eine Kopie der Servereinheitenkonfigurationsdaten zum Erstellungszeitpunkt des Wiederherstellungsplans. Das Dienstprogramm DSMSERV RESTORE DB liest mithilfe der Einheitenkonfigurationsdatei die Datenbanksicherungsdatenträger. Die Einheitenkonfigurationsdatei wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE verwendet.
DSMSERV.OPT.FILE	Enthält eine Kopie der Serveroptionsdatei. Diese Zeilengruppe wird vom Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE verwendet.
LICENSE.INFORMATION	Enthält eine Kopie der neuesten Ergebnisse der Lizenzprüfung und der Serverlizenzbedingungen.
MACHINE.GENERAL.INFORMATION	Stellt Informationen für die Servermaschine bereit, wie beispielsweise ihr Standort, die zum Wiederherstellen der Servermaschine erforderlich sind. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn die Maschineninformationen mithilfe des Befehls DEFINE MACHINE unter Angabe von ADSMSERVER=YES in der Datenbank gespeichert werden.
MACHINE.RECOVERY.INSTRUCTIONS	Stellt die Wiederherstellungsanweisungen für die Servermaschine bereit. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn die Wiederherstellungsanweisungen für die Maschine in der Datenbank gespeichert werden.
MACHINE.RECOVERY.CHARACTERISTICS	Stellt die Hardware- und Softwarekenndaten für die Servermaschine bereit. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn die Maschinenkenndaten in der Datenbank gespeichert werden.
MACHINE.RECOVERY.MEDIA	Stellt Informationen zu den Datenträgern bereit, die für die Wiederherstellung der Maschine, die den Server enthält, erforderlich sind. Diese Zeilengruppe wird in die Plandatei eingeschlossen, wenn Informationen zu Wiederherstellungsdatenträgern in der Datenbank gespeichert werden und der Maschine zugeordnet sind, die den Server enthält.

Server und Clientdaten mithilfe von DRM wiederherstellen

Verwenden Sie die Funktion 'Disaster Recovery Manager' (DRM), um den IBM Spectrum Protect-Server und Clientdaten im Katastrophenfall wiederherzustellen.

Vorbereitende Schritte

IBM Spectrum Protect ist für die Verwendung des Protokolls Secure Sockets Layer (SSL) für die Client/Server-Authentifizierung konfiguriert. Wenn Sie den Server starten, wird im Rahmen des Prozesses eine Datei mit einem digitalen Zertifikat (cert.kdb) erstellt. Diese Datei enthält den öffentlichen Schlüssel des Servers, der dem Client das Verschlüsseln von Daten ermöglicht. Die Datei mit dem digitalen Zertifikat kann nicht in der Serverdatenbank gespeichert werden, da Global Security Kit (GSKit) eine separate Datei in einem bestimmten Format erfordert.

Der Masterverschlüsselungsschlüssel ist in einer neuen, von GSKit verwalteten Schlüsseldatenbank, dsmkeydb.kdb, gespeichert. Wenn der Server über einen vorhandenen Masterverschlüsselungsschlüssel verfügt, wird der Masterverschlüsselungsschlüssel aus der Datei dsmserv.pwd in die Schlüsseldatenbank dsmkeydb.kdb umgelagert. Bewahren Sie Sicherungskopien der Dateien dsmkeydb.kdb und dsmkeydb.sth auf. Sie können den Befehl BACKUP DB zum Sichern des Masterverschlüsselungsschlüssels konfigurieren oder die Dateien dsmkeydb.kdb und dsmkeydb.sth selbst manuell sichern.

1. Bewahren Sie Sicherungskopien der Dateien cert.kdb, cert.sth und cert256.arm auf.
2. Wenn sowohl die ursprünglichen Zertifikatsdateien als auch alle Kopien verloren gehen oder beschädigt werden, generieren Sie neue Zertifikatsdateien.

Vorgehensweise

1. Rufen Sie den neuesten Wiederherstellungsplan ab.
2. Überprüfen Sie die Wiederherstellungsschritte, die in der Zeilengruppe RECOVERY.INSTRUCTIONS.GENERAL des Plans beschrieben sind.
3. Unterteilen Sie die Zeilengruppen der Plandatei nach allgemeinen Vorabanweisungen, Scripts zur Wiederherstellung des IBM Spectrum Protect-Servers und Anweisungen zur Clientwiederherstellung in einzelne Dateien.
4. Rufen Sie alle erforderlichen Wiederherstellungsdatenträger (wie in dem Plan aufgelistet) vom Aufbewahrungsort ab.
5. Überprüfen Sie die Einheitenkonfigurationsdatei, um sicherzustellen, dass die Hardwarekonfiguration am Wiederherstellungsstandort mit der am ursprünglichen Standort identisch ist. Alle Unterschiede müssen in der Einheitenkonfigurationsdatei aktualisiert werden. Für die folgenden Beispielkonfigurationsänderungen sind Aktualisierungen der Konfigurationsinformationen erforderlich:
   - Unterschiedliche Einheitennamen
   - Anforderung bei automatisierten Speicherarchiven, die Datenbanksicherungsdatenträger manuell in das automatisierte Speicherarchiv einlegen und die Konfigurationsinformationen aktualisieren zu müssen, um das Element in dem Speicherarchiv zu identifizieren. Dies ermöglicht es dem Server, die erforderlichen Datenbanksicherungsdatenträger zu lokalisieren.
6. Konfigurieren Sie Ersatzhardware für den IBM Spectrum Protect-Server, einschließlich der Installation des Betriebssystems und des IBM Spectrum Protect-Basisrelease.
7. Führen Sie die Scripts zur Wiederherstellung des IBM Spectrum Protect-Servers im Wiederherstellungsplan aus. Die Zeilengruppen RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE und RECOVERY.SCRIPT.NORMAL.MODE enthalten ausführbare Befehlsdateien, mit denen die Wiederherstellung des IBM Spectrum Protect-Servers gesteuert werden kann, indem andere im Plan generierte Befehlsdateien aufgerufen werden. Mit dem Script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE wird der Server bis zu dem Punkt wiederhergestellt, an dem Clients Zurückschreibungen direkt von den Kopienspeicherpooldatenträgern starten können.
8. Schreiben Sie die primären Speicherpools mithilfe des Scripts RECOVERY.SCRIPT.NORMAL.MODE zurück.
9. Starten Sie Clientzurückschreibungsoperationen beginnend mit der höchsten Priorität gemäß der allgemeinen Planung.

Nächste Schritte

Der IBM Spectrum Protect-Server kann jetzt für normale Serveroperationen verwendet werden. Stellen Sie sicher, dass alle erforderlichen Operationen geplant sind. Anweisungen finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren und Sicherungs- und Archivierungsoperationen planen.

Zugehörige Tasks:

Daten in Verzeichniscontainerspeicherpools reparieren und wiederherstellen

Zugehörige Verweise:

PREPARE (Wiederherstellungsplandatei erstellen)

Drilloperation für die Wiederherstellung nach einem Katastrophenfall ausführen

Planen Sie Drilloperationen für die Wiederherstellung nach einem Katastrophenfall als Vorbereitung für Prüfungen, mit denen die Wiederherstellbarkeit des IBM Spectrum Protect-Servers bestätigt wird, und um sicherzustellen, dass nach einem Ausfall Daten zurückgeschrieben und Operationen wiederaufgenommen werden können. Mithilfe einer Drilloperation können Sie außerdem vor dem Eintreten einer kritischen Situation sicherstellen, dass alle Daten zurückgeschrieben und Operationen wiederaufgenommen werden können.

Vorbereitende Schritte

Führen Sie die folgenden Tasks aus:

- Planen Sie die regelmäßige Ausführung von Aktivitäten, um den Server zu verwalten und zu schützen. Weitere Informationen zur Planung von Aktivitäten finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren. Stellen Sie sicher, dass Sie die folgenden Tasks planen:
  - Sichern der Datenbank.

- Versetzen von Datenträgern an einen anderen Standort.
- Sichern der Einheitenkonfigurationsdatei, der Protokolldatei für Datenträger und der Serveroptionsdatei dsmserv.opt.
- **Optional:** Ausgabe des Befehls PREPARE zum Erstellen der Plandatei zur Wiederherstellung nach einem Katastrophenfall.

Tipp:

Wenn Sie den Befehl PREPARE ausgeben, wird von der IBM Spectrum Protect-Funktion 'Disaster Recovery Manager' (DRM) exakt eine Kopie der Plandatei zur Wiederherstellung nach einem Katastrophenfall erstellt.

Sie können die Wiederherstellung nach einem Katastrophenfall mithilfe eines anderen Standorts ohne die Verwendung von DRM ausführen, DRM ist jedoch hilfreich, um Pläne, Scripts und andere Informationen, die während der Wiederherstellung nach einem Katastrophenfall erforderlich sind, zu konsolidieren.

Erstellen Sie zur Sicherheit mehrere Kopien des Plans. Bewahren Sie Kopien beispielsweise in gedruckter Form, auf einem USB-Flashlaufwerk, in Plattenspeicher an einem anderen Standort oder auf einem fernen Server auf. Die Wiederherstellungsplandatei wird täglich zusammen mit den Bändern ausgelagert. Weitere Informationen zu DRM finden Sie in Vorbereitungen für einen Katastrophenfall und Wiederherstellung nach einem Katastrophenfall mithilfe von DRM.

- Konfigurieren Sie die folgenden Ressourcen am Standort zur Wiederherstellung nach einem Katastrophenfall:
  1. Einen IBM Spectrum Protect-Wiederherstellungsserver. Der Server am Standort zur Wiederherstellung nach einem Katastrophenfall muss dieselbe Version wie der Server am Produktionsstandort haben.
  2. Ein Bandarchiv zum Speichern der Datenträger, die vom Produktionsstandort geliefert werden. Weitere Informationen zu Auslagerungsstandorten für die Wiederherstellung finden Sie in Auslagerung von Daten.
  3. Plattenspeicherplatz für die Datenbank, das Archivprotokoll, aktive Protokolldateien und Speicherpools.
  4. Clients zum Testen von Zurückschreibungsoperationen.

Informationen zu diesem Vorgang

Testen Sie den Plan zur Wiederherstellung nach einem Katastrophenfall und die Wiederherstellbarkeit des IBM Spectrum Protect-Servers häufig und in einer ähnlichen Umgebung wie der Produktionsumgebung.

Vorgehensweise

1. Stellen Sie sicher, dass Bänder vor Ort verfügbar sind. Geben Sie den Befehl QUERY LIBVOLUME aus, um Datenträger, die in ein automatisiertes Speicherarchiv zurückgestellt wurden, zu ermitteln.
2. Sichern Sie die Datenbank auf den Bändern vor Ort, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie auf der Seite Server im Operations Center den Server aus, dessen Datenbank gesichert werden soll.
   b. Klicken Sie auf Sichern und führen Sie die Anweisungen im Fenster Datenbank sichern aus.
3. Kopieren Sie die folgenden Dateien in das Ausgangsverzeichnis des Servers am Wiederherstellungsstandort:
   - Wiederherstellungsplandatei
   - Protokolldatei für Datenträger
   - Einheitenkonfigurationsdatei
   - Optional: Serveroptionsdatei dsmserv.opt
4. Senden Sie das Band an den Auslagerungsstandort für die Wiederherstellung.
5. Schreiben Sie die Serverdatenbank zurück, indem Sie auf dem Wiederherstellungsserver den Befehl DSMSERV RESTORE DB verwenden. Weitere Informationen zum Zurückschreiben der Serverdatenbank finden Sie in Datenbank zurückschreiben.
6. Geben Sie den Befehl UPDATE VOLUME unter Angabe des Parameters ACCESS=DESTROYED aus, um anzugeben, dass ein Datenträger vollständig zurückgeschrieben werden muss.
7. Schreiben Sie auf dem Wiederherstellungsserver die Speicherpooldatenträger mithilfe des Befehls RESTORE STGPOOL zurück.

Nächste Schritte

Stellen Sie sicher, dass Sie auf die Daten in dem Speicherarchiv zugreifen können, indem Sie einen Banddatenträger in dem zurückgeschriebenen Speicherpool prüfen, um zu verifizieren, dass die Daten konsistent sind. Geben Sie den Befehl AUDIT VOLUME aus, um einen Banddatenträger zu prüfen. Prüfen Sie für eine schnellere Verarbeitung nur zurückgeschriebene Daten.

Zugehörige Tasks:

Datenträgerbestand in einem Speicherarchiv prüfen

Zugehörige Verweise:

AUDIT VOLUME (Datenbankinformationen für einen Speicherpooldatenträger prüfen)

DSMSERV RESTORE DB (Datenbank zurückschreiben)

RESTORE STGPOOL (Speicherpooldaten zurückschreiben)

Datenbank zurückschreiben

Wenn die Funktion 'Disaster Recovery Manager' (DRM) aktiviert ist und Sie die Prozedur zur Vorbereitung auf einen Katastrophenfall ausgeführt haben, können Sie die Datenbank nach einem Katastrophenfall zurückschreiben. Wenn DRM nicht konfiguriert ist, können Sie die Datenbank dennoch zurückschreiben, vorausgesetzt, Sie verfügen über die erforderlichen Sicherungsdateien.

Vorbereitende Schritte

Wenn die Verzeichnisse für die Datenbank und das Wiederherstellungsprotokoll nicht mehr vorhanden sind, erstellen Sie diese erneut, bevor Sie das Serverdienstprogramm DSMSERV RESTORE DB ausführen.

Informationen zu diesem Vorgang

Sie können die Datenbank mit dem neuesten Stand oder mit dem Stand eines angegebenen Zeitpunkts zurückschreiben. Um die Datenbank mit dem Stand wiederherzustellen, den sie zu dem Zeitpunkt hatte, zu dem sie verloren ging, stellen Sie die Datenbank mit der neuesten Version wieder her.
Einschränkungen:

- Um die Datenbank mit der neuesten Version zurückzuschreiben, müssen Sie das Archivprotokollverzeichnis lokalisieren. Wenn Sie das Verzeichnis nicht lokalisieren können, kann die Datenbank nur mit dem Stand eines bestimmten Zeitpunkts zurückgeschrieben werden.
- Sie können das Protokoll Secure Sockets Layer (SSL) nicht für Datenbankzurückschreibungsoperationen verwenden.
- Wenn der Release-Level der Datenbanksicherung und der Release-Level des Servers, für den die Zurückschreibung erfolgt, unterschiedlich sind, können Sie die Serverdatenbank nicht zurückschreiben. Wenn Sie beispielsweise einen Server der Version 8.1 verwenden und versuchen, eine Datenbank der Version 7.1 zurückzuschreiben, tritt ein Fehler auf.

Vorgehensweise

Verwenden Sie das Serverdienstprogramm DSMSERV RESTORE DB, um die Datenbank zurückzuschreiben. Wählen Sie abhängig von der Version der Datenbank, die zurückgeschrieben werden soll, eine der folgenden Methoden aus:

- Zurückschreiben einer Datenbank mit der neuesten Version. Verwenden Sie beispielsweise den folgenden Befehl:

  ```
  dsmserv restore db
  ```

- Zurückschreiben einer Datenbank mit dem Stand eines bestimmten Zeitpunkts. Um beispielsweise die Datenbank mit einer Sicherungsserie zurückzuschreiben, die am 19. April 2017 erstellt wurde, verwenden Sie den folgenden Befehl:

  ```
  dsmserv restore db todate=04/19/2017
  ```

Zugehörige Verweise:
DSMSERV RESTORE DB (Datenbank zurückschreiben)

Serverlösungsdokumentation in PDF-Dateien

Vordefinierte PDF-Dateien für die IBM Spectrum Protect-Dokumentation sind zum Download verfügbar.

Die folgenden vordefinierten PDF-Dateien sind für IBM Spectrum Protect-Datenschutzlösungen verfügbar:

- Einführung in Datenschutzlösungen
- Plattenspeicherlösung für einen einzelnen Standort
- Plattenspeicherlösung für mehrere Standorte
- Bandspeicherlösung

Weitere vordefinierte PDF-Dateien der Serverdokumentation finden Sie in der vollständigen Liste.

IBM Spectrum Protect-Server

IBM Spectrum Protect-Server speichern und verwalten Sicherungsdaten, Archivierungsdaten und speicherverwaltete Daten für Clients für Sichern/Archivieren und andere IBM Spectrum Protect- und IBM Spectrum Protect Snapshot-Komponenten.

- Neuerungen
  Lesen Sie die Informationen zu neuen Funktionen und Aktualisierungen für Serverkomponenten in IBM Spectrum Protect Version 8.1.
- Installieren und Upgrade durchführen
  Sie können einzelne oder mehrere Komponenten in Ihrem Unternehmensnetz installieren oder für die Komponenten ein Upgrade durchführen. Mithilfe der verfügbaren Lösungsdokumentation können Sie eine Best-Practice-Lösung auf der Basis Ihrer Unternehmensanforderungen auswählen und dann diese Lösung installieren, konfigurieren und überwachen sowie mit dieser Lösung arbeiten.
- Konfigurieren und verwalten
  Lesen Sie die Informationen in der verfügbaren Dokumentation, um Konfigurationstasks für den Server auszuführen.
- Serverbefehle, -optionen und -dienstprogramme
  Verwenden Sie Befehle, um den Server zu verwalten und zu konfigurieren, verwenden Sie Optionen, um den Server anzupassen, und verwenden Sie Dienstprogramme, um spezielle Tasks auszuführen, wenn der Server nicht aktiv ist.
- Serverdokumentation in PDF-Dateien
  Vorgefertigte PDF-Dateien für die IBM Spectrum Protect-Dokumentation sind zum Herunterladen verfügbar.

Neuerungen

Lesen Sie die Informationen zu neuen Funktionen und Aktualisierungen für Serverkomponenten in IBM Spectrum Protect Version 8.1.

Tipp: Rufen Sie die Videobibliothek auf, um Videos zu den neuen Funktionen und Aktualisierungen anzuzeigen.
Folgen Sie den Links in der Tabelle, um Informationen zu den neuen Funktionen und Aktualisierungen zu erhalten.

Release	**Neue Funktionen und Aktualisierungen**
Version 8.1.2	Server • Daten in Microsoft Azure, einem cloudbasierten Objektspeichersystem, sichern • Clientdaten in einem Verzeichniscontainerspeicherpool verschlüsseln • NAS-Dateiserver in einem Verzeichniscontainerspeicherpool sichern • IBM Spectrum Protect unter dem Betriebssystem Linux on Power Systems (Little Endian) installieren • Speicherumgebung mit einem verbesserten Sicherheitsprotokoll schützen • Sicherheit mit dem automatisch generierten Masterverschlüsselungsschlüssel optimieren • Upgrade für den IBM Spectrum Protect-Server auf Version 8.1.2 vor dem Upgrade für Clients durchführen • Speicherumgebung mithilfe der Bandspeicherlösung konfigurieren • Automatische Aktualisierungen für Clients für Sichern/Archivieren planen • Veraltete und nicht mehr verwendete Serveroptionen, Befehle und Parameter Operations Center Aktualisierungen für das Operations Center
Version 8.1.1	Server • IBM Spectrum Protect unter dem Betriebssystem Linux on Power Systems (Little Endian) installieren • IBM Spectrum Protect unter dem Betriebssystem Microsoft Windows Server 2016 installieren • Speicherarchiv Quantum Scalar i6 verwenden • Gelöste Probleme überprüfen Operations Center • Gelöste Probleme überprüfen
Version 8.1	Server • Lernen Sie IBM Spectrum Protect kennen • Sichere Kommunikation durch die Verwendung des Protokolls TLS 1.2 • Bandspeicherpool in einen Containerspeicherpool konvertieren • Software-Upgrade für den Datenbankmanager des Servers • Mit dem Befehl REGISTER NODE wird eine Benutzer-ID mit Administratorberechtigung nicht mehr standardmäßig erstellt • Benutzerauthentifizierung mit einer Active Directory-Datenbank optimieren • Größere Flexibilität für den Schutz und die Konsolidierung von Banddatenträgern in Containerkopienspeicherpools • Unterstützte Betriebssysteme • System ohne Verwendung von SNMP überwachen Operations Center Aktualisierungen für das Operations Center

- Aktualisierungen für das Operations Center
  Neue Funktionen sind im IBM Spectrum Protect Operations Center Version 8.1.2 verfügbar. Mit dem aktualisierten Operations Center können Sie Daten im Microsoft Azure-Cloudspeicher sichern und von der erweiterten Sicherheitsdurchsetzung profitieren.
- Aktualisierungen für den IBM Spectrum Protect-Server
  Neue Funktionen und andere Änderungen sind im IBM Spectrum Protect-Server der Version 8.1.2 verfügbar.
- Releaseinformationen für Serverkomponenten der Version 8.1
  Releaseinformationen sind für V8.1-Komponenten verfügbar.
- Readme-Dateien für Serverkomponenten der Version 8.1
  Readme-Dateien für Fixpacks für Version 8.1 werden auf der IBM Software Support-Website veröffentlicht. Aktualisierungen können für Serverkomponenten, einschließlich für den Server selbst, für die Einheitenunterstützung und für das Operations Center verfügbar sein.

Zugehörige Informationen:
Videos zu Neuerungen in Version 7

Aktualisierungen für das Operations Center

Neue Funktionen sind im IBM Spectrum Protect Operations Center Version 8.1.2 verfügbar. Mit dem aktualisierten Operations Center können Sie Daten im Microsoft Azure-Cloudspeicher sichern und von der erweiterten Sicherheitsdurchsetzung profitieren.

Die folgenden funktionalen Erweiterungen wurden am Operations Center vorgenommen:

- Sie können den Assistenten 'Speicherpool hinzufügen' verwenden, um Cloud-Containerspeicherpools zu erstellen, die Microsoft Azure, ein cloudbasiertes Objektspeichersystem, zum Sichern von Daten verwenden.
- Das Operations Center stellt jetzt eine erweiterte Sicherheit bereit, indem die Verwendung der TLS 1.2-Verschlüsselung (Transport Layer Security 1.2) für die Kommunikation zwischen dem Operations Center und dem Hub-Server durchgesetzt wird.

Weitere Informationen zu diesen funktionalen Erweiterungen finden Sie in der Hilfe des Operations Center.

Aktualisierungen für den IBM Spectrum Protect-Server

Neue Funktionen und andere Änderungen sind im IBM Spectrum Protect-Server der Version 8.1.2 verfügbar.

- Daten in Microsoft Azure, einem cloudbasierten Objektspeichersystem, sichern
  Mit IBM Spectrum Protect Version 8.1.2 können Sie Cloud-Containerspeicherpools für die Verwendung von Microsoft Azure, einem cloudbasierten Objektspeichersystem, zum Sichern und Zurückschreiben von Daten konfigurieren.
- Clientdaten in einem Verzeichniscontainerspeicherpool verschlüsseln
  IBM Spectrum Protect Version 8.1.2 stellt erweiterten Schutz für Clientdaten bereit. Wenn ein früheres Release von IBM Spectrum Protect verwendet wurde, um Daten in einen Verzeichniscontainerspeicherpool zu schreiben, können Sie die vorhandenen Clientdaten in dem Speicherpool verschlüsseln. Sie können auch die Verschlüsselung neuer Clientdaten aktivieren, bevor sie in den Speicherpool geschrieben werden.
- NAS-Dateiserver in einem Verzeichniscontainerspeicherpool sichern
  Mit IBM Spectrum Protect Version 8.1.2 können Sie ein Dateisystem, das zu einem NAS-Dateiserver gehört, in einem Verzeichniscontainerspeicherpool sichern. Mithilfe von Verzeichniscontainerspeicherpools können Sie die Kosten für Speicherhardware reduzieren, die Serverleistung verbessern und die Sicherheit erweitern.
- IBM Spectrum Protect unter dem Betriebssystem Linux on Power Systems (Little Endian) installieren
  Sie können IBM Spectrum Protect Version 8.1.2 unter dem Betriebssystem Linux on Power Systems (Little Endian) installieren. In Version 8.1.1 wurde eine eingeschränkte Unterstützung für dieses Betriebssystem eingeführt und in Version 8.1.2 wird die vollständige Unterstützung bereitgestellt. Nachdem der Server der Version 8.1.2 unter Linux on Power Systems (Little Endian) installiert und konfiguriert wurde, können Sie Daten auf Platteneinheiten, im Cloudobjektspeicher und auf Bandeinheiten sichern.
- Speicherumgebung mit einem verbesserten Sicherheitsprotokoll schützen
  In IBM Spectrum Protect Version 8.1.2 wird ein verbessertes Sicherheitsprotokoll zur Verfügung gestellt.
- Sicherheit mit dem automatisch generierten Masterverschlüsselungsschlüssel optimieren
  Ab IBM Spectrum Protect Version 8.1.2 wird beim Start des Servers automatisch ein Masterverschlüsselungsschlüssel generiert, wenn der Masterverschlüsselungsschlüssel zuvor nicht vorhanden war.
- Speicherumgebung mithilfe der Bandspeicherlösung konfigurieren
  Die Dokumentation wurde aktualisiert, um die *IBM Spectrum Protect Bandspeicherlösung* einzuschließen. Mithilfe der Anweisungen in dem Handbuch können Sie eine bandbasierte Lösung konfigurieren, die die Speicherung optimiert und die Wiederherstellung nach einem Katastrophenfall unterstützt, indem sichergestellt wird, dass Daten an einem ausgelagerten Standort sicher gespeichert werden.
- Automatische Aktualisierungen für Clients für Sichern/Archivieren planen
  Mit IBM Spectrum Protect Version 8.1.2 können Sie die Implementierung von Software-Updates auf Systemen planen, auf denen der Client für Sichern/Archivieren bereits installiert ist.
- Upgrade für den IBM Spectrum Protect-Server auf Version 8.1.2 vor dem Upgrade für Clients durchführen
  Upgrade für den IBM Spectrum Protect-Server auf Version 8.1.2 vor dem Upgrade für Clients für Sichern/Archivieren durchführen.
- Veraltete und nicht mehr verwendete Serveroptionen, Befehle und Parameter
  Einige Serveroptionen, Befehle und Parameter sind veraltet oder ab IBM Spectrum Protect Version 8.1.2 nicht mehr verfügbar. Das Verhalten einiger Parameter und Optionen hat sich geändert.

Daten in Microsoft Azure, einem cloudbasierten Objektspeichersystem, sichern

Mit IBM Spectrum Protect Version 8.1.2 können Sie Cloud-Containerspeicherpools für die Verwendung von Microsoft Azure, einem cloudbasierten Objektspeichersystem, zum Sichern und Zurückschreiben von Daten konfigurieren.

Wenn Sie Cloud-Containerspeicherpools für die Verwendung von Azure konfigurieren, können Sie die Speicherverwaltung vereinfachen und Daten mithilfe der Verschlüsselung schützen.

Zugehörige Tasks:
Vorbereitungen für Azure treffen
Cloud-Containerspeicherpool konfigurieren
Zugehörige Verweise:
DEFINE STGPOOL (Cloud-Containerspeicherpool definieren)
UPDATE STGPOOL (Cloud-Containerspeicherpool aktualisieren)

Clientdaten in einem Verzeichniscontainerspeicherpool verschlüsseln

IBM Spectrum Protect Version 8.1.2 stellt erweiterten Schutz für Clientdaten bereit. Wenn ein früheres Release von IBM Spectrum Protect verwendet wurde, um Daten in einen Verzeichniscontainerspeicherpool zu schreiben, können Sie die vorhandenen Clientdaten in dem

Speicherpool verschlüsseln. Sie können auch die Verschlüsselung neuer Clientdaten aktivieren, bevor sie in den Speicherpool geschrieben werden.

Um die Verschlüsselung für einen vorhandenen Verzeichniscontainerspeicherpool zu aktivieren, geben Sie den Befehl UPDATE STGPOOL unter Angabe von ENCRYPT=YES aus. Um die Verschlüsselung für einen neuen Verzeichniscontainerspeicherpool zu aktivieren, definieren Sie den Speicherpool mithilfe des Befehls DEFINE STGPOOL unter Angabe von ENCRYPT=YES.

Zugehörige Tasks:
Verzeichniscontainerspeicherpool für die Datenspeicherung konfigurieren
Zugehörige Verweise:
DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren)
UPDATE STGPOOL (Verzeichniscontainerspeicherpool aktualisieren)

NAS-Dateiserver in einem Verzeichniscontainerspeicherpool sichern

Mit IBM Spectrum Protect Version 8.1.2 können Sie ein Dateisystem, das zu einem NAS-Dateiserver gehört, in einem Verzeichniscontainerspeicherpool sichern. Mithilfe von Verzeichniscontainerspeicherpools können Sie die Kosten für Speicherhardware reduzieren, die Serverleistung verbessern und die Sicherheit erweitern.

Verzeichniscontainerspeicherpools bieten die folgenden Vorteile:

- Sie können die Inline-Datendeduplizierung aktivieren, um doppelte Daten zu eliminieren, während die Daten in den Speicherpool geschrieben werden. Auf diese Weise können Sie die Notwendigkeit der Offlinereorganisation reduzieren, die Serverleistung verbessern und Kosten senken.
- Sie können die Inline-Komprimierung aktivieren, um den Umfang des Speicherbereichs zu reduzieren, der von Daten belegt wird.
- Sie können die Verschlüsselung aktivieren, um Clientdaten zu verschlüsseln, bevor sie in den Speicherpool geschrieben werden.
- Sie können Daten mithilfe des Befehls PROTECT STGPOOL schützen. Sie können eine Kopie der Daten in einem anderen Verzeichniscontainerspeicherpool auf einem Zielreplikationsserver oder auf Band in einem Containerkopienspeicherpool speichern. Um beschädigte Daten zurückzuschreiben, können Sie den Befehl REPAIR STGPOOL ausführen.

Zugehörige Tasks:
NAS-Dateiserver schützen
Zugehörige Verweise:
DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren)
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)
Betriebssysteme Linux

IBM Spectrum Protect unter dem Betriebssystem Linux on Power Systems (Little Endian) installieren

Sie können IBM Spectrum Protect Version 8.1.2 unter dem Betriebssystem Linux on Power Systems (Little Endian) installieren. In Version 8.1.1 wurde eine eingeschränkte Unterstützung für dieses Betriebssystem eingeführt und in Version 8.1.2 wird die vollständige Unterstützung bereitgestellt. Nachdem der Server der Version 8.1.2 unter Linux on Power Systems (Little Endian) installiert und konfiguriert wurde, können Sie Daten auf Platteneinheiten, im Cloudobjektspeicher und auf Bandeinheiten sichern.

Die Installationspakete umfassen den Server und die Lizenz, Einheitentreibertools, das Operations Center und den Speicheragenten. Es gelten die folgenden Einschränkungen:

- Es kann keine Clusterumgebung konfiguriert werden.
- Der Befehl QUERY SAN oder die Serveroption SANDISCOVERY kann nicht verwendet werden, um Einheiten in einem Speicherbereichsnetz zu erkennen, wenn die Einheiten mit einer Hostbusadapterkarte (HBA-Karte) verbunden sind, die unter Verwendung der NPIV-Methode (NPIV = N_Port ID Virtualization) konfiguriert wird.
- Sie können die Datenübertragung zu fernen Servern nicht optimieren, indem Sie die Aspera FASP-Technologie (FASP = Fast Adaptive Secure Protocol) aktivieren.
- Es können keine ACSLS-Speicherarchive konfiguriert werden.

Zugehörige Tasks:
Linux: Server installieren
Zugehörige Verweise:
Linux: Servermindestvoraussetzungen für Linux on Power Systems™ (Little Endian)

Speicherumgebung mit einem verbesserten Sicherheitsprotokoll schützen

In IBM Spectrum Protect Version 8.1.2 wird ein verbessertes Sicherheitsprotokoll zur Verfügung gestellt.

Um Ihre Speicherumgebung vor Sicherheitsbedrohungen zu schützen, verfügt IBM Spectrum Protect über ein verbessertes Sicherheitsprotokoll, das Transport Layer Security (TLS) 1.2 zum Verschlüsseln der gesamten Kommunikation zwischen dem Server, dem Speicheragenten und Clients verwendet. Ein neuer Parameter SESSIONSECURITY bestimmt, ob ein Administrator, ein Knoten oder ein Server die sichersten Einstellungen

verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. IBM Spectrum Protect-Server, -Clients und -Speicheragenten, die Software der Version 8.1.2 oder höher verwenden, werden automatisch für die Kommunikation miteinander unter Verwendung des Protokolls Secure Sockets Layer (SSL) konfiguriert. Zertifikate werden automatisch verteilt.

Eine ausführliche Beschreibung des Parameters SESSIONSECURITY finden Sie in den Befehlsabschnitten zum Registrieren und Aktualisieren von Administrator-IDs, Knoten und Servern. Die neuesten Informationen zu Sicherheitsupdates für Version 8.1.2, finden Sie in Technote 2004844.

Zugehörige Verweise:
DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
REGISTER ADMIN (Administrator-ID registrieren)
REGISTER NODE (Knoten registrieren)
UPDATE ADMIN (Administrator aktualisieren)
UPDATE NODE (Attribute eines Knotens aktualisieren)
UPDATE SERVER (Server aktualisieren, der für Übertragung zwischen Servern definiert ist)
Zugehörige Informationen:
Was Sie vor dem Upgrade des Servers über die Sicherheit wissen sollten (AIX)
Was Sie vor dem Upgrade des Servers über die Sicherheit wissen sollten (Linux)
Was Sie vor dem Upgrade des Servers über die Sicherheit wissen sollten (Windows)
Sicherheitskonzepte

Sicherheit mit dem automatisch generierten Masterverschlüsselungsschlüssel optimieren

Ab IBM Spectrum Protect Version 8.1.2 wird beim Start des Servers automatisch ein Masterverschlüsselungsschlüssel generiert, wenn der Masterverschlüsselungsschlüssel zuvor nicht vorhanden war.

Der neu generierte Masterverschlüsselungsschlüssel wird in einer neuen Schlüsseldatenbank, dsmkeydb.kdb, gespeichert. Wenn für den Server ein Masterverschlüsselungsschlüssel vorhanden ist, wird der Schlüssel aus der Datei dsmserv.pwd in die neue Schlüsseldatenbank migriert. Mit der automatischen Generierung des Masterverschlüsselungsschlüssels und der Speicherung in der neuen Schlüsseldatenbank soll die Systemsicherheit verbessert werden. Serverzertifikate werden weiterhin in der Schlüsseldatenbank cert.kdb gespeichert. Der Zugriff erfolgt durch die Stashdatei cert.sth.

Sie müssen sowohl die Schlüsseldatenbanken (cert.kdb und dsmkeydb.kdb) als auch die Stashdateien (cert.sth und dsmkeydb.sth), die den Zugriff auf die jeweilige Schlüsseldatenbank bereitstellen, schützen. Standardmäßig schützt der Befehl BACKUP DB den Masterverschlüsselungsschlüssel, aber Sie müssen sich das Kennwort der Datenbanksicherung merken, um die Datenbank zurückzuschreiben. Die IBM Spectrum Protect-Serverdatei dsmserv.pwd, die in früheren Releases zum Speichern des Masterverschlüsselungsschlüssels verwendet wurde, wird nicht mehr verwendet.

Zugehörige Verweise:
BACKUP DB (Datenbank sichern)
Zugehörige Informationen:
Daten mithilfe von DRM wiederherstellen

Speicherumgebung mithilfe der Bandspeicherlösung konfigurieren

Die Dokumentation wurde aktualisiert, um die *IBM Spectrum Protect Bandspeicherlösung* einzuschließen. Mithilfe der Anweisungen in dem Handbuch können Sie eine bandbasierte Lösung konfigurieren, die die Speicherung optimiert und die Wiederherstellung nach einem Katastrophenfall unterstützt, indem sichergestellt wird, dass Daten an einem ausgelagerten Standort sicher gespeichert werden.

Das Handbuch stellt Anweisungen zur Ausführung der folgenden Tasks bereit:

- Datenschutzlösung planen und implementieren, die eine oder mehrere Bandspeichereinheiten zum Sichern von Daten verwendet
- IBM Spectrum Protect-Bandspeicherlösung überwachen
- Bandeinheiten und Bandlaufwerke verwalten
- Daten nach einem Katastrophenfall oder einer ungeplanten Betriebsunterbrechung wiederherstellen

Zugehörige Informationen:
Bandspeicherlösung (PDF)
Bandspeicherlösung
Bandspeicherlösung planen, implementieren, überwachen und verwalten

Automatische Aktualisierungen für Clients für Sichern/Archivieren planen

Mit IBM Spectrum Protect Version 8.1.2 können Sie die Implementierung von Software-Updates auf Systemen planen, auf denen der Client für Sichern/Archivieren bereits installiert ist.

Sie können IBM Spectrum Protect-Serverbefehle verwenden, um Aktualisierungen für einen oder mehrere Clients für Sichern/Archivieren zu planen. Die Aktualisierungen können Fixpacks oder neue Releases sein. Diese Funktion war bereits in früheren Releases von IBM Spectrum

Protect verfügbar, aber für Version 8.1.2 steht eine verbesserte Prozedur zur Verfügung.

Weitere Informationen zur automatischen Implementierung der Clientaktualisierungen vom Server finden Sie in den folgenden Dokumenten:

- Für IBM Spectrum Protect-Server der Version 8.1.2 oder höher siehe Technote 2004596.
- Für IBM® Tivoli Storage Manager-Server der Version 7.1 und IBM Spectrum Protect-Server der Version 8.1.0 und Version 8.1.1 siehe Technote 1673299.

Upgrade für den IBM Spectrum Protect-Server auf Version 8.1.2 vor dem Upgrade für Clients durchführen

Upgrade für den IBM Spectrum Protect-Server auf Version 8.1.2 vor dem Upgrade für Clients für Sichern/Archivieren durchführen.

Wenn Sie das Upgrade nicht zuerst für Ihre Server durchführen, kann die Kommunikation zwischen Servern und Clients unterbrochen werden.

Zugehörige Informationen:
Was Sie vor dem Upgrade des Servers über die Sicherheit wissen sollten (AIX)
Was Sie vor dem Upgrade des Servers über die Sicherheit wissen sollten (Linux)
Was Sie vor dem Upgrade des Servers über die Sicherheit wissen sollten (Windows)

Veraltete und nicht mehr verwendete Serveroptionen, Befehle und Parameter

Einige Serveroptionen, Befehle und Parameter sind veraltet oder ab IBM Spectrum Protect Version 8.1.2 nicht mehr verfügbar. Das Verhalten einiger Parameter und Optionen hat sich geändert.

Aufgrund von Sicherheitsprotokolländerungen wurden im Produkt die folgenden Aktualisierungen durchgeführt:

- Zwei SSL-bezogene Parameter, VALIDATEPROTOCOL und SSLREQUIRED, sind veraltet und werden ignoriert. Diese Parameter werden durch den Parameter SESSIONSECURITY ersetzt.
- Vier SSL-bezogene Serveroptionen, USETLS12, SSLTLS12, SSLHIDELEGACY und SSLDISABLELEGACYTLS, sind nicht mehr verfügbar.
- Das Verhalten des Parameters SSL in den Befehlen DEFINE SERVER und UPDATE SERVER hat sich geändert. SSL wird jetzt verwendet, um einen Teil der Kommunikation mit dem Server zu verschlüsseln, auch wenn SSL=NO angegeben wird.
- Das Verhalten der Optionen TCPPORT und TCPADMINPORT hat sich geändert. Die in der Option TCPPORT oder TCPADMINPORT angegebene Anschlussnummer ist jetzt sowohl für TCP/IP-Sitzungen als auch für SSL-fähige Sitzungen empfangsbereit und akzeptiert diese Sitzungen. Sie müssen nicht mehr die Option SSLTCPPORT oder SSLTCPADMINPORT angeben, um SSL-fähige Sitzungen vom Client zu ermöglichen.
- Die Befehle SET AUTHENTICATION, SET REGISTRATION, DELETE KEYRING, QUERY SSLKEYRINGPW und SET SSLKEYRINGPW sind nicht mehr verfügbar.

Zugehörige Verweise:
DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
UPDATE SERVER (Server aktualisieren, der für Übertragung zwischen Servern definiert ist)

Releaseinformationen für Serverkomponenten der Version 8.1

Releaseinformationen sind für V8.1-Komponenten verfügbar.

- Releaseinformationen für IBM Spectrum Protect-Server Version 8.1
  Der IBM Spectrum Protect-Server Version 8.1 ist verfügbar. Informationen zur Kompatibilität und Installation sowie andere Informationen zu den ersten Schritten werden bereitgestellt.
- Releaseinformationen für Operations Center Version 8.1
  Das Operations Center ist eine webbasierte Schnittstelle, mit der Sie Ihre IBM Spectrum Protect-Umgebung verwalten können. Die Releaseinformationen bieten Ihnen Zugriff auf die Produktankündigung, bekannte Probleme, Systemvoraussetzungen, Installationsanweisungen und Aktualisierungen.
- Releaseinformationen für IBM Spectrum Protect-Einheitenunterstützung Version 8.1
  Die IBM Spectrum Protect-Einheitenunterstützung für Version 8.1 ist verfügbar. Informationen zur Kompatibilität und Installation sowie andere Informationen zu den ersten Schritten werden bereitgestellt.

Releaseinformationen für IBM Spectrum Protect-Server Version 8.1

Der IBM Spectrum Protect-Server Version 8.1 ist verfügbar. Informationen zur Kompatibilität und Installation sowie andere Informationen zu den ersten Schritten werden bereitgestellt.

Inhalt

- Beschreibung
- Ankündigung

- Kompatibilität mit früheren Versionen
- Systemvoraussetzungen
- IBM Spectrum Protect installieren und Upgrade durchführen
- Aktualisierungen, Einschränkungen und bekannte Probleme

Beschreibung

IBM Spectrum Protect stellt automatisierte, zentral geplante, maßnahmenverwaltete Sicherungs-, Archivierungs- und Speicherverwaltungsfunktionen für Dateiserver, Workstations, virtuelle Maschinen und Anwendungen bereit.

Ein Authorized Program Analysis Report (APAR) ist eine Anforderung für die Korrektur eines Fehlers in einem unterstützten Release eines von IBM gelieferten Programms. Eine Liste der behobenen APARs finden Sie in APARs fixed in IBM Spectrum Protect server Version 8.1.

Ankündigung

Die Ankündigung für die IBM Spectrum Protect-Produktfamilie der Version 8.1 enthält die folgenden Informationen:

- Ausführliche Produktbeschreibung, einschließlich Beschreibungen neuer Funktionen
- Produktpositionierungsanweisung
- Internationale Kompatibilitätsinformationen

Führen Sie die folgenden Schritte aus, um nach der Produktankündigung zu suchen:

1. Rufen Sie die Produktankündigungswebsite auf.
2. Geben Sie in das Feld Search for die Produkt-ID (PID) für Ihr Produkt ein. Die PID für IBM Spectrum Protect lautet 5725-W98.
3. Wählen Sie im Feld Information Type den Eintrag Announcement letters aus und klicken Sie auf Search.
4. Wählen Sie aus der Liste Search in den Eintrag Product Number aus.
5. Optional: Wählen Sie im Teilfenster 'Refine Your Search' auf der linken Seite des Fensters das Land aus, in dem Sie sich befinden.
6. Wählen Sie im Abschnitt Sort by den Eintrag Newest first aus.

Kompatibilität mit früheren Versionen

Informationen zur Kompatibilität mit früheren Versionen befinden sich unter IBM Spectrum Protect Server-Client Compatibility and Upgrade Considerations.

Systemvoraussetzungen

Informationen zu den Systemvoraussetzungen finden Sie unter IBM Spectrum Protect Supported Operating Systems.

IBM Spectrum Protect installieren und Upgrade durchführen

Anweisungen für die Serverinstallation finden Sie in der Prozedur für Ihr Betriebssystem:

IBM AIX
: Server installieren

Linux
: Server installieren

Microsoft Windows
: Server installieren

Upgradeanweisungen finden Sie in Upgrade auf Version 8.1 durchführen.

Aktualisierungen, Einschränkungen und bekannte Probleme

Aktualisierungen beschreiben neue Produktinformationen oder neue Produktfunktionen, die nach der Freigabe des Produkts verfügbar werden. Aktualisierungen, Einschränkungen und bekannte Probleme sind in Form von technischen Hinweisen in der Unterstützungswissensbasis im IBM® Support Portal dokumentiert. Durchsuchen Sie die Wissensbasis, um Fehlerumgehungen oder Lösungen für bekannte Probleme zu finden.

Aktualisierungen
: **Mit dem Befehl REGISTER NODE wird eine Benutzer-ID mit Administratorberechtigung nicht mehr standardmäßig erstellt**
Ab IBM Spectrum Protect Version 8.1 wird mit dem Befehl REGISTER NODE nicht automatisch eine Benutzer-ID mit Administratorberechtigung erstellt, die mit dem Knotennamen übereinstimmt. Diese Produktaktualisierung kann Auswirkungen auf den Prozess zum Registrieren von Clientknoten, einschließlich IBM Spectrum Protect-Knoten des Clients für Sichern/Archivieren, haben. In einigen Fällen müssen Sie möglicherweise eine Benutzer-ID mit Administratorberechtigung erstellen, indem Sie den Parameter USERID im Befehl REGISTER NODE angeben. Informationen zu den betroffenen Clienttypen finden Sie in Technote 7048963.

: Um nach den neuesten Aktualisierungen zu suchen, rufen Sie die Website Updates for IBM Spectrum Protect V8.1 auf.

Einschränkungen und bekannte Probleme
: Zum Zeitpunkt der Veröffentlichung waren keine Einschränkungen oder Probleme bekannt.

Die aktuellen Einschränkungen und bekannten Probleme, die weitere Einträge umfassen können, finden Sie in Limitations and known problems for IBM Spectrum Protect V8.1.

Releaseinformationen für Operations Center Version 8.1

Das Operations Center ist eine webbasierte Schnittstelle, mit der Sie Ihre IBM Spectrum Protect-Umgebung verwalten können. Die Releaseinformationen bieten Ihnen Zugriff auf die Produktankündigung, bekannte Probleme, Systemvoraussetzungen, Installationsanweisungen und Aktualisierungen.

Inhalt

- Beschreibung
- Ankündigung
- Kompatibilität mit dem IBM Spectrum Protect-Server
- Systemvoraussetzungen
- Operations Center installieren oder Upgrade für das Operations Center durchführen
- Aktualisierungen, Einschränkungen und bekannte Probleme

Beschreibung

Mit dem Operations Center können Sie die folgenden Aktionen ausführen:

- Potenzielle Probleme mit Ihrer IBM Spectrum Protect-Umgebung identifizieren
- Schlüsselaspekte der Speicherumgebung überwachen: Alerts, Clients, Server, Maßnahmen, Speicherpools und Speichereinheiten
- Clients registrieren
- Server hinzufügen, die überwacht werden sollen
- Clients, Serverdatenbanken und Speicherpools sichern
- Speicherpoolumlagerung und -konsolidierung starten
- Administratoren Alerts zuordnen und Alerts schließen
- Serverprozesse und Clientsitzungen anzeigen und abbrechen
- Einstellungen für Client, Server, Speicherpool und Speichereinheit ändern
- Clientzeitpläne erstellen und verwalten und Verwaltungszeitpläne anzeigen
- Primäre Speicherpools in Containerspeicherpools konvertieren
- Daten aus Verzeichniscontainerspeicherpools auf Band kopieren
- Replikation konfigurieren
- Maßnahmeneinstellungen ändern
- Clients stilllegen und Daten inaktivieren
- E-Mail-Berichte erstellen
- Front-End- und Back-End-Kapazitätsnutzung anzeigen, um die Lizenzeinhaltung zu überwachen
- Befehle an IBM Spectrum Protect-Server ausgeben

Ein Authorized Program Analysis Report (APAR) ist eine Anforderung für die Korrektur eines Fehlers in einem unterstützten Release eines von IBM gelieferten Programms. Eine Liste der behobenen APARs finden Sie in APARs fixed in IBM Spectrum Protect Operations Center Version 8.1.

Ankündigung

Das Operations Center ist Teil der IBM Spectrum Protect-Produktfamilie Version 8.1. Die Ankündigung für diese Produkte enthält die folgenden Informationen:

- Ausführliche Produktbeschreibung, einschließlich Beschreibungen neuer Funktionen
- Produktpositionierungsanweisung
- Internationale Kompatibilitätsinformationen

Führen Sie die folgenden Schritte aus, um nach der Produktankündigung zu suchen:

1. Rufen Sie die Produktankündigungswebsite auf.
2. Geben Sie in das Feld Search for die Produkt-ID (PID) für Ihr Produkt ein. Die PID für IBM Spectrum Protect lautet 5725-W98.
3. Wählen Sie im Feld Information Type den Eintrag Announcement letters aus und klicken Sie auf Search.
4. Wählen Sie aus der Liste Search in den Eintrag Product Number aus.
5. Optional: Wählen Sie im Teilfenster 'Refine Your Search' auf der linken Seite des Fensters das Land aus, in dem Sie sich befinden.
6. Wählen Sie im Abschnitt Sort by den Eintrag Newest first aus.

Kompatibilität mit dem IBM Spectrum Protect-Server

Kompatibilitätsinformationen befinden sich in IBM Spectrum Protect server and Operations Center compatibility.

Systemvoraussetzungen

Systemvoraussetzungen befinden sich in IBM Spectrum Protect Operations Center software and hardware requirements.

Operations Center installieren oder Upgrade für das Operations Center durchführen

Installationsanweisungen oder Informationen zur Durchführung eines Upgrades für die bisherige Version des Operations Center befinden sich in Operations Center installieren und Upgrade für das Operations Center durchführen.

Aktualisierungen, Einschränkungen und bekannte Probleme

Aktualisierungen beschreiben neue Produktinformationen oder neue Produktfunktionen, die nach der Freigabe des Produkts verfügbar werden. Aktualisierungen, Einschränkungen und bekannte Probleme sind in Form von technischen Hinweisen in der Unterstützungswissensbasis im IBM® Support Portal dokumentiert. Durchsuchen Sie die Wissensbasis, um Fehlerumgehungen oder Lösungen für bekannte Probleme zu finden.

Aktualisierungen

Eine aktuelle Liste der Aktualisierungen befindet sich in Search results for updates to Operations Center V8.1.

Einschränkungen und bekannte Probleme

- Eine Liste der Einschränkungen und bekannten Probleme befindet sich in Limitations and known issues with Operations Center V8.1.
- Um nach weiteren Problemen zu suchen, die nach der Freigabe des Produkts bekannt werden können, rufen Sie die Website Search results for known issues with Operations Center V8.1 auf.

Releaseinformationen für IBM Spectrum Protect-Einheitenunterstützung Version 8.1

Die IBM Spectrum Protect-Einheitenunterstützung für Version 8.1 ist verfügbar. Informationen zur Kompatibilität und Installation sowie andere Informationen zu den ersten Schritten werden bereitgestellt.

Inhalt

Beschreibung

Dieses Dokument enthält Informationen zu Einheitentreibern von IBM Spectrum Protect Version 8.1.

Ein Authorized Program Analysis Report (APAR) ist eine Anforderung für die Korrektur eines Fehlers in einem unterstützten Release eines von IBM gelieferten Programms. Eine Liste der behobenen APARs finden Sie in APARs Fixed in IBM Spectrum Protect device driver Version 8.1.

Ankündigung

Die IBM Spectrum Protect-Einheitenunterstützung für Version 8.1 wird als Teil der Ankündigung der IBM Spectrum Protect-Produktfamilie angekündigt. Die Ankündigung für diese Produkte enthält die folgenden Informationen:

- Ausführliche Produktbeschreibung, einschließlich Beschreibungen neuer Funktionen
- Produktpositionierungsanweisung
- Internationale Kompatibilitätsinformationen

Führen Sie die folgenden Schritte aus, um nach der Produktankündigung zu suchen:

1. Rufen Sie die Produktankündigungswebsite auf.
2. Geben Sie in das Feld Search for die Produkt-ID (PID) für Ihr Produkt ein. Die PID für IBM Spectrum Protect lautet 5725-W98.
3. Wählen Sie im Feld Information Type den Eintrag Announcement letters aus und klicken Sie auf Search.
4. Wählen Sie aus der Liste Search in den Eintrag Product Number aus.
5. Optional: Wählen Sie im Teilfenster 'Refine Your Search' auf der linken Seite des Fensters das Land aus, in dem Sie sich befinden.
6. Wählen Sie im Abschnitt Sort by den Eintrag Newest first aus.

Unterstützte Einheiten

Informationen zu den unterstützten Einheiten und zur unterstützten Hardware für IBM AIX- und Microsoft Windows-Systeme finden Sie unter Supported devices for AIX and Windows.

Informationen zu den unterstützten Einheiten und zur unterstützten Hardware für Linux-Systeme finden Sie unter Supported devices for Linux.

Einheitentreiberanforderungen

Anforderungen für Hostbusadapter
: Um die besten Ergebnisse zu erzielen, sollten Bandlaufwerke und Bandarchive an ihrem eigenen Hostbusadapter mit dem System verbunden werden. Verwenden Sie den Hostbusadapter nicht gemeinsam mit anderen Einheitentypen, wie z. B. DISK oder CD.

Maximale Anzahl Einheiten, die von IBM Spectrum Protect-Einheitentreibern unterstützt werden
: Informationen zur maximalen Anzahl von Einheiten, die von IBM Spectrum Protect-Einheitentreibern auf jedem Betriebssystem unterstützt werden können, befinden sich in Technote 1364225.

Unterstützung für seriell angeschlossene SCSI-Einheiten (Serial Attached SCSI - SAS)
: SAS-Einheiten können auf einigen Betriebssystemen und in einigen Architekturen verwendet werden. Informationen zu Betriebssystemen und Architekturen für SAS-Einheiten befinden sich in Technote 1396706.

IBM Spectrum Protect-Durchgriffstreiber mit einer Benutzer-ID ohne Rootberechtigung auf Linux-Betriebssystemen ausführen
: Informationen darüber, wie ein Benutzer ohne Rootberechtigung Einheiten mit dem IBM Spectrum Protect-Durchgriffstreiber unter Linux verwenden kann, befinden sich in Technote 1321130. Verwenden Sie Option -g oder -a des Einheitendienstprogramms autoconf, um sicherzustellen, dass Benutzer ohne Rootberechtigung Einheiten verwenden können, die mit dem IBM Spectrum Protect-Durchgriffstreiber konfiguriert sind. Verwenden Sie Option -g, um den Einheitendateien des generischen SCSI-Treibers (sg) Lese- und Schreibberechtigungen für Gruppen hinzuzufügen. Verwenden Sie Option -a, um den sg-Einheitendateien Lese- und Schreibberechtigungen für alle Benutzer hinzuzufügen.

Speicherarchivinformationen

- IBM Spectrum Protect Extended Edition ist für ein Speicherarchiv mit mehr als vier Laufwerken oder mehr als 48 Speicherschächten erforderlich.
- Die Elementadressen der Speicherschächte entsprechen möglicherweise nicht direkt den Nummern der Speicherschächte. Dies ist wichtig, da der IBM Spectrum Protect-Server auf die Speicherschächte immer mit Elementadressen und nicht mit den Nummern der Speicherschächte verweist. Elementadressen können der Seite für die Speicherarchivkonfiguration für jedes Speicherarchiv entnommen werden.
- Für ein Speicherarchiv mit mehreren Laufwerken ist eine Laufwerkelementadresse für die Befehle DEFINE und UPDATE DRIVE erforderlich. Meldet das Speicherarchiv jedoch Laufwerkseriennummern zurück, können Sie ELEMENT=AUTODETECT angeben und die Elementadresse ist nicht erforderlich.
- Die Prozedur zum Konfigurieren des Datenträgerwechslers und zum separaten Konfigurieren jedes Laufwerks befindet sich in Speichereinheiten konfigurieren und verwalten.

Aktualisierungen, Einschränkungen und bekannte Probleme

Aktualisierungen
: Einige Einheiten, die von früheren Releases von IBM Spectrum Protect unterstützt wurden, werden vom IBM Spectrum Protect-Server der Version 8.1 nicht mehr unterstützt. Für die aktuelle Liste der unterstützten Einheiten siehe die folgenden Links:

  - Supported devices for AIX and Windows
  - Supported devices for Linux

  Die neuesten Aktualisierungen, Einschränkungen und bekannten Probleme, die weitere Einträge umfassen können, finden Sie in Updates, limitations, and known problems for IBM Spectrum Protect V8.1 device support.

Readme-Dateien für Serverkomponenten der Version 8.1

Readme-Dateien für Fixpacks für Version 8.1 werden auf der IBM Software Support-Website veröffentlicht. Aktualisierungen können für Serverkomponenten, einschließlich für den Server selbst, für die Einheitenunterstützung und für das Operations Center verfügbar sein.

Readme-Dateien für Fixpacks für IBM Spectrum Protect-Server Version 8.1 anzeigen

Installieren und Upgrade durchführen

- IBM Spectrum Protect-Lösung implementieren
  Wenn Sie eine neue IBM Spectrum Protect-Serverumgebung implementieren, ziehen Sie die Implementierung einer Best-Practice-Konfiguration in Betracht.
- Server installieren und Upgrade durchführen
  Der IBM Spectrum Protect-Server stellt Sicherungs-, Archivierungs- und Speicherverwaltungsservices für Clients zur Verfügung. Sie können einzelne oder mehrere Server in Ihrem Unternehmensnetz installieren oder für die Server ein Upgrade durchführen.
- Operations Center installieren und Upgrade für das Operations Center durchführen
  Das Operations Center ist die webbasierte Schnittstelle zum Verwalten Ihrer Speicherumgebung.

IBM Spectrum Protect-Lösung implementieren

Wenn Sie eine neue IBM Spectrum Protect-Serverumgebung implementieren, ziehen Sie die Implementierung einer Best-Practice-Konfiguration in Betracht.

Mithilfe der verfügbaren IBM Spectrum Protect-Lösungsdokumentation können Sie eine Best-Practice-Lösung auf der Basis Ihrer Unternehmensanforderungen auswählen und dann diese Lösung installieren, konfigurieren und überwachen sowie mit dieser Lösung arbeiten.

Ausführliche Informationen finden Sie in IBM Spectrum Protect-Lösung auswählen.

Verfügbarkeit von Funktionen nach Betriebssystem

Die meisten IBM Spectrum Protect-Funktionen sind auf allen Betriebssystemen verfügbar, die für den Server unterstützt werden.

In der folgenden Tabelle gibt ein Haken an, dass eine Funktion verfügbar ist.

Tabelle 1. Verfügbarkeit von IBM Spectrum Protect-Funktionen nach Betriebssystem

Funktion	IBM® AIX	Linux x86_64	Linux on System z	Linux on Power Systems (Little Endian)	Microsoft Windows
Aspera FASP-Technologie (FASP = Fast Adaptive Secure Protocol): Datenübertragung zu einem fernen Server optimieren.		✓			
Cloudspeicher unter Verwendung von Amazon S3-Technologie (Amazon Simple Storage Service).	✓	✓		✓	✓
Cloudspeicher unter Verwendung von IBM Cloud Object Storage-Technologie.	✓	✓		✓	✓
Cloudspeicher unter Verwendung von IBM SoftLayer-Technologie (IBM Bluemix).	✓	✓		✓	✓
Cloudspeicher unter Verwendung von Microsoft Azure-Technologie.	✓	✓		✓	✓
Cloudspeicher unter Verwendung von OpenStack Swift-Technologie.	✓	✓		✓	✓
Datendeduplizierung: Verwenden Sie die *Inline-Datendeduplizierung*, um doppelte Daten zu eliminieren, während die Daten in einen Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool geschrieben werden. Mithilfe der Inline-Datendeduplizierung können Sie die Notwendigkeit der Offlinereorganisation reduzieren, die Serverleistung verbessern und die Kosten für Speicherhardware verringern.	✓	✓	✓	✓	✓
Datendeduplizierung: Verwenden Sie die *nachgeordnete Datendeduplizierung*, um doppelte Daten aus Plattenspeicherpools mit sequenziellem Zugriff zu elimieren. Diese Option kann zu längeren Verarbeitungszeiten führen, da der Server die Daten identifizieren und dann die Daten aus dem Speicherpool entfernen muss.	✓	✓	✓	✓	✓
Disaster Recovery Manager (DRM): Bereiten Sie einen Plan für die Wiederherstellung Ihrer Server- und Clientdaten vor, wenn ein Katastrophenfall eintritt.	✓	✓	✓	✓	✓

Funktion	IBM® AIX	Linux x86_64	Linux on System z	Linux on Power Systems (Little Endian)	Microsoft Windows
Inline-Datenkomprimierung: Komprimieren Sie Daten, wenn sie in einen Cloud-Containerspeicherpool oder Verzeichniscontainerspeicherpool geschrieben werden, um den Umfang des Speicherbereichs zu reduzieren, der von den Daten belegt wird.	✓	✓	✓	✓	✓
LDAP-Authentifizierung (LDAP = Lightweight Directory Access Protocol): Authentifizieren Sie Benutzer bei einer Active Directory-Datenbank auf einem LDAP-Server.	✓	✓	✓	✓	✓
Knotenreplikation: Kopieren Sie inkrementell Daten, die zu Knoten des Clients für Sichern/Archivieren gehören, von einem Server auf einen anderen Server.	✓	✓	✓	✓	✓
Operations Center: Überwachen und verwalten Sie die Speicherumgebung mithilfe des Operations Center, einer webbasierten Benutzerschnittstelle.	✓	✓	✓	✓	✓
Schutz von Verzeichniscontainerspeicherpools: Schützen Sie Daten in Verzeichniscontainerspeicherpools mithilfe des Befehls PROTECT STGPOOL. Sie können eine Kopie der Daten in einem anderen Verzeichniscontainerspeicherpool auf einem Zielreplikationsserver speichern oder eine Kopie auf Band in einem Containerkopienspeicherpool auf demselben Server speichern.	✓	✓	✓	✓	✓
Speicherpoolverschlüsselung: Verschlüsseln Sie Daten in Cloud-Containerspeicherpools.	✓	✓		✓	✓
Speicherpoolverschlüsselung: Verschlüsseln Sie Daten in Verzeichniscontainerspeicherpools.	✓	✓	✓	✓	✓
Bandspeicher: Speichern Sie Daten auf Band. Dadurch wird eine flexible und kosteneffiziente Option für die langfristige Datenaufbewahrung bereitgestellt.	✓	✓	✓	✓	✓
Protokoll Transport Layer Security (TLS) 1.2: Schützen Sie die Kommunikation mithilfe von TLS 1.2.	✓	✓	✓	✓	✓

Server installieren und Upgrade durchführen

Der IBM Spectrum Protect-Server stellt Sicherungs-, Archivierungs- und Speicherverwaltungsservices für Clients zur Verfügung. Sie können einzelne oder mehrere Server in Ihrem Unternehmensnetz installieren oder für die Server ein Upgrade durchführen.

- Server auf AIX-Systemen installieren
- Server auf Linux-Systemen installieren
- Server auf Windows-Systemen installieren
- Upgrade für den Server durchführen

AIX: Server installieren

Zur Installation des Servers gehören Planung, Installation und Erstkonfiguration.

- AIX
- AIX: Installation des Servers planen
  Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.
- AIX: Serverkomponenten installieren
  Für die Installation der Serverkomponenten der Version 8.1.2 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.
- AIX: Die ersten Schritte nach der Installation von IBM Spectrum Protect
  Nach der Installation von Version 8.1.2 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.
- AIX: IBM Spectrum Protect-Server-Fixpack installieren
  IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.
- AIX: Von Version 8.1.2 auf eine vorherige Serverversion zurücksetzen
  Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.
- AIX: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken
  Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.
- AIX: IBM Spectrum Protect deinstallieren
  Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

AIX: Installation des Servers planen

Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.

- AIX: Vorausgesetzte Kenntnisse
  Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.
- AIX: Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten
  Lesen Sie vor der Installation von IBM Spectrum Protect Version 8.1.2 oder höher die Informationen über die erweiterten Sicherheitsfunktionen und die Voraussetzungen für eine Aktualisierung Ihrer Umgebung.
- AIX: Planung für optimale Leistung
  Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.
-  AIX-BetriebssystemeAIX: Systemmindestvoraussetzungen für AIX-Systeme
  Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem AIX-Betriebssystem ohne Datendeduplizierung installieren.
-  AIX-BetriebssystemeAIX: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System
  Sie können andere Produkte, die DB2-Produkte auf demselben System wie der IBM Spectrum Protect-Server der Version 8.1.2 implementieren und verwenden, mit einigen Einschränkungen installieren.
- AIX: IBM Installation Manager
  IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.
- AIX: Arbeitsblätter für Planungsdetails für den Server
  Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.
- AIX: Kapazitätsplanung
  Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.
- AIX: Empfehlungen für die Serverbenennung
  Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.
- AIX: Installationsverzeichnisse
  Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

AIX: Vorausgesetzte Kenntnisse

Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.

Wartungsreleases, Client-Software und Veröffentlichungen für den Server stehen im IBM® Support Portal zur Verfügung.

 AIX-BetriebssystemeEinschränkung: Sie können den Server der Version 8.1.2 mit einigen Einschränkungen auf einem System installieren und ausführen, auf dem bereits DB2 installiert ist. Das gilt unabhängig davon, ob DB2 separat oder als Teil einer anderen Anwendung installiert wurde. Ausführliche Informationen finden Sie in dem Abschnitt über die Kompatibilität mit anderen DB2-Produkten.

Erfahrene DB2-Administratoren können erweiterte SQL-Abfragen durchführen und mithilfe von DB2-Tools die Datenbank überwachen. Sie dürfen die DB2-Tools jedoch nicht zur Änderung der von IBM Spectrum Protect vorgegebenen DB2-Konfigurationseinstellungen verwenden oder die DB2-Umgebung für IBM Spectrum Protect auf andere Weise ändern (z. B. mit anderen Produkten). Der Server der Version 8.1.2 wurde mit der Datendefinitionssprache (DDL) und der vom Server implementierten Datenbankkonfiguration erstellt und ausführlich getestet.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

AIX: Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten

Lesen Sie vor der Installation von IBM Spectrum Protect Version 8.1.2 oder höher die Informationen über die erweiterten Sicherheitsfunktionen und die Voraussetzungen für eine Aktualisierung Ihrer Umgebung.

Informationen zu diesem Vorgang

Die in Version 8.1.2 und höheren Versionen eingeführten Sicherheitserweiterungen setzen strengere Sicherheitseinstellungen durch. Führen Sie die Prozedur aus, um sicherzustellen, dass die Kommunikation zwischen Servern und Clients bei einer Installation oder einem Upgrade der IBM Spectrum Protect-Software auf Version 8.1.2 nicht unterbrochen wird.

Vorgehensweise

1. Führen Sie die Installation bzw. das Upgrade der IBM Spectrum Protect-Server mit Version 8.1.2 oder höher durch.
2. Führen Sie die Installation bzw. das Upgrade der Clients für Sichern/Archivieren durch. Weitere Informationen finden Sie in Clients installieren und konfigurieren.
   Informationen zur Planung der Implementierung von Clientaktualisierungen auf dem Server finden Sie in den folgenden Dokumenten:
   - Für Server mit IBM Spectrum Protect Version 8.1.2 oder einer höheren Version: Technote 2004596.
   - Für Server mit IBM® Tivoli Storage Manager Version 7.1 und IBM Spectrum Protect Version 8.1.0 und 8.1.1: Technote 1673299.
3. Konfigurieren Sie die Optionen für Clients für Sichern/Archivieren. Weitere Informationen finden Sie in Upgrade des IBM Spectrum Protect-Servers und des IBM Spectrum Protect-Clients durchführen.

AIX: Planung für optimale Leistung

Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.

Vorgehensweise

1. Lesen Sie den Abschnitt AIX: Vorausgesetzte Kenntnisse.
2. Lesen Sie jeden der folgenden Unterabschnitte.

- AIX: Planung für die Server-Hardware und das Betriebssystem
  Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- AIX: Planung für Platten für die Serverdatenbank
  Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- AIX: Planung für Platten für das Serverwiederherstellungsprotokoll
  Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- AIX: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools
  Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.
- AIX: Planung für Speicherpools auf DISK- oder FILE-Einheiten
  Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.
- AIX: Planung für die Auswahl des korrekten Speichertechnologietyps
  Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.

- AIX: Bewährte Verfahren bei der Serverinstallation anwenden
  Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

AIX: Planung für die Server-Hardware und das Betriebssystem

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Werden die Betriebssystem- und Hardwarevoraussetzungen erfüllt oder mehr als erfüllt? • Anzahl und Geschwindigkeit der Prozessoren • Systemspeicher • Unterstützte Betriebssystemversion	Wenn Sie die erforderliche Mindestspeicherkapazität verwenden, können Sie eine minimale Arbeitslast unterstützen. Sie können versuchsweise mehr Systemspeicher hinzufügen, um bestimmen zu können, ob sich die Leistung verbessert. Entscheiden Sie dann, ob der Systemspeicher dem Server zugeordnet bleiben soll. Testen Sie die verschiedenen Speicherkapazitäten jeweils anhand des gesamten Tageszyklus der Serverlast. Wenn Sie mehrere Server auf dem System ausführen, addieren Sie die Voraussetzungen für jeden Server, um die Voraussetzungen für das System zu bestimmen. AIX-Betriebssysteme Einschränkung: Active Memory Expansion (AME) darf nicht verwendet werden. Bei Verwendung von AME verwendet die IBM DB2-Software 4-KB-Seiten anstelle von 64-KB-Seiten. Jede 4-KB-Seite muss dekomprimiert werden, wenn auf sie zugegriffen wird; wird sie nicht benötigt, muss sie komprimiert werden. Bei der Komprimierung und Dekomprimierung warten DB2 und der Server auf den Zugriff auf die Seite, wodurch sich die Serverleistung verschlechtert.	Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309. Lesen Sie außerdem die Anweisungen in Tasks für Betriebssysteme und andere Anwendungen optimieren. Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation Weitere Informationen zu Anforderungen in Bezug auf die Größe des Servers und des Speichers finden Sie im IBM Spectrum Protect-Blueprint.
Sind Platten für die optimale Leistung konfiguriert?	Der Umfang der Optimierung, der für verschiedene Plattensysteme erfolgen kann, variiert. Stellen Sie sicher, dass die Warteschlangenlänge und andere Plattensystemoptionen entsprechend definiert sind.	Weitere Informationen finden Sie in: • "Planung für Platten für die Serverdatenbank" • "Planung für Platten für das Serverwiederherstellungsprotokoll" • "Planung für Speicherpools auf DISK- oder FILE-Einheiten"

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verfügt der Server über genügend Speicher?	Höhere Arbeitslasten und erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation erfordern mehr Systemspeicher als den Mindestspeicher, der im Dokument mit den Systemvoraussetzungen angegeben ist. Verwenden Sie die folgenden Richtlinien, um den Speicherbedarf für Datenbanken anzugeben, die nicht für die Datendeduplizierung aktiviert sind: • Für Datenbanken mit einer Größe unter 500 GB benötigen Sie 16 GB Speicher. • Für Datenbanken mit einer Größe von 500 GB bis 1 TB benötigen Sie 24 GB Speicher. • Für Datenbanken mit einer Größe von 1 TB bis 1,5 TB benötigen Sie 32 GB Speicher. • Für Datenbanken mit einer Größe über 1,5 TB benötigen Sie 40 GB Speicher. Stellen Sie sicher, dass Sie für die Replikationsverarbeitung zusätzlichen Speicherbereich für die aktive Protokolldatei und das Archivprotokoll zuordnen.	Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation • Speicherbedarf
Verfügt das System über genügend Hostbusadapter (HBAs), um die Datenoperationen, die der IBM Spectrum Protect-Server gleichzeitig ausführen muss, handhaben zu können?	Sie müssen wissen, für welche Operationen die gleichzeitige Verwendung von Hostbusadaptern erforderlich ist. Ein Server muss beispielsweise Sicherungsdaten mit 1 GB/s speichern, während er gleichzeitig eine Speicherpoolumlagerung ausführt, für deren Ausführung eine Kapazität von 0,5 GB/s erforderlich ist. Die Hostbusadapter müssen alle Daten mit der erforderlichen Geschwindigkeit handhaben können.	Siehe HBA-Kapazität optimieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Ist die Netzbandbreite größer als der geplante maximale Durchsatz für Sicherungen?	Die Netzbandbreite muss dem System die Ausführung von Operationen wie Sicherungen innerhalb der zulässigen Zeit oder gemäß den vereinbarten Service-Levels ermöglichen. Bei der Knotenreplikation muss die Netzbandbreite größer als der geplante maximale Durchsatz sein.	Weitere Informationen finden Sie in: • Netzleistung optimieren • Prüfliste für Knotenreplikation
Verwenden Sie ein bevorzugtes Dateisystem für IBM Spectrum Protect-Serverdateien?	Verwenden Sie ein Dateisystem, das optimale Leistung und Datenverfügbarkeit gewährleistet. Der Server verwendet die direkte E/A mit Dateisystemen, die die Funktion unterstützen. Die Verwendung der direkten E/A kann den Durchsatz verbessern und die Prozessornutzung verringern. Die folgende Liste zeigt das jeweils bevorzugte Dateisystem: • AIX-Betriebssysteme Verwenden Sie das JFS2-Dateisystem mit der Option rbrw.	Weitere Informationen finden Sie in Betriebssystem für die Plattenleistung konfigurieren.
Planen Sie, genügend Seitenauslagerungsbereich zu konfigurieren?	Seitenauslagerungsbereich (oder Auslagerungsspeicher) erweitert den Speicher, der für die Verarbeitung verfügbar ist. Wenn der freie Arbeitsspeicher im System knapp wird, werden Programme oder Daten, die nicht im Gebrauch sind, aus dem Speicher in den Seitenauslagerungsbereich versetzt. Mit dieser Aktion wird Speicherbereich für andere Aktivitäten, wie z. B. Datenbankoperationen, freigegeben. AIX-Betriebssysteme Verwenden Sie den größeren der beiden folgenden Werte: mindestens 32 GB Seitenauslagerungsbereich oder 50 % des Arbeitsspeichers.	

AIX: Planung für Platten für die Serverdatenbank

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Befindet sich die Datenbank auf schnellen Platten mit kurzer Latenzzeit?	Verwenden Sie die folgenden Laufwerke nicht für die IBM Spectrum Protect-Datenbank: • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) Verwenden Sie keine internen Platten, die standardmäßig Teil der Hardware der meisten Server ist. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung. Wenn Sie planen, die Datendeduplizierungsfunktionen von IBM Spectrum Protect zu verwenden, legen Sie den Schwerpunkt auf die Plattenleistung (gemessen in E/A-Operationen pro Sekunde).	Weitere Informationen finden Sie in Prüfliste für Datendeduplizierung.
Ist die Datenbank auf anderen Platten oder LUNs gespeichert als die aktive Protokolldatei, das Archivprotokoll und die Speicherpooldatenträger?	Das Trennen der Serverdatenbank von anderen Serverkomponenten trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei. Tipp: Die Datenbank und das Archivprotokoll können ein Array gemeinsam nutzen, wenn Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) verwenden.	
Wissen Sie bei Verwendung von RAID, wie die optimale RAID-Stufe für Ihr System ausgewählt wird? Definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ?	Wenn ein System viele Schreibvorgänge ausführen muss, ist die Leistung bei RAID 10 besser als bei RAID 5. RAID 10 benötigt jedoch mehr Platten als RAID 5, um dieselbe nutzbare Speichermenge bereitzustellen. Handelt es sich bei Ihrem Plattensystem um ein RAID-System, definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ. Verwenden Sie beispielsweise nicht gleichzeitig 4+1 RAID 5 mit 4+2 RAID 6.	
Planen Sie, wenn eine Option zum Definieren der Stripgröße oder der Segmentgröße verfügbar ist, die Größe beim Konfigurieren des Plattensystems zu optimieren?	Wenn Sie die Stripgröße oder Segmentgröße definieren können, verwenden Sie auf Plattensystemen für die Datenbank Größen von 64 KB oder 128 KB.	Die Blockgröße, die für die Datenbank verwendet wird, variiert abhängig vom Tabellenbereich. Die meisten Tabellenbereiche verwenden 8-KB-Blöcke; einige verwenden jedoch 32-KB-Blöcke.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Planen Sie, mindestens vier Verzeichnisse, die auch als Speicherpfade bezeichnet werden, auf vier verschiedenen LUNs für die Datenbank zu erstellen? Erstellen Sie exakt ein Verzeichnis pro Array in dem Subsystem. Wenn weniger als drei Arrays vorhanden sind, erstellen Sie in jedem Array einen anderen LUN-Datenträger.	Für größere Arbeitslasten und bei Verwendung einiger Funktionen sind mehr Datenbankspeicherpfade als die Mindestvoraussetzungen erforderlich. Serveroperationen wie die Datendeduplizierung verursachen eine hohe Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS) für die Datenbank. Die Leistung derartiger Operationen ist besser, wenn die Datenbank über mehr Verzeichnisse verfügt. Verwenden Sie für Serverdatenbanken, die größer als 2 TB sind oder die wahrscheinlich auf diese Größe anwachsen, acht Verzeichnisse. Berücksichtigen Sie das geplante Wachstum des Systems bei der Bestimmung der Anzahl zu erstellender Speicherpfade. Die höhere Anzahl Speicherpfade wird vom Server effizienter genutzt, wenn die Speicherpfade bei der Ersterstellung des Servers bereits vorhanden sind. Verwenden Sie die Variable *DB2_PARALLEL_IO*, um die parallele E/A für Tabellenbereiche mit einem einzelnen Container zu erzwingen oder für Tabellenbereiche, die über Container auf mehr als einer physischen Platte verfügen. Wenn Sie die Variable *DB2_PARALLEL_IO* nicht definieren, entspricht die E/A-Parallelität der Anzahl Container, die von dem Tabellenbereich verwendet werden. Wenn ein Tabellenbereich beispielsweise vier Container umfasst, beträgt der verwendete Grad an E/A-Parallelität 4.	Weitere Informationen finden Sie in: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation Hilfreiche Informationen zur Vorhersage des Wachstums beim Deduplizieren von Daten durch den Server finden Sie in Technote 1596944. Aktuelle Informationen zur Datenbankgröße, zur Datenbankreorganisation und zu Leistungsaspekten für IBM Spectrum Protect-Server finden Sie in Technote 1683633. Informationen zum Definieren der Variable *DB2_PARALLEL_IO* finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.
Haben alle Verzeichnisse für die Datenbank dieselbe Größe?	Verzeichnisse, die alle dieselbe Größe haben, stellen einen konsistenten Grad an Parallelität für Datenbankoperationen sicher. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als andere sind, verringert sich dadurch das Potenzial für den optimierten parallelen Vorablesezugriff. Diese Richtlinie gilt auch, wenn Sie nach der Erstkonfiguration des Servers Speicherpfade hinzufügen müssen.	
Planen Sie, die Warteschlangenlänge der Datenbank-LUNs auf AIX-Systemen zu erhöhen?	Die Standardwarteschlangenlänge ist häufig zu niedrig definiert.	Siehe AIX-Systeme für die Plattenleistung konfigurieren.

AIX: Planung für Platten für das Serverwiederherstellungsprotokoll

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Sind die aktive Protokolldatei und das Archivprotokoll auf anderen Platten oder LUNs gespeichert als die Datenbank und die Speicherpooldatenträger?	Stellen Sie sicher, dass die Platten, auf die die aktive Protokolldatei gestellt wird, auf dem Server oder System nicht für andere Zwecke verwendet werden. Stellen Sie die aktive Protokolldatei nicht auf Platten, die die Serverdatenbank, das Archivprotokoll oder Systemdateien, wie Seitenauslagerungsbereich oder Auslagerungsspeicher, enthalten.	Das Trennen der Serverdatenbank von der aktiven Protokolldatei und dem Archivprotokoll trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.
Befinden sich die Protokolle auf Platten mit nicht flüchtigem Schreibcache?	Nicht flüchtiger Schreibcache ermöglicht es, Daten so schnell wie möglich in die Protokolle zu schreiben. Schnellere Schreiboperationen für die Protokolle können die Leistung für Serveroperationen verbessern.	
Legen Sie für die Protokolle eine Größe fest, die der Arbeitslast entspricht?	Wenn Sie sich über die Arbeitslast im Unklaren sind, verwenden Sie die größtmögliche Größe. Aktive Protokolldatei Die maximale Größe beträgt 512 GB; sie wird über die Serveroption ACTIVELOGSIZE festgelegt. Stellen Sie sicher, dass mindestens 8 GB freier Speicherbereich im Dateisystem für aktive Protokolldateien verfügbar sind, nachdem die aktiven Protokolldateien mit fester Größe erstellt wurden. Archivprotokoll Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Das Archivprotokoll muss mindestens so groß wie die aktive Protokolldatei sein.	• Ausführliche Informationen zur Festlegung der Protokollgröße enthalten die Informationen zum Wiederherstellungsprotokoll in Technote 1421060. • Informationen zur Festlegung der Größe bei Verwendung der Datendeduplizierung finden Sie in Prüfliste für Datendeduplizierung.
Definieren Sie ein Archivübernahmeprotokoll ? Stellen Sie dieses Protokoll auf eine andere Platte als das Archivprotokoll?	Das Archivübernahmeprotokoll dient der Verwendung durch den Server im Notfall, wenn das Archivprotokoll voll ist. Für das Archivübernahmeprotokoll können langsamere Platten verwendet werden.	Geben Sie die Position des Archivübernahmeprotokolls mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY an. Überwachen Sie die Belegung des Verzeichnisses für das Archivübernahmeprotokoll. Wenn das Archivübernahmeprotokoll vom Server verwendet werden muss, ist der Speicherplatz für das Archivprotokoll möglicherweise nicht groß genug.
Verwenden Sie, wenn Sie die aktive Protokolldatei spiegeln, nur einen einzigen Typ von Spiegelung?	Sie können das Protokoll mithilfe einer der folgenden Methoden spiegeln. Verwenden Sie für das Protokoll nur einen einzigen Typ von Spiegelung. • Verwenden Sie die Option MIRRORLOGDIRECTORY, die für den IBM Spectrum Protect-Server verfügbar ist, um eine Position für die Spiegelung anzugeben. • Verwenden Sie die Softwarespiegelung, wie z. B. Logical Volume Manager (LVM) unter AIX. • Verwenden Sie die Spiegelung in der Hardware des Plattensystems.	Stellen Sie, wenn Sie die aktive Protokolldatei spiegeln, sicher, dass die Platten für die aktive Protokolldatei und die Spiegelkopie dieselbe Geschwindigkeit und Zuverlässigkeit haben. Weitere Informationen finden Sie in Wiederherstellungsprotokoll konfigurieren und optimieren.

AIX: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools

Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verwenden Sie, gemessen in Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS), schnellen Plattenspeicher für die IBM Spectrum Protect-Datenbank?	Verwenden Sie eine Hochleistungsplatte für die Datenbank. Verwenden Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) für die Datendeduplizierungsverarbeitung. Stellen Sie sicher, dass die Datenbank über eine Mindestkapazität von 3000 E/A-Operationen pro Sekunde (IOPS) verfügt. Addieren Sie zu diesem Mindestwert pro TB Daten, die täglich (vor der Datendeduplizierung) gesichert werden, 1000 E/A-Operationen pro Sekunde. Beispielsweise würde ein IBM Spectrum Protect-Server, der täglich 3 TB Daten aufnimmt, 6000 E/A-Operationen pro Sekunde (IOPS) für die Datenbankplatten benötigen: `mindestens 3000 IOPS + 3000 (3 TB x 1000 IOPS) = 6000 IOPS`	Empfehlungen zur Plattenauswahl finden Sie in "Planung für Platten für die Serverdatenbank". Weitere Informationen zu IOPS finden Sie in den IBM Spectrum Protect-Blueprints.
Ist genügend Speicherplatz für die Größe Ihrer Datenbank vorhanden?	Verwenden Sie mindestens 40 GB Systemspeicher für IBM Spectrum Protect-Server, die Daten deduplizieren, mit einer Datenbankgröße von 100 GB. Wenn die Speicherkapazität für Sicherungsdaten wächst, ist unter Umständen ein höherer Speicherbedarf erforderlich. Überwachen Sie regelmäßig die Speicherbelegung, um festzustellen, ob mehr Speicherplatz erforderlich ist. Verwenden Sie weiteren Systemspeicher, um das Caching von Datenbankseiten zu verbessern. Die folgenden Richtlinien für die Speichergröße basieren auf dem Volumen an neuen Daten, das jeden Tag gesichert wird: • 128 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 1 und 2 TB liegt • 192 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 2 und 4 TB liegt	Speicherbedarf

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie die Speicherkapazität für die die aktive Protokolldatei und das Archivprotokoll der Datenbank korrekt festgelegt?	Geben Sie in der Konfiguration des Servers eine minimale Größe von 128 GB für die aktive Protokolldatei an, indem Sie die Serveroption ACTIVELOGSIZE auf den Wert 131072 setzen. Als Anfangsgröße für das Archivprotokoll wird eine Größe von 1 TB vorgeschlagen. Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Stellen Sie sicher, dass im Vergleich zur Größe des Archivprotokolls mindestens 10 % zusätzlicher Plattenspeicher für das Dateisystem vorhanden sind. Verwenden Sie für die Datenbankarchivprotokolle ein Verzeichnis mit einer anfänglichen freien Kapazität von mindestens 1 TB. Geben Sie das Verzeichnis mithilfe der Serveroption ARCHLOGDIRECTORY an. Definieren Sie Speicherbereich für das Archivübernahmeprotokoll mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY.	Weitere Informationen zur Kapazitätsermittlung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.
Ist die Komprimierung für die Archivprotokoll- und Datenbanksicherungen aktiviert?	Aktivieren Sie die Serveroption ARCHLOGCOMPRESS, um Speicherbereich einzusparen. Diese Komprimierungsoption unterscheidet sich von der Inline-Komprimierung. Die Inline-Komprimierung ist ab IBM Spectrum Protect Version 7.1.5 und höher standardmäßig aktiviert. Einschränkung: Sie dürfen diese Option nicht verwenden, wenn das Volumen der pro Tag gesicherten Daten 6 TB überschreitet.	Weitere Informationen zur Komprimierung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.
Befinden sich die Datenbank und Protokolle von IBM Spectrum Protect auf separaten Plattendatenträgern (LUNs)? Ist der Datenträger, der für die Datenbank verwendet wird, gemäß den bewährten Verfahren für eine transaktionsorientierte Datenbank konfiguriert?	Die Datenbank darf keine Plattendatenträger mit IBM Spectrum Protect-Datenbankprotokollen oder -Speicherpools oder mit einer anderen Anwendung oder einem anderen Dateisystem gemeinsam nutzen.	Weitere Informationen zur Konfiguration der Serverdatenbank und des Wiederherstellungsprotokolls finden Sie in Konfiguration und Optimierung der Serverdatenbank und des Wiederherstellungsprotokolls.
Verwenden Sie mindestens acht Prozessorkerne (2,2-GHz-Prozessorkerne oder entsprechende Prozessorkerne) für jeden IBM Spectrum Protect-Server, der mit Datendeduplizierung verwendet werden soll?	Wenn die clientseitige Datendeduplizierung verwendet werden soll, müssen Sie sicherstellen, dass für Clientsysteme während einer Sicherungsoperation genügend Ressourcen zur Ausführung der Datendeduplizierungsverarbeitung verfügbar sind. Verwenden Sie pro Sicherungsprozess mit clientseitiger Datendeduplizierung einen Prozessor, der mindestens einem 2,2-GHz-Prozessorkern entspricht.	• Effektive Planung und Verwendung der Deduplizierung • IBM Spectrum Protect Blueprints

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie genügend Speicherplatz für die Datenbank zugeordnet?	Als grobe Schätzung sollten Sie 100 GB Datenbankspeicher für jeweils 50 TB Daten einplanen, die in deduplizierten Speicherpools geschützt werden sollen. *Geschützte Daten* ist das Datenvolumen vor der Datendeduplizierung, einschließlich aller Versionen gespeicherter Objekte. Als bewährtes Verfahren sollten Sie einen neuen Containerspeicherpool ausschließlich für die Datendeduplizierung definieren. Die Datendeduplizierung erfolgt auf der Speicherpoolebene; mit Ausnahme von verschlüsselten Daten werden alle Daten in einem Speicherpool dedupliziert.	
Haben Sie die Speicherpoolkapazität geschätzt, um genügend Speicherplatz für die Größe Ihrer Umgebung zu konfigurieren?	Sie können den Kapazitätsbedarf für einen deduplizierten Speicherpool wie folgt schätzen: 1. Schätzen Sie die Basisgröße der Quellendaten. 2. Schätzen Sie die Größe der täglichen Sicherung anhand einer geschätzten Änderungs- und Wachstumsrate. 3. Bestimmen Sie die Anforderungen in Bezug auf die Aufbewahrungsdauer. 4. Schätzen Sie das Gesamtvolumen an Quellendaten unter Berücksichtigung der Basisgröße, der Größe der täglichen Sicherung und der Anforderungen in Bezug auf die Aufbewahrungsdauer. 5. Wenden Sie den Faktor für das Deduplizierungsverhältnis an. 6. Wenden Sie den Faktor für das Komprimierungsverhältnis an. 7. Runden Sie die Schätzung auf, um die Nutzung transienter Speicherpools zu berücksichtigen.	Ein Beispiel zur Verwendung dieses Verfahrens finden Sie in Effektive Planung und Verwendung der Deduplizierung.
Haben Sie die Platten-E/A auf viele Platteneinheiten und Controller verteilt?	Verwenden Sie Arrays, die aus so vielen Platten wie möglich bestehen; dies wird auch als "Wide-Striping" bezeichnet. Stellen Sie sicher, dass Sie exakt ein Datenbankverzeichnis pro Array in dem Subsystem verwenden. Definieren Sie die Registry-Variable *DB2_PARALLEL_IO*, um die parallele E/A für jeden verwendeten Tabellenbereich zu aktivieren, wenn sich die Container in dem Tabellenbereich über mehrere physische Platten erstrecken. Wenn E/A-Bandbreite verfügbar ist und die Dateien groß sind (beispielsweise 1 MB), kann der Prozess zur Suche nach Duplikaten die Ressourcen eines gesamten Prozessors in Anspruch nehmen. Wenn Dateien kleiner sind, können andere Engpässe auftreten. Geben Sie acht oder mehr Dateisysteme für die Einheitenklasse des deduplizierten Speicherpools an, damit die Ein-/Ausgabe auf so viele LUNs und physische Einheiten wie möglich verteilt wird.	Richtlinien zur Konfiguration von Speicherpools finden Sie in "Planung für Speicherpools auf DISK- oder FILE-Einheiten". Informationen zum Definieren der Variable *DB2_PARALLEL_IO* finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie tägliche Operationen auf der Basis Ihrer Sicherungsstrategie geplant?	Die Operationsfolge sieht gemäß den bewährten Verfahren wie folgt aus: 1. Clientsicherung 2. Speicherpoolschutz 3. Knotenreplikation 4. Datenbanksicherung 5. Bestandsverfall	• Datendeduplizierungs- und Knotenreplikationsprozesse planen • Tägliche Operation für Verzeichniscontainerspeicherpools
Ist genügend Speicher zur Verwaltung der DB2-Sperrenliste vorhanden?	Wenn Sie Daten deduplizieren, die große Dateien oder gleichzeitig eine große Anzahl Dateien umfassen, kann der Prozess zur Speicherknappheit führen. Wenn der Sperrenlistenspeicher nicht ausreichend ist, können Sicherungsfehler, Datenverwaltungsprozessfehler oder Serverausfälle auftreten. Bei Dateigrößen über 500 GB, die durch die Datendeduplizierung verarbeitet werden, ist es sehr wahrscheinlich, dass der Speicherplatz knapp wird. Wenn jedoch viele Sicherungsoperationen die clientseitige Datendeduplizierung verwenden, kann dieses Problem auch bei Dateien mit geringerer Größe auftreten.	Informationen zur Optimierung des DB2-Parameters LOCKLIST finden Sie in Serverseitige Datendeduplizierung optimieren.
Ist genügend Bandbreite verfügbar, um Daten auf einen IBM Spectrum Protect-Server zu übertragen?	Um Daten auf einen IBM Spectrum Protect-Server zu übertragen, verwenden Sie die clientseitige oder serverseitige Datendeduplizierung und die Komprimierung, um die erforderliche Bandbreite zu verringern. Verwenden Sie einen Server der Version 7.1.5 oder höher, um die Inline-Komprimierung verwenden zu können, und einen Client der Version 7.1.6 oder höher, um die erweiterte Komprimierungsverarbeitung zu aktivieren.	Weitere Informationen finden Sie in der Beschreibung der Clientoption enablededup.
Haben Sie festgelegt, wie viele Speicherpoolverzeichnisse jedem Speicherpool zugeordnet werden sollen?	Ordnen Sie Verzeichnisse einem Speicherpool mithilfe des Befehls DEFINE STGPOOLDIRECTORY zu. Erstellen Sie mehrere Speicherpoolverzeichnisse und stellen Sie sicher, dass jedes Verzeichnis auf einem anderen Plattendatenträger (LUN) gesichert wird.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie genügend Plattenspeicherplatz in dem Cloud-Containerspeicherpool zugeordnet?	Um Sicherungsfehler zu verhindern, stellen Sie sicher, dass das lokale Verzeichnis über genügend Speicherplatz verfügt. Verwenden Sie die folgende Liste als Leitfaden für optimalen Plattenspeicherplatz: • Berechnen Sie für SAS-Platten (SAS = Serial-Attached SCSI) und rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu. • Stellen Sie 3 TB für flash-basierte Speichersysteme mit schnellen Netzverbindungen zu leistungsfähigen On-Premises-Cloudsystemen bereit. • Stellen Sie 5 TB für Systeme mit Solid-State-Laufwerk (SSD) mit schnellen Netzverbindungen zu leistungsfähigen Cloudsystemen bereit.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Haben Sie den geeigneten Typ des lokalen Speichers ausgewählt?	Stellen Sie sicher, dass Datenübertragungen aus dem lokalen Speicher in die Cloud beendet werden, bevor der nächste Sicherungszyklus beginnt.
	Tipp: Daten werden kurz nach dem Versetzen in die Cloud aus dem lokalen Speicher entfernt.
	Verwenden Sie die folgenden Richtlinien:
	• Verwenden Sie Flash- oder SSD-Speicher für große Systeme, die über leistungsfähige Cloudsysteme verfügen. Stellen Sie sicher, dass Sie über eine dedizierte 10-GB-WAN-Verbindung mit einer Hochgeschwindigkeitsverbindung zum Objektspeicher verfügen. Verwenden Sie beispielsweise Flash- oder SSD-Speicher, wenn Sie über eine dedizierte 10-GB-WAN-Verbindung sowie eine Hochgeschwindigkeitsverbindung zu einem IBM® Cloud Object Storage-Speicherort oder zu einem Amazon S3-Datencenter (Amazon S3 = Amazon Simple Storage Service) verfügen.
	• Verwenden Sie SAS-Platten mit 15000 U/min mit größerer Kapazität für die folgenden Szenarios:
	  ◦ Systeme mittlerer Größe
	  ◦ Langsamere Cloudverbindungen, z. B. 1 GB
	  ◦ Bei Verwendung von IBM Cloud Object Storage als Service-Provider in mehreren Regionen
	• Berechnen Sie für SAS-Platten oder rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.	

AIX: Planung für Speicherpools auf DISK- oder FILE-Einheiten

Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Können die Speicherpool-LUNs Durchsatzraten von 256 KB für sequenzielle Lese- und Schreibvorgänge aufrechterhalten, um die Arbeitslast innerhalb der Zeitvorgaben adäquat handhaben zu können?	Bei der Planung für Spitzenbelastungen müssen Sie alle Daten berücksichtigen, die der Server gleichzeitig aus Plattenspeicherpools lesen oder in Plattenspeicherpools schreiben soll. Berücksichtigen Sie beispielsweise den Spitzenwert für den Datenfluss bei Clientsicherungsoperationen und Serverdatenversetzungsoperationen, wie z. B. Umlagerung, die gleichzeitig ausgeführt werden. Der IBM Spectrum Protect-Server verwendet beim Lesen aus Speicherpools und Schreiben in Speicherpools in erster Linie 256-KB-Blöcke. Wenn das Plattensystem über die entsprechende Funktionalität verfügt, konfigurieren Sie das Plattensystem für die optimale Leistung mit sequenziellen Lese-/Schreiboperationen statt mit wahlfreien Lese-/Schreiboperationen.	Weitere Informationen finden Sie in Basisleistung von Plattensystemen analysieren.
Ist die Platte für die Verwendung von Lese- und Schreibcache konfiguriert?	Verwenden Sie mehr Cache, um eine bessere Leistung zu erzielen.	
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, eine geeignete Größe für die Speicherpooldatenträger festgelegt?	Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden. Wenn Sie nicht über die nötigen Informationen zum Schätzen der Größe für Datenträger mit der Einheitenklasse FILE verfügen, beginnen Sie mit einer Datenträgergröße von 50 GB.	In der Regel treten häufiger Probleme auf, wenn die Datenträger zu klein sind. Wenn Datenträger größer als erforderlich sind, treten nur selten Probleme auf. Wenn Sie die zu verwendende Datenträgergröße festlegen, sollten Sie als Vorsichtsmaßnahme eine größere Größe als erforderlich wählen.
Verwenden Sie für Speicherpools, die die Einheitenklasse FILE verwenden, vorab zugeordnete Datenträger?	Arbeitsdatenträger können eine Dateifragmentierung zur Folge haben. Um sicherzustellen, dass für einen Speicherpool immer genügend Datenträger verfügbar sind, setzen Sie den Parameter MAXSCRATCH auf einen Wert größer als null.	Ordnen Sie mithilfe des Befehls DEFINE VOLUME Datenträger in dem Speicherpool vorab zu. Verwenden Sie den Serverbefehl DEFINE STGPOOL oder UPDATE STGPOOL, um den Parameter MAXSCRATCH zu definieren.
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, die maximale Anzahl Clientsitzungen mit der Anzahl definierter Datenträger verglichen?	Es müssen immer genügend verwendbare Datenträger in den Speicherpools vorhanden sein, um die erwartete maximale Anzahl gleichzeitig ausgeführter Clientsitzungen handhaben zu können. Bei den Datenträgern kann es sich um Arbeitsdatenträger, leere Datenträger oder teilweise gefüllte Datenträger handeln.	Bei Speicherpools, die die Einheitenklasse FILE verwenden, kann jeweils nur eine einzige Sitzung oder ein einziger Prozess auf einen Datenträger schreiben.
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, den Parameter MOUNTLIMIT für die Einheitenklasse auf einen Wert gesetzt, der für die Anzahl Datenträger, die parallel angehängt werden könnten, ausreichend hoch ist?	Für Speicherpools, die die Datendeduplizierung verwenden, liegt der Wert für den Parameter MOUNTLIMIT in der Regel zwischen 500 und 1000. Setzen Sie den Wert für MOUNTLIMIT auf die maximale Anzahl Mountpunkte, die für alle aktiven Sitzungen erforderlich sind. Berücksichtigen Sie Parameter, die sich auf die maximale Anzahl erforderlicher Mountpunkte auswirken: • Die Serveroption MAXSESSIONS, die die maximal zulässige Anzahl gleichzeitig ablaufender IBM Spectrum Protect-Sitzungen angibt • Der Parameter MAXNUMMP, der die maximale Anzahl Mountpunkte definiert, die jeder Clientknoten verwenden kann Wenn beispielsweise die maximalen Anzahl Sicherungssitzungen für Clientknoten normalerweise 100 ist und für jeden der Knoten `MAXNUMMP=2` definiert ist, multiplizieren Sie 100 Knoten mit 2 Mountpunkten für jeden Knoten, um den Wert 200 für den Parameter MOUNTLIMIT zu erhalten.	Verwenden Sie den Serverbefehl REGISTER NODE oder UPDATE NODE, um den Parameter MAXNUMMP für Clientknoten zu definieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie für Speicherpools, die die Einheitenklasse DISK verwenden, festgelegt, wie viele Speicherpooldatenträger in jedes Dateisystem gestellt werden sollen?	Die Konfiguration des Speichers für einen Speicherpool, der eine Einheitenklasse DISK verwendet, ist davon abhängig, ob Sie RAID für das Plattensystem verwenden. Wenn Sie RAID nicht verwenden, konfigurieren Sie ein einzige Dateisystem pro physischer Platte und definieren Sie exakt einen Speicherpooldatenträger für jedes Dateisystem. Wenn Sie RAID 5 mit *n* + 1 Datenträgern verwenden, konfigurieren Sie den Speicher auf eine der folgenden Arten: • Konfigurieren Sie *n* Dateisysteme auf der LUN und definieren Sie exakt einen Speicherpooldatenträger pro Dateisystem. • Konfigurieren Sie ein einziges Dateisystem und *n* Speicherpooldatenträger für die LUN.	Ein Beispiellayout, bei dem diese Richtlinie eingehalten wird, zeigt Beispiellayout für Serverspeicherpools.
Haben Sie Ihre Speicherpools für die Verteilung der Ein-/Ausgabe auf mehrere Dateisysteme erstellt?	Stellen Sie sicher, dass sich jedes Dateisystem auf einer anderen LUN auf dem Plattensystem befindet. Normalerweise sind 10-30 Dateisysteme ein geeigneter Wert, Sie müssen jedoch sicherstellen, dass die Dateisysteme nicht kleiner als etwa 250 GB sind.	Ausführliche Informationen finden Sie in: • Plattenspeicher für den Server optimieren • Speicherpools und Datenträger optimieren und konfigurieren

AIX: Planung für die Auswahl des korrekten Speichertechnologietyps

Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.

Vorgehensweise

Die folgende Tabelle unterstützt Sie bei der Auswahl des korrekten Speichertechnologietyps für die Speicherressourcen, die der Server erfordert.

Tabelle 1. Speichertechnologietypen für IBM Spectrum Protect-Speicherbedarf

Speichertech-nologietyp	Datenbank	Aktive Protokolldatei	Archivprotokoll und Archivübernahmepro-tokoll	Speicherpools
Solid-State-Laufwerk (SSD)	Stellen Sie die Datenbank auf ein Solid-State-Laufwerk, wenn die folgenden Bedingungen erfüllt sind: • Sie verwenden die IBM Spectrum Protect-Datendeduplizie-rung. • Sie sichern täglich mehr als 8 TB neuer Daten.	Wenn Sie die IBM Spectrum Protect-Datenbank auf ein Solid-State-Laufwerk stellen (dies ist das bewährte Verfahren), stellen Sie auch die aktive Protokolldatei auf ein Solid-State-Laufwerk. Wenn kein Speicherplatz verfügbar ist, verwenden Sie stattdessen eine Hochleistungsplatte.	Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Das Archivprotokoll und die Archivüber-nahmeprotokolle können auf langsamere Speichertechno-logietypen gestellt werden.	Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Speicherpools können auf langsamere Speichertechnologie-typen gestellt werden.

Speichertech-nologietyp	Datenbank	Aktive Protokolldatei	Archivprotokoll und Archivübernahmepro-tokoll	Speicherpools
Hochleistungs-platte mit den folgenden Kenndaten: • **Platte mit 15.000 U/min** • **Fibre Channel- oder Serial-attached SCSI-Schnittstelle (SAS-Schnittstelle)**	Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind: • Der Server führt keine Datendeduplizierung aus. • Der Server führt keine Knotenreplikation aus. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.	Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind: • Der Server führt keine Datendeduplizierung aus. • Der Server führt keine Knotenreplikation aus. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.	Sie können Hochleistungsplatten für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.	Verwenden Sie Hochleistungsplatten für Speicherpools, wenn die folgenden Bedingungen erfüllt sind: • Daten werden häufig gelesen. • Daten werden häufig geschrieben. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.
Platte mit mittlerer Leistung oder Hochleis-tungsplatte mit den folgenden Kenndaten: • **Platte mit 10.000 U/min** • **Fibre Channel- oder SAS-Schnittstelle**	Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.	Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.	Sie können eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für das Archivprotokoll und die Archivüber-nahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.	Verwenden Sie eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für Speicherpools, wenn die folgenden Bedingungen erfüllt sind: • Daten werden häufig gelesen. • Daten werden häufig geschrieben. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.
SATA, Network-attached Storage (NAS)	Verwenden Sie diesen Speicher nicht für die Datenbank. Stellen Sie die Datenbank nicht auf XIV-Speichersysteme.	Verwenden Sie diesen Speicher nicht für die aktive Protokolldatei.	Die Verwendung dieser langsameren Speichertechnologie ist akzeptabel, da diese Protokolle einmal geschrieben und nur selten gelesen werden.	Verwenden Sie diese langsamere Speichertechnologie, wenn die folgenden Bedingungen erfüllt sind: • Daten werden selten geschrieben, beispielsweise einmal. • Daten werden selten gelesen. .
Bänder und virtuelle Bänder				Verwenden Sie diese Speichermedien für die langfristige Aufbewahrung oder wenn Daten nur selten verwendet werden.

AIX: Bewährte Verfahren bei der Serverinstallation anwenden

Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

Vorgehensweise

- Nachfolgend sind die wichtigsten bewährten Verfahren für die Erzielung der optimalen Leistung und die Vermeidung von Problemen aufgeführt.
- Bestimmen Sie anhand der Tabelle die bewährten Verfahren, die für Ihre Umgebung gelten.

Bewährtes Verfahren	**Weitere Informationen**
Verwenden Sie schnelle Platten für die Serverdatenbank. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung.	Verwenden Sie schnelle Platten mit kurzer Latenzzeit für die Datenbank. Die Verwendung von Solid-State-Laufwerken ist von entscheidender Bedeutung, wenn Sie die Datendeduplizierung und Knotenreplikation verwenden. Vermeiden Sie die Verwendung von SATA-Laufwerken (SATA = Serial Advanced Technology Attachment) und PATA-Laufwerken (PATA = Parallel Advanced Technology Attachment). Ausführliche Informationen und weitere Tipps finden Sie in: ○ "Planung für Platten für die Serverdatenbank" ○ "Planung für die Auswahl des korrekten Speichertechnologietyps"
Stellen Sie sicher, dass das Serversystem über genügend Speicher verfügt.	Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309. Höhere Arbeitslasten erfordern mehr als die Mindestvoraussetzungen. Erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation können mehr Speicher als den Mindestspeicher erfordern, der im Dokument mit den Systemvoraussetzungen angegeben ist. Wenn Sie die Ausführung mehrerer Instanzen planen, ist für jede Instanz der für einen einzelnen Server aufgelistete Speicher erforderlich. Multiplizieren Sie den für einen einzelnen Server erforderlichen Speicher mit der Anzahl der für das System geplanten Instanzen.
Trennen Sie die Serverdatenbank, die aktive Protokolldatei, das Archivprotokoll und die Plattenspeicherpools voneinander.	Stellen Sie alle IBM Spectrum Protect-Speicherressourcen auf unterschiedliche Platten. Trennen Sie Speicherpoolplatten von den Platten für die Serverdatenbank und die Protokolle. Speicherpooloperationen können Datenbankoperationen beeinträchtigen, wenn sich die Speicherpools und die Datenbank auf denselben Platten befinden. Im Idealfall werden auch die Serverdatenbank und die Protokolle voneinander getrennt. Ausführliche Informationen und weitere Tipps finden Sie in: ○ "Planung für Platten für die Serverdatenbank" ○ "Planung für Platten für das Serverwiederherstellungsprotokoll" ○ "Planung für Speicherpools auf DISK- oder FILE-Einheiten"
Verwenden Sie mindestens vier Verzeichnisse für die Serverdatenbank. Verwenden Sie für größere Server oder Server, die erweiterte Funktionen verwenden, acht Verzeichnisse.	Stellen Sie jedes Verzeichnis auf eine LUN, die von anderen LUNs und von anderen Anwendungen getrennt ist. Ein Server wird als großer Server betrachtet, wenn seine Datenbank größer als 2 TB ist oder wahrscheinlich diese Größe erreichen wird. Verwenden Sie für derartige Server acht Verzeichnisse. Siehe "Planung für Platten für die Serverdatenbank".
Wenn Sie die Datendeduplizierung und/oder die Knotenreplikation verwenden, beachten Sie die Richtlinien für die Datenbankkonfiguration und andere Elemente.	Konfigurieren Sie den Server gemäß den Richtlinien, da die Datenbank in Bezug darauf, wie gut die Ausführung des Servers bei Verwendung dieser Funktionen ist, extrem wichtig ist. Ausführliche Informationen und weitere Tipps finden Sie in: ○ Prüfliste für Datendeduplizierung ○ Prüfliste für Knotenreplikation

Bewährtes Verfahren	Weitere Informationen
Beachten Sie bei Speicherpools, die Einheitenklassen des Typs FILE verwenden, die Richtlinien für die Größe von Speicherpooldatenträgern. In der Regel sind Datenträger mit einer Größe von 50 GB am besten geeignet.	Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden zur Bestimmung der Datenträgergröße. Konfigurieren Sie Speicherpooleinheiten und Dateisysteme auf der Basis der Anforderungen in Bezug auf den Durchsatz und nicht nur auf der Basis der Kapazitätsanforderungen. Trennen Sie die Speichereinheiten, die von IBM Spectrum Protect verwendet werden, von anderen Anwendungen mit hoher Ein-/Ausgabe und stellen Sie sicher, dass der Durchsatz für diesen Speicher ausreichend ist. Weitere Informationen finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.
Planen Sie IBM Spectrum Protect-Clientoperationen und -Serververwaltungsaktivitäten, um eine Überschneidung von Operationen zu verhindern oder auf ein Mindestmaß zu reduzieren.	Weitere ausführliche Informationen liefern die folgenden Themen: ◦ Zeitplan für tägliche Operationen optimieren ◦ Prüfliste für Serverkonfiguration
Überwachen Sie Operationen kontinuierlich.	Die Überwachung ermöglicht es Ihnen, Probleme frühzeitig erkennen und Ursachen leichter ermitteln zu können. Bewahren Sie Aufzeichnungen von Überwachungsberichten bis zu einem Jahr lang auf, um Trends schneller erkennen und Wachstum besser planen zu können. Siehe Umgebung im Hinblick auf die Leistung überwachen und verwalten.

AIX: Systemmindestvoraussetzungen für AIX-Systeme

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem AIX-Betriebssystem ohne Datendeduplizierung installieren.

Hardware- und Softwarevoraussetzungen für die IBM Spectrum Protect-Serverinstallation

Die folgenden Tabellen enthalten die Mindesthardware- und -softwarevoraussetzungen für die Installation eines IBM Spectrum Protect-Servers. Verwenden Sie diese Voraussetzungen als Ausgangspunkt für Systeme ohne Datendeduplizierung. Die optimale IBM Spectrum Protect-Umgebung ist mit Datendeduplizierung mithilfe der IBM Spectrum Protect Blueprints konfiguriert. Die neuesten Informationen zu den Systemvoraussetzungen finden Sie unter Technote 1243309.

Hardwarevoraussetzungen

In Tabelle 1 sind die Hardwaremindestvoraussetzungen für den Server beschrieben. Wenn der Server die Mindestvoraussetzungen nicht erfüllt, schlägt die Installation fehl. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in AIX: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen

Hardwaretyp	Hardwarevoraussetzungen
Hardware	Ein ordnungsgemäß konfigurierter Computer mit POWER5-System oder höher (64-Bit)

Hardwaretyp	Hardwarevoraussetzungen
Plattenspeicher	Folgende Mindestwerte für den Plattenspeicher: • 5 GB für das Installationsverzeichnis • 512 MB für das Verzeichnis /var • 2 GB für das Verzeichnis /tmp • 128 MB im Ausgangsverzeichnis des Rootbenutzers • 2 GB für den Bereich der gemeinsam genutzten Ressourcen Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben. Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten. Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN. Lesen Sie den Abschnitt zur AIX: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.
Hauptspeicher	Die folgenden Werte geben den Mindestsystemspeicherbedarf für Server mit Datenbanken bis zu 500 GB und einer Aufnahme von maximal 200 GB pro Tag an: • 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation • 24 GB für Datendeduplizierung oder Knotenreplikation • 32 GB für Knotenreplikation mit Datendeduplizierung Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect. Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.

Softwarevoraussetzungen

In Tabelle 2 sind die für einen Server auf einem AIX-System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

Softwaretyp	Softwaremindestvoraussetzungen

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	AIX 6.1 in einer 64-Bit-Kernel-Umgebung mit folgenden zusätzlichen Voraussetzungen: • AIX 6.1 TL 7 und SP6. • C++-Mindestlaufzeitversion mit den Dateigruppen xlC.rte 12.1.0.1 oder höher. Die Dateigruppe wird automatisch aktualisiert, wenn die Version älter als 12.1.0.1 ist. Die Dateigruppe ist im Fixpackpaket für IBM® C++ Runtime Environment Components for AIX vom Juni 2008 enthalten. AIX 7.1 in einer 64-Bit-Kernel-Umgebung. • AIX 7.1 TL 4 und SP2. • C++-Mindestlaufzeitversion mit den Dateigruppen xlC.rte 12.1.0.1 oder höher. Die Dateigruppe wird automatisch aktualisiert, wenn die Version älter als 12.1.0.1 ist. Die Dateigruppe ist im Fixpackpaket für IBM C++ Runtime Environment Components for AIX vom Juni 2008 enthalten. AIX 7.2 in einer 64-Bit-Kernel-Umgebung. • AIX 7.2 TL 0 und SP2. • C++-Mindestlaufzeitversion mit den Dateigruppen xlC.rte 13.1.3.1 oder höher. Die Dateigruppe wird automatisch aktualisiert, wenn die Version älter als 13.1.3.1 ist. Aktuelle Empfehlungen für AIX-Programmfixes finden Sie unter Technote 21165448 Damit die Funktion NPIV (N_Port ID Virtualization) genutzt werden kann, müssen die folgenden Mindestvoraussetzungen erfüllt sein: • Virtual I/O Server 2.1.2 oder höher • AIX 7.1 oder höher • Ein vom entsprechenden AIX-Server und Virtual I/O Server unterstützter HBA-Adapter
Übertragungsprotokoll	Eine konfigurierte Übertragungsmethode.
Verarbeitung	Asynchrone Ein-/Ausgabe muss aktiviert sein.
Einheitentreiber	Der IBM Spectrum Protect-Einheitentreiber ist für Laufwerke und Bandarchive eines anderen Herstellers erforderlich. Das IBM Spectrum Protect-Einheitentreiberpaket enthält Einheitentreibertools und ACSLS-Dämonen. Für die Bandarchive bzw. Bandlaufwerke IBM 3590, 3592 oder Ultrium sind die IBM Einheitentreiber erforderlich. Installieren Sie die aktuellen Einheitentreiber. IBM-Treiberpakete finden Sie bei Fix Central. Konfigurieren Sie die Einheitentreiber, bevor Sie den Server für Bandeinheiten verwenden.
Dienstprogramm gunzip	Das Dienstprogramm gunzip muss auf Ihrem System verfügbar sein, bevor Sie den Server installieren oder aktualisieren. Stellen Sie sicher, dass das Dienstprogramm gunzip installiert ist und dass der entsprechende Pfad in der Umgebungsvariablen PATH definiert ist.
Sonstige Software	Korn-Shell (ksh) ist erforderlich. Konfigurieren Sie die I/O Completion Ports (IOCP) auf dem Betriebssystem. Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisserver verwenden: • Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2) • IBM Security Directory Server Version 6.3 • IBM Security Directory Server Version 6.4

AIX-Betriebssysteme

AIX: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System

Sie können andere Produkte, die DB2-Produkte auf demselben System wie der IBM Spectrum Protect-Server der Version 8.1.2 implementieren und verwenden, mit einigen Einschränkungen installieren.

Damit andere Produkte, die ein DB2-Produkt auf demselben System wie der IBM Spectrum Protect-Server verwenden, installiert und verwendet werden können, müssen die folgenden Bedingungen erfüllt sein:

Tabelle 1. Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System

Bedingung	Anweisungen

Bedingung	Anweisungen
Versionsstand	Die anderen Produkte, die ein DB2-Produkt verwenden, müssen DB2 Version 9 oder höher verwenden. DB2-Produkte verfügen ab Version 9 über die Unterstützung für Produktkapselung und -trennung. Ab dieser Version können Sie mehrere Kopien von DB2-Produkten mit unterschiedlichen Codeversionen auf demselben System ausführen. Ausführliche Informationen finden Sie in dem Abschnitt über mehrere DB2-Kopien in der Produktinformation zu DB2.
Benutzer-IDs und Verzeichnisse	Stellen Sie sicher, dass die Benutzer-IDs, die IDs der abgeschirmten Benutzer, die Installationsposition, andere Verzeichnisse und zugehörige Informationen nicht von mehreren DB2-Installationen gemeinsam genutzt werden. Ihre Angaben müssen sich von den IDs und Positionen unterscheiden, die Sie für die Installation und Konfiguration des IBM Spectrum Protect-Servers verwendet haben. Wenn Sie den Assistenten dsmicfgx für die Konfiguration des Servers verwendet haben, haben Sie diese Werte während der Ausführung des Assistenten eingegeben. Wenn Sie eine manuelle Konfiguration durchgeführt haben, überprüfen Sie im Bedarfsfall die verwendeten Prozeduren, um sich die für den Server verwendeten Werte in Erinnerung zu rufen.
Ressourcenzuordnung	Sie müssen die Ressourcen und das Leistungsspektrum des Systems gegen die Anforderungen für den IBM Spectrum Protect-Server und die anderen Anwendungen, die das DB2-Produkt verwenden, abwägen. Damit den anderen DB2-Anwendungen genügend Ressourcen zur Verfügung stehen, müssen Sie unter Umständen die Einstellungen des IBM Spectrum Protect-Servers ändern, so dass der Server weniger Systemspeicher und -ressourcen verwendet. Wenn die Verarbeitungsprozesse für die anderen DB2-Anwendungen und der IBM Spectrum Protect-Server um Prozessor- und Speicherressourcen konkurrieren, kann die Leistung des Servers in Bezug auf die Verarbeitung der erwarteten Clientauslastung oder anderer Serveroperationen beeinträchtigt werden. Um die Ressourcen zu trennen und die Möglichkeit zur Optimierung und Zuordnung von Prozessor-, Speicher- und anderen Systemressourcen für mehrere Anwendungen zu verbessern, sollten Sie Unterstützung für logische Partitionen (LPAR), Auslastungspartitionierung (WPAR) oder andere Unterstützung für virtuelle Workstations einsetzen. Führen Sie eine DB2-Anwendung beispielsweise auf einem eigenen virtuellen System aus.

AIX: IBM Installation Manager

IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager noch nicht installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie IBM Spectrum Protect installieren. Die Software muss auf dem System installiert bleiben, damit IBM Spectrum Protect später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

Angebot
: Eine installierbare Einheit eines Softwareprodukts.

  Das Angebot 'IBM Spectrum Protect' enthält alle Datenträger, die IBM Installation Manager für die Installation von IBM Spectrum Protect benötigt.

Paket
: Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.
  Das IBM Spectrum Protect-Paket enthält folgende Komponenten:

  - Installationsprogramm IBM Installation Manager
  - Das Angebot 'IBM Spectrum Protect'

Paketgruppe
: Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

  Die Standardpaketgruppe für das IBM Spectrum Protect-Paket ist `IBM Installation Manager`.

Repository
: Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

  Das IBM Spectrum Protect-Paket wird in einem Repository in IBM Fix Central gespeichert.

Verzeichnis für gemeinsam genutzte Ressourcen
: Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

  In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version von IBM Spectrum Protect verwendet werden.

AIX: Arbeitsblätter für Planungsdetails für den Server

Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.

Element	Erforderlicher Speicherbereich	Anzahl der Verzeichnisse	Position der Verzeichnisse
Die Datenbank			
Aktive Protokolldatei			
Archivprotokoll			
Optional: Protokollspiegel für die aktive Protokolldatei			
Optional: Sekundäres Archivprotokoll (Übernahmeverzeichnis für Archivprotokolle)			

Element	Namen und Benutzer-IDs	Position
Die *Instanzbenutzer-ID* für den Server. Mit dieser ID starten Sie den IBM Spectrum Protect-Server und führen ihn aus.		
Das *Ausgangsverzeichnis* des Servers. In diesem Verzeichnis befindet sich die Instanzbenutzer-ID.		
Der Datenbankinstanzname		
Das *Instanzverzeichnis* für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien).		
Der Servername; verwenden Sie einen eindeutigen Namen für jeden Server.		

AIX: Kapazitätsplanung

Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.

- AIX: Speicherbedarf für die Datenbank schätzen
  Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.
- AIX: Speicherplatzbedarf für das Wiederherstellungsprotokoll
  In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.
- AIX: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen
  Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.
- AIX: Rollbackdateien der Installation löschen
  Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

AIX: Speicherbedarf für die Datenbank schätzen

Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.

Informationen zu diesem Vorgang

Anfänglich sollte mindestens 25 GB Speicherplatz in der Datenbank verwendet werden. Stellen Sie entsprechend Speicherplatz im Dateisystem bereit. Eine Datenbankgröße von 25 GB ist für eine Testumgebung oder eine Umgebung, die nur einen Speicherarchivmanager umfasst, ausreichend. Für einen Produktionsserver, der Clientlasten unterstützt, sollte die Datenbank größer sein. Wenn Sie Plattenspeicherpools (DISK) mit wahlfreiem Zugriff verwenden, ist mehr Datenbank- und Protokollspeicherbereich erforderlich als für Speicherpools mit sequenziellem Zugriff.

Die maximale Größe der IBM Spectrum Protect-Datenbank beträgt 6 TB.

Informationen zur Festlegung der Größe einer Datenbank in einer Produktionsumgebung, die auf der Anzahl Dateien und der Speicherpoolgröße basiert, enthalten die folgenden Abschnitte.

- AIX: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen
  Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.
- AIX: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen
  Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz kapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.
- AIX: Datenbankmanager und temporärer Speicherbereich
  Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systemspeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

AIX: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen

Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.

Informationen zu diesem Vorgang

Um den Speicherbedarf auf der Basis der maximalen Anzahl Dateien im Serverspeicher zu schätzen, verwenden Sie die folgenden Richtlinien:

- 600-1000 Byte für jede gespeicherte Version einer Datei einschließlich der Imagesicherungen.
  Einschränkung: Diese Richtlinie umfasst nicht den Speicherplatz, der während der Datendeduplizierung verwendet wird.
- 100-200 Byte für jede Datei im Cache, jede Kopienspeicherpooldatei, jede Datei im Pool für aktive Daten und jede dedupliziert Datei.
- Zusätzlicher Speicherbereich ist für die Datenbankoptimierung erforderlich, um variable Datenzugriffsmuster und die Server-Back-End-Verarbeitung von Daten zu unterstützen. Die Größe des zusätzlichen Speicherplatzes entspricht 50 % der Schätzung für die Gesamtanzahl Byte für Dateiobjekte.

In dem folgenden Beispiel für einen einzelnen Client basieren bei Berechnungen auf den Maximalwerten in den vorhergehenden Richtlinien. Bei den Beispielen wird die mögliche Verwendung der Dateiaggregation nicht berücksichtigt. Im Allgemeinen wird durch das Aggregieren kleiner Dateien der erforderliche Speicherplatz in der Datenbank reduziert. Die Dateiaggregation betrifft keine speicherverwalteten Dateien.

Vorgehensweise

1. Berechnen Sie die Anzahl Dateiversionen. Addieren Sie alle folgenden Werte, um die Anzahl Dateiversionen zu erhalten:
   a. Berechnen Sie die Anzahl gesicherter Dateien. Beispiel: Möglicherweise werden bis zu 500.000 Clientdateien gleichzeitig gesichert. In diesem Beispiel sind die Speichermaßnahmen so definiert, dass maximal drei Kopien gesicherter Dateien aufbewahrt werden:

      ```
      500.000 Dateien * 3 Kopien = 1.500.000 Dateien
      ```

   b. Berechnen Sie die Anzahl Archivierungsdateien. Beispiel: Bis zu 100.000 Clientdateien können archivierte Kopien sein.
   c. Berechnen Sie die Anzahl speicherverwalteter Dateien. Beispiel: Bis zu 200.000 Clientdateien können von Client-Workstations umgelagert werden.

   Bei Verwendung von 1000 Byte pro Datei beträgt der Gesamtspeicherplatz in der Datenbank, der für die zu dem Client gehörigen Dateien erforderlich ist, 1,8 GB:

   ```
   (1.500.000 + 100.000 + 200.000) * 1000 = 1,8 GB
   ```

2. Berechnen Sie die Anzahl Dateien im Cache, Kopienspeicherpooldateien, Dateien im Pool für aktive Daten und deduplizierter Dateien:
   a. Berechnen Sie die Anzahl der Cachekopien. Beispiel: In einem Plattenspeicherpool mit 5 GB Kapazität ist Caching aktiviert. Die obere Umlagerungsschwelle des Pools ist 90 % und die untere Umlagerungsschwelle ist 70 %. Das heißt 20 % des Plattenpools (oder 1 GB) wird von Cachedateien belegt.
   Wenn die durchschnittliche Dateigröße ungefähr 10 KB beträgt, enthält der Cache zu jedem beliebigen Zeitpunkt etwa 100.000 Dateien:

```
100.000 Dateien * 200 Byte = 19 MB
```

b. Berechnen Sie die Anzahl Kopienspeicherpooldateien. Alle primären Speicherpools werden im Kopienspeicherpool gesichert:

```
(1.500.000 + 100.000 + 200.000) * 200 Byte = 343 MB
```

c. Berechnen Sie die Anzahl Dateien im Speicherpool für aktive Daten. Alle aktiven Clientsicherungsdaten in primären Speicherpools werden in den Speicherpool für aktive Daten kopiert. Angenommen, es sind 500.000 Versionen der 1.500.000 Sicherungsdateien im primären Speicherpool aktiv:

```
500.000 * 200 Byte = 95 MB
```

d. Berechnen Sie die Anzahl deduplizierter Dateien. Angenommen, ein deduplizierter Speicherpool enthält 50.000 Dateien:

```
50.000 * 200 Byte = 10 MB
```

Auf der Basis der vorhergehenden Berechnungen sind etwa 0,5 GB zusätzlicher Speicherplatz in der Datenbank für die Cachedateien, die Kopienspeicherpooldateien, die Dateien im Pool für aktive Daten und die deduplizierten Dateien des Clients erforderlich.

3. Berechnen Sie den zusätzlichen Speicherplatz, der für die Datenbankoptimierung benötigt wird. Um optimalen Datenzugriff und optimale Verwaltung durch den Server bereitzustellen, ist zusätzlicher Speicherplatz in der Datenbank erforderlich. Die Größe des zusätzlichen Speicherplatzes in der Datenbank beträgt 50 % des Gesamtspeicherbedarfs für Dateiobjekte.

```
(1,8 + 0,5) * 50 % = 1,2 GB
```

4. Die Gesamtgröße des für den Client erforderlichen Datenbankspeicherbereichs berechnen. Die Gesamtgröße beträgt ca. 3,5 GB:

```
1,8 + 0,5 + 1,2 = 3,5 GB
```

5. Berechnen Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist. Wenn der Client, der in den vorhergehenden Berechnungen verwendet wurde, ein typischer Client ist und Sie beispielsweise über 500 Clients verfügen, können Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist, mithilfe der folgenden Berechnung schätzen:

```
500 * 3,5 = 1,7 TB
```

Ergebnisse

Tipp: In den Beispielen oben handelt es sich bei den Ergebnissen um Schätzungen. Die tatsächliche Größe der Datenbank kann aufgrund von Faktoren wie beispielsweise der Anzahl Verzeichnisse und der Länge der Pfad- und Dateinamen von der geschätzten Größe abweichen. Sie sollten die Datenbank regelmäßig überwachen und die Größe wie erforderlich anpassen.

Nächste Schritte

Während des normalen Betriebs erfordert der IBM Spectrum Protect-Server möglicherweise temporären Speicherplatz in der Datenbank. Dieser Speicherplatz wird aus den folgenden Gründen benötigt:

- Zum Speichern der Ergebnisse der Sortierung oder Änderung der Reihenfolge, die noch nicht in der Datenbank aufbewahrt und in der Datenbank nicht unmittelbar optimiert werden. Die Ergebnisse werden vorübergehend in der Datenbank zur Verarbeitung gespeichert.
- Zum Erteilen des Verwaltungszugriffs auf die Datenbank über eine der folgenden Methoden:
  - Ein DB2-ODBC-Client (ODBC = Open Database Connectivity)
  - Ein Oracle-JDBC-Client (JDBC = Java™ Database Connectivity)
  - SQL (Structured Query Language) für den Server über die Befehlszeile eines Verwaltungsclients

Erwägen Sie die Verwendung von zusätzlichen 50 GB an temporärem Speicherplatz pro 500 GB Speicherbereich für Dateiobjekte und Optimierung. Siehe die Richtlinien in der folgenden Tabelle. In dem Beispiel, das im vorhergehenden Schritt verwendet wurde, sind insgesamt 1,7 TB Speicherplatz in der Datenbank für Dateiobjekte und die Optimierung für 500 Clients erforderlich. Auf der Basis dieser Berechnung sind 200 GB für temporären Speicherplatz erforderlich. Der erforderliche Gesamtspeicherplatz in der Datenbank beträgt 1,9 TB.

Datenbankgröße	Mindestens erforderlicher temporärer Speicherplatz
< 500 GB	50 GB
≥ 500 GB und < 1 TB	100 GB
≥ 1 TB und < 1,5 TB	150 GB
≥ 1,5 und < 2 TB	200 GB
≥ 2 und < 3 TB	250-300 GB
≥ 3 und < 4 TB	350-400 GB

AIX: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen

Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz kapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.

AIX: Datenbankmanager und temporärer Speicherbereich

Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systemspeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

Der Datenbankmanager sortiert Daten in einer bestimmten Reihenfolge, gemäß der SQL-Anweisung, mit der Sie die Daten anfordern. Je nach Auslastung des Servers und wenn es mehr Daten gibt, als der Datenbankmanager verwalten kann, werden die (der Reihenfolge nach sortierten) Daten temporärem Plattenspeicher zugeordnet. Daten werden temporärem Plattenspeicher zugeordnet, wenn die Ergebnismenge sehr umfangreich ist. Der Datenbankmanager verwaltet den verwendeten Speicher dynamisch, wenn Daten temporärem Plattenspeicher zugeordnet werden.

Bei der Verfallsverarbeitung kann beispielsweise eine umfangreiche Ergebnismenge generiert werden. Wenn der Systemspeicher in der Datenbank zur Speicherung der Ergebnismenge nicht ausreicht, wird ein Teil der Daten temporärem Plattenspeicher zugeordnet. Wenn während der Verfallsverarbeitung ein Knoten oder ein Dateibereich ausgewählt wird, der für die Verarbeitung zu groß ist, kann der Datenbankmanager die Daten im Speicher nicht sortieren. Der Datenbankmanager muss temporären Speicherbereich zum Sortieren der Daten verwenden.

Bei der Ausführung von Datenbankoperationen sollten Sie in den folgenden Szenarios eine Erweiterung des Speicherplatzes in der Datenbank vornehmen:

- Der Speicherbereich der Datenbank ist klein und die Serveroperation, die temporären Speicherbereich benötigt, belegt den verbleibenden freien Speicherbereich.
- Die Dateibereiche sind groß oder den Dateibereichen ist eine Maßnahme zugeordnet, durch die viele Dateiversionen erstellt werden.
- Der IBM Spectrum Protect-Server muss mit begrenztem Speicher ausgeführt werden. Die Datenbank verwendet den Hauptspeicher des IBM Spectrum Protect-Servers für Datenbankoperationen. Ist der verfügbare Speicher jedoch nicht ausreichend, ordnet der IBM Spectrum Protect-Server der Datenbank temporären Speicherbereich auf Platte zu. Wenn beispielsweise 10G Speicher zur Verfügung stehen und Datenbankoperationen 12G Speicher benötigen, verwendet die Datenbank temporären Speicherbereich.
- Bei der Implementierung eines IBM Spectrum Protect-Servers wird ein Fehler aufgrund fehlenden Datenbankspeicherbereichs (`out of database space`) angezeigt. Überwachen Sie das Serveraktivitätenprotokoll auf Nachrichten, die sich auf den Datenbankspeicherbereich beziehen.

Wichtig: Sie dürfen die DB2-Software, die mit IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht verändern. Führen Sie keine Installation bzw. kein Upgrade auf eine andere Version, ein anderes Release oder ein anderes Fixpack der DB2-Software durch, um eine Beschädigung der Datenbank zu vermeiden.

AIX: Speicherplatzbedarf für das Wiederherstellungsprotokoll

In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.

- AIX: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll
  Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.
- AIX: Speicherbereich des Spiegels für aktive Protokolldateien
  Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.
- AIX: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle
  Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

AIX: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll

Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.

In IBM Spectrum Protect-Servern der Version 7.1 und höher kann die aktive Protokolldatei eine maximale Größe von 512 GB haben. Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist.

Berücksichtigen Sie bei der Schätzung der Größe der aktiven Protokolldatei die folgenden allgemeinen Richtlinien:

- Die empfohlene Anfangsgröße für die aktive Protokolldatei ist 16 GB.
- Stellen Sie sicher, das die aktive Protokolldatei mindestens groß genug ist, um die gleichzeitig ablaufende Aktivität handhaben zu können, die der Server in der Regel handhabt. Versuchen Sie als Vorsichtsmaßnahme das größte Arbeitsvolumen zu schätzen, das der Server

jeweils handhabt. Stellen Sie für die aktive Protokolldatei zusätzlichen Speicherbereich bereit, der, falls erforderlich, verwendet werden kann. Ziehen Sie 20 % zusätzlichen Speicherbereich in Betracht.
- Überwachen Sie den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei. Passen Sie die Größe der aktiven Protokolldatei wie erforderlich abhängig von Faktoren wie Clientaktivität und Ebene der Serveroperationen an.
- Stellen Sie sicher, dass das Verzeichnis, das die aktive Protokolldatei enthält, mindestens genauso groß wie die aktive Protokolldatei ist. Ein Verzeichnis, das größer als die aktive Protokolldatei ist, kann Übernahmesituationen handhaben, sollten diese auftreten.
- Stellen Sie sicher, dass das Dateisystem, das das Verzeichnis für aktive Protokolldateien enthält, über mindestens 8 GB freien Speicherbereich für Anforderungen zum Versetzen temporärer Protokolle verfügt.

Die vorgeschlagene Anfangsgröße für das Archivprotokoll beträgt 48 GB.

Das Archivprotokollverzeichnis muss groß genug sein, um die Protokolldateien aufnehmen zu können, die seit der vorherigen Gesamtsicherung generiert wurden. Wenn Sie beispielsweise täglich eine Gesamtsicherung der Datenbank ausführen, muss das Archivprotokollverzeichnis groß genug sein, um die Protokolldateien für die gesamte Clientaktivität aufnehmen zu können, die während 24 Stunden stattfindet. Um Speicherbereich wiederherzustellen, löscht der Server veraltete Archivprotokolldateien nach einer Gesamtsicherung der Datenbank. Wenn das Archivprotokollverzeichnis voll wird und kein Verzeichnis für Archivübernahmeprotokolle vorhanden ist, verbleiben Protokolldateien im Verzeichnis für aktive Protokolldateien. Diese Bedingung kann zur Folge haben, dass das Verzeichnis für aktive Protokolldateien vollständig gefüllt und der Server gestoppt wird. Bei einem Serverneustart wird ein Teil des vorhandenen Speicherbereichs für die aktive Protokolldatei freigegeben wird.

Nach der Installation des Servers können Sie die Archivprotokollauslastung und den Speicherbereich im Archivprotokollverzeichnis überwachen. Wenn sich der Speicherbereich im Archivprotokollverzeichnis füllt, können die folgenden Probleme auftreten:

- Der Server kann keine Datenbankgesamtsicherungen ausführen. Untersuchen und beheben Sie dieses Problem.
- Andere Anwendungen schreiben in das Archivprotokollverzeichnis und belegen den für das Archivprotokoll erforderlichen Speicherbereich. Nutzen Sie den Speicherbereich für das Archivprotokoll nicht gemeinsam mit anderen Anwendungen, einschließlich anderer IBM Spectrum Protect-Server. Stellen Sie sicher, dass jeder Server über eine separate Speicherposition verfügt, dessen Eigner dieser spezifische Server ist und der von diesem spezifischen Server verwaltet wird.

- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen
  Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen
  Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen
  Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen
  Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datendeduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen
  Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.
- AIX: Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen
  Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.
- AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Datendeduplizierungsoperationen schätzen
  Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen

Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen zu bestimmen, führen Sie die folgende Berechnung aus:

```
Anzahl Clients  x  In jeder Transaktion gespeicherte Dateien
  x  Für jede Datei benötigter Protokollspeicherbereich
```

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Grundlegende Clientspeicheroperationen

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3053 Byte	Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	19,5 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 Byte = 3,5 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		
		`3,5 + 16 = 19,5 GB`

Archivprotokoll: vorgeschlagene Größe	58,5 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen.
		
		`3,5 x 3 = 10,5 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		
		`10,5 + 48 = 58,5 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen

Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, zu bestimmen, führen Sie die folgende Berechnung aus:

```
Anzahl Clients x Anzahl Sitzungen pro Client x Anzahl während
  jeder Transaktion gespeicherter Dateien x pro Datei erforderlicher
  Protokollspeicherbereich
```

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Mehrere Clientsitzungen

Element	Beispielwerte		Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	1000	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Mögliche Sitzungen für jeden Client	3	3	Die Einstellung der Clientoption RESOURCEUTILIZATION ist größer als der Standardwert. Jede Clientsitzung führt maximal drei Sitzungen parallel aus.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3053	3053	Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	26,5 GB [1]	51 GB [1]	Die folgende Berechnung wurde für 300 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.
			
			`(300 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 10,5 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`10,5 + 16 = 26,5 GB`
			
			Die folgende Berechnung wurde für 1000 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.
			
			`(1000 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 35 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`35 + 16 = 51 GB`

Archivprotokoll: vorgeschlagene Größe	79,5 GB [1]	153 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, wird die Schätzung für die aktive Protokolldatei mit 3 multipliziert:
			
			`10,5 x 3 = 31,5 GB`
			
			`35 x 3 = 105 GB`
			
			Erhöhen Sie diese Werte um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`31,5 + 48 = 79,5 GB`
			
			`105 + 48 = 153 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre aktive Protokolldatei und passen Sie die Größe, falls erforderlich, an.

AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen

Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.

Der Protokollspeicherbereich, der für jede Datei erforderlich ist, erhöht sich um ungefähr 200 Byte für jeden Kopienspeicherpool, der für eine Operation für gleichzeitiges Schreiben verwendet wird. In dem Beispiel in der folgenden Tabelle werden Daten in einem primären Speicherpool und darüber hinaus in zwei Kopienspeicherpools gespeichert. Die geschätzte Protokollgröße erhöht sich für jede Datei um 400 Byte. Wenn Sie den vorgeschlagenen Wert von 3053 Byte Protokollspeicherbereich pro Datei verwenden, sind insgesamt 3453 Byte erforderlich.

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Operationen für gleichzeitiges Schreiben

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3453 Byte	3053 Byte plus 200 Byte für jeden Kopienspeicherpool. Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	20 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		
		`4 + 16 = 20 GB`

Archivprotokoll: vorgeschlagene Größe	60 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Speicherbedarf für das Archivprotokoll zu schätzen:
		
		`4 GB x 3 = 12 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		
		`12 + 48 = 60 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen

Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datendeduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.

Beispielsweise wird bei der Umlagerung von Dateien aus dem Speicherpool mit wahlfreiem Zugriff (DISK) in einem Plattenspeicherpool mit sequenziellem Zugriff (FILE) für jede Datei, die umgelagert wird, ungefähr 110 Byte Protokollspeicherbereich verwendet. Beispiel: Angenommen, es sind 300 Clients für Sichern/Archivieren vorhanden, von denen jeder 100.000 Dateien jede Nacht sichert. Die Dateien sind anfänglich in einem DISK-Speicherpool gespeichert und werden dann in einen FILE-Speicherpool umgelagert. Um die Größe des Speicherbereichs für die aktive Protokolldatei zu schätzen, die für die Datenumlagerung erforderlich ist, verwenden Sie die folgende Berechnung. Die Anzahl Clients in der Berechnung stellt die maximale Anzahl zu einem beliebigen Zeitpunkt dar, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern.

```
300 Clients x 100.000 Dateien pro Client x 110 Byte = 3,1 GB
```

Addieren Sie diesen Wert zu der Schätzung für die Größe der aktiven Protokolldatei, die für grundlegende Clientspeicheroperationen berechnet wurde.

AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen

Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.

AIX: Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen

Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.

Wenn beispielsweise einmal pro Woche eine Datenbankgesamtsicherung ausgeführt wird, muss der Speicherbereich für das Archivprotokoll groß genug sein, um die Informationen einer vollständigen Woche im Archivprotokoll aufnehmen zu können.

Die unterschiedliche Größe des Archivprotokolls für täglich ausgeführte Datenbankgesamtsicherungen wird in dem Beispiel in der folgenden Tabelle gezeigt.

Tabelle 1. Datenbankgesamtsicherungen

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3453 Byte	3053 Byte für jede Datei plus 200 Byte für jeden Kopienspeicherpool. Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	20 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		
		`4 + 16 = 20 GB`

Element	Beispielwerte	Beschreibung

Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Tag	60 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Sicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen:
		`4 GB x 3 = 12 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		`12 + 48 = 60 GB`

Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Woche	132 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen. Multiplizieren Sie das Ergebnis mit der Anzahl Tage, die zwischen Datenbankgesamtsicherungen liegen.
		`(4 GB x 3 ) x 7 = 84 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		`84 + 48 = 132 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Anfangsgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

AIX: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Datendeduplizierungsoperationen schätzen

Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

Die folgenden Faktoren haben Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll:

Volumen der deduplizierten Daten
: Welche Auswirkungen die Datendeduplizierung auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll hat, ist von dem Prozentsatz an Daten abhängig, der für die Deduplizierung auswählbar ist. Ist der Prozentsatz an Daten, die dedupliziert werden können, relativ hoch, ist mehr Protokollspeicherbereich erforderlich.

Größe und Anzahl Speicherbereiche
: Für jeden Speicherbereich, der durch einen Prozess zum Identifizieren doppelter Daten identifiziert wird, sind ungefähr 1.500 Byte Speicherbereich für die aktive Protokolldatei erforderlich. Werden beispielsweise 250.000 Speicherbereiche durch einen erkennen identifiziert, beträgt die geschätzte Größe der aktiven Protokolldatei 358 MB:

```
250.000 während jedes Prozesses ermittelte Speicherbereiche x 1.500 Byte
 für jeden Speicherbereich = 358 MB
```

Betrachten Sie das folgende Szenario. 300 Clients für Sichern/Archivieren sichern jede Nacht bis zu 100.000 Dateien. Diese Aktivität hat eine Last von 30.000.000 Dateien zur Folge. Die durchschnittliche Anzahl Speicherbereiche für jede Datei ist 2. Demzufolge beträgt die Gesamtzahl Speicherbereiche 60.000.000 und der Speicherbedarf für das Archivprotokoll 84 GB:

```
60.000.000 Speicherbereiche x 1.500 Byte pro Speicherbereich = 84 GB
```

Ein Prozess zum Identifizieren doppelter Daten wird für Aggregate von Dateien ausgeführt. Ein Aggregat besteht aus Dateien, die in einer bestimmten Transaktion gespeichert sind, wie durch die Serveroption TXNGROUPMAX angegeben. Angenommen, die Serveroption TXNGROUPMAX ist auf den Standardwert 4096 gesetzt. Wenn die durchschnittliche Anzahl Speicherbereiche für jede Datei 2 beträgt, ist die Gesamtzahl Speicherbereiche in jedem Aggregat 8192 und der für die aktive Protokolldatei erforderliche Speicherbedarf 12 MB:

```
8192 Speicherbereiche in jedem Aggregat x 1500 Byte pro Speicherbereich =
   12 MB
```

Timing und Anzahl der Prozesse zum Identifizieren doppelter Daten
: Das Timing und die Anzahl Prozesse zum Identifizieren doppelter Daten haben ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei. Bei Verwendung der in dem vorhergehenden Beispiel berechneten Größe der aktiven Protokolldatei von 12 MB beträgt die gleichzeitige Last für die aktive Protokolldatei 120 MB, wenn 10 Prozesse zum Identifizieren doppelter Daten parallel ausgeführt werden:

```
12 MB pro Prozess x 10 Prozesse = 120 MB
```

Dateigröße

Große Dateien, die für die Identifizierung doppelter Daten verarbeitet werden, können ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei haben. Beispiel: Angenommen, ein Client für Sichern/Archivieren sichert ein Dateisystemimage mit einer Größe von 80 GB. Die Anzahl doppelter Speicherbereiche für dieses Objekt kann groß sein, wenn beispielsweise die in das Dateisystemimage eingeschlossenen Dateien mit Teilsicherungen gesichert wurden. Beispiel: Angenommen, ein Dateisystemimage hat 1,2 Millionen doppelte Speicherbereiche. Die 1,2 Millionen Speicherbereiche in dieser großen Datei stellen eine einzige Transaktion für einen Prozess zum Identifizieren doppelter Daten dar. Der Gesamtspeicherbereich in der aktiven Protokolldatei, der für dieses einzelne Objekt erforderlich ist, beträgt 1,7 GB:

```
1.200.000 Speicherbereich x 1.500 Byte pro Speicherbereich = 1,7 GB
```

Wenn andere, kleinere Prozesse zum Identifizieren doppelter Daten zu demselben Zeitpunkt ausgeführt werden wie der Prozess zum Identifizieren doppelter Daten für ein einzelnes großes Objekt, ist in der aktiven Protokolldatei möglicherweise nicht genügend Speicherbereich verfügbar. Beispiel: Angenommen, ein Speicherpool ist für die Deduplizierung aktiviert. Der Speicherpool enthält gemischte Daten, einschließlich vieler relativ kleiner Dateien mit einer Größe von 10 KB bis zu mehreren hundert KB. Der Speicherpool enthält außerdem einige wenige große Objekte mit einem hohen Prozentsatz an doppelten Speicherbereichen.

Um nicht nur den Speicherbedarf zu berücksichtigen, sondern auch das Timing und die Dauer gleichzeitig ablaufender Transaktionen, erhöhen Sie die geschätzte Größe der aktiven Protokolldatei um den Faktor 2. Beispiel: Angenommen, das Ergebnis Ihrer Berechnungen für den Speicherbedarf lautet 25 GB (23,3 GB + 1,7 GB für die Deduplizierung eines großen Objekts). Wenn Deduplizierungsverarbeitung gleichzeitig ausgeführt werden, beträgt die vorgeschlagene Größe der aktiven Protokolldatei 50 GB. Die vorgeschlagene Größe des Archivprotokolls ist 150 GB.

Die Beispiele in den folgenden Tabellen zeigen Berechnungen für aktive Protokolldateien und Archivprotokolle. In dem Beispiel in der ersten Tabelle wird eine durchschnittliche Größe von 700 KB für Speicherbereiche verwendet. In dem Beispiel in der zweiten Tabelle wird eine durchschnittliche Größe von 256 KB verwendet. Wie den Beispielen zu entnehmen ist, zeigt die durchschnittliche Größe doppelter Speicherbereiche von 256 KB eine größere geschätzte Größe für die aktive Protokolldatei an. Um betriebsbezogene Probleme für den Server auf ein Mindestmaß reduzieren oder zu verhindern, verwenden Sie 256 KB für die Schätzung der Größe der aktiven Protokolldatei in Ihrer Produktionsumgebung.

Tabelle 1. Durchschnittliche Größe doppelter Speicherbereiche von 700 KB

Element	**Beispielwerte**		**Beschreibung**
Größe des größten zu deduplizierenden Objekts	800 GB	4 TB	Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.
Durchschnittliche Größe der Speicherbereiche	700 KB	700 KB	Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.
Speicherbereiche für eine bestimmte Datei	1.198.372 Bit	6.135.667 Bit	Bei Verwendung der durchschnittlichen Speicherbereichsgröße (700 KB), geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an. Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt: `(800 GB ÷ 700 KB) = 1.198.372 Bit` Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt: `(4 TB ÷ 700 KB) = 6.135.667 Bit`
Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist	1,7 GB	8,6 GB	Der geschätzte Speicherbereich für die aktive Protokolldatei, der für diese Transaktion benötigt wird.

Element	Beispielwerte		Beschreibung

Aktive Protokolldatei: vorgeschlagene Gesamtgröße	66 GB [1]	79,8 GB [1]	Multiplizieren Sie, nachdem zusätzlich zur Deduplizierung andere Aspekte der Last auf dem Server berücksichtigt wurden, die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			`(23,3 GB + 1,7 GB) x 2 = 50 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`50 + 16 = 66 GB`
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			`(23,3 GB + 8,6 GB) x 2 = 63,8 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`63,8 + 16 = 79,8 GB`

Archivprotokoll: vorgeschlagene Größe	198 GB [1]	239,4 GB [1]	Multiplizieren Sie die geschätzte Größe der aktiven Protokolldatei mit dem Faktor 3.
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			`50 GB x 3 = 150 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			`150 + 48 = 198 GB`
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			`63,8 GB x 3 = 191,4 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			`191,4 + 48 = 239,4 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Tabelle 2. Durchschnittliche Größe doppelter Speicherbereiche von 256 KB

Element	Beispielwerte		Beschreibung
Größe des größten zu deduplizierenden Objekts	800 GB	4 TB	Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.

Element	Beispielwerte		Beschreibung
Durchschnittliche Größe der Speicherbereiche	256 KB	256 KB	Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.

Speicherbereiche für eine bestimmte Datei	3.276.800 Bit	16.777.216 Bit	Bei Verwendung der durchschnittlichen Speicherbereichsgröße, geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`(800 GB ÷ 256 KB) = 3.276.800 Bit`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`(4 TB ÷ 256 KB) = 16.777.216 Bit`

Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist	4,5 GB	23,4 GB	Die geschätzte Größe des Speicherbereichs für die aktive Protokolldatei, die für diese Transaktion erforderlich ist.

Aktive Protokolldatei: vorgeschlagene Gesamtgröße	71,6 GB [1]	109,4 GB [1]	Nachdem Sie neben der Deduplizierung andere Aspekte der Serverauslastung mit berücksichtigt haben, multiplizieren Sie die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`(23,3 GB + 4,5 GB) x 2 = 55,6 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`55,6 + 16 = 71,6 GB`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`(23,3 GB + 23,4 GB) x 2 = 93,4 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`93,4 + 16 = 109,4 GB`

Element	Beispielwerte		Beschreibung

Archivprotokoll: vorgeschlagene Größe	214,8 GB [1]	328,2 GB [1]	Die geschätzte Größe der aktiven Protokolldatei multipliziert mit dem Faktor 3.
			
			Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`55,6 GB x 3 = 166,8 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`166,8 + 48 = 214,8 GB`
			
			Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt:
			
			`93,4 GB x 3 = 280,2 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`280,2 + 48 = 328,2 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen. Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.			

AIX: Speicherbereich des Spiegels für aktive Protokolldateien

Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.

Die Erstellung einer Protokollspiegel ist eine vorgeschlagene Option. Wenn Sie die aktive Protokolldatei vergrößern, wird der Protokollspiegel automatisch vergrößert. Die Spiegelung des Protokolls kann sich negativ auf die Leistung auswirken, da die doppelte E/A-Aktivität erforderlich ist, um den Spiegel zu verwalten. Der zusätzliche Speicherbereich, den der Protokollspiegel benötigt, ist ein weiterer Faktor, der bei der Entscheidung über die Erstellung eines Protokollspiegels berücksichtigt werden muss.

Wenn das Spiegelprotokollverzeichnis voll wird, gibt der Server Fehlernachrichten in das Aktivitätenprotokoll und in die Datei db2diag.log aus. Die Serveraktivität wird fortgesetzt.

AIX: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle

Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

Durch Angabe eines Übernahmeverzeichnisses für Archivprotokolle können Probleme verhindert werden, die auftreten, wenn der Speicherbereich der Archivprotokolldatei nicht mehr ausreicht. Wenn sowohl das Verzeichnis für Archivprotokolle als auch das Laufwerk oder das Dateisystem, in dem sich das Übernahmeverzeichnis für Archivprotokolle befindet, voll wird, bleiben die Daten im Verzeichnis für aktive Protokolldateien. Dadurch kann die aktive Protokolldatei vollständig ausgefüllt werden, was einen Serverhalt verursacht.

AIX: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen

Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.

Aktive Protokolldatei

Wenn der verfügbare Speicherbereich für die aktive Protokolldatei zu gering ist, werden die folgenden Nachrichten im Aktivitätenprotokoll angezeigt:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER

Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Der IBM Spectrum Protect-Server startet eine Datenbankgesamtsicherung.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dsmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Sie müssen die Datenbank manuell sichern.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dsmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Wenn mindestens eine einzige Datenbankgesamtsicherung ausgeführt wurde, startet der IBM Spectrum Protect-Server eine Teilsicherung der Datenbank. Andernfalls startet der Server eine Datenbankgesamtsicherung.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Sie müssen die Datenbank manuell sichern.

Archivprotokoll

Wenn der verfügbare Speicherbereich für das Archivprotokoll zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
Das Verhältnis des belegten Speicherbereichs für das Archivprotokoll zum verfügbaren Speicherbereich für das Archivprotokoll überschreitet den Schwellenwert für die Protokollauslastung. Der IBM Spectrum Protect-Server startet eine automatische Datenbankgesamtsicherung.

Datenbank

Wenn der verfügbare Speicherbereich für Datenbankaktivitäten zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
Der belegte Speicherplatz in der Datenbank überschreitet den Schwellenwert für die Belegung des Speicherplatzes in der Datenbank. Um den Speicherplatz für die Datenbank zu vergrößern, verwenden Sie den Befehl EXTEND DBSPACE oder das Dienstprogramm DSMSERV FORMAT mit dem Parameter DBDIR.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB
Der verfügbare Speicherbereich in dem Verzeichnis, in dem sich die Serverdatenbankdateien befinden, beträgt weniger als 1 GB.

Wenn ein IBM Spectrum Protect-Server mit dem Dienstprogramm DSMSERV FORMAT oder dem Konfigurationsassistenten erstellt wird, werden auch eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien erstellt, in denen Datenbankinformationen gespeichert werden sollen, die vom Datenbankmanager verwendet werden. Der in dieser Nachricht angegebene Pfad gibt die Speicherposition der Datenbankinformationen an, die vom Datenbankmanager verwendet werden. Ist in dem Pfad kein Speicherbereich verfügbar, ist der Server nicht mehr funktionsfähig.

Sie müssen dem Dateisystem Speicherbereich hinzufügen oder in dem Dateisystem oder auf der Platte Speicherbereich freigeben.

AIX: Rollbackdateien der Installation löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

Informationen zu diesem Vorgang

Zum Löschen der nicht mehr benötigten Dateien verwenden Sie den grafisch orientierten Installationsassistenten oder die Befehlszeile im Konsolenmodus.

- AIX: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen
  Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.
- AIX: Rollbackdateien für die Installation mit der Befehlszeile löschen
  Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

AIX: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.

Vorgehensweise

1. Öffnen Sie IBM Installation Manager.
   AIX-BetriebssystemeIn dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus, um IBM Installation Manager zu starten:

   ```
   ./IBMIM
   ```

2. Klicken Sie auf Datei > Benutzervorgaben.
3. Wählen Sie Dateien für Rollback aus.
4. Klicken Sie auf Gespeicherte Dateien löschen und dann auf OK.

AIX: Rollbackdateien für die Installation mit der Befehlszeile löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

Vorgehensweise

1. In dem Verzeichnis, in dem IBM® Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
   - AIX-Betriebssystemeeclipse/tools

   Beispiel:

   - AIX-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Geben Sie im Verzeichnis tools den folgenden Befehl aus, um eine IBM Installation Manager-Befehlszeile zu starten:
   - AIX-Betriebssysteme`./imcl -c`
3. Geben Sie `P` ein, um Benutzervorgaben auszuwählen.
4. Geben Sie `3` ein, um Dateien für Rollback auszuwählen.
5. Geben Sie `D` ein, um die Dateien für Rollback zu löschen.
6. Geben Sie `A` ein, um die Änderungen anzuwenden und zum Benutzervorgabenmenü zurückzukehren.
7. Geben Sie `C` ein, um das Benutzervorgabenmenü zu verlassen.
8. Geben Sie `X` ein, um Installation Manager zu beenden.

AIX: Empfehlungen für die Serverbenennung

Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.

Instanzbenutzer-ID

Die Instanzbenutzer-ID wird als Basis für andere Namen verwendet, die sich auf die Serverinstanz beziehen. Die Instanzbenutzer-ID wird auch als Instanzeigner bezeichnet.

Zum Beispiel: tsminst1

Die Instanzbenutzer-ID ist die Benutzer-ID, die über das Eigentumsrecht oder über Schreib-/Lesezugriffsberechtigung für alle Verzeichnisse verfügen muss, die Sie für die Datenbank und das Wiederherstellungsprotokoll erstellen. Der Server wird standardmäßig mit der Instanzbenutzer-ID ausgeführt. Diese Benutzer-ID benötigt außerdem Schreib-/Lesezugriff für die Verzeichnisse, die für die Einheitenklasse FILE verwendet werden.

AIX-Betriebssysteme

Ausgangsverzeichnis für die Instanzbenutzer-ID

Das Ausgangsverzeichnis kann während der Erstellung der Instanzbenutzer-ID erstellt werden. Hierfür wird die Option für die Erstellung eines Ausgangsverzeichnisses (-m) verwendet, falls es noch nicht vorhanden ist. Abhängig von den lokalen Einstellungen kann das Verzeichnis folgendes Format haben: /home/*Instanzbenutzer-ID*

Zum Beispiel: /home/tsminst1

Das Ausgangsverzeichnis dient hauptsächlich zur Aufbewahrung des Profils für die Benutzer-ID und für Sicherheitseinstellungen.

AIX-Betriebssysteme

Datenbankinstanzname

Der Datenbankinstanzname muss mit der Instanzbenutzer-ID identisch sein, mit der Sie die Serverinstanz ausführen.

Zum Beispiel: tsminst1

 AIX-Betriebssysteme

Instanzverzeichnis

Das Instanzverzeichnis enthält spezielle Dateien für eine Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). Es kann einen beliebigen Name haben. Um die Identifizierung zu erleichtern, sollten Sie einen Namen verwenden, der das Verzeichnis mit dem Instanznamen verknüpft.

Sie können das Instanzverzeichnis als Unterverzeichnis des Ausgangsverzeichnisses für die Instanzbenutzer-ID erstellen. Zum Beispiel: /home/*Instanzbenutzer-ID*/*Instanzbenutzer-ID*

Im folgenden Beispiel befindet sich das Instanzverzeichnis im Ausgangsverzeichnis der Benutzer-ID tsminst1: /home/tsminst1/tsminst1

Sie können das Verzeichnis auch an einer anderen Position erstellen, zum Beispiel: /tsmserver/tsminst1

Im Instanzverzeichnis sind folgende Dateien für die Serverinstanz gespeichert:

- Serveroptionsdatei dsmserv.opt
- Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
- Einheitenkonfigurationsdatei, wenn die Serveroption DEVCONFIG keinen vollständig qualifizierten Namen angibt
- Protokolldatei für Datenträger, wenn die Serveroption VOLUMEHISTORY keinen vollständig qualifizierten Namen angibt
- Datenträger für Speicherpools mit dem Typ DEVTYPE=FILE, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
- Benutzerexits
- Traceausgabe (wenn nicht vollständig qualifiziert)

Datenbankname

Der Datenbankname lautet für jede Serverinstanz immer TSMDB1. Dieser Name kann nicht geändert werden.

Servername

Der Servername ist ein interner Name für IBM Spectrum Protect und wird für Operationen verwendet, bei denen eine Datenübertragung zwischen mehreren IBM Spectrum Protect-Servern auftritt. Zum Beispiel bei der Kommunikation zwischen Servern und bei der gemeinsamen Nutzung von Speicherarchiven.

 AIX-BetriebssystemeDer Servername wird auch verwendet, wenn Sie den Server dem Operations Center hinzufügen, so dass er mit dieser Schnittstelle verwaltet werden kann. Verwenden Sie einen eindeutigen Namen für jeden Server. Verwenden Sie einen Namen, der die Position oder den Zweck des Servers angibt, um die Identifikation im Operations Center (oder mit einem Befehl QUERY SERVER) zu erleichtern. Nachdem ein IBM Spectrum Protect-Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.

Wenn Sie den Assistenten verwenden, wird als Standardname der Hostname des von Ihnen verwendeten Systems vorgeschlagen. Sie können einen anderen, für Ihre Umgebung aussagekräftigen Namen verwenden. Befinden sich mehrere Server auf dem System, können Sie bei Verwendung des Assistenten den Standardnamen nur für einen der Server angeben. Sie müssen einen eindeutigen Namen für jeden Server eingeben.

 AIX-BetriebssystemeZum Beispiel:

- `LOHNBUCHHALTUNG`
- `VERTRIEB`

Verzeichnisse für Datenbankbereich und Wiederherstellungsprotokoll

Die Verzeichnisse können gemäß den lokalen Vorgaben benannt werden. Sie sollten Namen verwenden, die die Verzeichnisse mit der Serverinstanz verknüpfen, um die Identifikation zu erleichtern.

Beispiel für das Archivprotokoll:

-  AIX-Betriebssysteme/tsminst1_archlog

AIX: Installationsverzeichnisse

Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

Das Verzeichnis /opt/tivoli/tsm/server/bin ist das Standardverzeichnis, das den Servercode und die Lizenzierung enthält.

Das während der Installation des IBM Spectrum Protect-Servers installierte DB2-Produkt hat die in den DB2-Informationsquellen dokumentierte Verzeichnisstruktur. Schützen Sie diese Verzeichnisse und Dateien wie die Serververzeichnisse. Das Standardverzeichnis heißt /opt/tivoli/tsm/db2.

Sie können folgende Sprachen verwenden: Englisch (US), Deutsch, Französisch, Italienisch, Spanisch, Portugiesisch (Brasilien), Koreanisch, Japanisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Chinesisch GBK, Chinesisch Big5 und Russisch.

AIX: Serverkomponenten installieren

Für die Installation der Serverkomponenten der Version 8.1.2 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.

Informationen zu diesem Vorgang

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server
  Tipp: Die Datenbank (DB2), Global Security Kit (GSKit) und IBM® Java™ Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.
- Sprachen des Servers
- Lizenz
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

 AIX-BetriebssystemeFür die Installation eines Servers der Version 8.1.2 anhand dieses Leitfadens müssen Sie 30 - 45 Minuten einplanen.

- AIX: Installationspaket abrufen
  Das Installationspaket für IBM Spectrum Protect kann von einer IBM Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.
- AIX: IBM Spectrum Protect mit dem Installationsassistenten installieren
  Sie können den Server mit dem grafisch orientierten Assistenten von IBM Installation Manager installieren.
- AIX: IBM Spectrum Protect im Konsolenmodus installieren
  Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.
- AIX: IBM Spectrum Protect im unbeaufsichtigten Modus installieren
  Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.
- AIX: Serversprachenpakete installieren
  Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

AIX: Installationspaket abrufen

Das Installationspaket für IBM Spectrum Protect kann von einer IBM® Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.

 AIX-Betriebssysteme

Vorbereitende Schritte

Wenn Sie die Dateien herunterladen wollen, legen Sie als Systembenutzergrenzwert für die maximale Dateigröße 'unlimited' (unbegrenzt) fest, um sicherzustellen, dass die Dateien ordnungsgemäß heruntergeladen werden können:

1. Geben Sie den folgenden Befehl aus, um den Wert für die maximale Dateigröße abzufragen:

   ```
   ulimit -Hf
   ```

2. Wenn als Systembenutzergrenzwert für die maximale Dateigröße nicht 'unlimited' (unbegrenzt) angegeben ist, geben Sie 'unlimited' gemäß den Anweisungen in der Dokumentation Ihres Betriebssystems an.

Vorgehensweise

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:
   - Laden Sie das Serverpaket aus Passport Advantage oder Fix Central herunter.

- Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.

2. Gehen Sie wie folgt vor, wenn Sie das Paket von einer IBM Download-Site heruntergeladen haben:
   AIX-Betriebssysteme
   a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherplatzbedarf finden Sie im Downloaddokument:
      - IBM Spectrum Protect Technote 4042944
      - IBM Spectrum Protect Extended Edition Technote 4042945
      - IBM Spectrum Protect for Data Retention Technote 4042946

   b. Laden Sie die Paketdatei in ein beliebiges Verzeichnis herunter. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.
   c. Stellen Sie sicher, dass die Berechtigung zur Ausführung für das Paket definiert ist. Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

      ```
      chmod a+x Paketname.bin
      ```

   d. Geben Sie den folgenden Befehl aus, um das Paket zu extrahieren:

      ```
      ./Paketname.bin
      ```

      Paketname ist der Name der heruntergeladenen Datei. Zum Beispiel:

      AIX-Betriebssysteme

      ```
      8.1.x.000-IBM-SPSRV-AIX.bin
      ```

3. AIX-BetriebssystemeStellen Sie sicher, dass der folgende Befehl aktiviert ist, damit die IBM Spectrum Protect-Assistenten ordnungsgemäß funktionieren:
   - AIX-Betriebssysteme`lsuser`

   Der Befehl ist standardmäßig aktiviert.
4. Wählen Sie eine der folgenden Methoden für die Installation von IBM Spectrum Protect aus:
   - AIX: IBM Spectrum Protect mit dem Installationsassistenten installieren
   - AIX: IBM Spectrum Protect im Konsolenmodus installieren
   - AIX: IBM Spectrum Protect im unbeaufsichtigten Modus installieren
5. Nachdem Sie IBM Spectrum Protect installiert haben und bevor Sie IBM Spectrum Protect für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Support and downloads und legen Sie alle gültigen Fixes an.

AIX: IBM Spectrum Protect mit dem Installationsassistenten installieren

Sie können den Server mit dem grafisch orientierten Assistenten von IBM® Installation Manager installieren.

Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

- AIX-BetriebssystemeWenn die folgenden RPM-Dateien in Ihrem System nicht installiert sind, müssen Sie sie installieren. Anweisungen finden Sie in RPM-Dateien für den grafisch orientierten Assistenten installieren.
  - atk-1.12.3-2.aix5.2.ppc.rpm
  - cairo-1.8.8-1.aix5.2.ppc.rpm
  - expat-2.0.1-1.aix5.2.ppc.rpm
  - fontconfig-2.4.2-1.aix5.2.ppc.rpm
  - freetype2-2.3.9-1.aix5.2.ppc.rpm
  - gettext-0.10.40-6.aix5.1.ppc.rpm
  - glib2-2.12.4-2.aix5.2.ppc.rpm
  - gtk2-2.10.6-4.aix5.2.ppc.rpm
  - libjpeg-6b-6.aix5.1.ppc.rpm
  - libpng-1.2.32-2.aix5.2.ppc.rpm
  - libtiff-3.8.2-1.aix5.2.ppc.rpm
  - pango-1.14.5-4.aix5.2.ppc.rpm
  - pixman-0.12.0-3.aix5.2.ppc.rpm
  - xcursor-1.1.7-3.aix5.2.ppc.rpm
  - xft-2.1.6-5.aix5.1.ppc.rpm
  - xrender-0.9.1-3.aix5.2.ppc.rpm
  - zlib-1.2.3-3.aix5.1.ppc.rpm
- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.

Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

Option	Bezeichnung
Installation der Software mithilfe eines heruntergeladenen Pakets:	a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben. b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten zu starten: AIX-Betriebssysteme `./install.sh`

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis logs gespeichert werden.

  Installationsprotokolldateien können Sie anzeigen, indem Sie in Installation Manager auf Datei > Protokoll anzeigen klicken. Um diese Protokolldateien zu erfassen, klicken Sie in Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
- AIX-BetriebssystemeNachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.
- AIX-BetriebssystemeAIX: Vorausgesetzte RPM-Dateien für den grafisch orientierten Assistenten installieren
  Bevor Sie IBM Spectrum Protect mithilfe des grafisch orientierten Assistenten von IBM Installation Manager installieren können, müssen Sie sicherstellen, dass die erforderlichen RPM-Dateien installiert sind.

AIX: IBM Spectrum Protect im Konsolenmodus installieren

Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.

Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.

Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

Option	Bezeichnung
Installation der Software mithilfe eines heruntergeladenen Pakets:	a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben. b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten im Konsolenmodus zu starten: AIX-Betriebssysteme `./install.sh -c` Optional : Generieren Sie während einer Installation im Konsolenmodus eine Antwortdatei. Geben Sie die Optionen für die Installation im Konsolenmodus und in der Anzeige Zusammenfassung `G` an, um die Antworten zu generieren.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  - AIX-Betriebssysteme/var/ibm/InstallationManager/logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
- AIX-BetriebssystemeNachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

AIX: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.

Vorbereitende Schritte

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis input zur Verfügung, in dem das Installationspaket extrahiert wird:

install_response_sample.xml
: Verwenden Sie diese Datei für die Installation der IBM Spectrum Protect-Komponenten.

update_response_sample.xml
: Verwenden Sie diese Datei für das Upgrade der IBM Spectrum Protect-Komponenten.

Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Erstellen Sie eine Antwortdatei. Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.
2. Wenn Sie den Server und das Operations Center im unbeaufsichtigten Modus installieren, erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.
   Wenn Sie die Datei install_response_sample.xml verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist *mein_Kennwort* das Kennwort:

   ```
   <variable name='ssl.password' value='mein_Kennwort' />
   ```

   Weitere Informationen zu diesem Kennwort finden Sie in Prüfliste für die Installation.
   Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei update_response_sample.xml aktualisieren.
3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.
   - AIX-Betriebssysteme

     ```
     ./install.sh -s -input Antwortdatei -acceptLicense
     ```

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  - AIX-Betriebssysteme/var/ibm/InstallationManager/logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
- AIX-BetriebssystemeNachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

AIX-Betriebssysteme

AIX: Serversprachenpakete installieren

Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

Vorbereitende Schritte

Anweisungen zur Installation von von Sprachenpaketen für Speicheragenten finden Sie unter Language pack configuration for Storage Agent.

- AIX: Spracheinstellungen für den Server
  Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.
- AIX: Sprachenpaket konfigurieren
  Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.
- AIX: Sprachenpaket aktualisieren
  Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

AIX: Spracheinstellungen für den Server

Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.

AIX-BetriebssystemeDieses Sprachenpaket wird automatisch für die folgende Standardsprachenoption für IBM Spectrum Protect-Servernachrichten und -Hilfetext installiert:

- AIX-BetriebssystemeLANGUAGE en_US

Für vom Standard abweichende Sprachen oder Ländereinstellungen installieren Sie das für Ihre Installation erforderliche Sprachenpaket. Sie können die aufgeführten Sprachen verwenden:
AIX-Betriebssysteme

Tabelle 1. Serversprachen für AIX

Sprache	Wert der Option LANGUAGE
Chinesisch, vereinfacht	zh_CN
Chinesisch, vereinfacht (UTF-8)	ZH_CN
Chinesisch, traditionell (Big5)	Zh_TW
Chinesisch, traditionell (UTF-8)	ZH_TW
Chinesisch, traditionell (euc_tw)	zh_TW
Englisch	en_US
Englisch (UTF-8)	EN_US
Französisch	fr_FR
Französisch (UTF-8)	FR_FR
Deutsch	de_DE
Deutsch (UTF-8)	DE_DE
Italienisch	it_IT
Italienisch (UTF-8)	IT_IT
Japanisch, EUC	ja_JP
Japanisch, PC	Ja_JP
Japanisch, UTF8	JA_JP
Koreanisch	ko_KR
Koreanisch (UTF-8)	KO_KR
Portugiesisch, Brasilianisches	pt_BR
Portugiesisch, Brasilianisches (UTF-8)	PT_BR
Russisch	ru_RU
Russisch (UTF-8)	RU_RU
Spanisch	es_ES
Spanisch (UTF-8)	ES_ES

AIX-BetriebssystemeEinschränkung: Bei Verwendung des Operations Center werden einige Zeichen möglicherweise nicht ordnungsgemäß angezeigt, wenn der Web-Browsers und der Server nicht dieselbe Sprache verwenden. Wenn dieses Problem auftritt, geben Sie im Browser dieselbe Sprache wie im Server an.

AIX: Sprachenpaket konfigurieren

Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.

Informationen zu diesem Vorgang

AIX-BetriebssystemeFühren Sie eine der folgenden Tasks aus, um die Unterstützung für eine bestimmte Ländereinstellung zu aktivieren:

- Geben Sie in der Option LANGUAGE in der Serveroptionsdatei den Namen der Ländereinstellung an, die verwendet werden soll. Beispiel:
  - AIX-BetriebssystemeSoll die Ländereinstellung `it_IT` verwendet werden, setzen Sie die Option LANGUAGE auf `it_IT`. Siehe AIX: Spracheinstellungen für den Server.
- AIX-BetriebssystemeWenn Sie den Server im Vordergrund starten, definieren Sie die Umgebungsvariable `LC_ALL` gemäß dem in der Serveroptionsdatei definierten Wert. Soll beispielsweise die Umgebungsvariable für Italienisch definiert werden, geben Sie folgenden Wert ein:

  ```
  export LC_ALL=it_IT
  ```

Wenn die Ländereinstellung erfolgreich initialisiert wird, steuert sie die Datums-, Uhrzeit- und Zahlenformatierung für den Server. Wenn die Ländereinstellung nicht erfolgreich initialisiert wird, verwendet der Server die englischen (US) Nachrichtendateien und das Datums-, Uhrzeit- und Zahlenformat der englischen (US) Ländereinstellung.

AIX: Sprachenpaket aktualisieren

Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

Informationen zu diesem Vorgang

Sie können ein anderes Sprachenpaket in derselben IBM Spectrum Protect-Instanz installieren.

- Verwenden Sie die Funktion Ändern von IBM Installation Manager, um ein anderes Sprachenpaket zu installieren.
- Verwenden Sie die Funktion Aktualisieren von IBM Installation Manager, um eine Aktualisierung auf neuere Versionen der Sprachenpakete durchzuführen.

Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.

AIX: Die ersten Schritte nach der Installation von IBM Spectrum Protect

Nach der Installation von Version 8.1.2 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.

Informationen zu diesem Vorgang

1. Erstellen Sie die Verzeichnisse und die Benutzer-ID für die Serverinstanz. Siehe AIX: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen.
2. Konfigurieren Sie eine Serverinstanz. Wählen Sie eine der folgenden Optionen aus:
   - Verwenden Sie den Konfigurationsassistenten (die bevorzugte Methode). Siehe AIX: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren.
   - Konfigurieren Sie die neue Instanz manuell. Siehe AIX: Serverinstanz manuell konfigurieren. Führen Sie während einer manuellen Konfiguration die folgenden Schritte aus:
     a. Definieren Sie Ihre Verzeichnisse und erstellen Sie die IBM Spectrum Protect-Instanz. Siehe AIX: Serverinstanz erstellen.
     b. Erstellen Sie eine neue Serveroptionsdatei, indem Sie die Musterdatei kopieren, um die Datenübertragung zwischen dem Server und den Clients zu definieren. Siehe AIX-BetriebssystemeAIX: Server- und Clientübertragung konfigurieren.
     c. Geben Sie den Befehl DSMSERV FORMAT aus, um die Datenbank zu formatieren. Siehe AIX: Datenbank und Protokoll formatieren.
     d. Konfigurieren Sie Ihr System für die Datenbanksicherung. Siehe AIX: Datenbankmanager für die Datenbanksicherung vorbereiten.
3. Konfigurieren Sie Optionen, die die Ausführung der Datenbankreorganisation steuern. Siehe AIX: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren.
4. Starten Sie die Serverinstanz, falls noch nicht gestartet.
   - AIX-BetriebssystemeSiehe AIX: Serverinstanz starten.
5. Registrieren Sie Ihre Lizenz. Siehe AIX: Lizenzregistrierung.
6. Bereiten Sie Ihr System auf Datenbanksicherungen vor. Siehe AIX: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben.
7. Überwachen Sie den Server. Siehe AIX: Server überwachen.

- AIX: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen
  Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.
- AIX: IBM Spectrum Protect-Server konfigurieren
  Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.
- AIX: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren
  Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.
- AIX-BetriebssystemeAIX: Serverinstanz starten
  Sie können den Server mit der Instanzbenutzer-ID (bevorzugte Methode) oder mit der Rootbenutzer-ID starten.
- AIX: Server stoppen
  Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.
- AIX: Lizenzregistrierung
  Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.
- AIX: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben
  Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen

vorzubereiten.

- AIX: Mehrere Serverinstanzen auf einem System ausführen
  Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.
- AIX: Server überwachen
  Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

AIX: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen

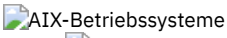
Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.

Vorbereitende Schritte

Lesen Sie die Informationen zur Planung des Speicherbereichs für den Server, bevor Sie diese Task ausführen. Siehe AIX: Arbeitsblätter für Planungsdetails für den Server.

Vorgehensweise

1. Erstellen Sie die Benutzer-ID, die Eigner der Serverinstanz sein soll. Diese Benutzer-ID verwenden Sie später bei der Erstellung der Serverinstanz.

   
   AIX-Betriebssysteme

   AIX-BetriebssystemeErstellen Sie eine Benutzer-ID und eine Gruppe, die Eigner der Serverinstanz sein sollen.

   a. Die folgenden Befehle können mit einer Verwaltungsbenutzer-ID ausgeführt werden, die den Benutzer und die Gruppe definieren soll. Erstellen Sie die Benutzer-ID und Gruppe im Ausgangsverzeichnis des Benutzers.
   Einschränkung: In der Benutzer-ID dürfen nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstreichungszeichen (_) verwendet werden. Die Benutzer-ID und der Gruppenname müssen die folgenden Regeln einhalten:
      - Die maximale Länge beträgt 8 Zeichen.
      - Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder mit einer Ziffer beginnen.
      - Als Benutzer-ID und Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* und kein reserviertes SQL-Wort verwendet werden.

      Erstellen Sie beispielsweise die Benutzer-ID `tsminst1` in der Gruppe `tsmsrvrs`. Die folgenden Beispiele zeigen, wie diese Benutzer-ID und diese Gruppe mit Betriebssystembefehlen erstellt werden.

      
      AIX-Betriebssysteme

      ```
      mkgroup id=1001 tsmsrvrs
      mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
      passwd tsminst1
      ```

      Einschränkung: DB2 unterstützt nicht die direkte Authentifizierung von Betriebssystembenutzern durch LDAP.

   b. Melden Sie sich ab und dann bei Ihrem System an. Wechseln Sie zu dem gerade erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, z. B. Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es ggf. ändern können.

2. Erstellen Sie die vom Server benötigten Verzeichnisse.
   
   AIX-BetriebssystemeErstellen Sie leere Verzeichnisse für jeden Tabelleneintrag und stellen Sie sicher, dass die neue Benutzer-ID, die Sie gerade erstellt haben, Eigner der Verzeichnisse ist. Hängen Sie den zugeordneten Speicher in jedem der Verzeichnisse für aktive Protokolldateien, für Archivprotokolle und Datenbanken an.

Element	Beispielbefehle für die Verzeichniserstellung	Ihre Verzeichnisse
Das *Instanzverzeichnis* für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien).	`mkdir /tsminst1`	

Die Datenbankverzeichnisse	`mkdir /tsmdb001`
	`mkdir /tsmdb002`
	`mkdir /tsmdb003`
	`mkdir /tsmdb004`	

Verzeichnis für aktive Protokolldateien	`mkdir /tsmlog`	
Verzeichnis für Archivprotokolle	`mkdir /tsmarchlog`	
Optional: Verzeichnis für den Protokollspiegel für die aktive Protokolldatei	`mkdir /tsmlogmirror`	

Element	Beispielbefehle für die Verzeichniserstellung	Ihre Verzeichnisse
Optional: Sekundäres Verzeichnis für Archivprotokolle (Übernahmeverzeichnis für Archivprotokolle)	`mkdir /tsmarchlogfailover`	

Wenn ein Server anfänglich mit dem Dienstprogramm DSMSERV FORMAT oder mit dem Konfigurationsassistenten erstellt wird, werden eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien zum Speichern von Datenbankinformationen erstellt, die vom Datenbankmanager verwendet werden.

3. Melden Sie die neue Benutzer-ID ab.

AIX: IBM Spectrum Protect-Server konfigurieren

Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.

Informationen zu diesem Vorgang

Wählen Sie eine der folgenden Optionen aus, um eine IBM Spectrum Protect-Serverinstanz zu konfigurieren:

- AIX: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren
  Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.
- AIX: Serverinstanz manuell konfigurieren
  Nach der Installation von IBM Spectrum Protect Version 8.1.2 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

AIX: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren

Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.

Vorbereitende Schritte

Bevor Sie den Konfigurationsassistenten starten, müssen Sie alle vorhergehenden Schritte zur Vorbereitung der Konfiguration ausführen. Zu diesen Schritten gehören die Installation von IBM Spectrum Protect, die Erstellung der Datenbank- und Protokollverzeichnisse und die Erstellung der Verzeichnisse und der Benutzer-ID für die Serverinstanz.

Vorgehensweise

1. Stellen Sie sicher, dass folgende Anforderungen erfüllt sind:  AIX-Betriebssysteme
   - Das System, auf dem Sie IBM Spectrum Protect installiert haben, muss über den X Window System-Client verfügen. Außerdem müssen Sie einen X Window System-Server auf Ihrem Desktop ausführen.
   - Im System muss das SSH-Protokoll (Secure Shell) aktiviert sein. Stellen Sie sicher, dass für den Port der Standardwert 22 definiert ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei `sshd_config` im Verzeichnis /etc/ssh/ aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämonservice über Zugriffsberechtigungen zum Herstellen einer Verbindung zum System mithilfe des Werts `localhost` verfügt.
   - Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt haben, mit dem SSH-Protokoll bei IBM Spectrum Protect anmelden können. Bei Verwendung des Assistenten müssen Sie diese Benutzer-ID und dieses Kennwort für den Zugriff auf dieses System angeben.
   - Starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.
2. Starten Sie die lokale Version des Assistenten:
   -  AIX-BetriebssystemeÖffnen Sie das Programm `dsmicfgx` im Verzeichnis /opt/tivoli/tsm/server/bin. Dieser Assistent kann nur als Root ausgeführt werden.

Befolgen Sie die Anweisungen zur Ausführung der Konfiguration. Der Assistent kann gestoppt und erneut gestartet werden. Der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

AIX: Serverinstanz manuell konfigurieren

Nach der Installation von IBM Spectrum Protect Version 8.1.2 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

- AIX: Serverinstanz erstellen
  Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl db2icrt.
- AIX-BetriebssystemeAIX: Server- und Clientübertragung konfigurieren
  Eine standardmäßige Beispielserveroptionsdatei mit dem Namen dsmserv.opt.smp wird während der IBM Spectrum Protect-Installation im Verzeichnis /opt/tivoli/tsm/server/bin erstellt. Sie müssen die Datenübertragung zwischen dem Server und den Clients definieren, indem Sie eine neue Serveroptionsdatei erstellen. Hierfür kopieren Sie die Musterdatei in das Verzeichnis für die Serverinstanz.
- AIX: Datenbank und Protokoll formatieren
  Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.
- AIX: Datenbankmanager für die Datenbanksicherung vorbereiten
  Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

AIX: Serverinstanz erstellen

Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl db2icrt.

Informationen zu diesem Vorgang

Auf einer Workstation kann mindestens eine Serverinstanz vorhanden sein.
AIX-BetriebssystemeWichtig: Stellen Sie Folgendes sicher, bevor der Befehl db2icrt ausgeführt wird:

- Das Ausgangsverzeichnis für den Benutzer (/home/tsminst1) ist vorhanden. Ist kein Ausgangsverzeichnis vorhanden, müssen Sie es erstellen.
  Im Instanzverzeichnis sind folgende Kerndateien gespeichert, die vom IBM Spectrum Protect-Server generiert werden:
  - Serveroptionsdatei dsmserv.opt
  - Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
  - Einheitenkonfigurationsdatei, wenn die Serveroption DEVCONFIG keinen vollständig qualifizierten Namen angibt
  - Protokolldatei für Datenträger, wenn die Serveroption VOLUMEHISTORY keinen vollständig qualifizierten Namen angibt
  - Datenträger für Speicherpools mit dem Typ DEVTYPE=FILE, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
  - Benutzerexits
  - Traceausgabe (wenn nicht vollständig qualifiziert)
- Eine Shellkonfigurationsdatei (z. B. .profile) ist im Ausgangsverzeichnis vorhanden. Die Rootbenutzer- und Instanzbenutzer-ID müssen über Schreibberechtigung für diese Datei verfügen. Weitere Informationen finden Sie in Produktinformation zu DB2. Suchen Sie dort nach den Einstellungen für Linux- und UNIX-Umgebungsvariablen.

AIX-Betriebssysteme

1. Melden Sie sich mit der Root-ID an und erstellen Sie eine IBM Spectrum Protect-Instanz. Der Name der Instanz muss mit dem Namen des Benutzers identisch sein, der Eigner der Instanz ist. Verwenden Sie den Befehl db2icrt und geben Sie den Befehl in eine Zeile ein:
   AIX-Betriebssysteme

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   Instanzname Instanzname
   ```

   Lautet Ihre Benutzer-ID für diese Instanz z. B. tsminst1, verwenden Sie den folgenden Befehl, um die Instanz zu erstellen. Geben Sie den Befehl in eine einzelne Zeile ein. AIX-Betriebssysteme

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   tsminst1 tsminst1
   ```

   Hinweis: Verwenden Sie ab diesem Punkt diese neue Benutzer-ID für die Konfiguration Ihres IBM Spectrum Protect-Servers. Melden Sie sich mit der Root-ID ab und mit der neuen Instanzbenutzer-ID an.
2. Geben Sie als Standardverzeichnis für die Datenbank das Instanzverzeichnis für den Server an. Sind mehrere Server vorhanden, melden Sie sich mit der Instanz-ID des jeweiligen Servers an. Geben Sie den folgenden Befehl aus:

   ```
   db2 update dbm cfg using dftdbpath Instanzverzeichnis
   ```

   Lautet das Instanzverzeichnis für den Server z. B. 'tsminst1', ändern Sie mit dem folgenden Befehl das Standardverzeichnis für die Datenbank in 'tsminst1':

   ```
   db2 update dbm cfg using dftdbpath /tsminst1
   ```

3. Ändern Sie den Bibliothekspfad, so dass die Version von IBM Global Security Kit (GSKit) verwendet wird, die mit dem Server installiert wird. In den folgenden Beispielen ist *server_bin_directory* ein Unterverzeichnis des Serverinstallationsverzeichnisses. Zum Beispiel /opt/tivoli/tsm/server/bin.
   - AIX-BetriebssystemeGeben Sie den folgenden Befehl in einer Zeile ein:

     ```
     export LIBPATH=server_bin_directory/dbbkapi:
     /usr/opt/ibm/gsk8_64/lib64:$LIBPATH
     ```

- Sie müssen die folgenden Dateien aktualisieren, um den Bibliothekspfad zu definieren, wenn DB2 oder der Server gestartet wird:

  Bash- oder Korn-Shell-Beispiel:

  ```
  Instanzbenutzer-Ausgangsverzeichnis/sqllib/userprofile
  ```

  C-Shell-Beispiel:

  ```
  Instanzbenutzer-Ausgangsverzeichnis/sqllib/usercshrc
  ```

- Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis*/sqllib/userprofile (Bash- oder Korn-Shell) hinzu. Jeder Eintrag befindet sich in jeweils einer Zeile. 

  ```
  LIBPATH=server_bin_directory/dbbkapi:
  /usr/opt/ibm/gsk8_64/lib64:$LIBPATH
  export LIBPATH
  ```

  Hinweis: Der Bibliothekspfad muss folgende Einträge enthalten:
  - /usr/local/ibm/gsk8_64/lib64
  - /opt/ibm/lib
  - /opt/ibm/lib64
  - /usr/lib64
- Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis*/sqllib/usercshrc (C-Shell) in einer einzigen Zeile hinzu:

  ```
  setenv LIBPATH server_bin_directory/dbbkapi:
  /usr/opt/ibm/gsk8_64/lib64:$LIBPATH
  ```

- Überprüfen Sie die Bibliothekspfadeinstellungen und ob die GSKit-Version 8.0.14.43 oder höher ist. Geben Sie die folgenden Befehle aus:

  ```
  echo $LIBPATH
  gsk8capicmd_64 -version
  gsk8ver_64
  ```

  Ist die GSKit-Version nicht 8.0.14.43 oder höher, müssen Sie den IBM Spectrum Protect-Server erneut installieren. Die Neuinstallation stellt sicher, dass die richtige GSKit-Version verfügbar ist.

4. Erstellen Sie eine neue Serveroptionsdatei. Siehe AIX: Server- und Clientübertragung konfigurieren.

AIX: Server- und Clientübertragung konfigurieren

Eine standardmäßige Beispielserveroptionsdatei mit dem Namen dsmserv.opt.smp wird während der IBM Spectrum Protect-Installation im Verzeichnis /opt/tivoli/tsm/server/bin erstellt. Sie müssen die Datenübertragung zwischen dem Server und den Clients definieren, indem Sie eine neue Serveroptionsdatei erstellen. Hierfür kopieren Sie die Musterdatei in das Verzeichnis für die Serverinstanz.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass ein Serverinstanzverzeichnis, z. B. /tsminst1, vorhanden ist und kopieren Sie die Musterdatei in dieses Verzeichnis. Nennen Sie die neue Datei `dsmserv.opt` und editieren Sie die Optionen. Führen Sie diese Konfiguration vor der Initialisierung der Serverdatenbank aus. Jedes Beispiel bzw. jeder Standardeintrag in der Beispieloptionsdatei ist ein Kommentar in einer Zeile, die mit einem Stern (*) beginnt. Bei Optionen muss die Groß-/Kleinschreibung nicht beachtet werden, und zwischen Schlüsselwörtern und Werten dürfen sich ein oder mehrere Leerzeichen befinden.

Für das Editieren der Optionsdatei gelten folgende Richtlinien:

- Entfernen Sie den Stern am Anfang der Zeile, um eine Option zu aktivieren.
- Beginnen Sie mit der Eingabe der Optionen in einer beliebigen Spalte.
- Geben Sie nur eine Option pro Zeile ein. Die Option muss auf einer Zeile stehen.
- Werden mehrere Einträge für ein Schlüsselwort vorgenommen, verwendet der IBM Spectrum Protect-Server den letzten Eintrag.

Wenn Sie die Serveroptionsdatei ändern, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

Sie können mindestens eine der folgenden Übertragungsmethoden angeben:

- TCP/IP Version 4 oder Version 6
- Shared Memory
- Secure Sockets Layer (SSL)
  Tipp: Sie können Kennwörter im LDAP-Verzeichnisserver oder im IBM Spectrum Protect-Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.

- AIX-BetriebssystemeAIX: TCP/IP-Optionen definieren
  Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.
- AIX-BetriebssystemeAIX: Shared Memory-Optionen definieren
  Sie können die Shared Memory-Übertragung zwischen Clients und Servern auf demselben System verwenden. Für die Verwendung von Shared Memory muss TCP/IP Version 4 auf dem System installiert sein.
- AIX-BetriebssystemeAIX: Secure Sockets Layer-Optionen definieren
  Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

AIX: TCP/IP-Optionen definieren

Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt eine Liste der TCP/IP-Optionen, mit denen Sie Ihr System definieren können.

```
commmethod        tcpip
  tcpport         1500
  tcpwindowsize   0
  tcpnodelay      yes
```

Tipp: Sie können TCP/IP Version 4 und/oder Version 6 verwenden.

TCPPORT
: Die Adresse des Server-Ports für TCP/IP- und SSL-Kommunikation. Der Standardwert ist 1500.

AIX-BetriebssystemeTCPWINDOWSIZE
: AIX-BetriebssystemeGibt die Größe des TCP/IP-Puffers an, der beim Senden oder Empfangen von Daten verwendet wird. Die in einer Sitzung verwendete Fenstergröße ist der kleinere Wert der Server- und Clientfenstergröße. Größere Fenstergrößen benötigen zusätzlichen Speicher, können jedoch die Leistung verbessern.

  Sie können eine ganze Zahl von 0 bis 2048 angeben. Soll die Standardfenstergröße für das Betriebssystem verwendet werden, geben Sie 0 an.

TCPNODELAY
: Gibt an, ob der Server kleine Nachrichten sendet oder ob TCP/IP die Nachrichten puffern soll. Das Senden kleiner Nachrichten kann den Durchsatz verbessern, erhöht jedoch die Anzahl der im Netz gesendeten Pakete. Geben Sie YES an, wenn kleine Nachrichten gesendet werden sollen, oder NO, wenn sie TCP/IP puffern soll. Der Standardwert ist YES.

TCPADMINPORT
: Gibt die Anschlussnummer an, an der der TCP/IP-DFV-Treiber des Servers auf TCP/IP- oder SSL-fähige Kommunikationsanforderungen warten soll, die keine Clientsitzungen sind. Der Standardwert ist der Wert von TCPPORT.

SSLTCPPORT
: (Nur SSL) Gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen des Befehlszeilenclients für Sichern/Archivieren und des Verwaltungsbefehlszeilenclients wartet.

SSLTCPADMINPORT
: (Nur SSL) Gibt die Anschlussadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen für den Verwaltungsbefehlszeilenclient wartet.

AIX: Shared Memory-Optionen definieren

Sie können die Shared Memory-Übertragung zwischen Clients und Servern auf demselben System verwenden. Für die Verwendung von Shared Memory muss TCP/IP Version 4 auf dem System installiert sein.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt eine Einstellung für Shared Memory:

```
commmethod      sharedmem
   shmport      1510
```

In diesem Beispiel gibt SHMPORT die TCP/IP-Anschlussadresse eines Servers bei Verwendung von Shared Memory an. Verwenden Sie die Option SHMPORT, um einen anderen TCP/IP-Anschluss anzugeben. Die Standardanschlussadresse ist 1510.
COMMMETHOD kann in der IBM Spectrum Protect-Serveroptionsdatei mehrfach mit einem jeweils anderen Wert verwendet werden. Die folgende Angabe ist beispielsweise möglich:

```
commmethod tcpip
commmethod sharedmem
```

AIX-BetriebssystemeDie maximale Anzahl gleichzeitig ablaufender Shared Memory-Sitzungen basiert auf den verfügbaren Systemressourcen. Jede Shared Memory-Sitzung verwendet eine Shared Memory-Region mit maximal 4 MB und vier IPCS-Nachrichtenwarteschlangen, abhängig

von der Version des IBM Spectrum Protect-Clients.

AIX-BetriebssystemeWerden der Server und der Client nicht unter derselben Benutzer-ID ausgeführt, muss der Server der Root sein. Damit werden Shared Memory-Übertragungsfehler vermieden.

AIX: Secure Sockets Layer-Optionen definieren

Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

Vorbereitende Schritte

SSL ist die Standardtechnologie für die Erstellung verschlüsselter Sitzungen zwischen Servern und Clients. SSL stellt einen sicheren Kanal für die Server- und Clientkommunikation über offene Kommunikationspfade zur Verfügung. Bei SSL wird die Identität des Servers durch Verwendung digitaler Zertifikate überprüft.

Verwenden Sie SSL für Sitzungen nur im Bedarfsfall, um eine bessere Systemleistung sicherzustellen. Sie könnten die Prozessorressourcen auf dem IBM Spectrum Protect-Server erweitern, um den erhöhten Anforderungen gerecht zu werden.

AIX: Datenbank und Protokoll formatieren

Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.

Nach der Konfiguration der Serverübertragung können Sie die Datenbank initialisieren. Sie müssen sich mit der Instanzbenutzer-ID anmelden. Fügen Sie die Verzeichnisse nicht in Dateisysteme ein, deren Speicherplatz nicht ausreichen könnte. Wenn bestimmte Verzeichnisse (z. B. das Archivprotokoll) nicht verfügbar oder voll werden, stoppt der Server.

Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.

Exitlistenhandler definieren

Geben Sie für jede Serverinstanz ON für die Registry-Variable DB2NOEXITLIST an. Melden Sie sich als Serverinstanzeigner beim System an und geben Sie den folgenden Befehl aus:

```
db2set -i Name_der_Serverinstanz DB2NOEXITLIST=ON
```

Beispiel: AIX-Betriebssysteme

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```

Serverinstanz initialisieren

Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Wenn das Verzeichnis der Serverinstanz z. B. */tsminst1* lautet, geben Sie die folgenden Befehle aus: AIX-Betriebssysteme

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsize=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zu Grunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.
AIX-BetriebssystemeTipp: Wenn DB2 nach Ausgabe des Befehls DSMSERV FORMAT nicht startet, müssen Sie möglicherweise die Mountoption NOSUID des Dateisystems inaktivieren. Wird diese Option in dem Dateisystem definiert, in dem sich das Verzeichnis des DB2-Instanzeigners befindet, oder in einem beliebigen Dateisystem, in dem sich die DB2-Datenbank, aktive Protokolldateien, Archivprotokolle, Übernahmeprotokolle oder Spiegelprotokolle befinden, muss die Option inaktiviert werden, um das System starten zu können.
Nach der Inaktivierung der Option NOSUID hängen Sie das Dateisystem erneut an. Dann starten Sie DB2 mit dem folgenden Befehl:

```
db2start
```

Zugehörige Informationen:
DSMSERV FORMAT (Datenbank und Protokoll formatieren)

AIX: Datenbankmanager für die Datenbanksicherung vorbereiten

Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

Informationen zu diesem Vorgang

AIX-BetriebssystemeAb IBM Spectrum Protect Version 7.1 ist es nicht mehr erforderlich, das API-Kennwort während einer manuellen Konfiguration des Servers zu definieren. Wenn Sie das API-Kennwort während des manuellen Konfigurationsprozesses definieren, können Datenbanksicherungsversuche fehlschlagen.

Wenn Sie den Konfigurationsassistenten verwenden, um eine IBM Spectrum Protect-Serverinstanz zu erstellen, müssen Sie diese Schritte nicht ausführen. Wenn Sie eine Instanz manuell konfigurieren, führen Sie die folgenden Schritte aus, bevor Sie den Befehl BACKUP DB oder RESTORE DB ausgeben.

Achtung: Wenn die Datenbank nicht verwendet werden kann, ist der gesamte IBM Spectrum Protect-Server nicht verfügbar. Wenn eine Datenbank verloren geht und nicht wiederhergestellt werden kann, kann die Wiederherstellung der von diesem Server verwalteten Daten schwierig oder unmöglich sein. Daher ist es unbedingt erforderlich, die Datenbank zu sichern.
AIX-BetriebssystemeIn den folgenden Befehlen müssen Sie die Beispielwerte durch Ihre tatsächlichen Werte ersetzen. In den Beispielen wird `tsminst1` für die Benutzer-ID der Serverinstanz, /tsminst1 für das Verzeichnis der Serverinstanz und /home/tsminst1 als Ausgangsverzeichnis der Serverinstanzbenutzer verwendet.

1. Definieren Sie die Umgebungsvariablenkonfiguration der IBM Spectrum Protect-API für die Datenbankinstanz:
   a. Melden Sie sich mit der Benutzer-ID `tsminst1` an.
   b. Wenn der Benutzer `tsminst1` angemeldet ist, stellen Sie sicher, dass die DB2-Umgebung ordnungsgemäß initialisiert wird. Die DB2-Umgebung wird durch Ausführung des Scripts /home/tsminst1/sqllib/db2profile initialisiert, das normalerweise automatisch über das Profil der Benutzer-ID ausgeführt wird. Stellen Sie sicher, dass die `.profile`-Datei im Ausgangsverzeichnis der Instanzbenutzer vorhanden ist, z. B. /home/tsminst1/.profile. Wenn `.profile` das Script `db2profile` nicht ausführt, fügen Sie folgende Zeilen hinzu:

      ```
      if [ -f /home/tsminst1/sqllib/db2profile ]; then
            . /home/tsminst1/sqllib/db2profile
        fi
      ```

   c. Fügen Sie in der Datei *Instanzverzeichnis*/sqllib/userprofile die folgenden Zeilen hinzu:

      ```
      DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
      DSMI_DIR=Serververzeichnis_bin/dbbkapi
      DSMI_LOG=Serverinstanzverzeichnis
      export DSMI_CONFIG DSMI_DIR DSMI_LOG
      ```

      Hierbei gilt Folgendes:
      - *Instanzverzeichnis* ist das Ausgangsverzeichnis des Serverinstanzbenutzers.
      - *Serverinstanzverzeichnis* ist das Serverinstanzverzeichnis.
      - *Serververzeichnis_bin* ist das Serververzeichnis 'bin'. Die Standardposition ist /opt/tivoli/tsm/server/bin.

      Fügen Sie in der Datei *Instanzverzeichnis*/sqllib/usercshrc die folgenden Zeilen hinzu:

      ```
      setenv DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
      setenv DSMI_DIR=Serververzeichnis_bin/dbbkapi
      setenv DSMI_LOG=Serverinstanzverzeichnis
      ```

2. Melden Sie sich ab und als `tsminst1` erneut an oder geben Sie den folgenden Befehl aus:

   ```
   . ~/.profile
   ```

   Tipp: Stellen Sie sicher, dass Sie ein Leerzeichen nach dem ersten Punkt (.) eingeben.
3. Erstellen Sie eine Datei mit dem Namen `tsmdbmgr.opt` im Verzeichnis *Serverinstanz*, das sich in diesem Beispiel im Verzeichnis /tsminst1 befindet, und fügen Sie folgende Zeile hinzu:

   ```
   SERVERNAME TSMDBMGR_TSMINST1
   ```

   Hinweis: Der Wert für `SERVERNAME` muss in den Dateien `tsmdbmgr.opt` und `dsm.sys` konsistent sein.
4. Fügen Sie als Rootbenutzer die folgenden Zeilen zur Konfigurationsdatei `dsm.sys` der IBM Spectrum Protect-API hinzu. Die Konfigurationsdatei `dsm.sys` befindet sich standardmäßig in folgendem Standardverzeichnis:
   - *Serververzeichnis_bin*/dbbkapi/dsm.sys

   ```
   servername TSMDBMGR_TSMINST1
   commmethod tcpip
   tcpserveraddr localhost
   tcpport 1500
   errorlogname /tsminst1/tsmdbmgr.log
   nodename $$_TSMDBMGR_$$
   ```

   Erläuterungen:
   - *Servername* stimmt mit dem Wert für `servername` in der Datei `tsmdbmgr.opt` überein.
   - *Commethod* gibt die Client-API an, mit der Kontakt zum Server wegen der Datenbanksicherung hergestellt wird. Gültige Werte sind `tcpip` und `sharedmem`. Weitere Informationen zu Shared Memory (gemeinsam genutzter Speicher) finden Sie in Schritt 5.

- *Tcpserveraddr* gibt die Serveradresse an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `localhost` lauten.
- *Tcpport* gibt die Anschlussnummer an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Sie müssen denselben `tcpport`-Wert wie in der Serveroptionsdatei dsmserv.opt angeben.
- *Errorlogname* gibt das Fehlerprotokoll an, in dem die Client-API Fehler protokolliert, die während einer Datenbanksicherung auftreten. Dieses Protokoll befindet sich normalerweise im Serverinstanzverzeichnis. Dieses Protokoll kann sich jedoch an jeder beliebigen Position befinden, für die die Instanzbenutzer-ID Schreibberechtigung hat.
- *Nodename* gibt den Knotennamen an, mit dem die Client-API während einer Datenbanksicherung eine Verbindung zum Server herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `$$_TSMDBMGR_$$` lauten.

5. Optional: Konfigurieren Sie den Server für die Datenbanksicherung mithilfe von Shared Memory. Auf diese Weise könnten Sie die Prozessorauslastung verringern und den Durchsatz verbessern. Führen Sie die folgenden Schritte aus:
   a. Überprüfen Sie die Datei dsmserv.opt. Fügen Sie die folgenden Zeilen in die Datei ein, falls nicht vorhanden:

      ```
      commmethod sharedmem
      shmport Anschlussnummer
      ```

      Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.
   b. Suchen Sie in der Konfigurationsdatei dsm.sys die folgenden Zeilen:

      ```
      commmethod tcpip
      tcpserveraddr localhost
      tcpport Anschlussnummer
      ```

      Ersetzen Sie die angegebenen Zeilen durch die folgenden Zeilen:

      ```
      commmethod sharedmem
      shmport Anschlussnummer
      ```

      Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.

AIX: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren

Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.

Informationen zu diesem Vorgang

Die Tabellen- und Indexreorganisation erfordert in hohem Umfang Prozessorressourcen, Speicherbereich für die aktive Protokolldatei und Speicherbereich für das Archivprotokoll. Da die Datenbanksicherung Vorrang vor der Reorganisation hat, wählen Sie den Zeitpunkt und die Dauer für die Reorganisation aus, um sicherzustellen, dass sich die Prozesse nicht überlappen und die Reorganisation ausgeführt werden kann.

AIX-BetriebssystemeSie können die Index- und Tabellenreorganisation für die Serverdatenbank optimieren. Auf diese Weise können Sie die Vermeidung von unerwartetem Datenbankwachstum und Leistungsproblemen verbessern. Anweisungen finden Sie in Technote 1683633.

Wenn Sie diese Serveroptionen aktualisieren, während der Server aktiv ist, müssen Sie den Server stoppen und erneut starten, damit die aktualisierten Werte wirksam werden.

Vorgehensweise

1. Ändern Sie die Serveroptionen.
   AIX-BetriebssystemeBearbeiten Sie die Serveroptionsdatei dsmserv.opt im Serverinstanzverzeichnis. Beachten Sie bei der Bearbeitung der Serveroptionsdatei die folgenden Richtlinien:
   - Entfernen Sie den Stern am Zeilenanfang, um eine Option zu aktivieren.
   - Geben Sie eine Option in einer beliebigen Zeile ein.
   - Geben Sie nur eine Option pro Zeile ein. Die vollständige Option mit ihrem Wert muss sich in einer Zeile befinden.
   - Haben Sie mehrere Einträge für eine Option in der Datei, verwendet der Server den letzten Eintrag.

   Die verfügbaren Serveroptionen können Sie mit der Musterdatei dsmserv.opt.smp im Verzeichnis /opt/tivoli/tsm/server/bin anzeigen.
2. Ist die Verwendung der Datendeduplizierung geplant, aktivieren Sie die Serveroption ALLOWREORGINDEX. Fügen Sie der Serveroptionsdatei die folgende Option und den folgenden Wert hinzu:

   ```
   allowreorgindex yes
   ```

3. Definieren Sie die Serveroptionen REORGBEGINTIME und REORGDURATION, mit denen gesteuert wird, wann die Reorganisation gestartet und wie lange sie ausgeführt wird. Wählen Sie den Zeitpunkt und die Dauer so aus, dass die Reorganisation ausgeführt wird, wenn der Server voraussichtlich am wenigsten ausgelastet ist. Diese Serveroptionen steuern sowohl die Tabellen- als auch die Indexreorganisationsprozesse.
   a. Definieren Sie die Startzeit der Reorganisation mit der Serveroption REORGBEGINTIME. Geben Sie die Zeit im 24-Stunden-Format an. Um beispielsweise als Startzeit der Reorganisation 20:30 Uhr festzulegen, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

```
reorgbegintime 20:30
```

b. Definieren Sie das Intervall, in dem der Server die Reorganisation starten kann. Um beispielsweise anzugeben, dass der Server die Reorganisation innerhalb von 4 Stunden nach dem mit der Serveroption REORGBEGINTIME definierten Zeitpunkt starten kann, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

```
reorgduration 4
```

4. War der Server aktiv, während Sie die Serveroptionsdatei aktualisiert haben, stoppen Sie den Server und starten Sie ihn erneut.

Zugehörige Informationen:
ALLOWREORGINDEX
ALLOWREORGTABLE
REORGBEGINTIME
REORGDURATION
AIX-Betriebssysteme

AIX: Serverinstanz starten

Sie können den Server mit der Instanzbenutzer-ID (bevorzugte Methode) oder mit der Rootbenutzer-ID starten.

Vorbereitende Schritte

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden.

AIX-BetriebssystemeAnweisungen finden Sie in Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

Informationen zu diesem Vorgang

Wenn Sie den Server unter Verwendung der Instanzbenutzer-ID starten, wird der Konfigurationsprozess vereinfacht und potenzielle Probleme werden vermieden. In einigen Fällen kann jedoch die Verwendung der Rootbenutzer-ID zum Starten des Servers erforderlich sein. Beispielsweise kann die Rootbenutzer-ID verwendet werden, um sicherzustellen, dass der Server auf bestimmte Einheiten zugreifen kann. Sie können den automatischen Serverstart mit der Instanzbenutzer-ID oder mit der Rootbenutzer-ID konfigurieren.

AIX-BetriebssystemeWenn Sie Verwaltungs- oder Rekonfigurationstasks ausführen müssen, starten Sie den Server im Verwaltungsmodus.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um den Server zu starten:

- Starten Sie den Server mithilfe der Instanzbenutzer-ID.

  AIX-BetriebssystemeAnweisungen finden Sie in Server mit der Instanzbenutzer-ID starten.

- Starten Sie den Server mithilfe der Rootbenutzer-ID.

  Anweisungen zum Berechtigen von Rootbenutzer-IDs zum Starten des Servers finden Sie in Rootbenutzer-IDs zum Starten des Servers berechtigen (Version 7.1.1). Anweisungen zum Starten des Servers mit der Rootbenutzer-ID finden Sie in Server mit der Rootbenutzer-ID starten (Version 7.1.1).

- AIX-BetriebssystemeStarten Sie den Server automatisch.

  AIX-BetriebssystemeAnweisungen siehe AIX: Server automatisch starten.

- AIX-BetriebssystemeStarten Sie den Server im Verwaltungsmodus.

  Anweisungen siehe AIX: Server im Verwaltungsmodus starten.

AIX-Betriebssysteme

AIX: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen

Vor dem Start des Servers überprüfen Sie Zugriffsberechtigungen und Benutzergrenzwerte.

Informationen zu diesem Vorgang

Wenn Sie die Benutzergrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, nicht überprüfen, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann. Die müssen auch den systemweiten Grenzwert für die maximale Anzahl offener Dateien überprüfen. Der systemweite Grenzwert muss größer-gleich dem Benutzergrenzwert sein.

Vorgehensweise

1. Überprüfen Sie, ob die Benutzer-ID der Serverinstanz über Berechtigungen zum Starten des Servers verfügt.
2. Stellen Sie für die Serverinstanz, die Sie starten wollen, sicher, dass Sie über die Berechtigung zum Lesen und Schreiben von Dateien im Serverinstanzverzeichnis verfügen. Stellen Sie sicher, dass die Datei dsmserv.opt im Serverinstanzverzeichnis vorhanden ist und dass die Datei Parameter für die Serverinstanz enthält.
3. Wenn der Server mit einem Bandlaufwerk, einem Datenträgerwechsler oder mit einer Einheit für austauschbare Datenträger verbunden ist und Sie den Server mit der Instanzbenutzer-ID starten wollen, erteilen Sie der Instanzbenutzer-ID Schreib-/Lesezugriff für diese Einheiten. Führen Sie einen der folgenden Schritte aus, um Berechtigungen festzulegen:
   - Bei einem für IBM Spectrum Protect dediziertem System, auf das nur der IBM Spectrum Protect-Administrator zugreifen kann, erteilen Sie globale Schreibberechtigung für die Gerätedateien der Einheiten. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

     ```
     chmod +w /dev/rmtX
     ```

   - Verfügt das System über mehrere Benutzer, können Sie den Zugriff einschränken, indem Sie die IBM Spectrum Protect-Instanzbenutzer-ID zum Eigner der Gerätedateien der Einheit machen. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

     ```
     chmod u+w /dev/rmtX
     ```

   - Sind mehrere Benutzerinstanzen auf einem System aktiv, ändern Sie den Gruppennamen (z. B. TAPEUSERS) und fügen Sie jede IBM Spectrum Protect-Instanzbenutzer-ID dieser Gruppe hinzu. Übertragen Sie dann das Eigentumsrecht der Gerätedateien der Einheiten an die Gruppe TAPEUSERS und erteilen Sie Schreibberechtigung für die Gruppe. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

     ```
     chmod g+w /dev/rmtX
     ```

4. Überprüfen Sie die folgenden Benutzergrenzwerte anhand der Richtlinien in der Tabelle.

   Tabelle 1. Benutzergrenzwerte (ulimit-Werte)

Typ des Benutzergrenzwerts	Bevorzugter Wert	Befehl zum Abfragen des Werts
Maximale Größe erstellter Kerndateien	Unlimited	`ulimit -Hc`
Maximale Größe eines Datensegments für einen Prozess	Unlimited	`ulimit -Hd`
Maximale Dateigröße	Unlimited	`ulimit -Hf`
Maximale Anzahl offener Dateien	65536	`ulimit -Hn`
Maximale Prozessorzeit in Sekunden	Unlimited	`ulimit -Ht`

   Für die Änderung von Benutzergrenzwerten befolgen Sie die Anweisungen in der Dokumentation Ihres Betriebssystems.

   Tipp: Wenn Sie den Server mithilfe eines Scripts automatisch starten wollen, können Sie die Benutzergrenzwerte in dem Script definieren.
5. Stellen Sie sicher, dass als Benutzergrenzwert für die maximale Anzahl Benutzerprozesse (`nproc`-Einstellung) der empfohlene Mindestwert 16384 festgelegt wird.
   a. Geben Sie den Befehl `ulimit -Hu` mithilfe der Instanzbenutzer-ID aus, um den aktuellen Benutzergrenzwert zu überprüfen. Zum Beispiel:

      ```
      [user@Machine ~]$ ulimit -Hu
      16384
      ```

   b. Lautet der Grenzwert für die maximale Anzahl Benutzerprozesse nicht 16384, geben Sie den Wert 16384 an.
   AIX-BetriebssystemeFügen Sie der Datei /etc/security/limits die folgende Zeile hinzu:

      ```
      Instanzbenutzer-ID        -    nproc          16384
      ```

      Hierbei gibt *Instanzbenutzer-ID* die Benutzer-ID der Serverinstanz an.

 AIX-Betriebssysteme

AIX: Server mit der Instanzbenutzer-ID starten

Um den Server mit der Instanzbenutzer-ID zu starten, melden Sie sich mit der Instanzbenutzer-ID an und geben Sie im Serverinstanzverzeichnis den entsprechenden Befehl ein.

Vorbereitende Schritte

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden. Anweisungen siehe AIX: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

Vorgehensweise

1. Melden Sie sich bei dem System, auf dem IBM Spectrum Protect installiert ist, unter Verwendung der Instanzbenutzer-ID für den Server an.
2. Wenn Sie über kein Benutzerprofil zur Ausführung des Scripts `db2profile` verfügen, geben Sie den folgenden Befehl ein:

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

   Tipp: Anweisungen zur Aktualisierung des Benutzer-ID-Anmeldescripts zur automatischen Ausführung des Scripts `db2profile` finden Sie in der DB2-Dokumentation.
3. Geben Sie den folgenden Befehl in einer Zeile im Verzeichnis der Serverinstanz aus, um den Server zu starten:

   
   AIX-Betriebssysteme

   ```
   LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
   usr/bin/dsmserv
   ```

   
   AIX-BetriebssystemeAchten Sie darauf, ein Leerzeichen hinter `SHMPSIZE=64K` einzufügen. Wenn Sie den Server mit diesem Befehl starten, aktivieren Sie 64-KB-Speicherseiten für den Server. Diese Einstellung hilft Ihnen bei der Optimierung der Serverleistung.

   Tipp: Der Befehl wird im Vordergrund ausgeführt, sodass Sie eine Administrator-ID definieren und der Serverinstanz zuordnen können.
   
   AIX-BetriebssystemeHat beispielsweise die Serverinstanz den Namen `tsminst1` und das Serverinstanzverzeichnis den Namen /tsminst1, können Sie die Instanz starten, indem Sie die folgenden Befehle ausgeben:

   ```
   cd /tsminst1
    . ~/sqllib/db2profile
   LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
   usr/bin/dsmserv
   ```


AIX-Betriebssysteme

AIX: Server automatisch starten

Sie können den Server so konfigurieren, dass er beim Systemstart automatisch gestartet wird. Zu diesem Zweck wird das Script rc.dsmserv zur Verfügung gestellt.

Vorbereitende Schritte

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden.


AIX-BetriebssystemeAnweisungen finden Sie in Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

Informationen zu diesem Vorgang

Das Script rc.dsmserv befindet sich im Serverinstallationsverzeichnis, z. B. in /opt/tivoli/tsm/server/bin.


AIX-BetriebssystemeTipp: Wenn Sie den Konfigurationsassistenten verwendet hatten, hatten Sie möglicherweise die Auswahl getroffen, den Server beim Systemneustart automatisch zu starten. Wenn Sie diese Auswahl getroffen hatten, wurde der Datei /etc/inittab automatisch ein Eintrag zum Starten des Servers hinzugefügt.

Vorgehensweise

Wenn Sie keinen Assistenten zur Konfiguration des Servers verwendet haben, fügen Sie der Datei /etc/inittab für jeden Server, der automatisch gestartet werden soll, einen Eintrag hinzu:

1. Setzen Sie die Ausführungsebene auf den Wert, der dem Mehrbenutzermodus mit aktiviertem Netzbetrieb entspricht. Normalerweise ist der zu verwendende Wert für die Ausführungsebene abhängig vom Betriebssystem und seiner Konfiguration 2, 3 oder 5. Stellen Sie sicher, dass die Ausführungsebene in der Datei /etc/inittab mit der Ausführungsebene des Betriebssystems übereinstimmt. Weitere Informationen zum Mehrbenutzermodus und zu Ausführungsebenen enthält die Dokumentation zu Ihrem Betriebssystem.
2. Geben Sie im Befehl rc.dsmserv in der Datei /etc/inittab die Instanzbenutzer-ID mit der Option -u und die Position des Serverinstanzverzeichnisses mit der Option -i an. Wenn mehrere Serverinstanzen automatisch gestartet werden sollen, fügen Sie für jede Serverinstanz einen Eintrag hinzu. Informationen zur Überprüfung der Syntax finden Sie in der Dokumentation zu Ihrem Betriebssystem.
   Tipp: Um eine Serverinstanz automatisch mit der Rootbenutzer-ID zu starten, verwenden Sie die Option -U.

Beispiel

Hat beispielsweise der Instanzeigner den Namen tsminst1 und das Serverinstanzverzeichnis den Namen /home/tsminst1/tsminst1, fügen Sie /etc/inittab in einer einzigen Zeile den folgenden Eintrag hinzu:


AIX-Betriebssysteme

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
   -i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
```

In diesem Beispiel ist die Prozess-ID `tsm1` und die Ausführungsebene ist mit 2 definiert.

Wenn Sie mehrere Serverinstanzen ausführen möchten, fügen Sie für jede Serverinstanz einen Eintrag hinzu. Sind beispielsweise die Instanzeigner-IDs tsminst1 und tsminst2 und die Instanzverzeichnisse /home/tsminst1/tsminst1 und /home/tsminst2/tsminst2 definiert, fügen Sie /etc/inittab die folgenden Einträge hinzu. Jeder Eintrag befindet sich in jeweils einer Zeile.


AIX-Betriebssysteme

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
   -i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
tsm2:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst2
   -i /home/tsminst2/tsminst2 -q >/dev/console 2>&1
```

Zugehörige Verweise:
Serverstartscript: rc.dsmserv

AIX-Betriebssysteme

AIX: Server im Verwaltungsmodus starten

Sie können den Server im Verwaltungsmodus starten, um Unterbrechungen während Verwaltungs- oder Rekonfigurationstasks zu vermeiden.

Informationen zu diesem Vorgang

Führen Sie das Dienstprogramm DSMSERV mit dem Parameter MAINTENANCE aus, um den Server im Verwaltungsmodus zu starten.

Die folgenden Operationen sind im Verwaltungsmodus inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Wiederherstellung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Außerdem wird verhindert, dass Clients Sitzungen mit dem Server starten.
Tipps:

- Sie müssen die Serveroptionsdatei dsmserv.opt nicht bearbeiten, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Prozesse für die Speicherbereichswiederherstellung, den Bestandsverfall und die Speicherpoolumlagerung manuell starten.

Vorgehensweise

Geben Sie den folgenden Befehl aus, um den Server im Verwaltungsmodus zu starten:

```
dsmserv maintenance
```

Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann unter Server im Verwaltungsmodus starten angezeigt werden.

Nächste Schritte

Gehen Sie wie folgt vor, um den Serverbetrieb im Produktionsmodus fortzusetzen:

1. Geben Sie den Befehl HALT aus, um den Server herunterzufahren:

   ```
   halt
   ```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden.

Die während des Verwaltungsmodus inaktivierten Operationen werden wieder aktiviert.

AIX: Server stoppen

Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.

Informationen zu diesem Vorgang

Geben Sie den folgenden Befehl in die IBM Spectrum Protect-Befehlszeile ein, um den Server zu stoppen:

```
halt
```

AIX-BetriebssystemeWenn Sie keine Verbindung zum Server mit einem Verwaltungsclient herstellen können und wenn der Server gestoppt werden soll, müssen Sie den Prozess mit dem Befehl kill mit der Prozess-ID (PID) abbrechen. Die PID wird bei der Initialisierung angezeigt.
Wichtig: Bevor der Befehl kill eingegeben wird, müssen Sie sicherstellen, dass die korrekte Prozess-ID für den IBM Spectrum Protect-Server bekannt ist.
Die Prozess-ID des mit dem Befehl kill abzubrechenden Prozesses kann mithilfe der Datei `dsmserv.v6lock` in dem Verzeichnis, in dem der Server ausgeführt wird, ermittelt werden. Geben Sie Folgendes ein, um die Datei anzuzeigen:

```
cat /instance_dir/dsmserv.v6lock
```

AIX-BetriebssystemeGeben Sie den folgenden Befehl aus, um den Server zu stoppen:

```
kill -36 dsmserv_pid
```

Hierbei steht *dsmserv_pid* für die Prozess-ID.

AIX: Lizenzregistrierung

Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.

Informationen zu diesem Vorgang

Verwenden Sie hierfür den Befehl REGISTER LICENSE. Weitere Informationen siehe REGISTER LICENSE.

Beispiel: Lizenz registrieren

Die IBM Spectrum Protect-Basislizenz registrieren.

```
register license file=tsmbasic.lic
```

AIX: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben

Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.

Vorbereitende Schritte

Stellen Sie sicher, dass eine Bandeinheitenklasse oder eine Einheitenklasse FILE definiert wurde. Ausführliche Informationen finden Sie in DEFINE DEVCLASS oder suchen Sie nach 'Einheitenklasse definieren'.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Ihr System für Datenbanksicherungen zu konfigurieren.

Vorgehensweise

1. Wenn Sie den Server nicht mit dem Konfigurationsassistenten (dsmicfgx) konfiguriert haben, müssen Sie sicherstellen, dass die Schritte zur manuellen Konfiguration des Systems für Datenbanksicherungen ausgeführt werden.
2. Wählen Sie die für Datenbanksicherungen zu verwendende Einheitenklasse aus. Geben Sie den folgenden Befehl über eine IBM Spectrum Protect-Verwaltungsbefehlszeile aus.

   ```
   set dbrecovery Einheitenklassenname
   ```

   Die angegebene Einheitenklasse wird vom Datenbankmanager für Datenbanksicherungen verwendet. Wenn Sie keine Einheitenklasse mit dem Befehl SET DBRECOVERY angeben, schlägt die Sicherung fehl.

Beispiel

Geben Sie beispielsweise den folgenden Befehl aus, um anzugeben, dass die Einheitenklasse DBBACK verwendet werden soll:

```
set dbrecovery dbback
```

AIX: Mehrere Serverinstanzen auf einem System ausführen

Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.

Multiplizieren Sie den Speicherbedarf und andere Systemvoraussetzungen für einen Server mit der geplanten Instanzzahl für das System.

 AIX-BetriebssystemeDie Gruppe der Dateien für eine Instanz des Servers wird getrennt von den Dateien gespeichert, die von einer anderen Serverinstanz auf demselben System verwendet werden. Gehen Sie wie in AIX: Serverinstanz erstellen beschrieben für jede neue Instanz vor, einschließlich der Erstellung des neuen Instanzbenutzers.

Zur Verwaltung des von jedem Server verwendeten Systemspeichers begrenzen Sie mit der Serveroption DBMEMPERCENT den Prozentsatz des Systemspeichers. Haben alle Server denselben Stellenwert, verwenden Sie für jeden Server denselben Wert. Ist ein Server ein Produktionsserver und andere Server sind Testserver, geben Sie für den Produktionsserver einen höheren Wert an als für die Testserver.

Von Version 6.3 auf Version 7.1 ist ein direktes Upgrade möglich. Weitere Informationen finden Sie im Abschnitt über das Upgrade (Upgrade auf Version 8.1 durchführen). Wenn Sie ein Upgrade durchführen und mehrere Server auf dem System haben, müssen Sie den Installationsassistenten nur einmal ausführen. Der Installationsassistent erfasst die Datenbank- und Variablendaten für alle ursprünglichen Serverinstanzen.

Wenn Sie ein Upgrade von IBM Spectrum Protect Version 6.3 auf Version 8.1.2 durchführen und sich mehrere Server auf Ihrem System befinden, werden alle in DB2 Version 9.7 vorhandenen Instanzen gelöscht und in DB2 Version 11.1 erneut erstellt. Der Assistent gibt den Befehl `db2 upgrade DB DB-Name` für jede Datenbank aus. Die Datenbankumgebungsvariablen für jede Instanz auf Ihrem System werden ebenfalls während des Upgradeprozesses neu konfiguriert.

Zugehörige Tasks:
Mehrere Serverinstanzen auf einem einzigen System ausführen (Version 7.1.1)

AIX: Server überwachen

Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

Vorgehensweise

1. Überwachen Sie die aktive Protokolldatei, um sicherzustellen, dass die Größe für die Auslastung der Serverinstanz korrekt ist.

   Wenn die Serverauslastung ihren normalen erwarteten Stand erreicht hat, belegt der von der aktiven Protokolldatei verwendete Speicherbereich 80 bis 90 Prozent des Speicherbereichs, der für das Verzeichnis für aktive Protokolldateien zur Verfügung steht. An diesem Punkt müssen Sie den Speicherbereich möglicherweise vergrößern. Die Vergrößerung des Speicherbereichs ist von der Art der Transaktionen in der Serververarbeitung abhängig. Transaktionsmerkmale wirken sich auf die Belegung des Speicherbereichs der aktiven Protokolldateien aus.

   Die folgenden Transaktionsmerkmale können sich auf die Speicherbereichsbelegung in der aktiven Protokolldatei auswirken:

   - Die Anzahl und Größe der Dateien in Sicherungsoperationen
     - Clients, wie z. B. Dateiserver, die zahlreiche kleine Dateien sichern, können zahlreiche Transaktionen verursachen, die in kurzer Zeit ausgeführt werden. Die Transaktionen können sehr viel Speicherbereich in der aktiven Protokolldatei belegen, jedoch nur für kurze Zeit.
     - Clients, wie z. B. E-Mail-Server oder ein Datenbankserver, die große Datenvolumen in wenigen Transaktionen sichern, können wenige Transaktionen verursachen, deren Auführung viel Zeit in Anspruch nimmt. Die Transaktionen können wenig Speicherbereich in der aktiven Protokolldatei belegen, jedoch für lange Zeit.
   - Netzverbindungstypen
     - Mit schnellen Netzverbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, die schneller ausgeführt werden. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen kürzeren Zeitraum.
     - Mit langsameren Verbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, deren Ausführung länger dauert. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen längeren Zeitraum.

   Wenn der Server Transaktionen mit sehr unterschiedlichen Merkmalen verarbeitet, kann der für die aktive Protokolldatei verwendete Speicherbereich im Lauf der Zeit sehr stark schwanken. Für einen solchen Server müssen Sie unter Umständen dafür sorgen, dass ein niedrigerer Prozentsatz des Speicherbereichs der aktiven Protokolldatei verwendet wird. Der zusätzliche Speicherbereich gestattet eine Vergrößerung der aktiven Protokolldatei für Transaktionen, die viel Zeit in Anspruch nehmen.

2. Überwachen Sie das Archivprotokoll, um sicherzustellen, dass immer Speicherbereich verfügbar ist.
   Hinweis: Wenn das Archivprotokoll und das Übernahmearchivprotokoll voll werden, kann die aktive Protokolldatei voll werden, so dass der Server stoppt. Für das Archivprotokoll muss so viel Speicherbereich zur Verfügung stehen, dass dieser niemals vollständig belegt wird.
   Sie werden wahrscheinlich Folgendes feststellen:
   a. Am Anfang wird das Archivprotokoll schnell größer, wenn normale Clientsicherungsoperationen ausgeführt werden.
   b. Datenbanksicherungen werden regelmäßig ausgeführt, entweder mit einem Zeitplan oder manuell.
   c. Nach mindestens zwei Datenbankgesamtsicherungen wird das Abschneiden des Protokolls automatisch ausgeführt. Der vom Archivprotokoll belegte Speicherbereich verringert sich durch das Abschneiden.
   d. Normale Clientoperationen werden fortgesetzt und das Archivprotokoll wird wieder größer.
   e. Datenbanksicherungen finden regelmäßig statt und die Häufigkeit der Protokollbereinigung ist von der Häufigkeit der Datenbankgesamtsicherungen abhängig.

   Nach diesem Muster nimmt die Größe des Archivprotokolls zunächst zu, verringert sich und nimmt dann eventuell wieder zu. Im Laufe der Zeit sollte der vom Archivprotokoll belegte Speicherbereich während der normalen Verarbeitung einen relativ konstanten Stand erreichen.

Wenn die Größe des Archivprotokolls weiter zunimmt, sollten Sie eine oder beide der folgenden Maßnahmen in Betracht ziehen:
    - Ordnen Sie dem Archivprotokoll weiteren Speicherbereich zu. Sie müssen unter Umständen das Archivprotokoll in ein anderes Dateisystem versetzen.
    - Erhöhen Sie die Häufigkeit der Datenbankgesamtsicherungen, so dass die Protokollbereinigung häufiger stattfindet.
3. Wenn Sie ein Verzeichnis für das Übernahmearchivprotokoll definiert haben, überprüfen Sie, ob darin Protokolle während der normalen Verarbeitung gespeichert werden. Wenn der Speicherbereich des Übernahmeprotokolls verwendet wird, sollten Sie das Archivprotokoll vergrößern. Das Übernahmearchivprotokoll sollte nur unter außergewöhnlichen Bedingungen verwendet werden, nicht während der normalen Verarbeitung.

AIX: IBM Spectrum Protect-Server-Fixpack installieren

IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.

Vorbereitende Schritte

Damit ein Fixpack oder ein vorläufiger Fix auf dem Server installiert werden kann, müssen Sie den Server mit der Stufe installieren, auf der er ausgeführt werden soll. Sie müssen die Serverinstallation nicht mit dem Basisrelease beginnen. Wenn momentan beispielsweise Version 8.1.1 installiert ist, können Sie das aktuelle Fixpack für Version 8.1 direkt verwenden. Sie müssen nicht mit der Installation von Version 8.1.0 beginnen, wenn eine Wartungsaktualisierung verfügbar ist.

Das IBM Spectrum Protect-Lizenzpaket muss installiert sein. Das Lizenzpaket wird beim Kauf eines Basisreleases bereitgestellt. Wenn Sie ein Fixpack oder einen vorläufigen Fix von Fix Central herunterladen, installieren Sie die Serverlizenz, die auf der Website von Passport Advantage zur Verfügung steht. Sollen Nachrichten und Hilfetext nicht in Englisch angezeigt werden, installieren Sie das gewünschte Sprachenpaket.

Wenn Sie ein Upgrade des Servers auf Version 8.1.2 oder höher durchführen und den Server dann auf einen Stand vor Version 8.1.2 zurücksetzen, müssen Sie die Datenbank auf einen Zeitpunkt vor dem Upgrade zurückschreiben. Führen Sie während des Upgrades die erforderlichen Schritte aus, mit denen sichergestellt wird, dass die Datenbank zurückgeschrieben werden kann: Sichern Sie die Datenbank, die Protokolldatei für Datenträger, die Einheitenkonfigurationsdatei und die Serveroptionsdatei. Weitere Informationen finden Sie in AIX: Von Version 8.1.2 auf eine vorherige Serverversion zurücksetzen.

Wenn Sie den Clientverwaltungsservice verwenden, müssen Sie ein Upgrade dieses Service auf dieselbe Version wie beim IBM Spectrum Protect-Server durchführen.

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des installierten Servers aufbewahrt werden. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Rufen Sie das IBM® Support Portal auf. Hier finden Sie folgende Informationen:

- Eine Liste der neuesten Wartungs- und Download-Fixes. Klicken Sie auf **Download** und legen Sie alle gültigen Fixes an.
- Informationen zum Erwerb eines Basislizenzpakets. Suchen Sie nach **Downloads > Passport Advantage**.
- Unterstützte Plattformen und Systemvoraussetzungen. Suchen Sie nach **IBM Spectrum Protect supported operating systems**.

Sie müssen ein Upgrade des Servers durchführen, bevor Sie ein Upgrade der Clients für Sichern/Archivieren durchführen. Wenn Sie das Upgrade des Servers nicht zuerst durchführen, könnte die Kommunikation zwischen dem Server und den Clients unterbrochen werden.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Fixpack oder einen vorläufigen Fix zu installieren:

1. Sichern Sie die Datenbank. Die bevorzugte Methode ist eine Momentaufnahmesicherung. Bei einer Momentaufnahmesicherung handelt es sich um eine Datenbankgesamtsicherung, bei der geplante Datenbanksicherungen nicht unterbrochen werden. Geben Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Sichern Sie die Einheitenkonfigurationsdaten. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup devconfig filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.
3. Speichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis oder benennen Sie die Datei um. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup volhistory filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.

4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
5. Halten Sie den Server vor der Installation eines Fixpacks oder eines vorläufigen Fixes an. Verwenden Sie den Befehl HALT.
6. Stellen Sie sicher, dass im Installationsverzeichnis zusätzlicher Speicherplatz zur Verfügung steht. Für die Installation dieses Fixpacks kann zusätzlicher temporärer Plattenspeicherplatz im Installationsverzeichnis des Servers erforderlich sein. Die Größe des zusätzlichen Plattenspeicherplatzes kann der Größe entsprechen, die für die Installation einer neuen Datenbank während einer IBM Spectrum Protect-Installation benötigt wird. Der IBM Spectrum Protect-Installationsassistent zeigt an, wie viel Speicherplatz für die Installation des Fixpacks benötigt wird und wie viel Platz zur Verfügung steht. Wenn der erforderliche Speicherplatz größer ist als der verfügbare Speicherplatz, stoppt die Installation. Wenn die Installation stoppt, fügen Sie dem Dateisystem den erforderlichen Plattenspeicherplatz hinzu und starten Sie die Installation erneut.
7. AIX-BetriebssystemeMelden Sie sich als Root an.
8. Laden Sie die Paketdatei für das Fixpack bzw. den vorläufigen Fix, das bzw. der installiert werden soll, über IBM Support Portal, Passport Advantage oder Fix Central herunter.
9. AIX-BetriebssystemeWechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet, und führen Sie die folgenden Schritte aus.
   Tipp: Die Dateien werden in das aktuelle Verzeichnis extrahiert. Stellen Sie sicher, dass sich die ausführbare Datei in dem Verzeichnis befindet, in dem sich die extrahierten Dateien befinden sollen.
   a. Geben Sie den folgenden Befehl ein, um die Dateiberechtigungen zu ändern:

      ```
      chmod a+x 8.x.x.x-IBM-SPSRV-Plattform.bin
      ```

      Hierbei steht *Plattform* für die Architektur, in der IBM Spectrum Protect installiert werden soll.
   b. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

      ```
      ./8.x.x.x-IBM-SPSRV-Plattform.bin
      ```

10. Wählen Sie eine der folgenden Möglichkeiten für die Installation von IBM Spectrum Protect aus.
    Wichtig: Nach der Installation eines Fixpacks muss die Konfiguration nicht wiederholt werden. Sie können nach Beendigung der Installation stoppen, alle Fehler beheben und dann Ihre Server erneut starten.
    Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden:

    Installationsassistent
    : Befolgen Sie die Anweisungen für Ihr Betriebssystem:
      AIX: IBM Spectrum Protect mit dem Installationsassistenten installieren

    Tipp: Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Aktualisieren. Klicken Sie nicht auf das Symbol Installieren oder Ändern.

    Befehlszeile im Konsolenmodus
    : Befolgen Sie die Anweisungen für Ihr Betriebssystem:
      AIX: IBM Spectrum Protect im Konsolenmodus installieren

    Unbeaufsichtigter Modus
    : Befolgen Sie die Anweisungen für Ihr Betriebssystem:
      AIX: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

    Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, führen Sie den Installationsassistenten nur einmal aus. Der Installationsassistent führt ein Upgrade aller Serverinstanzen durch.

Ergebnisse

Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf Datei > Protokoll anzeigen. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:

- AIX-Betriebssysteme/var/ibm/InstallationManager/logs
- AIX-BetriebssystemeAIX: Fixpack auf IBM Spectrum Protect Version 8.1.2 in einer Clusterumgebung unter AIX anwenden
  IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe. Es ist möglich, ein Fixpack auf eine Clusterumgebung für AIX anzuwenden.

AIX: Von Version 8.1.2 auf eine vorherige Serverversion zurücksetzen

Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und

Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.

Vorbereitende Schritte

Sie benötigen die folgenden Elemente aus der früheren Version des Servers:

- Serverdatenbanksicherung
- Protokolldatei für Datenträger
- Einheitenkonfigurationsdatei
- Serveroptionsdatei

Informationen zu diesem Vorgang

Die Anweisungen sind für das Zurücksetzen innerhalb eines Releases oder von einem Release auf ein vorheriges Release identisch, z. B. von 8.1.2 auf 8.1.1 oder von 8.1.2 auf 7.1.2. Die ältere Version muss mit der Version übereinstimmen, die Sie vor dem Upgrade auf Version 8.1 verwendet haben.

Achtung: Geben Sie den Parameter REUSEDELAY an, um den Verlust von Daten des Clients für Sichern/Archivieren verhindern zu helfen, wenn Sie den Server auf eine vorherige Version zurücksetzen.

Vorgehensweise beim Zurücksetzen auf vorherige Serverversion

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte auf dem System aus, auf dem sich der Server der Version 8.1 befindet.

Vorgehensweise

1. Stoppen Sie den Server, um alle Serveroperationen zu beenden. Verwenden Sie hierfür den Befehl HALT.
2. Entfernen Sie die Datenbank aus dem Datenbankmanager und löschen Sie anschließend die Datenbank- und Wiederherstellungsprotokollverzeichnisse.
   a. Entfernen Sie die Datenbank manuell. Eine Möglichkeit zum Entfernen ist der folgende Befehl: 

      ```
      dsmserv removedb tsmdb1
      ```

   b. Wenn Sie den von den Datenbank- und Wiederherstellungsprotokollverzeichnissen belegten Speicherplatz wiederverwenden müssen, können Sie diese Verzeichnisse jetzt löschen.
3. Deinstallieren Sie den Server der Version 8.1 mit dem Deinstallationsprogramm. Bei der Deinstallation werden der Server und der Datenbankmanager mit den jeweiligen Verzeichnissen entfernt. Ausführliche Informationen siehe AIX: IBM Spectrum Protect deinstallieren.
4. Stoppen Sie den Clusterdienst. Installieren Sie die Version des Serverprogramms, die Sie vor dem Upgrade auf Version 8.1.2 verwendet haben, erneut. Diese Version muss mit der Version übereinstimmen, die auf Ihrem Server verwendet wurde, als Sie die Datenbanksicherung erstellt haben, die Sie zu einem späteren Zeitpunkt wiederherstellen wollen. Wenn der Server vor dem Upgrade z. B. die Version 7.1.7 hatte und wenn Sie die Datenbanksicherung verwenden wollen, die auf diesem Server verwendet wurde, müssen Sie das Fixpack V7.1.7 installieren, damit Sie die Datenbanksicherung zurückschreiben können.
5. Konfigurieren Sie die neue Serverdatenbank mithilfe des Konfigurationsassistenten. Geben Sie den folgenden Befehl aus, um den Assistenten zu starten: 

   ```
   . /dsmicfgx
   ```

6. Stellen Sie sicher, dass keine Server im Hintergrund ausgeführt werden.
7. Schreiben Sie die Datenbank zu einem Zeitpunkt vor dem Upgrade zurück.
8. Kopieren Sie die folgenden Dateien in das Instanzverzeichnis.
   - Einheitenkonfigurationsdatei
   - Protokolldatei für Datenträger
   - Serveroptionsdatei (normalerweise dsmserv.opt)
9. Wenn Sie die Datendeduplizierung für Speicherpools des Typs FILE, die vor dem Upgrade vorhanden waren, aktiviert haben oder wenn Sie während der Verwendung des Servers der Version 8.1.2 Daten, die vor dem Upgrade vorhanden waren, in neue Speicherpools verschoben haben, müssen Sie zusätzliche Schritte ausführen. Weitere Informationen finden Sie in Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung.
10. Wenn die Einstellung des Parameters REUSEDELAY für Speicherpools das Alter der zurückgeschriebenen Datenbank unterschreitet, schreiben Sie Datenträger auf allen Speicherpools mit sequenziellem Zugriff, die nach dieser Datenbanksicherung wiederhergestellt wurden, zurück. Verwenden Sie den Befehl RESTORE VOLUME.
    Wenn keine Sicherung eines Speicherpools vorliegt, prüfen Sie die wiederhergestellten Datenträger mit dem Befehl AUDIT VOLUME und dem Parameter FIX=YES, um Inkonsistenzen zu beheben. Beispiel:

    ```
    audit volume Datenträgername fix=yes
    ```

11. Wurden mit dem Server der Version 8.1 Clientsicherungs- oder -archivierungsoperationen ausgeführt, prüfen Sie die Speicherpooldatenträger, auf denen die Daten gespeichert wurden.

Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung

Wenn Sie während der Ausführung des Servers mit Version 8.1.2 neue Speicherpools erstellt und/oder die Datendeduplizierung für Speicherpools des Typs FILE aktiviert haben, müssen Sie zusätzliche Schritte ausführen, um die vorherige Serverversion wiederherzustellen.

Vorbereitende Schritte

Für diese Task benötigen Sie eine Gesamtsicherung des Speicherpools, die vor dem Upgrade auf Version 8.1.2 erstellt wurde.

Informationen zu diesem Vorgang

Verwenden Sie diese Informationen, wenn Sie einen oder beide der folgenden Schritte ausgeführt haben, während Ihr Server mit Version 8.1.2 ausgeführt wurde:

- Sie haben die Datendeduplizierungsfunktion für beliebige Speicherpools aktiviert, die vor dem Upgrade auf Version 8.1.2 bereits vorhanden waren. Die Datendeduplizierung ist nur für Speicherpools gültig, die den Einheitentyp FILE verwenden.
- Sie haben neue primäre Speicherpools nach dem Upgrade erstellt *und* Daten, die in anderen Speicherpools gespeichert waren, in die neuen Speicherpools versetzt.

Führen Sie diese Schritte aus, nachdem der Server wieder auf Version 7 zurückgesetzt wurde.

Vorgehensweise

- Schreiben Sie für jeden Speicherpool, für den Sie die Datendeduplizierungsfunktion aktiviert haben, den gesamten Speicherpool mit dem Befehl RESTORE STGPOOL zurück.
- Bestimmen Sie für Speicherpools, die Sie nach dem Upgrade erstellt haben, welche Maßnahme durchzuführen ist. Daten, die aus vorhandenen Speicherpools der Version 8 in die neuen Speicherpools versetzt wurden, gehen möglicherweise verloren, weil die neuen Speicherpools auf Ihrem auf Version 8 zurückgesetzten Server nicht mehr vorhanden sind. Die Wiederherstellungsmaßnahmen sind vom Typ des Speicherpools abhängig:
  - Wurden Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, wurde der von den versetzten Daten belegte Speicherplatz wahrscheinlich wiederverwendet. Daher müssen Sie die ursprünglichen Speicherpools der Version 8 mithilfe der Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.2 erstellt wurden.

    Wurden *keine* Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, müssen Sie die Speicherpooldatenträger in diesen Speicherpools des Typs DISK prüfen.

  - Wurden Daten aus Speicherpools mit sequenziellem Zugriff der Version 8 in einen neuen Speicherpool versetzt, sind diese Daten möglicherweise noch vorhanden und sie können eventuell auf Speicherpooldatenträgern auf dem wiederhergestellten Server der Version 8 verwendet werden. Die Daten können verwendbar sein, wenn für den Parameter REUSEDELAY des Speicherpools ein Wert definiert wurde, der die Wiederherstellung verhindert hat, während der Server mit der Version 8.1.2 ausgeführt wurde. Wurden Datenträger wiederhergestellt, während der Server mit der Version 8.1.2 ausgeführt wurde, müssen Sie diese Datenträger aus Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.2 erstellt wurden.

AIX: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken

Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.

Zweck

Nach der Installation und Konfiguration von IBM Spectrum Protect mithilfe der Assistenten müssen Sie DB2-Befehle nur selten verwenden. Eine begrenzte Gruppe von DB2-Befehlen, die Sie verwenden bzw. zu deren Verwendung Sie aufgefordert werden könnten, ist in Tabelle 1 aufgelistet. Diese Liste ist nicht umfassend, es handelt sich lediglich um ergänzende Informationen. Es besteht keine Implikation, dass ein IBM Spectrum Protect-Administrator sie täglich oder regelmäßig verwendet. Beispiele einiger Befehle sind angegeben. Ausgabedaten sind nicht enthalten.

Vollständige Erläuterungen zu den hier beschriebenen Befehlen und zu deren Syntax finden Sie in der Produktinformation zu DB2.

Tabelle 1. DB2-Befehle

Befehl	Beschreibung	Beispiel

Befehl	Beschreibung	Beispiel
db2icrt	Erstellt DB2-Instanzen im Ausgangsverzeichnis des Instanzeigners. Tipp: Der IBM Spectrum Protect-Konfigurationsassistent erstellt die vom Server und von der Datenbank verwendete Instanz. Nach der Installation und Konfiguration eines Servers mithilfe des Konfigurationsassistenten wird der Befehl db2icrt in der Regel nicht verwendet.  AIX-BetriebssystemeDieses Dienstprogramm befindet sich im Verzeichnis DB2DIR/instance. Hierbei steht DB2DIR für das Installationsverzeichnis, in dem die aktuelle Version des DB2-Datenbanksystems installiert ist.	IBM Spectrum Protect-Instanz manuell erstellen (geben Sie den Befehl in einer einzigen Zeile ein): `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u` *`Instanzname Instanzname`*
db2set	Zeigt DB2-Variablen an.	DB2-Variablen auflisten: `db2set`
CATALOG DATABASE	Speichert Informationen zur Speicherposition der Datenbank im Systemdatenbankverzeichnis. Die Datenbank kann sich auf der lokalen Workstation oder auf einem fernen Datenbankpartitionsserver befinden. Der Serverkonfigurationsassistent kümmert sich um jeden Katalog, der zur Verwendung der Serverdatenbank benötigt wird. Führen Sie diesen Befehl nach der Konfiguration und Aktivierung eines Servers nur dann manuell aus, wenn es eine Änderung oder Beschädigung in der Umgebung gibt.	Datenbank katalogisieren: `db2 catalog database tsmdb1`
CONNECT TO DATABASE	Stellt eine Verbindung zu einer angegebenen Datenbank für Befehlszeilenschnittstellenzwecke her.	Eine Verbindung zur IBM Spectrum Protect-Datenbank über eine DB2-Befehlszeilenschnittstelle herstellen: `db2 connect to tsmdb1`

GET DATABASE CONFIGURATION	Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.
	Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.
		Die Konfigurationsdaten für einen Datenbankaliasnamen anzeigen:
		`db2 get db cfg for tsmdb1`
		
		Informationen abrufen, um Einstellungen zu überprüfen (z. B. Datenbankkonfiguration, Protokollmodus und Pflege).
		`db2 get db config for tsmdb1 show detail`

Befehl	Beschreibung	Beispiel
GET DATABASE MANAGER CONFIGURATION	Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück. Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.	Konfigurationsdaten für den Datenbankmanager abrufen: `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Ruft die Informationen zum Allgemeinzustand für den Datenbankmanager und seine Datenbanken ab. Die zurückgegebenen Informationen stellen eine Momentaufnahme des Status zum Zeitpunkt der Befehlsausgabe dar. IBM Spectrum Protect überwacht den Status der Datenbank mithilfe der Diagnosemomentaufnahme und anderer Mechanismen, die von DB2 bereitgestellt werden. Es kann vorkommen, dass die Diagnosemomentaufnahme oder andere DB2-Dokumentation anzeigt, dass sich ein Element bzw. eine Datenbankressource im Alertstatus befindet. In einem solchen Fall müssen entsprechende Schritte zur Behebung der Situation in Betracht gezogen werden. IBM Spectrum Protect überwacht die Bedingung und reagiert entsprechend. Nicht alle deklarierten Alerts der DB2-Datenbank haben Maßnahmen zur Folge.	Einen Bericht über Anzeiger des DB2-Diagnosemonitors abrufen: `db2 get health snapshot for database on tsmdb1`

GRANT (Datenbank-berechtigungen)	Erteilt Berechtigungen, die sich auf die gesamte Datenbank beziehen, und keine Zugriffsrechte, die sich auf bestimmte Objekte in der Datenbank beziehen.	Der Benutzer-ID itmuser Zugriffsberechtigung erteilen:
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

RUNSTATS	Aktualisiert statistische Daten zu den Merkmalen einer Tabelle und der zugeordneten Indizes oder Statistiksichten. Zu diesen Merkmalen gehören die Anzahl der Datensätze, die Anzahl der Seiten und die durchschnittliche Datensatzlänge. Soll eine Tabelle angezeigt werden, verwenden Sie dieses Dienstprogramm nach dem Aktualisieren oder Reorganisieren der Tabelle. Eine Sicht muss für die Optimierung aktiviert sein, damit ihre statistischen Daten für die Optimierung einer Abfrage verwendet werden können. Eine für die Optimierung aktivierte Sicht wird als Statistiksicht bezeichnet. Sie können eine Sicht mit der DB2-Anweisung ALTER VIEW für die Optimierung aktivieren. Verwenden Sie das Dienstprogramm RUNSTATS, wenn sich Änderungen zugrunde liegender Tabellen auf die von der Sicht zurückgegebenen Zeilen auswirken. Tipp: Der Server konfiguriert DB2 so, dass der Befehl RUNSTATS nach Bedarf ausgeführt wird.	Statistische Daten für eine einzelne Tabelle aktualisieren. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
SET SCHEMA	Ändert den Wert des Sonderregisters CURRENT SCHEMA als Vorbereitung für die direkte Ausgabe von SQL-Befehlen über die DB2-Befehlszeilenschnittstelle. Tipp: Ein Sonderregister ist ein Speicherbereich, den der Datenbankmanager für einen Anwendungsprozess definiert. In diesem Bereich werden Informationen gespeichert, auf die in SQL-Anweisungen verwiesen werden kann.	Das Schema für IBM Spectrum Protect festlegen: `db2 set schema tsmdb1`

Befehl	Beschreibung	Beispiel
START DATABASE MANAGER	Startet die Hintergrundprozesse der aktuellen Datenbankmanagerinstanz. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers. Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.	Den Datenbankmanager starten: `db2start`
STOP DATABASE MANAGER	Stoppt die aktuelle Datenbankmanagerinstanz. Der Datenbankmanager bleibt so lange aktiv, bis er explizit gestoppt wird. Dieser Befehl stoppt die Datenbankmanagerinstanz nicht, wenn Anwendungen mit Datenbanken verbunden sind. Liegen keine Datenbankverbindungen, aber Instanzverbindungen vor, erzwingt der Befehl zunächst das Stoppen der Instanzverbindungen. Dann wird der Datenbankmanager gestoppt. Dieser Befehl inaktiviert außerdem alle ausstehenden Datenbankaktivierungen, bevor der Datenbankmanager gestoppt wird. Dieser Befehl ist auf einem Client nicht gültig. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers. Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.	Den Datenbankmanager stoppen: `db2 stop dbm`

AIX: IBM Spectrum Protect deinstallieren

Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

Vorbereitende Schritte

Führen Sie folgende Schritte aus, bevor Sie IBM Spectrum Protect deinstallieren:

- Führen Sie eine Gesamtsicherung der Datenbank aus.
- Speichern Sie eine Kopie der Datenträgerhistory- und Einheitenkonfigurationsdateien.
- Bewahren Sie die Ausgabedatenträger an einem sicheren Ort auf.

Informationen zu diesem Vorgang

Sie können IBM Spectrum Protect mit jeder der folgenden Methoden deinstallieren: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

- AIX: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren
  Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.
- AIX: IBM Spectrum Protect im Konsolenmodus deinstallieren
  Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.
- AIX: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren
  Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.
- AIX: IBM Spectrum Protect deinstallieren und erneut installieren
  Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.
- AIX: IBM Installation Manager deinstallieren
  Sie können IBM Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

Nächste Schritte

Die Vorgehensweise für die Reinstallation der IBM Spectrum Protect-Komponenten finden Sie in AIX: Serverkomponenten installieren.

AIX: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren

Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.

Vorgehensweise

1. Starten Sie Installation Manager.
    AIX-BetriebssystemeIn dem Verzeichnis, in dem Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus:

   ```
   ./IBMIM
   ```

2. Klicken Sie auf Deinstallieren.
3. Wählen Sie IBM Spectrum Protect-Server aus und klicken Sie auf Weiter.
4. Klicken Sie auf Deinstallieren.
5. Klicken Sie auf Fertigstellen.

AIX: IBM Spectrum Protect im Konsolenmodus deinstallieren

Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.

Vorgehensweise

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
   -  AIX-Betriebssystemeeclipse/tools

   Beispiel:

   -  AIX-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus:
   -  AIX-Betriebssysteme`./imcl -c`
3. Für die Deinstallation geben Sie `5` ein.
4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
5. Geben Sie `N` für 'Next' (Weiter) ein.
6. Wählen Sie die Deinstallation des IBM Spectrum Protect-Serverpakets aus.
7. Geben Sie `N` für 'Next' (Weiter) ein.
8. Geben Sie `U` für 'Uninstall' (Deinstallieren) ein.
9. Geben Sie `F` für 'Finish' (Fertigstellen) ein.

AIX: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren

Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

Vorbereitende Schritte

Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation der IBM Spectrum Protect-Serverkomponenten mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, uninstall_response_sample.xml, im Verzeichnis input, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie alle IBM Spectrum Protect-Komponenten deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für jede Komponente in der Antwortdatei unverändert. Wenn Sie eine Komponente nicht deinstallieren wollen, geben Sie den Wert `modify="true"` an.

Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
   -  AIX-Betriebssystemeeclipse/tools

   Beispiel:

   -  AIX-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:
    AIX-Betriebssysteme

   ```
   ./imcl -input Antwortdatei -silent
   ```

   Der folgende Befehl ist ein Beispiel:

    AIX-Betriebssysteme

```
./imcl -input /tmp/input/uninstall_response.xml -silent
```

AIX: IBM Spectrum Protect deinstallieren und erneut installieren

Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um IBM Spectrum Protect manuell zu deinstallieren und erneut zu installieren:

1. AIX-BetriebssystemeErstellen Sie eine Liste Ihrer aktuellen Serverinstanzen, bevor Sie mit der Deinstallation beginnen. Führen Sie den folgenden Befehl aus:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

2. Führen Sie die folgenden Befehle für jede Serverinstanz aus:
   AIX-Betriebssysteme

   ```
   db2 attach to Instanzname
   db2 get dbm cfg show detail
   db2 detach
   ```

   Notieren Sie den Datenbankpfad für jede Instanz.
3. Deinstallieren Sie IBM Spectrum Protect. Siehe AIX: IBM Spectrum Protect deinstallieren.
4. Wenn Sie eine beliebige unterstützte Version von IBM Spectrum Protect deinstallieren (einschließlich Fixpack), wird eine Instanzdatei erstellt. Die Instanzdatei wird erstellt, um die Reinstallation von IBM Spectrum Protect zu erleichtern. Überprüfen Sie diese Datei und verwenden Sie die Informationen, wenn Sie bei der Reinstallation zur Eingabe der Berechtigungsnachweise der Instanz aufgefordert werden. Bei der unbeaufsichtigten Installation geben Sie diese Berechtigungsnachweise mit der Variablen `INSTANCE_CRED` an.
   Sie finden die Instanzdatei an der folgenden Position:
   - AIX-Betriebssysteme/etc/tivoli/tsm/instanceList.obj
5. Installieren Sie IBM Spectrum Protect erneut. Siehe AIX: Serverkomponenten installieren.

   Ist die Datei `instanceList.obj` nicht vorhanden, müssen Sie Ihre Serverinstanzen wie folgt erneut erstellen:

   a. Erstellen Sie Ihre Serverinstanzen erneut. Siehe AIX: Serverinstanz erstellen.
      Tipp: Der Installationsassistent konfiguriert die Serverinstanzen, Sie müssen jedoch überprüfen, ob sie vorhanden sind. Wenn sie nicht vorhanden sind, müssen Sie sie manuell konfigurieren.
   b. Katalogisieren Sie die Datenbank. Melden Sie sich bei jeder Serverinstanz nacheinander als Instanzbenutzer an und geben Sie folgende Befehle aus:
      AIX-Betriebssysteme

      ```
      db2 catalog database tsmdb1
      db2 attach to Instanzname
      db2 update dbm cfg using dftdbpath Instanzverzeichnis
      db2 detach
      ```

   c. AIX-BetriebssystemeÜberprüfen Sie, ob die Serverinstanz erfolgreich erstellt wurde. Geben Sie den folgenden Befehl aus:

      ```
      /opt/tivoli/tsm/db2/instance/db2ilist
      ```

   d. Überprüfen Sie, ob IBM Spectrum Protect die Serverinstanz erkennt, indem Sie Ihre Verzeichnisse auflisten. Ihr Ausgangsverzeichnis wird angezeigt, wenn Sie es nicht geändert haben. Ihr Instanzverzeichnis wird angezeigt, wenn Sie den Konfigurationsassistenten verwendet haben. Geben Sie den folgenden Befehl aus:

      ```
      db2 list database directory
      ```

      Wenn Sie TSMDB1 in der Liste finden, können Sie den Server starten.

AIX: IBM Installation Manager deinstallieren

Sie können IBM® Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

Vorbereitende Schritte

Bevor Sie IBM Installation Manager deinstallieren, müssen Sie sicherstellen, dass alle mit IBM Installation Manager installierten Pakete deinstalliert sind. Schließen Sie IBM Installation Manager, bevor Sie den Deinstallationsprozess starten.

AIX-BetriebssystemeGeben Sie den folgenden Befehl in eine Befehlszeile ein, um installierte Pakete anzuzeigen:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

Vorgehensweise

Gehen Sie wie folgt vor, um IBM Installation Manager zu deinstallieren:

 AIX-Betriebssysteme

1. Öffnen Sie eine Befehlszeile und wechseln Sie in das Verzeichnis /var/ibm/InstallationManager/uninstall.
2. Geben Sie den folgenden Befehl aus:

   ```
   ./uninstall
   ```

   Einschränkung: Sie müssen mit der Benutzer-ID `root` am System angemeldet sein.

Linux: Server installieren

Zur Installation des Servers gehören Planung, Installation und Erstkonfiguration.

- Linux
- Linux: Installation des Servers planen
  Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.
- Linux: Serverkomponenten installieren
  Für die Installation der Serverkomponenten der Version 8.1.2 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.
- Linux: Die ersten Schritte nach der Installation von IBM Spectrum Protect
  Nach der Installation von Version 8.1.2 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.
- Linux: IBM Spectrum Protect-Server-Fixpack installieren
  IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.
- Linux: Von Version 8.1.2 auf eine vorherige Serverversion zurücksetzen
  Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.
- Linux: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken
  Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.
- Linux: IBM Spectrum Protect deinstallieren
  Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

Linux: Installation des Servers planen

Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.

- Linux: Vorausgesetzte Kenntnisse
  Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.
- Linux: Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten
  Lesen Sie vor der Installation von IBM Spectrum Protect Version 8.1.2 oder höher die Informationen über die erweiterten Sicherheitsfunktionen und die Voraussetzungen für eine Aktualisierung Ihrer Umgebung.
- Linux: Planung für optimale Leistung
  Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.
-  Linux-BetriebssystemeLinux: Systemmindestvoraussetzungen für Linux-Systeme
  Für die Installation des IBM Spectrum Protect-Servers auf einem Linux-System wird ein Minimum an Hardware und Software benötigt. Hierzu gehören eine Übertragungsmethode und der aktuelle Einheitentreiber.
-  Linux-BetriebssystemeLinux: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System
  Sie können andere Produkte, die DB2-Produkte auf demselben System wie der IBM Spectrum Protect-Server der Version 8.1.2 implementieren und verwenden, mit einigen Einschränkungen installieren.
- Linux: IBM Installation Manager
  IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.
- Linux: Arbeitsblätter für Planungsdetails für den Server
  Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers

verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.

- Linux: Kapazitätsplanung
  Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.
- Linux: Empfehlungen für die Serverbenennung
  Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.
- Linux: Installationsverzeichnisse
  Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

Linux: Vorausgesetzte Kenntnisse

Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.

Wartungsreleases, Client-Software und Veröffentlichungen für den Server stehen im IBM® Support Portal zur Verfügung.

 Linux-BetriebssystemeEinschränkung: Sie können den Server der Version 8.1.2 mit einigen Einschränkungen auf einem System installieren und ausführen, auf dem bereits DB2 installiert ist. Das gilt unabhängig davon, ob DB2 separat oder als Teil einer anderen Anwendung installiert wurde. Ausführliche Informationen finden Sie in dem Abschnitt über die Kompatibilität mit anderen DB2-Produkten.

Erfahrene DB2-Administratoren können erweiterte SQL-Abfragen durchführen und mithilfe von DB2-Tools die Datenbank überwachen. Sie dürfen die DB2-Tools jedoch nicht zur Änderung der von IBM Spectrum Protect vorgegebenen DB2-Konfigurationseinstellungen verwenden oder die DB2-Umgebung für IBM Spectrum Protect auf andere Weise ändern (z. B. mit anderen Produkten). Der Server der Version 8.1.2 wurde mit der Datendefinitionssprache (DDL) und der vom Server implementierten Datenbankkonfiguration erstellt und ausführlich getestet.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

Linux: Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten

Lesen Sie vor der Installation von IBM Spectrum Protect Version 8.1.2 oder höher die Informationen über die erweiterten Sicherheitsfunktionen und die Voraussetzungen für eine Aktualisierung Ihrer Umgebung.

Informationen zu diesem Vorgang

Die in Version 8.1.2 und höheren Versionen eingeführten Sicherheitserweiterungen setzen strengere Sicherheitseinstellungen durch. Führen Sie die Prozedur aus, um sicherzustellen, dass die Kommunikation zwischen Servern und Clients bei einer Installation oder einem Upgrade der IBM Spectrum Protect-Software auf Version 8.1.2 nicht unterbrochen wird.

Vorgehensweise

1. Führen Sie die Installation bzw. das Upgrade der IBM Spectrum Protect-Server mit Version 8.1.2 oder höher durch.
2. Führen Sie die Installation bzw. das Upgrade der Clients für Sichern/Archivieren durch. Weitere Informationen finden Sie in Clients installieren und konfigurieren.
   Informationen zur Planung der Implementierung von Clientaktualisierungen auf dem Server finden Sie in den folgenden Dokumenten:
   - Für Server mit IBM Spectrum Protect Version 8.1.2 oder einer höheren Version: Technote 2004596.
   - Für Server mit IBM® Tivoli Storage Manager Version 7.1 und IBM Spectrum Protect Version 8.1.0 und 8.1.1: Technote 1673299.
3. Konfigurieren Sie die Optionen für Clients für Sichern/Archivieren. Weitere Informationen finden Sie in Upgrade des IBM Spectrum Protect-Servers und des IBM Spectrum Protect-Clients durchführen.

Linux: Planung für optimale Leistung

Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.

Vorgehensweise

1. Lesen Sie den Abschnitt Linux: Vorausgesetzte Kenntnisse.
2. Lesen Sie jeden der folgenden Unterabschnitte.

- Linux: Planung für die Server-Hardware und das Betriebssystem
  Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- Linux: Planung für Platten für die Serverdatenbank
  Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- Linux: Planung für Platten für das Serverwiederherstellungsprotokoll
  Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- Linux: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools
  Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.
- Linux: Planung für Speicherpools auf DISK- oder FILE-Einheiten
  Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.
- Linux: Planung für die Auswahl des korrekten Speichertechnologietyps
  Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.
- Linux: Bewährte Verfahren bei der Serverinstallation anwenden
  Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

Linux: Planung für die Server-Hardware und das Betriebssystem

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Werden die Betriebssystem- und Hardwarevoraussetzungen erfüllt oder mehr als erfüllt? • Anzahl und Geschwindigkeit der Prozessoren • Systemspeicher • Unterstützte Betriebssystemversion	Wenn Sie die erforderliche Mindestspeicherkapazität verwenden, können Sie eine minimale Arbeitslast unterstützen. Sie können versuchsweise mehr Systemspeicher hinzufügen, um bestimmen zu können, ob sich die Leistung verbessert. Entscheiden Sie dann, ob der Systemspeicher dem Server zugeordnet bleiben soll. Testen Sie die verschiedenen Speicherkapazitäten jeweils anhand des gesamten Tageszyklus der Serverlast. Wenn Sie mehrere Server auf dem System ausführen, addieren Sie die Voraussetzungen für jeden Server, um die Voraussetzungen für das System zu bestimmen.	Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309. Lesen Sie außerdem die Anweisungen in Tasks für Betriebssysteme und andere Anwendungen optimieren. Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation Weitere Informationen zu Anforderungen in Bezug auf die Größe des Servers und des Speichers finden Sie im IBM Spectrum Protect-Blueprint.
Sind Platten für die optimale Leistung konfiguriert?	Der Umfang der Optimierung, der für verschiedene Plattensysteme erfolgen kann, variiert. Stellen Sie sicher, dass die Warteschlangenlänge und andere Plattensystemoptionen entsprechend definiert sind.	Weitere Informationen finden Sie in: • "Planung für Platten für die Serverdatenbank" • "Planung für Platten für das Serverwiederherstellungsprotokoll" • "Planung für Speicherpools auf DISK- oder FILE-Einheiten"

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verfügt der Server über genügend Speicher?	Höhere Arbeitslasten und erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation erfordern mehr Systemspeicher als den Mindestspeicher, der im Dokument mit den Systemvoraussetzungen angegeben ist. Verwenden Sie die folgenden Richtlinien, um den Speicherbedarf für Datenbanken anzugeben, die nicht für die Datendeduplizierung aktiviert sind: • Für Datenbanken mit einer Größe unter 500 GB benötigen Sie 16 GB Speicher. • Für Datenbanken mit einer Größe von 500 GB bis 1 TB benötigen Sie 24 GB Speicher. • Für Datenbanken mit einer Größe von 1 TB bis 1,5 TB benötigen Sie 32 GB Speicher. • Für Datenbanken mit einer Größe über 1,5 TB benötigen Sie 40 GB Speicher. Stellen Sie sicher, dass Sie für die Replikationsverarbeitung zusätzlichen Speicherbereich für die aktive Protokolldatei und das Archivprotokoll zuordnen.	Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation • Speicherbedarf
Verfügt das System über genügend Hostbusadapter (HBAs), um die Datenoperationen, die der IBM Spectrum Protect-Server gleichzeitig ausführen muss, handhaben zu können?	Sie müssen wissen, für welche Operationen die gleichzeitige Verwendung von Hostbusadaptern erforderlich ist. Ein Server muss beispielsweise Sicherungsdaten mit 1 GB/s speichern, während er gleichzeitig eine Speicherpoolumlagerung ausführt, für deren Ausführung eine Kapazität von 0,5 GB/s erforderlich ist. Die Hostbusadapter müssen alle Daten mit der erforderlichen Geschwindigkeit handhaben können.	Siehe HBA-Kapazität optimieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Ist die Netzbandbreite größer als der geplante maximale Durchsatz für Sicherungen?	Die Netzbandbreite muss dem System die Ausführung von Operationen wie Sicherungen innerhalb der zulässigen Zeit oder gemäß den vereinbarten Service-Levels ermöglichen. Bei der Knotenreplikation muss die Netzbandbreite größer als der geplante maximale Durchsatz sein.	Weitere Informationen finden Sie in: • Netzleistung optimieren • Prüfliste für Knotenreplikation

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Verwenden Sie ein bevorzugtes Dateisystem für IBM Spectrum Protect-Serverdateien?	Verwenden Sie ein Dateisystem, das optimale Leistung und Datenverfügbarkeit gewährleistet. Der Server verwendet die direkte E/A mit Dateisystemen, die die Funktion unterstützen. Die Verwendung der direkten E/A kann den Durchsatz verbessern und die Prozessornutzung verringern. Die folgende Liste zeigt das jeweils bevorzugte Dateisystem:
	  Linux-
	• Betriebssysteme Verwenden Sie das ext3-, ext4- oder xfs-Dateisystem für die Datenbank, für das Wiederherstellungsprotokoll und für Speicherpooldaten. Verwenden Sie das folgende für Ihr Betriebssystem und Ihre Betriebssystemversion geeignete Dateisystem:
	  ◦ Verwenden Sie für Red Hat Enterprise Linux x86_64 das ext3-, ext4- oder xfs-Dateisystem. Wenn Red Hat Enterprise Linux 6.4 oder höher installiert ist, verwenden Sie das ext4- oder xfs-Dateisystem.
	  ◦ Verwenden Sie für SUSE Linux Enterprise Server und für Red Hat Enterprise Linux ppc64 das ext3- oder xfs-Dateisystem. Für die Verwendung von xfs unter SUSE Linux Enterprise Server 12 ist kernel-default-3.12.32-33.1.x86_64.rpm oder höher erforderlich.
		Weitere Informationen finden Sie in Betriebssystem für die Plattenleistung konfigurieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Planen Sie, genügend Seitenauslagerungsbereich zu konfigurieren?	Seitenauslagerungsbereich (oder Auslagerungsspeicher) erweitert den Speicher, der für die Verarbeitung verfügbar ist. Wenn der freie Arbeitsspeicher im System knapp wird, werden Programme oder Daten, die nicht im Gebrauch sind, aus dem Speicher in den Seitenauslagerungsbereich versetzt. Mit dieser Aktion wird Speicherbereich für andere Aktivitäten, wie z. B. Datenbankoperationen, freigegeben. Linux-Betriebssysteme Verwenden Sie den größeren der beiden folgenden Werte: mindestens 32 GB Seitenauslagerungsbereich oder 50 % des Arbeitsspeichers.	
Linux-Betriebssysteme Planen Sie, nach der Installation des Servers die Kernelparameter zu optimieren?	Linux-BetriebssystemeSie müssen Kernelparameter optimieren.	Linux-BetriebssystemeInformationen zur Optimierung von Kernelparametern finden Sie in Linux: Kernelparameter für Linux-Systeme optimieren.

Linux: Planung für Platten für die Serverdatenbank

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Befindet sich die Datenbank auf schnellen Platten mit kurzer Latenzzeit?	Verwenden Sie die folgenden Laufwerke nicht für die IBM Spectrum Protect-Datenbank: • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) Verwenden Sie keine internen Platten, die standardmäßig Teil der Hardware der meisten Server ist. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung. Wenn Sie planen, die Datendeduplizierungsfunktionen von IBM Spectrum Protect zu verwenden, legen Sie den Schwerpunkt auf die Plattenleistung (gemessen in E/A-Operationen pro Sekunde).	Weitere Informationen finden Sie in Prüfliste für Datendeduplizierung.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Ist die Datenbank auf anderen Platten oder LUNs gespeichert als die aktive Protokolldatei, das Archivprotokoll und die Speicherpooldatenträger?	Das Trennen der Serverdatenbank von anderen Serverkomponenten trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei. Tipp: Die Datenbank und das Archivprotokoll können ein Array gemeinsam nutzen, wenn Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) verwenden.	
Wissen Sie bei Verwendung von RAID, wie die optimale RAID-Stufe für Ihr System ausgewählt wird? Definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ?	Wenn ein System viele Schreibvorgänge ausführen muss, ist die Leistung bei RAID 10 besser als bei RAID 5. RAID 10 benötigt jedoch mehr Platten als RAID 5, um dieselbe nutzbare Speichermenge bereitzustellen. Handelt es sich bei Ihrem Plattensystem um ein RAID-System, definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ. Verwenden Sie beispielsweise nicht gleichzeitig 4+1 RAID 5 mit 4+2 RAID 6.	
Planen Sie, wenn eine Option zum Definieren der Stripgröße oder der Segmentgröße verfügbar ist, die Größe beim Konfigurieren des Plattensystems zu optimieren?	Wenn Sie die Stripgröße oder Segmentgröße definieren können, verwenden Sie auf Plattensystemen für die Datenbank Größen von 64 KB oder 128 KB.	Die Blockgröße, die für die Datenbank verwendet wird, variiert abhängig vom Tabellenbereich. Die meisten Tabellenbereiche verwenden 8-KB-Blöcke; einige verwenden jedoch 32-KB-Blöcke.
Planen Sie, mindestens vier Verzeichnisse, die auch als Speicherpfade bezeichnet werden, auf vier verschiedenen LUNs für die Datenbank zu erstellen? Erstellen Sie exakt ein Verzeichnis pro Array in dem Subsystem. Wenn weniger als drei Arrays vorhanden sind, erstellen Sie in jedem Array einen anderen LUN-Datenträger.	Für größere Arbeitslasten und bei Verwendung einiger Funktionen sind mehr Datenbankspeicherpfade als die Mindestvoraussetzungen erforderlich. Serveroperationen wie die Datendeduplizierung verursachen eine hohe Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS) für die Datenbank. Die Leistung derartiger Operationen ist besser, wenn die Datenbank über mehr Verzeichnisse verfügt. Verwenden Sie für Serverdatenbanken, die größer als 2 TB sind oder die wahrscheinlich auf diese Größe anwachsen, acht Verzeichnisse. Berücksichtigen Sie das geplante Wachstum des Systems bei der Bestimmung der Anzahl zu erstellender Speicherpfade. Die höhere Anzahl Speicherpfade wird vom Server effizienter genutzt, wenn die Speicherpfade bei der Ersterstellung des Servers bereits vorhanden sind. Verwenden Sie die Variable *DB2_PARALLEL_IO*, um die parallele E/A für Tabellenbereiche mit einem einzelnen Container zu erzwingen oder für Tabellenbereiche, die über Container auf mehr als einer physischen Platte verfügen. Wenn Sie die Variable *DB2_PARALLEL_IO* nicht definieren, entspricht die E/A-Parallelität der Anzahl Container, die von dem Tabellenbereich verwendet werden. Wenn ein Tabellenbereich beispielsweise vier Container umfasst, beträgt der verwendete Grad an E/A-Parallelität 4.	Weitere Informationen finden Sie in: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation Hilfreiche Informationen zur Vorhersage des Wachstums beim Deduplizieren von Daten durch den Server finden Sie in Technote 1596944. Aktuelle Informationen zur Datenbankgröße, zur Datenbankreorganisation und zu Leistungsaspekten für IBM Spectrum Protect-Server finden Sie in Technote 1683633. Informationen zum Definieren der Variable *DB2_PARALLEL_IO* finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben alle Verzeichnisse für die Datenbank dieselbe Größe?	Verzeichnisse, die alle dieselbe Größe haben, stellen einen konsistenten Grad an Parallelität für Datenbankoperationen sicher. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als andere sind, verringert sich dadurch das Potenzial für den optimierten parallelen Vorablesezugriff. Diese Richtlinie gilt auch, wenn Sie nach der Erstkonfiguration des Servers Speicherpfade hinzufügen müssen.	
Planen Sie, die Warteschlangenlänge der Datenbank-LUNs auf AIX-Systemen zu erhöhen?	Die Standardwarteschlangenlänge ist häufig zu niedrig definiert.	Siehe AIX-Systeme für die Plattenleistung konfigurieren.

Linux: Planung für Platten für das Serverwiederherstellungsprotokoll

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Sind die aktive Protokolldatei und das Archivprotokoll auf anderen Platten oder LUNs gespeichert als die Datenbank und die Speicherpooldatenträger?	Stellen Sie sicher, dass die Platten, auf die die aktive Protokolldatei gestellt wird, auf dem Server oder System nicht für andere Zwecke verwendet werden. Stellen Sie die aktive Protokolldatei nicht auf Platten, die die Serverdatenbank, das Archivprotokoll oder Systemdateien, wie Seitenauslagerungsbereich oder Auslagerungsspeicher, enthalten.	Das Trennen der Serverdatenbank von der aktiven Protokolldatei und dem Archivprotokoll trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.
Befinden sich die Protokolle auf Platten mit nicht flüchtigem Schreibcache?	Nicht flüchtiger Schreibcache ermöglicht es, Daten so schnell wie möglich in die Protokolle zu schreiben. Schnellere Schreiboperationen für die Protokolle können die Leistung für Serveroperationen verbessern.	
Legen Sie für die Protokolle eine Größe fest, die der Arbeitslast entspricht?	Wenn Sie sich über die Arbeitslast im Unklaren sind, verwenden Sie die größtmögliche Größe. Aktive Protokolldatei Die maximale Größe beträgt 512 GB; sie wird über die Serveroption ACTIVELOGSIZE festgelegt. Stellen Sie sicher, dass mindestens 8 GB freier Speicherbereich im Dateisystem für aktive Protokolldateien verfügbar sind, nachdem die aktiven Protokolldateien mit fester Größe erstellt wurden. Archivprotokoll Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Das Archivprotokoll muss mindestens so groß wie die aktive Protokolldatei sein.	• Ausführliche Informationen zur Festlegung der Protokollgröße enthalten die Informationen zum Wiederherstellungsprotokoll in Technote 1421060. • Informationen zur Festlegung der Größe bei Verwendung der Datendeduplizierung finden Sie in Prüfliste für Datendeduplizierung.
Definieren Sie ein Archivübernahmeprotokoll ? Stellen Sie dieses Protokoll auf eine andere Platte als das Archivprotokoll?	Das Archivübernahmeprotokoll dient der Verwendung durch den Server im Notfall, wenn das Archivprotokoll voll ist. Für das Archivübernahmeprotokoll können langsamere Platten verwendet werden.	Geben Sie die Position des Archivübernahmeprotokolls mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY an. Überwachen Sie die Belegung des Verzeichnisses für das Archivübernahmeprotokoll. Wenn das Archivübernahmeprotokoll vom Server verwendet werden muss, ist der Speicherplatz für das Archivprotokoll möglicherweise nicht groß genug.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verwenden Sie, wenn Sie die aktive Protokolldatei spiegeln, nur einen einzigen Typ von Spiegelung?	Sie können das Protokoll mithilfe einer der folgenden Methoden spiegeln. Verwenden Sie für das Protokoll nur einen einzigen Typ von Spiegelung. • Verwenden Sie die Option MIRRORLOGDIRECTORY, die für den IBM Spectrum Protect-Server verfügbar ist, um eine Position für die Spiegelung anzugeben. • Verwenden Sie die Softwarespiegelung, wie z. B. Logical Volume Manager (LVM) unter AIX. • Verwenden Sie die Spiegelung in der Hardware des Plattensystems.	Stellen Sie, wenn Sie die aktive Protokolldatei spiegeln, sicher, dass die Platten für die aktive Protokolldatei und die Spiegelkopie dieselbe Geschwindigkeit und Zuverlässigkeit haben. Weitere Informationen finden Sie in Wiederherstellungsprotokoll konfigurieren und optimieren.

Linux: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools

Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verwenden Sie, gemessen in Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS), schnellen Plattenspeicher für die IBM Spectrum Protect-Datenbank?	Verwenden Sie eine Hochleistungsplatte für die Datenbank. Verwenden Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) für die Datendeduplizierungsverarbeitung. Stellen Sie sicher, dass die Datenbank über eine Mindestkapazität von 3000 E/A-Operationen pro Sekunde (IOPS) verfügt. Addieren Sie zu diesem Mindestwert pro TB Daten, die täglich (vor der Datendeduplizierung) gesichert werden, 1000 E/A-Operationen pro Sekunde. Beispielsweise würde ein IBM Spectrum Protect-Server, der täglich 3 TB Daten aufnimmt, 6000 E/A-Operationen pro Sekunde (IOPS) für die Datenbankplatten benötigen: `mindestens 3000 IOPS + 3000 (3 TB x 1000 IOPS) = 6000 IOPS`	Empfehlungen zur Plattenauswahl finden Sie in "Planung für Platten für die Serverdatenbank". Weitere Informationen zu IOPS finden Sie in den IBM Spectrum Protect-Blueprints.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Ist genügend Speicherplatz für die Größe Ihrer Datenbank vorhanden?	Verwenden Sie mindestens 40 GB Systemspeicher für IBM Spectrum Protect-Server, die Daten deduplizieren, mit einer Datenbankgröße von 100 GB. Wenn die Speicherkapazität für Sicherungsdaten wächst, ist unter Umständen ein höherer Speicherbedarf erforderlich. Überwachen Sie regelmäßig die Speicherbelegung, um festzustellen, ob mehr Speicherplatz erforderlich ist. Verwenden Sie weiteren Systemspeicher, um das Caching von Datenbankseiten zu verbessern. Die folgenden Richtlinien für die Speichergröße basieren auf dem Volumen an neuen Daten, das jeden Tag gesichert wird: • 128 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 1 und 2 TB liegt • 192 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 2 und 4 TB liegt	Speicherbedarf
Haben Sie die Speicherkapazität für die die aktive Protokolldatei und das Archivprotokoll der Datenbank korrekt festgelegt?	Geben Sie in der Konfiguration des Servers eine minimale Größe von 128 GB für die aktive Protokolldatei an, indem Sie die Serveroption ACTIVELOGSIZE auf den Wert 131072 setzen. Als Anfangsgröße für das Archivprotokoll wird eine Größe von 1 TB vorgeschlagen. Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Stellen Sie sicher, dass im Vergleich zur Größe des Archivprotokolls mindestens 10 % zusätzlicher Plattenspeicher für das Dateisystem vorhanden sind. Verwenden Sie für die Datenbankarchivprotokolle ein Verzeichnis mit einer anfänglichen freien Kapazität von mindestens 1 TB. Geben Sie das Verzeichnis mithilfe der Serveroption ARCHLOGDIRECTORY an. Definieren Sie Speicherbereich für das Archivübernahmeprotokoll mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY.	Weitere Informationen zur Kapazitätsermittlung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.
Ist die Komprimierung für die Archivprotokoll- und Datenbanksicherungen aktiviert?	Aktivieren Sie die Serveroption ARCHLOGCOMPRESS, um Speicherbereich einzusparen. Diese Komprimierungsoption unterscheidet sich von der Inline-Komprimierung. Die Inline-Komprimierung ist ab IBM Spectrum Protect Version 7.1.5 und höher standardmäßig aktiviert. Einschränkung: Sie dürfen diese Option nicht verwenden, wenn das Volumen der pro Tag gesicherten Daten 6 TB überschreitet.	Weitere Informationen zur Komprimierung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Befinden sich die Datenbank und Protokolle von IBM Spectrum Protect auf separaten Plattendatenträgern (LUNs)? Ist der Datenträger, der für die Datenbank verwendet wird, gemäß den bewährten Verfahren für eine transaktionsorientierte Datenbank konfiguriert?	Die Datenbank darf keine Plattendatenträger mit IBM Spectrum Protect-Datenbankprotokollen oder -Speicherpools oder mit einer anderen Anwendung oder einem anderen Dateisystem gemeinsam nutzen.	Weitere Informationen zur Konfiguration der Serverdatenbank und des Wiederherstellungsprotokolls finden Sie in Konfiguration und Optimierung der Serverdatenbank und des Wiederherstellungsprotokolls.
Verwenden Sie mindestens acht Prozessorkerne (2,2-GHz-Prozessorkerne oder entsprechende Prozessorkerne) für jeden IBM Spectrum Protect-Server, der mit Datendeduplizierung verwendet werden soll?	Wenn die clientseitige Datendeduplizierung verwendet werden soll, müssen Sie sicherstellen, dass für Clientsysteme während einer Sicherungsoperation genügend Ressourcen zur Ausführung der Datendeduplizierungsverarbeitung verfügbar sind. Verwenden Sie pro Sicherungsprozess mit clientseitiger Datendeduplizierung einen Prozessor, der mindestens einem 2,2-GHz-Prozessorkern entspricht.	• Effektive Planung und Verwendung der Deduplizierung • IBM Spectrum Protect Blueprints
Haben Sie genügend Speicherplatz für die Datenbank zugeordnet?	Als grobe Schätzung sollten Sie 100 GB Datenbankspeicher für jeweils 50 TB Daten einplanen, die in deduplizierten Speicherpools geschützt werden sollen. *Geschützte Daten* ist das Datenvolumen vor der Datendeduplizierung, einschließlich aller Versionen gespeicherter Objekte. Als bewährtes Verfahren sollten Sie einen neuen Containerspeicherpool ausschließlich für die Datendeduplizierung definieren. Die Datendeduplizierung erfolgt auf der Speicherpoolebene; mit Ausnahme von verschlüsselten Daten werden alle Daten in einem Speicherpool dedupliziert.	
Haben Sie die Speicherpoolkapazität geschätzt, um genügend Speicherplatz für die Größe Ihrer Umgebung zu konfigurieren?	Sie können den Kapazitätsbedarf für einen deduplizierten Speicherpool wie folgt schätzen: 1. Schätzen Sie die Basisgröße der Quellendaten. 2. Schätzen Sie die Größe der täglichen Sicherung anhand einer geschätzten Änderungs- und Wachstumsrate. 3. Bestimmen Sie die Anforderungen in Bezug auf die Aufbewahrungsdauer. 4. Schätzen Sie das Gesamtvolumen an Quellendaten unter Berücksichtigung der Basisgröße, der Größe der täglichen Sicherung und der Anforderungen in Bezug auf die Aufbewahrungsdauer. 5. Wenden Sie den Faktor für das Deduplizierungsverhältnis an. 6. Wenden Sie den Faktor für das Komprimierungsverhältnis an. 7. Runden Sie die Schätzung auf, um die Nutzung transienter Speicherpools zu berücksichtigen.	Ein Beispiel zur Verwendung dieses Verfahrens finden Sie in Effektive Planung und Verwendung der Deduplizierung.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie die Platten-E/A auf viele Platteneinheiten und Controller verteilt?	Verwenden Sie Arrays, die aus so vielen Platten wie möglich bestehen; dies wird auch als "Wide-Striping" bezeichnet. Stellen Sie sicher, dass Sie exakt ein Datenbankverzeichnis pro Array in dem Subsystem verwenden. Definieren Sie die Registry-Variable *DB2_PARALLEL_IO*, um die parallele E/A für jeden verwendeten Tabellenbereich zu aktivieren, wenn sich die Container in dem Tabellenbereich über mehrere physische Platten erstrecken. Wenn E/A-Bandbreite verfügbar ist und die Dateien groß sind (beispielsweise 1 MB), kann der Prozess zur Suche nach Duplikaten die Ressourcen eines gesamten Prozessors in Anspruch nehmen. Wenn Dateien kleiner sind, können andere Engpässe auftreten. Geben Sie acht oder mehr Dateisysteme für die Einheitenklasse des deduplizierten Speicherpools an, damit die Ein-/Ausgabe auf so viele LUNs und physische Einheiten wie möglich verteilt wird.	Richtlinien zur Konfiguration von Speicherpools finden Sie in "Planung für Speicherpools auf DISK- oder FILE-Einheiten". Informationen zum Definieren der Variable *DB2_PARALLEL_IO* finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.
Haben Sie tägliche Operationen auf der Basis Ihrer Sicherungsstrategie geplant?	Die Operationsfolge sieht gemäß den bewährten Verfahren wie folgt aus: 1. Clientsicherung 2. Speicherpoolschutz 3. Knotenreplikation 4. Datenbanksicherung 5. Bestandsverfall	• Datendeduplizierungs- und Knotenreplikationsprozesse planen • Tägliche Operation für Verzeichniscontainerspeicherpools
Ist genügend Speicher zur Verwaltung der DB2-Sperrenliste vorhanden?	Wenn Sie Daten deduplizieren, die große Dateien oder gleichzeitig eine große Anzahl Dateien umfassen, kann der Prozess zur Speicherknappheit führen. Wenn der Sperrenlistenspeicher nicht ausreichend ist, können Sicherungsfehler, Datenverwaltungsprozessfehler oder Serverausfälle auftreten. Bei Dateigrößen über 500 GB, die durch die Datendeduplizierung verarbeitet werden, ist es sehr wahrscheinlich, dass der Speicherplatz knapp wird. Wenn jedoch viele Sicherungsoperationen die clientseitige Datendeduplizierung verwenden, kann dieses Problem auch bei Dateien mit geringerer Größe auftreten.	Informationen zur Optimierung des DB2-Parameters LOCKLIST finden Sie in Serverseitige Datendeduplizierung optimieren.
Ist genügend Bandbreite verfügbar, um Daten auf einen IBM Spectrum Protect-Server zu übertragen?	Um Daten auf einen IBM Spectrum Protect-Server zu übertragen, verwenden Sie die clientseitige oder serverseitige Datendeduplizierung und die Komprimierung, um die erforderliche Bandbreite zu verringern. Verwenden Sie einen Server der Version 7.1.5 oder höher, um die Inline-Komprimierung verwenden zu können, und einen Client der Version 7.1.6 oder höher, um die erweiterte Komprimierungsverarbeitung zu aktivieren.	Weitere Informationen finden Sie in der Beschreibung der Clientoption enablededup.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie festgelegt, wie viele Speicherpoolverzeichnisse jedem Speicherpool zugeordnet werden sollen?	Ordnen Sie Verzeichnisse einem Speicherpool mithilfe des Befehls DEFINE STGPOOLDIRECTORY zu. Erstellen Sie mehrere Speicherpoolverzeichnisse und stellen Sie sicher, dass jedes Verzeichnis auf einem anderen Plattendatenträger (LUN) gesichert wird.	
Haben Sie genügend Plattenspeicherplatz in dem Cloud-Containerspeicherpool zugeordnet?	Um Sicherungsfehler zu verhindern, stellen Sie sicher, dass das lokale Verzeichnis über genügend Speicherplatz verfügt. Verwenden Sie die folgende Liste als Leitfaden für optimalen Plattenspeicherplatz: • Berechnen Sie für SAS-Platten (SAS = Serial-Attached SCSI) und rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu. • Stellen Sie 3 TB für flash-basierte Speichersysteme mit schnellen Netzverbindungen zu leistungsfähigen On-Premises-Cloudsystemen bereit. • Stellen Sie 5 TB für Systeme mit Solid-State-Laufwerk (SSD) mit schnellen Netzverbindungen zu leistungsfähigen Cloudsystemen bereit.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Haben Sie den geeigneten Typ des lokalen Speichers ausgewählt?	Stellen Sie sicher, dass Datenübertragungen aus dem lokalen Speicher in die Cloud beendet werden, bevor der nächste Sicherungszyklus beginnt.
	Tipp: Daten werden kurz nach dem Versetzen in die Cloud aus dem lokalen Speicher entfernt.
	Verwenden Sie die folgenden Richtlinien:
	• Verwenden Sie Flash- oder SSD-Speicher für große Systeme, die über leistungsfähige Cloudsysteme verfügen. Stellen Sie sicher, dass Sie über eine dedizierte 10-GB-WAN-Verbindung mit einer Hochgeschwindigkeitsverbindung zum Objektspeicher verfügen. Verwenden Sie beispielsweise Flash- oder SSD-Speicher, wenn Sie über eine dedizierte 10-GB-WAN-Verbindung sowie eine Hochgeschwindigkeitsverbindung zu einem IBM® Cloud Object Storage-Speicherort oder zu einem Amazon S3-Datencenter (Amazon S3 = Amazon Simple Storage Service) verfügen.
	• Verwenden Sie SAS-Platten mit 15000 U/min mit größerer Kapazität für die folgenden Szenarios:
	  ○ Systeme mittlerer Größe
	  ○ Langsamere Cloudverbindungen, z. B. 1 GB
	  ○ Bei Verwendung von IBM Cloud Object Storage als Service-Provider in mehreren Regionen
	• Berechnen Sie für SAS-Platten oder rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.	

Linux: Planung für Speicherpools auf DISK- oder FILE-Einheiten

Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Können die Speicherpool-LUNs Durchsatzraten von 256 KB für sequenzielle Lese- und Schreibvorgänge aufrechterhalten, um die Arbeitslast innerhalb der Zeitvorgaben adäquat handhaben zu können?	Bei der Planung für Spitzenbelastungen müssen Sie alle Daten berücksichtigen, die der Server gleichzeitig aus Plattenspeicherpools lesen oder in Plattenspeicherpools schreiben soll. Berücksichtigen Sie beispielsweise den Spitzenwert für den Datenfluss bei Clientsicherungsoperationen und Serverdatenversetzungsoperationen, wie z. B. Umlagerung, die gleichzeitig ausgeführt werden. Der IBM Spectrum Protect-Server verwendet beim Lesen aus Speicherpools und Schreiben in Speicherpools in erster Linie 256-KB-Blöcke. Wenn das Plattensystem über die entsprechende Funktionalität verfügt, konfigurieren Sie das Plattensystem für die optimale Leistung mit sequenziellen Lese-/Schreiboperationen statt mit wahlfreien Lese-/Schreiboperationen.	Weitere Informationen finden Sie in Basisleistung von Plattensystemen analysieren.
Ist die Platte für die Verwendung von Lese- und Schreibcache konfiguriert?	Verwenden Sie mehr Cache, um eine bessere Leistung zu erzielen.	
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, eine geeignete Größe für die Speicherpooldatenträger festgelegt?	Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden. Wenn Sie nicht über die nötigen Informationen zum Schätzen der Größe für Datenträger mit der Einheitenklasse FILE verfügen, beginnen Sie mit einer Datenträgergröße von 50 GB.	In der Regel treten häufiger Probleme auf, wenn die Datenträger zu klein sind. Wenn Datenträger größer als erforderlich sind, treten nur selten Probleme auf. Wenn Sie die zu verwendende Datenträgergröße festlegen, sollten Sie als Vorsichtsmaßnahme eine größere Größe als erforderlich wählen.
Verwenden Sie für Speicherpools, die die Einheitenklasse FILE verwenden, vorab zugeordnete Datenträger?	Arbeitsdatenträger können eine Dateifragmentierung zur Folge haben. Um sicherzustellen, dass für einen Speicherpool immer genügend Datenträger verfügbar sind, setzen Sie den Parameter MAXSCRATCH auf einen Wert größer als null.	Ordnen Sie mithilfe des Befehls DEFINE VOLUME Datenträger in dem Speicherpool vorab zu. Verwenden Sie den Serverbefehl DEFINE STGPOOL oder UPDATE STGPOOL, um den Parameter MAXSCRATCH zu definieren.
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, die maximale Anzahl Clientsitzungen mit der Anzahl definierter Datenträger verglichen?	Es müssen immer genügend verwendbare Datenträger in den Speicherpools vorhanden sein, um die erwartete maximale Anzahl gleichzeitig ausgeführter Clientsitzungen handhaben zu können. Bei den Datenträgern kann es sich um Arbeitsdatenträger, leere Datenträger oder teilweise gefüllte Datenträger handeln.	Bei Speicherpools, die die Einheitenklasse FILE verwenden, kann jeweils nur eine einzige Sitzung oder ein einziger Prozess auf einen Datenträger schreiben.
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, den Parameter MOUNTLIMIT für die Einheitenklasse auf einen Wert gesetzt, der für die Anzahl Datenträger, die parallel angehängt werden könnten, ausreichend hoch ist?	Für Speicherpools, die die Datendeduplizierung verwenden, liegt der Wert für den Parameter MOUNTLIMIT in der Regel zwischen 500 und 1000. Setzen Sie den Wert für MOUNTLIMIT auf die maximale Anzahl Mountpunkte, die für alle aktiven Sitzungen erforderlich sind. Berücksichtigen Sie Parameter, die sich auf die maximale Anzahl erforderlicher Mountpunkte auswirken: • Die Serveroption MAXSESSIONS, die die maximal zulässige Anzahl gleichzeitig ablaufender IBM Spectrum Protect-Sitzungen angibt • Der Parameter MAXNUMMP, der die maximale Anzahl Mountpunkte definiert, die jeder Clientknoten verwenden kann Wenn beispielsweise die maximalen Anzahl Sicherungssitzungen für Clientknoten normalerweise 100 ist und für jeden der Knoten `MAXNUMMP=2` definiert ist, multiplizieren Sie 100 Knoten mit 2 Mountpunkten für jeden Knoten, um den Wert 200 für den Parameter MOUNTLIMIT zu erhalten.	Verwenden Sie den Serverbefehl REGISTER NODE oder UPDATE NODE, um den Parameter MAXNUMMP für Clientknoten zu definieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie für Speicherpools, die die Einheitenklasse DISK verwenden, festgelegt, wie viele Speicherpooldatenträger in jedes Dateisystem gestellt werden sollen?	Die Konfiguration des Speichers für einen Speicherpool, der eine Einheitenklasse DISK verwendet, ist davon abhängig, ob Sie RAID für das Plattensystem verwenden. Wenn Sie RAID nicht verwenden, konfigurieren Sie ein einzige Dateisystem pro physischer Platte und definieren Sie exakt einen Speicherpooldatenträger für jedes Dateisystem. Wenn Sie RAID 5 mit *n* + 1 Datenträgern verwenden, konfigurieren Sie den Speicher auf eine der folgenden Arten: • Konfigurieren Sie *n* Dateisysteme auf der LUN und definieren Sie exakt einen Speicherpooldatenträger pro Dateisystem. • Konfigurieren Sie ein einziges Dateisystem und *n* Speicherpooldatenträger für die LUN.	Ein Beispiellayout, bei dem diese Richtlinie eingehalten wird, zeigt Beispiellayout für Serverspeicherpools.
Haben Sie Ihre Speicherpools für die Verteilung der Ein-/Ausgabe auf mehrere Dateisysteme erstellt?	Stellen Sie sicher, dass sich jedes Dateisystem auf einer anderen LUN auf dem Plattensystem befindet. Normalerweise sind 10-30 Dateisysteme ein geeigneter Wert, Sie müssen jedoch sicherstellen, dass die Dateisysteme nicht kleiner als etwa 250 GB sind.	Ausführliche Informationen finden Sie in: • Plattenspeicher für den Server optimieren • Speicherpools und Datenträger optimieren und konfigurieren

Linux: Planung für die Auswahl des korrekten Speichertechnologietyps

Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.

Vorgehensweise

Die folgende Tabelle unterstützt Sie bei der Auswahl des korrekten Speichertechnologietyps für die Speicherressourcen, die der Server erfordert.

Tabelle 1. Speichertechnologietypen für IBM Spectrum Protect-Speicherbedarf

Speichertechnologietyp	Datenbank	Aktive Protokolldatei	Archivprotokoll und Archivübernahmeprotokoll	Speicherpools
Solid-State-Laufwerk (SSD)	Stellen Sie die Datenbank auf ein Solid-State-Laufwerk, wenn die folgenden Bedingungen erfüllt sind: • Sie verwenden die IBM Spectrum Protect-Datendeduplizierung. • Sie sichern täglich mehr als 8 TB neuer Daten.	Wenn Sie die IBM Spectrum Protect-Datenbank auf ein Solid-State-Laufwerk stellen (dies ist das bewährte Verfahren), stellen Sie auch die aktive Protokolldatei auf ein Solid-State-Laufwerk. Wenn kein Speicherplatz verfügbar ist, verwenden Sie stattdessen eine Hochleistungsplatte.	Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Das Archivprotokoll und die Archivübernahmeprotokolle können auf langsamere Speichertechnologietypen gestellt werden.	Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Speicherpools können auf langsamere Speichertechnologietypen gestellt werden.

Speichertech-nologietyp	Datenbank	Aktive Protokolldatei	Archivprotokoll und Archivübernahmepro-tokoll	Speicherpools
Hochleistungs-platte mit den folgenden Kenndaten: • **Platte mit 15.000 U/min** • **Fibre Channel- oder Serial-attached SCSI-Schnittstelle (SAS-Schnittstelle)**	Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind: • Der Server führt keine Datendeduplizierung aus. • Der Server führt keine Knotenreplikation aus. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.	Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind: • Der Server führt keine Datendeduplizierung aus. • Der Server führt keine Knotenreplikation aus. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.	Sie können Hochleistungsplatten für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.	Verwenden Sie Hochleistungsplatten für Speicherpools, wenn die folgenden Bedingungen erfüllt sind: • Daten werden häufig gelesen. • Daten werden häufig geschrieben. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.
Platte mit mittlerer Leistung oder Hochleis-tungsplatte mit den folgenden Kenndaten: • **Platte mit 10.000 U/min** • **Fibre Channel- oder SAS-Schnittstelle**	Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.	Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.	Sie können eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für das Archivprotokoll und die Archivüber-nahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.	Verwenden Sie eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für Speicherpools, wenn die folgenden Bedingungen erfüllt sind: • Daten werden häufig gelesen. • Daten werden häufig geschrieben. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.
SATA, Network-attached Storage (NAS)	Verwenden Sie diesen Speicher nicht für die Datenbank. Stellen Sie die Datenbank nicht auf XIV-Speichersysteme.	Verwenden Sie diesen Speicher nicht für die aktive Protokolldatei.	Die Verwendung dieser langsameren Speichertechnologie ist akzeptabel, da diese Protokolle einmal geschrieben und nur selten gelesen werden.	Verwenden Sie diese langsamere Speichertechnologie, wenn die folgenden Bedingungen erfüllt sind: • Daten werden selten geschrieben, beispielsweise einmal. • Daten werden selten gelesen. .
Bänder und virtuelle Bänder				Verwenden Sie diese Speichermedien für die langfristige Aufbewahrung oder wenn Daten nur selten verwendet werden.

Linux: Bewährte Verfahren bei der Serverinstallation anwenden

Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

Vorgehensweise

- Nachfolgend sind die wichtigsten bewährten Verfahren für die Erzielung der optimalen Leistung und die Vermeidung von Problemen aufgeführt.
- Bestimmen Sie anhand der Tabelle die bewährten Verfahren, die für Ihre Umgebung gelten.

Bewährtes Verfahren	**Weitere Informationen**
Verwenden Sie schnelle Platten für die Serverdatenbank. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung.	Verwenden Sie schnelle Platten mit kurzer Latenzzeit für die Datenbank. Die Verwendung von Solid-State-Laufwerken ist von entscheidender Bedeutung, wenn Sie die Datendeduplizierung und Knotenreplikation verwenden. Vermeiden Sie die Verwendung von SATA-Laufwerken (SATA = Serial Advanced Technology Attachment) und PATA-Laufwerken (PATA = Parallel Advanced Technology Attachment). Ausführliche Informationen und weitere Tipps finden Sie in: ◦ "Planung für Platten für die Serverdatenbank" ◦ "Planung für die Auswahl des korrekten Speichertechnologietyps"
Stellen Sie sicher, dass das Serversystem über genügend Speicher verfügt.	Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309. Höhere Arbeitslasten erfordern mehr als die Mindestvoraussetzungen. Erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation können mehr Speicher als den Mindestspeicher erfordern, der im Dokument mit den Systemvoraussetzungen angegeben ist. Wenn Sie die Ausführung mehrerer Instanzen planen, ist für jede Instanz der für einen einzelnen Server aufgelistete Speicher erforderlich. Multiplizieren Sie den für einen einzelnen Server erforderlichen Speicher mit der Anzahl der für das System geplanten Instanzen.
Trennen Sie die Serverdatenbank, die aktive Protokolldatei, das Archivprotokoll und die Plattenspeicherpools voneinander.	Stellen Sie alle IBM Spectrum Protect-Speicherressourcen auf unterschiedliche Platten. Trennen Sie Speicherpoolplatten von den Platten für die Serverdatenbank und die Protokolle. Speicherpooloperationen können Datenbankoperationen beeinträchtigen, wenn sich die Speicherpools und die Datenbank auf denselben Platten befinden. Im Idealfall werden auch die Serverdatenbank und die Protokolle voneinander getrennt. Ausführliche Informationen und weitere Tipps finden Sie in: ◦ "Planung für Platten für die Serverdatenbank" ◦ "Planung für Platten für das Serverwiederherstellungsprotokoll" ◦ "Planung für Speicherpools auf DISK- oder FILE-Einheiten"
Verwenden Sie mindestens vier Verzeichnisse für die Serverdatenbank. Verwenden Sie für größere Server oder Server, die erweiterte Funktionen verwenden, acht Verzeichnisse.	Stellen Sie jedes Verzeichnis auf eine LUN, die von anderen LUNs und von anderen Anwendungen getrennt ist. Ein Server wird als großer Server betrachtet, wenn seine Datenbank größer als 2 TB ist oder wahrscheinlich diese Größe erreichen wird. Verwenden Sie für derartige Server acht Verzeichnisse. Siehe "Planung für Platten für die Serverdatenbank".
Wenn Sie die Datendeduplizierung und/oder die Knotenreplikation verwenden, beachten Sie die Richtlinien für die Datenbankkonfiguration und andere Elemente.	Konfigurieren Sie den Server gemäß den Richtlinien, da die Datenbank in Bezug darauf, wie gut die Ausführung des Servers bei Verwendung dieser Funktionen ist, extrem wichtig ist. Ausführliche Informationen und weitere Tipps finden Sie in: ◦ Prüfliste für Datendeduplizierung ◦ Prüfliste für Knotenreplikation

Bewährtes Verfahren	Weitere Informationen
Beachten Sie bei Speicherpools, die Einheitenklassen des Typs FILE verwenden, die Richtlinien für die Größe von Speicherpooldatenträgern. In der Regel sind Datenträger mit einer Größe von 50 GB am besten geeignet.	Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden zur Bestimmung der Datenträgergröße. Konfigurieren Sie Speicherpooleinheiten und Dateisysteme auf der Basis der Anforderungen in Bezug auf den Durchsatz und nicht nur auf der Basis der Kapazitätsanforderungen. Trennen Sie die Speichereinheiten, die von IBM Spectrum Protect verwendet werden, von anderen Anwendungen mit hoher Ein-/Ausgabe und stellen Sie sicher, dass der Durchsatz für diesen Speicher ausreichend ist. Weitere Informationen finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.
Planen Sie IBM Spectrum Protect-Clientoperationen und -Serververwaltungsaktivitäten, um eine Überschneidung von Operationen zu verhindern oder auf ein Mindestmaß zu reduzieren.	Weitere ausführliche Informationen liefern die folgenden Themen: ◦ Zeitplan für tägliche Operationen optimieren ◦ Prüfliste für Serverkonfiguration
Überwachen Sie Operationen kontinuierlich.	Die Überwachung ermöglicht es Ihnen, Probleme frühzeitig erkennen und Ursachen leichter ermitteln zu können. Bewahren Sie Aufzeichnungen von Überwachungsberichten bis zu einem Jahr lang auf, um Trends schneller erkennen und Wachstum besser planen zu können. Siehe Umgebung im Hinblick auf die Leistung überwachen und verwalten.

Linux: Systemmindestvoraussetzungen für Linux-Systeme

Für die Installation des IBM Spectrum Protect-Servers auf einem Linux-System wird ein Minimum an Hardware und Software benötigt. Hierzu gehören eine Übertragungsmethode und der aktuelle Einheitentreiber.

Die folgenden Tabellen enthalten die Mindesthardware- und -softwarevoraussetzungen für die Installation eines IBM Spectrum Protect-Servers. Verwenden Sie diese Voraussetzungen als Ausgangspunkt für Systeme ohne Datendeduplizierung. Die optimale IBM Spectrum Protect-Umgebung ist mit Datendeduplizierung mithilfe der IBM Spectrum Protect Blueprints konfiguriert. Die neuesten Informationen zu den Systemvoraussetzungen finden Sie unter Technote 1243309.

Das IBM Spectrum Protect-Einheitentreiberpaket enthält keinen Einheitentreiber für dieses Betriebssystem, weil ein generischer SCSI-Einheitentreiber verwendet wird. Konfigurieren Sie den Einheitentreiber, bevor der IBM Spectrum Protect-Server für Bandeinheiten verwendet wird. Das IBM Spectrum Protect-Treiberpaket enthält Treibertools und ACSLS-Dämonen. IBM®-Treiberpakete finden Sie auf der Fix Central-Website.

Informationen zu Voraussetzungen, unterstützten Einheiten, Clientinstallationspaketen und Fixes sind im IBM Support Portal for IBM Spectrum Protect verfügbar. Rufen Sie nach der Installation von IBM Spectrum Protect und vor der individuellen Anpassung die Website auf, laden Sie alle anwendbaren Fixes herunter und wenden Sie diese Fixes an.

- Linux-BetriebssystemeLinux: Servermindestvoraussetzungen für Linux X86_64
  Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux X86_64-Betriebssystem installieren.
- Linux-BetriebssystemeLinux: Servermindestvoraussetzungen für Linux on System z
  Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on System z-Betriebssystem installieren.
- Linux-BetriebssystemeLinux: Servermindestvoraussetzungen für Linux on Power Systems (Little Endian)
  Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on Power Systems-Betriebssystem (Little Endian) installieren.

Linux: Servermindestvoraussetzungen für Linux X86_64

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux X86_64-Betriebssystem installieren.

Hardwarevoraussetzungen

In Tabelle 1 sind die Hardwaremindestvoraussetzungen für den Server beschrieben. Wenn der Server die Mindestvoraussetzungen nicht erfüllt, schlägt die Installation fehl. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in Linux: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen

Hardwaretyp	Hardwarevoraussetzungen
Server	Ein AMD64- oder Intel EMT-64-Prozessor
Plattenspeicher	Folgende Mindestwerte für den Plattenspeicher: • 5 GB für das Installationsverzeichnis • 512 MB für das Verzeichnis /var • 2 GB für das Verzeichnis /tmp • 128 MB im Ausgangsverzeichnis des Rootbenutzers • 2 GB für den Bereich der gemeinsam genutzten Ressourcen Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben. Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten. Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN. Lesen Sie den Abschnitt zur Linux: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.
Hauptspeicher	Folgende Mindestwerte für den Hauptspeicher: • 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation • 24 GB für Datendeduplizierung oder Knotenreplikation • 32 GB für Knotenreplikation mit Datendeduplizierung Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect. Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.

Softwarevoraussetzungen

In Tabelle 2 sind die für einen Server auf einem Linux X86_64-System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Für den IBM Spectrum Protect-Server unter Linux X86_64 ist eines der folgenden Betriebssysteme erforderlich: • Red Hat Enterprise Linux 6.7 • Red Hat Enterprise Linux 7, einschließlich Updates • SUSE Linux Enterprise Server 11, Service-Pack 4 oder höher • SUSE Linux Enterprise Server 12

Softwaretyp	Softwaremindestvoraussetzungen
Bibliotheken	Auf dem IBM Spectrum Protect-System installierte GNU C-Bibliotheken Version 2.3.3-98.38 oder höher. Für SUSE Linux Enterprise Server: • libaio • libstdc++.so.6 Version 4.3 oder höher (32- und 64-Bit-Pakete sind erforderlich) Für Red Hat Enterprise Linux Server: • libaio • libstdc++.so.6 (32- und 64-Bit-Pakete sind erforderlich) • numactl.x86_64 Führen Sie einen der folgenden Schritte aus, um festzustellen, ob SELinux installiert ist und sich im restriktiven Modus befindet: • Überprüfen Sie die Datei /etc/sysconfig/selinux. • Führen Sie den Betriebssystembefehl sestatus aus. • Überprüfen Sie die Datei /var/log/messages auf SELinux-Nachrichten. Führen Sie einen der folgenden Schritte aus, um SELinux zu inaktivieren: • Geben Sie den toleranten Modus an, indem Sie den Befehl `setenforce 0` als Superuser ausgeben. • Ändern Sie die Datei /etc/sysconfig/selinux und führen Sie einen Neustart der Maschine durch.
Übertragungsprotokoll	• TCP/IP Version 4 oder Version 6 (Standard für Linux) • Shared Memory-Protokoll (mit IBM Spectrum Protect Linux X86_64-Client)
Verarbeitung	Asynchrone Ein-/Ausgabe muss aktiviert sein. Installieren Sie für Linux-Kernel mit 2.6 oder höher die Bibliothek libaio, um die asynchrone Ein-/Ausgabe zu aktivieren.
Einheitentreiber	Der IBM Spectrum Protect-Durchgriffseinheitentreiber wird für Einheiten eines anderen Herstellers verwendet. Er verwendet die SCSI-Durchgriffsschnittstelle für die Kommunikation mit Bandeinheiten und Bandarchiven. Der generische Linux-SCSI-Einheitentreiber (sg) ist für Bandlaufwerke und Bandarchive erforderlich. Das IBM Spectrum Protect-Einheitentreiberpaket enthält Einheitentreibertools und ACSLS-Dämonen. Für die Bandarchive bzw. Bandlaufwerke IBM® 3590, 3592 oder Ultrium sind die IBM Einheitentreiber erforderlich. Installieren Sie die aktuellen Einheitentreiber. IBM-Treiberpakete finden Sie bei Fix Central. Konfigurieren Sie die Einheitentreiber, bevor Sie den Server für Bandeinheiten verwenden.
Sonstige Software	Korn-Shell (ksh) ist erforderlich. Konfigurieren Sie die I/O Completion Ports (IOCP) auf dem Betriebssystem. Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisserver verwenden: • Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2) • IBM Security Directory Server Version 6.3 • IBM Security Directory Server Version 6.4

Linux: Servermindestvoraussetzungen für Linux on System z

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on System z-Betriebssystem installieren.

Hardwarevoraussetzungen

In Tabelle 1 sind die für Ihr IBM Spectrum Protect-System unter Linux on System z erforderlichen Hardwaremindestvoraussetzungen beschrieben. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in Linux: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen

Hardwaretyp	Hardwarevoraussetzungen
Server	Eine native logische 64-Bit-Partition (LPAR) oder eine z/VM-Gastmaschine unter IBM® zSeries, IBM System z9, IBM System z10 oder IBM zEnterprise System (z114 und z196).

Hardwaretyp	Hardwarevoraussetzungen
Plattenspeicher	Folgende Mindestwerte für den Plattenspeicher: • 5 GB für das Installationsverzeichnis • 512 MB für das Verzeichnis /var • 2 GB für das Verzeichnis /tmp • 128 MB im Ausgangsverzeichnis des Rootbenutzers • 2 GB für den Bereich der gemeinsam genutzten Ressourcen Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben. Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten. Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN. Lesen Sie den Abschnitt zur Linux: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.
Hauptspeicher	Folgende Mindestwerte für den Hauptspeicher: • 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation • 24 GB für Datendeduplizierung oder Knotenreplikation • 32 GB für Knotenreplikation mit Datendeduplizierung Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect. Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.

Softwarevoraussetzungen

In Tabelle 2 sind die für Ihr IBM Spectrum Protect-System unter Linux on System z erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

Softwaretyp	Softwaremindestvoraussetzungen
Server	Für den IBM Spectrum Protect-Server unter Linux on System z (s390x-64-Bit-Architektur) ist eines der folgenden Betriebssysteme erforderlich: • Red Hat Enterprise Linux 7.1 • SUSE Linux Enterprise Server 12
Bibliotheken	Eine auf dem IBM Spectrum Protect-System installierte GNU C-Bibliothek Version 2.4-31.43.6. Für SUSE Linux Enterprise Server: • libaio • libstdc++.so.6 Version 4.3 oder höher (32- und 64-Bit-Pakete sind erforderlich) • libxlc-1.2.0.0.151119a.s390x oder höher Für Red Hat Enterprise Linux Server: • libaio • libstdc++.so.6 (32- und 64-Bit-Pakete sind erforderlich) • numactl.x86_64 • libxlc-1.2.0.0.151119a.s390x oder höher

Softwaretyp	Softwaremindestvoraussetzungen
Übertragungsprotokoll	• TCP/IP Version 4 oder Version 6 (Standard für Linux) • Shared Memory-Protokoll (mit IBM Spectrum Protect Version 8.1.2 Linux on System z-Client)
Verarbeitung	Asynchrone Ein-/Ausgabe muss aktiviert sein. Installieren Sie für Linux-Kernel mit 2.6 oder höher die Bibliothek libaio, um die asynchrone Ein-/Ausgabe zu aktivieren.
Sonstige Software	Korn-Shell (ksh) ist erforderlich. Konfigurieren Sie die I/O Completion Ports (IOCP) auf dem Betriebssystem. Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisserver verwenden: • Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2) • IBM Security Directory Server Version 6.3 • IBM Security Directory Server Version 6.4

Linux: Servermindestvoraussetzungen für Linux on Power Systems (Little Endian)

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on Power Systems-Betriebssystem (Little Endian) installieren.

Hardwarevoraussetzungen

In Tabelle 1 sind die Hardwaremindestvoraussetzungen für den Server beschrieben. Wenn der Server die Mindestvoraussetzungen nicht erfüllt, schlägt die Installation fehl. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in Linux: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen

Hardwaretyp	Hardwarevoraussetzungen
Server	Ein Linux on Power Systems-Server (Little Endian) auf einem IBM® System. Zum Beispiel ein auf der Website Linux on IBM Power Systems aufgelisteter Server.
Plattenspeicher	Folgender Mindestplattenspeicher: • 5 GB für das Installationsverzeichnis • 128 MB im Ausgangsverzeichnis des Rootbenutzers • 2 GB für den Bereich der gemeinsam genutzten Ressourcen Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben. Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten. Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN. Lesen Sie den Abschnitt zur Linux: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.
Hauptspeicher	• 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation • 24 GB für Datendeduplizierung oder Knotenreplikation • 32 GB für Knotenreplikation mit Datendeduplizierung Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect. Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.

Softwarevoraussetzungen

In Tabelle 2 sind die für Ihr System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Red Hat Enterprise Linux (RHEL) 7.3 mit PPC64LE-Architektur.
Bibliotheken	GNU-C-Bibliotheken Version 2.4-31.30 und höher. libaio.so.1 (32- und 64-Bit-Pakete).
Übertragungsprotokoll	• TCP/IP Version 4 oder Version 6 (Standard für Linux) • Shared Memory-Protokoll (mit einem Client der Version 8.1.2)
Verarbeitung	Asynchrone Ein-/Ausgabe muss aktiviert sein. Installieren Sie für Linux-Kernel mit 2.6 oder höher die Bibliothek libaio, um die asynchrone Ein-/Ausgabe zu aktivieren.
Sonstige Software	Korn-Shell (ksh) ist erforderlich. Konfigurieren Sie die I/O Completion Ports (IOCP) auf dem Betriebssystem. Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisserver verwenden: • Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2) • IBM Security Directory Server Version 6.3 • IBM Security Directory Server Version 6.4

Einschränkung: Unformatierte logische Datenträger werden nicht unterstützt.
Linux-Betriebssysteme

Linux: Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System

Sie können andere Produkte, die DB2-Produkte auf demselben System wie der IBM Spectrum Protect-Server der Version 8.1.2 implementieren und verwenden, mit einigen Einschränkungen installieren.

Damit andere Produkte, die ein DB2-Produkt auf demselben System wie der IBM Spectrum Protect-Server verwenden, installiert und verwendet werden können, müssen die folgenden Bedingungen erfüllt sein:

Tabelle 1. Kompatibilität des IBM Spectrum Protect-Servers mit anderen DB2-Produkten auf dem System

Bedingung	Anweisungen
Versionsstand	Die anderen Produkte, die ein DB2-Produkt verwenden, müssen DB2 Version 9 oder höher verwenden. DB2-Produkte verfügen ab Version 9 über die Unterstützung für Produktkapselung und -trennung. Ab dieser Version können Sie mehrere Kopien von DB2-Produkten mit unterschiedlichen Codeversionen auf demselben System ausführen. Ausführliche Informationen finden Sie in dem Abschnitt über mehrere DB2-Kopien in der Produktinformation zu DB2.
Benutzer-IDs und Verzeichnisse	Stellen Sie sicher, dass die Benutzer-IDs, die IDs der abgeschirmten Benutzer, die Installationsposition, andere Verzeichnisse und zugehörige Informationen nicht von mehreren DB2-Installationen gemeinsam genutzt werden. Ihre Angaben müssen sich von den IDs und Positionen unterscheiden, die Sie für die Installation und Konfiguration des IBM Spectrum Protect-Servers verwendet haben. Wenn Sie den Assistenten dsmicfgx für die Konfiguration des Servers verwendet haben, haben Sie diese Werte während der Ausführung des Assistenten eingegeben. Wenn Sie eine manuelle Konfiguration durchgeführt haben, überprüfen Sie im Bedarfsfall die verwendeten Prozeduren, um sich die für den Server verwendeten Werte in Erinnerung zu rufen.
Ressourcenzuordnung	Sie müssen die Ressourcen und das Leistungsspektrum des Systems gegen die Anforderungen für den IBM Spectrum Protect-Server und die anderen Anwendungen, die das DB2-Produkt verwenden, abwägen. Damit den anderen DB2-Anwendungen genügend Ressourcen zur Verfügung stehen, müssen Sie unter Umständen die Einstellungen des IBM Spectrum Protect-Servers ändern, so dass der Server weniger Systemspeicher und -ressourcen verwendet. Wenn die Verarbeitungsprozesse für die anderen DB2-Anwendungen und der IBM Spectrum Protect-Server um Prozessor- und Speicherressourcen konkurrieren, kann die Leistung des Servers in Bezug auf die Verarbeitung der erwarteten Clientauslastung oder anderer Serveroperationen beeinträchtigt werden. Um die Ressourcen zu trennen und die Möglichkeit zur Optimierung und Zuordnung von Prozessor-, Speicher- und anderen Systemressourcen für mehrere Anwendungen zu verbessern, sollten Sie Unterstützung für logische Partitionen (LPAR), Auslastungspartitionierung (WPAR) oder andere Unterstützung für virtuelle Workstations einsetzen. Führen Sie eine DB2-Anwendung beispielsweise auf einem eigenen virtuellen System aus.

Linux: IBM Installation Manager

IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager noch nicht installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie IBM Spectrum Protect installieren. Die Software muss auf dem System installiert bleiben, damit IBM Spectrum Protect später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

Angebot
: Eine installierbare Einheit eines Softwareprodukts.

  Das Angebot 'IBM Spectrum Protect' enthält alle Datenträger, die IBM Installation Manager für die Installation von IBM Spectrum Protect benötigt.

Paket
: Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.
  Das IBM Spectrum Protect-Paket enthält folgende Komponenten:

  - Installationsprogramm IBM Installation Manager
  - Das Angebot 'IBM Spectrum Protect'

Paketgruppe
: Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

  Die Standardpaketgruppe für das IBM Spectrum Protect-Paket ist `IBM Installation Manager`.

Repository
: Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

  Das IBM Spectrum Protect-Paket wird in einem Repository in IBM Fix Central gespeichert.

Verzeichnis für gemeinsam genutzte Ressourcen
: Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

  In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version von IBM Spectrum Protect verwendet werden.

Linux: Arbeitsblätter für Planungsdetails für den Server

Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.

Element	Erforderlicher Speicherbereich	Anzahl der Verzeichnisse	Position der Verzeichnisse
Die Datenbank			
Aktive Protokolldatei			
Archivprotokoll			
Optional: Protokollspiegel für die aktive Protokolldatei			
Optional: Sekundäres Archivprotokoll (Übernahmeverzeichnis für Archivprotokolle)			

Element	Namen und Benutzer-IDs	Position
Die *Instanzbenutzer-ID* für den Server. Mit dieser ID starten Sie den IBM Spectrum Protect-Server und führen ihn aus.		
Das *Ausgangsverzeichnis* des Servers. In diesem Verzeichnis befindet sich die Instanzbenutzer-ID.		
Der Datenbankinstanzname		

Element	Namen und Benutzer-IDs	Position
Das *Instanzverzeichnis* für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien).		
Der Servername; verwenden Sie einen eindeutigen Namen für jeden Server.		

Linux: Kapazitätsplanung

Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.

- Linux: Speicherbedarf für die Datenbank schätzen
  Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.
- Linux: Speicherplatzbedarf für das Wiederherstellungsprotokoll
  In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.
- Linux: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen
  Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.
- Linux: Rollbackdateien der Installation löschen
  Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

Linux: Speicherbedarf für die Datenbank schätzen

Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.

Informationen zu diesem Vorgang

Anfänglich sollte mindestens 25 GB Speicherplatz in der Datenbank verwendet werden. Stellen Sie entsprechend Speicherplatz im Dateisystem bereit. Eine Datenbankgröße von 25 GB ist für eine Testumgebung oder eine Umgebung, die nur einen Speicherarchivmanager umfasst, ausreichend. Für einen Produktionsserver, der Clientlasten unterstützt, sollte die Datenbank größer sein. Wenn Sie Plattenspeicherpools (DISK) mit wahlfreiem Zugriff verwenden, ist mehr Datenbank- und Protokollspeicherbereich erforderlich als für Speicherpools mit sequenziellem Zugriff.

Die maximale Größe der IBM Spectrum Protect-Datenbank beträgt 6 TB.

Informationen zur Festlegung der Größe einer Datenbank in einer Produktionsumgebung, die auf der Anzahl Dateien und der Speicherpoolgröße basiert, enthalten die folgenden Abschnitte.

- Linux: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen
  Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.
- Linux: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen
  Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz kapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.
- Linux: Datenbankmanager und temporärer Speicherbereich
  Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systemspeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

Linux: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen

Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.

Informationen zu diesem Vorgang

Um den Speicherbedarf auf der Basis der maximalen Anzahl Dateien im Serverspeicher zu schätzen, verwenden Sie die folgenden Richtlinien:

- 600-1000 Byte für jede gespeicherte Version einer Datei einschließlich der Imagesicherungen.
  Einschränkung: Diese Richtlinie umfasst nicht den Speicherplatz, der während der Datendeduplizierung verwendet wird.
- 100-200 Byte für jede Datei im Cache, jede Kopienspeicherpooldatei, jede Datei im Pool für aktive Daten und jede deduplizierte Datei.
- Zusätzlicher Speicherbereich ist für die Datenbankoptimierung erforderlich, um variable Datenzugriffsmuster und die Server-Back-End-Verarbeitung von Daten zu unterstützen. Die Größe des zusätzlichen Speicherplatzes entspricht 50 % der Schätzung für die Gesamtanzahl Byte für Dateiobjekte.

In dem folgenden Beispiel für einen einzelnen Client basieren bei Berechnungen auf den Maximalwerten in den vorhergehenden Richtlinien. Bei den Beispielen wird die mögliche Verwendung der Dateiaggregation nicht berücksichtigt. Im Allgemeinen wird durch das Aggregieren kleiner Dateien der erforderliche Speicherplatz in der Datenbank reduziert. Die Dateiaggregation betrifft keine speicherverwalteten Dateien.

Vorgehensweise

1. Berechnen Sie die Anzahl Dateiversionen. Addieren Sie alle folgenden Werte, um die Anzahl Dateiversionen zu erhalten:
   a. Berechnen Sie die Anzahl gesicherter Dateien. Beispiel: Möglicherweise werden bis zu 500.000 Clientdateien gleichzeitig gesichert. In diesem Beispiel sind die Speichermaßnahmen so definiert, dass maximal drei Kopien gesicherter Dateien aufbewahrt werden:

      ```
      500.000 Dateien * 3 Kopien = 1.500.000 Dateien
      ```

   b. Berechnen Sie die Anzahl Archivierungsdateien. Beispiel: Bis zu 100.000 Clientdateien können archivierte Kopien sein.
   c. Berechnen Sie die Anzahl speicherverwalteter Dateien. Beispiel: Bis zu 200.000 Clientdateien können von Client-Workstations umgelagert werden.

   Bei Verwendung von 1000 Byte pro Datei beträgt der Gesamtspeicherplatz in der Datenbank, der für die zu dem Client gehörigen Dateien erforderlich ist, 1,8 GB:

   ```
   (1.500.000 + 100.000 + 200.000) * 1000 = 1,8 GB
   ```

2. Berechnen Sie die Anzahl Dateien im Cache, Kopienspeicherpooldateien, Dateien im Pool für aktive Daten und deduplizierter Dateien:
   a. Berechnen Sie die Anzahl der Cachekopien. Beispiel: In einem Plattenspeicherpool mit 5 GB Kapazität ist Caching aktiviert. Die obere Umlagerungsschwelle des Pools ist 90 % und die untere Umlagerungsschwelle ist 70 %. Das heißt 20 % des Plattenpools (oder 1 GB) wird von Cachedateien belegt.
   Wenn die durchschnittliche Dateigröße ungefähr 10 KB beträgt, enthält der Cache zu jedem beliebigen Zeitpunkt etwa 100.000 Dateien:

      ```
      100.000 Dateien * 200 Byte = 19 MB
      ```

   b. Berechnen Sie die Anzahl Kopienspeicherpooldateien. Alle primären Speicherpools werden im Kopienspeicherpool gesichert:

      ```
      (1.500.000 + 100.000 + 200.000) * 200 Byte = 343 MB
      ```

   c. Berechnen Sie die Anzahl Dateien im Speicherpool für aktive Daten. Alle aktiven Clientsicherungsdaten in primären Speicherpools werden in den Speicherpool für aktive Daten kopiert. Angenommen, es sind 500.000 Versionen der 1.500.000 Sicherungsdateien im primären Speicherpool aktiv:

      ```
      500.000 * 200 Byte = 95 MB
      ```

   d. Berechnen Sie die Anzahl deduplizierter Dateien. Angenommen, ein deduplizierter Speicherpool enthält 50.000 Dateien:

      ```
      50.000 * 200 Byte = 10 MB
      ```

   Auf der Basis der vorhergehenden Berechnungen sind etwa 0,5 GB zusätzlicher Speicherplatz in der Datenbank für die Cachedateien, die Kopienspeicherpooldateien, die Dateien im Pool für aktive Daten und die deduplizierten Dateien des Clients erforderlich.
3. Berechnen Sie den zusätzlichen Speicherplatz, der für die Datenbankoptimierung benötigt wird. Um optimalen Datenzugriff und optimale Verwaltung durch den Server bereitzustellen, ist zusätzlicher Speicherplatz in der Datenbank erforderlich. Die Größe des zusätzlichen Speicherplatzes in der Datenbank beträgt 50 % des Gesamtspeicherbedarfs für Dateiobjekte.

   ```
   (1,8 + 0,5) * 50 % = 1,2 GB
   ```

4. Die Gesamtgröße des für den Client erforderlichen Datenbankspeicherbereichs berechnen. Die Gesamtgröße beträgt ca. 3,5 GB:

   ```
   1,8 + 0,5 + 1,2 = 3,5 GB
   ```

5. Berechnen Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist. Wenn der Client, der in den vorhergehenden Berechnungen verwendet wurde, ein typischer Client ist und Sie beispielsweise über 500 Clients verfügen, können Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist, mithilfe der folgenden Berechnung schätzen:

   ```
   500 * 3,5 = 1,7 TB
   ```

Ergebnisse

Tipp: In den Beispielen oben handelt es sich bei den Ergebnissen um Schätzungen. Die tatsächliche Größe der Datenbank kann aufgrund von Faktoren wie beispielsweise der Anzahl Verzeichnisse und der Länge der Pfad- und Dateinamen von der geschätzten Größe abweichen. Sie sollten die Datenbank regelmäßig überwachen und die Größe wie erforderlich anpassen.

Nächste Schritte

Während des normalen Betriebs erfordert der IBM Spectrum Protect-Server möglicherweise temporären Speicherplatz in der Datenbank. Dieser Speicherplatz wird aus den folgenden Gründen benötigt:

- Zum Speichern der Ergebnisse der Sortierung oder Änderung der Reihenfolge, die noch nicht in der Datenbank aufbewahrt und in der Datenbank nicht unmittelbar optimiert werden. Die Ergebnisse werden vorübergehend in der Datenbank zur Verarbeitung gespeichert.
- Zum Erteilen des Verwaltungszugriffs auf die Datenbank über eine der folgenden Methoden:
  - Ein DB2-ODBC-Client (ODBC = Open Database Connectivity)
  - Ein Oracle-JDBC-Client (JDBC = Java™ Database Connectivity)
  - SQL (Structured Query Language) für den Server über die Befehlszeile eines Verwaltungsclients

Erwägen Sie die Verwendung von zusätzlichen 50 GB an temporärem Speicherplatz pro 500 GB Speicherbereich für Dateiobjekte und Optimierung. Siehe die Richtlinien in der folgenden Tabelle. In dem Beispiel, das im vorhergehenden Schritt verwendet wurde, sind insgesamt 1,7 TB Speicherplatz in der Datenbank für Dateiobjekte und die Optimierung für 500 Clients erforderlich. Auf der Basis dieser Berechnung sind 200 GB für temporären Speicherplatz erforderlich. Der erforderliche Gesamtspeicherplatz in der Datenbank beträgt 1,9 TB.

Datenbankgröße	Mindestens erforderlicher temporärer Speicherplatz
< 500 GB	50 GB
≥ 500 GB und < 1 TB	100 GB
≥ 1 TB und < 1,5 TB	150 GB
≥ 1,5 und < 2 TB	200 GB
≥ 2 und < 3 TB	250-300 GB
≥ 3 und < 4 TB	350-400 GB

Linux: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen

Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz kapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.

Linux: Datenbankmanager und temporärer Speicherbereich

Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systemspeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

Der Datenbankmanager sortiert Daten in einer bestimmten Reihenfolge, gemäß der SQL-Anweisung, mit der Sie die Daten anfordern. Je nach Auslastung des Servers und wenn es mehr Daten gibt, als der Datenbankmanager verwalten kann, werden die (der Reihenfolge nach sortierten) Daten temporärem Plattenspeicher zugeordnet. Daten werden temporärem Plattenspeicher zugeordnet, wenn die Ergebnismenge sehr umfangreich ist. Der Datenbankmanager verwaltet den verwendeten Speicher dynamisch, wenn Daten temporärem Plattenspeicher zugeordnet werden.

Bei der Verfallsverarbeitung kann beispielsweise eine umfangreiche Ergebnismenge generiert werden. Wenn der Systemspeicher in der Datenbank zur Speicherung der Ergebnismenge nicht ausreicht, wird ein Teil der Daten temporärem Plattenspeicher zugeordnet. Wenn während der Verfallsverarbeitung ein Knoten oder ein Dateibereich ausgewählt wird, der für die Verarbeitung zu groß ist, kann der Datenbankmanager die Daten im Speicher nicht sortieren. Der Datenbankmanager muss temporären Speicherbereich zum Sortieren der Daten verwenden.

Bei der Ausführung von Datenbankoperationen sollten Sie in den folgenden Szenarios eine Erweiterung des Speicherplatzes in der Datenbank vornehmen:

- Der Speicherbereich der Datenbank ist klein und die Serveroperation, die temporären Speicherbereich benötigt, belegt den verbleibenden freien Speicherbereich.
- Die Dateibereiche sind groß oder den Dateibereichen ist eine Maßnahme zugeordnet, durch die viele Dateiversionen erstellt werden.
- Der IBM Spectrum Protect-Server muss mit begrenztem Speicher ausgeführt werden. Die Datenbank verwendet den Hauptspeicher des IBM Spectrum Protect-Servers für Datenbankoperationen. Ist der verfügbare Speicher jedoch nicht ausreichend, ordnet der IBM Spectrum

Protect-Server der Datenbank temporären Speicherbereich auf Platte zu. Wenn beispielsweise 10G Speicher zur Verfügung stehen und Datenbankoperationen 12G Speicher benötigen, verwendet die Datenbank temporären Speicherbereich.
- Bei der Implementierung eines IBM Spectrum Protect-Servers wird ein Fehler aufgrund fehlenden Datenbankspeicherbereichs (`out of database space`) angezeigt. Überwachen Sie das Serveraktivitätenprotokoll auf Nachrichten, die sich auf den Datenbankspeicherbereich beziehen.

Wichtig: Sie dürfen die DB2-Software, die mit IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht verändern. Führen Sie keine Installation bzw. kein Upgrade auf eine andere Version, ein anderes Release oder ein anderes Fixpack der DB2-Software durch, um eine Beschädigung der Datenbank zu vermeiden.

Linux: Speicherplatzbedarf für das Wiederherstellungsprotokoll

In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.

- Linux: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll
  Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.
- Linux: Speicherbereich des Spiegels für aktive Protokolldateien
  Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.
- Linux: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle
  Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

Linux: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll

Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.

In IBM Spectrum Protect-Servern der Version 7.1 und höher kann die aktive Protokolldatei eine maximale Größe von 512 GB haben. Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist.

Berücksichtigen Sie bei der Schätzung der Größe der aktiven Protokolldatei die folgenden allgemeinen Richtlinien:

- Die empfohlene Anfangsgröße für die aktive Protokolldatei ist 16 GB.
- Stellen Sie sicher, das die aktive Protokolldatei mindestens groß genug ist, um die gleichzeitig ablaufende Aktivität handhaben zu können, die der Server in der Regel handhabt. Versuchen Sie als Vorsichtsmaßnahme das größte Arbeitsvolumen zu schätzen, das der Server jeweils handhabt. Stellen Sie für die aktive Protokolldatei zusätzlichen Speicherbereich bereit, der, falls erforderlich, verwendet werden kann. Ziehen Sie 20 % zusätzlichen Speicherbereich in Betracht.
- Überwachen Sie den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei. Passen Sie die Größe der aktiven Protokolldatei wie erforderlich abhängig von Faktoren wie Clientaktivität und Ebene der Serveroperationen an.
- Stellen Sie sicher, dass das Verzeichnis, das die aktive Protokolldatei enthält, mindestens genauso groß wie die aktive Protokolldatei ist. Ein Verzeichnis, das größer als die aktive Protokolldatei ist, kann Übernahmesituationen handhaben, sollten diese auftreten.
- Stellen Sie sicher, dass das Dateisystem, das das Verzeichnis für aktive Protokolldateien enthält, über mindestens 8 GB freien Speicherbereich für Anforderungen zum Versetzen temporärer Protokolle verfügt.

Die vorgeschlagene Anfangsgröße für das Archivprotokoll beträgt 48 GB.

Das Archivprotokollverzeichnis muss groß genug sein, um die Protokolldateien aufnehmen zu können, die seit der vorherigen Gesamtsicherung generiert wurden. Wenn Sie beispielsweise täglich eine Gesamtsicherung der Datenbank ausführen, muss das Archivprotokollverzeichnis groß genug sein, um die Protokolldateien für die gesamte Clientaktivität aufnehmen zu können, die während 24 Stunden stattfindet. Um Speicherbereich wiederherzustellen, löscht der Server veraltete Archivprotokolldateien nach einer Gesamtsicherung der Datenbank. Wenn das Archivprotokollverzeichnis voll wird und kein Verzeichnis für Archivübernahmeprotokolle vorhanden ist, verbleiben Protokolldateien im Verzeichnis für aktive Protokolldateien. Diese Bedingung kann zur Folge haben, dass das Verzeichnis für aktive Protokolldateien vollständig gefüllt und der Server gestoppt wird. Bei einem Serverneustart wird ein Teil des vorhandenen Speicherbereichs für die aktive Protokolldatei freigegeben wird.

Nach der Installation des Servers können Sie die Archivprotokollauslastung und den Speicherbereich im Archivprotokollverzeichnis überwachen. Wenn sich der Speicherbereich im Archivprotokollverzeichnis füllt, können die folgenden Probleme auftreten:

- Der Server kann keine Datenbankgesamtsicherungen ausführen. Untersuchen und beheben Sie dieses Problem.
- Andere Anwendungen schreiben in das Archivprotokollverzeichnis und belegen den für das Archivprotokoll erforderlichen Speicherbereich. Nutzen Sie den Speicherbereich für das Archivprotokoll nicht gemeinsam mit anderen Anwendungen, einschließlich anderer IBM Spectrum Protect-Server. Stellen Sie sicher, dass jeder Server über eine separate Speicherposition verfügt, dessen Eigner dieser spezifische Server ist und der von diesem spezifischen Server verwaltet wird.

- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen
  Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der

Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.

- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen
  Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen
  Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen
  Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datendeduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen
  Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.
- Linux: Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen
  Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.
- Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Datendeduplizierungsoperationen schätzen
  Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen

Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen zu bestimmen, führen Sie die folgende Berechnung aus:

```
Anzahl Clients  x  In jeder Transaktion gespeicherte Dateien
  x  Für jede Datei benötigter Protokollspeicherbereich
```

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Grundlegende Clientspeicheroperationen

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3053 Byte	Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Element	Beispielwerte	Beschreibung

Aktive Protokolldatei: vorgeschlagene Größe	19,5 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 Byte = 3,5 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		
		`3,5 + 16 = 19,5 GB`

Archivprotokoll: vorgeschlagene Größe	58,5 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen.
		
		`3,5 x 3 = 10,5 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		
		`10,5 + 48 = 58,5 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen. Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.		

Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen

Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, zu bestimmen, führen Sie die folgende Berechnung aus:

```
Anzahl Clients x Anzahl Sitzungen pro Client x Anzahl während
  jeder Transaktion gespeicherter Dateien x pro Datei erforderlicher
  Protokollspeicherbereich
```

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Mehrere Clientsitzungen

Element	Beispielwerte		Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	1000	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Mögliche Sitzungen für jeden Client	3	3	Die Einstellung der Clientoption RESOURCEUTILIZATION ist größer als der Standardwert. Jede Clientsitzung führt maximal drei Sitzungen parallel aus.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3053	3053	Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Element	Beispielwerte		Beschreibung

Aktive Protokolldatei: vorgeschlagene Größe	26,5 GB [1]	51 GB [1]	Die folgende Berechnung wurde für 300 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.
			`(300 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 10,5 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`10,5 + 16 = 26,5 GB`
			Die folgende Berechnung wurde für 1000 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.
			`(1000 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 35 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`35 + 16 = 51 GB`

Archivprotokoll: vorgeschlagene Größe	79,5 GB [1]	153 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, wird die Schätzung für die aktive Protokolldatei mit 3 multipliziert:
			`10,5 x 3 = 31,5 GB`
			`35 x 3 = 105 GB`
			Erhöhen Sie diese Werte um die vorgeschlagene Anfangsgröße von 48 GB:
			`31,5 + 48 = 79,5 GB`
			`105 + 48 = 153 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen. Überwachen Sie Ihre aktive Protokolldatei und passen Sie die Größe, falls erforderlich, an.			

Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen

Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.

Der Protokollspeicherbereich, der für jede Datei erforderlich ist, erhöht sich um ungefähr 200 Byte für jeden Kopienspeicherpool, der für eine Operation für gleichzeitiges Schreiben verwendet wird. In dem Beispiel in der folgenden Tabelle werden Daten in einem primären Speicherpool und darüber hinaus in zwei Kopienspeicherpools gespeichert. Die geschätzte Protokollgröße erhöht sich für jede Datei um 400 Byte. Wenn Sie den vorgeschlagenen Wert von 3053 Byte Protokollspeicherbereich pro Datei verwenden, sind insgesamt 3453 Byte erforderlich.

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Operationen für gleichzeitiges Schreiben

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.

Element	Beispielwerte	Beschreibung
Für jede Datei erforderlicher Protokollspeicherbereich	3453 Byte	3053 Byte plus 200 Byte für jeden Kopienspeicherpool. Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	20 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		
		`4 + 16 = 20 GB`

Archivprotokoll: vorgeschlagene Größe	60 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Speicherbedarf für das Archivprotokoll zu schätzen:
		
		`4 GB x 3 = 12 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		
		`12 + 48 = 60 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen

Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datendeduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.

Beispielsweise wird bei der Umlagerung von Dateien aus dem Speicherpool mit wahlfreiem Zugriff (DISK) in einem Plattenspeicherpool mit sequenziellem Zugriff (FILE) für jede Datei, die umgelagert wird, ungefähr 110 Byte Protokollspeicherbereich verwendet. Beispiel: Angenommen, es sind 300 Clients für Sichern/Archivieren vorhanden, von denen jeder 100.000 Dateien jede Nacht sichert. Die Dateien sind anfänglich in einem DISK-Speicherpool gespeichert und werden dann in einen FILE-Speicherpool umgelagert. Um die Größe des Speicherbereichs für die aktive Protokolldatei zu schätzen, die für die Datenumlagerung erforderlich ist, verwenden Sie die folgende Berechnung. Die Anzahl Clients in der Berechnung stellt die maximale Anzahl zu einem beliebigen Zeitpunkt dar, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern.

```
300 Clients x 100.000 Dateien pro Client x 110 Byte = 3,1 GB
```

Addieren Sie diesen Wert zu der Schätzung für die Größe der aktiven Protokolldatei, die für grundlegende Clientspeicheroperationen berechnet wurde.

Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen

Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.

Linux: Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen

Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.

Wenn beispielsweise einmal pro Woche eine Datenbankgesamtsicherung ausgeführt wird, muss der Speicherbereich für das Archivprotokoll groß genug sein, um die Informationen einer vollständigen Woche im Archivprotokoll aufnehmen zu können.

Die unterschiedliche Größe des Archivprotokolls für täglich ausgeführte Datenbankgesamtsicherungen wird in dem Beispiel in der folgenden Tabelle gezeigt.

Tabelle 1. Datenbankgesamtsicherungen

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3453 Byte	3053 Byte für jede Datei plus 200 Byte für jeden Kopienspeicherpool. Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	20 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		
		`4 + 16 = 20 GB`

Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Tag	60 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Sicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen:
		
		`4 GB x 3 = 12 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		
		`12 + 48 = 60 GB`

Element	Beispielwerte	Beschreibung

Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Woche	132 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen. Multiplizieren Sie das Ergebnis mit der Anzahl Tage, die zwischen Datenbankgesamtsicherungen liegen.
		`(4 GB x 3 ) x 7 = 84 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		`84 + 48 = 132 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Anfangsgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Linux: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Datendeduplizierungsoperationen schätzen

Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

Die folgenden Faktoren haben Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll:

Volumen der deduplizierten Daten
: Welche Auswirkungen die Datendeduplizierung auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll hat, ist von dem Prozentsatz an Daten abhängig, der für die Deduplizierung auswählbar ist. Ist der Prozentsatz an Daten, die dedupliziert werden können, relativ hoch, ist mehr Protokollspeicherbereich erforderlich.

Größe und Anzahl Speicherbereiche
: Für jeden Speicherbereich, der durch einen Prozess zum Identifizieren doppelter Daten identifiziert wird, sind ungefähr 1.500 Byte Speicherbereich für die aktive Protokolldatei erforderlich. Werden beispielsweise 250.000 Speicherbereiche durch einen erkennen identifiziert, beträgt die geschätzte Größe der aktiven Protokolldatei 358 MB:

```
250.000 während jedes Prozesses ermittelte Speicherbereiche x 1.500 Byte
 für jeden Speicherbereich = 358 MB
```

Betrachten Sie das folgende Szenario. 300 Clients für Sichern/Archivieren sichern jede Nacht bis zu 100.000 Dateien. Diese Aktivität hat eine Last von 30.000.000 Dateien zur Folge. Die durchschnittliche Anzahl Speicherbereiche für jede Datei ist 2. Demzufolge beträgt die Gesamtzahl Speicherbereiche 60.000.000 und der Speicherbedarf für das Archivprotokoll 84 GB:

```
60.000.000 Speicherbereiche x 1.500 Byte pro Speicherbereich = 84 GB
```

Ein Prozess zum Identifizieren doppelter Daten wird für Aggregate von Dateien ausgeführt. Ein Aggregat besteht aus Dateien, die in einer bestimmten Transaktion gespeichert sind, wie durch die Serveroption TXNGROUPMAX angegeben. Angenommen, die Serveroption TXNGROUPMAX ist auf den Standardwert 4096 gesetzt. Wenn die durchschnittliche Anzahl Speicherbereiche für jede Datei 2 beträgt, ist die Gesamtzahl Speicherbereiche in jedem Aggregat 8192 und der für die aktive Protokolldatei erforderliche Speicherbedarf 12 MB:

```
8192 Speicherbereiche in jedem Aggregat x 1500 Byte pro Speicherbereich =
   12 MB
```

Timing und Anzahl der Prozesse zum Identifizieren doppelter Daten
: Das Timing und die Anzahl Prozesse zum Identifizieren doppelter Daten haben ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei. Bei Verwendung der in dem vorhergehenden Beispiel berechneten Größe der aktiven Protokolldatei von 12 MB beträgt die gleichzeitige Last für die aktive Protokolldatei 120 MB, wenn 10 Prozesse zum Identifizieren doppelter Daten parallel ausgeführt werden:

```
12 MB pro Prozess x 10 Prozesse = 120 MB
```

Dateigröße
: Große Dateien, die für die Identifizierung doppelter Daten verarbeitet werden, können ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei haben. Beispiel: Angenommen, ein Client für Sichern/Archivieren sichert ein Dateisystemimage mit einer Größe von 80 GB. Die Anzahl doppelter Speicherbereiche für dieses Objekt kann groß sein, wenn beispielsweise die in das Dateisystemimage eingeschlossenen Dateien mit Teilsicherungen gesichert wurden. Beispiel: Angenommen, ein Dateisystemimage hat 1,2 Millionen doppelte Speicherbereiche. Die 1,2 Millionen Speicherbereiche in dieser großen Datei stellen eine einzige Transaktion für einen Prozess zum

Identifizieren doppelter Daten dar. Der Gesamtspeicherbereich in der aktiven Protokolldatei, der für dieses einzelne Objekt erforderlich ist, beträgt 1,7 GB:

```
1.200.000 Speicherbereich x 1.500 Byte pro Speicherbereich = 1,7 GB
```

Wenn andere, kleinere Prozesse zum Identifizieren doppelter Daten zu demselben Zeitpunkt ausgeführt werden wie der Prozess zum Identifizieren doppelter Daten für ein einzelnes großes Objekt, ist in der aktiven Protokolldatei möglicherweise nicht genügend Speicherbereich verfügbar. Beispiel: Angenommen, ein Speicherpool ist für die Deduplizierung aktiviert. Der Speicherpool enthält gemischte Daten, einschließlich vieler relativ kleiner Dateien mit einer Größe von 10 KB bis zu mehreren hundert KB. Der Speicherpool enthält außerdem einige wenige große Objekte mit einem hohen Prozentsatz an doppelten Speicherbereichen.

Um nicht nur den Speicherbedarf zu berücksichtigen, sondern auch das Timing und die Dauer gleichzeitig ablaufender Transaktionen, erhöhen Sie die geschätzte Größe der aktiven Protokolldatei um den Faktor 2. Beispiel: Angenommen, das Ergebnis Ihrer Berechnungen für den Speicherbedarf lautet 25 GB (23,3 GB + 1,7 GB für die Deduplizierung eines großen Objekts). Wenn Deduplizierungsverarbeitung gleichzeitig ausgeführt werden, beträgt die vorgeschlagene Größe der aktiven Protokolldatei 50 GB. Die vorgeschlagene Größe des Archivprotokolls ist 150 GB.

Die Beispiele in den folgenden Tabellen zeigen Berechnungen für aktive Protokolldateien und Archivprotokolle. In dem Beispiel in der ersten Tabelle wird eine durchschnittliche Größe von 700 KB für Speicherbereiche verwendet. In dem Beispiel in der zweiten Tabelle wird eine durchschnittliche Größe von 256 KB verwendet. Wie den Beispielen zu entnehmen ist, zeigt die durchschnittliche Größe doppelter Speicherbereiche von 256 KB eine größere geschätzte Größe für die aktive Protokolldatei an. Um betriebsbezogene Probleme für den Server auf ein Mindestmaß reduzieren oder zu verhindern, verwenden Sie 256 KB für die Schätzung der Größe der aktiven Protokolldatei in Ihrer Produktionsumgebung.

Tabelle 1. Durchschnittliche Größe doppelter Speicherbereiche von 700 KB

Element	**Beispielwerte**		**Beschreibung**
Größe des größten zu deduplizierenden Objekts	800 GB	4 TB	Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.
Durchschnittliche Größe der Speicherbereiche	700 KB	700 KB	Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.
Speicherbereiche für eine bestimmte Datei	1.198.372 Bit	6.135.667 Bit	Bei Verwendung der durchschnittlichen Speicherbereichsgröße (700 KB), geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an. Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt: `(800 GB ÷ 700 KB) = 1.198.372 Bit` Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt: `(4 TB ÷ 700 KB) = 6.135.667 Bit`
Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist	1,7 GB	8,6 GB	Der geschätzte Speicherbereich für die aktive Protokolldatei, der für diese Transaktion benötigt wird.

Element	Beispielwerte		Beschreibung

Aktive Protokolldatei: vorgeschlagene Gesamtgröße	66 GB [1]	79,8 GB [1]	Multiplizieren Sie, nachdem zusätzlich zur Deduplizierung andere Aspekte der Last auf dem Server berücksichtigt wurden, die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`(23,3 GB + 1,7 GB) x 2 = 50 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`50 + 16 = 66 GB`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`(23,3 GB + 8,6 GB) x 2 = 63,8 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`63,8 + 16 = 79,8 GB`

Archivprotokoll: vorgeschlagene Größe	198 GB [1]	239,4 GB [1]	Multiplizieren Sie die geschätzte Größe der aktiven Protokolldatei mit dem Faktor 3.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`50 GB x 3 = 150 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`150 + 48 = 198 GB`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`63,8 GB x 3 = 191,4 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`191,4 + 48 = 239,4 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Tabelle 2. Durchschnittliche Größe doppelter Speicherbereiche von 256 KB

Element	Beispielwerte		Beschreibung
Größe des größten zu deduplizierenden Objekts	800 GB	4 TB	Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.
Durchschnittliche Größe der Speicherbereiche	256 KB	256 KB	Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.

Element	Beispielwerte		Beschreibung

Speicherbereiche für eine bestimmte Datei	3.276.800 Bit	16.777.216 Bit	Bei Verwendung der durchschnittlichen Speicherbereichsgröße, geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`(800 GB ÷ 256 KB) = 3.276.800 Bit`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`(4 TB ÷ 256 KB) = 16.777.216 Bit`

Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist	4,5 GB	23,4 GB	Die geschätzte Größe des Speicherbereichs für die aktive Protokolldatei, die für diese Transaktion erforderlich ist.

Aktive Protokolldatei: vorgeschlagene Gesamtgröße	71,6 GB [1]	109,4 GB [1]	Nachdem Sie neben der Deduplizierung andere Aspekte der Serverauslastung mit berücksichtigt haben, multiplizieren Sie die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`(23,3 GB + 4,5 GB) x 2 = 55,6 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`55,6 + 16 = 71,6 GB`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`(23,3 GB + 23,4 GB) x 2 = 93,4 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`93,4 + 16 = 109,4 GB`

Archivprotokoll: vorgeschlagene Größe	214,8 GB [1]	328,2 GB [1]	Die geschätzte Größe der aktiven Protokolldatei multipliziert mit dem Faktor 3.
			
			Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`55,6 GB x 3 = 166,8 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`166,8 + 48 = 214,8 GB`
			
			Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt:
			
			`93,4 GB x 3 = 280,2 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`280,2 + 48 = 328,2 GB`

Element	Beispielwerte	Beschreibung
[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen. Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.		

Linux: Speicherbereich des Spiegels für aktive Protokolldateien

Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.

Die Erstellung einer Protokollspiegel ist eine vorgeschlagene Option. Wenn Sie die aktive Protokolldatei vergrößern, wird der Protokollspiegel automatisch vergrößert. Die Spiegelung des Protokolls kann sich negativ auf die Leistung auswirken, da die doppelte E/A-Aktivität erforderlich ist, um den Spiegel zu verwalten. Der zusätzliche Speicherbereich, den der Protokollspiegel benötigt, ist ein weiterer Faktor, der bei der Entscheidung über die Erstellung eines Protokollspiegels berücksichtigt werden muss.

Wenn das Spiegelprotokollverzeichnis voll wird, gibt der Server Fehlernachrichten in das Aktivitätenprotokoll und in die Datei db2diag.log aus. Die Serveraktivität wird fortgesetzt.

Linux: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle

Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

Durch Angabe eines Übernahmeverzeichnisses für Archivprotokolle können Probleme verhindert werden, die auftreten, wenn der Speicherbereich der Archivprotokolldatei nicht mehr ausreicht. Wenn sowohl das Verzeichnis für Archivprotokolle als auch das Laufwerk oder das Dateisystem, in dem sich das Übernahmeverzeichnis für Archivprotokolle befindet, voll wird, bleiben die Daten im Verzeichnis für aktive Protokolldateien. Dadurch kann die aktive Protokolldatei vollständig ausgefüllt werden, was einen Serverhalt verursacht.

Linux: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen

Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.

Aktive Protokolldatei

Wenn der verfügbare Speicherbereich für die aktive Protokolldatei zu gering ist, werden die folgenden Nachrichten im Aktivitätenprotokoll angezeigt:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER
: Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Der IBM Spectrum Protect-Server startet eine Datenbankgesamtsicherung.

  Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dsmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
: Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Sie müssen die Datenbank manuell sichern.

  Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dsmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
: Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Wenn mindestens eine einzige Datenbankgesamtsicherung ausgeführt wurde, startet der IBM Spectrum Protect-Server eine Teilsicherung der Datenbank. Andernfalls startet der Server eine Datenbankgesamtsicherung.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
: Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Sie müssen die Datenbank manuell sichern.

Archivprotokoll

Wenn der verfügbare Speicherbereich für das Archivprotokoll zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
Das Verhältnis des belegten Speicherbereichs für das Archivprotokoll zum verfügbaren Speicherbereich für das Archivprotokoll überschreitet den Schwellenwert für die Protokollauslastung. Der IBM Spectrum Protect-Server startet eine automatische Datenbankgesamtsicherung.

Datenbank

Wenn der verfügbare Speicherbereich für Datenbankaktivitäten zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
Der belegte Speicherplatz in der Datenbank überschreitet den Schwellenwert für die Belegung des Speicherplatzes in der Datenbank. Um den Speicherplatz für die Datenbank zu vergrößern, verwenden Sie den Befehl EXTEND DBSPACE oder das Dienstprogramm DSMSERV FORMAT mit dem Parameter DBDIR.
ANR1546W: FILESYSTEM_DBPATH_LESS_1GB
Der verfügbare Speicherbereich in dem Verzeichnis, in dem sich die Serverdatenbankdateien befinden, beträgt weniger als 1 GB.

Wenn ein IBM Spectrum Protect-Server mit dem Dienstprogramm DSMSERV FORMAT oder dem Konfigurationsassistenten erstellt wird, werden auch eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien erstellt, in denen Datenbankinformationen gespeichert werden sollen, die vom Datenbankmanager verwendet werden. Der in dieser Nachricht angegebene Pfad gibt die Speicherposition der Datenbankinformationen an, die vom Datenbankmanager verwendet werden. Ist in dem Pfad kein Speicherbereich verfügbar, ist der Server nicht mehr funktionsfähig.

Sie müssen dem Dateisystem Speicherbereich hinzufügen oder in dem Dateisystem oder auf der Platte Speicherbereich freigeben.

Linux: Rollbackdateien der Installation löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

Informationen zu diesem Vorgang

Zum Löschen der nicht mehr benötigten Dateien verwenden Sie den grafisch orientierten Installationsassistenten oder die Befehlszeile im Konsolenmodus.

- Linux: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen
  Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.
- Linux: Rollbackdateien für die Installation mit der Befehlszeile löschen
  Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

Linux: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.

Vorgehensweise

1. Öffnen Sie IBM Installation Manager.
   Linux-BetriebssystemeIn dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus, um IBM Installation Manager zu starten:

   ```
   ./IBMIM
   ```

2. Klicken Sie auf Datei > Benutzervorgaben.
3. Wählen Sie Dateien für Rollback aus.
4. Klicken Sie auf Gespeicherte Dateien löschen und dann auf OK.

Linux: Rollbackdateien für die Installation mit der Befehlszeile löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

Vorgehensweise

1. In dem Verzeichnis, in dem IBM® Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
   - Linux-Betriebssystemeeclipse/tools

   Beispiel:

   - Linux-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Geben Sie im Verzeichnis tools den folgenden Befehl aus, um eine IBM Installation Manager-Befehlszeile zu starten:
   - Linux-Betriebssysteme `./imcl -c`
3. Geben Sie `P` ein, um Benutzervorgaben auszuwählen.
4. Geben Sie `3` ein, um Dateien für Rollback auszuwählen.
5. Geben Sie `D` ein, um die Dateien für Rollback zu löschen.
6. Geben Sie `A` ein, um die Änderungen anzuwenden und zum Benutzervorgabenmenü zurückzukehren.
7. Geben Sie `C` ein, um das Benutzervorgabenmenü zu verlassen.
8. Geben Sie `X` ein, um Installation Manager zu beenden.

Linux: Empfehlungen für die Serverbenennung

Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.

Instanzbenutzer-ID

Die Instanzbenutzer-ID wird als Basis für andere Namen verwendet, die sich auf die Serverinstanz beziehen. Die Instanzbenutzer-ID wird auch als Instanzeigner bezeichnet.

Zum Beispiel: tsminst1

Die Instanzbenutzer-ID ist die Benutzer-ID, die über das Eigentumsrecht oder über Schreib-/Lesezugriffsberechtigung für alle Verzeichnisse verfügen muss, die Sie für die Datenbank und das Wiederherstellungsprotokoll erstellen. Der Server wird standardmäßig mit der Instanzbenutzer-ID ausgeführt. Diese Benutzer-ID benötigt außerdem Schreib-/Lesezugriff für die Verzeichnisse, die für die Einheitenklasse FILE verwendet werden.

Linux-Betriebssysteme

Ausgangsverzeichnis für die Instanzbenutzer-ID

Das Ausgangsverzeichnis kann während der Erstellung der Instanzbenutzer-ID erstellt werden. Hierfür wird die Option für die Erstellung eines Ausgangsverzeichnisses (-m) verwendet, falls es noch nicht vorhanden ist. Abhängig von den lokalen Einstellungen kann das Verzeichnis folgendes Format haben: /home/*Instanzbenutzer-ID*

Zum Beispiel: /home/tsminst1

Das Ausgangsverzeichnis dient hauptsächlich zur Aufbewahrung des Profils für die Benutzer-ID und für Sicherheitseinstellungen.

Linux-Betriebssysteme

Datenbankinstanzname

Der Datenbankinstanzname muss mit der Instanzbenutzer-ID identisch sein, mit der Sie die Serverinstanz ausführen.

Zum Beispiel: tsminst1

Linux-Betriebssysteme

Instanzverzeichnis

Das Instanzverzeichnis enthält spezielle Dateien für eine Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). Es kann einen beliebigen Name haben. Um die Identifizierung zu erleichtern, sollten Sie einen Namen verwenden, der das Verzeichnis mit dem Instanznamen verknüpft.

Sie können das Instanzverzeichnis als Unterverzeichnis des Ausgangsverzeichnisses für die Instanzbenutzer-ID erstellen. Zum Beispiel: /home/*Instanzbenutzer-ID*/*Instanzbenutzer-ID*

Im folgenden Beispiel befindet sich das Instanzverzeichnis im Ausgangsverzeichnis der Benutzer-ID tsminst1: /home/tsminst1/tsminst1

Sie können das Verzeichnis auch an einer anderen Position erstellen, zum Beispiel: /tsmserver/tsminst1

Im Instanzverzeichnis sind folgende Dateien für die Serverinstanz gespeichert:

- Serveroptionsdatei dsmserv.opt

- Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
- Einheitenkonfigurationsdatei, wenn die Serveroption DEVCONFIG keinen vollständig qualifizierten Namen angibt
- Protokolldatei für Datenträger, wenn die Serveroption VOLUMEHISTORY keinen vollständig qualifizierten Namen angibt
- Datenträger für Speicherpools mit dem Typ DEVTYPE=FILE, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
- Benutzerexits
- Traceausgabe (wenn nicht vollständig qualifiziert)

Datenbankname

Der Datenbankname lautet für jede Serverinstanz immer TSMDB1. Dieser Name kann nicht geändert werden.

Servername

Der Servername ist ein interner Name für IBM Spectrum Protect und wird für Operationen verwendet, bei denen eine Datenübertragung zwischen mehreren IBM Spectrum Protect-Servern auftritt. Zum Beispiel bei der Kommunikation zwischen Servern und bei der gemeinsamen Nutzung von Speicherarchiven.

Linux-BetriebssystemeDer Servername wird auch verwendet, wenn Sie den Server dem Operations Center hinzufügen, so dass er mit dieser Schnittstelle verwaltet werden kann. Verwenden Sie einen eindeutigen Namen für jeden Server. Verwenden Sie einen Namen, der die Position oder den Zweck des Servers angibt, um die Identifikation im Operations Center (oder mit einem Befehl QUERY SERVER) zu erleichtern. Nachdem ein IBM Spectrum Protect-Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.

Wenn Sie den Assistenten verwenden, wird als Standardname der Hostname des von Ihnen verwendeten Systems vorgeschlagen. Sie können einen anderen, für Ihre Umgebung aussagekräftigen Namen verwenden. Befinden sich mehrere Server auf dem System, können Sie bei Verwendung des Assistenten den Standardnamen nur für einen der Server angeben. Sie müssen einen eindeutigen Namen für jeden Server eingeben.

Linux-BetriebssystemeZum Beispiel:

- `LOHNBUCHHALTUNG`
- `VERTRIEB`

Verzeichnisse für Datenbankbereich und Wiederherstellungsprotokoll

Die Verzeichnisse können gemäß den lokalen Vorgaben benannt werden. Sie sollten Namen verwenden, die die Verzeichnisse mit der Serverinstanz verknüpfen, um die Identifikation zu erleichtern.

Beispiel für das Archivprotokoll:

- Linux-Betriebssysteme/tsminst1_archlog

Linux: Installationsverzeichnisse

Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

Das Verzeichnis /opt/tivoli/tsm/server/bin ist das Standardverzeichnis, das den Servercode und die Lizenzierung enthält.

Das während der Installation des IBM Spectrum Protect-Servers installierte DB2-Produkt hat die in den DB2-Informationsquellen dokumentierte Verzeichnisstruktur. Schützen Sie diese Verzeichnisse und Dateien wie die Serververzeichnisse. Das Standardverzeichnis heißt /opt/tivoli/tsm/db2.

Sie können folgende Sprachen verwenden: Englisch (US), Deutsch, Französisch, Italienisch, Spanisch, Portugiesisch (Brasilien), Koreanisch, Japanisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Chinesisch GBK, Chinesisch Big5 und Russisch.

Linux: Serverkomponenten installieren

Für die Installation der Serverkomponenten der Version 8.1.2 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.

Informationen zu diesem Vorgang

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server
  Tipp: Die Datenbank (DB2), Global Security Kit (GSKit) und IBM® Java™ Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.

- Sprachen des Servers
- Lizenz
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

Linux-BetriebssystemeFür die Installation eines Servers der Version 8.1.2 anhand dieses Leitfadens müssen Sie 30 - 45 Minuten einplanen.

- Linux: Installationspaket abrufen
  Das Installationspaket für IBM Spectrum Protect kann von einer IBM Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.
- Linux: IBM Spectrum Protect mit dem Installationsassistenten installieren
  Sie können den Server mit dem grafisch orientierten Assistenten von IBM Installation Manager installieren.
- Linux: IBM Spectrum Protect im Konsolenmodus installieren
  Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.
- Linux: IBM Spectrum Protect im unbeaufsichtigten Modus installieren
  Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.
- Linux: Serversprachenpakete installieren
  Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

Linux: Installationspaket abrufen

Das Installationspaket für IBM Spectrum Protect kann von einer IBM® Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.

Linux-Betriebssysteme

Vorbereitende Schritte

Wenn Sie die Dateien herunterladen wollen, legen Sie als Systembenutzergrenzwert für die maximale Dateigröße 'unlimited' (unbegrenzt) fest, um sicherzustellen, dass die Dateien ordnungsgemäß heruntergeladen werden können:

1. Geben Sie den folgenden Befehl aus, um den Wert für die maximale Dateigröße abzufragen:

   ```
   ulimit -Hf
   ```

2. Wenn als Systembenutzergrenzwert für die maximale Dateigröße nicht 'unlimited' (unbegrenzt) angegeben ist, geben Sie 'unlimited' gemäß den Anweisungen in der Dokumentation Ihres Betriebssystems an.

Vorgehensweise

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:
   - Laden Sie das Serverpaket aus Passport Advantage oder Fix Central herunter.
   - Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.
2. Gehen Sie wie folgt vor, wenn Sie das Paket von einer IBM Download-Site heruntergeladen haben:
   Linux-Betriebssysteme
   a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherplatzbedarf finden Sie im Downloaddokument:
      - IBM Spectrum Protect Technote 4042944
      - IBM Spectrum Protect Extended Edition Technote 4042945
      - IBM Spectrum Protect for Data Retention Technote 4042946

   b. Laden Sie die Paketdatei in ein beliebiges Verzeichnis herunter. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.

   c. Stellen Sie sicher, dass die Berechtigung zur Ausführung für das Paket definiert ist. Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

      ```
      chmod a+x Paketname.bin
      ```

   d. Geben Sie den folgenden Befehl aus, um das Paket zu extrahieren:

      ```
      ./Paketname.bin
      ```

      Paketname ist der Name der heruntergeladenen Datei. Zum Beispiel:

      Linux-Betriebssysteme

      ```
      8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
      8.1.x.000-IBM-SPSRV-Linuxs390x.bin
      8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
      ```

3. Wählen Sie eine der folgenden Methoden für die Installation von IBM Spectrum Protect aus:
    - Linux: IBM Spectrum Protect mit dem Installationsassistenten installieren
    - Linux: IBM Spectrum Protect im Konsolenmodus installieren
    - Linux: IBM Spectrum Protect im unbeaufsichtigten Modus installieren
4. Nachdem Sie IBM Spectrum Protect installiert haben und bevor Sie IBM Spectrum Protect für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Support and downloads und legen Sie alle gültigen Fixes an.

Linux: IBM Spectrum Protect mit dem Installationsassistenten installieren

Sie können den Server mit dem grafisch orientierten Assistenten von IBM® Installation Manager installieren.

Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.

Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

Option	Bezeichnung
Installation der Software mithilfe eines heruntergeladenen Pakets:	a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben. b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten zu starten: Linux-Betriebssysteme `./install.sh`

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis logs gespeichert werden.

  Installationsprotokolldateien können Sie anzeigen, indem Sie in Installation Manager auf Datei > Protokoll anzeigen klicken. Um diese Protokolldateien zu erfassen, klicken Sie in Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.

- Linux-BetriebssystemeNachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

Linux: IBM Spectrum Protect im Konsolenmodus installieren

Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.

Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.

Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

Option	Bezeichnung

Option	Bezeichnung
Installation der Software mithilfe eines heruntergeladenen Pakets:	a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben. b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten im Konsolenmodus zu starten: Linux-Betriebssysteme `./install.sh -c` Optional : Generieren Sie während einer Installation im Konsolenmodus eine Antwortdatei. Geben Sie die Optionen für die Installation im Konsolenmodus und in der Anzeige Zusammenfassung `G` an, um die Antworten zu generieren.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  - Linux-Betriebssysteme/var/ibm/InstallationManager/logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
- LinuxBetriebssystemeNachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

Linux: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.

Vorbereitende Schritte

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis input zur Verfügung, in dem das Installationspaket extrahiert wird:

install_response_sample.xml
: Verwenden Sie diese Datei für die Installation der IBM Spectrum Protect-Komponenten.

update_response_sample.xml
: Verwenden Sie diese Datei für das Upgrade der IBM Spectrum Protect-Komponenten.

Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Erstellen Sie eine Antwortdatei. Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.
2. Wenn Sie den Server und das Operations Center im unbeaufsichtigten Modus installieren, erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.
   Wenn Sie die Datei install_response_sample.xml verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist *`mein_Kennwort`* das Kennwort:

   ```
   <variable name='ssl.password' value='mein_Kennwort' />
   ```

   Weitere Informationen zu diesem Kennwort finden Sie in Prüfliste für die Installation.
   Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei update_response_sample.xml aktualisieren.
3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.
   - Linux-Betriebssysteme

     ```
     ./install.sh -s -input Antwortdatei -acceptLicense
     ```

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  - Linux-Betriebssysteme/var/ibm/InstallationManager/logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.

- Linux-BetriebssystemeNachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.

Linux-Betriebssysteme

Linux: Serversprachenpakete installieren

Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

Vorbereitende Schritte

Anweisungen zur Installation von von Sprachenpaketen für Speicheragenten finden Sie unter Language pack configuration for Storage Agent.

- Linux: Spracheinstellungen für den Server
  Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.
- Linux: Sprachenpaket konfigurieren
  Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.
- Linux: Sprachenpaket aktualisieren
  Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

Linux: Spracheinstellungen für den Server

Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.

Linux-BetriebssystemeDieses Sprachenpaket wird automatisch für die folgende Standardsprachenoption für IBM Spectrum Protect-Servernachrichten und -Hilfetext installiert:

- Linux-BetriebssystemeLANGUAGE en_US

Für vom Standard abweichende Sprachen oder Ländereinstellungen installieren Sie das für Ihre Installation erforderliche Sprachenpaket. Sie können die aufgeführten Sprachen verwenden:
Linux-Betriebssysteme

Tabelle 1. Serversprachen für Linux

Sprache	Wert der Option LANGUAGE
Chinesisch, vereinfacht	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chinesisch, traditionell	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
Englisch, Vereinigte Staaten	en_US
	en_US.utf8
Französisch	fr_FR
	fr_FR.utf8
Deutsch	de_DE
	de_DE.utf8
Italienisch	it_IT
	it_IT.utf8
Japanisch	ja_JP
	ja_JP.utf8
Koreanisch	ko_KR
	ko_KR.utf8
Portugiesisch, Brasilianisches	pt_BR
	pt_BR.utf8

Sprache	Wert der Option LANGUAGE
Russisch	ru_RU
	ru_RU.utf8
Spanisch	es_ES
	es_ES.utf8

Linux-BetriebssystemeEinschränkung: Bei Verwendung des Operations Center werden einige Zeichen möglicherweise nicht ordnungsgemäß angezeigt, wenn der Web-Browsers und der Server nicht dieselbe Sprache verwenden. Wenn dieses Problem auftritt, geben Sie im Browser dieselbe Sprache wie im Server an.

Linux: Sprachenpaket konfigurieren

Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.

Informationen zu diesem Vorgang

Linux-BetriebssystemeFühren Sie eine der folgenden Tasks aus, um die Unterstützung für eine bestimmte Ländereinstellung zu aktivieren:

- Geben Sie in der Option LANGUAGE in der Serveroptionsdatei den Namen der Ländereinstellung an, die verwendet werden soll. Beispiel:
  - Linux-BetriebssystemeSoll die Ländereinstellung `it_IT` verwendet werden, setzen Sie die Option LANGUAGE auf `it_IT`. Siehe Linux: Spracheinstellungen für den Server.
- Linux-BetriebssystemeWenn Sie den Server im Vordergrund starten, definieren Sie die Umgebungsvariable `LC_ALL` gemäß dem in der Serveroptionsdatei definierten Wert. Soll beispielsweise die Umgebungsvariable für Italienisch definiert werden, geben Sie folgenden Wert ein:

  ```
  export LC_ALL=it_IT
  ```

Wenn die Ländereinstellung erfolgreich initialisiert wird, steuert sie die Datums-, Uhrzeit- und Zahlenformatierung für den Server. Wenn die Ländereinstellung nicht erfolgreich initialisiert wird, verwendet der Server die englischen (US) Nachrichtendateien und das Datums-, Uhrzeit- und Zahlenformat der englischen (US) Ländereinstellung.

Linux: Sprachenpaket aktualisieren

Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

Informationen zu diesem Vorgang

Sie können ein anderes Sprachenpaket in derselben IBM Spectrum Protect-Instanz installieren.

- Verwenden Sie die Funktion Ändern von IBM Installation Manager, um ein anderes Sprachenpaket zu installieren.
- Verwenden Sie die Funktion Aktualisieren von IBM Installation Manager, um eine Aktualisierung auf neuere Versionen der Sprachenpakete durchzuführen.

Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.

Linux: Die ersten Schritte nach der Installation von IBM Spectrum Protect

Nach der Installation von Version 8.1.2 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.

Informationen zu diesem Vorgang

1. Linux-BetriebssystemeAktualisieren Sie die Kernelparameterwerte.

   Linux-BetriebssystemeSiehe Linux: Kernelparameter für Linux-Systeme optimieren.

2. Erstellen Sie die Verzeichnisse und die Benutzer-ID für die Serverinstanz. Siehe Linux: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen.
3. Konfigurieren Sie eine Serverinstanz. Wählen Sie eine der folgenden Optionen aus:
   - Verwenden Sie den Konfigurationsassistenten (die bevorzugte Methode). Siehe Linux: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren.
   - Konfigurieren Sie die neue Instanz manuell. Siehe Linux: Serverinstanz manuell konfigurieren. Führen Sie während einer manuellen Konfiguration die folgenden Schritte aus:
     a. Definieren Sie Ihre Verzeichnisse und erstellen Sie die IBM Spectrum Protect-Instanz. Siehe Linux: Serverinstanz erstellen.

b. Erstellen Sie eine neue Serveroptionsdatei, indem Sie die Musterdatei kopieren, um die Datenübertragung zwischen dem Server und den Clients zu definieren. Siehe Linux-BetriebssystemeLinux: Server- und Clientübertragung konfigurieren.
c. Geben Sie den Befehl DSMSERV FORMAT aus, um die Datenbank zu formatieren. Siehe Linux: Datenbank und Protokoll formatieren.
d. Konfigurieren Sie Ihr System für die Datenbanksicherung. Siehe Linux: Datenbankmanager für die Datenbanksicherung vorbereiten.

4. Konfigurieren Sie Optionen, die die Ausführung der Datenbankreorganisation steuern. Siehe Linux: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren.
5. Starten Sie die Serverinstanz, falls noch nicht gestartet.
   - Linux-BetriebssystemeSiehe Linux: Serverinstanz starten.
6. Registrieren Sie Ihre Lizenz. Siehe Linux: Lizenzregistrierung.
7. Bereiten Sie Ihr System auf Datenbanksicherungen vor. Siehe Linux: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben.
8. Überwachen Sie den Server. Siehe Linux: Server überwachen.

- Linux-BetriebssystemeLinux: Kernelparameter für Linux-Systeme optimieren
  Damit IBM Spectrum Protect und DB2 unter Linux ordnungsgemäß installiert und ausgeführt werden, müssen Sie die Kernelkonfigurationsparameter aktualisieren.
- Linux: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen
  Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.
- Linux: IBM Spectrum Protect-Server konfigurieren
  Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.
- Linux: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren
  Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.
- Linux-BetriebssystemeLinux: Serverinstanz starten
  Sie können den Server mit der Instanzbenutzer-ID (bevorzugte Methode) oder mit der Rootbenutzer-ID starten.
- Linux: Server stoppen
  Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.
- Linux: Lizenzregistrierung
  Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.
- Linux: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben
  Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.
- Linux: Mehrere Serverinstanzen auf einem System ausführen
  Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.
- Linux: Server überwachen
  Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

Linux-Betriebssysteme

Linux: Kernelparameter für Linux-Systeme optimieren

Damit IBM Spectrum Protect und DB2 unter Linux ordnungsgemäß installiert und ausgeführt werden, müssen Sie die Kernelkonfigurationsparameter aktualisieren.

Informationen zu diesem Vorgang

Wenn Sie diese Parameter nicht aktualisieren, kann die Installation von DB2 und IBM Spectrum Protect fehlschlagen. Auch wenn die Installation erfolgreich verläuft, können Betriebsfehler auftreten, wenn Sie keine Parameterwerte definieren.

- Linux-BetriebssystemeLinux: Kernelparameter unter Linux aktualisieren
  DB2 erhöht IPC-Kernelparameterwerte automatisch auf die bevorzugten Einstellungen (IPC = Interprocess Communication, Interprozesskommunikation).
- Linux-BetriebssystemeLinux: Wertvorschläge für Kernelparameter unter Linux
  Stellen Sie sicher, dass die Werte für Kernelparameter ausreichen, um Betriebsfehler während der Ausführung des IBM Spectrum Protect-Servers zu verhindern.

Linux-Betriebssysteme

Linux: Kernelparameter unter Linux aktualisieren

DB2 erhöht IPC-Kernelparameterwerte automatisch auf die bevorzugten Einstellungen (IPC = Interprocess Communication, Interprozesskommunikation).

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um die Kernelparameter auf Linux-Servern zu aktualisieren:

Vorgehensweise

1. Geben Sie den Befehl ipcs -l aus, um die Parameterwerte aufzulisten.
2. Analysieren Sie die Ergebnisse, um festzustellen, ob für Ihr System Änderungen erforderlich sind. Wenn Änderungen erforderlich sind, können Sie den Parameter in der Datei /etc/sysctl.conf definieren. Der Parameterwert wird beim Systemstart angewendet.

Nächste Schritte

In Red Hat Enterprise Linux 6 (RHEL6) müssen Sie den Parameter `kernel.shmmax` in der Datei /etc/sysctl.conf definieren, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird.

Ausführliche Informationen zur DB2-Datenbank für Linux finden Sie in der Produktinformation zu DB2.


Linux-Betriebssysteme

Linux: Wertvorschläge für Kernelparameter unter Linux

Stellen Sie sicher, dass die Werte für Kernelparameter ausreichen, um Betriebsfehler während der Ausführung des IBM Spectrum Protect-Servers zu verhindern.

Informationen zu diesem Vorgang

Die folgende Tabelle enthält die Vorschläge für Kernelparametereinstellungen für die Ausführung von IBM Spectrum Protect und DB2.

Parameter	Beschreibung	Bevorzugter Wert
kernel.randomize_va_space	Der Parameter kernel.randomize_va_space konfiguriert die Verwendung von Speicher-ASLR des Kernels. Wenn Sie den Wert 0 definieren (`kernel.randomize_va_space=0`), wird ASLR inaktiviert. DB2-Datenserver sind für bestimmte Objekte des gemeinsam genutzten Speichers auf festgelegte Adressen angewiesen und ASLR (Address Space Layout Randomization) kann bei einigen Aktivitäten Fehler verursachen. Ausführliche Informationen zu Linux ASLR und DB2 finden Sie in http://www.ibm.com/support/docview.wss?uid=swg21365583.	0
vm.swappiness	Der Parameter vm.swappiness legt fest, ob der Kernel Anwendungsspeicher aus dem physischen Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern finden Sie unter Produktinformation zu DB2.	0
vm.overcommit_memory	Der Parameter vm.overcommit_memory hat Einfluss auf die Größe des virtuellen Speichers, deren Zuordnung der Kernel zulassen kann. Weitere Informationen zu Kernelparametern finden Sie unter Produktinformation zu DB2.	0

Linux: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen

Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.

Vorbereitende Schritte

Lesen Sie die Informationen zur Planung des Speicherbereichs für den Server, bevor Sie diese Task ausführen. Siehe Linux: Arbeitsblätter für Planungsdetails für den Server.

Vorgehensweise

1. Erstellen Sie die Benutzer-ID, die Eigner der Serverinstanz sein soll. Diese Benutzer-ID verwenden Sie später bei der Erstellung der Serverinstanz.

   Linux-Betriebssysteme
   Linux-BetriebssystemeErstellen Sie eine Benutzer-ID und eine Gruppe, die Eigner der Serverinstanz sein sollen.
   a. Die folgenden Befehle können mit einer Verwaltungsbenutzer-ID ausgeführt werden, die den Benutzer und die Gruppe definieren soll. Erstellen Sie die Benutzer-ID und Gruppe im Ausgangsverzeichnis des Benutzers.
   Einschränkung: In der Benutzer-ID dürfen nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstreichungszeichen (_) verwendet werden. Die Benutzer-ID und der Gruppenname müssen die folgenden Regeln einhalten:
      - Die maximale Länge beträgt 8 Zeichen.
      - Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder mit einer Ziffer beginnen.
      - Als Benutzer-ID und Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* und kein reserviertes SQL-Wort verwendet werden.

      Erstellen Sie beispielsweise die Benutzer-ID `tsminst1` in der Gruppe `tsmsrvrs`. Die folgenden Beispiele zeigen, wie diese Benutzer-ID und diese Gruppe mit Betriebssystembefehlen erstellt werden.

      Linux-Betriebssysteme

      ```
      groupadd tsmsrvrs -g 1111
      useradd -d /home/tsminst1 -u 2222 -g 1111 -s /bin/bash tsminst1
      passwd tsminst1
      ```

      Einschränkung: DB2 unterstützt nicht die direkte Authentifizierung von Betriebssystembenutzern durch LDAP.
   b. Melden Sie sich ab und dann bei Ihrem System an. Wechseln Sie zu dem gerade erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, z. B. Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es ggf. ändern können.

2. Erstellen Sie die vom Server benötigten Verzeichnisse.
   Linux-BetriebssystemeErstellen Sie leere Verzeichnisse für jeden Tabelleneintrag und stellen Sie sicher, dass die neue Benutzer-ID, die Sie gerade erstellt haben, Eigner der Verzeichnisse ist. Hängen Sie den zugeordneten Speicher in jedem der Verzeichnisse für aktive Protokolldateien, für Archivprotokolle und Datenbanken an.

Element	Beispielbefehle für die Verzeichniserstellung	Ihre Verzeichnisse
Das *Instanzverzeichnis* für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien).	`mkdir /tsminst1`	

Die Datenbankverzeichnisse	`mkdir /tsmdb001`
	`mkdir /tsmdb002`
	`mkdir /tsmdb003`
	`mkdir /tsmdb004`	

Verzeichnis für aktive Protokolldateien	`mkdir /tsmlog`	
Verzeichnis für Archivprotokolle	`mkdir /tsmarchlog`	
Optional: Verzeichnis für den Protokollspiegel für die aktive Protokolldatei	`mkdir /tsmlogmirror`	
Optional: Sekundäres Verzeichnis für Archivprotokolle (Übernahmeverzeichnis für Archivprotokolle)	`mkdir /tsmarchlogfailover`	

   Wenn ein Server anfänglich mit dem Dienstprogramm DSMSERV FORMAT oder mit dem Konfigurationsassistenten erstellt wird, werden eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien zum Speichern von Datenbankinformationen erstellt, die vom Datenbankmanager verwendet werden.

3. Melden Sie die neue Benutzer-ID ab.

Linux: IBM Spectrum Protect-Server konfigurieren

Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.

Informationen zu diesem Vorgang

Wählen Sie eine der folgenden Optionen aus, um eine IBM Spectrum Protect-Serverinstanz zu konfigurieren:

- Linux: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren
  Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI)

verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.

- Linux: Serverinstanz manuell konfigurieren
  Nach der Installation von IBM Spectrum Protect Version 8.1.2 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

Linux: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren

Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.

Vorbereitende Schritte

Bevor Sie den Konfigurationsassistenten starten, müssen Sie alle vorhergehenden Schritte zur Vorbereitung der Konfiguration ausführen. Zu diesen Schritten gehören die Installation von IBM Spectrum Protect, die Erstellung der Datenbank- und Protokollverzeichnisse und die Erstellung der Verzeichnisse und der Benutzer-ID für die Serverinstanz.

Vorgehensweise

1. Stellen Sie sicher, dass folgende Anforderungen erfüllt sind:  Linux-Betriebssysteme
   - Das System, auf dem Sie IBM Spectrum Protect installiert haben, muss über den X Window System-Client verfügen. Außerdem müssen Sie einen X Window System-Server auf Ihrem Desktop ausführen.
   - Im System muss das SSH-Protokoll (Secure Shell) aktiviert sein. Stellen Sie sicher, dass für den Port der Standardwert 22 definiert ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei `sshd_config` im Verzeichnis /etc/ssh/ aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämonservice über Zugriffsberechtigungen zum Herstellen einer Verbindung zum System mithilfe des Werts `localhost` verfügt.
   - Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt haben, mit dem SSH-Protokoll bei IBM Spectrum Protect anmelden können. Bei Verwendung des Assistenten müssen Sie diese Benutzer-ID und dieses Kennwort für den Zugriff auf dieses System angeben.
   - Starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.
2. Starten Sie die lokale Version des Assistenten:
   -  Linux-BetriebssystemeÖffnen Sie das Programm `dsmicfgx` im Verzeichnis /opt/tivoli/tsm/server/bin. Dieser Assistent kann nur als Root ausgeführt werden.

   Befolgen Sie die Anweisungen zur Ausführung der Konfiguration. Der Assistent kann gestoppt und erneut gestartet werden. Der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

Linux: Serverinstanz manuell konfigurieren

Nach der Installation von IBM Spectrum Protect Version 8.1.2 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

- Linux: Serverinstanz erstellen
  Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl db2icrt.
-  Linux-BetriebssystemeLinux: Server- und Clientübertragung konfigurieren
  Eine standardmäßige Beispielserveroptionsdatei mit dem Namen dsmserv.opt.smp wird während der IBM Spectrum Protect-Installation im Verzeichnis /opt/tivoli/tsm/server/bin erstellt. Sie müssen die Datenübertragung zwischen dem Server und den Clients definieren, indem Sie eine neue Serveroptionsdatei erstellen. Hierfür kopieren Sie die Musterdatei in das Verzeichnis für die Serverinstanz.
- Linux: Datenbank und Protokoll formatieren
  Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.
- Linux: Datenbankmanager für die Datenbanksicherung vorbereiten
  Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

Linux: Serverinstanz erstellen

Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl db2icrt.

Informationen zu diesem Vorgang

Auf einer Workstation kann mindestens eine Serverinstanz vorhanden sein.
 Linux-BetriebssystemeWichtig: Stellen Sie Folgendes sicher, bevor der Befehl db2icrt ausgeführt wird:

- Das Ausgangsverzeichnis für den Benutzer (/home/tsminst1) ist vorhanden. Ist kein Ausgangsverzeichnis vorhanden, müssen Sie es erstellen.

Im Instanzverzeichnis sind folgende Kerndateien gespeichert, die vom IBM Spectrum Protect-Server generiert werden:
  - Serveroptionsdatei dsmserv.opt
  - Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
  - Einheitenkonfigurationsdatei, wenn die Serveroption DEVCONFIG keinen vollständig qualifizierten Namen angibt
  - Protokolldatei für Datenträger, wenn die Serveroption VOLUMEHISTORY keinen vollständig qualifizierten Namen angibt
  - Datenträger für Speicherpools mit dem Typ DEVTYPE=FILE, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
  - Benutzerexits
  - Traceausgabe (wenn nicht vollständig qualifiziert)
- Eine Shellkonfigurationsdatei (z. B. .profile) ist im Ausgangsverzeichnis vorhanden. Die Rootbenutzer- und Instanzbenutzer-ID müssen über Schreibberechtigung für diese Datei verfügen. Weitere Informationen finden Sie in Produktinformation zu DB2. Suchen Sie dort nach den Einstellungen für Linux- und UNIX-Umgebungsvariablen.

Linux-Betriebssysteme

1. Melden Sie sich mit der Root-ID an und erstellen Sie eine IBM Spectrum Protect-Instanz. Der Name der Instanz muss mit dem Namen des Benutzers identisch sein, der Eigner der Instanz ist. Verwenden Sie den Befehl db2icrt und geben Sie den Befehl in eine Zeile ein: Linux-Betriebssysteme

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   Instanzname Instanzname
   ```

   Lautet Ihre Benutzer-ID für diese Instanz z. B. tsminst1, verwenden Sie den folgenden Befehl, um die Instanz zu erstellen. Geben Sie den Befehl in eine einzelne Zeile ein. Linux-Betriebssysteme

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   tsminst1 tsminst1
   ```

   Hinweis: Verwenden Sie ab diesem Punkt diese neue Benutzer-ID für die Konfiguration Ihres IBM Spectrum Protect-Servers. Melden Sie sich mit der Root-ID ab und mit der neuen Instanzbenutzer-ID an.
2. Geben Sie als Standardverzeichnis für die Datenbank das Instanzverzeichnis für den Server an. Sind mehrere Server vorhanden, melden Sie sich mit der Instanz-ID des jeweiligen Servers an. Geben Sie den folgenden Befehl aus:

   ```
   db2 update dbm cfg using dftdbpath Instanzverzeichnis
   ```

   Lautet das Instanzverzeichnis für den Server z. B. 'tsminst1', ändern Sie mit dem folgenden Befehl das Standardverzeichnis für die Datenbank in 'tsminst1':

   ```
   db2 update dbm cfg using dftdbpath /tsminst1
   ```

3. Ändern Sie den Bibliothekspfad, so dass die Version von IBM Global Security Kit (GSKit) verwendet wird, die mit dem Server installiert wird. In den folgenden Beispielen ist *server_bin_directory* ein Unterverzeichnis des Serverinstallationsverzeichnisses. Zum Beispiel /opt/tivoli/tsm/server/bin.
   - Sie müssen die folgenden Dateien aktualisieren, um den Bibliothekspfad zu definieren, wenn DB2 oder der Server gestartet wird:

     Bash- oder Korn-Shell-Beispiel:

     ```
     Instanzbenutzer-Ausgangsverzeichnis/sqllib/userprofile
     ```

     C-Shell-Beispiel:

     ```
     Instanzbenutzer-Ausgangsverzeichnis/sqllib/usercshrc
     ```

   - Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis*/sqllib/userprofile (Bash- oder Korn-Shell) hinzu. Jeder Eintrag befindet sich in jeweils einer Zeile.Linux-Betriebssysteme

     ```
     LD_LIBRARY_PATH=server_bin_directory/dbbkapi:
     /opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH

     export LD_LIBRARY_PATH
     ```

     Hinweis: Der Bibliothekspfad muss folgende Einträge enthalten:
     - /usr/local/ibm/gsk8_64/lib64
     - /opt/ibm/lib
     - /opt/ibm/lib64
     - /usr/lib64
   - Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis*/sqllib/usercshrc (C-Shell) in einer einzigen Zeile hinzu: Linux-Betriebssysteme

     ```
     setenv LD_LIBRARY_PATH server_bin_directory/dbbkapi:
     /opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
     ```

   - Überprüfen Sie die Bibliothekspfadeinstellungen und ob die GSKit-Version 8.0.14.43 oder höher ist. Geben Sie die folgenden Befehle aus: Linux-Betriebssysteme

```
echo $LD_LIBRARY_PATH
gsk8capicmd_64 -version
gsk8ver_64
```

Ist die GSKit-Version nicht 8.0.14.43 oder höher, müssen Sie den IBM Spectrum Protect-Server erneut installieren. Die Neuinstallation stellt sicher, dass die richtige GSKit-Version verfügbar ist.

4. Erstellen Sie eine neue Serveroptionsdatei. Siehe Linux: Server- und Clientübertragung konfigurieren.


Linux-Betriebssysteme

Linux: Server- und Clientübertragung konfigurieren

Eine standardmäßige Beispielserveroptionsdatei mit dem Namen dsmserv.opt.smp wird während der IBM Spectrum Protect-Installation im Verzeichnis /opt/tivoli/tsm/server/bin erstellt. Sie müssen die Datenübertragung zwischen dem Server und den Clients definieren, indem Sie eine neue Serveroptionsdatei erstellen. Hierfür kopieren Sie die Musterdatei in das Verzeichnis für die Serverinstanz.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass ein Serverinstanzverzeichnis, z. B. /tsminst1, vorhanden ist und kopieren Sie die Musterdatei in dieses Verzeichnis. Nennen Sie die neue Datei `dsmserv.opt` und editieren Sie die Optionen. Führen Sie diese Konfiguration vor der Initialisierung der Serverdatenbank aus. Jedes Beispiel bzw. jeder Standardeintrag in der Beispieloptionsdatei ist ein Kommentar in einer Zeile, die mit einem Stern (*) beginnt. Bei Optionen muss die Groß-/Kleinschreibung nicht beachtet werden, und zwischen Schlüsselwörtern und Werten dürfen sich ein oder mehrere Leerzeichen befinden.

Für das Editieren der Optionsdatei gelten folgende Richtlinien:

- Entfernen Sie den Stern am Anfang der Zeile, um eine Option zu aktivieren.
- Beginnen Sie mit der Eingabe der Optionen in einer beliebigen Spalte.
- Geben Sie nur eine Option pro Zeile ein. Die Option muss auf einer Zeile stehen.
- Werden mehrere Einträge für ein Schlüsselwort vorgenommen, verwendet der IBM Spectrum Protect-Server den letzten Eintrag.

Wenn Sie die Serveroptionsdatei ändern, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

Sie können mindestens eine der folgenden Übertragungsmethoden angeben:

- TCP/IP Version 4 oder Version 6
- Shared Memory
- Secure Sockets Layer (SSL)
  Tipp: Sie können Kennwörter im LDAP-Verzeichnisserver oder im IBM Spectrum Protect-Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.

- 
Linux-BetriebssystemeLinux: TCP/IP-Optionen definieren
  Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.
- 
Linux-BetriebssystemeLinux: Shared Memory-Optionen definieren
  Sie können die Shared Memory-Übertragung zwischen Clients und Servern auf demselben System verwenden. Für die Verwendung von Shared Memory muss TCP/IP Version 4 auf dem System installiert sein.
- 
Linux-BetriebssystemeLinux: Secure Sockets Layer-Optionen definieren
  Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

Linux: TCP/IP-Optionen definieren

Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt eine Liste der TCP/IP-Optionen, mit denen Sie Ihr System definieren können.

```
commmethod         tcpip
  tcpport          1500
  tcpwindowsize    0
  tcpnodelay       yes
```

Tipp: Sie können TCP/IP Version 4 und/oder Version 6 verwenden.

TCPPORT
Die Adresse des Server-Ports für TCP/IP- und SSL-Kommunikation. Der Standardwert ist 1500.

Linux-BetriebssystemeTCPWINDOWSIZE

Linux-BetriebssystemeGibt die Größe des TCP/IP-Puffers an, der beim Senden oder Empfangen von Daten verwendet wird. Die in einer Sitzung verwendete Fenstergröße ist der kleinere Wert der Server- und Clientfenstergröße. Größere Fenstergrößen benötigen zusätzlichen

Speicher, können jedoch die Leistung verbessern.

Sie können eine ganze Zahl von 0 bis 2048 angeben. Soll die Standardfenstergröße für das Betriebssystem verwendet werden, geben Sie 0 an.

TCPNODELAY
: Gibt an, ob der Server kleine Nachrichten sendet oder ob TCP/IP die Nachrichten puffern soll. Das Senden kleiner Nachrichten kann den Durchsatz verbessern, erhöht jedoch die Anzahl der im Netz gesendeten Pakete. Geben Sie YES an, wenn kleine Nachrichten gesendet werden sollen, oder NO, wenn sie TCP/IP puffern soll. Der Standardwert ist YES.

TCPADMINPORT
: Gibt die Anschlussnummer an, an der der TCP/IP-DFV-Treiber des Servers auf TCP/IP- oder SSL-fähige Kommunikationsanforderungen warten soll, die keine Clientsitzungen sind. Der Standardwert ist der Wert von TCPPORT.

SSLTCPPORT
: (Nur SSL) Gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen des Befehlszeilenclients für Sichern/Archivieren und des Verwaltungsbefehlszeilenclients wartet.

SSLTCPADMINPORT
: (Nur SSL) Gibt die Anschlussadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen für den Verwaltungsbefehlszeilenclient wartet.

Linux: Shared Memory-Optionen definieren

Sie können die Shared Memory-Übertragung zwischen Clients und Servern auf demselben System verwenden. Für die Verwendung von Shared Memory muss TCP/IP Version 4 auf dem System installiert sein.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt eine Einstellung für Shared Memory:

```
commmethod      sharedmem
   shmport      1510
```

In diesem Beispiel gibt SHMPORT die TCP/IP-Anschlussadresse eines Servers bei Verwendung von Shared Memory an. Verwenden Sie die Option SHMPORT, um einen anderen TCP/IP-Anschluss anzugeben. Die Standardanschlussadresse ist 1510.
COMMMETHOD kann in der IBM Spectrum Protect-Serveroptionsdatei mehrfach mit einem jeweils anderen Wert verwendet werden. Die folgende Angabe ist beispielsweise möglich:

```
commmethod tcpip
commmethod sharedmem
```

 Linux-BetriebssystemeBei Verwendung von Shared Memory empfangen Sie möglicherweise die folgende Nachricht vom Server:

```
ANR9999D shmcomm.c(1598): Thread-ID<39>
Fehler von msgget (2), Fehlernummer = 28
```

Die Nachricht bedeutet, dass eine Nachrichtenwarteschlange erstellt werden muss, der Systemgrenzwert für die maximale Anzahl Nachrichtenwarteschlangen (MSGMNI) jedoch überschritten würde.
 Linux-BetriebssystemeUm die maximale Anzahl der Nachrichtenwarteschlangen (MSGMNI) auf Ihrem System zu bestimmen, geben Sie den folgenden Befehl aus:

```
cat /proc/sys/kernel/msgmni
```

Geben Sie folgenden Befehl aus, um den Wert für MSGMNI auf Ihrem System zu erhöhen:

```
sysctl -w kernel.msgmni=n
```

Dabei ist **n** die maximale Anzahl der Nachrichtenwarteschlangen, die auf dem System zulässig sein sollen.

Linux: Secure Sockets Layer-Optionen definieren

Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

Vorbereitende Schritte

SSL ist die Standardtechnologie für die Erstellung verschlüsselter Sitzungen zwischen Servern und Clients. SSL stellt einen sicheren Kanal für die Server- und Clientkommunikation über offene Kommunikationspfade zur Verfügung. Bei SSL wird die Identität des Servers durch Verwendung digitaler Zertifikate überprüft.

Verwenden Sie SSL für Sitzungen nur im Bedarfsfall, um eine bessere Systemleistung sicherzustellen. Sie könnten die Prozessorressourcen auf dem IBM Spectrum Protect-Server erweitern, um den erhöhten Anforderungen gerecht zu werden.

Linux: Datenbank und Protokoll formatieren

Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.

Nach der Konfiguration der Serverübertragung können Sie die Datenbank initialisieren. Sie müssen sich mit der Instanzbenutzer-ID anmelden. Fügen Sie die Verzeichnisse nicht in Dateisysteme ein, deren Speicherplatz nicht ausreichen könnte. Wenn bestimmte Verzeichnisse (z. B. das Archivprotokoll) nicht verfügbar oder voll werden, stoppt der Server.

Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.

Exitlistenhandler definieren

Geben Sie für jede Serverinstanz ON für die Registry-Variable DB2NOEXITLIST an. Melden Sie sich als Serverinstanzeigner beim System an und geben Sie den folgenden Befehl aus:

```
db2set -i Name_der_Serverinstanz DB2NOEXITLIST=ON
```

Beispiel: Linux-Betriebssysteme

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```

Serverinstanz initialisieren

Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Wenn das Verzeichnis der Serverinstanz z. B. */tsminst1* lautet, geben Sie die folgenden Befehle aus: Linux-Betriebssysteme

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsize=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zu Grunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.
Linux-BetriebssystemeTipp: Wenn DB2 nach Ausgabe des Befehls DSMSERV FORMAT nicht startet, müssen Sie möglicherweise die Mountoption NOSUID des Dateisystems inaktivieren. Wird diese Option in dem Dateisystem definiert, in dem sich das Verzeichnis des DB2-Instanzeigners befindet, oder in einem beliebigen Dateisystem, in dem sich die DB2-Datenbank, aktive Protokolldateien, Archivprotokolle, Übernahmeprotokolle oder Spiegelprotokolle befinden, muss die Option inaktiviert werden, um das System starten zu können.
Nach der Inaktivierung der Option NOSUID hängen Sie das Dateisystem erneut an. Dann starten Sie DB2 mit dem folgenden Befehl:

```
db2start
```

Zugehörige Informationen:
DSMSERV FORMAT (Datenbank und Protokoll formatieren)

Linux: Datenbankmanager für die Datenbanksicherung vorbereiten

Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

Informationen zu diesem Vorgang

Linux-BetriebssystemeAb IBM Spectrum Protect Version 7.1 ist es nicht mehr erforderlich, das API-Kennwort während einer manuellen Konfiguration des Servers zu definieren. Wenn Sie das API-Kennwort während des manuellen Konfigurationsprozesses definieren, können Datenbanksicherungsversuche fehlschlagen.

Wenn Sie den Konfigurationsassistenten verwenden, um eine IBM Spectrum Protect-Serverinstanz zu erstellen, müssen Sie diese Schritte nicht ausführen. Wenn Sie eine Instanz manuell konfigurieren, führen Sie die folgenden Schritte aus, bevor Sie den Befehl BACKUP DB oder RESTORE DB ausgeben.

Achtung: Wenn die Datenbank nicht verwendet werden kann, ist der gesamte IBM Spectrum Protect-Server nicht verfügbar. Wenn eine Datenbank verloren geht und nicht wiederhergestellt werden kann, kann die Wiederherstellung der von diesem Server verwalteten Daten schwierig oder unmöglich sein. Daher ist es unbedingt erforderlich, die Datenbank zu sichern.
Linux-BetriebssystemeIn den folgenden Befehlen müssen Sie die Beispielwerte durch Ihre tatsächlichen Werte ersetzen. In den Beispielen wird `tsminst1` für die Benutzer-ID der Serverinstanz, /tsminst1 für das Verzeichnis der Serverinstanz und /home/tsminst1 als Ausgangsverzeichnis der Serverinstanzbenutzer verwendet.

1. Definieren Sie die Umgebungsvariablenkonfiguration der IBM Spectrum Protect-API für die Datenbankinstanz:
   a. Melden Sie sich mit der Benutzer-ID `tsminst1` an.

b. Wenn der Benutzer `tsminst1` angemeldet ist, stellen Sie sicher, dass die DB2-Umgebung ordnungsgemäß initialisiert wird. Die DB2-Umgebung wird durch Ausführung des Scripts /home/tsminst1/sqllib/db2profile initialisiert, das normalerweise automatisch über das Profil der Benutzer-ID ausgeführt wird. Stellen Sie sicher, dass die `.profile`-Datei im Ausgangsverzeichnis der Instanzbenutzer vorhanden ist, z. B. /home/tsminst1/.profile. Wenn `.profile` das Script `db2profile` nicht ausführt, fügen Sie folgende Zeilen hinzu:

```
if [ -f /home/tsminst1/sqllib/db2profile ]; then
      . /home/tsminst1/sqllib/db2profile
  fi
```

c. Fügen Sie in der Datei *Instanzverzeichnis*/sqllib/userprofile die folgenden Zeilen hinzu:

```
DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
DSMI_DIR=Serververzeichnis_bin/dbbkapi
DSMI_LOG=Serverinstanzverzeichnis
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

Hierbei gilt Folgendes:

- *Instanzverzeichnis* ist das Ausgangsverzeichnis des Serverinstanzbenutzers.
- *Serverinstanzverzeichnis* ist das Serverinstanzverzeichnis.
- *Serververzeichnis_bin* ist das Serververzeichnis 'bin'. Die Standardposition ist /opt/tivoli/tsm/server/bin.

Fügen Sie in der Datei *Instanzverzeichnis*/sqllib/usercshrc die folgenden Zeilen hinzu:

```
setenv DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
setenv DSMI_DIR=Serververzeichnis_bin/dbbkapi
setenv DSMI_LOG=Serverinstanzverzeichnis
```

2. Melden Sie sich ab und als `tsminst1` erneut an oder geben Sie den folgenden Befehl aus:

```
. ~/.profile
```

Tipp: Stellen Sie sicher, dass Sie ein Leerzeichen nach dem ersten Punkt (.) eingeben.

3. Erstellen Sie eine Datei mit dem Namen `tsmdbmgr.opt` im Verzeichnis *Serverinstanz*, das sich in diesem Beispiel im Verzeichnis /tsminst1 befindet, und fügen Sie folgende Zeile hinzu:

```
SERVERNAME TSMDBMGR_TSMINST1
```

Hinweis: Der Wert für `SERVERNAME` muss in den Dateien `tsmdbmgr.opt` und `dsm.sys` konsistent sein.

4. Fügen Sie als Rootbenutzer die folgenden Zeilen zur Konfigurationsdatei `dsm.sys` der IBM Spectrum Protect-API hinzu. Die Konfigurationsdatei `dsm.sys` befindet sich standardmäßig in folgendem Standardverzeichnis:
   - *Serververzeichnis_bin*/dbbkapi/dsm.sys

```
servername TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
tcpport 1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

Erläuterungen:

- *Servername* stimmt mit dem Wert für `servername` in der Datei `tsmdbmgr.opt` überein.
- *Commethod* gibt die Client-API an, mit der Kontakt zum Server wegen der Datenbanksicherung hergestellt wird. Gültige Werte sind `tcpip` und `sharedmem`. Weitere Informationen zu Shared Memory (gemeinsam genutzter Speicher) finden Sie in Schritt 5.
- *Tcpserveraddr* gibt die Serveradresse an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `localhost` lauten.
- *Tcpport* gibt die Anschlussnummer an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Sie müssen denselben `tcpport`-Wert wie in der Serveroptionsdatei dsmserv.opt angeben.
- *Errorlogname* gibt das Fehlerprotokoll an, in dem die Client-API Fehler protokolliert, die während einer Datenbanksicherung auftreten. Dieses Protokoll befindet sich normalerweise im Serverinstanzverzeichnis. Dieses Protokoll kann sich jedoch an jeder beliebigen Position befinden, für die die Instanzbenutzer-ID Schreibberechtigung hat.
- *Nodename* gibt den Knotennamen an, mit dem die Client-API während einer Datenbanksicherung eine Verbindung zum Server herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `$$_TSMDBMGR_$$` lauten.

Linux-BetriebssystemeAchtung: Fügen Sie nicht die Option PASSWORDACCESS generate zur Konfigurationsdatei dsm.sys hinzu. Diese Option kann einen Datenbanksicherungsfehler verursachen.

5. Optional: Konfigurieren Sie den Server für die Datenbanksicherung mithilfe von Shared Memory. Auf diese Weise könnten Sie die Prozessorauslastung verringern und den Durchsatz verbessern. Führen Sie die folgenden Schritte aus:
   a. Überprüfen Sie die Datei dsmserv.opt. Fügen Sie die folgenden Zeilen in die Datei ein, falls nicht vorhanden:

```
commmethod sharedmem
shmport Anschlussnummer
```

Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.

   b. Suchen Sie in der Konfigurationsdatei dsm.sys die folgenden Zeilen:

```
commmethod tcpip
tcpserveraddr localhost
```

```
tcpport Anschlussnummer
```

Ersetzen Sie die angegebenen Zeilen durch die folgenden Zeilen:

```
commmethod sharedmem
shmport Anschlussnummer
```

Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.

Linux: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren

Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.

Informationen zu diesem Vorgang

Die Tabellen- und Indexreorganisation erfordert in hohem Umfang Prozessorressourcen, Speicherbereich für die aktive Protokolldatei und Speicherbereich für das Archivprotokoll. Da die Datenbanksicherung Vorrang vor der Reorganisation hat, wählen Sie den Zeitpunkt und die Dauer für die Reorganisation aus, um sicherzustellen, dass sich die Prozesse nicht überlappen und die Reorganisation ausgeführt werden kann.

Linux-BetriebssystemeSie können die Index- und Tabellenreorganisation für die Serverdatenbank optimieren. Auf diese Weise können Sie die Vermeidung von unerwartetem Datenbankwachstum und Leistungsproblemen verbessern. Anweisungen finden Sie in Technote 1683633.

Wenn Sie diese Serveroptionen aktualisieren, während der Server aktiv ist, müssen Sie den Server stoppen und erneut starten, damit die aktualisierten Werte wirksam werden.

Vorgehensweise

1. Ändern Sie die Serveroptionen.
   Linux-BetriebssystemeBearbeiten Sie die Serveroptionsdatei dsmserv.opt im Serverinstanzverzeichnis. Beachten Sie bei der Bearbeitung der Serveroptionsdatei die folgenden Richtlinien:
   - Entfernen Sie den Stern am Zeilenanfang, um eine Option zu aktivieren.
   - Geben Sie eine Option in einer beliebigen Zeile ein.
   - Geben Sie nur eine Option pro Zeile ein. Die vollständige Option mit ihrem Wert muss sich in einer Zeile befinden.
   - Haben Sie mehrere Einträge für eine Option in der Datei, verwendet der Server den letzten Eintrag.

   Die verfügbaren Serveroptionen können Sie mit der Musterdatei dsmserv.opt.smp im Verzeichnis /opt/tivoli/tsm/server/bin anzeigen.
2. Ist die Verwendung der Datendeduplizierung geplant, aktivieren Sie die Serveroption ALLOWREORGINDEX. Fügen Sie der Serveroptionsdatei die folgende Option und den folgenden Wert hinzu:

   ```
   allowreorgindex yes
   ```

3. Definieren Sie die Serveroptionen REORGBEGINTIME und REORGDURATION, mit denen gesteuert wird, wann die Reorganisation gestartet und wie lange sie ausgeführt wird. Wählen Sie den Zeitpunkt und die Dauer so aus, dass die Reorganisation ausgeführt wird, wenn der Server voraussichtlich am wenigsten ausgelastet ist. Diese Serveroptionen steuern sowohl die Tabellen- als auch die Indexreorganisationsprozesse.
   a. Definieren Sie die Startzeit der Reorganisation mit der Serveroption REORGBEGINTIME. Geben Sie die Zeit im 24-Stunden-Format an. Um beispielsweise als Startzeit der Reorganisation 20:30 Uhr festzulegen, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

      ```
      reorgbegintime 20:30
      ```

   b. Definieren Sie das Intervall, in dem der Server die Reorganisation starten kann. Um beispielsweise anzugeben, dass der Server die Reorganisation innerhalb von 4 Stunden nach dem mit der Serveroption REORGBEGINTIME definierten Zeitpunkt starten kann, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

      ```
      reorgduration 4
      ```

4. War der Server aktiv, während Sie die Serveroptionsdatei aktualisiert haben, stoppen Sie den Server und starten Sie ihn erneut.

Zugehörige Informationen:
ALLOWREORGINDEX
ALLOWREORGTABLE
REORGBEGINTIME
REORGDURATION
Linux-Betriebssysteme

Linux: Serverinstanz starten

Sie können den Server mit der Instanzbenutzer-ID (bevorzugte Methode) oder mit der Rootbenutzer-ID starten.

Vorbereitende Schritte

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden.

Linux-BetriebssystemeAnweisungen finden Sie in Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

Informationen zu diesem Vorgang

Wenn Sie den Server unter Verwendung der Instanzbenutzer-ID starten, wird der Konfigurationsprozess vereinfacht und potenzielle Probleme werden vermieden. In einigen Fällen kann jedoch die Verwendung der Rootbenutzer-ID zum Starten des Servers erforderlich sein. Beispielsweise kann die Rootbenutzer-ID verwendet werden, um sicherzustellen, dass der Server auf bestimmte Einheiten zugreifen kann. Sie können den automatischen Serverstart mit der Instanzbenutzer-ID oder mit der Rootbenutzer-ID konfigurieren.

Linux-BetriebssystemeWenn Sie Verwaltungs- oder Rekonfigurationstasks ausführen müssen, starten Sie den Server im Verwaltungsmodus.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um den Server zu starten:

- Starten Sie den Server mithilfe der Instanzbenutzer-ID.

  Linux-BetriebssystemeAnweisungen finden Sie in Server mit der Instanzbenutzer-ID starten.

- Starten Sie den Server mithilfe der Rootbenutzer-ID.

  Anweisungen zum Berechtigen von Rootbenutzer-IDs zum Starten des Servers finden Sie in Rootbenutzer-IDs zum Starten des Servers berechtigen (Version 7.1.1). Anweisungen zum Starten des Servers mit der Rootbenutzer-ID finden Sie in Server mit der Rootbenutzer-ID starten (Version 7.1.1).

- Linux-BetriebssystemeStarten Sie den Server automatisch.

  Linux-BetriebssystemeAnweisungen siehe Linux: Server auf Linux-Systemen automatisch starten.

- Linux-BetriebssystemeStarten Sie den Server im Verwaltungsmodus.

  Anweisungen siehe Linux: Server im Verwaltungsmodus starten.

Linux-Betriebssysteme

Linux: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen

Vor dem Start des Servers überprüfen Sie Zugriffsberechtigungen und Benutzergrenzwerte.

Informationen zu diesem Vorgang

Wenn Sie die Benutzergrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, nicht überprüfen, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann. Die müssen auch den systemweiten Grenzwert für die maximale Anzahl offener Dateien überprüfen. Der systemweite Grenzwert muss größer-gleich dem Benutzergrenzwert sein.

Vorgehensweise

1. Überprüfen Sie, ob die Benutzer-ID der Serverinstanz über Berechtigungen zum Starten des Servers verfügt.
2. Stellen Sie für die Serverinstanz, die Sie starten wollen, sicher, dass Sie über die Berechtigung zum Lesen und Schreiben von Dateien im Serverinstanzverzeichnis verfügen. Stellen Sie sicher, dass die Datei dsmserv.opt im Serverinstanzverzeichnis vorhanden ist und dass die Datei Parameter für die Serverinstanz enthält.
3. Wenn der Server mit einem Bandlaufwerk, einem Datenträgerwechsler oder mit einer Einheit für austauschbare Datenträger verbunden ist und Sie den Server mit der Instanzbenutzer-ID starten wollen, erteilen Sie der Instanzbenutzer-ID Schreib-/Lesezugriff für diese Einheiten. Führen Sie einen der folgenden Schritte aus, um Berechtigungen festzulegen:
   - Bei einem für IBM Spectrum Protect dediziertem System, auf das nur der IBM Spectrum Protect-Administrator zugreifen kann, erteilen Sie globale Schreibberechtigung für die Gerätedateien der Einheiten. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

     ```
     chmod +w /dev/rmtX
     ```

   - Verfügt das System über mehrere Benutzer, können Sie den Zugriff einschränken, indem Sie die IBM Spectrum Protect-Instanzbenutzer-ID zum Eigner der Gerätedateien der Einheit machen. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

     ```
     chmod u+w /dev/rmtX
     ```

- Sind mehrere Benutzerinstanzen auf einem System aktiv, ändern Sie den Gruppennamen (z. B. TAPEUSERS) und fügen Sie jede IBM Spectrum Protect-Instanzbenutzer-ID dieser Gruppe hinzu. Übertragen Sie dann das Eigentumsrecht der Gerätedateien der Einheiten an die Gruppe TAPEUSERS und erteilen Sie Schreibberechtigung für die Gruppe. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

  ```
  chmod g+w /dev/rmtX
  ```

4. Linux-Betriebssysteme Wenn Sie den IBM Spectrum Protect-Einheitentreiber und das Dienstprogramm autoconf verwenden, erteilen Sie der Instanzbenutzer-ID mithilfe der Option -a Schreib-/Lesezugriff.
5. Linux-BetriebssystemeUm Serverfehler während der Interaktion mit DB2 zu verhindern, optimieren Sie die Kernelparameter.

   Linux-BetriebssystemeAnweisungen zur Optimierung von Kernelparametern finden Sie in Linux: Kernelparameter für Linux-Systeme optimieren.

6. Überprüfen Sie die folgenden Benutzergrenzwerte anhand der Richtlinien in der Tabelle.

   Tabelle 1. Benutzergrenzwerte (ulimit-Werte)

Typ des Benutzergrenzwerts	Bevorzugter Wert	Befehl zum Abfragen des Werts
Maximale Größe erstellter Kerndateien	Unlimited	`ulimit -Hc`
Maximale Größe eines Datensegments für einen Prozess	Unlimited	`ulimit -Hd`
Maximale Dateigröße	Unlimited	`ulimit -Hf`
Maximale Anzahl offener Dateien	65536	`ulimit -Hn`
Maximale Prozessorzeit in Sekunden	Unlimited	`ulimit -Ht`

   Für die Änderung von Benutzergrenzwerten befolgen Sie die Anweisungen in der Dokumentation Ihres Betriebssystems.

   Tipp: Wenn Sie den Server mithilfe eines Scripts automatisch starten wollen, können Sie die Benutzergrenzwerte in dem Script definieren.
7. Stellen Sie sicher, dass als Benutzergrenzwert für die maximale Anzahl Benutzerprozesse (`nproc`-Einstellung) der empfohlene Mindestwert 16384 festgelegt wird.
   a. Geben Sie den Befehl `ulimit -Hu` mithilfe der Instanzbenutzer-ID aus, um den aktuellen Benutzergrenzwert zu überprüfen. Zum Beispiel:

      ```
      [user@Machine ~]$ ulimit -Hu
      16384
      ```

   b. Lautet der Grenzwert für die maximale Anzahl Benutzerprozesse nicht 16384, geben Sie den Wert 16384 an.
      Linux-BetriebssystemeFügen Sie der Datei /etc/security/limits.conf die folgende Zeile hinzu:

      ```
      Instanzbenutzer-ID        -    nproc          16384
      ```

      Hierbei gibt *Instanzbenutzer-ID* die Benutzer-ID der Serverinstanz an.
      Linux-BetriebssystemeWenn der Server im Betriebssystem Red Hat Enterprise Linux 6 installiert ist, legen Sie den Benutzergrenzwert durch Bearbeitung der Datei /etc/security/limits.d/90-nproc.conf im Verzeichnis /etc/security/limits.d fest. Diese Datei überschreibt die Einstellungen in der Datei /etc/security/limits.conf.
      Tipp: Der Standardbenutzergrenzwert für die maximale Anzahl der Benutzerprozesse hat sich bei einigen Versionen des Betriebssystems Linux geändert. Der Standardwert ist 1024. Wenn Sie diesen Wert nicht durch den empfohlenen Mindestwert 16384 ersetzen, kann es zu einem Fehler oder einer Blockierung des Servers kommen.

Linux-Betriebssysteme

Linux: Server mit der Instanzbenutzer-ID starten

Um den Server mit der Instanzbenutzer-ID zu starten, melden Sie sich mit der Instanzbenutzer-ID an und geben Sie im Serverinstanzverzeichnis den entsprechenden Befehl ein.

Vorbereitende Schritte

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden. Anweisungen siehe Linux: Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

Vorgehensweise

1. Melden Sie sich bei dem System, auf dem IBM Spectrum Protect installiert ist, unter Verwendung der Instanzbenutzer-ID für den Server an.
2. Wenn Sie über kein Benutzerprofil zur Ausführung des Scripts `db2profile` verfügen, geben Sie den folgenden Befehl ein:

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

   Tipp: Anweisungen zur Aktualisierung des Benutzer-ID-Anmeldescripts zur automatischen Ausführung des Scripts `db2profile` finden Sie in der DB2-Dokumentation.

3. Geben Sie den folgenden Befehl in einer Zeile im Verzeichnis der Serverinstanz aus, um den Server zu starten:

   Linux-Betriebssysteme

   ```
   usr/bin/dsmserv
   ```

   Tipp: Der Befehl wird im Vordergrund ausgeführt, sodass Sie eine Administrator-ID definieren und der Serverinstanz zuordnen können.
   LinuxBetriebssystemeHat beispielsweise die Serverinstanz den Namen `tsminst1` und das Serverinstanzverzeichnis den Namen /tsminst1, können Sie die Instanz starten, indem Sie die folgenden Befehle ausgeben:

   ```
   cd /tsminst1
    . ~/sqllib/db2profile
   /usr/bin/dsmserv
   ```

Linux-Betriebssysteme

Linux: Server auf Linux-Systemen automatisch starten

Um einen Server unter einem Linux-Betriebssystem automatisch zu starten, verwenden Sie das Script dsmserv.rc.

Vorbereitende Schritte

Stellen Sie sicher, dass Kernelparameter korrekt definiert werden. Anweisungen finden Sie in Kernelparameter für Linux-Systeme optimieren.

Stellen Sie sicher, dass die Serverinstanz mit der Benutzer-ID des Instanzeigners ausgeführt wird.

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden. Anweisungen finden Sie in Zugriffsberechtigungen und Benutzergrenzwerte überprüfen.

Informationen zu diesem Vorgang

Das Script dsmserv.rc befindet sich im Serverinstallationsverzeichnis, z. B. /opt/tivoli/tsm/server/bin.

Das Script dsmserv.rc kann entweder zum manuellen Starten des Servers oder zum automatischen Starten des Servers verwendet werden, indem dem Verzeichnis /etc/rc.d/init.d Einträge hinzugefügt werden. Das Script wird zusammen mit Linux-Dienstprogrammen wie CHKCONFIG und SERVICE eingesetzt.

Vorgehensweise

Führen Sie für jede Serverinstanz, die automatisch gestartet werden soll, die folgenden Schritte aus:

1. Stellen Sie eine Kopie des Scripts dsmserv.rc in das Verzeichnis /init.d, beispielsweise /etc/rc.d/init.d.

   Achten Sie darauf, dass Änderungen nur in der Kopie des Scripts vorgenommen werden. Ändern Sie nicht das Originalscript.

2. Benennen Sie die Kopie des Scripts so um, dass sie dem Namen des Serverinstanzeigners entspricht, beispielsweise `tsminst1`.

   Das Script wurde unter der Voraussetzung erstellt, dass das Serverinstanzverzeichnis *Ausgangsverzeichnis*/tsminst1 ist, beispielsweise /home/tsminst1/tsminst1.

3. Wenn das Serverinstanzverzeichnis nicht *Ausgangsverzeichnis*/tsminst1 ist, suchen Sie in der Kopie des Scripts nach der folgenden Zeile:

   ```
   instance_dir="${Instanzausgangsverzeichnis}/tsminst1"
   ```

   Ändern Sie die Zeile so, dass sie auf Ihr Serverinstanzverzeichnis verweist. Zum Beispiel:

   ```
   instance_dir="/tsminst1"
   ```

4. Suchen Sie in der Kopie des Scripts nach der folgenden Zeile:

   ```
   # pidfile: /var/run/dsmserv_Instanzname.pid
   ```

   Ändern Sie den Wert für den Instanznamen in den Namen des Serverinstanzeigners. Hat beispielsweise der Serverinstanzeigner den Namen tsminst1, aktualisieren Sie die Zeile wie folgt:

   ```
   # pidfile: /var/run/dsmserv_tsminst1.pid
   ```

5. Konfigurieren Sie die Ausführungsebene, auf der der Server automatisch gestartet wird. Geben Sie mithilfe von Tools wie z. B. dem Dienstprogramm CHKCONFIG einen Wert an, der einem Mehrbenutzermodus mit aktiviertem Netzbetrieb entspricht. Normalerweise ist der zu verwendende Wert für die Ausführungsebene abhängig vom Betriebssystem und seiner Konfiguration 3 oder 5. Weitere Informationen zum Mehrbenutzermodus und zu Ausführungsebenen enthält die Dokumentation zu Ihrem Betriebssystem.
6. Um den Server zu starten oder zu stoppen, geben Sie einen der folgenden Befehle aus:
   - Zum Starten des Servers:

     ```
     service tsminst1 start
     ```

- Zum Stoppen des Servers:

  ```
  service tsminst1 stop
  ```

Beispiel

In diesem Beispiel werden die folgenden Werte verwendet:

- Der Instanzeigner ist tsminst1.
- Das Serverinstanzverzeichnis lautet /home/tsminst1/tsminst1.
- Die Kopie des Scripts dsmserv.rc hat den Namen `tsminst1`.
- Das Dienstprogramm CHKCONFIG wird verwendet, um das Starten des Scripts auf den Ausführungsebenen 3, 4 und 5 zu konfigurieren.

```
cp /opt/tivoli/tsm/server/bin/dsmserv.rc /etc/rc.d/init.d/tsminst1
sed -i 's/dsmserv_Instanzname.pid/dsmserv_tsminst1.pid/' /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in
any runlevel (run 'chkconfig --add tsminst1')
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 345 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

Zugehörige Verweise:
Serverstartscript: dsmserv.rc
Linux-Betriebssysteme

Linux: Server im Verwaltungsmodus starten

Sie können den Server im Verwaltungsmodus starten, um Unterbrechungen während Verwaltungs- oder Rekonfigurationstasks zu vermeiden.

Informationen zu diesem Vorgang

Führen Sie das Dienstprogramm DSMSERV mit dem Parameter MAINTENANCE aus, um den Server im Verwaltungsmodus zu starten.

Die folgenden Operationen sind im Verwaltungsmodus inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Wiederherstellung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Außerdem wird verhindert, dass Clients Sitzungen mit dem Server starten.
Tipps:

- Sie müssen die Serveroptionsdatei dsmserv.opt nicht bearbeiten, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Prozesse für die Speicherbereichswiederherstellung, den Bestandsverfall und die Speicherpoolumlagerung manuell starten.

Vorgehensweise

Geben Sie den folgenden Befehl aus, um den Server im Verwaltungsmodus zu starten:

```
dsmserv maintenance
```

Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann unter Server im Verwaltungsmodus starten angezeigt werden.

Nächste Schritte

Gehen Sie wie folgt vor, um den Serverbetrieb im Produktionsmodus fortzusetzen:

1. Geben Sie den Befehl HALT aus, um den Server herunterzufahren:

   ```
   halt
   ```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden.

Die während des Verwaltungsmodus inaktivierten Operationen werden wieder aktiviert.

Linux: Server stoppen

Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.

Informationen zu diesem Vorgang

Geben Sie den folgenden Befehl in die IBM Spectrum Protect-Befehlszeile ein, um den Server zu stoppen:

```
halt
```

 Wenn Sie keine Verbindung zum Server mit einem Verwaltungsclient herstellen können und wenn der Server gestoppt werden soll, müssen Sie den Prozess mit dem Befehl kill mit der Prozess-ID (PID) abbrechen. Die PID wird bei der Initialisierung angezeigt.
Wichtig: Bevor der Befehl kill eingegeben wird, müssen Sie sicherstellen, dass die korrekte Prozess-ID für den IBM Spectrum Protect-Server bekannt ist.
Die Prozess-ID des mit dem Befehl kill abzubrechenden Prozesses kann mithilfe der Datei `dsmserv.v6lock` in dem Verzeichnis, in dem der Server ausgeführt wird, ermittelt werden. Geben Sie Folgendes ein, um die Datei anzuzeigen:

```
cat /instance_dir/dsmserv.v6lock
```

 Geben Sie den folgenden Befehl aus, um den Server zu stoppen:

```
kill -23 dsmserv_pid
```

Hierbei steht *dsmserv_pid* für die Prozess-ID.

Linux: Lizenzregistrierung

Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.

Informationen zu diesem Vorgang

Verwenden Sie hierfür den Befehl REGISTER LICENSE. Weitere Informationen siehe REGISTER LICENSE.

Beispiel: Lizenz registrieren

Die IBM Spectrum Protect-Basislizenz registrieren.

```
register license file=tsmbasic.lic
```

Linux: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben

Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.

Vorbereitende Schritte

Stellen Sie sicher, dass eine Bandeinheitenklasse oder eine Einheitenklasse FILE definiert wurde. Ausführliche Informationen finden Sie in DEFINE DEVCLASS oder suchen Sie nach 'Einheitenklasse definieren'.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Ihr System für Datenbanksicherungen zu konfigurieren.

Vorgehensweise

1. Wenn Sie den Server nicht mit dem Konfigurationsassistenten (dsmicfgx) konfiguriert haben, müssen Sie sicherstellen, dass die Schritte zur manuellen Konfiguration des Systems für Datenbanksicherungen ausgeführt werden.
2. Wählen Sie die für Datenbanksicherungen zu verwendende Einheitenklasse aus. Geben Sie den folgenden Befehl über eine IBM Spectrum Protect-Verwaltungsbefehlszeile aus.

   ```
   set dbrecovery Einheitenklassenname
   ```

   Die angegebene Einheitenklasse wird vom Datenbankmanager für Datenbanksicherungen verwendet. Wenn Sie keine Einheitenklasse mit dem Befehl SET DBRECOVERY angeben, schlägt die Sicherung fehl.

Beispiel

Geben Sie beispielsweise den folgenden Befehl aus, um anzugeben, dass die Einheitenklasse DBBACK verwendet werden soll:

```
set dbrecovery dbback
```

Linux: Mehrere Serverinstanzen auf einem System ausführen

Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.

Multiplizieren Sie den Speicherbedarf und andere Systemvoraussetzungen für einen Server mit der geplanten Instanzzahl für das System.

 Linux-BetriebssystemeDie Gruppe der Dateien für eine Instanz des Servers wird getrennt von den Dateien gespeichert, die von einer anderen Serverinstanz auf demselben System verwendet werden. Gehen Sie wie in Linux: Serverinstanz erstellen beschrieben für jede neue Instanz vor, einschließlich der Erstellung des neuen Instanzbenutzers.

Zur Verwaltung des von jedem Server verwendeten Systemspeichers begrenzen Sie mit der Serveroption DBMEMPERCENT den Prozentsatz des Systemspeichers. Haben alle Server denselben Stellenwert, verwenden Sie für jeden Server denselben Wert. Ist ein Server ein Produktionsserver und andere Server sind Testserver, geben Sie für den Produktionsserver einen höheren Wert an als für die Testserver.

Von Version 6.3 auf Version 7.1 ist ein direktes Upgrade möglich. Weitere Informationen finden Sie im Abschnitt über das Upgrade (Upgrade auf Version 8.1 durchführen). Wenn Sie ein Upgrade durchführen und mehrere Server auf dem System haben, müssen Sie den Installationsassistenten nur einmal ausführen. Der Installationsassistent erfasst die Datenbank- und Variablendaten für alle ursprünglichen Serverinstanzen.

Wenn Sie ein Upgrade von IBM Spectrum Protect Version 6.3 auf Version 8.1.2 durchführen und sich mehrere Server auf Ihrem System befinden, werden alle in DB2 Version 9.7 vorhandenen Instanzen gelöscht und in DB2 Version 11.1 erneut erstellt. Der Assistent gibt den Befehl `db2 upgrade DB DB-Name` für jede Datenbank aus. Die Datenbankumgebungsvariablen für jede Instanz auf Ihrem System werden ebenfalls während des Upgradeprozesses neu konfiguriert.

Zugehörige Tasks:
Mehrere Serverinstanzen auf einem einzigen System ausführen (Version 7.1.1)

Linux: Server überwachen

Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

Vorgehensweise

1. Überwachen Sie die aktive Protokolldatei, um sicherzustellen, dass die Größe für die Auslastung der Serverinstanz korrekt ist.

   Wenn die Serverauslastung ihren normalen erwarteten Stand erreicht hat, belegt der von der aktiven Protokolldatei verwendete Speicherbereich 80 bis 90 Prozent des Speicherbereichs, der für das Verzeichnis für aktive Protokolldateien zur Verfügung steht. An diesem Punkt müssen Sie den Speicherbereich möglicherweise vergrößern. Die Vergrößerung des Speicherbereichs ist von der Art der Transaktionen in der Serververarbeitung abhängig. Transaktionsmerkmale wirken sich auf die Belegung des Speicherbereichs der aktiven Protokolldateien aus.

   Die folgenden Transaktionsmerkmale können sich auf die Speicherbereichsbelegung in der aktiven Protokolldatei auswirken:

   - Die Anzahl und Größe der Dateien in Sicherungsoperationen
     - Clients, wie z. B. Dateiserver, die zahlreiche kleine Dateien sichern, können zahlreiche Transaktionen verursachen, die in kurzer Zeit ausgeführt werden. Die Transaktionen können sehr viel Speicherbereich in der aktiven Protokolldatei belegen, jedoch nur für kurze Zeit.
     - Clients, wie z. B. E-Mail-Server oder ein Datenbankserver, die große Datenvolumen in wenigen Transaktionen sichern, können wenige Transaktionen verursachen, deren Auführung viel Zeit in Anspruch nimmt. Die Transaktionen können wenig Speicherbereich in der aktiven Protokolldatei belegen, jedoch für lange Zeit.
   - Netzverbindungstypen
     - Mit schnellen Netzverbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, die schneller ausgeführt werden. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen kürzeren Zeitraum.
     - Mit langsameren Verbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, deren Ausführung länger dauert. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen längeren Zeitraum.

   Wenn der Server Transaktionen mit sehr unterschiedlichen Merkmalen verarbeitet, kann der für die aktive Protokolldatei verwendete Speicherbereich im Lauf der Zeit sehr stark schwanken. Für einen solchen Server müssen Sie unter Umständen dafür sorgen, dass ein niedrigerer Prozentsatz des Speicherbereichs der aktiven Protokolldatei verwendet wird. Der zusätzliche Speicherbereich gestattet eine Vergrößerung der aktiven Protokolldatei für Transaktionen, die viel Zeit in Anspruch nehmen.

2. Überwachen Sie das Archivprotokoll, um sicherzustellen, dass immer Speicherbereich verfügbar ist.
   Hinweis: Wenn das Archivprotokoll und das Übernahmearchivprotokoll voll werden, kann die aktive Protokolldatei voll werden, so dass der Server stoppt. Für das Archivprotokoll muss so viel Speicherbereich zur Verfügung stehen, dass dieser niemals vollständig belegt wird.
   Sie werden wahrscheinlich Folgendes feststellen:
   a. Am Anfang wird das Archivprotokoll schnell größer, wenn normale Clientsicherungsoperationen ausgeführt werden.

b. Datenbanksicherungen werden regelmäßig ausgeführt, entweder mit einem Zeitplan oder manuell.
c. Nach mindestens zwei Datenbankgesamtsicherungen wird das Abschneiden des Protokolls automatisch ausgeführt. Der vom Archivprotokoll belegte Speicherbereich verringert sich durch das Abschneiden.
d. Normale Clientoperationen werden fortgesetzt und das Archivprotokoll wird wieder größer.
e. Datenbanksicherungen finden regelmäßig statt und die Häufigkeit der Protokollbereinigung ist von der Häufigkeit der Datenbankgesamtsicherungen abhängig.

Nach diesem Muster nimmt die Größe des Archivprotokolls zunächst zu, verringert sich und nimmt dann eventuell wieder zu. Im Laufe der Zeit sollte der vom Archivprotokoll belegte Speicherbereich während der normalen Verarbeitung einen relativ konstanten Stand erreichen.

Wenn die Größe des Archivprotokolls weiter zunimmt, sollten Sie eine oder beide der folgenden Maßnahmen in Betracht ziehen:
- Ordnen Sie dem Archivprotokoll weiteren Speicherbereich zu. Sie müssen unter Umständen das Archivprotokoll in ein anderes Dateisystem versetzen.
- Erhöhen Sie die Häufigkeit der Datenbankgesamtsicherungen, so dass die Protokollbereinigung häufiger stattfindet.

3. Wenn Sie ein Verzeichnis für das Übernahmearchivprotokoll definiert haben, überprüfen Sie, ob darin Protokolle während der normalen Verarbeitung gespeichert werden. Wenn der Speicherbereich des Übernahmeprotokolls verwendet wird, sollten Sie das Archivprotokoll vergrößern. Das Übernahmearchivprotokoll sollte nur unter außergewöhnlichen Bedingungen verwendet werden, nicht während der normalen Verarbeitung.

Linux: IBM Spectrum Protect-Server-Fixpack installieren

IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.

Vorbereitende Schritte

Damit ein Fixpack oder ein vorläufiger Fix auf dem Server installiert werden kann, müssen Sie den Server mit der Stufe installieren, auf der er ausgeführt werden soll. Sie müssen die Serverinstallation nicht mit dem Basisrelease beginnen. Wenn momentan beispielsweise Version 8.1.1 installiert ist, können Sie das aktuelle Fixpack für Version 8.1 direkt verwenden. Sie müssen nicht mit der Installation von Version 8.1.0 beginnen, wenn eine Wartungsaktualisierung verfügbar ist.

Das IBM Spectrum Protect-Lizenzpaket muss installiert sein. Das Lizenzpaket wird beim Kauf eines Basisreleases bereitgestellt. Wenn Sie ein Fixpack oder einen vorläufigen Fix von Fix Central herunterladen, installieren Sie die Serverlizenz, die auf der Website von Passport Advantage zur Verfügung steht. Sollen Nachrichten und Hilfetext nicht in Englisch angezeigt werden, installieren Sie das gewünschte Sprachenpaket.

Wenn Sie ein Upgrade des Servers auf Version 8.1.2 oder höher durchführen und den Server dann auf einen Stand vor Version 8.1.2 zurücksetzen, müssen Sie die Datenbank auf einen Zeitpunkt vor dem Upgrade zurückschreiben. Führen Sie während des Upgrades die erforderlichen Schritte aus, mit denen sichergestellt wird, dass die Datenbank zurückgeschrieben werden kann: Sichern Sie die Datenbank, die Protokolldatei für Datenträger, die Einheitenkonfigurationsdatei und die Serveroptionsdatei. Weitere Informationen finden Sie in Linux: Von Version 8.1.2 auf eine vorherige Serverversion zurücksetzen.

Wenn Sie den Clientverwaltungsservice verwenden, müssen Sie ein Upgrade dieses Service auf dieselbe Version wie beim IBM Spectrum Protect-Server durchführen.

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des installierten Servers aufbewahrt werden. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Rufen Sie das IBM® Support Portal auf. Hier finden Sie folgende Informationen:

- Eine Liste der neuesten Wartungs- und Download-Fixes. Klicken Sie auf **Download** und legen Sie alle gültigen Fixes an.
- Informationen zum Erwerb eines Basislizenzpakets. Suchen Sie nach **Downloads > Passport Advantage**.
- Unterstützte Plattformen und Systemvoraussetzungen. Suchen Sie nach **IBM Spectrum Protect supported operating systems**.

Sie müssen ein Upgrade des Servers durchführen, bevor Sie ein Upgrade der Clients für Sichern/Archivieren durchführen. Wenn Sie das Upgrade des Servers nicht zuerst durchführen, könnte die Kommunikation zwischen dem Server und den Clients unterbrochen werden.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Fixpack oder einen vorläufigen Fix zu installieren:

1. Sichern Sie die Datenbank. Die bevorzugte Methode ist eine Momentaufnahmesicherung. Bei einer Momentaufnahmesicherung handelt es sich um eine Datenbankgesamtsicherung, bei der geplante Datenbanksicherungen nicht unterbrochen werden. Geben Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Sichern Sie die Einheitenkonfigurationsdaten. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup devconfig filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.
3. Speichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis oder benennen Sie die Datei um. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup volhistory filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.
4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
5. Halten Sie den Server vor der Installation eines Fixpacks oder eines vorläufigen Fixes an. Verwenden Sie den Befehl HALT.
6. Stellen Sie sicher, dass im Installationsverzeichnis zusätzlicher Speicherplatz zur Verfügung steht. Für die Installation dieses Fixpacks kann zusätzlicher temporärer Plattenspeicherplatz im Installationsverzeichnis des Servers erforderlich sein. Die Größe des zusätzlichen Plattenspeicherplatzes kann der Größe entsprechen, die für die Installation einer neuen Datenbank während einer IBM Spectrum Protect-Installation benötigt wird. Der IBM Spectrum Protect-Installationsassistent zeigt an, wie viel Speicherplatz für die Installation des Fixpacks benötigt wird und wie viel Platz zur Verfügung steht. Wenn der erforderliche Speicherplatz größer ist als der verfügbare Speicherplatz, stoppt die Installation. Wenn die Installation stoppt, fügen Sie dem Dateisystem den erforderlichen Plattenspeicherplatz hinzu und starten Sie die Installation erneut.
7. Linux-BetriebssystemeMelden Sie sich als Root an.
8. Laden Sie die Paketdatei für das Fixpack bzw. den vorläufigen Fix, das bzw. der installiert werden soll, über IBM Support Portal, Passport Advantage oder Fix Central herunter.
9. Linux-BetriebssystemeWechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet, und führen Sie die folgenden Schritte aus.
   Tipp: Die Dateien werden in das aktuelle Verzeichnis extrahiert. Stellen Sie sicher, dass sich die ausführbare Datei in dem Verzeichnis befindet, in dem sich die extrahierten Dateien befinden sollen.
   a. Geben Sie den folgenden Befehl ein, um die Dateiberechtigungen zu ändern:

      ```
      chmod a+x 8.x.x.x-IBM-SPSRV-Plattform.bin
      ```

      Hierbei steht *Plattform* für die Architektur, in der IBM Spectrum Protect installiert werden soll.
   b. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

      ```
      ./8.x.x.x-IBM-SPSRV-Plattform.bin
      ```

10. Wählen Sie eine der folgenden Möglichkeiten für die Installation von IBM Spectrum Protect aus.
    Wichtig: Nach der Installation eines Fixpacks muss die Konfiguration nicht wiederholt werden. Sie können nach Beendigung der Installation stoppen, alle Fehler beheben und dann Ihre Server erneut starten.
    Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden:

    Installationsassistent
    : Befolgen Sie die Anweisungen für Ihr Betriebssystem:
      Linux: IBM Spectrum Protect mit dem Installationsassistenten installieren

    Tipp: Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Aktualisieren. Klicken Sie nicht auf das Symbol Installieren oder Ändern.

    Befehlszeile im Konsolenmodus
    : Befolgen Sie die Anweisungen für Ihr Betriebssystem:
      Linux: IBM Spectrum Protect im Konsolenmodus installieren

    Unbeaufsichtigter Modus
    : Befolgen Sie die Anweisungen für Ihr Betriebssystem:
      Linux: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

    Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, führen Sie den Installationsassistenten nur einmal aus. Der Installationsassistent führt ein Upgrade aller Serverinstanzen durch.

Ergebnisse

Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf Datei > Protokoll anzeigen. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:

- Linux-Betriebssysteme/var/ibm/InstallationManager/logs

Linux: Von Version 8.1.2 auf eine vorherige Serverversion zurücksetzen

Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.

Vorbereitende Schritte

Sie benötigen die folgenden Elemente aus der früheren Version des Servers:

- Serverdatenbanksicherung
- Protokolldatei für Datenträger
- Einheitenkonfigurationsdatei
- Serveroptionsdatei

Informationen zu diesem Vorgang

Die Anweisungen sind für das Zurücksetzen innerhalb eines Releases oder von einem Release auf ein vorheriges Release identisch, z. B. von 8.1.2 auf 8.1.1 oder von 8.1.2 auf 7.1.2. Die ältere Version muss mit der Version übereinstimmen, die Sie vor dem Upgrade auf Version 8.1 verwendet haben.

Achtung: Geben Sie den Parameter REUSEDELAY an, um den Verlust von Daten des Clients für Sichern/Archivieren verhindern zu helfen, wenn Sie den Server auf eine vorherige Version zurücksetzen.

Vorgehensweise beim Zurücksetzen auf vorherige Serverversion

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte auf dem System aus, auf dem sich der Server der Version 8.1 befindet.

Vorgehensweise

1. Stoppen Sie den Server, um alle Serveroperationen zu beenden. Verwenden Sie hierfür den Befehl HALT.
2. Entfernen Sie die Datenbank aus dem Datenbankmanager und löschen Sie anschließend die Datenbank- und Wiederherstellungsprotokollverzeichnisse.
   a. Entfernen Sie die Datenbank manuell. Eine Möglichkeit zum Entfernen ist der folgende Befehl: Linux-Betriebssysteme

      ```
      dsmserv removedb tsmdb1
      ```

   b. Wenn Sie den von den Datenbank- und Wiederherstellungsprotokollverzeichnissen belegten Speicherplatz wiederverwenden müssen, können Sie diese Verzeichnisse jetzt löschen.
3. Deinstallieren Sie den Server der Version 8.1 mit dem Deinstallationsprogramm. Bei der Deinstallation werden der Server und der Datenbankmanager mit den jeweiligen Verzeichnissen entfernt. Ausführliche Informationen siehe Linux: IBM Spectrum Protect deinstallieren.
4. Stoppen Sie den Clusterdienst. Installieren Sie die Version des Serverprogramms, die Sie vor dem Upgrade auf Version 8.1.2 verwendet haben, erneut. Diese Version muss mit der Version übereinstimmen, die auf Ihrem Server verwendet wurde, als Sie die Datenbanksicherung erstellt haben, die Sie zu einem späteren Zeitpunkt wiederherstellen wollen. Wenn der Server vor dem Upgrade z. B. die Version 7.1.7 hatte und wenn Sie die Datenbanksicherung verwenden wollen, die auf diesem Server verwendet wurde, müssen Sie das Fixpack V7.1.7 installieren, damit Sie die Datenbanksicherung zurückschreiben können.
5. Konfigurieren Sie die neue Serverdatenbank mithilfe des Konfigurationsassistenten. Geben Sie den folgenden Befehl aus, um den Assistenten zu starten: Linux-Betriebssysteme

   ```
   . /dsmicfgx
   ```

6. Stellen Sie sicher, dass keine Server im Hintergrund ausgeführt werden.
7. Schreiben Sie die Datenbank zu einem Zeitpunkt vor dem Upgrade zurück.
8. Kopieren Sie die folgenden Dateien in das Instanzverzeichnis.
   - Einheitenkonfigurationsdatei
   - Protokolldatei für Datenträger
   - Serveroptionsdatei (normalerweise dsmserv.opt)
9. Wenn Sie die Datendeduplizierung für Speicherpools des Typs FILE, die vor dem Upgrade vorhanden waren, aktiviert haben oder wenn Sie während der Verwendung des Servers der Version 8.1.2 Daten, die vor dem Upgrade vorhanden waren, in neue Speicherpools verschoben haben, müssen Sie zusätzliche Schritte ausführen. Weitere Informationen finden Sie in Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung.
10. Wenn die Einstellung des Parameters REUSEDELAY für Speicherpools das Alter der zurückgeschriebenen Datenbank unterschreitet, schreiben Sie Datenträger auf allen Speicherpools mit sequenziellem Zugriff, die nach dieser Datenbanksicherung wiederhergestellt wurden, zurück. Verwenden Sie den Befehl RESTORE VOLUME.

Wenn keine Sicherung eines Speicherpools vorliegt, prüfen Sie die wiederhergestellten Datenträger mit dem Befehl AUDIT VOLUME und dem Parameter FIX=YES, um Inkonsistenzen zu beheben. Beispiel:

```
audit volume Datenträgername fix=yes
```

11. Wurden mit dem Server der Version 8.1 Clientsicherungs- oder -archivierungsoperationen ausgeführt, prüfen Sie die Speicherpooldatenträger, auf denen die Daten gespeichert wurden.

Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung

Wenn Sie während der Ausführung des Servers mit Version 8.1.2 neue Speicherpools erstellt und/oder die Datendeduplizierung für Speicherpools des Typs FILE aktiviert haben, müssen Sie zusätzliche Schritte ausführen, um die vorherige Serverversion wiederherzustellen.

Vorbereitende Schritte

Für diese Task benötigen Sie eine Gesamtsicherung des Speicherpools, die vor dem Upgrade auf Version 8.1.2 erstellt wurde.

Informationen zu diesem Vorgang

Verwenden Sie diese Informationen, wenn Sie einen oder beide der folgenden Schritte ausgeführt haben, während Ihr Server mit Version 8.1.2 ausgeführt wurde:

- Sie haben die Datendeduplizierungsfunktion für beliebige Speicherpools aktiviert, die vor dem Upgrade auf Version 8.1.2 bereits vorhanden waren. Die Datendeduplizierung ist nur für Speicherpools gültig, die den Einheitentyp FILE verwenden.
- Sie haben neue primäre Speicherpools nach dem Upgrade erstellt *und* Daten, die in anderen Speicherpools gespeichert waren, in die neuen Speicherpools versetzt.

Führen Sie diese Schritte aus, nachdem der Server wieder auf Version 7 zurückgesetzt wurde.

Vorgehensweise

- Schreiben Sie für jeden Speicherpool, für den Sie die Datendeduplizierungsfunktion aktiviert haben, den gesamten Speicherpool mit dem Befehl RESTORE STGPOOL zurück.
- Bestimmen Sie für Speicherpools, die Sie nach dem Upgrade erstellt haben, welche Maßnahme durchzuführen ist. Daten, die aus vorhandenen Speicherpools der Version 8 in die neuen Speicherpools versetzt wurden, gehen möglicherweise verloren, weil die neuen Speicherpools auf Ihrem auf Version 8 zurückgesetzten Server nicht mehr vorhanden sind. Die Wiederherstellungsmaßnahmen sind vom Typ des Speicherpools abhängig:
  - Wurden Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, wurde der von den versetzten Daten belegte Speicherplatz wahrscheinlich wiederverwendet. Daher müssen Sie die ursprünglichen Speicherpools der Version 8 mithilfe der Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.2 erstellt wurden.

    Wurden *keine* Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, müssen Sie die Speicherpooldatenträger in diesen Speicherpools des Typs DISK prüfen.

  - Wurden Daten aus Speicherpools mit sequenziellem Zugriff der Version 8 in einen neuen Speicherpool versetzt, sind diese Daten möglicherweise noch vorhanden und sie können eventuell auf Speicherpooldatenträgern auf dem wiederhergestellten Server der Version 8 verwendet werden. Die Daten können verwendbar sein, wenn für den Parameter REUSEDELAY des Speicherpools ein Wert definiert wurde, der die Wiederherstellung verhindert hat, während der Server mit der Version 8.1.2 ausgeführt wurde. Wurden Datenträger wiederhergestellt, während der Server mit der Version 8.1.2 ausgeführt wurde, müssen Sie diese Datenträger aus Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.2 erstellt wurden.

Linux: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken

Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.

Zweck

Nach der Installation und Konfiguration von IBM Spectrum Protect mithilfe der Assistenten müssen Sie DB2-Befehle nur selten verwenden. Eine begrenzte Gruppe von DB2-Befehlen, die Sie verwenden bzw. zu deren Verwendung Sie aufgefordert werden könnten, ist in Tabelle 1 aufgelistet. Diese Liste ist nicht umfassend, es handelt sich lediglich um ergänzende Informationen. Es besteht keine Implikation, dass ein IBM Spectrum Protect-Administrator sie täglich oder regelmäßig verwendet. Beispiele einiger Befehle sind angegeben. Ausgabedaten sind nicht enthalten.

Vollständige Erläuterungen zu den hier beschriebenen Befehlen und zu deren Syntax finden Sie in der Produktinformation zu DB2.

Tabelle 1. DB2-Befehle

Befehl	Beschreibung	Beispiel

Befehl	Beschreibung	Beispiel
db2icrt	Erstellt DB2-Instanzen im Ausgangsverzeichnis des Instanzeigners. Tipp: Der IBM Spectrum Protect-Konfigurationsassistent erstellt die vom Server und von der Datenbank verwendete Instanz. Nach der Installation und Konfiguration eines Servers mithilfe des Konfigurationsassistenten wird der Befehl db2icrt in der Regel nicht verwendet.  Linux-BetriebssystemeDieses Dienstprogramm befindet sich im Verzeichnis DB2DIR/instance. Hierbei steht DB2DIR für das Installationsverzeichnis, in dem die aktuelle Version des DB2-Datenbanksystems installiert ist.	IBM Spectrum Protect-Instanz manuell erstellen (geben Sie den Befehl in einer einzigen Zeile ein): `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u` *`Instanzname Instanzname`*
db2set	Zeigt DB2-Variablen an.	DB2-Variablen auflisten: `db2set`
CATALOG DATABASE	Speichert Informationen zur Speicherposition der Datenbank im Systemdatenbankverzeichnis. Die Datenbank kann sich auf der lokalen Workstation oder auf einem fernen Datenbankpartitionsserver befinden. Der Serverkonfigurationsassistent kümmert sich um jeden Katalog, der zur Verwendung der Serverdatenbank benötigt wird. Führen Sie diesen Befehl nach der Konfiguration und Aktivierung eines Servers nur dann manuell aus, wenn es eine Änderung oder Beschädigung in der Umgebung gibt.	Datenbank katalogisieren: `db2 catalog database tsmdb1`
CONNECT TO DATABASE	Stellt eine Verbindung zu einer angegebenen Datenbank für Befehlszeilenschnittstellenzwecke her.	Eine Verbindung zur IBM Spectrum Protect-Datenbank über eine DB2-Befehlszeilenschnittstelle herstellen: `db2 connect to tsmdb1`

GET DATABASE CONFIGURATION	Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.
	Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.
		Die Konfigurationsdaten für einen Datenbankaliasnamen anzeigen:
		`db2 get db cfg for tsmdb1`
		Informationen abrufen, um Einstellungen zu überprüfen (z. B. Datenbankkonfiguration, Protokollmodus und Pflege).
		`db2 get db config for tsmdb1 show detail`

Befehl	Beschreibung	Beispiel
GET DATABASE MANAGER CONFIGURATION	Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück. Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.	Konfigurationsdaten für den Datenbankmanager abrufen: `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Ruft die Informationen zum Allgemeinzustand für den Datenbankmanager und seine Datenbanken ab. Die zurückgegebenen Informationen stellen eine Momentaufnahme des Status zum Zeitpunkt der Befehlsausgabe dar. IBM Spectrum Protect überwacht den Status der Datenbank mithilfe der Diagnosemomentaufnahme und anderer Mechanismen, die von DB2 bereitgestellt werden. Es kann vorkommen, dass die Diagnosemomentaufnahme oder andere DB2-Dokumentation anzeigt, dass sich ein Element bzw. eine Datenbankressource im Alertstatus befindet. In einem solchen Fall müssen entsprechende Schritte zur Behebung der Situation in Betracht gezogen werden. IBM Spectrum Protect überwacht die Bedingung und reagiert entsprechend. Nicht alle deklarierten Alerts der DB2-Datenbank haben Maßnahmen zur Folge.	Einen Bericht über Anzeiger des DB2-Diagnosemonitors abrufen: `db2 get health snapshot for database on tsmdb1`

GRANT (Datenbank-berechtigungen)	Erteilt Berechtigungen, die sich auf die gesamte Datenbank beziehen, und keine Zugriffsrechte, die sich auf bestimmte Objekte in der Datenbank beziehen.	Der Benutzer-ID itmuser Zugriffsberechtigung erteilen:
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

RUNSTATS	Aktualisiert statistische Daten zu den Merkmalen einer Tabelle und der zugeordneten Indizes oder Statistiksichten. Zu diesen Merkmalen gehören die Anzahl der Datensätze, die Anzahl der Seiten und die durchschnittliche Datensatzlänge. Soll eine Tabelle angezeigt werden, verwenden Sie dieses Dienstprogramm nach dem Aktualisieren oder Reorganisieren der Tabelle. Eine Sicht muss für die Optimierung aktiviert sein, damit ihre statistischen Daten für die Optimierung einer Abfrage verwendet werden können. Eine für die Optimierung aktivierte Sicht wird als Statistiksicht bezeichnet. Sie können eine Sicht mit der DB2-Anweisung ALTER VIEW für die Optimierung aktivieren. Verwenden Sie das Dienstprogramm RUNSTATS, wenn sich Änderungen zugrunde liegender Tabellen auf die von der Sicht zurückgegebenen Zeilen auswirken. Tipp: Der Server konfiguriert DB2 so, dass der Befehl RUNSTATS nach Bedarf ausgeführt wird.	Statistische Daten für eine einzelne Tabelle aktualisieren. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
SET SCHEMA	Ändert den Wert des Sonderregisters CURRENT SCHEMA als Vorbereitung für die direkte Ausgabe von SQL-Befehlen über die DB2-Befehlszeilenschnittstelle. Tipp: Ein Sonderregister ist ein Speicherbereich, den der Datenbankmanager für einen Anwendungsprozess definiert. In diesem Bereich werden Informationen gespeichert, auf die in SQL-Anweisungen verwiesen werden kann.	Das Schema für IBM Spectrum Protect festlegen: `db2 set schema tsmdb1`

Befehl	Beschreibung	Beispiel
START DATABASE MANAGER	Startet die Hintergrundprozesse der aktuellen Datenbankmanagerinstanz. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers. Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.	Den Datenbankmanager starten: `db2start`
STOP DATABASE MANAGER	Stoppt die aktuelle Datenbankmanagerinstanz. Der Datenbankmanager bleibt so lange aktiv, bis er explizit gestoppt wird. Dieser Befehl stoppt die Datenbankmanagerinstanz nicht, wenn Anwendungen mit Datenbanken verbunden sind. Liegen keine Datenbankverbindungen, aber Instanzverbindungen vor, erzwingt der Befehl zunächst das Stoppen der Instanzverbindungen. Dann wird der Datenbankmanager gestoppt. Dieser Befehl inaktiviert außerdem alle ausstehenden Datenbankaktivierungen, bevor der Datenbankmanager gestoppt wird. Dieser Befehl ist auf einem Client nicht gültig. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers. Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.	Den Datenbankmanager stoppen: `db2 stop dbm`

Linux: IBM Spectrum Protect deinstallieren

Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

Vorbereitende Schritte

Führen Sie folgende Schritte aus, bevor Sie IBM Spectrum Protect deinstallieren:

- Führen Sie eine Gesamtsicherung der Datenbank aus.
- Speichern Sie eine Kopie der Datenträgerhistory- und Einheitenkonfigurationsdateien.
- Bewahren Sie die Ausgabedatenträger an einem sicheren Ort auf.

Informationen zu diesem Vorgang

Sie können IBM Spectrum Protect mit jeder der folgenden Methoden deinstallieren: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

- Linux: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren
  Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.
- Linux: IBM Spectrum Protect im Konsolenmodus deinstallieren
  Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.
- Linux: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren
  Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.
- Linux: IBM Spectrum Protect deinstallieren und erneut installieren
  Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.
- Linux: IBM Installation Manager deinstallieren
  Sie können IBM Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

Nächste Schritte

Die Vorgehensweise für die Reinstallation der IBM Spectrum Protect-Komponenten finden Sie in Linux: Serverkomponenten installieren.

Linux: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren

Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.

Vorgehensweise

1. Starten Sie Installation Manager.
   Linux-BetriebssystemeIn dem Verzeichnis, in dem Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus:

   ```
   ./IBMIM
   ```

2. Klicken Sie auf Deinstallieren.
3. Wählen Sie IBM Spectrum Protect-Server aus und klicken Sie auf Weiter.
4. Klicken Sie auf Deinstallieren.
5. Klicken Sie auf Fertigstellen.

Linux: IBM Spectrum Protect im Konsolenmodus deinstallieren

Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.

Vorgehensweise

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
   - Linux-Betriebssystemeeclipse/tools

   Beispiel:

   - Linux-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus:
   - Linux-Betriebssysteme`./imcl -c`
3. Für die Deinstallation geben Sie `5` ein.
4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
5. Geben Sie `N` für 'Next' (Weiter) ein.
6. Wählen Sie die Deinstallation des IBM Spectrum Protect-Serverpakets aus.
7. Geben Sie `N` für 'Next' (Weiter) ein.
8. Geben Sie `U` für 'Uninstall' (Deinstallieren) ein.
9. Geben Sie `F` für 'Finish' (Fertigstellen) ein.

Linux: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren

Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

Vorbereitende Schritte

Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation der IBM Spectrum Protect-Serverkomponenten mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, uninstall_response_sample.xml, im Verzeichnis input, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie alle IBM Spectrum Protect-Komponenten deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für jede Komponente in der Antwortdatei unverändert. Wenn Sie eine Komponente nicht deinstallieren wollen, geben Sie den Wert `modify="true"` an.

Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
   - Linux-Betriebssystemeeclipse/tools

   Beispiel:

   - Linux-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:
   Linux-Betriebssysteme

   ```
   ./imcl -input Antwortdatei -silent
   ```

   Der folgende Befehl ist ein Beispiel:

   Linux-Betriebssysteme

```
./imcl -input /tmp/input/uninstall_response.xml -silent
```

Linux: IBM Spectrum Protect deinstallieren und erneut installieren

Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um IBM Spectrum Protect manuell zu deinstallieren und erneut zu installieren:

1. Linux-BetriebssystemeErstellen Sie eine Liste Ihrer aktuellen Serverinstanzen, bevor Sie mit der Deinstallation beginnen. Führen Sie den folgenden Befehl aus:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

2. Führen Sie die folgenden Befehle für jede Serverinstanz aus:
   Linux-Betriebssysteme

   ```
   db2 attach to Instanzname
   db2 get dbm cfg show detail
   db2 detach
   ```

   Notieren Sie den Datenbankpfad für jede Instanz.
3. Deinstallieren Sie IBM Spectrum Protect. Siehe Linux: IBM Spectrum Protect deinstallieren.
4. Wenn Sie eine beliebige unterstützte Version von IBM Spectrum Protect deinstallieren (einschließlich Fixpack), wird eine Instanzdatei erstellt. Die Instanzdatei wird erstellt, um die Reinstallation von IBM Spectrum Protect zu erleichtern. Überprüfen Sie diese Datei und verwenden Sie die Informationen, wenn Sie bei der Reinstallation zur Eingabe der Berechtigungsnachweise der Instanz aufgefordert werden. Bei der unbeaufsichtigten Installation geben Sie diese Berechtigungsnachweise mit der Variablen `INSTANCE_CRED` an.
   Sie finden die Instanzdatei an der folgenden Position:
   - Linux-Betriebssysteme/etc/tivoli/tsm/instanceList.obj
5. Installieren Sie IBM Spectrum Protect erneut. Siehe Linux: Serverkomponenten installieren.

   Ist die Datei `instanceList.obj` nicht vorhanden, müssen Sie Ihre Serverinstanzen wie folgt erneut erstellen:

   a. Erstellen Sie Ihre Serverinstanzen erneut. Siehe Linux: Serverinstanz erstellen.
      Tipp: Der Installationsassistent konfiguriert die Serverinstanzen, Sie müssen jedoch überprüfen, ob sie vorhanden sind. Wenn sie nicht vorhanden sind, müssen Sie sie manuell konfigurieren.
   b. Katalogisieren Sie die Datenbank. Melden Sie sich bei jeder Serverinstanz nacheinander als Instanzbenutzer an und geben Sie folgende Befehle aus:
      Linux-Betriebssysteme

      ```
      db2 catalog database tsmdb1
      db2 attach to Instanzname
      db2 update dbm cfg using dftdbpath Instanzverzeichnis
      db2 detach
      ```

   c. Linux-BetriebssystemeÜberprüfen Sie, ob die Serverinstanz erfolgreich erstellt wurde. Geben Sie den folgenden Befehl aus:

      ```
      /opt/tivoli/tsm/db2/instance/db2ilist
      ```

   d. Überprüfen Sie, ob IBM Spectrum Protect die Serverinstanz erkennt, indem Sie Ihre Verzeichnisse auflisten. Ihr Ausgangsverzeichnis wird angezeigt, wenn Sie es nicht geändert haben. Ihr Instanzverzeichnis wird angezeigt, wenn Sie den Konfigurationsassistenten verwendet haben. Geben Sie den folgenden Befehl aus:

      ```
      db2 list database directory
      ```

      Wenn Sie TSMDB1 in der Liste finden, können Sie den Server starten.

Linux: IBM Installation Manager deinstallieren

Sie können IBM® Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

Vorbereitende Schritte

Bevor Sie IBM Installation Manager deinstallieren, müssen Sie sicherstellen, dass alle mit IBM Installation Manager installierten Pakete deinstalliert sind. Schließen Sie IBM Installation Manager, bevor Sie den Deinstallationsprozess starten.

Linux-BetriebssystemeGeben Sie den folgenden Befehl in eine Befehlszeile ein, um installierte Pakete anzuzeigen:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

Vorgehensweise

Gehen Sie wie folgt vor, um IBM Installation Manager zu deinstallieren:

 Linux-Betriebssysteme

1. Öffnen Sie eine Befehlszeile und wechseln Sie in das Verzeichnis /var/ibm/InstallationManager/uninstall.
2. Geben Sie den folgenden Befehl aus:

   ```
   ./uninstall
   ```

   Einschränkung: Sie müssen mit der Benutzer-ID `root` am System angemeldet sein.

Windows: Server installieren

Zur Installation des Servers gehören Planung, Installation und Erstkonfiguration.

- Windows
- Windows: Installation des Servers planen
  Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.
- Windows: Serverkomponenten installieren
  Für die Installation der Serverkomponenten der Version 8.1.2 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.
- Windows: Die ersten Schritte nach der Installation von IBM Spectrum Protect
  Nach der Installation von Version 8.1.2 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.
- Windows: IBM Spectrum Protect-Server-Fixpack installieren
  IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.
- Windows: Von Version 8.1.2 auf eine vorherige Serverversion zurücksetzen
  Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.
- Windows: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken
  Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.
- Windows: IBM Spectrum Protect deinstallieren
  Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

Windows: Installation des Servers planen

Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.

- Windows: Vorausgesetzte Kenntnisse
  Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.
- Windows: Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten
  Lesen Sie vor der Installation von IBM Spectrum Protect Version 8.1.2 oder höher die Informationen über die erweiterten Sicherheitsfunktionen und die Voraussetzungen für eine Aktualisierung Ihrer Umgebung.
- Windows: Planung für optimale Leistung
  Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.
-  Windows-BetriebssystemeWindows: Systemmindestvoraussetzungen für Windows-Systeme
  Für den Server können sehr viel Speicherplatz, eine große Netzbandbreite und viele Prozessorressourcen erforderlich sein. In vielen Fällen ist die Leistung des Servers am besten, wenn andere Anwendungen nicht auf demselben System installiert sind.
- Windows: IBM Installation Manager
  IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.
- Windows: Arbeitsblätter für Planungsdetails für den Server
  Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.
- Windows: Kapazitätsplanung
  Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das

Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.

- Windows: Empfehlungen für die Serverbenennung
  Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.
- Windows: Installationsverzeichnisse
  Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

Windows: Vorausgesetzte Kenntnisse

Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.

Wartungsreleases, Client-Software und Veröffentlichungen für den Server stehen im IBM® Support Portal zur Verfügung.

 Windows-BetriebssystemeEinschränkung: Sie können den Server der Version 8.1.2 nicht auf einem System installieren und ausführen, auf dem bereits DB2 installiert ist. Das gilt unabhängig davon, ob DB2 separat oder als Teil einer anderen Anwendung installiert wurde. Für den Server der Version 8.1.2 muss die DB2-Version installiert und verwendet werden, die im Paket des Servers der Version 8.1.2 enthalten ist. Es darf keine andere DB2-Version auf dem System vorhanden sein.

 Windows-BetriebssystemeSie können den IBM Spectrum Protect-Server auf einem Domänencontroller installieren. Auf dem Server kann jedoch eine hohe Prozessorauslastung auftreten, wodurch andere Anwendungen betroffen sein und blockiert werden können.

Erfahrene DB2-Administratoren können erweiterte SQL-Abfragen durchführen und mithilfe von DB2-Tools die Datenbank überwachen. Sie dürfen die DB2-Tools jedoch nicht zur Änderung der von IBM Spectrum Protect vorgegebenen DB2-Konfigurationseinstellungen verwenden oder die DB2-Umgebung für IBM Spectrum Protect auf andere Weise ändern (z. B. mit anderen Produkten). Der Server der Version 8.1.2 wurde mit der Datendefinitionssprache (DDL) und der vom Server implementierten Datenbankkonfiguration erstellt und ausführlich getestet.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

Windows: Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten

Lesen Sie vor der Installation von IBM Spectrum Protect Version 8.1.2 oder höher die Informationen über die erweiterten Sicherheitsfunktionen und die Voraussetzungen für eine Aktualisierung Ihrer Umgebung.

Informationen zu diesem Vorgang

Die in Version 8.1.2 und höheren Versionen eingeführten Sicherheitserweiterungen setzen strengere Sicherheitseinstellungen durch. Führen Sie die Prozedur aus, um sicherzustellen, dass die Kommunikation zwischen Servern und Clients bei einer Installation oder einem Upgrade der IBM Spectrum Protect-Software auf Version 8.1.2 nicht unterbrochen wird.

Vorgehensweise

1. Führen Sie die Installation bzw. das Upgrade der IBM Spectrum Protect-Server mit Version 8.1.2 oder höher durch.
2. Führen Sie die Installation bzw. das Upgrade der Clients für Sichern/Archivieren durch. Weitere Informationen finden Sie in Clients installieren und konfigurieren.
   Informationen zur Planung der Implementierung von Clientaktualisierungen auf dem Server finden Sie in den folgenden Dokumenten:
   - Für Server mit IBM Spectrum Protect Version 8.1.2 oder einer höheren Version: Technote 2004596.
   - Für Server mit IBM® Tivoli Storage Manager Version 7.1 und IBM Spectrum Protect Version 8.1.0 und 8.1.1: Technote 1673299.
3. Konfigurieren Sie die Optionen für Clients für Sichern/Archivieren. Weitere Informationen finden Sie in Upgrade des IBM Spectrum Protect-Servers und des IBM Spectrum Protect-Clients durchführen.

Windows: Planung für optimale Leistung

Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.

Vorgehensweise

1. Lesen Sie den Abschnitt Windows: Vorausgesetzte Kenntnisse.
2. Lesen Sie jeden der folgenden Unterabschnitte.

- Windows: Planung für die Server-Hardware und das Betriebssystem
  Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- Windows: Planung für Platten für die Serverdatenbank
  Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- Windows: Planung für Platten für das Serverwiederherstellungsprotokoll
  Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.
- Windows: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools
  Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.
- Windows: Planung für Speicherpools auf DISK- oder FILE-Einheiten
  Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.
- Windows: Planung für die Auswahl des korrekten Speichertechnologietyps
  Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.
- Windows: Bewährte Verfahren bei der Serverinstallation anwenden
  Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

Windows: Planung für die Server-Hardware und das Betriebssystem

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Werden die Betriebssystem- und Hardwarevoraussetzungen erfüllt oder mehr als erfüllt? • Anzahl und Geschwindigkeit der Prozessoren • Systemspeicher • Unterstützte Betriebssystemversion	Wenn Sie die erforderliche Mindestspeicherkapazität verwenden, können Sie eine minimale Arbeitslast unterstützen. Sie können versuchsweise mehr Systemspeicher hinzufügen, um bestimmen zu können, ob sich die Leistung verbessert. Entscheiden Sie dann, ob der Systemspeicher dem Server zugeordnet bleiben soll. Testen Sie die verschiedenen Speicherkapazitäten jeweils anhand des gesamten Tageszyklus der Serverlast. Wenn Sie mehrere Server auf dem System ausführen, addieren Sie die Voraussetzungen für jeden Server, um die Voraussetzungen für das System zu bestimmen.	Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309. Lesen Sie außerdem die Anweisungen in Tasks für Betriebssysteme und andere Anwendungen optimieren. Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation Weitere Informationen zu Anforderungen in Bezug auf die Größe des Servers und des Speichers finden Sie im IBM Spectrum Protect-Blueprint.
Sind Platten für die optimale Leistung konfiguriert?	Der Umfang der Optimierung, der für verschiedene Plattensysteme erfolgen kann, variiert. Stellen Sie sicher, dass die Warteschlangenlänge und andere Plattensystemoptionen entsprechend definiert sind.	Weitere Informationen finden Sie in: • "Planung für Platten für die Serverdatenbank" • "Planung für Platten für das Serverwiederherstellungsprotokoll" • "Planung für Speicherpools auf DISK- oder FILE-Einheiten"

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verfügt der Server über genügend Speicher?	Höhere Arbeitslasten und erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation erfordern mehr Systemspeicher als den Mindestspeicher, der im Dokument mit den Systemvoraussetzungen angegeben ist. Verwenden Sie die folgenden Richtlinien, um den Speicherbedarf für Datenbanken anzugeben, die nicht für die Datendeduplizierung aktiviert sind: • Für Datenbanken mit einer Größe unter 500 GB benötigen Sie 16 GB Speicher. • Für Datenbanken mit einer Größe von 500 GB bis 1 TB benötigen Sie 24 GB Speicher. • Für Datenbanken mit einer Größe von 1 TB bis 1,5 TB benötigen Sie 32 GB Speicher. • Für Datenbanken mit einer Größe über 1,5 TB benötigen Sie 40 GB Speicher. Stellen Sie sicher, dass Sie für die Replikationsverarbeitung zusätzlichen Speicherbereich für die aktive Protokolldatei und das Archivprotokoll zuordnen.	Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation • Speicherbedarf
Verfügt das System über genügend Hostbusadapter (HBAs), um die Datenoperationen, die der IBM Spectrum Protect-Server gleichzeitig ausführen muss, handhaben zu können?	Sie müssen wissen, für welche Operationen die gleichzeitige Verwendung von Hostbusadaptern erforderlich ist. Ein Server muss beispielsweise Sicherungsdaten mit 1 GB/s speichern, während er gleichzeitig eine Speicherpoolumlagerung ausführt, für deren Ausführung eine Kapazität von 0,5 GB/s erforderlich ist. Die Hostbusadapter müssen alle Daten mit der erforderlichen Geschwindigkeit handhaben können.	Siehe HBA-Kapazität optimieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Ist die Netzbandbreite größer als der geplante maximale Durchsatz für Sicherungen?	Die Netzbandbreite muss dem System die Ausführung von Operationen wie Sicherungen innerhalb der zulässigen Zeit oder gemäß den vereinbarten Service-Levels ermöglichen. Bei der Knotenreplikation muss die Netzbandbreite größer als der geplante maximale Durchsatz sein.	Weitere Informationen finden Sie in: • Netzleistung optimieren • Prüfliste für Knotenreplikation
Verwenden Sie ein bevorzugtes Dateisystem für IBM Spectrum Protect-Serverdateien?	Verwenden Sie ein Dateisystem, das optimale Leistung und Datenverfügbarkeit gewährleistet. Der Server verwendet die direkte E/A mit Dateisystemen, die die Funktion unterstützen. Die Verwendung der direkten E/A kann den Durchsatz verbessern und die Prozessornutzung verringern. Die folgende Liste zeigt das jeweils bevorzugte Dateisystem: • Windows-Betriebssysteme Verwenden Sie NTFS (New Technology File System) ohne Komprimierung.	Weitere Informationen finden Sie in Betriebssystem für die Plattenleistung konfigurieren.
Planen Sie, genügend Seitenauslagerungsbereich zu konfigurieren?	Seitenauslagerungsbereich (oder Auslagerungsspeicher) erweitert den Speicher, der für die Verarbeitung verfügbar ist. Wenn der freie Arbeitsspeicher im System knapp wird, werden Programme oder Daten, die nicht im Gebrauch sind, aus dem Speicher in den Seitenauslagerungsbereich versetzt. Mit dieser Aktion wird Speicherbereich für andere Aktivitäten, wie z. B. Datenbankoperationen, freigegeben. Windows-Betriebssysteme Der Seitenauslagerungsbereich wird automatisch konfiguriert.	

Windows: Planung für Platten für die Serverdatenbank

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Befindet sich die Datenbank auf schnellen Platten mit kurzer Latenzzeit?	Verwenden Sie die folgenden Laufwerke nicht für die IBM Spectrum Protect-Datenbank: • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) Verwenden Sie keine internen Platten, die standardmäßig Teil der Hardware der meisten Server ist. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung. Wenn Sie planen, die Datendeduplizierungsfunktionen von IBM Spectrum Protect zu verwenden, legen Sie den Schwerpunkt auf die Plattenleistung (gemessen in E/A-Operationen pro Sekunde).	Weitere Informationen finden Sie in Prüfliste für Datendeduplizierung.
Ist die Datenbank auf anderen Platten oder LUNs gespeichert als die aktive Protokolldatei, das Archivprotokoll und die Speicherpooldatenträger?	Das Trennen der Serverdatenbank von anderen Serverkomponenten trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei. Tipp: Die Datenbank und das Archivprotokoll können ein Array gemeinsam nutzen, wenn Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) verwenden.	
Wissen Sie bei Verwendung von RAID, wie die optimale RAID-Stufe für Ihr System ausgewählt wird? Definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ?	Wenn ein System viele Schreibvorgänge ausführen muss, ist die Leistung bei RAID 10 besser als bei RAID 5. RAID 10 benötigt jedoch mehr Platten als RAID 5, um dieselbe nutzbare Speichermenge bereitzustellen. Handelt es sich bei Ihrem Plattensystem um ein RAID-System, definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ. Verwenden Sie beispielsweise nicht gleichzeitig 4+1 RAID 5 mit 4+2 RAID 6.	
Planen Sie, wenn eine Option zum Definieren der Stripgröße oder der Segmentgröße verfügbar ist, die Größe beim Konfigurieren des Plattensystems zu optimieren?	Wenn Sie die Stripgröße oder Segmentgröße definieren können, verwenden Sie auf Plattensystemen für die Datenbank Größen von 64 KB oder 128 KB.	Die Blockgröße, die für die Datenbank verwendet wird, variiert abhängig vom Tabellenbereich. Die meisten Tabellenbereiche verwenden 8-KB-Blöcke; einige verwenden jedoch 32-KB-Blöcke.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Planen Sie, mindestens vier Verzeichnisse, die auch als Speicherpfade bezeichnet werden, auf vier verschiedenen LUNs für die Datenbank zu erstellen? Erstellen Sie exakt ein Verzeichnis pro Array in dem Subsystem. Wenn weniger als drei Arrays vorhanden sind, erstellen Sie in jedem Array einen anderen LUN-Datenträger.	Für größere Arbeitslasten und bei Verwendung einiger Funktionen sind mehr Datenbankspeicherpfade als die Mindestvoraussetzungen erforderlich. Serveroperationen wie die Datendeduplizierung verursachen eine hohe Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS) für die Datenbank. Die Leistung derartiger Operationen ist besser, wenn die Datenbank über mehr Verzeichnisse verfügt. Verwenden Sie für Serverdatenbanken, die größer als 2 TB sind oder die wahrscheinlich auf diese Größe anwachsen, acht Verzeichnisse. Berücksichtigen Sie das geplante Wachstum des Systems bei der Bestimmung der Anzahl zu erstellender Speicherpfade. Die höhere Anzahl Speicherpfade wird vom Server effizienter genutzt, wenn die Speicherpfade bei der Ersterstellung des Servers bereits vorhanden sind. Verwenden Sie die Variable *DB2_PARALLEL_IO*, um die parallele E/A für Tabellenbereiche mit einem einzelnen Container zu erzwingen oder für Tabellenbereiche, die über Container auf mehr als einer physischen Platte verfügen. Wenn Sie die Variable *DB2_PARALLEL_IO* nicht definieren, entspricht die E/A-Parallelität der Anzahl Container, die von dem Tabellenbereich verwendet werden. Wenn ein Tabellenbereich beispielsweise vier Container umfasst, beträgt der verwendete Grad an E/A-Parallelität 4.	Weitere Informationen finden Sie in: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation Hilfreiche Informationen zur Vorhersage des Wachstums beim Deduplizieren von Daten durch den Server finden Sie in Technote 1596944. Aktuelle Informationen zur Datenbankgröße, zur Datenbankreorganisation und zu Leistungsaspekten für IBM Spectrum Protect-Server finden Sie in Technote 1683633. Informationen zum Definieren der Variable *DB2_PARALLEL_IO* finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.
Haben alle Verzeichnisse für die Datenbank dieselbe Größe?	Verzeichnisse, die alle dieselbe Größe haben, stellen einen konsistenten Grad an Parallelität für Datenbankoperationen sicher. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als andere sind, verringert sich dadurch das Potenzial für den optimierten parallelen Vorablesezugriff. Diese Richtlinie gilt auch, wenn Sie nach der Erstkonfiguration des Servers Speicherpfade hinzufügen müssen.	
Planen Sie, die Warteschlangenlänge der Datenbank-LUNs auf AIX-Systemen zu erhöhen?	Die Standardwarteschlangenlänge ist häufig zu niedrig definiert.	Siehe AIX-Systeme für die Plattenleistung konfigurieren.

Windows: Planung für Platten für das Serverwiederherstellungsprotokoll

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Sind die aktive Protokolldatei und das Archivprotokoll auf anderen Platten oder LUNs gespeichert als die Datenbank und die Speicherpooldatenträger?	Stellen Sie sicher, dass die Platten, auf die die aktive Protokolldatei gestellt wird, auf dem Server oder System nicht für andere Zwecke verwendet werden. Stellen Sie die aktive Protokolldatei nicht auf Platten, die die Serverdatenbank, das Archivprotokoll oder Systemdateien, wie Seitenauslagerungsbereich oder Auslagerungsspeicher, enthalten.	Das Trennen der Serverdatenbank von der aktiven Protokolldatei und dem Archivprotokoll trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.
Befinden sich die Protokolle auf Platten mit nicht flüchtigem Schreibcache?	Nicht flüchtiger Schreibcache ermöglicht es, Daten so schnell wie möglich in die Protokolle zu schreiben. Schnellere Schreiboperationen für die Protokolle können die Leistung für Serveroperationen verbessern.	
Legen Sie für die Protokolle eine Größe fest, die der Arbeitslast entspricht?	Wenn Sie sich über die Arbeitslast im Unklaren sind, verwenden Sie die größtmögliche Größe. Aktive Protokolldatei Die maximale Größe beträgt 512 GB; sie wird über die Serveroption ACTIVELOGSIZE festgelegt. Stellen Sie sicher, dass mindestens 8 GB freier Speicherbereich im Dateisystem für aktive Protokolldateien verfügbar sind, nachdem die aktiven Protokolldateien mit fester Größe erstellt wurden. Archivprotokoll Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Das Archivprotokoll muss mindestens so groß wie die aktive Protokolldatei sein.	• Ausführliche Informationen zur Festlegung der Protokollgröße enthalten die Informationen zum Wiederherstellungsprotokoll in Technote 1421060. • Informationen zur Festlegung der Größe bei Verwendung der Datendeduplizierung finden Sie in Prüfliste für Datendeduplizierung.
Definieren Sie ein Archivübernahmeprotokoll ? Stellen Sie dieses Protokoll auf eine andere Platte als das Archivprotokoll?	Das Archivübernahmeprotokoll dient der Verwendung durch den Server im Notfall, wenn das Archivprotokoll voll ist. Für das Archivübernahmeprotokoll können langsamere Platten verwendet werden.	Geben Sie die Position des Archivübernahmeprotokolls mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY an. Überwachen Sie die Belegung des Verzeichnisses für das Archivübernahmeprotokoll. Wenn das Archivübernahmeprotokoll vom Server verwendet werden muss, ist der Speicherplatz für das Archivprotokoll möglicherweise nicht groß genug.
Verwenden Sie, wenn Sie die aktive Protokolldatei spiegeln, nur einen einzigen Typ von Spiegelung?	Sie können das Protokoll mithilfe einer der folgenden Methoden spiegeln. Verwenden Sie für das Protokoll nur einen einzigen Typ von Spiegelung. • Verwenden Sie die Option MIRRORLOGDIRECTORY, die für den IBM Spectrum Protect-Server verfügbar ist, um eine Position für die Spiegelung anzugeben. • Verwenden Sie die Softwarespiegelung, wie z. B. Logical Volume Manager (LVM) unter AIX. • Verwenden Sie die Spiegelung in der Hardware des Plattensystems.	Stellen Sie, wenn Sie die aktive Protokolldatei spiegeln, sicher, dass die Platten für die aktive Protokolldatei und die Spiegelkopie dieselbe Geschwindigkeit und Zuverlässigkeit haben. Weitere Informationen finden Sie in Wiederherstellungsprotokoll konfigurieren und optimieren.

Windows: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools

Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verwenden Sie, gemessen in Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS), schnellen Plattenspeicher für die IBM Spectrum Protect-Datenbank?	Verwenden Sie eine Hochleistungsplatte für die Datenbank. Verwenden Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) für die Datendeduplizierungsverarbeitung. Stellen Sie sicher, dass die Datenbank über eine Mindestkapazität von 3000 E/A-Operationen pro Sekunde (IOPS) verfügt. Addieren Sie zu diesem Mindestwert pro TB Daten, die täglich (vor der Datendeduplizierung) gesichert werden, 1000 E/A-Operationen pro Sekunde. Beispielsweise würde ein IBM Spectrum Protect-Server, der täglich 3 TB Daten aufnimmt, 6000 E/A-Operationen pro Sekunde (IOPS) für die Datenbankplatten benötigen: `mindestens 3000 IOPS + 3000 (3 TB x 1000 IOPS) = 6000 IOPS`	Empfehlungen zur Plattenauswahl finden Sie in "Planung für Platten für die Serverdatenbank". Weitere Informationen zu IOPS finden Sie in den IBM Spectrum Protect-Blueprints.
Ist genügend Speicherplatz für die Größe Ihrer Datenbank vorhanden?	Verwenden Sie mindestens 40 GB Systemspeicher für IBM Spectrum Protect-Server, die Daten deduplizieren, mit einer Datenbankgröße von 100 GB. Wenn die Speicherkapazität für Sicherungsdaten wächst, ist unter Umständen ein höherer Speicherbedarf erforderlich. Überwachen Sie regelmäßig die Speicherbelegung, um festzustellen, ob mehr Speicherplatz erforderlich ist. Verwenden Sie weiteren Systemspeicher, um das Caching von Datenbankseiten zu verbessern. Die folgenden Richtlinien für die Speichergröße basieren auf dem Volumen an neuen Daten, das jeden Tag gesichert wird: • 128 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 1 und 2 TB liegt • 192 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 2 und 4 TB liegt	Speicherbedarf

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie die Speicherkapazität für die die aktive Protokolldatei und das Archivprotokoll der Datenbank korrekt festgelegt?	Geben Sie in der Konfiguration des Servers eine minimale Größe von 128 GB für die aktive Protokolldatei an, indem Sie die Serveroption ACTIVELOGSIZE auf den Wert 131072 setzen. Als Anfangsgröße für das Archivprotokoll wird eine Größe von 1 TB vorgeschlagen. Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Stellen Sie sicher, dass im Vergleich zur Größe des Archivprotokolls mindestens 10 % zusätzlicher Plattenspeicher für das Dateisystem vorhanden sind. Verwenden Sie für die Datenbankarchivprotokolle ein Verzeichnis mit einer anfänglichen freien Kapazität von mindestens 1 TB. Geben Sie das Verzeichnis mithilfe der Serveroption ARCHLOGDIRECTORY an. Definieren Sie Speicherbereich für das Archivübernahmeprotokoll mithilfe der Serveroption ARCHFAILOVERLOGDIRECTORY.	Weitere Informationen zur Kapazitätsermittlung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.
Ist die Komprimierung für die Archivprotokoll- und Datenbanksicherungen aktiviert?	Aktivieren Sie die Serveroption ARCHLOGCOMPRESS, um Speicherbereich einzusparen. Diese Komprimierungsoption unterscheidet sich von der Inline-Komprimierung. Die Inline-Komprimierung ist ab IBM Spectrum Protect Version 7.1.5 und höher standardmäßig aktiviert. Einschränkung: Sie dürfen diese Option nicht verwenden, wenn das Volumen der pro Tag gesicherten Daten 6 TB überschreitet.	Weitere Informationen zur Komprimierung für Ihr System finden Sie in den IBM Spectrum Protect-Blueprints.
Befinden sich die Datenbank und Protokolle von IBM Spectrum Protect auf separaten Plattendatenträgern (LUNs)? Ist der Datenträger, der für die Datenbank verwendet wird, gemäß den bewährten Verfahren für eine transaktionsorientierte Datenbank konfiguriert?	Die Datenbank darf keine Plattendatenträger mit IBM Spectrum Protect-Datenbankprotokollen oder -Speicherpools oder mit einer anderen Anwendung oder einem anderen Dateisystem gemeinsam nutzen.	Weitere Informationen zur Konfiguration der Serverdatenbank und des Wiederherstellungsprotokolls finden Sie in Konfiguration und Optimierung der Serverdatenbank und des Wiederherstellungsprotokolls.
Verwenden Sie mindestens acht Prozessorkerne (2,2-GHz-Prozessorkerne oder entsprechende Prozessorkerne) für jeden IBM Spectrum Protect-Server, der mit Datendeduplizierung verwendet werden soll?	Wenn die clientseitige Datendeduplizierung verwendet werden soll, müssen Sie sicherstellen, dass für Clientsysteme während einer Sicherungsoperation genügend Ressourcen zur Ausführung der Datendeduplizierungsverarbeitung verfügbar sind. Verwenden Sie pro Sicherungsprozess mit clientseitiger Datendeduplizierung einen Prozessor, der mindestens einem 2,2-GHz-Prozessorkern entspricht.	• Effektive Planung und Verwendung der Deduplizierung • IBM Spectrum Protect Blueprints

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie genügend Speicherplatz für die Datenbank zugeordnet?	Als grobe Schätzung sollten Sie 100 GB Datenbankspeicher für jeweils 50 TB Daten einplanen, die in deduplizierten Speicherpools geschützt werden sollen. *Geschützte Daten* ist das Datenvolumen vor der Datendeduplizierung, einschließlich aller Versionen gespeicherter Objekte. Als bewährtes Verfahren sollten Sie einen neuen Containerspeicherpool ausschließlich für die Datendeduplizierung definieren. Die Datendeduplizierung erfolgt auf der Speicherpoolebene; mit Ausnahme von verschlüsselten Daten werden alle Daten in einem Speicherpool dedupliziert.	
Haben Sie die Speicherpoolkapazität geschätzt, um genügend Speicherplatz für die Größe Ihrer Umgebung zu konfigurieren?	Sie können den Kapazitätsbedarf für einen deduplizierten Speicherpool wie folgt schätzen: 1. Schätzen Sie die Basisgröße der Quellendaten. 2. Schätzen Sie die Größe der täglichen Sicherung anhand einer geschätzten Änderungs- und Wachstumsrate. 3. Bestimmen Sie die Anforderungen in Bezug auf die Aufbewahrungsdauer. 4. Schätzen Sie das Gesamtvolumen an Quellendaten unter Berücksichtigung der Basisgröße, der Größe der täglichen Sicherung und der Anforderungen in Bezug auf die Aufbewahrungsdauer. 5. Wenden Sie den Faktor für das Deduplizierungsverhältnis an. 6. Wenden Sie den Faktor für das Komprimierungsverhältnis an. 7. Runden Sie die Schätzung auf, um die Nutzung transienter Speicherpools zu berücksichtigen.	Ein Beispiel zur Verwendung dieses Verfahrens finden Sie in Effektive Planung und Verwendung der Deduplizierung.
Haben Sie die Platten-E/A auf viele Platteneinheiten und Controller verteilt?	Verwenden Sie Arrays, die aus so vielen Platten wie möglich bestehen; dies wird auch als "Wide-Striping" bezeichnet. Stellen Sie sicher, dass Sie exakt ein Datenbankverzeichnis pro Array in dem Subsystem verwenden. Definieren Sie die Registry-Variable *DB2_PARALLEL_IO*, um die parallele E/A für jeden verwendeten Tabellenbereich zu aktivieren, wenn sich die Container in dem Tabellenbereich über mehrere physische Platten erstrecken. Wenn E/A-Bandbreite verfügbar ist und die Dateien groß sind (beispielsweise 1 MB), kann der Prozess zur Suche nach Duplikaten die Ressourcen eines gesamten Prozessors in Anspruch nehmen. Wenn Dateien kleiner sind, können andere Engpässe auftreten. Geben Sie acht oder mehr Dateisysteme für die Einheitenklasse des deduplizierten Speicherpools an, damit die Ein-/Ausgabe auf so viele LUNs und physische Einheiten wie möglich verteilt wird.	Richtlinien zur Konfiguration von Speicherpools finden Sie in "Planung für Speicherpools auf DISK- oder FILE-Einheiten". Informationen zum Definieren der Variable *DB2_PARALLEL_IO* finden Sie in Empfohlene Einstellungen für IBM DB2-Registry-Variablen.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie tägliche Operationen auf der Basis Ihrer Sicherungsstrategie geplant?	Die Operationsfolge sieht gemäß den bewährten Verfahren wie folgt aus: 1. Clientsicherung 2. Speicherpoolschutz 3. Knotenreplikation 4. Datenbanksicherung 5. Bestandsverfall	• Datendeduplizierungs- und Knotenreplikationsprozesse planen • Tägliche Operation für Verzeichniscontainerspeicherpools
Ist genügend Speicher zur Verwaltung der DB2-Sperrenliste vorhanden?	Wenn Sie Daten deduplizieren, die große Dateien oder gleichzeitig eine große Anzahl Dateien umfassen, kann der Prozess zur Speicherknappheit führen. Wenn der Sperrenlistenspeicher nicht ausreichend ist, können Sicherungsfehler, Datenverwaltungsprozessfehler oder Serverausfälle auftreten. Bei Dateigrößen über 500 GB, die durch die Datendeduplizierung verarbeitet werden, ist es sehr wahrscheinlich, dass der Speicherplatz knapp wird. Wenn jedoch viele Sicherungsoperationen die clientseitige Datendeduplizierung verwenden, kann dieses Problem auch bei Dateien mit geringerer Größe auftreten.	Informationen zur Optimierung des DB2-Parameters LOCKLIST finden Sie in Serverseitige Datendeduplizierung optimieren.
Ist genügend Bandbreite verfügbar, um Daten auf einen IBM Spectrum Protect-Server zu übertragen?	Um Daten auf einen IBM Spectrum Protect-Server zu übertragen, verwenden Sie die clientseitige oder serverseitige Datendeduplizierung und die Komprimierung, um die erforderliche Bandbreite zu verringern. Verwenden Sie einen Server der Version 7.1.5 oder höher, um die Inline-Komprimierung verwenden zu können, und einen Client der Version 7.1.6 oder höher, um die erweiterte Komprimierungsverarbeitung zu aktivieren.	Weitere Informationen finden Sie in der Beschreibung der Clientoption enablededup.
Haben Sie festgelegt, wie viele Speicherpoolverzeichnisse jedem Speicherpool zugeordnet werden sollen?	Ordnen Sie Verzeichnisse einem Speicherpool mithilfe des Befehls DEFINE STGPOOLDIRECTORY zu. Erstellen Sie mehrere Speicherpoolverzeichnisse und stellen Sie sicher, dass jedes Verzeichnis auf einem anderen Plattendatenträger (LUN) gesichert wird.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie genügend Plattenspeicherplatz in dem Cloud-Containerspeicherpool zugeordnet?	Um Sicherungsfehler zu verhindern, stellen Sie sicher, dass das lokale Verzeichnis über genügend Speicherplatz verfügt. Verwenden Sie die folgende Liste als Leitfaden für optimalen Plattenspeicherplatz: • Berechnen Sie für SAS-Platten (SAS = Serial-Attached SCSI) und rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu. • Stellen Sie 3 TB für flash-basierte Speichersysteme mit schnellen Netzverbindungen zu leistungsfähigen On-Premises-Cloudsystemen bereit. • Stellen Sie 5 TB für Systeme mit Solid-State-Laufwerk (SSD) mit schnellen Netzverbindungen zu leistungsfähigen Cloudsystemen bereit.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Haben Sie den geeigneten Typ des lokalen Speichers ausgewählt?	Stellen Sie sicher, dass Datenübertragungen aus dem lokalen Speicher in die Cloud beendet werden, bevor der nächste Sicherungszyklus beginnt.
	Tipp: Daten werden kurz nach dem Versetzen in die Cloud aus dem lokalen Speicher entfernt.
	Verwenden Sie die folgenden Richtlinien:
	• Verwenden Sie Flash- oder SSD-Speicher für große Systeme, die über leistungsfähige Cloudsysteme verfügen. Stellen Sie sicher, dass Sie über eine dedizierte 10-GB-WAN-Verbindung mit einer Hochgeschwindigkeitsverbindung zum Objektspeicher verfügen. Verwenden Sie beispielsweise Flash- oder SSD-Speicher, wenn Sie über eine dedizierte 10-GB-WAN-Verbindung sowie eine Hochgeschwindigkeitsverbindung zu einem IBM® Cloud Object Storage-Speicherort oder zu einem Amazon S3-Datencenter (Amazon S3 = Amazon Simple Storage Service) verfügen.
	• Verwenden Sie SAS-Platten mit 15000 U/min mit größerer Kapazität für die folgenden Szenarios:
	  ○ Systeme mittlerer Größe
	  ○ Langsamere Cloudverbindungen, z. B. 1 GB
	  ○ Bei Verwendung von IBM Cloud Object Storage als Service-Provider in mehreren Regionen
	• Berechnen Sie für SAS-Platten oder rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.	

Windows: Planung für Speicherpools auf DISK- oder FILE-Einheiten

Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Können die Speicherpool-LUNs Durchsatzraten von 256 KB für sequenzielle Lese- und Schreibvorgänge aufrechterhalten, um die Arbeitslast innerhalb der Zeitvorgaben adäquat handhaben zu können?	Bei der Planung für Spitzenbelastungen müssen Sie alle Daten berücksichtigen, die der Server gleichzeitig aus Plattenspeicherpools lesen oder in Plattenspeicherpools schreiben soll. Berücksichtigen Sie beispielsweise den Spitzenwert für den Datenfluss bei Clientsicherungsoperationen und Serverdatenversetzungsoperationen, wie z. B. Umlagerung, die gleichzeitig ausgeführt werden. Der IBM Spectrum Protect-Server verwendet beim Lesen aus Speicherpools und Schreiben in Speicherpools in erster Linie 256-KB-Blöcke. Wenn das Plattensystem über die entsprechende Funktionalität verfügt, konfigurieren Sie das Plattensystem für die optimale Leistung mit sequenziellen Lese-/Schreiboperationen statt mit wahlfreien Lese-/Schreiboperationen.	Weitere Informationen finden Sie in Basisleistung von Plattensystemen analysieren.
Ist die Platte für die Verwendung von Lese- und Schreibcache konfiguriert?	Verwenden Sie mehr Cache, um eine bessere Leistung zu erzielen.	
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, eine geeignete Größe für die Speicherpooldatenträger festgelegt?	Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden. Wenn Sie nicht über die nötigen Informationen zum Schätzen der Größe für Datenträger mit der Einheitenklasse FILE verfügen, beginnen Sie mit einer Datenträgergröße von 50 GB.	In der Regel treten häufiger Probleme auf, wenn die Datenträger zu klein sind. Wenn Datenträger größer als erforderlich sind, treten nur selten Probleme auf. Wenn Sie die zu verwendende Datenträgergröße festlegen, sollten Sie als Vorsichtsmaßnahme eine größere Größe als erforderlich wählen.
Verwenden Sie für Speicherpools, die die Einheitenklasse FILE verwenden, vorab zugeordnete Datenträger?	Arbeitsdatenträger können eine Dateifragmentierung zur Folge haben. Um sicherzustellen, dass für einen Speicherpool immer genügend Datenträger verfügbar sind, setzen Sie den Parameter MAXSCRATCH auf einen Wert größer als null.	Ordnen Sie mithilfe des Befehls DEFINE VOLUME Datenträger in dem Speicherpool vorab zu. Verwenden Sie den Serverbefehl DEFINE STGPOOL oder UPDATE STGPOOL, um den Parameter MAXSCRATCH zu definieren.
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, die maximale Anzahl Clientsitzungen mit der Anzahl definierter Datenträger verglichen?	Es müssen immer genügend verwendbare Datenträger in den Speicherpools vorhanden sein, um die erwartete maximale Anzahl gleichzeitig ausgeführter Clientsitzungen handhaben zu können. Bei den Datenträgern kann es sich um Arbeitsdatenträger, leere Datenträger oder teilweise gefüllte Datenträger handeln.	Bei Speicherpools, die die Einheitenklasse FILE verwenden, kann jeweils nur eine einzige Sitzung oder ein einziger Prozess auf einen Datenträger schreiben.
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, den Parameter MOUNTLIMIT für die Einheitenklasse auf einen Wert gesetzt, der für die Anzahl Datenträger, die parallel angehängt werden könnten, ausreichend hoch ist?	Für Speicherpools, die die Datendeduplizierung verwenden, liegt der Wert für den Parameter MOUNTLIMIT in der Regel zwischen 500 und 1000. Setzen Sie den Wert für MOUNTLIMIT auf die maximale Anzahl Mountpunkte, die für alle aktiven Sitzungen erforderlich sind. Berücksichtigen Sie Parameter, die sich auf die maximale Anzahl erforderlicher Mountpunkte auswirken: • Die Serveroption MAXSESSIONS, die die maximal zulässige Anzahl gleichzeitig ablaufender IBM Spectrum Protect-Sitzungen angibt • Der Parameter MAXNUMMP, der die maximale Anzahl Mountpunkte definiert, die jeder Clientknoten verwenden kann Wenn beispielsweise die maximalen Anzahl Sicherungssitzungen für Clientknoten normalerweise 100 ist und für jeden der Knoten `MAXNUMMP=2` definiert ist, multiplizieren Sie 100 Knoten mit 2 Mountpunkten für jeden Knoten, um den Wert 200 für den Parameter MOUNTLIMIT zu erhalten.	Verwenden Sie den Serverbefehl REGISTER NODE oder UPDATE NODE, um den Parameter MAXNUMMP für Clientknoten zu definieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie für Speicherpools, die die Einheitenklasse DISK verwenden, festgelegt, wie viele Speicherpooldatenträger in jedes Dateisystem gestellt werden sollen?	Die Konfiguration des Speichers für einen Speicherpool, der eine Einheitenklasse DISK verwendet, ist davon abhängig, ob Sie RAID für das Plattensystem verwenden. Wenn Sie RAID nicht verwenden, konfigurieren Sie ein einzige Dateisystem pro physischer Platte und definieren Sie exakt einen Speicherpooldatenträger für jedes Dateisystem. Wenn Sie RAID 5 mit *n* + 1 Datenträgern verwenden, konfigurieren Sie den Speicher auf eine der folgenden Arten: • Konfigurieren Sie *n* Dateisysteme auf der LUN und definieren Sie exakt einen Speicherpooldatenträger pro Dateisystem. • Konfigurieren Sie ein einziges Dateisystem und *n* Speicherpooldatenträger für die LUN.	Ein Beispiellayout, bei dem diese Richtlinie eingehalten wird, zeigt Beispiellayout für Serverspeicherpools.
Haben Sie Ihre Speicherpools für die Verteilung der Ein-/Ausgabe auf mehrere Dateisysteme erstellt?	Stellen Sie sicher, dass sich jedes Dateisystem auf einer anderen LUN auf dem Plattensystem befindet. Normalerweise sind 10-30 Dateisysteme ein geeigneter Wert, Sie müssen jedoch sicherstellen, dass die Dateisysteme nicht kleiner als etwa 250 GB sind.	Ausführliche Informationen finden Sie in: • Plattenspeicher für den Server optimieren • Speicherpools und Datenträger optimieren und konfigurieren

Windows: Planung für die Auswahl des korrekten Speichertechnologietyps

Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.

Vorgehensweise

Die folgende Tabelle unterstützt Sie bei der Auswahl des korrekten Speichertechnologietyps für die Speicherressourcen, die der Server erfordert.

Tabelle 1. Speichertechnologietypen für IBM Spectrum Protect-Speicherbedarf

Speichertechnologietyp	Datenbank	Aktive Protokolldatei	Archivprotokoll und Archivübernahmeprotokoll	Speicherpools
Solid-State-Laufwerk (SSD)	Stellen Sie die Datenbank auf ein Solid-State-Laufwerk, wenn die folgenden Bedingungen erfüllt sind: • Sie verwenden die IBM Spectrum Protect-Datendeduplizierung. • Sie sichern täglich mehr als 8 TB neuer Daten.	Wenn Sie die IBM Spectrum Protect-Datenbank auf ein Solid-State-Laufwerk stellen (dies ist das bewährte Verfahren), stellen Sie auch die aktive Protokolldatei auf ein Solid-State-Laufwerk. Wenn kein Speicherplatz verfügbar ist, verwenden Sie stattdessen eine Hochleistungsplatte.	Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Das Archivprotokoll und die Archivübernahmeprotokolle können auf langsamere Speichertechnologietypen gestellt werden.	Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Speicherpools können auf langsamere Speichertechnologietypen gestellt werden.

Speichertech-nologietyp	Datenbank	Aktive Protokolldatei	Archivprotokoll und Archivübernahmepro-tokoll	Speicherpools
Hochleistungs-platte mit den folgenden Kenndaten: • **Platte mit 15.000 U/min** • **Fibre Channel- oder Serial-attached SCSI-Schnittstelle (SAS-Schnittstelle)**	Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind: • Der Server führt keine Datendeduplizierung aus. • Der Server führt keine Knotenreplikation aus. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.	Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind: • Der Server führt keine Datendeduplizierung aus. • Der Server führt keine Knotenreplikation aus. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.	Sie können Hochleistungsplatten für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.	Verwenden Sie Hochleistungsplatten für Speicherpools, wenn die folgenden Bedingungen erfüllt sind: • Daten werden häufig gelesen. • Daten werden häufig geschrieben. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.
Platte mit mittlerer Leistung oder Hochleis-tungsplatte mit den folgenden Kenndaten: • **Platte mit 10.000 U/min** • **Fibre Channel- oder SAS-Schnittstelle**	Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.	Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.	Sie können eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für das Archivprotokoll und die Archivüber-nahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.	Verwenden Sie eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für Speicherpools, wenn die folgenden Bedingungen erfüllt sind: • Daten werden häufig gelesen. • Daten werden häufig geschrieben. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.
SATA, Network-attached Storage (NAS)	Verwenden Sie diesen Speicher nicht für die Datenbank. Stellen Sie die Datenbank nicht auf XIV-Speichersysteme.	Verwenden Sie diesen Speicher nicht für die aktive Protokolldatei.	Die Verwendung dieser langsameren Speichertechnologie ist akzeptabel, da diese Protokolle einmal geschrieben und nur selten gelesen werden.	Verwenden Sie diese langsamere Speichertechnologie, wenn die folgenden Bedingungen erfüllt sind: • Daten werden selten geschrieben, beispielsweise einmal. • Daten werden selten gelesen. .
Bänder und virtuelle Bänder				Verwenden Sie diese Speichermedien für die langfristige Aufbewahrung oder wenn Daten nur selten verwendet werden.

Windows: Bewährte Verfahren bei der Serverinstallation anwenden

Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

Vorgehensweise

- Nachfolgend sind die wichtigsten bewährten Verfahren für die Erzielung der optimalen Leistung und die Vermeidung von Problemen aufgeführt.
- Bestimmen Sie anhand der Tabelle die bewährten Verfahren, die für Ihre Umgebung gelten.

Bewährtes Verfahren	Weitere Informationen
Verwenden Sie schnelle Platten für die Serverdatenbank. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung.	Verwenden Sie schnelle Platten mit kurzer Latenzzeit für die Datenbank. Die Verwendung von Solid-State-Laufwerken ist von entscheidender Bedeutung, wenn Sie die Datendeduplizierung und Knotenreplikation verwenden. Vermeiden Sie die Verwendung von SATA-Laufwerken (SATA = Serial Advanced Technology Attachment) und PATA-Laufwerken (PATA = Parallel Advanced Technology Attachment). Ausführliche Informationen und weitere Tipps finden Sie in: ◦ "Planung für Platten für die Serverdatenbank" ◦ "Planung für die Auswahl des korrekten Speichertechnologietyps"
Stellen Sie sicher, dass das Serversystem über genügend Speicher verfügt.	Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 1243309. Höhere Arbeitslasten erfordern mehr als die Mindestvoraussetzungen. Erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation können mehr Speicher als den Mindestspeicher erfordern, der im Dokument mit den Systemvoraussetzungen angegeben ist. Wenn Sie die Ausführung mehrerer Instanzen planen, ist für jede Instanz der für einen einzelnen Server aufgelistete Speicher erforderlich. Multiplizieren Sie den für einen einzelnen Server erforderlichen Speicher mit der Anzahl der für das System geplanten Instanzen.
Trennen Sie die Serverdatenbank, die aktive Protokolldatei, das Archivprotokoll und die Plattenspeicherpools voneinander.	Stellen Sie alle IBM Spectrum Protect-Speicherressourcen auf unterschiedliche Platten. Trennen Sie Speicherpoolplatten von den Platten für die Serverdatenbank und die Protokolle. Speicherpooloperationen können Datenbankoperationen beeinträchtigen, wenn sich die Speicherpools und die Datenbank auf denselben Platten befinden. Im Idealfall werden auch die Serverdatenbank und die Protokolle voneinander getrennt. Ausführliche Informationen und weitere Tipps finden Sie in: ◦ "Planung für Platten für die Serverdatenbank" ◦ "Planung für Platten für das Serverwiederherstellungsprotokoll" ◦ "Planung für Speicherpools auf DISK- oder FILE-Einheiten"
Verwenden Sie mindestens vier Verzeichnisse für die Serverdatenbank. Verwenden Sie für größere Server oder Server, die erweiterte Funktionen verwenden, acht Verzeichnisse.	Stellen Sie jedes Verzeichnis auf eine LUN, die von anderen LUNs und von anderen Anwendungen getrennt ist. Ein Server wird als großer Server betrachtet, wenn seine Datenbank größer als 2 TB ist oder wahrscheinlich diese Größe erreichen wird. Verwenden Sie für derartige Server acht Verzeichnisse. Siehe "Planung für Platten für die Serverdatenbank".
Wenn Sie die Datendeduplizierung und/oder die Knotenreplikation verwenden, beachten Sie die Richtlinien für die Datenbankkonfiguration und andere Elemente.	Konfigurieren Sie den Server gemäß den Richtlinien, da die Datenbank in Bezug darauf, wie gut die Ausführung des Servers bei Verwendung dieser Funktionen ist, extrem wichtig ist. Ausführliche Informationen und weitere Tipps finden Sie in: ◦ Prüfliste für Datendeduplizierung ◦ Prüfliste für Knotenreplikation

Bewährtes Verfahren	Weitere Informationen
Beachten Sie bei Speicherpools, die Einheitenklassen des Typs FILE verwenden, die Richtlinien für die Größe von Speicherpooldatenträgern. In der Regel sind Datenträger mit einer Größe von 50 GB am besten geeignet.	Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden zur Bestimmung der Datenträgergröße. Konfigurieren Sie Speicherpooleinheiten und Dateisysteme auf der Basis der Anforderungen in Bezug auf den Durchsatz und nicht nur auf der Basis der Kapazitätsanforderungen. Trennen Sie die Speichereinheiten, die von IBM Spectrum Protect verwendet werden, von anderen Anwendungen mit hoher Ein-/Ausgabe und stellen Sie sicher, dass der Durchsatz für diesen Speicher ausreichend ist. Weitere Informationen finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.
Planen Sie IBM Spectrum Protect-Clientoperationen und -Serververwaltungsaktivitäten, um eine Überschneidung von Operationen zu verhindern oder auf ein Mindestmaß zu reduzieren.	Weitere ausführliche Informationen liefern die folgenden Themen: ◦ Zeitplan für tägliche Operationen optimieren ◦ Prüfliste für Serverkonfiguration
Überwachen Sie Operationen kontinuierlich.	Die Überwachung ermöglicht es Ihnen, Probleme frühzeitig erkennen und Ursachen leichter ermitteln zu können. Bewahren Sie Aufzeichnungen von Überwachungsberichten bis zu einem Jahr lang auf, um Trends schneller erkennen und Wachstum besser planen zu können. Siehe Umgebung im Hinblick auf die Leistung überwachen und verwalten.

Windows: Systemmindestvoraussetzungen für Windows-Systeme

Für den Server können sehr viel Speicherplatz, eine große Netzbandbreite und viele Prozessorressourcen erforderlich sein. In vielen Fällen ist die Leistung des Servers am besten, wenn andere Anwendungen nicht auf demselben System installiert sind.

Hardware- und Softwarevoraussetzungen für die IBM Spectrum Protect-Serverinstallation

Die folgenden Tabellen enthalten die Mindesthardware- und -softwarevoraussetzungen für die Installation eines IBM Spectrum Protect-Servers. Verwenden Sie diese Voraussetzungen als Ausgangspunkt für Systeme ohne Datendeduplizierung. Die optimale IBM Spectrum Protect-Umgebung ist mit Datendeduplizierung mithilfe der IBM Spectrum Protect Blueprints konfiguriert. Die neuesten Informationen zu den Systemvoraussetzungen finden Sie unter Technote 1243309.

Hardwarevoraussetzungen

In Tabelle 1 sind die Hardwaremindestvoraussetzungen für den Server beschrieben. Wenn der Server die Mindestvoraussetzungen nicht erfüllt, schlägt die Installation fehl. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in Windows: Kapazitätsplanung.

Tabelle 1. Hardwarevoraussetzungen

Hardwaretyp	Hardwarevoraussetzungen
Hardware	Ein AMD64- oder Intel EMT-64-Prozessor

Hardwaretyp	Hardwarevoraussetzungen
Plattenspeicher	Folgende Mindestwerte für den Plattenspeicher: • Mindestens 7,5 GB freier Plattenspeicher für eine Standardinstallation • 60 MB im temporären Verzeichnisbereich • 2 GB Partitionsgröße im Laufwerk C:\ • 300 MB im Instanzverzeichnis • 2 GB für den Bereich der gemeinsam genutzten Ressourcen Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben. Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten. Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN. Lesen Sie den Abschnitt zur Windows: Kapazitätsplanung, um weitere Informationen zum Plattenspeicherplatz zu erhalten.
Hauptspeicher	Folgende Mindestwerte für den Hauptspeicher: • 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation • 24 GB für Datendeduplizierung oder Knotenreplikation • 32 GB für Knotenreplikation mit Datendeduplizierung Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect. Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.

Softwarevoraussetzungen

In Tabelle 2 sind die für einen Server auf einem Windows-System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 2. Softwarevoraussetzungen

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Eines der folgenden Betriebssysteme: • Microsoft Windows Server 2012: Standard, Enterprise oder Datacenter Edition (64-Bit) • Microsoft Windows Server 2012 R2 (64-Bit) • Microsoft Windows Server 2016
Übertragungsprotokoll	Mindestens eins der folgenden Übertragungsprotokolle (standardmäßig mit den aktuellen Windows-Betriebssystemen installiert): • Benannte Pipes • TCP/IP Version 4 oder Version 6
Einheitentreiber	Der für Laufwerke und Bandarchive eines anderen Herstellers erforderliche IBM Spectrum Protect-Durchgriffseinheitentreiber. Der systemeigene Windows-Einheitentreiber wird für Bandlaufwerke und Bandarchive empfohlen. Andernfalls kann der IBM Spectrum Protect-Kerneleinheitentreiber verwendet werden. Für die Bandarchive bzw. Bandlaufwerke IBM® 3590, 3592 oder Ultrium sind die IBM Einheitentreiber erforderlich. Installieren Sie die aktuellen Einheitentreiber. IBM-Treiberpakete finden Sie bei Fix Central. Konfigurieren Sie die Einheitentreiber, bevor Sie den Server für Bandeinheiten verwenden.

Softwaretyp	Softwaremindestvoraussetzungen
Sonstige Software	Für Windows 2012, Windows 2012 R2 und Windows 2016 muss .NET Framework 3.5 installiert und aktiviert sein. Die folgenden Richtlinien für die Benutzerkontensteuerung müssen inaktiviert werden: • Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto • Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen Um IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) zu authentifizieren, müssen Sie einen der folgenden Verzeichnisserver verwenden: • Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2) • IBM Security Directory Server Version 6.3 • IBM Security Directory Server Version 6.4

Windows: IBM Installation Manager

IBM Spectrum Protect verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager noch nicht installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie IBM Spectrum Protect installieren. Die Software muss auf dem System installiert bleiben, damit IBM Spectrum Protect später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

Angebot
: Eine installierbare Einheit eines Softwareprodukts.

  Das Angebot 'IBM Spectrum Protect' enthält alle Datenträger, die IBM Installation Manager für die Installation von IBM Spectrum Protect benötigt.

Paket
: Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.
  Das IBM Spectrum Protect-Paket enthält folgende Komponenten:

  • Installationsprogramm IBM Installation Manager
  • Das Angebot 'IBM Spectrum Protect'

Paketgruppe
: Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

  Die Standardpaketgruppe für das IBM Spectrum Protect-Paket ist `IBM Installation Manager`.

Repository
: Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

  Das IBM Spectrum Protect-Paket wird in einem Repository in IBM Fix Central gespeichert.

Verzeichnis für gemeinsam genutzte Ressourcen
: Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

  In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version von IBM Spectrum Protect verwendet werden.

Windows: Arbeitsblätter für Planungsdetails für den Server

Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.

 Windows-BetriebssystemeEinschränkung: Wenn Sie ein FAT- oder FAT32- oder ein NTFS-Dateisystemformat verwenden, können Sie nicht das Stammverzeichnis dieses Systems als Position eines Datenbank- oder Protokollverzeichnisses angeben (FAT = File Allocation Table, NTFS = New Technology File System). Stattdessen müssen Sie mindestens ein Unterverzeichnis in dem Stammverzeichnis erstellen. Dann erstellen Sie die Datenbankverzeichnisse und Protokollverzeichnisse in den Unterverzeichnissen.

Element	Erforderlicher Speicherbereich	Anzahl der Verzeichnisse	Position der Verzeichnisse
Die Datenbank			
Aktive Protokolldatei			

Element	Erforderlicher Speicherbereich	Anzahl der Verzeichnisse	Position der Verzeichnisse
Archivprotokoll			
Optional: Protokollspiegel für die aktive Protokolldatei			
Optional: Sekundäres Archivprotokoll (Übernahmeverzeichnis für Archivprotokolle)			

Element	Namen und Benutzer-IDs	Position
Die *Instanzbenutzer-ID* für den Server. Mit dieser ID starten Sie den IBM Spectrum Protect-Server und führen ihn aus.		
Das *Ausgangsverzeichnis* des Servers. In diesem Verzeichnis befindet sich die Instanzbenutzer-ID.		
Der Datenbankinstanzname		
Das *Instanzverzeichnis* für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien).		
Der Servername; verwenden Sie einen eindeutigen Namen für jeden Server.		

Windows: Kapazitätsplanung

Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen. Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.

- Windows: Speicherbedarf für die Datenbank schätzen
  Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.
- Windows: Speicherplatzbedarf für das Wiederherstellungsprotokoll
  In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.
- Windows: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen
  Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.
- Windows: Rollbackdateien der Installation löschen
  Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

Windows: Speicherbedarf für die Datenbank schätzen

Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.

Informationen zu diesem Vorgang

Anfänglich sollte mindestens 25 GB Speicherplatz in der Datenbank verwendet werden. Stellen Sie entsprechend Speicherplatz im Dateisystem bereit. Eine Datenbankgröße von 25 GB ist für eine Testumgebung oder eine Umgebung, die nur einen Speicherarchivmanager umfasst, ausreichend. Für einen Produktionsserver, der Clientlasten unterstützt, sollte die Datenbank größer sein. Wenn Sie Plattenspeicherpools (DISK) mit wahlfreiem Zugriff verwenden, ist mehr Datenbank- und Protokollspeicherbereich erforderlich als für Speicherpools mit sequenziellem Zugriff.

Die maximale Größe der IBM Spectrum Protect-Datenbank beträgt 6 TB.

Informationen zur Festlegung der Größe einer Datenbank in einer Produktionsumgebung, die auf der Anzahl Dateien und der Speicherpoolgröße basiert, enthalten die folgenden Abschnitte.

- Windows: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen
  Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.
- Windows: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen
  Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz kapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.
- Windows: Datenbankmanager und temporärer Speicherbereich
  Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systemspeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

Windows: Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen

Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.

Informationen zu diesem Vorgang

Um den Speicherbedarf auf der Basis der maximalen Anzahl Dateien im Serverspeicher zu schätzen, verwenden Sie die folgenden Richtlinien:

- 600-1000 Byte für jede gespeicherte Version einer Datei einschließlich der Imagesicherungen.
  Einschränkung: Diese Richtlinie umfasst nicht den Speicherplatz, der während der Datendeduplizierung verwendet wird.
- 100-200 Byte für jede Datei im Cache, jede Kopienspeicherpooldatei, jede Datei im Pool für aktive Daten und jede dedupizierte Datei.
- Zusätzlicher Speicherbereich ist für die Datenbankoptimierung erforderlich, um variable Datenzugriffsmuster und die Server-Back-End-Verarbeitung von Daten zu unterstützen. Die Größe des zusätzlichen Speicherplatzes entspricht 50 % der Schätzung für die Gesamtanzahl Byte für Dateiobjekte.

In dem folgenden Beispiel für einen einzelnen Client basieren bei Berechnungen auf den Maximalwerten in den vorhergehenden Richtlinien. Bei den Beispielen wird die mögliche Verwendung der Dateiaggregation nicht berücksichtigt. Im Allgemeinen wird durch das Aggregieren kleiner Dateien der erforderliche Speicherplatz in der Datenbank reduziert. Die Dateiaggregation betrifft keine speicherverwalteten Dateien.

Vorgehensweise

1. Berechnen Sie die Anzahl Dateiversionen. Addieren Sie alle folgenden Werte, um die Anzahl Dateiversionen zu erhalten:
   a. Berechnen Sie die Anzahl gesicherter Dateien. Beispiel: Möglicherweise werden bis zu 500.000 Clientdateien gleichzeitig gesichert. In diesem Beispiel sind die Speichermaßnahmen so definiert, dass maximal drei Kopien gesicherter Dateien aufbewahrt werden:

      ```
      500.000 Dateien * 3 Kopien = 1.500.000 Dateien
      ```

   b. Berechnen Sie die Anzahl Archivierungsdateien. Beispiel: Bis zu 100.000 Clientdateien können archivierte Kopien sein.
   c. Berechnen Sie die Anzahl speicherverwalteter Dateien. Beispiel: Bis zu 200.000 Clientdateien können von Client-Workstations umgelagert werden.

   Bei Verwendung von 1000 Byte pro Datei beträgt der Gesamtspeicherplatz in der Datenbank, der für die zu dem Client gehörigen Dateien erforderlich ist, 1,8 GB:

   ```
   (1.500.000 + 100.000 + 200.000) * 1000 = 1,8 GB
   ```

2. Berechnen Sie die Anzahl Dateien im Cache, Kopienspeicherpooldateien, Dateien im Pool für aktive Daten und dedupizierter Dateien:
   a. Berechnen Sie die Anzahl der Cachekopien. Beispiel: In einem Plattenspeicherpool mit 5 GB Kapazität ist Caching aktiviert. Die obere Umlagerungsschwelle des Pools ist 90 % und die untere Umlagerungsschwelle ist 70 %. Das heißt 20 % des Plattenpools (oder 1 GB) wird von Cachedateien belegt.
      Wenn die durchschnittliche Dateigröße ungefähr 10 KB beträgt, enthält der Cache zu jedem beliebigen Zeitpunkt etwa 100.000 Dateien:

      ```
      100.000 Dateien * 200 Byte = 19 MB
      ```

   b. Berechnen Sie die Anzahl Kopienspeicherpooldateien. Alle primären Speicherpools werden im Kopienspeicherpool gesichert:

      ```
      (1.500.000 + 100.000 + 200.000) * 200 Byte = 343 MB
      ```

   c. Berechnen Sie die Anzahl Dateien im Speicherpool für aktive Daten. Alle aktiven Clientsicherungsdaten in primären Speicherpools werden in den Speicherpool für aktive Daten kopiert. Angenommen, es sind 500.000 Versionen der 1.500.000 Sicherungsdateien im primären Speicherpool aktiv:

      ```
      500.000 * 200 Byte = 95 MB
      ```

d. Berechnen Sie die Anzahl deduplizierter Dateien. Angenommen, ein deduplizierter Speicherpool enthält 50.000 Dateien:

```
50.000 * 200 Byte = 10 MB
```

Auf der Basis der vorhergehenden Berechnungen sind etwa 0,5 GB zusätzlicher Speicherplatz in der Datenbank für die Cachedateien, die Kopienspeicherpooldateien, die Dateien im Pool für aktive Daten und die deduplizierten Dateien des Clients erforderlich.

3. Berechnen Sie den zusätzlichen Speicherplatz, der für die Datenbankoptimierung benötigt wird. Um optimalen Datenzugriff und optimale Verwaltung durch den Server bereitzustellen, ist zusätzlicher Speicherplatz in der Datenbank erforderlich. Die Größe des zusätzlichen Speicherplatzes in der Datenbank beträgt 50 % des Gesamtspeicherbedarfs für Dateiobjekte.

   ```
   (1,8 + 0,5) * 50 % = 1,2 GB
   ```

4. Die Gesamtgröße des für den Client erforderlichen Datenbankspeicherbereichs berechnen. Die Gesamtgröße beträgt ca. 3,5 GB:

   ```
   1,8 + 0,5 + 1,2 = 3,5 GB
   ```

5. Berechnen Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist. Wenn der Client, der in den vorhergehenden Berechnungen verwendet wurde, ein typischer Client ist und Sie beispielsweise über 500 Clients verfügen, können Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist, mithilfe der folgenden Berechnung schätzen:

   ```
   500 * 3,5 = 1,7 TB
   ```

Ergebnisse

Tipp: In den Beispielen oben handelt es sich bei den Ergebnissen um Schätzungen. Die tatsächliche Größe der Datenbank kann aufgrund von Faktoren wie beispielsweise der Anzahl Verzeichnisse und der Länge der Pfad- und Dateinamen von der geschätzten Größe abweichen. Sie sollten die Datenbank regelmäßig überwachen und die Größe wie erforderlich anpassen.

Nächste Schritte

Während des normalen Betriebs erfordert der IBM Spectrum Protect-Server möglicherweise temporären Speicherplatz in der Datenbank. Dieser Speicherplatz wird aus den folgenden Gründen benötigt:

- Zum Speichern der Ergebnisse der Sortierung oder Änderung der Reihenfolge, die noch nicht in der Datenbank aufbewahrt und in der Datenbank nicht unmittelbar optimiert werden. Die Ergebnisse werden vorübergehend in der Datenbank zur Verarbeitung gespeichert.
- Zum Erteilen des Verwaltungszugriffs auf die Datenbank über eine der folgenden Methoden:
  - Ein DB2-ODBC-Client (ODBC = Open Database Connectivity)
  - Ein Oracle-JDBC-Client (JDBC = Java™ Database Connectivity)
  - SQL (Structured Query Language) für den Server über die Befehlszeile eines Verwaltungsclients

Erwägen Sie die Verwendung von zusätzlichen 50 GB an temporärem Speicherplatz pro 500 GB Speicherbereich für Dateiobjekte und Optimierung. Siehe die Richtlinien in der folgenden Tabelle. In dem Beispiel, das im vorhergehenden Schritt verwendet wurde, sind insgesamt 1,7 TB Speicherplatz in der Datenbank für Dateiobjekte und die Optimierung für 500 Clients erforderlich. Auf der Basis dieser Berechnung sind 200 GB für temporären Speicherplatz erforderlich. Der erforderliche Gesamtspeicherplatz in der Datenbank beträgt 1,9 TB.

Datenbankgröße	Mindestens erforderlicher temporärer Speicherplatz
< 500 GB	50 GB
≥ 500 GB und < 1 TB	100 GB
≥ 1 TB und < 1,5 TB	150 GB
≥ 1,5 und < 2 TB	200 GB
≥ 2 und < 3 TB	250-300 GB
≥ 3 und < 4 TB	350-400 GB

Windows: Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen

Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz kapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.

Windows: Datenbankmanager und temporärer Speicherbereich

Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systemspeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

Der Datenbankmanager sortiert Daten in einer bestimmten Reihenfolge, gemäß der SQL-Anweisung, mit der Sie die Daten anfordern. Je nach Auslastung des Servers und wenn es mehr Daten gibt, als der Datenbankmanager verwalten kann, werden die (der Reihenfolge nach sortierten) Daten temporärem Plattenspeicher zugeordnet. Daten werden temporärem Plattenspeicher zugeordnet, wenn die Ergebnismenge sehr umfangreich ist. Der Datenbankmanager verwaltet den verwendeten Speicher dynamisch, wenn Daten temporärem Plattenspeicher zugeordnet werden.

Bei der Verfallsverarbeitung kann beispielsweise eine umfangreiche Ergebnismenge generiert werden. Wenn der Systemspeicher in der Datenbank zur Speicherung der Ergebnismenge nicht ausreicht, wird ein Teil der Daten temporärem Plattenspeicher zugeordnet. Wenn während der Verfallsverarbeitung ein Knoten oder ein Dateibereich ausgewählt wird, der für die Verarbeitung zu groß ist, kann der Datenbankmanager die Daten im Speicher nicht sortieren. Der Datenbankmanager muss temporären Speicherbereich zum Sortieren der Daten verwenden.

Bei der Ausführung von Datenbankoperationen sollten Sie in den folgenden Szenarios eine Erweiterung des Speicherplatzes in der Datenbank vornehmen:

- Der Speicherbereich der Datenbank ist klein und die Serveroperation, die temporären Speicherbereich benötigt, belegt den verbleibenden freien Speicherbereich.
- Die Dateibereiche sind groß oder den Dateibereichen ist eine Maßnahme zugeordnet, durch die viele Dateiversionen erstellt werden.
- Der IBM Spectrum Protect-Server muss mit begrenztem Speicher ausgeführt werden. Die Datenbank verwendet den Hauptspeicher des IBM Spectrum Protect-Servers für Datenbankoperationen. Ist der verfügbare Speicher jedoch nicht ausreichend, ordnet der IBM Spectrum Protect-Server der Datenbank temporären Speicherbereich auf Platte zu. Wenn beispielsweise 10G Speicher zur Verfügung stehen und Datenbankoperationen 12G Speicher benötigen, verwendet die Datenbank temporären Speicherbereich.
- Bei der Implementierung eines IBM Spectrum Protect-Servers wird ein Fehler aufgrund fehlenden Datenbankspeicherbereichs (`out of database space`) angezeigt. Überwachen Sie das Serveraktivitätenprotokoll auf Nachrichten, die sich auf den Datenbankspeicherbereich beziehen.

Wichtig: Sie dürfen die DB2-Software, die mit IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht verändern. Führen Sie keine Installation bzw. kein Upgrade auf eine andere Version, ein anderes Release oder ein anderes Fixpack der DB2-Software durch, um eine Beschädigung der Datenbank zu vermeiden.

Windows: Speicherplatzbedarf für das Wiederherstellungsprotokoll

In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.

- Windows: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll
  Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.
- Windows: Speicherbereich des Spiegels für aktive Protokolldateien
  Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.
- Windows: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle
  Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

Windows: Speicherbereich für die aktive Protokolldatei und das Archivprotokoll

Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.

In IBM Spectrum Protect-Servern der Version 7.1 und höher kann die aktive Protokolldatei eine maximale Größe von 512 GB haben. Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist.

Berücksichtigen Sie bei der Schätzung der Größe der aktiven Protokolldatei die folgenden allgemeinen Richtlinien:

- Die empfohlene Anfangsgröße für die aktive Protokolldatei ist 16 GB.
- Stellen Sie sicher, das die aktive Protokolldatei mindestens groß genug ist, um die gleichzeitig ablaufende Aktivität handhaben zu können, die der Server in der Regel handhabt. Versuchen Sie als Vorsichtsmaßnahme das größte Arbeitsvolumen zu schätzen, das der Server jeweils handhabt. Stellen Sie für die aktive Protokolldatei zusätzlichen Speicherbereich bereit, der, falls erforderlich, verwendet werden kann. Ziehen Sie 20 % zusätzlichen Speicherbereich in Betracht.
- Überwachen Sie den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei. Passen Sie die Größe der aktiven Protokolldatei wie erforderlich abhängig von Faktoren wie Clientaktivität und Ebene der Serveroperationen an.
- Stellen Sie sicher, dass das Verzeichnis, das die aktive Protokolldatei enthält, mindestens genauso groß wie die aktive Protokolldatei ist. Ein Verzeichnis, das größer als die aktive Protokolldatei ist, kann Übernahmesituationen handhaben, sollten diese auftreten.
- Stellen Sie sicher, dass das Dateisystem, das das Verzeichnis für aktive Protokolldateien enthält, über mindestens 8 GB freien Speicherbereich für Anforderungen zum Versetzen temporärer Protokolle verfügt.

Die vorgeschlagene Anfangsgröße für das Archivprotokoll beträgt 48 GB.

Das Archivprotokollverzeichnis muss groß genug sein, um die Protokolldateien aufnehmen zu können, die seit der vorherigen Gesamtsicherung generiert wurden. Wenn Sie beispielsweise täglich eine Gesamtsicherung der Datenbank ausführen, muss das Archivprotokollverzeichnis groß genug sein, um die Protokolldateien für die gesamte Clientaktivität aufnehmen zu können, die während 24 Stunden stattfindet. Um Speicherbereich wiederherzustellen, löscht der Server veraltete Archivprotokolldateien nach einer Gesamtsicherung der Datenbank. Wenn das Archivprotokollverzeichnis voll wird und kein Verzeichnis für Archivübernahmeprotokolle vorhanden ist, verbleiben Protokolldateien im Verzeichnis für aktive Protokolldateien. Diese Bedingung kann zur Folge haben, dass das Verzeichnis für aktive Protokolldateien vollständig gefüllt und der Server gestoppt wird. Bei einem Serverneustart wird ein Teil des vorhandenen Speicherbereichs für die aktive Protokolldatei freigegeben wird.

Nach der Installation des Servers können Sie die Archivprotokollauslastung und den Speicherbereich im Archivprotokollverzeichnis überwachen. Wenn sich der Speicherbereich im Archivprotokollverzeichnis füllt, können die folgenden Probleme auftreten:

- Der Server kann keine Datenbankgesamtsicherungen ausführen. Untersuchen und beheben Sie dieses Problem.
- Andere Anwendungen schreiben in das Archivprotokollverzeichnis und belegen den für das Archivprotokoll erforderlichen Speicherbereich. Nutzen Sie den Speicherbereich für das Archivprotokoll nicht gemeinsam mit anderen Anwendungen, einschließlich anderer IBM Spectrum Protect-Server. Stellen Sie sicher, dass jeder Server über eine separate Speicherposition verfügt, dessen Eigner dieser spezifische Server ist und der von diesem spezifischen Server verwaltet wird.

- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen
  Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen
  Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen
  Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen
  Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datendeduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen
  Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.
- Windows: Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen
  Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.
- Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Datendeduplizierungsoperationen schätzen
  Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen

Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen zu bestimmen, führen Sie die folgende Berechnung aus:

```
Anzahl Clients  x  In jeder Transaktion gespeicherte Dateien
  x  Für jede Datei benötigter Protokollspeicherbereich
```

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Grundlegende Clientspeicheroperationen

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.

Element	Beispielwerte	Beschreibung
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3053 Byte	Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	19,5 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 Byte = 3,5 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		
		`3,5 + 16 = 19,5 GB`

Archivprotokoll: vorgeschlagene Größe	58,5 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen.
		
		`3,5 x 3 = 10,5 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		
		`10,5 + 48 = 58,5 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen

Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, zu bestimmen, führen Sie die folgende Berechnung aus:

```
Anzahl Clients x Anzahl Sitzungen pro Client x Anzahl während
  jeder Transaktion gespeicherter Dateien x pro Datei erforderlicher
  Protokollspeicherbereich
```

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Mehrere Clientsitzungen

Element	Beispielwerte		Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	1000	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Mögliche Sitzungen für jeden Client	3	3	Die Einstellung der Clientoption RESOURCEUTILIZATION ist größer als der Standardwert. Jede Clientsitzung führt maximal drei Sitzungen parallel aus.

Element	Beispielwerte		Beschreibung
Anzahl während jeder Transaktion gespeicherter Dateien	4096	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3053	3053	Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	26,5 GB [1]	51 GB [1]	Die folgende Berechnung wurde für 300 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.
			
			`(300 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 10,5 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`10,5 + 16 = 26,5 GB`
			
			Die folgende Berechnung wurde für 1000 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.
			
			`(1000 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 35 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`35 + 16 = 51 GB`

Archivprotokoll: vorgeschlagene Größe	79,5 GB [1]	153 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, wird die Schätzung für die aktive Protokolldatei mit 3 multipliziert:
			
			`10,5 x 3 = 31,5 GB`
			
			`35 x 3 = 105 GB`
			
			Erhöhen Sie diese Werte um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`31,5 + 48 = 79,5 GB`
			
			`105 + 48 = 153 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre aktive Protokolldatei und passen Sie die Größe, falls erforderlich, an.

Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen

Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.

Der Protokollspeicherbereich, der für jede Datei erforderlich ist, erhöht sich um ungefähr 200 Byte für jeden Kopienspeicherpool, der für eine Operation für gleichzeitiges Schreiben verwendet wird. In dem Beispiel in der folgenden Tabelle werden Daten in einem primären Speicherpool und darüber hinaus in zwei Kopienspeicherpools gespeichert. Die geschätzte Protokollgröße erhöht sich für jede Datei um 400 Byte. Wenn Sie den vorgeschlagenen Wert von 3053 Byte Protokollspeicherbereich pro Datei verwenden, sind insgesamt 3453 Byte erforderlich.

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 1. Operationen für gleichzeitiges Schreiben

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3453 Byte	3053 Byte plus 200 Byte für jeden Kopienspeicherpool. Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	20 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		
		`4 + 16 = 20 GB`

Archivprotokoll: vorgeschlagene Größe	60 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Speicherbedarf für das Archivprotokoll zu schätzen:
		
		`4 GB x 3 = 12 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		
		`12 + 48 = 60 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen

Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datendeduplizierung, Wiederherstellung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.

Beispielsweise wird bei der Umlagerung von Dateien aus dem Speicherpool mit wahlfreiem Zugriff (DISK) in einem Plattenspeicherpool mit sequenziellem Zugriff (FILE) für jede Datei, die umgelagert wird, ungefähr 110 Byte Protokollspeicherbereich verwendet. Beispiel: Angenommen, es sind 300 Clients für Sichern/Archivieren vorhanden, von denen jeder 100.000 Dateien jede Nacht sichert. Die Dateien sind anfänglich in einem DISK-Speicherpool gespeichert und werden dann in einen FILE-Speicherpool umgelagert. Um die Größe des Speicherbereichs für die aktive Protokolldatei zu schätzen, die für die Datenumlagerung erforderlich ist, verwenden Sie die folgende Berechnung. Die Anzahl Clients in der Berechnung stellt die maximale Anzahl zu einem beliebigen Zeitpunkt dar, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern.

```
300 Clients x 100.000 Dateien pro Client x 110 Byte = 3,1 GB
```

Addieren Sie diesen Wert zu der Schätzung für die Größe der aktiven Protokolldatei, die für grundlegende Clientspeicheroperationen berechnet wurde.

Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen

Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.

Windows: Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen

Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.

Wenn beispielsweise einmal pro Woche eine Datenbankgesamtsicherung ausgeführt wird, muss der Speicherbereich für das Archivprotokoll groß genug sein, um die Informationen einer vollständigen Woche im Archivprotokoll aufnehmen zu können.

Die unterschiedliche Größe des Archivprotokolls für täglich ausgeführte Datenbankgesamtsicherungen wird in dem Beispiel in der folgenden Tabelle gezeigt.

Tabelle 1. Datenbankgesamtsicherungen

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3453 Byte	3053 Byte für jede Datei plus 200 Byte für jeden Kopienspeicherpool. Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	20 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		
		`4 + 16 = 20 GB`

Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Tag	60 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Sicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen:
		
		`4 GB x 3 = 12 GB`
		
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		
		`12 + 48 = 60 GB`

Element	Beispielwerte	Beschreibung

Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Woche	132 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen. Multiplizieren Sie das Ergebnis mit der Anzahl Tage, die zwischen Datenbankgesamtsicherungen liegen.
		`(4 GB x 3 ) x 7 = 84 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		`84 + 48 = 132 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Anfangsgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen. Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.		

Windows: Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Datendeduplizierungsoperationen schätzen

Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

Die folgenden Faktoren haben Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll:

Volumen der deduplizierten Daten
: Welche Auswirkungen die Datendeduplizierung auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll hat, ist von dem Prozentsatz an Daten abhängig, der für die Deduplizierung auswählbar ist. Ist der Prozentsatz an Daten, die dedupliziert werden können, relativ hoch, ist mehr Protokollspeicherbereich erforderlich.

Größe und Anzahl Speicherbereiche
: Für jeden Speicherbereich, der durch einen Prozess zum Identifizieren doppelter Daten identifiziert wird, sind ungefähr 1.500 Byte Speicherbereich für die aktive Protokolldatei erforderlich. Werden beispielsweise 250.000 Speicherbereiche durch einen erkennen identifiziert, beträgt die geschätzte Größe der aktiven Protokolldatei 358 MB:

  ```
  250.000 während jedes Prozesses ermittelte Speicherbereiche x 1.500 Byte
   für jeden Speicherbereich = 358 MB
  ```

  Betrachten Sie das folgende Szenario. 300 Clients für Sichern/Archivieren sichern jede Nacht bis zu 100.000 Dateien. Diese Aktivität hat eine Last von 30.000.000 Dateien zur Folge. Die durchschnittliche Anzahl Speicherbereiche für jede Datei ist 2. Demzufolge beträgt die Gesamtzahl Speicherbereiche 60.000.000 und der Speicherbedarf für das Archivprotokoll 84 GB:

  ```
  60.000.000 Speicherbereiche x 1.500 Byte pro Speicherbereich = 84 GB
  ```

  Ein Prozess zum Identifizieren doppelter Daten wird für Aggregate von Dateien ausgeführt. Ein Aggregat besteht aus Dateien, die in einer bestimmten Transaktion gespeichert sind, wie durch die Serveroption TXNGROUPMAX angegeben. Angenommen, die Serveroption TXNGROUPMAX ist auf den Standardwert 4096 gesetzt. Wenn die durchschnittliche Anzahl Speicherbereiche für jede Datei 2 beträgt, ist die Gesamtzahl Speicherbereiche in jedem Aggregat 8192 und der für die aktive Protokolldatei erforderliche Speicherbedarf 12 MB:

  ```
  8192 Speicherbereiche in jedem Aggregat x 1500 Byte pro Speicherbereich =
     12 MB
  ```

Timing und Anzahl der Prozesse zum Identifizieren doppelter Daten
: Das Timing und die Anzahl Prozesse zum Identifizieren doppelter Daten haben ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei. Bei Verwendung der in dem vorhergehenden Beispiel berechneten Größe der aktiven Protokolldatei von 12 MB beträgt die gleichzeitige Last für die aktive Protokolldatei 120 MB, wenn 10 Prozesse zum Identifizieren doppelter Daten parallel ausgeführt werden:

  ```
  12 MB pro Prozess x 10 Prozesse = 120 MB
  ```

Dateigröße
: Große Dateien, die für die Identifizierung doppelter Daten verarbeitet werden, können ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei haben. Beispiel: Angenommen, ein Client für Sichern/Archivieren sichert ein Dateisystemimage mit einer Größe von 80 GB. Die Anzahl doppelter Speicherbereiche für dieses Objekt kann groß sein, wenn beispielsweise die in das Dateisystemimage eingeschlossenen Dateien mit Teilsicherungen gesichert wurden. Beispiel: Angenommen, ein Dateisystemimage hat 1,2 Millionen doppelte Speicherbereiche. Die 1,2 Millionen Speicherbereiche in dieser großen Datei stellen eine einzige Transaktion für einen Prozess zum Identifizieren doppelter Daten dar. Der Gesamtspeicherbereich in der aktiven Protokolldatei, der für dieses einzelne Objekt erforderlich ist, beträgt 1,7 GB:

```
1.200.000 Speicherbereich x 1.500 Byte pro Speicherbereich = 1,7 GB
```

Wenn andere, kleinere Prozesse zum Identifizieren doppelter Daten zu demselben Zeitpunkt ausgeführt werden wie der Prozess zum Identifizieren doppelter Daten für ein einzelnes großes Objekt, ist in der aktiven Protokolldatei möglicherweise nicht genügend Speicherbereich verfügbar. Beispiel: Angenommen, ein Speicherpool ist für die Deduplizierung aktiviert. Der Speicherpool enthält gemischte Daten, einschließlich vieler relativ kleiner Dateien mit einer Größe von 10 KB bis zu mehreren hundert KB. Der Speicherpool enthält außerdem einige wenige große Objekte mit einem hohen Prozentsatz an doppelten Speicherbereichen.

Um nicht nur den Speicherbedarf zu berücksichtigen, sondern auch das Timing und die Dauer gleichzeitig ablaufender Transaktionen, erhöhen Sie die geschätzte Größe der aktiven Protokolldatei um den Faktor 2. Beispiel: Angenommen, das Ergebnis Ihrer Berechnungen für den Speicherbedarf lautet 25 GB (23,3 GB + 1,7 GB für die Deduplizierung eines großen Objekts). Wenn Deduplizierungsverarbeitung gleichzeitig ausgeführt werden, beträgt die vorgeschlagene Größe der aktiven Protokolldatei 50 GB. Die vorgeschlagene Größe des Archivprotokolls ist 150 GB.

Die Beispiele in den folgenden Tabellen zeigen Berechnungen für aktive Protokolldateien und Archivprotokolle. In dem Beispiel in der ersten Tabelle wird eine durchschnittliche Größe von 700 KB für Speicherbereiche verwendet. In dem Beispiel in der zweiten Tabelle wird eine durchschnittliche Größe von 256 KB verwendet. Wie den Beispielen zu entnehmen ist, zeigt die durchschnittliche Größe doppelter Speicherbereiche von 256 KB eine größere geschätzte Größe für die aktive Protokolldatei an. Um betriebsbezogene Probleme für den Server auf ein Mindestmaß reduzieren oder zu verhindern, verwenden Sie 256 KB für die Schätzung der Größe der aktiven Protokolldatei in Ihrer Produktionsumgebung.

Tabelle 1. Durchschnittliche Größe doppelter Speicherbereiche von 700 KB

Element	**Beispielwerte**		**Beschreibung**
Größe des größten zu deduplizierenden Objekts	800 GB	4 TB	Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.
Durchschnittliche Größe der Speicherbereiche	700 KB	700 KB	Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.
Speicherbereiche für eine bestimmte Datei	1.198.372 Bit	6.135.667 Bit	Bei Verwendung der durchschnittlichen Speicherbereichsgröße (700 KB), geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an. Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt: `(800 GB ÷ 700 KB) = 1.198.372 Bit` Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt: `(4 TB ÷ 700 KB) = 6.135.667 Bit`
Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist	1,7 GB	8,6 GB	Der geschätzte Speicherbereich für die aktive Protokolldatei, der für diese Transaktion benötigt wird.

Element	Beispielwerte		Beschreibung

Aktive Protokolldatei: vorgeschlagene Gesamtgröße	66 GB [1]	79,8 GB [1]	Multiplizieren Sie, nachdem zusätzlich zur Deduplizierung andere Aspekte der Last auf dem Server berücksichtigt wurden, die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`(23,3 GB + 1,7 GB) x 2 = 50 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`50 + 16 = 66 GB`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`(23,3 GB + 8,6 GB) x 2 = 63,8 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`63,8 + 16 = 79,8 GB`

Archivprotokoll: vorgeschlagene Größe	198 GB [1]	239,4 GB [1]	Multiplizieren Sie die geschätzte Größe der aktiven Protokolldatei mit dem Faktor 3.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`50 GB x 3 = 150 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`150 + 48 = 198 GB`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`63,8 GB x 3 = 191,4 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`191,4 + 48 = 239,4 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen. Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.			

Tabelle 2. Durchschnittliche Größe doppelter Speicherbereiche von 256 KB

Element	Beispielwerte		Beschreibung
Größe des größten zu deduplizierenden Objekts	800 GB	4 TB	Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.

Element	Beispielwerte		Beschreibung
Durchschnittliche Größe der Speicherbereiche	256 KB	256 KB	Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.

Speicherbereiche für eine bestimmte Datei	3.276.800 Bit	16.777.216 Bit	Bei Verwendung der durchschnittlichen Speicherbereichsgröße, geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`(800 GB ÷ 256 KB) = 3.276.800 Bit`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`(4 TB ÷ 256 KB) = 16.777.216 Bit`

Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist	4,5 GB	23,4 GB	Die geschätzte Größe des Speicherbereichs für die aktive Protokolldatei, die für diese Transaktion erforderlich ist.

Aktive Protokolldatei: vorgeschlagene Gesamtgröße	71,6 GB [1]	109,4 GB [1]	Nachdem Sie neben der Deduplizierung andere Aspekte der Serverauslastung mit berücksichtigt haben, multiplizieren Sie die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`(23,3 GB + 4,5 GB) x 2 = 55,6 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`55,6 + 16 = 71,6 GB`
			
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			
			`(23,3 GB + 23,4 GB) x 2 = 93,4 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			
			`93,4 + 16 = 109,4 GB`

Element	Beispielwerte		Beschreibung

Archivprotokoll: vorgeschlagene Größe	214,8 GB [1]	328,2 GB [1]	Die geschätzte Größe der aktiven Protokolldatei multipliziert mit dem Faktor 3.
			
			Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt:
			
			`55,6 GB x 3 = 166,8 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`166,8 + 48 = 214,8 GB`
			
			Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt:
			
			`93,4 GB x 3 = 280,2 GB`
			
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			
			`280,2 + 48 = 328,2 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Windows: Speicherbereich des Spiegels für aktive Protokolldateien

Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.

Die Erstellung einer Protokollspiegel ist eine vorgeschlagene Option. Wenn Sie die aktive Protokolldatei vergrößern, wird der Protokollspiegel automatisch vergrößert. Die Spiegelung des Protokolls kann sich negativ auf die Leistung auswirken, da die doppelte E/A-Aktivität erforderlich ist, um den Spiegel zu verwalten. Der zusätzliche Speicherbereich, den der Protokollspiegel benötigt, ist ein weiterer Faktor, der bei der Entscheidung über die Erstellung eines Protokollspiegels berücksichtigt werden muss.

Wenn das Spiegelprotokollverzeichnis voll wird, gibt der Server Fehlernachrichten in das Aktivitätenprotokoll und in die Datei db2diag.log aus. Die Serveraktivität wird fortgesetzt.

Windows: Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle

Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

Durch Angabe eines Übernahmeverzeichnisses für Archivprotokolle können Probleme verhindert werden, die auftreten, wenn der Speicherbereich der Archivprotokolldatei nicht mehr ausreicht. Wenn sowohl das Verzeichnis für Archivprotokolle als auch das Laufwerk oder das Dateisystem, in dem sich das Übernahmeverzeichnis für Archivprotokolle befindet, voll wird, bleiben die Daten im Verzeichnis für aktive Protokolldateien. Dadurch kann die aktive Protokolldatei vollständig ausgefüllt werden, was einen Serverhalt verursacht.

Windows: Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen

Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl QUERY LOG ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.

Aktive Protokolldatei

Wenn der verfügbare Speicherbereich für die aktive Protokolldatei zu gering ist, werden die folgenden Nachrichten im Aktivitätenprotokoll angezeigt:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER

Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Der IBM Spectrum Protect-Server startet eine Datenbankgesamtsicherung.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dsmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Sie müssen die Datenbank manuell sichern.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei dsmserv.opt und geben Sie für die Option ACTIVELOGSIZE einen neuen Wert an. Starten Sie anschließend den Server erneut.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Wenn mindestens eine einzige Datenbankgesamtsicherung ausgeführt wurde, startet der IBM Spectrum Protect-Server eine Teilsicherung der Datenbank. Andernfalls startet der Server eine Datenbankgesamtsicherung.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Sie müssen die Datenbank manuell sichern.

Archivprotokoll

Wenn der verfügbare Speicherbereich für das Archivprotokoll zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
Das Verhältnis des belegten Speicherbereichs für das Archivprotokoll zum verfügbaren Speicherbereich für das Archivprotokoll überschreitet den Schwellenwert für die Protokollauslastung. Der IBM Spectrum Protect-Server startet eine automatische Datenbankgesamtsicherung.

Datenbank

Wenn der verfügbare Speicherbereich für Datenbankaktivitäten zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
Der belegte Speicherplatz in der Datenbank überschreitet den Schwellenwert für die Belegung des Speicherplatzes in der Datenbank. Um den Speicherplatz für die Datenbank zu vergrößern, verwenden Sie den Befehl EXTEND DBSPACE oder das Dienstprogramm DSMSERV FORMAT mit dem Parameter DBDIR.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB
Der verfügbare Speicherbereich in dem Verzeichnis, in dem sich die Serverdatenbankdateien befinden, beträgt weniger als 1 GB.

Wenn ein IBM Spectrum Protect-Server mit dem Dienstprogramm DSMSERV FORMAT oder dem Konfigurationsassistenten erstellt wird, werden auch eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien erstellt, in denen Datenbankinformationen gespeichert werden sollen, die vom Datenbankmanager verwendet werden. Der in dieser Nachricht angegebene Pfad gibt die Speicherposition der Datenbankinformationen an, die vom Datenbankmanager verwendet werden. Ist in dem Pfad kein Speicherbereich verfügbar, ist der Server nicht mehr funktionsfähig.

Sie müssen dem Dateisystem Speicherbereich hinzufügen oder in dem Dateisystem oder auf der Platte Speicherbereich freigeben.

Windows: Rollbackdateien der Installation löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

Informationen zu diesem Vorgang

Zum Löschen der nicht mehr benötigten Dateien verwenden Sie den grafisch orientierten Installationsassistenten oder die Befehlszeile im Konsolenmodus.

- Windows: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen
  Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.
- Windows: Rollbackdateien für die Installation mit der Befehlszeile löschen
  Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

Windows: Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM® Installation Manager-Benutzerschnittstelle löschen.

Vorgehensweise

1. Öffnen Sie IBM Installation Manager.
2. Klicken Sie auf Datei > Benutzervorgaben.
3. Wählen Sie Dateien für Rollback aus.
4. Klicken Sie auf Gespeicherte Dateien löschen und dann auf OK.

Windows: Rollbackdateien für die Installation mit der Befehlszeile löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

Vorgehensweise

1. In dem Verzeichnis, in dem IBM® Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
   -  Windows-Betriebssystemeeclipse\tools

   Beispiel:

   -  Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\eclipse\tools
2. Geben Sie im Verzeichnis tools den folgenden Befehl aus, um eine IBM Installation Manager-Befehlszeile zu starten:
   -  Windows-Betriebssystemeimcl.exe -c
3. Geben Sie `P` ein, um Benutzervorgaben auszuwählen.
4. Geben Sie `3` ein, um Dateien für Rollback auszuwählen.
5. Geben Sie `D` ein, um die Dateien für Rollback zu löschen.
6. Geben Sie `A` ein, um die Änderungen anzuwenden und zum Benutzervorgabenmenü zurückzukehren.
7. Geben Sie `C` ein, um das Benutzervorgabenmenü zu verlassen.
8. Geben Sie `X` ein, um Installation Manager zu beenden.

Windows: Empfehlungen für die Serverbenennung

Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.

Instanzbenutzer-ID

Die Instanzbenutzer-ID wird als Basis für andere Namen verwendet, die sich auf die Serverinstanz beziehen. Die Instanzbenutzer-ID wird auch als Instanzeigner bezeichnet.

Zum Beispiel: tsminst1

Die Instanzbenutzer-ID ist die Benutzer-ID, die über das Eigentumsrecht oder über Schreib-/Lesezugriffsberechtigung für alle Verzeichnisse verfügen muss, die Sie für die Datenbank und das Wiederherstellungsprotokoll erstellen. Der Server wird standardmäßig mit der Instanzbenutzer-ID ausgeführt. Diese Benutzer-ID benötigt außerdem Schreib-/Lesezugriff für die Verzeichnisse, die für die Einheitenklasse FILE verwendet werden.

 Windows-Betriebssysteme

Datenbankinstanzname

Der Datenbankinstanzname ist der Name der Serverinstanz in der Registrierung.

Zum Beispiel: Server1

 Windows-Betriebssysteme

Instanzverzeichnis

Das Instanzverzeichnis enthält spezielle Dateien für eine Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). Es kann einen beliebigen Name haben. Um die Identifizierung zu erleichtern, sollten Sie einen Namen verwenden, der das Verzeichnis mit dem Instanznamen verknüpft.

Sie können einen Namen verwenden, der den Namen der Serverinstanz enthält, der in der Registrierung angezeigt wird. Standardnamen für die Serverinstanz haben das Format **Server*x***.

Zum Beispiel: C:\tsm\server1

Im Instanzverzeichnis sind folgende Dateien für die Serverinstanz gespeichert:

- Serveroptionsdatei dsmserv.opt
- Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
- Einheitenkonfigurationsdatei, wenn die Serveroption DEVCONFIG keinen vollständig qualifizierten Namen angibt
- Protokolldatei für Datenträger, wenn die Serveroption VOLUMEHISTORY keinen vollständig qualifizierten Namen angibt
- Datenträger für Speicherpools mit dem Typ DEVTYPE=FILE, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
- Benutzerexits
- Traceausgabe (wenn nicht vollständig qualifiziert)

Datenbankname

Der Datenbankname lautet für jede Serverinstanz immer TSMDB1. Dieser Name kann nicht geändert werden.

Servername

Der Servername ist ein interner Name für IBM Spectrum Protect und wird für Operationen verwendet, bei denen eine Datenübertragung zwischen mehreren IBM Spectrum Protect-Servern auftritt. Zum Beispiel bei der Kommunikation zwischen Servern und bei der gemeinsamen Nutzung von Speicherarchiven.

 Der Servername wird auch verwendet, wenn Sie den Server dem Operations Center hinzufügen, so dass er mit dieser Schnittstelle verwaltet werden kann. Verwenden Sie einen eindeutigen Namen für jeden Server. Verwenden Sie einen Namen, der die Position oder den Zweck des Servers angibt, um die Identifikation im Operations Center (oder mit einem Befehl QUERY SERVER) zu erleichtern. Nachdem ein IBM Spectrum Protect-Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.

Wenn Sie den Assistenten verwenden, wird als Standardname der Hostname des von Ihnen verwendeten Systems vorgeschlagen. Sie können einen anderen, für Ihre Umgebung aussagekräftigen Namen verwenden. Befinden sich mehrere Server auf dem System, können Sie bei Verwendung des Assistenten den Standardnamen nur für einen der Server angeben. Sie müssen einen eindeutigen Namen für jeden Server eingeben.

 Zum Beispiel:

- `TUCSON_SERVER1`
- `TUCSON_SERVER2`

Verzeichnisse für Datenbankbereich und Wiederherstellungsprotokoll

Die Verzeichnisse können gemäß den lokalen Vorgaben benannt werden. Sie sollten Namen verwenden, die die Verzeichnisse mit der Serverinstanz verknüpfen, um die Identifikation zu erleichtern.

Beispiel für das Archivprotokoll:

-  f:\server1\archlog

Windows: Installationsverzeichnisse

Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, DB2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

Das Verzeichnis /opt/tivoli/tsm/server/bin ist das Standardverzeichnis, das den Servercode und die Lizenzierung enthält.

Das während der Installation des IBM Spectrum Protect-Servers installierte DB2-Produkt hat die in den DB2-Informationsquellen dokumentierte Verzeichnisstruktur. Schützen Sie diese Verzeichnisse und Dateien wie die Serververzeichnisse. Das Standardverzeichnis heißt /opt/tivoli/tsm/db2.

Sie können folgende Sprachen verwenden: Englisch (US), Deutsch, Französisch, Italienisch, Spanisch, Portugiesisch (Brasilien), Koreanisch, Japanisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Chinesisch GBK, Chinesisch Big5 und Russisch.

Windows: Serverkomponenten installieren

Für die Installation der Serverkomponenten der Version 8.1.2 können Sie den Installationsassistenten, die Befehlszeile im Konsolenmodus oder den unbeaufsichtigten Modus verwenden.

Informationen zu diesem Vorgang

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server
  Tipp: Die Datenbank (DB2), Global Security Kit (GSKit) und IBM® Java™ Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.
- Sprachen des Servers
- Lizenz
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

 Für die Installation eines Servers der Version 8.1.2 anhand dieses Leitfadens müssen Sie 15 - 30 Minuten einplanen.

- Windows: Installationspaket abrufen
  Das Installationspaket für IBM Spectrum Protect kann von einer IBM Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.
- Windows: IBM Spectrum Protect mit dem Installationsassistenten installieren
  Sie können den Server mit dem grafisch orientierten Assistenten von IBM Installation Manager installieren.
- Windows: IBM Spectrum Protect im Konsolenmodus installieren
  Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.
- Windows: IBM Spectrum Protect im unbeaufsichtigten Modus installieren
  Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.
- Windows: Sersprachenpakete installieren
  Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

Windows: Installationspaket abrufen

Das Installationspaket für IBM Spectrum Protect kann von einer IBM® Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.

Vorgehensweise

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:
   - Laden Sie das Serverpaket aus Passport Advantage oder Fix Central herunter.
   - Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.
2. Gehen Sie wie folgt vor, wenn Sie das Paket von einer IBM Download-Site heruntergeladen haben:
   
   a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherplatzbedarf finden Sie im Downloaddokument:
      - IBM Spectrum Protect Technote 4042944
      - IBM Spectrum Protect Extended Edition Technote 4042945
      - IBM Spectrum Protect for Data Retention Technote 4042946

   b. Wechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet.
   Wichtig: Im nächsten Schritt werden die Dateien in das aktuelle Verzeichnis extrahiert. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.

   c. Klicken Sie entweder doppelt auf die ausführbare Datei oder geben Sie den folgenden Befehl in die Befehlszeile ein, um die Installationsdateien zu extrahieren. Die Dateien werden in das aktuelle Verzeichnis extrahiert.

   ```
   Paketname.exe
   ```

   Paketname sieht wie in dem folgenden Beispiel aus:*8.1.x.000*-IBM-SPSRV-WindowsX64.exe

3. Wählen Sie eine der folgenden Methoden für die Installation von IBM Spectrum Protect aus:
   - Windows: IBM Spectrum Protect mit dem Installationsassistenten installieren
   - Windows: IBM Spectrum Protect im Konsolenmodus installieren
   - Windows: IBM Spectrum Protect im unbeaufsichtigten Modus installieren
4. Nachdem Sie IBM Spectrum Protect installiert haben und bevor Sie IBM Spectrum Protect für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Support and downloads und legen Sie alle gültigen Fixes an.

Windows: IBM Spectrum Protect mit dem Installationsassistenten installieren

Sie können den Server mit dem grafisch orientierten Assistenten von IBM® Installation Manager installieren.

Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.
- Windows-BetriebssystemeStellen Sie sicher, dass die Benutzer-ID, die Sie während der Installation verwenden wollen, ein Benutzer mit der Berechtigung eines lokalen Administrators ist.

Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

Option	Bezeichnung
Installation der Software mithilfe eines heruntergeladenen Pakets:	a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben. b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten zu starten: Windows-Betriebssysteme `install.bat` Windows-BetriebssystemeSie können auch in dem Verzeichnis, in dem die Installationsdateien extrahiert wurden, doppelt auf die Datei install.bat klicken.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis logs gespeichert werden.

  Installationsprotokolldateien können Sie anzeigen, indem Sie in Installation Manager auf Datei > Protokoll anzeigen klicken. Um diese Protokolldateien zu erfassen, klicken Sie in Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.

- Windows-BetriebssystemeNachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.
- Windows-BetriebssystemeIst unter Windows ein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den nativen Einheitentreiber. Ist unter Windows kein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls `dpinst.exe /a`. Die Datei `dpinst.exe` befindet sich im Verzeichnis des Einheitentreibers. Das Standardverzeichnis ist C:\Programme\Tivoli\TSM\device\drivers.

Windows: IBM Spectrum Protect im Konsolenmodus installieren

Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.

Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.
- Windows-BetriebssystemeStellen Sie sicher, dass die Benutzer-ID, die Sie während der Installation verwenden wollen, ein Benutzer mit der Berechtigung eines lokalen Administrators ist.

Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

Option	Bezeichnung

Option	Bezeichnung
Installation der Software mithilfe eines heruntergeladenen Pakets:	a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben. b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten im Konsolenmodus zu starten: Windows-Betriebssysteme `install.bat -c` Optional : Generieren Sie während einer Installation im Konsolenmodus eine Antwortdatei. Geben Sie die Optionen für die Installation im Konsolenmodus und in der Anzeige Zusammenfassung `G` an, um die Antworten zu generieren.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  - Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
- Windows-BetriebssystemeNachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.
- Windows-BetriebssystemeIst unter Windows ein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den nativen Einheitentreiber. Ist unter Windows kein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls `dpinst.exe /a`. Die Datei `dpinst.exe` befindet sich im Verzeichnis des Einheitentreibers. Das Standardverzeichnis ist C:\Programme\Tivoli\TSM\device\drivers.

Windows: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.

Vorbereitende Schritte

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis input zur Verfügung, in dem das Installationspaket extrahiert wird:

install_response_sample.xml
: Verwenden Sie diese Datei für die Installation der IBM Spectrum Protect-Komponenten.

update_response_sample.xml
: Verwenden Sie diese Datei für das Upgrade der IBM Spectrum Protect-Komponenten.

Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Erstellen Sie eine Antwortdatei. Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.
2. Wenn Sie den Server und das Operations Center im unbeaufsichtigten Modus installieren, erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.
   Wenn Sie die Datei install_response_sample.xml verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist *`mein_Kennwort`* das Kennwort:

   ```
   <variable name='ssl.password' value='mein_Kennwort' />
   ```

   Weitere Informationen zu diesem Kennwort finden Sie in Prüfliste für die Installation.
   Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei update_response_sample.xml aktualisieren.
3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.
   - Windows-Betriebssysteme

     ```
     install.bat -s -input Antwortdatei -acceptLicense
     ```

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM® Installation Manager-Verzeichnis logs gespeichert werden. Zum Beispiel:
  - Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\logs
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf Downloads (fixes and PTFs) und legen Sie alle gültigen Fixes an.
- Windows-BetriebssystemeNachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Die ersten Schritte nach der Installation von IBM Spectrum Protect, um zu erfahren, wie Ihr Server konfiguriert wird.
- Windows-BetriebssystemeIst unter Windows ein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den nativen Einheitentreiber. Ist unter Windows kein nativer Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls `dpinst.exe /a`. Die Datei `dpinst.exe` befindet sich im Verzeichnis des Einheitentreibers. Das Standardverzeichnis ist C:\Programme\Tivoli\TSM\device\drivers.

Windows-Betriebssysteme

Windows: Serversprachenpakete installieren

Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.

Vorbereitende Schritte

Anweisungen zur Installation von von Sprachenpaketen für Speicheragenten finden Sie unter Language pack configuration for Storage Agent.

- Windows: Spracheinstellungen für den Server
  Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.
- Windows: Sprachenpaket konfigurieren
  Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.
- Windows: Sprachenpaket aktualisieren
  Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

Windows: Spracheinstellungen für den Server

Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.

Windows-BetriebssystemeDieses Sprachenpaket wird automatisch für die folgende Standardsprachenoption für Servernachrichten und Hilfetext installiert: LANGUAGE AMENG.

Für vom Standard abweichende Sprachen oder Ländereinstellungen installieren Sie das für Ihre Installation erforderliche Sprachenpaket. Sie können die aufgeführten Sprachen verwenden:
Windows-Betriebssysteme

Tabelle 1. Serversprachen für Windows

Sprache	Wert der Option LANGUAGE
Chinesisch, vereinfacht	chs
Chinesisch, traditionell	cht
Englisch	ameng
Französisch	fra
Deutsch	deu
Italienisch	ita
Japanisch (Shift-JIS)	jpn
Koreanisch	kor
Portugiesisch, Brasilianisches	ptb
Russisch	rus
Spanisch	esp

Windows-BetriebssystemeEinschränkung: Bei Verwendung des Operations Center werden einige Zeichen möglicherweise nicht ordnungsgemäß angezeigt, wenn der Web-Browsers und der Server nicht dieselbe Sprache verwenden. Wenn dieses Problem auftritt, geben Sie im Browser dieselbe Sprache wie im Server an.

Windows: Sprachenpaket konfigurieren

Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.

Informationen zu diesem Vorgang

 Windows-BetriebssystemeGeben Sie in der Option LANGUAGE in der Serveroptionsdatei den Namen der Ländereinstellung an, die verwendet werden soll. Soll beispielsweise die Ländereinstellung `ita` verwendet werden, setzen Sie die Option LANGUAGE auf `ita`. Siehe Windows: Spracheinstellungen für den Server.

Wenn die Ländereinstellung erfolgreich initialisiert wird, steuert sie die Datums-, Uhrzeit- und Zahlenformatierung für den Server. Wenn die Ländereinstellung nicht erfolgreich initialisiert wird, verwendet der Server die englischen (US) Nachrichtendateien und das Datums-, Uhrzeit- und Zahlenformat der englischen (US) Ländereinstellung.

Windows: Sprachenpaket aktualisieren

Sie können ein Sprachenpaket mithilfe von IBM® Installation Manager ändern oder aktualisieren.

Informationen zu diesem Vorgang

Sie können ein anderes Sprachenpaket in derselben IBM Spectrum Protect-Instanz installieren.

- Verwenden Sie die Funktion Ändern von IBM Installation Manager, um ein anderes Sprachenpaket zu installieren.
- Verwenden Sie die Funktion Aktualisieren von IBM Installation Manager, um eine Aktualisierung auf neuere Versionen der Sprachenpakete durchzuführen.

Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.

Windows: Die ersten Schritte nach der Installation von IBM Spectrum Protect

Nach der Installation von Version 8.1.2 bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.

Informationen zu diesem Vorgang

1. Erstellen Sie die Verzeichnisse und die Benutzer-ID für die Serverinstanz. Siehe Windows: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen.
2. Konfigurieren Sie eine Serverinstanz. Wählen Sie eine der folgenden Optionen aus:
   - Verwenden Sie den Konfigurationsassistenten (die bevorzugte Methode). Siehe Windows: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren.
   - Konfigurieren Sie die neue Instanz manuell. Siehe Windows: Serverinstanz manuell konfigurieren. Führen Sie während einer manuellen Konfiguration die folgenden Schritte aus:
     a. Definieren Sie Ihre Verzeichnisse und erstellen Sie die IBM Spectrum Protect-Instanz. Siehe Windows: Serverinstanz erstellen.
     b. Erstellen Sie eine neue Serveroptionsdatei, indem Sie die Musterdatei kopieren, um die Datenübertragung zwischen dem Server und den Clients zu definieren. Siehe  Windows-BetriebssystemeWindows: Server- und Clientübertragung konfigurieren.
     c. Geben Sie den Befehl DSMSERV FORMAT aus, um die Datenbank zu formatieren. Siehe Windows: Datenbank und Protokoll formatieren.
     d. Konfigurieren Sie Ihr System für die Datenbanksicherung. Siehe Windows: Datenbankmanager für die Datenbanksicherung vorbereiten.
3. Konfigurieren Sie Optionen, die die Ausführung der Datenbankreorganisation steuern. Siehe Windows: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren.
4. Starten Sie die Serverinstanz, falls noch nicht gestartet.
   -  Windows-BetriebssystemeSiehe Windows: Serverinstanz auf Windows-Systemen starten.
5. Registrieren Sie Ihre Lizenz. Siehe Windows: Lizenzregistrierung.
6. Bereiten Sie Ihr System auf Datenbanksicherungen vor. Siehe Windows: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben.
7. Überwachen Sie den Server. Siehe Windows: Server überwachen.

- Windows: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen
  Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.
- Windows: IBM Spectrum Protect-Server konfigurieren
  Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.

- Windows: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren
  Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.
- Windows-BetriebssystemeWindows: Serverinstanz auf Windows-Systemen starten
  In einer Produktionsumgebung ist die bevorzugte Methode zum Starten des Servers der Start als Windows-Dienst. In einer Umgebung, in der Sie rekonfigurieren, testen oder Verwaltungstasks ausführen, starten Sie den Server im Vordergrund oder verwenden Sie den Verwaltungsmodus.
- Windows: Server stoppen
  Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.
- Windows: Lizenzregistrierung
  Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.
- Windows: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben
  Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.
- Windows: Mehrere Serverinstanzen auf einem System ausführen
  Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.
- Windows: Server überwachen
  Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

Windows: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen

Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.

Vorbereitende Schritte

Lesen Sie die Informationen zur Planung des Speicherbereichs für den Server, bevor Sie diese Task ausführen. Siehe Windows: Arbeitsblätter für Planungsdetails für den Server.

Vorgehensweise

1. Erstellen Sie die Benutzer-ID, die Eigner der Serverinstanz sein soll. Diese Benutzer-ID verwenden Sie später bei der Erstellung der Serverinstanz.

   Windows-Betriebssysteme
   Windows-BetriebssystemeErstellen Sie eine Benutzer-ID, die Eigner der IBM Spectrum Protect-Serverinstanz sein soll. Eine Benutzer-ID kann Eigner mehrerer IBM Spectrum Protect-Serverinstanzen sein. Geben Sie das Benutzerkonto an, das Eigner der Serverinstanz sein soll.

   Wenn der Server als Windows-Dienst gestartet wird, ist dies das Konto, bei dem sich der Dienst anmeldet. Das Benutzerkonto benötigt Administratorberechtigung auf dem System. Ein Benutzerkonto kann Eigner mehrerer Serverinstanzen sein.

   Befinden sich mehrere Server auf einem System und möchten Sie jeden Server mit einem anderen Benutzerkonto ausführen, erstellen Sie ein neues Benutzerkonto in diesem Schritt.

   Erstellen Sie die Benutzer-ID.
   Einschränkung: Die Benutzer-ID muss die folgende Regel einhalten:

   In der Benutzer-ID dürfen nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstreichungszeichen (_) verwendet werden. Die Benutzer-ID darf maximal 30 Zeichen lang sein und sie darf nicht mit *ibm*, *sql*, *sys* oder mit einer Ziffer beginnen. Als Benutzer-ID und Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* und kein reserviertes SQL-Wort verwendet werden.

   a. Erstellen Sie die Benutzer-ID mit dem folgenden Betriebssystembefehl:

      ```
      net user Benutzer-ID */add
      ```

      Sie werden zur Erstellung und Überprüfung eines Kennworts für die neue Benutzer-ID aufgefordert.
   b. Geben Sie die folgenden Betriebssystembefehle aus, um die neue Benutzer-ID den Administratorgruppen hinzuzufügen:

      ```
      net localgroup Administrators Benutzer-ID /add
      net localgroup DB2ADMNS Benutzer-ID /add
      ```

2. Erstellen Sie die vom Server benötigten Verzeichnisse.
   Windows-BetriebssystemeErstellen Sie leere Verzeichnisse für jeden Tabelleneintrag und stellen Sie sicher, dass die neue Benutzer-ID, die Sie gerade erstellt haben, über Schreib-/Leseberechtigung für die Verzeichnisse verfügt. Die Datenbank, das Archivprotokoll und die

aktive Protokolldatei müssen sich auf verschiedenen physischen Datenträgern befinden.

Element	Beispielbefehle für die Verzeichniserstellung	Ihre Verzeichnisse
Das *Instanzverzeichnis* für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien).	`mkdir d:\tsm\server1`	

Die Datenbankverzeichnisse	`mkdir d:\tsm\db001`
	`mkdir e:\tsm\db002`
	`mkdir f:\tsm\db003`
	`mkdir g:\tsm\db004`	

Verzeichnis für aktive Protokolldateien	`mkdir h:\tsm\log`	
Verzeichnis für Archivprotokolle	`mkdir i:\tsm\archlog`	
Optional: Verzeichnis für den Protokollspiegel für die aktive Protokolldatei	`mkdir j:\tsm\logmirror`	
Optional: Sekundäres Verzeichnis für Archivprotokolle (Übernahmeverzeichnis für Archivprotokolle)	`mkdir k:\tsm\archlogfailover`	

Wenn ein Server anfänglich mit dem Dienstprogramm DSMSERV FORMAT oder mit dem Konfigurationsassistenten erstellt wird, werden eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien zum Speichern von Datenbankinformationen erstellt, die vom Datenbankmanager verwendet werden.

3. Melden Sie die neue Benutzer-ID ab.

Windows: IBM Spectrum Protect-Server konfigurieren

Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.

Informationen zu diesem Vorgang

 Tipp: Die IBM Spectrum Protect-Verwaltungskonsole, bei der es sich um ein Microsoft Management Console-Snap-in (MMC-Snap-in) handelt, wird nicht mehr mit IBM Spectrum Protect bereitgestellt. Die bevorzugte Methode für die Konfiguration des Servers ist der Konfigurationsassistent. Mit dem Assistenten können Sie mehrere Serverkonfigurationstasks ausführen. Sie können mit dem Assistenten jedoch nicht das Active Directory-Schema erweitern, so dass Clients Server automatisch erkennen können.
Wählen Sie eine der folgenden Optionen aus, um eine IBM Spectrum Protect-Serverinstanz zu konfigurieren:

- Windows: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren
  Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.
- Windows: Serverinstanz manuell konfigurieren
  Nach der Installation von IBM Spectrum Protect Version 8.1.2 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

Windows: IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren

Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.

Vorbereitende Schritte

Bevor Sie den Konfigurationsassistenten starten, müssen Sie alle vorhergehenden Schritte zur Vorbereitung der Konfiguration ausführen. Zu diesen Schritten gehören die Installation von IBM Spectrum Protect, die Erstellung der Datenbank- und Protokollverzeichnisse und die Erstellung der Verzeichnisse und der Benutzer-ID für die Serverinstanz.


Informationen zu diesem Vorgang

Windows-BetriebssystemeTipp: Die IBM Spectrum Protect-Konsole, bei der es sich um ein Microsoft Management Console-Snap-in (MMC-Snap-in) handelt, wird nicht mehr mit IBM Spectrum Protect bereitgestellt. Die bevorzugte Methode für die Konfiguration der Serverinstanz ist der Konfigurationsassistent. Mit dem Assistenten können Sie mehrere Konfigurationstasks ausführen.

Vorgehensweise

1. Stellen Sie sicher, dass folgende Anforderungen erfüllt sind: Windows-Betriebssysteme
   - Stellen Sie sicher, dass folgende Anforderungen erfüllt sind:
     a. Klicken Sie auf Start > Verwaltung > Dienste.
     b. Wählen Sie im Fenster Dienste den Dienst Remoteregistrierung aus, wenn er nicht gestartet wurde, und klicken Sie auf Starten.
   - Stellen Sie sicher, dass die Anschlüsse 137, 139 und 445 nicht durch eine Firewall blockiert sind:
     a. Klicken Sie auf Start > Systemsteuerung > Windows-Firewall.
     b. Wählen Sie Erweiterte Einstellungen aus.
     c. Wählen Sie Eingehende Regeln im linken Teilfenster aus.
     d. Wählen Sie Neue Regel im rechten Teilfenster aus.
     e. Erstellen Sie eine Anschlussregel für die TCP-Anschlüsse 137, 139 und 445, die Verbindungen für Domänen und private Netze zulässt.
   - Konfigurieren Sie die Benutzerkontensteuerung:

     Greifen Sie auf alle drei der Konfigurationseinstellungen für die Benutzerkontensteuerung zu, indem Sie zunächst wie folgt auf die Optionen für die Lokale Sicherheitsrichtlinie zugreifen:

     a. Aktivieren Sie das integrierte Administratorkonto:
        - Wählen Sie Konten: Administratorkontostatus aus.
        - Wählen Sie Aktiviert aus und klicken Sie auf OK.
     b. Inaktivieren Sie die Benutzerkontensteuerung für alle Windows-Administratoren:
        - Wählen Sie Benutzerkontensteuerung: Alle Administratoren im Administratorbestätigungsmodus ausführen aus.
        - Wählen Sie Deaktivieren aus und klicken Sie auf OK.
     c. Inaktivieren Sie die Benutzerkontensteuerung für das integrierte Administratorkonto:
        - Wählen Sie Benutzerkontensteuerung: Administratorbestätigungsmodus für das integrierte Administratorkonto aus.
        - Wählen Sie Deaktivieren aus und klicken Sie auf OK.
   - Starten Sie den Server erneut, bevor Sie mit dem Konfigurationsassistenten fortfahren.
2. Starten Sie die lokale Version des Assistenten:
   - Windows-BetriebssystemeKlicken Sie auf Start > Alle Programme > IBM Spectrum Protect > Konfigurationsassistent. Sie können auch doppelt auf das Programm `dsmicfgx.exe` in *Installationsverzeichnis*\server klicken. Das Standardverzeichnis ist C:\Programme\Tivoli\TSM.

   Befolgen Sie die Anweisungen zur Ausführung der Konfiguration. Der Assistent kann gestoppt und erneut gestartet werden. Der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

- Windows-BetriebssystemeWindows: Remote Execution Protocol unter Windows konfigurieren
  Fernzugriffseinstellungen mit diesen Prozeduren konfigurieren.

Windows: Serverinstanz manuell konfigurieren

Nach der Installation von IBM Spectrum Protect Version 8.1.2 können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

- Windows: Serverinstanz erstellen
  Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl db2icrt.
- Windows-BetriebssystemeWindows: Server- und Clientübertragung konfigurieren
  Nach der Installation des Servers können Sie die Client- und Serverübertragung definieren, indem Sie Optionen in den Server- und Clientoptionsdateien angeben.
- Windows: Datenbank und Protokoll formatieren
  Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.
- Windows: Datenbankmanager für die Datenbanksicherung vorbereiten
  Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

Windows: Serverinstanz erstellen

Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl db2icrt.

Informationen zu diesem Vorgang

Auf einer Workstation kann mindestens eine Serverinstanz vorhanden sein.

 Windows-BetriebssystemeWichtig: Stellen Sie sicher, dass der Benutzer und das Instanzverzeichnis des Benutzers vorhanden sind, bevor der Befehl db2icrt ausgeführt wird. Ist kein Instanzverzeichnis vorhanden, müssen Sie es erstellen.
Im Instanzverzeichnis sind folgende Dateien für die Serverinstanz gespeichert:

- Serveroptionsdatei dsmserv.opt
- Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
- Einheitenkonfigurationsdatei, wenn die Serveroption DEVCONFIG keinen vollständig qualifizierten Namen angibt
- Protokolldatei für Datenträger, wenn die Serveroption VOLUMEHISTORY keinen vollständig qualifizierten Namen angibt
- Datenträger für Speicherpools mit dem Typ DEVTYPE=FILE, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
- Benutzerexits
- Traceausgabe (wenn nicht vollständig qualifiziert)

 Windows-Betriebssysteme

1. Melden Sie sich als Administrator an und erstellen Sie mithilfe des Befehls db2icrt eine IBM Spectrum Protect-Instanz. Geben Sie den folgenden Befehl in eine Zeile ein. Das von Ihnen angegebene Benutzerkonto wird zu der Benutzer-ID, die Eigner des Servers der Version 8.1.2 ist (die Instanzbenutzer-ID).

   ```
   db2icrt -u Benutzerkonto Instanzname
   ```

   Lautet das Benutzerkonto beispielsweise *tsminst1* und die Serverinstanz *Server1*, geben Sie folgenden Befehl ein:

   ```
   db2icrt -u tsminst1 server1
   ```

   Sie müssen das Kennwort für die Benutzer-ID *tsminst1* eingeben. Wenn Sie später die Datenbank erstellen und formatieren, verwenden Sie den in diesem Befehl angegebenen Instanznamen mit der Option -k.
2. Geben Sie als Standardpfad für die Datenbank das Laufwerk an, in dem sich das Instanzverzeichnis für den Server befindet. Führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf Start > Programme > IBM DB2 > DB2TSM1 > Befehlszeilentools > Befehlszeilenprozessor.
   b. Geben Sie `quit` ein, um den Befehlszeilenprozessor zu beenden.

      Jetzt sollte ein Fenster mit einer Eingabeaufforderung geöffnet werden, in dem die Umgebung für eine erfolgreiche Eingabe der Befehle in den nächsten Schritten ordnungsgemäß eingerichtet ist.

   c. Geben Sie in die Eingabeaufforderung dieses Fensters den folgenden Befehl ein, um die Umgebungsvariable für die Serverinstanz zu definieren, mit der Sie arbeiten:

      ```
      set db2instance=Instanzname
      ```

      Der *Instanzname* ist mit dem Instanznamen identisch, den Sie bei Ausgabe des Befehls db2icrt angegeben haben. Geben Sie beispielsweise folgenden Befehl aus, um die Umgebungsvariable für die Serverinstanz *Server1* zu definieren:

      ```
      set db2instance=server1
      ```

   d. Geben Sie den Befehl zur Definition des Standardlaufwerks aus:

      ```
      db2 update dbm cfg using dftdbpath Instanzposition
      ```

      Das Instanzverzeichnis ist beispielsweise d:\tsm\server1 und die Instanzposition ist Laufwerk d:. Geben Sie folgenden Befehl ein:

      ```
      db2 update dbm cfg using dftdbpath d:
      ```
3. Erstellen Sie eine neue Serveroptionsdatei. Siehe Windows: Server- und Clientübertragung konfigurieren.

 Windows-Betriebssysteme

Windows: Server- und Clientübertragung konfigurieren

Nach der Installation des Servers können Sie die Client- und Serverübertragung definieren, indem Sie Optionen in den Server- und Clientoptionsdateien angeben.

Informationen zu diesem Vorgang

Definieren Sie diese Serveroptionen vor dem Start des Servers. Wenn Sie den Server starten, werden die neuen Optionen wirksam. Wenn Sie Serveroptionen nach dem Serverstart ändern, müssen Sie den Server stoppen und erneut starten, um die aktualisierten Optionen zu aktivieren.

Sie können Serverübertragungsoptionen in der Serveroptionsdatei (`dsmserv.opt.smp`), die sich im Serverinstanzverzeichnis befindet, anzeigen und angeben. Der Server verwendet standardmäßig die Übertragungsmethoden TCP/IP und Named Pipes (Benannte Pipes).

Tipp: Wenn Sie die Serverkonsole starten und in Warnungen angezeigt wird, dass der Server ein Protokoll nicht verwenden konnte, ist entweder das Protokoll nicht installiert oder die Einstellungen entsprechen nicht den Windows-Protokolleinstellungen.

Damit ein Client ein Protokoll verwenden kann, das auf dem Server aktiviert ist, muss die Clientoptionsdatei entsprechende Werte für Übertragungsoptionen enthalten. In der Serveroptionsdatei können Sie die Werte für jedes Protokoll anzeigen.

Sie können mindestens eine der folgenden Übertragungsmethoden angeben:

- TCP/IP Version 4 oder Version 6
- Benannte Pipes
- Shared Memory
- Secure Sockets Layer (SSL)
  Tipp: Sie können Kennwörter im LDAP-Verzeichnisserver oder im Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.

-  Windows: TCP/IP-Optionen definieren
  Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.
-  Windows: Optionen für benannte Pipes definieren
  Die Übertragungsmethode benannte Pipes (Named Pipes) ist ideal, wenn der Server und der Client auf derselben Windows-Maschine ausgeführt werden. Für benannte Pipes ist keine besondere Konfiguration erforderlich.
-  Windows: Secure Sockets Layer-Optionen definieren
  Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

Windows: TCP/IP-Optionen definieren

Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt eine Liste der TCP/IP-Optionen, mit denen Sie Ihr System definieren können.

```
commmethod         tcpip
  tcpport          1500
  tcpwindowsize    0
  tcpnodelay       yes
```

Tipp: Sie können TCP/IP Version 4 und/oder Version 6 verwenden.

TCPPORT
: Die Adresse des Server-Ports für TCP/IP- und SSL-Kommunikation. Der Standardwert ist 1500.

Windows-BetriebssystemeTCPWINDOWSIZE
:  Windows-BetriebssystemeGibt die Größe des TCP/IP-Puffers an, der beim Senden oder Empfangen von Daten verwendet wird. Die in einer Sitzung verwendete Fenstergröße ist der kleinere Wert der Server- und Clientfenstergröße. Größere Fenstergrößen benötigen zusätzlichen Speicher, können jedoch die Leistung verbessern.

  Soll die Standardfenstergröße für das Betriebssystem verwendet werden, geben Sie 0 an.

TCPNODELAY
: Gibt an, ob der Server kleine Nachrichten sendet oder ob TCP/IP die Nachrichten puffern soll. Das Senden kleiner Nachrichten kann den Durchsatz verbessern, erhöht jedoch die Anzahl der im Netz gesendeten Pakete. Geben Sie YES an, wenn kleine Nachrichten gesendet werden sollen, oder NO, wenn sie TCP/IP puffern soll. Der Standardwert ist YES.

TCPADMINPORT
: Gibt die Anschlussnummer an, an der der TCP/IP-DFV-Treiber des Servers auf TCP/IP- oder SSL-fähige Kommunikationsanforderungen warten soll, die keine Clientsitzungen sind. Der Standardwert ist der Wert von TCPPORT.

SSLTCPPORT
: (Nur SSL) Gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen des Befehlszeilenclients für Sichern/Archivieren und des Verwaltungsbefehlszeilenclients wartet.

SSLTCPADMINPORT
: (Nur SSL) Gibt die Anschlussadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen für den Verwaltungsbefehlszeilenclient wartet.

Windows: Optionen für benannte Pipes definieren

Die Übertragungsmethode benannte Pipes (Named Pipes) ist ideal, wenn der Server und der Client auf derselben Windows-Maschine ausgeführt werden. Für benannte Pipes ist keine besondere Konfiguration erforderlich.

Informationen zu diesem Vorgang

Eine Beispieleinstellung für benannte Pipes:

```
commmethod                  namedpipe
     namedpipename          \\.\pipe\adsmpipe
```

COMMMETHOD kann in der IBM Spectrum Protect-Serveroptionsdatei mehrfach mit einem jeweils anderen Wert verwendet werden. Die folgende Angabe ist beispielsweise möglich:

```
commmethod tcpip
commmethod namedpipe
```

Windows: Secure Sockets Layer-Optionen definieren

Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

Vorbereitende Schritte

SSL ist die Standardtechnologie für die Erstellung verschlüsselter Sitzungen zwischen Servern und Clients. SSL stellt einen sicheren Kanal für die Server- und Clientkommunikation über offene Kommunikationspfade zur Verfügung. Bei SSL wird die Identität des Servers durch Verwendung digitaler Zertifikate überprüft.

Verwenden Sie SSL für Sitzungen nur im Bedarfsfall, um eine bessere Systemleistung sicherzustellen. Sie könnten die Prozessorressourcen auf dem IBM Spectrum Protect-Server erweitern, um den erhöhten Anforderungen gerecht zu werden.

Windows: Datenbank und Protokoll formatieren

Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.

Nach der Konfiguration der Serverübertragung können Sie die Datenbank initialisieren. Sie müssen sich mit der Instanzbenutzer-ID anmelden. Fügen Sie die Verzeichnisse nicht in Dateisysteme ein, deren Speicherplatz nicht ausreichen könnte. Wenn bestimmte Verzeichnisse (z. B. das Archivprotokoll) nicht verfügbar oder voll werden, stoppt der Server.

Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN.

 Windows-BetriebssystemeWichtig: Das Installationsprogramm erstellt eine Gruppe von Registrierungsschlüsseln. Einer dieser Schlüssel verweist auf das Verzeichnis, in dem ein Standardserver mit dem Namen SERVER1 erstellt wird. Soll ein zusätzlicher Server installiert werden, erstellen Sie ein Verzeichnis und verwenden Sie das Dienstprogramm DSMSERV FORMAT mit dem Parameter -k in diesem Verzeichnis. Dieses Verzeichnis wird die Position des Servers. In der Registrierung werden die installierten Server aufgezeichnet.

Exitlistenhandler definieren

Geben Sie für jede Serverinstanz ON für die Registry-Variable DB2NOEXITLIST an. Melden Sie sich als Serverinstanzeigner beim System an und geben Sie den folgenden Befehl aus:

```
db2set -i Name_der_Serverinstanz DB2NOEXITLIST=ON
```

Beispiel:  Windows-Betriebssysteme

```
db2set -i server1 DB2NOEXITLIST=ON
```

Serverinstanz initialisieren

Mit dem Dienstprogramm DSMSERV FORMAT können Sie eine Serverinstanz initialisieren. Wenn das Verzeichnis der Serverinstanz z. B. */tsminst1* lautet, geben Sie die folgenden Befehle aus:  Windows-Betriebssysteme

```
cd \tsminst1
dsmserv -k server2 format dbdir=d:\tsm\db001 activelogsize=32768
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zu Grunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.

Zugehörige Informationen:

DSMSERV FORMAT (Datenbank und Protokoll formatieren)

Windows: Datenbankmanager für die Datenbanksicherung vorbereiten

Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

Informationen zu diesem Vorgang

Wenn Sie den Konfigurationsassistenten verwenden, um eine IBM Spectrum Protect-Serverinstanz zu erstellen, müssen Sie diese Schritte nicht ausführen. Wenn Sie eine Instanz manuell konfigurieren, führen Sie die folgenden Schritte aus, bevor Sie den Befehl BACKUP DB oder RESTORE DB ausgeben.

Achtung: Wenn die Datenbank nicht verwendet werden kann, ist der gesamte IBM Spectrum Protect-Server nicht verfügbar. Wenn eine Datenbank verloren geht und nicht wiederhergestellt werden kann, kann die Wiederherstellung der von diesem Server verwalteten Daten schwierig oder unmöglich sein. Daher ist es unbedingt erforderlich, die Datenbank zu sichern.
Windows-BetriebssystemeEinschränkung: Auf Windows-Systemen ist die Datenbanksicherung und -zurückschreibung für gemeinsam genutzten Speicher nicht verfügbar.
Windows-BetriebssystemeIn den folgenden Befehlen werden `server1` für die Datenbankinstanz und d:\tsmserver1 für das IBM Spectrum Protect-Serververzeichnis als Beispiele verwendet. Ersetzen Sie diese Werte durch tatsächliche Werte in den Befehlen.

1. Erstellen Sie eine Datei mit dem Namen `tsmdbmgr.env` im Verzeichnis d:\tsmserver1 mit folgendem Inhalt:

   ```
   DSMI_CONFIG=Serverinstanzverzeichnis\tsmdbmgr.opt
   DSMI_LOG=Serverinstanzverzeichnis
   ```

2. Definieren Sie die Konfiguration der API-Umgebungsvariablen DSMI_ für die Datenbankinstanz:
   a. Öffnen Sie ein DB2-Befehlsfenster. Sie können hierfür in das Verzeichnis C:\Programme\Tivoli\TSM\db2\bin wechseln oder, wenn Sie IBM Spectrum Protect an einer anderen Position installiert haben, in das Unterverzeichnis db2\bin in Ihrem Hauptinstallationsverzeichnis. Geben Sie dann den folgenden Befehl aus:

      ```
      db2cmd
      ```

   b. Geben Sie den folgenden Befehl aus:

      ```
      db2set -i server1 DB2_VENDOR_INI=d:\tsmserver1\tsmdbmgr.env
      ```

3. Erstellen Sie eine Datei mit dem Namen `tsmdbmgr.opt` im Verzeichnis d:\tsmserver1 mit folgendem Inhalt:

   ```
   ************************************************
   nodename $$_TSMDBMGR_$$
   commmethod tcpip
   tcpserveraddr localhost
   tcpport 1500
   passwordaccess generate
   errorlogname d:\tsmserver1\tsmdbmgr.log
   ```

   Erläuterungen:
   - *Nodename* gibt den Knotennamen an, mit dem die Client-API während einer Datenbanksicherung eine Verbindung zum Server herstellt. Dieser Wert muss `$$_TSMDBMGR_$$` lauten, damit die Datenbanksicherung funktioniert.
   - *Commethod* gibt die Client-API an, mit der Kontakt zum Server wegen der Datenbanksicherung hergestellt wird.
   - *Tcpserveraddr* gibt die Serveradresse an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `localhost` lauten.
   - *Tcpport* gibt die Anschlussnummer an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Sie müssen denselben `tcpport`-Wert wie in der Serveroptionsdatei dsmserv.opt angeben.
   - *Passwordaccess* ist für die Verbindung des Sicherungsknotens zum Server auf Windows-Systemen erforderlich.
   - *Errorlogname* gibt das Fehlerprotokoll an, in dem die Client-API Fehler protokolliert, die während einer Datenbanksicherung auftreten. Dieses Protokoll befindet sich normalerweise im Serverinstanzverzeichnis. Dieses Protokoll kann sich jedoch an jeder beliebigen Position befinden, für die die Instanzbenutzer-ID Schreibberechtigung hat.

Windows: Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren

Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.

Informationen zu diesem Vorgang

Die Tabellen- und Indexreorganisation erfordert in hohem Umfang Prozessorressourcen, Speicherbereich für die aktive Protokolldatei und Speicherbereich für das Archivprotokoll. Da die Datenbanksicherung Vorrang vor der Reorganisation hat, wählen Sie den Zeitpunkt und die Dauer für die Reorganisation aus, um sicherzustellen, dass sich die Prozesse nicht überlappen und die Reorganisation ausgeführt werden kann.

Windows-BetriebssystemeSie können die Index- und Tabellenreorganisation für die Serverdatenbank optimieren. Auf diese Weise können Sie die Vermeidung von unerwartetem Datenbankwachstum und Leistungsproblemen verbessern. Anweisungen finden Sie in Technote 1683633.

Wenn Sie diese Serveroptionen aktualisieren, während der Server aktiv ist, müssen Sie den Server stoppen und erneut starten, damit die aktualisierten Werte wirksam werden.

Vorgehensweise

1. Ändern Sie die Serveroptionen.
    Bearbeiten Sie die Serveroptionsdatei dsmserv.opt im Serverinstanzverzeichnis mithilfe eines Texteditors.
   Beachten Sie bei der Bearbeitung der Serveroptionsdatei die folgenden Richtlinien:
   - Entfernen Sie den Stern am Zeilenanfang, um eine Option zu aktivieren.
   - Geben Sie eine Option in einer beliebigen Zeile ein.
   - Geben Sie nur eine Option pro Zeile ein. Die vollständige Option mit ihrem Wert muss sich in einer Zeile befinden.
   - Haben Sie mehrere Einträge für eine Option in der Datei, verwendet der Server den letzten Eintrag.

   Die verfügbaren Serveroptionen können Sie mit der Musterdatei dsmserv.opt.smp im Verzeichnis c:\Programme\Tivoli\TSM anzeigen.
2. Ist die Verwendung der Datendeduplizierung geplant, aktivieren Sie die Serveroption ALLOWREORGINDEX. Fügen Sie der Serveroptionsdatei die folgende Option und den folgenden Wert hinzu:

   ```
   allowreorgindex yes
   ```

3. Definieren Sie die Serveroptionen REORGBEGINTIME und REORGDURATION, mit denen gesteuert wird, wann die Reorganisation gestartet und wie lange sie ausgeführt wird. Wählen Sie den Zeitpunkt und die Dauer so aus, dass die Reorganisation ausgeführt wird, wenn der Server voraussichtlich am wenigsten ausgelastet ist. Diese Serveroptionen steuern sowohl die Tabellen- als auch die Indexreorganisationsprozesse.
   a. Definieren Sie die Startzeit der Reorganisation mit der Serveroption REORGBEGINTIME. Geben Sie die Zeit im 24-Stunden-Format an. Um beispielsweise als Startzeit der Reorganisation 20:30 Uhr festzulegen, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

      ```
      reorgbegintime 20:30
      ```

   b. Definieren Sie das Intervall, in dem der Server die Reorganisation starten kann. Um beispielsweise anzugeben, dass der Server die Reorganisation innerhalb von 4 Stunden nach dem mit der Serveroption REORGBEGINTIME definierten Zeitpunkt starten kann, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

      ```
      reorgduration 4
      ```

4. War der Server aktiv, während Sie die Serveroptionsdatei aktualisiert haben, stoppen Sie den Server und starten Sie ihn erneut.

Zugehörige Informationen:
ALLOWREORGINDEX
ALLOWREORGTABLE
REORGBEGINTIME
REORGDURATION

Windows: Serverinstanz auf Windows-Systemen starten

In einer Produktionsumgebung ist die bevorzugte Methode zum Starten des Servers der Start als Windows-Dienst. In einer Umgebung, in der Sie rekonfigurieren, testen oder Verwaltungstasks ausführen, starten Sie den Server im Vordergrund oder verwenden Sie den Verwaltungsmodus.

Vorbereitende Schritte

Wählen Sie eine der folgenden Methoden zum Starten des Servers aus:

Als Windows-Dienst
: Diese Methode ist in einer Produktionsumgebung nützlich. Wenn Sie die Ausführung des Servers als Dienst konfigurieren, können Sie angeben, dass der Server bei jedem Systemstart automatisch startet.

Im Vordergrund
: Diese Methode ist für die Konfiguration oder den Test des Servers nützlich. Wenn Sie den Server im Vordergrund starten, stellt IBM Spectrum Protect eine spezielle Administrator-ID mit dem Namen SERVER_CONSOLE bereit. Alle Servernachrichten werden im Vordergrund angezeigt. Die Nachrichten können hilfreich sein, wenn Sie Startprobleme beheben müssen.

Im Verwaltungsmodus
: Diese Methode ist bei der Ausführung von Verwaltungs- oder Rekonfigurationstasks nützlich. Wenn Sie den Server im Verwaltungsmodus starten, inaktivieren Sie damit Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten.

Vorgehensweise

Befolgen Sie die Anweisungen für Ihr ausgewählte Option:

Option	Bezeichnung

Option	Bezeichnung
Server als Windows-Dienst starten	Führen Sie einen der folgenden Schritte aus, um den Server als Windows-Dienst zu starten: • Wenn Sie den Server mithilfe des Konfigurationsassistenten konfiguriert haben, führen Sie die folgenden Schritte aus: a. Befolgen Sie die Anweisungen in Windows: Server für den Start als Windows-Dienst konfigurieren, um den Server für den Start als Windows-Dienst zu konfigurieren. b. Befolgen Sie die Anweisungen in Windows: Server als Windows-Dienst starten, um den Server zu starten. • Wenn Sie den Konfigurationsassistenten nicht verwendet haben, befolgen Sie die Anweisungen in Windows: Windows-Dienst manuell erstellen und konfigurieren, um den Windows-Dienst zu erstellen und zu konfigurieren.
Server im Vordergrund starten	Server im Hintergrund starten: Befolgen Sie die Anweisungen in Windows: Server im Vordergrund starten.
Server im Verwaltungsmodus starten	Server im Verwaltungsmodus starten: Befolgen Sie die Anweisungen in Windows: Server im Verwaltungsmodus starten.

Windows-Betriebssysteme

Windows: Server für den Start als Windows-Dienst konfigurieren

Bevor Sie den Server als Windows-Dienst starten können, müssen Sie sicherstellen, dass Optionen und Zugriffsberechtigungen ordnungsgemäß definiert sind.

Vorbereitende Schritte

Ein Windows-Dienst muss erstellt werden. Wenn Sie den Server mithilfe des Konfigurationsassistenten konfiguriert haben, wurde automatisch ein Windows-Dienst erstellt. In diesem Fall führen Sie diese Prozedur aus, um den Server für den Start als Windows-Dienst zu konfigurieren.

Wenn Sie keinen Assistenten verwendet haben, müssen Sie den Windows-Dienst manuell erstellen und konfigurieren. Führen Sie hierfür die Schritte in Windows: Windows-Dienst manuell erstellen und konfigurieren aus.

Vorgehensweise

1. Klicken Sie im Windows-Menü Start auf Ausführen, geben Sie `services.msc` ein und klicken Sie auf OK.
2. Wählen Sie im Fenster Dienste die Serverinstanz aus, die als Dienst gestartet werden soll, und klicken Sie auf Eigenschaften. Wählen Sie beispielsweise TSM INST1 aus und klicken Sie auf Eigenschaften.
3. Um sicherzustellen, dass der Serverdienst automatisch gestartet wird, klicken Sie auf die Registerkarte Allgemein. Wählen Sie in der Liste bei Starttyp Automatisch aus.
4. Um den Benutzer zum Starten des Serverdienstes zu definieren, klicken Sie auf die Registerkarte Anmelden und führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie den Serverdienst unter dem lokalen Systemkonto ausführen wollen, wählen Sie Lokales Systemkonto aus und klicken Sie auf OK.
   - Wenn der Serverdienst unter der Instanzbenutzer-ID ausgeführt werden soll, führen Sie folgende Aktionen aus:
     a. Wählen Sie Dieses Konto aus und suchen Sie nach der Benutzer-ID, die Eigner der DB2-Serverinstanz ist und über Berechtigungen zum Starten des Servers verfügt.
     b. Geben Sie im Fenster Benutzer auswählen im Feld Namen des auszuwählenden Objekts eingeben die Benutzer-ID ein.
     c. Klicken Sie auf Namen überprüfen.
     d. Klicken Sie zweimal auf OK.
5. Wenn der Serverdienst für die Ausführung unter dem lokalen Systemkonto konfiguriert wurde, müssen Sie dem lokalen Systemkonto Datenbankzugriffsberechtigung erteilen:
   a. Melden Sie sich mit der Benutzer-ID an, die zum Erstellen der Serverdatenbank verwendet wurde. Dabei handelt es sich um die Benutzer-ID, die zur Ausführung des Dienstprogramms DSMSERV FORMAT zum Initialisieren der Serverdatenbank verwendet wurde. Wenn der Server mithilfe des Konfigurationsassistenten dsmicfgx konfiguriert wurde, handelt es sich um die Benutzer-ID, mit der die Instanz erstellt wurde.
   b. Öffnen Sie ein DB2-Befehlsfenster. Wenn der Server unter Windows Server 2012 installiert ist, öffnen Sie das Fenster Start und klicken Sie auf DB2-Befehlsfenster - Administrator.
   c. Geben Sie im DB2-Befehlsfenster die folgenden Befehle ein:

```
set DB2INSTANCE=server1
db2 connect to TSMDB1
db2 grant dbadm with dataaccess with accessctrl on database to user system
db2 grant secadm on database to user system
```

   Tipp: Wenn der Serverdienst für die Ausführung unter dem lokalen Systemkonto konfiguriert ist, kann jeder Administrator im System auf die Datenbank zugreifen. Darüber hinaus kann jeder Administrator, der sich am System anmelden kann, den Server ausführen.

Nächste Schritte

Befolgen Sie die Anweisungen in Windows: Server als Windows-Dienst starten, um den Dienst zu starten.

Windows-Betriebssysteme

Windows: Server als Windows-Dienst starten

Wenn Sie IBM Spectrum Protect unter einem Windows-Betriebssystem ausführen, können Sie den Server als Dienst starten.

Vorbereitende Schritte

Ein Windows-Dienst muss erstellt werden. Der Dienst wurde automatisch erstellt, wenn Sie den Server mithilfe des Konfigurationsassistenten konfiguriert haben. Wenn der Dienst automatisch erstellt wurde, müssen Sie den Start des Servers als Dienst konfigurieren. Führen Sie hierfür die Schritte in Windows: Server für den Start als Windows-Dienst konfigurieren aus. Führen Sie anschließend die Schritte dieser Prozedur aus, um den Server als Dienst zu starten.

Wenn Sie den Dienst nicht mithilfe des Konfigurationsassistenten erstellt haben, müssen Sie den Dienst manuell erstellen und konfigurieren. Führen Sie die Schritte in Windows: Windows-Dienst manuell erstellen und konfigurieren aus.

Vorgehensweise

Gehen Sie wie folgt vor, um den Server als Windows-Dienst zu starten:

1. Melden Sie sich beim Server mit einer Benutzer-ID an, die zur Gruppe 'Administratoren' gehört.
2. Klicken Sie im Windows-Menü Start auf Ausführen, geben Sie `services.msc` ein und klicken Sie auf OK.
3. Wählen Sie im Fenster Dienste die Serverinstanz aus, die Sie starten wollen, und klicken Sie auf Starten.

Nächste Schritte

Da der Serverdienst Anforderungen ausgeben kann, die eine Aktion erfordern, muss die Serveraktivität mit dem Operations Center oder dem Verwaltungsclient überwacht werden.

Um Abschlussnachrichten für das Starten und Stoppen anzuzeigen, die im Anwendungsprotokoll von Windows protokolliert sind, verwenden Sie das Tool Ereignisanzeige im Ordner Verwaltung.


Windows-Betriebssysteme

Windows: Windows-Dienst manuell erstellen und konfigurieren

Wenn Sie den Server mithilfe des Konfigurationsassistenten konfiguriert hatten, wurde automatisch ein Windows-Dienst erstellt. Wenn kein Dienst automatisch erstellt wurde, müssen Sie ihn erstellen.

Vorbereitende Schritte

Für diese Prozedur müssen Sie sich mit einer Benutzer-ID anmelden, die zur Gruppe 'Administratoren' gehört.

Vorgehensweise

Gehen Sie wie folgt vor, um einen Windows-Dienst zu erstellen und die Startoptionen für den Dienst zu konfigurieren:

Öffnen Sie ein Befehlsfenster und geben Sie den Befehl sc.exe create ein:

```
sc.exe create Servername binPath= "Serverpfad -k Instanzname"
start= Starttyp obj= Kontoname password= Kennwort
```

Hierbei gilt Folgendes:

Servername
: Gibt den Namen des Serverdienstes an.

Serverpfad
: Gibt den Pfad zur ausführbaren Datei dsmsvc.exe und den Dateinamen an. Der Standardpfad lautet:

  C:\Programme\Tivoli\TSM\server

Instanzname
: Gibt den Namen der DB2-Instanz an, der mit dem Namen der Serverinstanz identisch ist, z. B. Server1.

Starttyp
: Gibt die Startmethode für den Dienst an. Soll der Dienst automatisch gestartet werden, geben Sie `auto` ein. Wenn Sie die Option `auto` angeben, wird der Dienst automatisch beim Systemstart gestartet und bei jedem Neustart des Systems automatisch erneut gestartet. Soll

der Dienst manuell gestartet werden, geben Sie `demand` ein.

Kontoname
Gibt die Benutzer-ID für das Konto an, unter dem der Dienst ausgeführt wird. Der Kontoname könnten z. B. 'Administrator' lauten. Dieser Parameter ist optional. Wird er nicht angegeben, wird das Konto 'Lokales System' verwendet.

Kennwort
Gibt das Kennwort für das Benutzerkonto *Kontoname* an.

Tipp: Achten Sie bei der Befehlseingabe darauf, dass hinter jedem Gleichheitszeichen (=) ein Leerzeichen eingegeben wird.

Ergebnisse

Der Server wird als Windows-Dienst gestartet.
 Windows-Betriebssysteme

Windows: Server im Vordergrund starten

Um direkt mit dem IBM Spectrum Protect-Server interagieren zu können, starten Sie den Server im Vordergrund. Wenn Sie beispielsweise Befehle eingeben möchten, starten Sie den Server im Vordergrund.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis, in dem der Server installiert ist. Wechseln Sie beispielsweise in das Verzeichnis c:\Programme\tivoli\tsm\server.
2. Geben Sie den folgenden Befehl ein:

   ```
   dsmserv -k Instanzname
   ```

   Dabei gibt *Instanzname* die Serverinstanz an.

 Windows-Betriebssysteme

Windows: Dem Server zugeordnete Services auf Windows-Systemen

Wenn Sie den IBM Spectrum Protect-Server als Dienst starten, starten andere Services automatisch. Diese Services sind dem Datenbankmanager, DB2, zugeordnet.

Die folgenden Services sind dem Server zugeordnet.

Servicename	Zweck	Kommentare
`TSM Serverinstanz`	Der Service für die Serverinstanz mit dem Namen *Serverinstanz*. Zum Beispiel: `TSM Server1`	Definieren Sie die Start- und Stoppoptionen für diesen Service, um die Serverinstanz automatisch zu starten und zu stoppen. Jede Serverinstanz wird als separater Service ausgeführt.
`DB2 - DB2TSM1 - SERVERINSTANZ`	Der DB2-Service für die Serverinstanz mit dem Namen *Serverinstanz*. Zum Beispiel: `DB2 - DB2TSM1 - SERVER1`	Dieser Service wird automatisch gestartet, wenn der Service für die Serverinstanz gestartet wird. Der DB2-Service wird nicht automatisch gestoppt, wenn Sie den Service für den Server stoppen. Das System verfügt über einen dieser Services für jeden Serverinstanzservice, der auf dem System gestartet wird.
`DB2 Governor (DB2TSM1)`	Ein DB2-Service, der während der Installation erstellt wird und für alle Serverinstanzen benötigt wird.	Ändern Sie nicht die Optionen für diesen Service.
`DB2 License Server (DB2TSM1)`	Ein DB2-Service, der während der Installation erstellt wird und für alle Serverinstanzen benötigt wird.	Ändern Sie nicht die Optionen für diesen Service.
`DB2 Management Server (DB2TSM1)`	Ein DB2-Service, der während der Installation erstellt wird und für alle Serverinstanzen benötigt wird.	Ändern Sie nicht die Optionen für diesen Service.
`DB2 Remote Command Server (DB2TSM1)`	Ein DB2-Service, der während der Installation erstellt wird und für alle Serverinstanzen benötigt wird.	Ändern Sie nicht die Optionen für diesen Service.

 Windows-Betriebssysteme

Windows: Server im Verwaltungsmodus starten

Sie können den Server im Verwaltungsmodus starten, um Unterbrechungen während Verwaltungs- oder Rekonfigurationstasks zu vermeiden.

Informationen zu diesem Vorgang

Führen Sie das Dienstprogramm DSMSERV mit dem Parameter MAINTENANCE aus, um den Server im Verwaltungsmodus zu starten.

Die folgenden Operationen sind im Verwaltungsmodus inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Wiederherstellung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Außerdem wird verhindert, dass Clients Sitzungen mit dem Server starten.
Tipps:

- Sie müssen die Serveroptionsdatei dsmserv.opt nicht bearbeiten, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Prozesse für die Speicherbereichswiederherstellung, den Bestandsverfall und die Speicherpoolumlagerung manuell starten.

Vorgehensweise

Geben Sie den folgenden Befehl aus, um den Server im Verwaltungsmodus zu starten:

```
dsmserv maintenance
```

Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann unter Server im Verwaltungsmodus starten angezeigt werden.

Nächste Schritte

Gehen Sie wie folgt vor, um den Serverbetrieb im Produktionsmodus fortzusetzen:

1. Geben Sie den Befehl HALT aus, um den Server herunterzufahren:

   ```
   halt
   ```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden.

Die während des Verwaltungsmodus inaktivierten Operationen werden wieder aktiviert.

Windows: Server stoppen

Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.

Informationen zu diesem Vorgang

Geben Sie den folgenden Befehl in die IBM Spectrum Protect-Befehlszeile ein, um den Server zu stoppen:

```
halt
```

Windows: Lizenzregistrierung

Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.

Informationen zu diesem Vorgang

Verwenden Sie hierfür den Befehl REGISTER LICENSE. Weitere Informationen siehe REGISTER LICENSE.

Beispiel: Lizenz registrieren

Die IBM Spectrum Protect-Basislizenz registrieren.

```
register license file=tsmbasic.lic
```

Windows: Einheitenklasse als Vorbereitung für Datenbanksicherungen angeben

Sie müssen die zu verwendende Einheitenklasse angeben, um das System für automatische oder manuelle Datenbanksicherungen vorzubereiten.

Vorbereitende Schritte

Stellen Sie sicher, dass eine Bandeinheitenklasse oder eine Einheitenklasse FILE definiert wurde. Ausführliche Informationen finden Sie in DEFINE DEVCLASS oder suchen Sie nach 'Einheitenklasse definieren'.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Ihr System für Datenbanksicherungen zu konfigurieren.

Vorgehensweise

1. Wenn Sie den Server nicht mit dem Konfigurationsassistenten (dsmicfgx) konfiguriert haben, müssen Sie sicherstellen, dass die Schritte zur manuellen Konfiguration des Systems für Datenbanksicherungen ausgeführt werden.
2. Wählen Sie die für Datenbanksicherungen zu verwendende Einheitenklasse aus. Geben Sie den folgenden Befehl über eine IBM Spectrum Protect-Verwaltungsbefehlszeile aus.

   ```
   set dbrecovery Einheitenklassenname
   ```

   Die angegebene Einheitenklasse wird vom Datenbankmanager für Datenbanksicherungen verwendet. Wenn Sie keine Einheitenklasse mit dem Befehl SET DBRECOVERY angeben, schlägt die Sicherung fehl.

Beispiel

Geben Sie beispielsweise den folgenden Befehl aus, um anzugeben, dass die Einheitenklasse DBBACK verwendet werden soll:

```
set dbrecovery dbback
```

Windows: Mehrere Serverinstanzen auf einem System ausführen

Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.

Multiplizieren Sie den Speicherbedarf und andere Systemvoraussetzungen für einen Server mit der geplanten Instanzzahl für das System.

 Windows-BetriebssystemeDie Gruppe der Dateien für eine Instanz des Servers wird getrennt von den Dateien gespeichert, die von einer anderen Serverinstanz auf demselben System verwendet werden. Gehen Sie wie in Windows: Serverinstanz erstellen beschrieben für jede neue Instanz vor, mit wahlweiser Erstellung des neuen Instanzbenutzers.

Zur Verwaltung des von jedem Server verwendeten Systemspeichers begrenzen Sie mit der Serveroption DBMEMPERCENT den Prozentsatz des Systemspeichers. Haben alle Server denselben Stellenwert, verwenden Sie für jeden Server denselben Wert. Ist ein Server ein Produktionsserver und andere Server sind Testserver, geben Sie für den Produktionsserver einen höheren Wert an als für die Testserver.

Von Version 6.3 auf Version 7.1 ist ein direktes Upgrade möglich. Weitere Informationen finden Sie im Abschnitt über das Upgrade (Upgrade auf Version 8.1 durchführen). Wenn Sie ein Upgrade durchführen und mehrere Server auf dem System haben, müssen Sie den Installationsassistenten nur einmal ausführen. Der Installationsassistent erfasst die Datenbank- und Variablendaten für alle ursprünglichen Serverinstanzen.

Wenn Sie ein Upgrade von IBM Spectrum Protect Version 6.3 auf Version 8.1.2 durchführen und sich mehrere Server auf Ihrem System befinden, werden alle in DB2 Version 9.7 vorhandenen Instanzen gelöscht und in DB2 Version 11.1 erneut erstellt. Der Assistent gibt den Befehl `db2 upgrade DB DB-Name` für jede Datenbank aus. Die Datenbankumgebungsvariablen für jede Instanz auf Ihrem System werden ebenfalls während des Upgradeprozesses neu konfiguriert.

 Windows-BetriebssystemeZu einer IBM Spectrum Protect-Standardinstallation gehört eine Serverinstanz auf dem IBM Spectrum Protect-Server-Computer. Sie können eine zweite Instanz installieren, wenn Sie eine Clusterumgebung konfigurieren. Sie können auch mehrere Server auf einem großen Computer ausführen, wenn Sie über mehrere Bandarchive oder über eine Konfiguration verfügen, die nur aus Plattenspeicher besteht. Nach der Installation und Konfiguration des ersten IBM Spectrum Protect-Servers erstellen Sie mithilfe des Assistenten für Serverinitialisierung weitere IBM Spectrum Protect-Serverinstanzen auf demselben Computer.

 Windows-BetriebssystemeMithilfe des Assistenten für Serverinitialisierung können Sie bis zu vier IBM Spectrum Protect-Serverinstanzen in einem einzelnen System oder Cluster installieren.

Zugehörige Tasks:
Mehrere Serverinstanzen auf einem einzigen System ausführen (Version 7.1.1)

Windows: Server überwachen

Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

Vorgehensweise

1. Überwachen Sie die aktive Protokolldatei, um sicherzustellen, dass die Größe für die Auslastung der Serverinstanz korrekt ist.

   Wenn die Serverauslastung ihren normalen erwarteten Stand erreicht hat, belegt der von der aktiven Protokolldatei verwendete Speicherbereich 80 bis 90 Prozent des Speicherbereichs, der für das Verzeichnis für aktive Protokolldateien zur Verfügung steht. An diesem Punkt müssen Sie den Speicherbereich möglicherweise vergrößern. Die Vergrößerung des Speicherbereichs ist von der Art der Transaktionen in der Serververarbeitung abhängig. Transaktionsmerkmale wirken sich auf die Belegung des Speicherbereichs der aktiven Protokolldateien aus.

   Die folgenden Transaktionsmerkmale können sich auf die Speicherbereichsbelegung in der aktiven Protokolldatei auswirken:

   - Die Anzahl und Größe der Dateien in Sicherungsoperationen
     - Clients, wie z. B. Dateiserver, die zahlreiche kleine Dateien sichern, können zahlreiche Transaktionen verursachen, die in kurzer Zeit ausgeführt werden. Die Transaktionen können sehr viel Speicherbereich in der aktiven Protokolldatei belegen, jedoch nur für kurze Zeit.
     - Clients, wie z. B. E-Mail-Server oder ein Datenbankserver, die große Datenvolumen in wenigen Transaktionen sichern, können wenige Transaktionen verursachen, deren Auführung viel Zeit in Anspruch nimmt. Die Transaktionen können wenig Speicherbereich in der aktiven Protokolldatei belegen, jedoch für lange Zeit.
   - Netzverbindungstypen
     - Mit schnellen Netzverbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, die schneller ausgeführt werden. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen kürzeren Zeitraum.
     - Mit langsameren Verbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, deren Ausführung länger dauert. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen längeren Zeitraum.

   Wenn der Server Transaktionen mit sehr unterschiedlichen Merkmalen verarbeitet, kann der für die aktive Protokolldatei verwendete Speicherbereich im Lauf der Zeit sehr stark schwanken. Für einen solchen Server müssen Sie unter Umständen dafür sorgen, dass ein niedrigerer Prozentsatz des Speicherbereichs der aktiven Protokolldatei verwendet wird. Der zusätzliche Speicherbereich gestattet eine Vergrößerung der aktiven Protokolldatei für Transaktionen, die viel Zeit in Anspruch nehmen.

2. Überwachen Sie das Archivprotokoll, um sicherzustellen, dass immer Speicherbereich verfügbar ist.
   Hinweis: Wenn das Archivprotokoll und das Übernahmearchivprotokoll voll werden, kann die aktive Protokolldatei voll werden, so dass der Server stoppt. Für das Archivprotokoll muss so viel Speicherbereich zur Verfügung stehen, dass dieser niemals vollständig belegt wird.
   Sie werden wahrscheinlich Folgendes feststellen:
   a. Am Anfang wird das Archivprotokoll schnell größer, wenn normale Clientsicherungsoperationen ausgeführt werden.
   b. Datenbanksicherungen werden regelmäßig ausgeführt, entweder mit einem Zeitplan oder manuell.
   c. Nach mindestens zwei Datenbankgesamtsicherungen wird das Abschneiden des Protokolls automatisch ausgeführt. Der vom Archivprotokoll belegte Speicherbereich verringert sich durch das Abschneiden.
   d. Normale Clientoperationen werden fortgesetzt und das Archivprotokoll wird wieder größer.
   e. Datenbanksicherungen finden regelmäßig statt und die Häufigkeit der Protokollbereinigung ist von der Häufigkeit der Datenbankgesamtsicherungen abhängig.

   Nach diesem Muster nimmt die Größe des Archivprotokolls zunächst zu, verringert sich und nimmt dann eventuell wieder zu. Im Laufe der Zeit sollte der vom Archivprotokoll belegte Speicherbereich während der normalen Verarbeitung einen relativ konstanten Stand erreichen.

   Wenn die Größe des Archivprotokolls weiter zunimmt, sollten Sie eine oder beide der folgenden Maßnahmen in Betracht ziehen:
   - Ordnen Sie dem Archivprotokoll weiteren Speicherbereich zu. Sie müssen unter Umständen das Archivprotokoll in ein anderes Dateisystem versetzen.
   - Erhöhen Sie die Häufigkeit der Datenbankgesamtsicherungen, so dass die Protokollbereinigung häufiger stattfindet.
3. Wenn Sie ein Verzeichnis für das Übernahmearchivprotokoll definiert haben, überprüfen Sie, ob darin Protokolle während der normalen Verarbeitung gespeichert werden. Wenn der Speicherbereich des Übernahmeprotokolls verwendet wird, sollten Sie das Archivprotokoll vergrößern. Das Übernahmearchivprotokoll sollte nur unter außergewöhnlichen Bedingungen verwendet werden, nicht während der normalen Verarbeitung.

Windows: IBM Spectrum Protect-Server-Fixpack installieren

IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.

Vorbereitende Schritte

Damit ein Fixpack oder ein vorläufiger Fix auf dem Server installiert werden kann, müssen Sie den Server mit der Stufe installieren, auf der er ausgeführt werden soll. Sie müssen die Serverinstallation nicht mit dem Basisrelease beginnen. Wenn momentan beispielsweise Version 8.1.1 installiert ist, können Sie das aktuelle Fixpack für Version 8.1 direkt verwenden. Sie müssen nicht mit der Installation von Version 8.1.0 beginnen, wenn eine Wartungsaktualisierung verfügbar ist.

Das IBM Spectrum Protect-Lizenzpaket muss installiert sein. Das Lizenzpaket wird beim Kauf eines Basisreleases bereitgestellt. Wenn Sie ein Fixpack oder einen vorläufigen Fix von Fix Central herunterladen, installieren Sie die Serverlizenz, die auf der Website von Passport Advantage zur Verfügung steht. Sollen Nachrichten und Hilfetext nicht in Englisch angezeigt werden, installieren Sie das gewünschte Sprachenpaket.

Wenn Sie ein Upgrade des Servers auf Version 8.1.2 oder höher durchführen und den Server dann auf einen Stand vor Version 8.1.2 zurücksetzen, müssen Sie die Datenbank auf einen Zeitpunkt vor dem Upgrade zurückschreiben. Führen Sie während des Upgrades die erforderlichen Schritte aus, mit denen sichergestellt wird, dass die Datenbank zurückgeschrieben werden kann: Sichern Sie die Datenbank, die Protokolldatei für Datenträger, die Einheitenkonfigurationsdatei und die Serveroptionsdatei. Weitere Informationen finden Sie in Windows: Von Version 8.1.2 auf eine vorherige Serverversion zurücksetzen.

Wenn Sie den Clientverwaltungsservice verwenden, müssen Sie ein Upgrade dieses Service auf dieselbe Version wie beim IBM Spectrum Protect-Server durchführen.

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des installierten Servers aufbewahrt werden. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Rufen Sie das IBM® Support Portal auf. Hier finden Sie folgende Informationen:

- Eine Liste der neuesten Wartungs- und Download-Fixes. Klicken Sie auf **Download** und legen Sie alle gültigen Fixes an.
- Informationen zum Erwerb eines Basislizenzpakets. Suchen Sie nach **Downloads > Passport Advantage**.
- Unterstützte Plattformen und Systemvoraussetzungen. Suchen Sie nach **IBM Spectrum Protect supported operating systems**.

Sie müssen ein Upgrade des Servers durchführen, bevor Sie ein Upgrade der Clients für Sichern/Archivieren durchführen. Wenn Sie das Upgrade des Servers nicht zuerst durchführen, könnte die Kommunikation zwischen dem Server und den Clients unterbrochen werden.

Achtung: Sie dürfen die DB2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der DB2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Fixpack oder einen vorläufigen Fix zu installieren:

1. Sichern Sie die Datenbank. Die bevorzugte Methode ist eine Momentaufnahmesicherung. Bei einer Momentaufnahmesicherung handelt es sich um eine Datenbankgesamtsicherung, bei der geplante Datenbanksicherungen nicht unterbrochen werden. Geben Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Sichern Sie die Einheitenkonfigurationsdaten. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup devconfig filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.
3. Speichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis oder benennen Sie die Datei um. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup volhistory filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.
4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
5. Halten Sie den Server vor der Installation eines Fixpacks oder eines vorläufigen Fixes an. Verwenden Sie den Befehl HALT.
6. Stellen Sie sicher, dass im Installationsverzeichnis zusätzlicher Speicherplatz zur Verfügung steht. Für die Installation dieses Fixpacks kann zusätzlicher temporärer Plattenspeicherplatz im Installationsverzeichnis des Servers erforderlich sein. Die Größe des zusätzlichen Plattenspeicherplatzes kann der Größe entsprechen, die für die Installation einer neuen Datenbank während einer IBM Spectrum Protect-Installation benötigt wird. Der IBM Spectrum Protect-Installationsassistent zeigt an, wie viel Speicherplatz für die Installation des Fixpacks benötigt wird und wie viel Platz zur Verfügung steht. Wenn der erforderliche Speicherplatz größer ist als der verfügbare Speicherplatz, stoppt die Installation. Wenn die Installation stoppt, fügen Sie dem Dateisystem den erforderlichen Plattenspeicherplatz hinzu und starten Sie die Installation erneut.
7. Laden Sie die Paketdatei für das Fixpack bzw. den vorläufigen Fix, das bzw. der installiert werden soll, über IBM Support Portal, Passport Advantage oder Fix Central herunter.
8. Windows-BetriebssystemeWechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet. Klicken Sie dann entweder doppelt auf die folgende ausführbare Datei oder geben Sie den folgenden Befehl in die Befehlszeile ein, um die Installationsdateien zu extrahieren.
   Tipp: Die Dateien werden in das aktuelle Verzeichnis extrahiert. Stellen Sie sicher, dass sich die ausführbare Datei in dem Verzeichnis befindet, in dem sich die extrahierten Dateien befinden sollen.

   ```
   8.x.x.x-IBM-SPSRV-Plattform.exe
   ```

   Hierbei steht *Plattform* für das Betriebssystem, in dem IBM Spectrum Protect installiert werden soll.
9. Wählen Sie eine der folgenden Möglichkeiten für die Installation von IBM Spectrum Protect aus.
   Wichtig: Nach der Installation eines Fixpacks muss die Konfiguration nicht wiederholt werden. Sie können nach Beendigung der Installation stoppen, alle Fehler beheben und dann Ihre Server erneut starten.
   Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden:

Installationsassistent
: Befolgen Sie die Anweisungen für Ihr Betriebssystem:
Windows: IBM Spectrum Protect mit dem Installationsassistenten installieren

Tipp: Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Aktualisieren. Klicken Sie nicht auf das Symbol Installieren oder Ändern.

Befehlszeile im Konsolenmodus
: Befolgen Sie die Anweisungen für Ihr Betriebssystem:
Windows: IBM Spectrum Protect im Konsolenmodus installieren

Unbeaufsichtigter Modus
: Befolgen Sie die Anweisungen für Ihr Betriebssystem:
Windows: IBM Spectrum Protect im unbeaufsichtigten Modus installieren

Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, führen Sie den Installationsassistenten nur einmal aus. Der Installationsassistent führt ein Upgrade aller Serverinstanzen durch.

Ergebnisse

Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf Datei > Protokoll anzeigen. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:

- Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\logs
- WindowsWindows: Fixpack auf IBM Spectrum Protect 8.1.2 in einer Clusterumgebung unter Windows anwenden
  Damit neue Produktfunktionen genutzt werden können, können Sie ein Upgrade eines Servers, der unter einem Windows-Betriebssystem in einer Clusterumgebung installiert ist, von Version 6.3 oder Version 7.1 auf IBM Spectrum Protect Version 8.1.2 durchführen.

Windows: Von Version 8.1.2 auf eine vorherige Serverversion zurücksetzen

Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.

Vorbereitende Schritte

Sie benötigen die folgenden Elemente aus der früheren Version des Servers:

- Serverdatenbanksicherung
- Protokolldatei für Datenträger
- Einheitenkonfigurationsdatei
- Serveroptionsdatei

Informationen zu diesem Vorgang

Die Anweisungen sind für das Zurücksetzen innerhalb eines Releases oder von einem Release auf ein vorheriges Release identisch, z. B. von 8.1.2 auf 8.1.1 oder von 8.1.2 auf 7.1.2. Die ältere Version muss mit der Version übereinstimmen, die Sie vor dem Upgrade auf Version 8.1 verwendet haben.

Achtung: Geben Sie den Parameter REUSEDELAY an, um den Verlust von Daten des Clients für Sichern/Archivieren verhindern zu helfen, wenn Sie den Server auf eine vorherige Version zurücksetzen.

- WindowsWindows: Zurücksetzen auf vorherige Serverversion in einer Clusterkonfiguration
  Wenn Sie nach einem Upgrade auf die vorherige Version des Servers zurücksetzen müssen, benötigen Sie eine Datenbankgesamtsicherung der ursprünglichen Version. Außerdem benötigen Sie die Serverinstallationsmedien für Ihre ursprüngliche Version und Schlüsselkonfigurationsdateien. Führen Sie die Schritte zur Vorbereitung sorgfältig aus, bevor Sie das Upgrade des Servers durchführen. Dadurch könnte das Zurücksetzen auf die vorherige Version des IBM Spectrum Protect-Servers mit minimalem Datenverlust möglich sein.

Vorgehensweise beim Zurücksetzen auf vorherige Serverversion

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte auf dem System aus, auf dem sich der Server der Version 8.1 befindet.

Vorgehensweise

1. Stoppen Sie den Server, um alle Serveroperationen zu beenden. Verwenden Sie hierfür den Befehl HALT.
2. Entfernen Sie die Datenbank aus dem Datenbankmanager und löschen Sie anschließend die Datenbank- und Wiederherstellungsprotokollverzeichnisse.
   a. Entfernen Sie die Datenbank manuell. Eine Möglichkeit zum Entfernen ist der folgende Befehl:  Windows-Betriebssysteme

      ```
      dsmserv -k Instanzname removedb tsmdb1
      ```

   b. Wenn Sie den von den Datenbank- und Wiederherstellungsprotokollverzeichnissen belegten Speicherplatz wiederverwenden müssen, können Sie diese Verzeichnisse jetzt löschen.
3. Deinstallieren Sie den Server der Version 8.1 mit dem Deinstallationsprogramm. Bei der Deinstallation werden der Server und der Datenbankmanager mit den jeweiligen Verzeichnissen entfernt. Ausführliche Informationen siehe Windows: IBM Spectrum Protect deinstallieren.
4. Stoppen Sie den Clusterdienst. Installieren Sie die Version des Serverprogramms, die Sie vor dem Upgrade auf Version 8.1.2 verwendet haben, erneut. Diese Version muss mit der Version übereinstimmen, die auf Ihrem Server verwendet wurde, als Sie die Datenbanksicherung erstellt haben, die Sie zu einem späteren Zeitpunkt wiederherstellen wollen. Wenn der Server vor dem Upgrade z. B. die Version 7.1.7 hatte und wenn Sie die Datenbanksicherung verwenden wollen, die auf diesem Server verwendet wurde, müssen Sie das Fixpack V7.1.7 installieren, damit Sie die Datenbanksicherung zurückschreiben können.
5. Konfigurieren Sie die neue Serverdatenbank mithilfe des Konfigurationsassistenten. Geben Sie den folgenden Befehl aus, um den Assistenten zu starten:  Windows-Betriebssysteme

   ```
   /dsmicfgx
   ```

6. Stellen Sie sicher, dass keine Server im Hintergrund ausgeführt werden.
7. Schreiben Sie die Datenbank zu einem Zeitpunkt vor dem Upgrade zurück.
8. Kopieren Sie die folgenden Dateien in das Instanzverzeichnis.
   - Einheitenkonfigurationsdatei
   - Protokolldatei für Datenträger
   - Serveroptionsdatei (normalerweise dsmserv.opt)
9. Wenn Sie die Datendeduplizierung für Speicherpools des Typs FILE, die vor dem Upgrade vorhanden waren, aktiviert haben oder wenn Sie während der Verwendung des Servers der Version 8.1.2 Daten, die vor dem Upgrade vorhanden waren, in neue Speicherpools verschoben haben, müssen Sie zusätzliche Schritte ausführen. Weitere Informationen finden Sie in Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung.
10. Wenn die Einstellung des Parameters REUSEDELAY für Speicherpools das Alter der zurückgeschriebenen Datenbank unterschreitet, schreiben Sie Datenträger auf allen Speicherpools mit sequenziellem Zugriff, die nach dieser Datenbanksicherung wiederhergestellt wurden, zurück. Verwenden Sie den Befehl RESTORE VOLUME.
    Wenn keine Sicherung eines Speicherpools vorliegt, prüfen Sie die wiederhergestellten Datenträger mit dem Befehl AUDIT VOLUME und dem Parameter FIX=YES, um Inkonsistenzen zu beheben. Beispiel:

    ```
    audit volume Datenträgername fix=yes
    ```

11. Wurden mit dem Server der Version 8.1 Clientsicherungs- oder -archivierungsoperationen ausgeführt, prüfen Sie die Speicherpooldatenträger, auf denen die Daten gespeichert wurden.

Zusätzliche Wiederherstellungsschritte wegen der Erstellung neuer Speicherpools oder der Aktivierung der Datendeduplizierung

Wenn Sie während der Ausführung des Servers mit Version 8.1.2 neue Speicherpools erstellt und/oder die Datendeduplizierung für Speicherpools des Typs FILE aktiviert haben, müssen Sie zusätzliche Schritte ausführen, um die vorherige Serverversion wiederherzustellen.

Vorbereitende Schritte

Für diese Task benötigen Sie eine Gesamtsicherung des Speicherpools, die vor dem Upgrade auf Version 8.1.2 erstellt wurde.

Informationen zu diesem Vorgang

Verwenden Sie diese Informationen, wenn Sie einen oder beide der folgenden Schritte ausgeführt haben, während Ihr Server mit Version 8.1.2 ausgeführt wurde:

- Sie haben die Datendeduplizierungsfunktion für beliebige Speicherpools aktiviert, die vor dem Upgrade auf Version 8.1.2 bereits vorhanden waren. Die Datendeduplizierung ist nur für Speicherpools gültig, die den Einheitentyp FILE verwenden.
- Sie haben neue primäre Speicherpools nach dem Upgrade erstellt *und* Daten, die in anderen Speicherpools gespeichert waren, in die neuen Speicherpools versetzt.

Führen Sie diese Schritte aus, nachdem der Server wieder auf Version 7 zurückgesetzt wurde.

Vorgehensweise

- Schreiben Sie für jeden Speicherpool, für den Sie die Datendeduplizierungsfunktion aktiviert haben, den gesamten Speicherpool mit dem Befehl RESTORE STGPOOL zurück.
- Bestimmen Sie für Speicherpools, die Sie nach dem Upgrade erstellt haben, welche Maßnahme durchzuführen ist. Daten, die aus vorhandenen Speicherpools der Version 8 in die neuen Speicherpools versetzt wurden, gehen möglicherweise verloren, weil die neuen Speicherpools auf Ihrem auf Version 8 zurückgesetzten Server nicht mehr vorhanden sind. Die Wiederherstellungsmaßnahmen sind vom Typ des Speicherpools abhängig:
  - Wurden Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, wurde der von den versetzten Daten belegte Speicherplatz wahrscheinlich wiederverwendet. Daher müssen Sie die ursprünglichen Speicherpools der Version 8 mithilfe der Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.2 erstellt wurden.

    Wurden *keine* Daten aus Speicherpools des Typs DISK der Version 8 in einen neuen Speicherpool versetzt, müssen Sie die Speicherpooldatenträger in diesen Speicherpools des Typs DISK prüfen.

  - Wurden Daten aus Speicherpools mit sequenziellem Zugriff der Version 8 in einen neuen Speicherpool versetzt, sind diese Daten möglicherweise noch vorhanden und sie können eventuell auf Speicherpooldatenträgern auf dem wiederhergestellten Server der Version 8 verwendet werden. Die Daten können verwendbar sein, wenn für den Parameter REUSEDELAY des Speicherpools ein Wert definiert wurde, der die Wiederherstellung verhindert hat, während der Server mit der Version 8.1.2 ausgeführt wurde. Wurden Datenträger wiederhergestellt, während der Server mit der Version 8.1.2 ausgeführt wurde, müssen Sie diese Datenträger aus Speicherpoolsicherungen zurückschreiben, die vor dem Upgrade auf Version 8.1.2 erstellt wurden.

Windows: Referenz: DB2-Befehle für IBM Spectrum Protect-Serverdatenbanken

Verwenden Sie diese Liste als Referenz, wenn der IBM® Support Sie anweist, DB2-Befehle auszugeben.

Zweck

Nach der Installation und Konfiguration von IBM Spectrum Protect mithilfe der Assistenten müssen Sie DB2-Befehle nur selten verwenden. Eine begrenzte Gruppe von DB2-Befehlen, die Sie verwenden bzw. zu deren Verwendung Sie aufgefordert werden könnten, ist in Tabelle 1 aufgelistet. Diese Liste ist nicht umfassend, es handelt sich lediglich um ergänzende Informationen. Es besteht keine Implikation, dass ein IBM Spectrum Protect-Administrator sie täglich oder regelmäßig verwendet. Beispiele einiger Befehle sind angegeben. Ausgabedaten sind nicht enthalten.

Vollständige Erläuterungen zu den hier beschriebenen Befehlen und zu deren Syntax finden Sie in der Produktinformation zu DB2.

Tabelle 1. DB2-Befehle

Befehl	Beschreibung	Beispiel
Windows-Betriebssysteme db2cmd	Windows-BetriebssystemeÖffnet das DB2-Fenster mit dem Befehlszeilenprozessor und initialisiert die DB2-Befehlszeilenumgebung.	Windows-Betriebssysteme DB2-Befehlsfenster öffnen: `db2cmd`
db2icrt	Erstellt DB2-Instanzen im Ausgangsverzeichnis des Instanzeigners. Tipp: Der IBM Spectrum Protect-Konfigurationsassistent erstellt die vom Server und von der Datenbank verwendete Instanz. Nach der Installation und Konfiguration eines Servers mithilfe des Konfigurationsassistenten wird der Befehl db2icrt in der Regel nicht verwendet. Windows-BetriebssystemeDieses Dienstprogramm befindet sich im Verzeichnis DB2PATH\bin. Hierbei steht DB2PATH für das Verzeichnis, in dem die DB2-Kopie installiert ist.	IBM Spectrum Protect-Instanz manuell erstellen (geben Sie den Befehl in einer einzigen Zeile ein): `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u` *`Instanzname Instanzname`*
db2set	Zeigt DB2-Variablen an.	DB2-Variablen auflisten: `db2set`

Befehl	Beschreibung	Beispiel
CATALOG DATABASE	Speichert Informationen zur Speicherposition der Datenbank im Systemdatenbankverzeichnis. Die Datenbank kann sich auf der lokalen Workstation oder auf einem fernen Datenbankpartitionsserver befinden. Der Serverkonfigurationsassistent kümmert sich um jeden Katalog, der zur Verwendung der Serverdatenbank benötigt wird. Führen Sie diesen Befehl nach der Konfiguration und Aktivierung eines Servers nur dann manuell aus, wenn es eine Änderung oder Beschädigung in der Umgebung gibt.	Datenbank katalogisieren: `db2 catalog database tsmdb1`
CONNECT TO DATABASE	Stellt eine Verbindung zu einer angegebenen Datenbank für Befehlszeilenschnittstellenzwecke her.	Eine Verbindung zur IBM Spectrum Protect-Datenbank über eine DB2-Befehlszeilenschnittstelle herstellen: `db2 connect to tsmdb1`

GET DATABASE CONFIGURATION	Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.
	Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.
		Die Konfigurationsdaten für einen Datenbankaliasnamen anzeigen:
		
		`db2 get db cfg for tsmdb1`
		
		Informationen abrufen, um Einstellungen zu überprüfen (z. B. Datenbankkonfiguration, Protokollmodus und Pflege).
		
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück. Wichtig: Dieser Befehl und seine Parameter werden direkt von DB2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.	Konfigurationsdaten für den Datenbankmanager abrufen: `db2 get dbm cfg`

Befehl	Beschreibung	Beispiel
GET HEALTH SNAPSHOT	Ruft die Informationen zum Allgemeinzustand für den Datenbankmanager und seine Datenbanken ab. Die zurückgegebenen Informationen stellen eine Momentaufnahme des Status zum Zeitpunkt der Befehlsausgabe dar. IBM Spectrum Protect überwacht den Status der Datenbank mithilfe der Diagnosemomentaufnahme und anderer Mechanismen, die von DB2 bereitgestellt werden. Es kann vorkommen, dass die Diagnosemomentaufnahme oder andere DB2-Dokumentation anzeigt, dass sich ein Element bzw. eine Datenbankressource im Alertstatus befindet. In einem solchen Fall müssen entsprechende Schritte zur Behebung der Situation in Betracht gezogen werden. IBM Spectrum Protect überwacht die Bedingung und reagiert entsprechend. Nicht alle deklarierten Alerts der DB2-Datenbank haben Maßnahmen zur Folge.	Einen Bericht über Anzeiger des DB2-Diagnosemonitors abrufen: `db2 get health snapshot for database on tsmdb1`

GRANT (Datenbank-berechtigungen)	Erteilt Berechtigungen, die sich auf die gesamte Datenbank beziehen, und keine Zugriffsrechte, die sich auf bestimmte Objekte in der Datenbank beziehen.	Der Benutzer-ID itmuser Zugriffsberechtigung erteilen:
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

RUNSTATS	Aktualisiert statistische Daten zu den Merkmalen einer Tabelle und der zugeordneten Indizes oder Statistiksichten. Zu diesen Merkmalen gehören die Anzahl der Datensätze, die Anzahl der Seiten und die durchschnittliche Datensatzlänge. Soll eine Tabelle angezeigt werden, verwenden Sie dieses Dienstprogramm nach dem Aktualisieren oder Reorganisieren der Tabelle. Eine Sicht muss für die Optimierung aktiviert sein, damit ihre statistischen Daten für die Optimierung einer Abfrage verwendet werden können. Eine für die Optimierung aktivierte Sicht wird als Statistiksicht bezeichnet. Sie können eine Sicht mit der DB2-Anweisung ALTER VIEW für die Optimierung aktivieren. Verwenden Sie das Dienstprogramm RUNSTATS, wenn sich Änderungen zugrunde liegender Tabellen auf die von der Sicht zurückgegebenen Zeilen auswirken. Tipp: Der Server konfiguriert DB2 so, dass der Befehl RUNSTATS nach Bedarf ausgeführt wird.	Statistische Daten für eine einzelne Tabelle aktualisieren. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
Windows-Betriebssysteme set db2instance	Windows-BetriebssystemeLegt fest, welche Instanz für die aktuelle Sitzung gültig ist.	Windows-Betriebssysteme Die gültige Instanz festlegen: `set db2instance=tsminst1`
SET SCHEMA	Ändert den Wert des Sonderregisters CURRENT SCHEMA als Vorbereitung für die direkte Ausgabe von SQL-Befehlen über die DB2-Befehlszeilenschnittstelle. Tipp: Ein Sonderregister ist ein Speicherbereich, den der Datenbankmanager für einen Anwendungsprozess definiert. In diesem Bereich werden Informationen gespeichert, auf die in SQL-Anweisungen verwiesen werden kann.	Das Schema für IBM Spectrum Protect festlegen: `db2 set schema tsmdb1`

Befehl	Beschreibung	Beispiel
START DATABASE MANAGER	Startet die Hintergrundprozesse der aktuellen Datenbankmanagerinstanz. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers. Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.	Den Datenbankmanager starten: `db2start`
STOP DATABASE MANAGER	Stoppt die aktuelle Datenbankmanagerinstanz. Der Datenbankmanager bleibt so lange aktiv, bis er explizit gestoppt wird. Dieser Befehl stoppt die Datenbankmanagerinstanz nicht, wenn Anwendungen mit Datenbanken verbunden sind. Liegen keine Datenbankverbindungen, aber Instanzverbindungen vor, erzwingt der Befehl zunächst das Stoppen der Instanzverbindungen. Dann wird der Datenbankmanager gestoppt. Dieser Befehl inaktiviert außerdem alle ausstehenden Datenbankaktivierungen, bevor der Datenbankmanager gestoppt wird. Dieser Befehl ist auf einem Client nicht gültig. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers. Wichtig: Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.	Den Datenbankmanager stoppen: `db2 stop dbm`

Windows: IBM Spectrum Protect deinstallieren

Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

Vorbereitende Schritte

Führen Sie folgende Schritte aus, bevor Sie IBM Spectrum Protect deinstallieren:

- Führen Sie eine Gesamtsicherung der Datenbank aus.
- Speichern Sie eine Kopie der Datenträgerhistory- und Einheitenkonfigurationsdateien.
- Bewahren Sie die Ausgabedatenträger an einem sicheren Ort auf.

Windows-BetriebssystemeAchtung: Verwenden Sie nicht das Tool zum Hinzufügen/Entfernen von Programmen in der Windows-Systemsteuerung, um IBM Spectrum Protect zu deinstallieren. Verwenden Sie nur die in diesem Abschnitt beschriebene Deinstallationsprozedur.

Informationen zu diesem Vorgang

Sie können IBM Spectrum Protect mit jeder der folgenden Methoden deinstallieren: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

- Windows: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren
  Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.
- Windows: IBM Spectrum Protect im Konsolenmodus deinstallieren
  Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.
- Windows: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren
  Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.
- Windows: IBM Spectrum Protect deinstallieren und erneut installieren
  Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.
- Windows: IBM Installation Manager deinstallieren
  Sie können IBM Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

Nächste Schritte

Die Vorgehensweise für die Reinstallation der IBM Spectrum Protect-Komponenten finden Sie in Windows: Serverkomponenten installieren.

Windows: IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren

Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM® Installation Manager deinstallieren.

Vorgehensweise

1. Starten Sie Installation Manager.

   Windows-BetriebssystemeÖffnen Sie Installation Manager über das Menü Start.

2. Klicken Sie auf Deinstallieren.
3. Wählen Sie IBM Spectrum Protect-Server aus und klicken Sie auf Weiter.
4. Klicken Sie auf Deinstallieren.
5. Klicken Sie auf Fertigstellen.

Windows: IBM Spectrum Protect im Konsolenmodus deinstallieren

Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.

Vorgehensweise

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
   - Windows-Betriebssystemeeclipse\tools

   Beispiel:

   - Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\eclipse\tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus:
   - Windows-Betriebssysteme`imcl.exe -c`
3. Für die Deinstallation geben Sie `5` ein.
4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
5. Geben Sie `N` für 'Next' (Weiter) ein.
6. Wählen Sie die Deinstallation des IBM Spectrum Protect-Serverpakets aus.
7. Geben Sie `N` für 'Next' (Weiter) ein.
8. Geben Sie `U` für 'Uninstall' (Deinstallieren) ein.
9. Geben Sie `F` für 'Finish' (Fertigstellen) ein.

Windows: IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren

Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

Vorbereitende Schritte

Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation der IBM Spectrum Protect-Serverkomponenten mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, uninstall_response_sample.xml, im Verzeichnis input, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie alle IBM Spectrum Protect-Komponenten deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für jede Komponente in der Antwortdatei unverändert. Wenn Sie eine Komponente nicht deinstallieren wollen, geben Sie den Wert `modify="true"` an.

Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:
   - Windows-Betriebssystemeeclipse\tools

   Beispiel:

   - Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\eclipse\tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:
   Windows-Betriebssysteme

   ```
   imcl.exe -input Antwortdatei -silent
   ```

   Der folgende Befehl ist ein Beispiel:

   Windows-Betriebssysteme

```
imcl.exe -input C:\tmp\input\uninstall_response.xml -silent
```

Windows: IBM Spectrum Protect deinstallieren und erneut installieren

Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um IBM Spectrum Protect manuell zu deinstallieren und erneut zu installieren:

1.  Erstellen Sie eine Liste Ihrer aktuellen Serverinstanzen, bevor Sie mit der Deinstallation beginnen. Führen Sie den folgenden Befehl aus:

   ```
   db2ilist
   ```

2. Führen Sie die folgenden Befehle für jede Serverinstanz aus:
   

   ```
   db2 attach to server1
   db2 get dbm cfg show detail
   db2 detach
   ```

   Notieren Sie den Datenbankpfad für jede Instanz.
3. Deinstallieren Sie IBM Spectrum Protect. Siehe Windows: IBM Spectrum Protect deinstallieren.

    Überprüfen Sie nach der Deinstallation von IBM Spectrum Protect über Systemsteuerung > Software, ob IBM Spectrum Protect DB2 deinstalliert ist.

4. Wenn Sie eine beliebige unterstützte Version von IBM Spectrum Protect deinstallieren (einschließlich Fixpack), wird eine Instanzdatei erstellt. Die Instanzdatei wird erstellt, um die Reinstallation von IBM Spectrum Protect zu erleichtern. Überprüfen Sie diese Datei und verwenden Sie die Informationen, wenn Sie bei der Reinstallation zur Eingabe der Berechtigungsnachweise der Instanz aufgefordert werden. Bei der unbeaufsichtigten Installation geben Sie diese Berechtigungsnachweise mit der Variablen `INSTANCE_CRED` an.
   Sie finden die Instanzdatei an der folgenden Position:
   -  `C:\ProgramData\IBM\Tivoli\TSM\instanceList.obj` im Installationsverzeichnis des IBM Spectrum Protect-Servers
5. Installieren Sie IBM Spectrum Protect erneut. Siehe Windows: Serverkomponenten installieren.

   Ist die Datei `instanceList.obj` nicht vorhanden, müssen Sie Ihre Serverinstanzen wie folgt erneut erstellen:

   a. Erstellen Sie Ihre Serverinstanzen erneut. Siehe Windows: Serverinstanz erstellen.
      Tipp: Der Installationsassistent konfiguriert die Serverinstanzen, Sie müssen jedoch überprüfen, ob sie vorhanden sind. Wenn sie nicht vorhanden sind, müssen Sie sie manuell konfigurieren.
   b. Katalogisieren Sie die Datenbank. Melden Sie sich bei jeder Serverinstanz nacheinander als Instanzbenutzer an und geben Sie folgende Befehle aus:


      ```
      set db2instance=server1
      db2 catalog database tsmdb1
      db2 attach to server1
      db2 update dbm cfg using dftdbpath Instanzlaufwerk
      db2 detach
      ```

   c. Überprüfen Sie, ob IBM Spectrum Protect die Serverinstanz erkennt, indem Sie Ihre Verzeichnisse auflisten. Ihr Ausgangsverzeichnis wird angezeigt, wenn Sie es nicht geändert haben. Ihr Instanzverzeichnis wird angezeigt, wenn Sie den Konfigurationsassistenten verwendet haben. Geben Sie den folgenden Befehl aus:

      ```
      db2 list database directory
      ```

      Wenn Sie TSMDB1 in der Liste finden, können Sie den Server starten.

Windows: IBM Installation Manager deinstallieren

Sie können IBM® Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

Vorbereitende Schritte

Bevor Sie IBM Installation Manager deinstallieren, müssen Sie sicherstellen, dass alle mit IBM Installation Manager installierten Pakete deinstalliert sind. Schließen Sie IBM Installation Manager, bevor Sie den Deinstallationsprozess starten.

Windows-BetriebssystemeKlicken Sie auf Start > Alle Programme > IBM Installation Manager > Installierte Pakete anzeigen.

Vorgehensweise

Gehen Sie wie folgt vor, um IBM Installation Manager zu deinstallieren:

Windows-Betriebssysteme

1. Klicken Sie im Menü Start auf Systemsteuerung > Programme und Funktionen.
2. Wählen Sie IBM Installation Manager aus und klicken Sie auf Deinstallieren.

Upgrade auf Version 8.1 durchführen

Führen Sie ein Upgrade des IBM Spectrum Protect-Servers auf Version 8.1.2 durch, damit neue Produktfunktionen und Aktualisierungen genutzt werden können.

Vorbereitende Schritte

Führen Sie das Upgrade des IBM Spectrum Protect-Servers vor der Aktualisierung der Clients durch. Weitere Informationen finden Sie in:

AIX-BetriebssystemeWas Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten

Linux-BetriebssystemeWas Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten

Windows-BetriebssystemeWas Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten

Informationen zu diesem Vorgang

Informationen zum Upgrade des Servers auf demselben Betriebssystem finden Sie in den Upgradeanweisungen. Anweisungen zur Migration des Servers in ein anderes Betriebssystem finden Sie in IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions.

Tabelle 1. Upgradeanweisungen

Upgrade von Version	Auf Version	Siehe
Version 8.1	Version 8.1, Fixpack oder vorläufiger Fix	AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
Version 7.1	Version 8.1	Server installieren und Upgrade prüfen
Version 7.1	Version 8.1, Fixpack oder vorläufiger Fix	AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
Version 5.5, 6.2 oder 6.3	Version 8.1	IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions

Ein Upgrade von Version 7 auf Version 8.1 dauert ca. 20 - 50 Minuten. Die Ergebnisse in Ihrer Umgebung können von den im Labor erzielten Ergebnissen abweichen.

Informationen zu Upgrades in einer Clusterumgebung finden Sie in Server-Upgrade in einer Clusterumgebung durchführen.

Soll nach einem Upgrade oder einer Migration auf eine frühere Version des Servers zurückgesetzt werden, benötigen Sie eine Datenbankgesamtsicherung und die Installationssoftware für den ursprünglichen Server. Sie benötigen außerdem die folgenden Schlüsselkonfigurationsdateien:

- Protokolldatei für Datenträger
- Einheitenkonfigurationsdatei
- Serveroptionsdatei

- Upgrade auf Version 8.1 durchführen
  Von Version 7.1 auf Version 8.1 ist ein direktes Upgrade des Servers möglich. Sie müssen Version 7.1 nicht deinstallieren.
- Server-Upgrade in einer Clusterumgebung durchführen
  Sie müssen Vorbereitungs- und Installationstasks ausführen, um ein Upgrade eines Servers auf Version 8.1.2 in einer Clusterumgebung durchzuführen. Die Vorgehensweise ist vom Betriebssystem und vom Release abhängig.
- Windows-BetriebssystemeGSKit Version 7 nach einem Upgrade auf IBM Spectrum Protect Version 8.1.2 entfernen
  Der IBM Spectrum Protect-Installationsassistent führt ein Upgrade für GSKit Version 8 und höher durch. GSKit Version 7 wird nicht entfernt oder aktualisiert, wenn Sie ein Upgrade auf IBM Spectrum Protect Version 8.1.2 durchführen, auch wenn GSKit mit einer früheren Version von IBM Spectrum Protect installiert wurde.

Zugehörige Informationen:
IBM Spectrum Protect-Upgrade- und -Migrationsprozess - Häufig gestellte Fragen

Upgrade auf Version 8.1 durchführen

Von Version 7.1 auf Version 8.1 ist ein direktes Upgrade des Servers möglich. Sie müssen Version 7.1 nicht deinstallieren.

Vorbereitende Schritte

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease der Server, für das Sie ein Upgrade durchführen wollen, vorhanden sind. Wenn Sie die Serverkomponenten von DVD installiert haben, stellen Sie sicher, dass die DVD verfügbar ist. Wenn Sie die Serverkomponenten über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.
Tipp: Bei Version 8.1 und höher sind DVDs nicht mehr verfügbar.

Vorgehensweise

Führen Sie folgende Tasks aus, um ein Upgrade des Servers auf Version 8.1 durchzuführen:

- Planung des Upgrades
  Bevor Sie ein Upgrade des Servers von Version 7.1 auf Version 8.1 durchführen, müssen Sie die relevanten Planungsinformationen lesen, z. B. die Systemvoraussetzungen und die Releaseinformationen. Dann wählen Sie einen geeigneten Zeitpunkt für das Systemupgrade aus, um die Auswirkung auf den Produktionsbetrieb so gering wie möglich zu halten.
- Vorbereitung des Systems
  Um das System für das Upgrade von Version 7.1 auf Version 8.1 vorzubereiten, müssen Sie Informationen zu jeder DB2-Instanz zusammenstellen. Dann sichern Sie die Serverdatenbank, speichern Sie Schlüsselkonfigurationsdateien, brechen Sie Sitzungen ab und stoppen Sie den Server.
- Server installieren und Upgrade prüfen
  Sie müssen den Server der Version Version 8.1 installieren, um den Upgradeprozess des Servers auf Version 8.1 abzuschließen. Dann überprüfen Sie, ob das Upgrade erfolgreich war, indem Sie die Serverinstanz starten.

Planung des Upgrades

Bevor Sie ein Upgrade des Servers von Version 7.1 auf Version 8.1 durchführen, müssen Sie die relevanten Planungsinformationen lesen, z. B. die Systemvoraussetzungen und die Releaseinformationen. Dann wählen Sie einen geeigneten Zeitpunkt für das Systemupgrade aus, um die Auswirkung auf den Produktionsbetrieb so gering wie möglich zu halten.

Informationen zu diesem Vorgang

In Labortests dauerte der Upgradeprozess für den Server von Version 7.1 auf Version 8.1 14 bis 45 Minuten. Die Dauer in Ihrer Umgebung kann abweichen und ist von Ihrer Hardware und Software sowie der Größe der Serverdatenbank abhängig.

Vorgehensweise

1. Überprüfen Sie die Hardware- und Softwarevoraussetzungen:

   AIX-BetriebssystemeSystemvoraussetzungen für AIX-Systeme

   Linux-BetriebssystemeSystemvoraussetzungen für Linux-Systeme

   Windows-BetriebssystemeSystemvoraussetzungen für Windows-Systeme

   Aktuelle Informationen zu den Systemvoraussetzungen finden Sie auf der IBM Spectrum Protect-Unterstützungswebsite unter Technote 1243309.

2. Lesen Sie die Releaseinformationen für Serverkomponenten der Version 8.1 und die Readme-Dateien für Fixpacks für den IBM Spectrum Protect-Server der Version 8.1, die spezielle Anweisungen und Informationen für Ihr Betriebssystem enthalten.
3. Wählen Sie einen geeigneten Zeitpunkt für das Systemupgrade aus, um die Auswirkung auf den Produktionsbetrieb so gering wie möglich zu halten. Die für die Aktualisierung des Systems erforderliche Zeit ist von der Größe der Datenbank und vielen anderen Faktoren abhängig. Wenn Sie den Upgradeprozess starten, können Clients keine Verbindung zum Server herstellen, bis die neue Software installiert ist und alle erforderlichen Lizenzen wieder registriert sind.
4. Wenn Sie ein Upgrade des Servers von Version 6 oder Version 7 auf Version 8.1 durchführen, müssen Sie die System-ID und das Kennwort für die DB2-Instanz des IBM Spectrum Protect-Servers kennen. Diese Berechtigungsnachweise sind für ein Upgrade des Systems erforderlich.

Vorbereitung des Systems

Um das System für das Upgrade von Version 7.1 auf Version 8.1 vorzubereiten, müssen Sie Informationen zu jeder DB2-Instanz zusammenstellen. Dann sichern Sie die Serverdatenbank, speichern Sie Schlüsselkonfigurationsdateien, brechen Sie Sitzungen ab und stoppen Sie den Server.

Vorgehensweise

1. Melden Sie sich bei dem Computer an, auf dem der Server installiert ist.

   AIX-BetriebssystemeLinux-BetriebssystemeStellen Sie sicher, dass Sie mit der Instanzbenutzer-ID angemeldet sind.

   Windows-BetriebssystemeStellen Sie sicher, dass Sie mit der Benutzer-ID mit Administratorberechtigung angemeldet sind, mit der der Server der Version 7.1 installiert wurde.

2. Rufen Sie eine Liste der DB2-Instanzen ab. Geben Sie den folgenden Systembefehl aus:

   AIX-BetriebssystemeLinux-Betriebssysteme

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

   Windows-Betriebssysteme

   ```
   db2ilist
   ```

   Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

   AIX-BetriebssystemeLinux-Betriebssysteme

   ```
   tsminst1
   ```

   Windows-Betriebssysteme

   ```
   SERVER1
   ```

   Stellen Sie sicher, dass jede Instanz einem Server entspricht, der auf dem System aktiv ist.
3. AIX-BetriebssystemeLinux-BetriebssystemeNotieren Sie für jede DB2-Instanz den Standarddatenbankpfad, den tatsächlichen Datenbankpfad, den Datenbanknamen, den Aliasnamen der Datenbank und alle DB2-Variablen, die für die Instanz konfiguriert wurden. Bewahren Sie die Aufzeichnung für spätere Referenzzwecke auf. Diese Informationen werden für die Zurückschreibung der Datenbank der Version 7.1 benötigt.
4. Windows-BetriebssystemeStellen Sie Informationen zu jeder DB2-Instanz zusammen. Notieren Sie den Standarddatenbankpfad, den tatsächlichen Datenbankpfad, den Datenbanknamen, den Aliasnamen der Datenbank und alle DB2-Variablen, die für die Instanz konfiguriert wurden. Bewahren Sie die Aufzeichnung für spätere Referenzzwecke auf. Diese Informationen werden für die Zurückschreibung der Datenbank der Version 7.1 benötigt.
   a. Geben Sie folgenden Systembefehl aus, um das DB2-Befehlsfenster zu öffnen:

      ```
      db2cmd
      ```

   b. Geben Sie den folgenden Systembefehl aus, um die Instanz zu ändern:

      ```
      set DB2INSTANCE=Instanz
      ```

      Instanz gibt die DB2-Instanz an.
   c. Geben Sie den folgenden Systembefehl aus, um den Standarddatenbankpfad der DB2-Instanz abzurufen:

      ```
      db2 get dbm cfg | findstr DFTDBPATH
      ```

      Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

      ```
      Standarddatenbankpfad                       (DFTDBPATH) = D:
      ```

   d. Geben Sie den folgenden Systembefehl aus, um Informationen zu den DB2-Instanzdatenbanken abzurufen:

      ```
      db2 list database directory
      ```

      Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

      ```
      Systemdatenbankverzeichnis

                      Anzahl Einträge im Verzeichnis = 2

                     Eintrag für Datenbank 1:

                      Aliasname der Datenbank              = TSMAL001
                      Datenbankname                        = TSMDB1
                      Knotenname                           = TSMNODE1
                      Release-Level der Datenbank          = d.00
                      Kommentar                            = TSM SERVER DATABASE VIA TCPIP
                      Verzeichniseintragungsart            = Fern
                      Datenbankpartitionsnummer für Katalog= -1
      ```

```
 Hostname des Alternativservers       =
 Portnummer des Alternativservers     =

Eintrag für Datenbank 2:

 Aliasname der Datenbank              = TSMDB1
 Datenbankname                        = TSMDB1
                Lokales Datenbankverzeichnis         = D:
 Release-Level der Datenbank          = d.00
 Kommentar                            =
 Verzeichniseintragungsart            = Indirekt
 Datenbankpartitionsnummer für Katalog= 0
 Hostname des Alternativservers       =
 Portnummer des Alternativservers     =
```

e. Geben Sie den folgenden Systembefehl aus, um die DB2-Instanzvariablen abzurufen:

```
db2set -all
```

Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

```
[e] DB2CODEPAGE=1208
[e] DB2PATH=D:\TSM\db2
[i] DB2_PMODEL_SETTINGS=MAX_BACKGROUND_SYSAPPS:500
[i] DB2_SKIPINSERTED=ON
[i] DB2_KEEPTABLELOCK=OFF
[i] DB2_EVALUNCOMMITTED=ON
[i] DB2_VENDOR_INI=D:\Server1\tsmdbmgr.env
[i] DB2_SKIPDELETED=ON
[i] DB2INSTPROF=C:\ProgramData\IBM\DB2\DB2TSM1
[i] DB2COMM=TCPIP
[i] DB2CODEPAGE=819
[i] DB2_PARALLEL_IO=*
[g] DB2_EXTSECURITY=YES
[g] DB2_COMMON_APP_DATA_PATH=C:\ProgramData

[g] DB2PATH=D:\TSM\db2
[g] DB2INSTDEF=SERVER1
```

5. Stellen Sie mithilfe der Benutzer-ID mit Administratorberechtigung eine Verbindung zum Server her.
6. Sichern Sie die Datenbank mit dem Befehl BACKUP DB. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamtsicherung erstellt wird, ohne geplante Datenbanksicherungen zu unterbrechen. Sie können eine Momentaufnahmesicherung beispielsweise mit dem folgenden Befehl erstellen:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

7. Geben Sie den folgenden Verwaltungsbefehl aus, um die Einheitenkonfigurationsdaten in einem anderen Verzeichnis zu sichern:

   ```
   backup devconfig filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.
   Tipp: Diese Datei wird benötigt, wenn die Datenbank der Version 7.1 zurückgeschrieben werden soll.
8. Sichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis. Geben Sie den folgenden Verwaltungsbefehl aus:

   ```
   backup volhistory filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.
   Tipp: Diese Datei wird benötigt, wenn die Datenbank der Version 7.1 zurückgeschrieben werden soll.
9. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
10. Verhindern Sie Aktivität auf dem Server durch Inaktivierung neuer Sitzungen. Geben Sie die folgenden Verwaltungsbefehle aus:

    ```
    disable sessions client
    disable sessions server
    ```

11. Überprüfen Sie, ob Sitzungen bestehen, und benachrichtigen Sie die Benutzer, dass der Server gestoppt wird. Geben Sie den folgenden Verwaltungsbefehl aus, um auf bestehende Sitzungen zu überprüfen:

    ```
    query session
    ```

12. Geben Sie den folgenden Verwaltungsbefehl aus, um Sitzungen abzubrechen:

    ```
    cancel session all
    ```

    Dieser Befehl bricht alle Sitzungen außer der aktuellen Sitzung ab.
13. Geben Sie den folgenden Verwaltungsbefehl aus, um den Server zu stoppen:

    ```
    halt
    ```

14. Stellen Sie sicher, dass der Server heruntergefahren wird und dass keine Prozesse ausgeführt werden.

AIX-BetriebssystemeLinux-BetriebssystemeGeben Sie den folgenden Befehl aus:

```
ps -ef | grep dsmserv
```

Windows-BetriebssystemeÖffnen Sie die Windows-Anwendung 'Task-Manager' und überprüfen Sie die Liste der aktiven Prozesse.

15. Suchen Sie die Datei NODELOCK im Serverinstanzverzeichnis Ihrer Installation und verschieben Sie sie in ein anderes Verzeichnis, in dem Sie Konfigurationsdateien speichern. Die Datei NODELOCK enthält die vorherigen Lizenzinformationen für Ihre Installation. Diese Lizenzinformationen werden bei Beendigung des Upgrades ersetzt.

Zugehörige Verweise:
BACKUP DB (Datenbank sichern)
BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)
BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)
DISABLE SESSIONS (Verhindern, dass neue Sitzungen auf Tivoli Storage Manager zugreifen)
QUERY SESSION (Clientsitzungen abfragen)
CANCEL SESSION (Clientsitzungen abbrechen)
HALT (Server herunterfahren)

Server installieren und Upgrade prüfen

Sie müssen den Server der Version Version 8.1 installieren, um den Upgradeprozess des Servers auf Version 8.1 abzuschließen. Dann überprüfen Sie, ob das Upgrade erfolgreich war, indem Sie die Serverinstanz starten.

Vorbereitende Schritte

AIX-BetriebssystemeLinux-BetriebssystemeSie müssen mit der Rootbenutzer-ID am System angemeldet sein.

Windows-BetriebssystemeSie müssen mit der Benutzer-ID mit Administratorberechtigung, die für die Installation des Servers der früheren Version verwendet wurde, am System angemeldet sein.

Das Installationspaket kann von einer IBM® Download-Site heruntergeladen werden.

AIX-BetriebssystemeLinux-BetriebssystemeLegen Sie als Systembenutzergrenzwert für die maximale Dateigröße 'unlimited' (unbegrenzt) fest, um sicherzustellen, dass die Dateien ordnungsgemäß heruntergeladen werden können.

1. Führen Sie den folgenden Befehl aus, um den Wert für die maximale Dateigröße abzufragen:

   ```
   ulimit -Hf
   ```

2. Wenn als Systembenutzergrenzwert für die maximale Dateigröße nicht 'unlimited' (unbegrenzt) angegeben ist, geben Sie 'unlimited' gemäß den Anweisungen in der Dokumentation Ihres Betriebssystems an.

Informationen zu diesem Vorgang

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server
  Tipp: Die Datenbank (DB2), Global Security Kit (GSKit) und IBM Java™ Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.
- Sprachen des Servers
- Lizenzen
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

Vorgehensweise

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:
   - Laden Sie das Serverpaket über Passport Advantage oder Fix Central herunter.
   - Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.
2. Führen Sie die folgenden Schritte aus:

   AIX-BetriebssystemeLinux-Betriebssysteme
   AIX-BetriebssystemeLinux-Betriebssysteme
   a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherbedarf finden Sie im Downloaddokument für Ihr Produkt.
      - IBM Spectrum Protect Technote 4042944
      - IBM Spectrum Protect Extended Edition Technote 4042945
      - IBM Spectrum Protect for Data Retention Technote 4042946

b. Laden Sie die Paketdatei in ein beliebiges Verzeichnis herunter. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.

   Stellen Sie außerdem sicher, dass Sie über die Ausführberechtigung für die Paketdatei verfügen.

c. Falls erforderlich, führen Sie den folgenden Befehl aus, um die Dateiberechtigungen zu ändern:

   ```
   chmod a+x Paketname.bin
   ```

   Paketname sieht wie in dem folgenden Beispiel aus:

    AIX-Betriebssysteme

   ```
   8.1.x.000-IBM-SPSRV-AIX.bin
   ```

    Linux-Betriebssysteme

   ```
   8.1.x.000-IBM-SPSRV-Linuxs390x.bin
   8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
   8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
   ```

   In den Beispielen gibt *8.1.x.000* das Release-Level des Produkts an.

d. Führen Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

   ```
   ./Paketname.bin
   ```

   Die Extraktion nimmt etwas Zeit in Anspruch, weil das Paket groß ist.

 Windows-Betriebssysteme

 Windows-Betriebssysteme

a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherbedarf finden Sie im Downloaddokument für Ihr Produkt.
   - IBM Spectrum Protect Technote 4042944
   - IBM Spectrum Protect Extended Edition Technote 4042945
   - IBM Spectrum Protect for Data Retention Technote 4042946

b. Wechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet.
   Tipp: Im nächsten Schritt werden die Dateien in das aktuelle Verzeichnis extrahiert. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.

c. Doppelklicken Sie auf der ausführbaren Datei, um die Installationsdateien zu extrahieren:

   ```
   Paketname.exe
   ```

   Paketname sieht wie in dem folgenden Beispiel aus:

   ```
   8.1.x.000-SPSRV-WindowsX64.exe
   ```

   Die Extraktion nimmt etwas Zeit in Anspruch, weil das Paket groß ist.

3.  AIX-BetriebssystemePrüfen Sie, ob der folgende Befehl aktiviert ist, um sicherzustellen, dass die IBM Spectrum Protect-Assistenten ordnungsgemäß funktionieren:
   -  AIX-Betriebssysteme`lsuser`

   Der Befehl ist standardmäßig aktiviert.
4. Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden. Installieren Sie die IBM Spectrum Protect-Lizenz während des Installationsprozesses.
   Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, installieren Sie die IBM Spectrum Protect-Software nur einmal, um alle Serverinstanzen zu aktualisieren.

   Installationsassistent

    AIX-BetriebssystemeBefolgen Sie die Anweisungen in IBM Spectrum Protect mit dem Installationsassistenten installieren, um den Server mithilfe des grafisch orientierten Assistenten von IBM Installation Manager zu installieren.

    Linux-BetriebssystemeBefolgen Sie die Anweisungen in IBM Spectrum Protect mit dem Installationsassistenten installieren, um den Server mithilfe des grafisch orientierten Assistenten von IBM Installation Manager zu installieren.

    Windows-BetriebssystemeBefolgen Sie die Anweisungen in IBM Spectrum Protect mit dem Installationsassistenten installieren, um den Server mithilfe des grafisch orientierten Assistenten von IBM Installation Manager zu installieren.

   Stellen Sie sicher, dass Ihr System die Voraussetzungen für die Verwendung des Installationsassistenten erfüllt. Führen Sie anschließend die Installationsschritte aus. Klicken Sie im Fenster von IBM Installation Manager auf das Symbol Aktualisieren oder Ändern.

   Server im Konsolenmodus installieren

AIX-BetriebssystemeBefolgen Sie die Anweisungen in Tivoli Storage Manager im Konsolenmodus installieren, um den Server im Konsolenmodus zu installieren.

Linux-BetriebssystemeBefolgen Sie die Anweisungen in Tivoli Storage Manager im Konsolenmodus installieren, um den Server im Konsolenmodus zu installieren.

Windows-BetriebssystemeBefolgen Sie die Anweisungen in Tivoli Storage Manager im Konsolenmodus installieren, um den Server im Konsolenmodus zu installieren.

Lesen Sie die Informationen zur Installation des Servers im Konsolenmodus und führen Sie anschließend die Installationsschritte aus.

Unbeaufsichtigter Modus

AIX-BetriebssystemeBefolgen Sie die Anweisungen in Tivoli Storage Manager im unbeaufsichtigten Modus installieren, um den Server im unbeaufsichtigten Modus zu installieren.

Linux-BetriebssystemeBefolgen Sie die Anweisungen in Tivoli Storage Manager im unbeaufsichtigten Modus installieren, um den Server im unbeaufsichtigten Modus zu installieren.

Windows-BetriebssystemeBefolgen Sie die Anweisungen in Tivoli Storage Manager im unbeaufsichtigten Modus installieren, um den Server im unbeaufsichtigten Modus zu installieren.

Lesen Sie die Informationen zur Installation des Servers im unbeaufsichtigten Modus und führen Sie anschließend die Installationsschritte aus.

Nach der Installation der Software müssen Sie das System nicht rekonfigurieren.

5. Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

   Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf Datei > Protokoll anzeigen. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf Hilfe > Daten zur Fehleranalyse exportieren.

   Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:
   - AIX-BetriebssystemeLinux-Betriebssysteme/var/ibm/InstallationManager/logs
   - Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\logs
6. Rufen Sie das IBM Support Portal auf, um Fixes abzurufen. Klicken Sie auf Fixes, updates, and drivers und legen Sie alle gültigen Fixes an.
7. AIX-BetriebssystemeLinux-BetriebssystemeÜberprüfen Sie, ob das Upgrade erfolgreich war:
   a. Starten Sie die Serverinstanz.

      AIX-BetriebssystemeAnweisungen finden Sie in Serverinstanz starten.

      Linux-BetriebssystemeAnweisungen finden Sie in Serverinstanz starten.

   b. Überwachen Sie die Nachrichten, die der Server bei seinem Start ausgibt. Achten Sie auf Fehlernachrichten und Warnungen und lösen Sie alle Probleme.
   c. Überprüfen Sie, ob Sie mithilfe des Verwaltungsclients eine Verbindung zum Server herstellen können. Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um eine Verwaltungsclientsitzung zu starten:

      ```
      dsmadmc
      ```

   d. Führen Sie QUERY-Befehle aus, um Informationen zum aktualisierten System abzurufen. Führen Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um konsolidierte Informationen zum System abzurufen:

      ```
      query system
      ```

      Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um Informationen zur Datenbank abzurufen:

      ```
      query db format=detailed
      ```

8. Windows-BetriebssystemeÜberprüfen Sie, ob das Upgrade erfolgreich war:
   a. Starten Sie die Serverinstanz. Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um den Server aus dem Standardverzeichnis C:\Programme\Tivoli\TSM zu starten:

      ```
      dsmserv -k Serverinstanz
      ```

      Serverinstanz ist der Name Ihrer Serverinstanz. Server1 ist der Standardname für die erste Instanz des IBM Spectrum Protect-Servers.

      Wenn Sie den Server als Dienst im lokalen Systemkonto ausführen wollen, muss dem lokalen Systemkonto die Zugriffsberechtigung für die Serverdatenbank explizit erteilt werden. Anweisungen finden Sie in Server mit Windows-Diensten starten.

   b. Überwachen Sie die Nachrichten, die der Server bei seinem Start ausgibt. Achten Sie auf Fehlernachrichten und Warnungen und lösen Sie alle Probleme.

c. Überprüfen Sie, ob Sie mithilfe des Verwaltungsclients eine Verbindung zum Server herstellen können. Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um eine Verwaltungsclientsitzung zu starten:

```
dsmadmc
```

d. Führen Sie QUERY-Befehle aus, um Informationen zum aktualisierten System abzurufen. Führen Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um konsolidierte Informationen zum System abzurufen:

```
query system
```

Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um Informationen zur Datenbank abzurufen:

```
query db format=detailed
```

9.  AIX-Betriebssysteme  Linux-BetriebssystemeRegistrieren Sie die Lizenzen für die IBM Spectrum Protect-Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

```
register license file=Installationsverzeichnis/server/bin/Komponentenname.lic
```

Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

Wenn Sie den Server beispielsweise im Standardverzeichnis /opt/tivoli/tsm installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Einschränkung:
Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

10.  Windows-BetriebssystemeRegistrieren Sie die Lizenzen für die Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

```
register license file=Installationsverzeichnis\server\Komponentenname.lic
```

Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

Wenn Sie den Server beispielsweise im Standardverzeichnis c:\Programme\Tivoli\TSM installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

```
register license file=c:\Programme\Tivoli\TSM\server\tsmbasic.lic
```

Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis c:\Programme\Tivoli\TSM installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=c:\Programme\Tivoli\TSM\server\tsmee.lic
```

Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis c:\Programme\Tivoli\TSM installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=c:\Programme\Tivoli\TSM\server\dataret.lic
```

Einschränkung:
Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

11. Optional: Für die Installation eines zusätzlichen Sprachenpakets verwenden Sie die Funktion 'Ändern' von IBM Installation Manager.

12. Optional: Für ein Upgrade auf eine neuere Version eines Sprachenpakets verwenden Sie die Funktion 'Aktualisieren' von IBM Installation Manager.

Nächste Schritte

Sie können Kennwörter im LDAP-Verzeichnisserver oder im IBM Spectrum Protect-Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.

 Ist unter Windows ein Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den Einheitentreiber. Ist unter Windows kein Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls `dpinst.exe /a`. Die Datei `dpinst.exe` befindet sich im Verzeichnis des Einheitentreibers. Das Standardverzeichnis ist C:\Programme\Tivoli\TSM\device\drivers.

Zugehörige Verweise:
QUERY SYSTEM (Systemkonfiguration und Kapazität abfragen)
QUERY DB (Datenbankinformationen anzeigen)
REGISTER LICENSE (Neue Lizenz registrieren)


Server-Upgrade in einer Clusterumgebung durchführen

Sie müssen Vorbereitungs- und Installationstasks ausführen, um ein Upgrade eines Servers auf Version 8.1.2 in einer Clusterumgebung durchzuführen. Die Vorgehensweise ist vom Betriebssystem und vom Release abhängig.

Vorgehensweise

Führen Sie die Schritte für Ihr Betriebssystem, Quellenrelease und Zielrelease aus:


Tabelle 1. Prozeduren für ein Upgrade des Servers in einer Clusterumgebung in einem AIX-Betriebssystem

Quellenrelease	Zielrelease	Prozedur
Version 8.1.2	Fixpack für Version 8.1.2	Fixpack auf Version 8 in einer Clusterumgebung unter AIX anwenden
Version 6.3 oder Version 7.1	Version 8.1.2	Upgrade für IBM Spectrum Protect von Version 6.3 oder Version 7.1 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen Upgrade von Version 6.3 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen
Version 6.1	Version 8.1.2	IBM Spectrum Protect-Upgrade von Version 6.1 auf Version 8.1.2 in einer Clusterumgebung unter AIX durchführen
Version 5	Version 7.1.1 oder höher	Upgrade für den Server auf Version 7.1.1 in einer AIX-Clusterumgebung durchführen

Tabelle 2. Prozeduren für ein Upgrade des Servers in einer Clusterumgebung in einem Linux-Betriebssystem

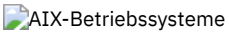
Quellenrelease	Zielrelease	Prozedur
Version 6 oder Version 7	Version 8.1.2	Upgrade für einen Server durchführen, der mit Tivoli System Automation konfiguriert ist

Tabelle 3. Prozeduren für ein Upgrade des Servers in einer Clusterumgebung in einem Windows-Betriebssystem

Quellenrelease	Zielrelease	Prozedur
Version 8.1.2	Fixpack für Version 8.1.2	Fixpack auf Version 8 in einer Clusterumgebung unter Windows anwenden
Version 6.3 oder Version 7.1	Version 8.1.2	Upgrade von Version 6.3 oder Version 7.1 auf Version 8.1 in einer Clusterumgebung unter Windows durchführen
Version 6.1	Version 8.1.2	Upgrade von Version 6.1 auf Version 8.1 in einer Clusterumgebung unter Windows durchführen
Version 5	Version 7.1 oder höher	Upgrade des Servers auf Version 7.1 oder höher in einer Windows-Clusterumgebung durchführen

- Upgrade für IBM Spectrum Protect von Version 6.3 oder Version 7.1 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen
  Sie können ein Upgrade des IBM Spectrum Protect-Servers von Version 6.3 oder Version 7.1 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen. Auf diese Weise können Sie die neuen Funktionen in IBM Spectrum Protect Version 8.1.2 nutzen.

- Upgrade von Version 6.3 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen
  Sie können ein Upgrade des Servers von Version 6.3 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen. Auf diese Weise können Sie die neuen Funktionen in Version 8.1.2 nutzen.
- IBM Spectrum Protect-Upgrade von Version 6.1 auf Version 8.1.2 in einer Clusterumgebung unter AIX durchführen
  Sie können ein Upgrade des IBM Spectrum Protect-Servers unter AIX von Version 6.1 auf Version 8.1.2 in einer Clusterumgebung durchführen. Nach dem Upgrade können Sie die neuen Funktionen in Version 8.1.2 nutzen.
- IBM Spectrum Protect-Upgrade auf Version 8.1.2 in einer Clusterumgebung unter Linux durchführen
  Damit neue Funktionen in IBM Spectrum Protect genutzt werden können, können Sie ein Upgrade des IBM Spectrum Protect-Servers, der unter einem Linux-Betriebssystem in einer Clusterumgebung installiert ist, durchführen.
- Upgrade eines Servers der Version 6.3 oder Version 7.1 auf Version 8.1.2 in einer Clusterumgebung unter Windows durchführen
  Damit neue Produktfunktionen genutzt werden können, können Sie ein Upgrade eines Servers, der unter einem Windows-Betriebssystem in einer Clusterumgebung installiert ist, von Version 6.3 oder Version 7.1 auf IBM Spectrum Protect Version 8.1.2 durchführen.
- IBM Tivoli Storage Manager-Upgrade von Version 6.1 auf IBM Spectrum Protect Version 8.1.2 in einer Clusterumgebung unter Windows durchführen
  Damit neue Funktionen genutzt werden können, können Sie ein Upgrade eines Servers, der unter einem Windows-Betriebssystem in einer Clusterumgebung installiert ist, von Version 6.1 auf Version 8.1.2 durchführen.



Upgrade für IBM Spectrum Protect von Version 6.3 oder Version 7.1 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen

Sie können ein Upgrade des IBM Spectrum Protect-Servers von Version 6.3 oder Version 7.1 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen. Auf diese Weise können Sie die neuen Funktionen in IBM Spectrum Protect Version 8.1.2 nutzen.

Vorbereitende Schritte

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des Servers der Version 6.3 oder Version 7.1, für das Sie ein Upgrade durchführen wollen, vorhanden sind. Wenn Sie IBM Spectrum Protect von DVD installiert haben, stellen Sie sicher, dass die DVD verfügbar ist. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, müssen Sie die Lizenz von den Installationsmedien des Serverbasisrelease erneut installieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, wenn das DB2-Instanzverzeichnis von den Knoten im Cluster gemeinsam genutzt wird. Das DB2-Instanzverzeichnis befindet sich an der folgenden Position:

```
/home/tsminst1/sqllib
```

Wenn das DB2-Instanzverzeichnis von den Knoten nicht gemeinsam genutzt wird, führen Sie die Anweisungen in Upgrade von Version 6.3 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen aus.

Vorgehensweise

1. Sichern Sie die Datenbank mit dem Befehl BACKUP DB. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamtsicherung erstellt wird, ohne geplante Sicherungen zu unterbrechen. Sie können eine Momentaufnahmesicherung beispielsweise mit dem folgenden Befehl erstellen:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Führen Sie den folgenden Befehl aus, um die Einheitenkonfigurationsdaten in einem anderen Verzeichnis zu sichern:

   ```
   backup devconfig filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.
3. Führen Sie den folgenden Befehl aus, um die Protokolldatei für Datenträger in einem anderen Verzeichnis zu sichern:

   ```
   backup volhistory filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Datenträgerprotokolldaten gespeichert werden sollen.
4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt und sich im Serverinstanzverzeichnis befindet.
5. Stoppen Sie alle Instanzen des Servers. Stellen Sie sicher, dass keine Serverprozesse ausgeführt werden. Wenn Sie die Überwachung auf Anwendungsebene für den IBM Spectrum Protect-Server verwenden, setzen Sie die Überwachung der dsmserv-Anwendungsressource mit Ihrem Cluster-Tool aus.
6. Stellen Sie sicher, dass der Datenbankmanager auf keiner Instanz ausgeführt wird. Stellen Sie fest, ob db2sysc-Prozesse ausgeführt werden. Der Eigner aktiver Prozesse zeigt an, welche Instanzen aktiv sind. Führen Sie für jeden Serverinstanzeigner den folgenden Befehl

aus, um DB2 zu stoppen:

```
db2stop
```

7. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.2 auf dem primären Knoten. Führen Sie hierfür den Befehl ./install.sh aus. Anweisungen finden Sie in Serverkomponenten installieren. Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Installieren. Klicken Sie nicht auf das Symbol Aktualisieren oder Ändern.
8. Starten Sie jeden Server der Version 8.1.2 im Vordergrund:
   a. Stellen Sie sicher, dass Sie mit der Instanzeigner-ID angemeldet sind.
   b. Navigieren Sie zum Instanzverzeichnis und führen Sie den folgenden Befehl aus:

      ```
      /opt/tivoli/tsm/server/bin/dsmserv
      ```

      Warten Sie, bis die Eingabeaufforderung des Servers angezeigt wird, was bedeutet, dass der Server gestartet wurde.

9. Stoppen Sie den Server für jede IBM Spectrum Protect-Instanz, die aktualisiert wird. Geben Sie den folgenden Befehl aus:

   ```
   halt
   ```

   Tipp: Weil das DB2-Instanzverzeichnis von den Knoten im Cluster gemeinsam genutzt wird, müssen Sie die gemeinsam genutzten Ressourcen nicht auf den sekundären Knoten im Cluster verschieben.
10. Führen Sie auf jedem sekundären Knoten im Cluster die folgenden Schritte aus:
    a. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.2 mit dem Befehl ./install.sh. Anweisungen finden Sie in Serverkomponenten installieren.
       i. Wenn Sie den Installationsassistenten ausführen, klicken Sie im Fenster von IBM Installation Manager auf das Symbol Installieren. Klicken Sie nicht auf das Symbol Aktualisieren oder Ändern.
       ii. Wenn Sie den Installationsassistenten ausführen, wählen Sie im Fenster Instanzberechtigungsnachweise das Kontrollkästchen Diese Instanz aktualisieren für jede Instanz ab.
       iii. Wenn Sie den Server im Konsolenmodus installieren, geben Sie an der Eingabeaufforderung `Soll diese Instanz aktualisiert werden?` für jede Instanz `Nein` ein.
       iv. Wenn Sie den Server im unbeaufsichtigten Modus installieren, geben Sie `FALSE` als Wert der Variablen `user.`*`Instanzname`*`_update` für jede Instanz an.
    b. Stellen Sie sicher, dass jeder IBM Spectrum Protect-Server der Version 8.1.2 startet. Wenn Sie die Überwachung auf Anwendungsebene verwenden, starten Sie den Server mithilfe des Cluster-Tools.

       Anweisungen zum Starten des Servers finden Sie in Serverinstanz starten.

11. Registrieren Sie die Lizenzen für die Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

    ```
    register license file=Installationsverzeichnis/server/bin/Komponentenname.lic
    ```

    Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

    Wenn Sie den Server beispielsweise im Standardverzeichnis /opt/tivoli/tsm installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
    ```

    Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
    ```

    Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:

    ```
    register license file=/opt/tivoli/tsm/server/bin/dataret.lic
    ```

    Einschränkung:
    Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:
    - IBM Spectrum Protect for Mail
    - IBM Spectrum Protect for Databases
    - IBM Spectrum Protect for ERP
    - IBM Spectrum Protect for Space Management

    Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

Zugehörige Verweise:
BACKUP DB (Datenbank sichern)
BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)
BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)
HALT (Server herunterfahren)
REGISTER LICENSE (Neue Lizenz registrieren)

Upgrade von Version 6.3 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen

Sie können ein Upgrade des Servers von Version 6.3 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit separaten Datenbankinstanzen durchführen. Auf diese Weise können Sie die neuen Funktionen in Version 8.1.2 nutzen.

Vorbereitende Schritte

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des Servers der Version 6.3 oder Version 7.1, für das Sie ein Upgrade durchführen wollen, vorhanden sind. Wenn Sie IBM Spectrum Protect von DVD installiert haben, stellen Sie sicher, dass die DVD verfügbar ist. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, müssen Sie die Lizenz von den Installationsmedien des Serverbasisrelease erneut installieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, wenn das DB2-Instanzverzeichnis von den Knoten im Cluster nicht gemeinsam genutzt wird. Das DB2-Instanzverzeichnis befindet sich an der folgenden Position:

```
/home/tsminst1/sqllib
```

Wenn das DB2-Instanzverzeichnis von den Knoten im Cluster gemeinsam genutzt wird, führen Sie die Anweisungen in Upgrade für IBM Spectrum Protect von Version 6.3 oder Version 7.1 auf Version 8.1.2 in einer Clusterumgebung unter AIX mit einer gemeinsam genutzten Datenbankinstanz durchführen aus.

Vorgehensweise

1. Sichern Sie die Datenbank mit dem Befehl BACKUP DB. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamtsicherung erstellt wird, ohne geplante Sicherungen zu unterbrechen. Sie können eine Momentaufnahmesicherung beispielsweise mit dem folgenden Befehl erstellen:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Führen Sie den folgenden Befehl aus, um die Einheitenkonfigurationsdaten in einem anderen Verzeichnis zu sichern:

   ```
   backup devconfig filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.
3. Führen Sie den folgenden Befehl aus, um die Protokolldatei für Datenträger in einem anderen Verzeichnis zu sichern:

   ```
   backup volhistory filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Datenträgerprotokolldaten gespeichert werden sollen.
4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt und sich im Serverinstanzverzeichnis befindet.
5. Stoppen Sie alle Instanzen des Servers. Stellen Sie sicher, dass keine Serverprozesse ausgeführt werden. Wenn Sie die Überwachung auf Anwendungsebene für den IBM Spectrum Protect-Server verwenden, setzen Sie die Überwachung der dsmserv-Anwendungsressource mit Ihrem Cluster-Tool aus.
6. Stellen Sie sicher, dass der Datenbankmanager auf keiner Instanz ausgeführt wird. Stellen Sie fest, ob db2sysc-Prozesse ausgeführt werden. Der Eigner aktiver Prozesse zeigt an, welche Instanzen aktiv sind. Führen Sie für jeden Serverinstanzeigner den folgenden Befehl aus, um DB2 zu stoppen:

   ```
   db2stop
   ```

7. Stellen Sie sicher, dass sich die gemeinsam genutzten Ressourcen für alle IBM Spectrum Protect-Instanzen auf dem primären Knoten befinden. Stellen Sie sicher, dass keine anderen Knoten Schreibzugriff auf diese Ressourcen während des Upgrades haben. Wenn in der Umgebung mehrere Instanzen des Servers vorhanden sind, muss der primäre Knoten auf gemeinsam genutzte Ressourcen für alle Instanzen zugreifen können.
8. Installieren Sie den Server der Version 8.1.2 auf dem primären Knoten. Führen Sie hierfür den Befehl ./install.sh aus. Anweisungen finden Sie in Serverkomponenten installieren. Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Installieren. Klicken Sie nicht auf das Symbol Aktualisieren oder Ändern. Sie müssen den Server der Version 8.1.2 installieren, um das Upgrade von Version 6.3 auf Version 8.1.2 abzuschließen.
9. Starten Sie jeden Server der Version 8.1.2 im Vordergrund:
   a. Stellen Sie sicher, dass Sie mit der Instanzeigner-ID angemeldet sind.
   b. Navigieren Sie zum Instanzverzeichnis und führen Sie den folgenden Befehl aus:

      ```
      /opt/tivoli/tsm/server/bin/dsmserv
      ```

      Warten Sie, bis die Eingabeaufforderung des Servers angezeigt wird, was bedeutet, dass der Server gestartet wurde.

10. Stoppen Sie den Server für jede IBM Spectrum Protect-Instanz, die aktualisiert wird. Führen Sie den folgenden Befehl aus:

    ```
    halt
    ```

11. Führen Sie auf jedem sekundären Knoten im Cluster die folgenden Schritte aus:
    a. Verschieben Sie alle gemeinsam genutzten Ressource auf den sekundären Knoten. Wenn in der Umgebung mehrere Instanzen des Servers vorhanden sind, müssen die sekundären Knoten während des Upgrades auf gemeinsam genutzte Ressourcen für alle Instanzen zugreifen können.
    b. Stoppen Sie alle Instanzen des Servers. Stellen Sie sicher, dass keine Serverprozesse ausgeführt werden.
    c. Stellen Sie sicher, dass der Datenbankmanager auf keiner Instanz ausgeführt wird. Stellen Sie fest, ob db2sysc-Prozesse ausgeführt werden. Der Eigner aktiver Prozesse zeigt an, welche Instanzen aktiv sind. Führen Sie für jeden Serverinstanzeigner den folgenden Befehl aus, um DB2 zu stoppen:

       ```
       db2stop
       ```

    d. Installieren Sie den Server der Version 8.1.2 mit dem Befehl ./install.sh. Anweisungen finden Sie in Serverkomponenten installieren.
       i. Wenn Sie den Installationsassistenten verwenden, klicken Sie im Fenster von IBM Installation Manager auf das Symbol Installieren. Klicken Sie nicht auf das Symbol Aktualisieren oder Ändern.
       ii. Wenn Sie den Installationsassistenten verwenden, wählen Sie auf der Seite Instanzberechtigungsnachweise das Kontrollkästchen Diese Instanz auf einem sekundären Knoten des Clusters konfigurieren für jede Instanz aus, die Sie konfigurieren wollen.
       iii. Wenn Sie den Server im Konsolenmodus installieren, geben Sie an der Eingabeaufforderung `Diese Instanz auf einem sekundären Knoten des Clusters konfigurieren?` für jede Instanz `Ja` ein.
       iv. Wenn Sie den Server im unbeaufsichtigten Modus installieren, geben Sie `TRUE` als Wert der Variablen `user.`*`Instanzname`*`_secondaryNode` für jede Instanz an.
    e. Stellen Sie sicher, dass jeder Server der Version 8.1.2 startet. Wenn Sie die Überwachung auf Anwendungsebene verwenden, starten Sie den Server mithilfe des Cluster-Tools.

       Anweisungen zum Starten des Servers finden Sie in Serverinstanz starten.

12. Registrieren Sie die Lizenzen für die Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

    ```
    register license file=Installationsverzeichnis/server/bin/Komponentenname.lic
    ```

    Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

    Wenn Sie den Server beispielsweise im Standardverzeichnis /opt/tivoli/tsm installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
    ```

    Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:

    ```
    register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
    ```

    Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:

    ```
    register license file=/opt/tivoli/tsm/server/bin/dataret.lic
    ```

    Einschränkung:
    Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:
    - IBM Spectrum Protect for Mail
    - IBM Spectrum Protect for Databases
    - IBM Spectrum Protect for ERP
    - IBM Spectrum Protect for Space Management

    Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

Zugehörige Verweise:
BACKUP DB (Datenbank sichern)
BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)
BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)
HALT (Server herunterfahren)
REGISTER LICENSE (Neue Lizenz registrieren)
 AIX-Betriebssysteme

IBM Spectrum Protect-Upgrade von Version 6.1 auf Version 8.1.2 in einer Clusterumgebung unter AIX durchführen

Sie können ein Upgrade des IBM Spectrum Protect-Servers unter AIX von Version 6.1 auf Version 8.1.2 in einer Clusterumgebung durchführen. Nach dem Upgrade können Sie die neuen Funktionen in Version 8.1.2 nutzen.

Vorbereitende Schritte

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease der Server der Versionen 6.1 und 6.3 vorhanden sind. Wenn die Server-Software von einer DVD stammt, stellen Sie sicher, dass die DVD verfügbar ist. Wenn die Server-Software von einem heruntergeladenen Paket stammt, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Informationen zu diesem Vorgang

Wenn die Clusterumgebung mehrere Serverinstanzen enthält, verschieben Sie während des Upgrades alle für die Instanzen erforderlichen Ressourcen auf einen einzelnen Clusterknoten, den primären Knoten.

Vorgehensweise

1. Sichern Sie die Datenbank mit dem Befehl BACKUP DB. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamtsicherung erstellt wird, ohne geplante Sicherungen zu unterbrechen. Sie können eine Momentaufnahmesicherung beispielsweise mit dem folgenden Befehl erstellen:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Führen Sie den folgenden Befehl aus, um die Einheitenkonfigurationsdaten in einem anderen Verzeichnis zu sichern:

   ```
   backup devconfig filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.
3. Führen Sie den folgenden Befehl aus, um die Protokolldatei für Datenträger in einem anderen Verzeichnis zu sichern:

   ```
   backup volhistory filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Datenträgerprotokolldaten gespeichert werden sollen.
4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
5. Stoppen Sie alle Instanzen des IBM Spectrum Protect-Servers. Stellen Sie sicher, dass keine IBM Spectrum Protect-Serverprozesse ausgeführt werden. Wenn Sie die Überwachung auf Anwendungsebene für den IBM Spectrum Protect-Server verwenden, setzen Sie die Überwachung der dsmserv-Anwendungsressource mit Ihrem Cluster-Tool aus.
6. Stellen Sie sicher, dass der Datenbankmanager auf keiner Instanz ausgeführt wird. Stellen Sie fest, ob db2sysc-Prozesse ausgeführt werden. Der Eigner aktiver Prozesse zeigt an, welche Instanzen aktiv sind. Führen Sie für jeden Serverinstanzeigner den folgenden Befehl aus, um DB2 zu stoppen:

   ```
   db2stop
   ```

7. Stellen Sie sicher, dass sich die gemeinsam genutzten Ressourcen für alle IBM Spectrum Protect-Instanzen auf dem primären Knoten befinden. Stellen Sie sicher, dass keine anderen Knoten Schreibzugriff auf diese Ressourcen während des Upgrades haben.
8. Installieren Sie den Server der Version 6.3 auf dem primären Knoten. Führen Sie hierfür den Befehl ./install.bin aus. Ausführliche Informationen zur Installation des Servers der Version 6.3 finden Sie in Serverkomponenten installieren.
9. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.2 auf dem primären Knoten. Führen Sie hierfür den Befehl ./install.sh aus. Anweisungen finden Sie in Serverkomponenten installieren. Klicken Sie nach dem Start des Assistenten im Fenster von IBM Installation Manager auf das Symbol Installieren. Klicken Sie nicht auf das Symbol Aktualisieren oder Ändern.
10. Starten Sie jeden IBM Spectrum Protect-Server der Version 8.1.2 im Vordergrund. Navigieren Sie mit der Instanzeigner-ID zum Instanzverzeichnis und geben Sie den folgenden Befehl aus:

    ```
    /opt/tivoli/tsm/server/bin/dsmserv
    ```

    Warten Sie, bis die Eingabeaufforderung des Servers angezeigt wird, was bedeutet, dass der Server gestartet wurde.

11. Stoppen Sie den Server für jede IBM Spectrum Protect-Instanz, die aktualisiert wird.
12. Führen Sie auf jedem sekundären Knoten im Cluster die folgenden Schritte aus:
    a. Verschieben Sie alle gemeinsam genutzten Ressource auf den sekundären Knoten. Wenn in Ihrer Umgebung mehrere Instanzen von IBM Spectrum Protect vorhanden sind, müssen die sekundären Knoten während des Upgrades auf gemeinsam genutzte Ressourcen für alle Instanzen zugreifen können.
    b. Stoppen Sie alle Instanzen des IBM Spectrum Protect-Servers. Stellen Sie sicher, dass keine IBM Spectrum Protect-Serverprozesse ausgeführt werden.
    c. Stellen Sie sicher, dass der Datenbankmanager auf keiner Instanz ausgeführt wird. Stellen Sie fest, ob db2sysc-Prozesse ausgeführt werden. Der Eigner aktiver Prozesse zeigt an, welche Instanzen aktiv sind. Führen Sie für jeden Serverinstanzeigner den folgenden Befehl aus, um DB2 zu stoppen:

       ```
       db2stop
       ```

    d. Deinstallieren Sie den Server der Version 6.1:

i. Geben Sie im Verzeichnis /opt/tivoli/tsm/_uninst den folgenden Befehl aus:

```
cd _uninst
```

ii. Geben Sie den folgenden Befehl aus:

```
./Uninstall_Tivoli_Storage_Manager
```

Ausführliche Informationen zur Deinstallation des Servers finden Sie in der Dokumentation für Tivoli Storage Manager Version 6.1.

e. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.2 mit dem Befehl ./install.sh. Klicken Sie im Fenster von IBM Installation Manager auf das Symbol Installieren. Klicken Sie nicht auf das Symbol Aktualisieren oder Ändern. Anweisungen zur Installation des Servers finden Sie in Serverkomponenten installieren.

f. Stellen Sie sicher, dass jeder IBM Spectrum Protect-Server der Version 8.1.2 startet.

13. Registrieren Sie die Lizenzen für die Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

```
register license file=Installationsverzeichnis/server/bin/Komponentenname.lic
```

Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

Wenn Sie den Server beispielsweise im Standardverzeichnis /opt/tivoli/tsm installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis /opt/tivoli/tsm installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Einschränkung:
Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

Zugehörige Verweise:
BACKUP DB (Datenbank sichern)
BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)
BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)
HALT (Server herunterfahren)
REGISTER LICENSE (Neue Lizenz registrieren)
Linux-Betriebssysteme

IBM Spectrum Protect-Upgrade auf Version 8.1.2 in einer Clusterumgebung unter Linux durchführen

Damit neue Funktionen in IBM Spectrum Protect genutzt werden können, können Sie ein Upgrade des IBM Spectrum Protect-Servers, der unter einem Linux-Betriebssystem in einer Clusterumgebung installiert ist, durchführen.

Vorgehensweise

Befolgen Sie die Anweisungen in Linux-Umgebung für Clustering konfigurieren.
Windows-Betriebssysteme

Upgrade eines Servers der Version 6.3 oder Version 7.1 auf Version 8.1.2 in einer Clusterumgebung unter Windows durchführen

Damit neue Produktfunktionen genutzt werden können, können Sie ein Upgrade eines Servers, der unter einem Windows-Betriebssystem in einer Clusterumgebung installiert ist, von Version 6.3 oder Version 7.1 auf IBM Spectrum Protect Version 8.1.2 durchführen.

Vorbereitende Schritte

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des Servers der Version 6.3 oder Version 7.1, für das Sie ein Upgrade durchführen wollen, vorhanden sind. Wenn Sie den Server über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, müssen Sie die Lizenz von den Installationsmedien des Serverbasisrelease erneut installieren.

Vorgehensweise

1. Wenn Sie den IBM Spectrum Protect-Server der Version 8.1.2 im Betriebssystem Windows Server 2012 installieren wollen, installieren Sie zunächst den Automatisierungsserver für den Failovercluster und die Befehlsschnittstelle für den Failovercluster. Zum Installieren dieser Komponenten geben Sie die folgenden Befehle über die Windows 2.0 PowerShell aus:

   ```
   Install-WindowsFeature -Name RSAT-Clustering-AutomationServer
   Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
   ```

2. Sichern Sie die Datenbank mit dem Befehl BACKUP DB. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamtsicherung erstellt wird, ohne geplante Sicherungen zu unterbrechen. Sie können beispielsweise den folgenden Befehl ausführen, um eine Momentaufnahmesicherung zu erstellen:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

3. Sichern Sie die Einheitenkonfigurationsdaten in einem anderen Verzeichnis. Führen Sie den folgenden Befehl aus:

   ```
   backup devconfig filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.
4. Sichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis. Führen Sie den folgenden Befehl aus:

   ```
   backup volhistory filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Datenträgerprotokolldaten gespeichert werden sollen.
5. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt und sich im Serverinstanzverzeichnis befindet.
6. Stellen Sie sicher, dass sich die Ressourcengruppe im primären Knoten befindet und dass alle Knoten im Cluster aktiv sind. Führen Sie auf dem primären Knoten die folgenden Schritte aus:
   a. Schalten Sie im Fenster Failovercluster-Manager die Serverressource offline und löschen Sie sie:
      i. Wählen Sie Dienste und Anwendungen und dann die Clustergruppe aus. Die Serverressource wird im Abschnitt Andere Ressourcen angezeigt.
      ii. Wählen Sie die Serverressource aus und klicken Sie auf Diese Ressource offline schalten.
      iii. Um die Serverressource zu löschen, wählen Sie sie aus und klicken Sie auf Löschen.
   b. Löschen Sie den Netznamen und die IP-Adresse im Fenster Failovercluster-Manager:
      i. Blenden Sie im Abschnitt Servername den Netznamen ein, um die IP-Adresse anzuzeigen. Notieren Sie den Netznamen und die IP-Adresse.
      ii. Wählen Sie den Netznamen und die IP-Adresse aus und klicken Sie auf Entfernen.
   c. Schalten Sie im Fenster Failovercluster-Manager die DB2-Serverressource offline:
      i. Wählen Sie Dienste und Anwendungen und dann die Clustergruppe aus. Die IBM Spectrum Protect-Serverressource wird im Abschnitt Andere Ressourcen angezeigt.
      ii. Wählen Sie eine DB2-Serverressource aus (z. B. SERVER1) und klicken Sie auf Diese Ressource offline schalten.
7. Führen Sie auf dem primären Knoten den folgenden Befehl aus, um das DB2-Clustering aus jeder IBM Spectrum Protect-Instanz im Cluster zu entfernen:

   ```
   db2mscs -u:Instanzname
   ```

   Führen Sie beispielsweise den folgenden Befehl aus, um das DB2-Clustering aus der Instanz SERVER1 zu entfernen:

   ```
   db2mscs -u:server1
   ```

   Tipp: Möglicherweise wird eine Fehlernachricht wegen einer fehlenden Clusterressource angezeigt. Ignorieren Sie diese Nachricht.
8. Prüfen Sie auf dem primären Knoten im Fenster Failovercluster-Manager den Abschnitt Zusammenfassung der Ressourcengruppe. Stellen Sie sicher, dass nur die gemeinsam genutzten Platten und Bandressourcen in der Ressourcengruppe verbleiben.
9. Stoppen Sie den Clusterdienst auf jedem Knoten in dem Cluster und löschen Sie die DLL-Dateien des Server-Clusters. Starten Sie dann den Clusterdienst erneut.
10. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.2 auf jedem Knoten im Cluster. Anweisungen finden Sie in IBM Spectrum Protect-Serverkomponenten installieren. Wenn Sie den Installationsassistenten für die Serverinstallation verwenden, klicken Sie im Fenster von IBM Installation Manager auf das Symbol Aktualisieren. Klicken Sie nicht auf das Symbol Installieren oder Ändern.
11. Starten Sie den Server auf dem Primärknoten im Vordergrund, damit die Abstimmung und die Konfiguration des Datenbankschemas ausgeführt werden können. Wenn der Server startet, halten Sie ihn mit dem Befehl HALT an. Enthält Ihre Umgebung mehrere Serverinstanzen, führen Sie diesen Schritt für jede Instanz aus.
12. Auf dem primären Knoten starten Sie den Konfigurationsassistenten, indem Sie Start > Alle Programme > IBM Spectrum Protect-Server > Konfigurationsassistent auswählen. Führen Sie die folgenden Schritte im Konfigurationsassistenten aus:
    a. Wenn Sie zur Eingabe der Benutzer-ID aufgefordert werden, geben Sie den Namen des Domänenkontos ein, das dem Cluster zugeordnet ist.

b. Wenn Sie zur Eingabe des Instanznamens aufgefordert werden, geben Sie den Namen der Instanz ein, deren Cluster geändert wird.
c. Wenn Sie aufgefordert werden anzugeben, ob die Clusterbildung geändert werden soll, klicken Sie auf Ja.
d. Setzen Sie die Schritte des Assistenten fort, bis in einer Nachricht angezeigt wird, dass die Konfiguration erfolgreich war.

13. Registrieren Sie die Lizenzen für die IBM Spectrum Protect-Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

    ```
    register license file=Installationsverzeichnis\server\Komponentenname.lic
    ```

    Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

    Wenn Sie den Server beispielsweise im Standardverzeichnis c:\Programme\Tivoli\TSM installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

    ```
    register license file=c:\Programme\Tivoli\TSM\server\tsmbasic.lic
    ```

    Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis c:\Programme\Tivoli\TSM installiert haben, führen Sie den folgenden Befehl aus:

    ```
    register license file=c:\Programme\Tivoli\TSM\server\tsmee.lic
    ```

    Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis c:\Programme\Tivoli\TSM installiert haben, führen Sie den folgenden Befehl aus:

    ```
    register license file=c:\Programme\Tivoli\TSM\server\dataret.lic
    ```

    Einschränkung:
    Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:
    - IBM Spectrum Protect for Mail
    - IBM Spectrum Protect for Databases
    - IBM Spectrum Protect for ERP
    - IBM Spectrum Protect for Space Management

    Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

Nächste Schritte

Ist unter Windows ein Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den Einheitentreiber. Ist kein Einheitentreiber vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls dpinst.exe /a. Die Datei dpinst.exe befindet sich im Verzeichnis des Einheitentreibers und die Standardposition ist C:\Programme\Tivoli\TSM\device\drivers.
Zugehörige Verweise:
BACKUP DB (Datenbank sichern)
BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)
BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)
REGISTER LICENSE (Neue Lizenz registrieren)
Windows-Betriebssysteme

IBM® Tivoli Storage Manager-Upgrade von Version 6.1 auf IBM Spectrum Protect Version 8.1.2 in einer Clusterumgebung unter Windows durchführen

Damit neue Funktionen genutzt werden können, können Sie ein Upgrade eines Servers, der unter einem Windows-Betriebssystem in einer Clusterumgebung installiert ist, von Version 6.1 auf Version 8.1.2 durchführen.

Vorbereitende Schritte

Stellen Sie sicher, dass die Installationsmedien für die Basisreleases der Server der Versionen 6.1 und 6.3 vorhanden sind. Wenn die Server-Software von einem heruntergeladenen Paket stammt, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Vorgehensweise

1. Wenn Sie den IBM Spectrum Protect-Server der Version 8.1.2 im Betriebssystem Windows Server 2012 installieren wollen, installieren Sie zunächst den Automatisierungsserver für den Failovercluster und die Befehlsschnittstelle für den Failovercluster. Zum Installieren dieser Komponenten geben Sie die folgenden Befehle über die Windows 2.0 PowerShell aus:

   ```
   Install-WindowsFeature -Name RSAT-Clustering-AutomationServer
   Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
   ```

2. Sichern Sie die Datenbank mit dem Befehl BACKUP DB. Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamtsicherung erstellt wird, ohne geplante Sicherungen zu unterbrechen. Sie können beispielsweise den folgenden Befehl ausführen, um eine Momentaufnahmesicherung zu erstellen:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

3. Sichern Sie die Einheitenkonfigurationsdaten in einem anderen Verzeichnis. Führen Sie den folgenden Befehl aus:

   ```
   backup devconfig filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.
4. Sichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis. Führen Sie den folgenden Befehl aus:

   ```
   backup volhistory filenames=Dateiname
   ```

   Hierbei gibt *Dateiname* den Namen der Datei an, in der Datenträgerprotokolldaten gespeichert werden sollen.
5. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise dsmserv.opt heißt und sich im Serverinstanzverzeichnis befindet.
6. Stellen Sie sicher, dass sich die Ressourcengruppe im primären Knoten befindet und dass alle Knoten im Cluster aktiv sind. Führen Sie auf dem primären Knoten die folgenden Schritte aus:
   a. Schalten Sie im Fenster Failovercluster-Manager die Serverressource offline und löschen Sie sie:
      i. Wählen Sie Dienste und Anwendungen und dann die Clustergruppe aus. Die Serverressource wird im Abschnitt Andere Ressourcen angezeigt.
      ii. Wählen Sie die Serverressource aus und klicken Sie auf Diese Ressource offline schalten.
      iii. Um die Serverressource zu löschen, wählen Sie sie aus und klicken Sie auf Löschen.
   b. Löschen Sie den Netznamen und die IP-Adresse im Fenster Failovercluster-Manager:
      i. Blenden Sie im Abschnitt Servername den Netznamen ein, um die IP-Adresse anzuzeigen. Notieren Sie den Netznamen und die IP-Adresse.
      ii. Wählen Sie den Netznamen und die IP-Adresse aus und klicken Sie auf Entfernen.
   c. Schalten Sie im Fenster Failovercluster-Manager die DB2-Serverressource offline:
      i. Wählen Sie Dienste und Anwendungen und dann die Clustergruppe aus. Die IBM Spectrum Protect-Serverressource wird im Abschnitt Andere Ressourcen angezeigt.
      ii. Wählen Sie eine DB2-Serverressource aus (z. B. SERVER1) und klicken Sie auf Diese Ressource offline schalten.
7. Um das DB2-Clustering aus der Instanz zu entfernen, geben Sie auf dem primären Knoten für jede IBM Spectrum Protect-Instanz im Cluster den folgenden Befehl aus:

   ```
   db2mscs -u:Instanzname
   ```

   Zum Beispiel:

   ```
   db2mscs -u:server1
   ```

   Tipp: Möglicherweise wird eine Fehlernachricht wegen einer fehlenden Clusterressource angezeigt. Ignorieren Sie diese Nachricht.
8. Stellen Sie auf dem primären Knoten im Fenster Failovercluster-Manager im Abschnitt Zusammenfassung der Ressourcengruppe sicher, dass nur die gemeinsam genutzten Platten und Bandressourcen in der Ressourcengruppe verbleiben.
9. Installieren Sie den Server der Version 6.3 auf dem primären Knoten. Führen Sie hierfür den Befehl install.exe aus. Ausführliche Informationen zur Installation des Servers der Version 6.3 finden Sie in Serverkomponenten installieren.
10. Installieren Sie den IBM Spectrum Protect-Server der Version 8.1.2 auf dem primären Knoten. Anweisungen finden Sie in Serverkomponenten installieren. Wenn Sie den Installationsassistenten für die Serverinstallation verwenden, klicken Sie im Fenster von IBM Installation Manager auf das Symbol Installieren. Klicken Sie nicht auf das Symbol Aktualisieren oder Ändern.
11. Deinstallieren Sie Version 6.1 auf jedem sekundären Knoten:
    a. Wechseln Sie in das folgende Verzeichnis:

       ```
       C:\Programme\Tivoli\TSM\_uninst
       ```

    b. Geben Sie den folgenden Befehl aus:

       ```
       Uninstall Tivoli Storage Manager.exe
       ```

12. Auf dem primären Knoten starten Sie den Konfigurationsassistenten, indem Sie Start > Alle Programme > IBM Spectrum Protect-Server > Konfigurationsassistent auswählen. Führen Sie die Schritte des Konfigurationsassistenten aus.
    a. Wenn Sie zur Eingabe des Instanznamens aufgefordert werden, geben Sie den Namen der Instanz ein, deren Cluster geändert wird.
    b. Wenn Sie zur Eingabe der Benutzer-ID aufgefordert werden, geben Sie den Namen des Domänenkontos ein, das dem Cluster zugeordnet ist.
    c. Wenn Sie aufgefordert werden anzugeben, ob die Clusterbildung geändert werden soll, klicken Sie auf Ja.
    d. Setzen Sie die Schritte des Assistenten fort, bis in einer Nachricht angezeigt wird, dass die Konfiguration erfolgreich war.
13. Registrieren Sie die Lizenzen für die IBM Spectrum Protect-Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl REGISTER LICENSE aus:

    ```
    register license file=Installationsverzeichnis\server\Komponentenname.lic
    ```

    Hierbei gibt *Installationsverzeichnis* das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

Wenn Sie den Server beispielsweise im Standardverzeichnis c:\Programme\Tivoli\TSM installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

```
register license file=c:\Programme\Tivoli\TSM\server\tsmbasic.lic
```

Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis c:\Programme\Tivoli\TSM installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=c:\Programme\Tivoli\TSM\server\tsmee.lic
```

Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis c:\Programme\Tivoli\TSM installiert haben, führen Sie den folgenden Befehl aus:

```
register license file=c:\Programme\Tivoli\TSM\server\dataret.lic
```

Einschränkung:
Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

Der Befehl REGISTER LICENSE ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

Nächste Schritte

Ist unter Windows ein Einheitentreiber für die Bandlaufwerke oder Datenträgerwechsler, die Sie verwenden wollen, vorhanden, verwenden Sie den Einheitentreiber. Ist kein Einheitentreiber vorhanden, installieren Sie den IBM Spectrum Protect-Einheitentreiber mithilfe des Befehls dpinst.exe /a. Die Datei dpinst.exe befindet sich im Verzeichnis des Einheitentreibers und die Standardposition ist C:\Programme\Tivoli\TSM\device\drivers.
Zugehörige Verweise:
BACKUP DB (Datenbank sichern)
BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)
BACKUP VOLHISTORY (History-Daten für sequentielle Datenträger sichern)
REGISTER LICENSE (Neue Lizenz registrieren)
 Windows-Betriebssysteme

GSKit Version 7 nach einem Upgrade auf IBM Spectrum Protect Version 8.1.2 entfernen

Der IBM Spectrum Protect-Installationsassistent führt ein Upgrade für GSKit Version 8 und höher durch. GSKit Version 7 wird nicht entfernt oder aktualisiert, wenn Sie ein Upgrade auf IBM Spectrum Protect Version 8.1.2 durchführen, auch wenn GSKit mit einer früheren Version von IBM Spectrum Protect installiert wurde.

Informationen zu diesem Vorgang

Wenn Sie GSKit Version 7 nicht mehr benötigen und Speicherplatz auf Ihrem System freigeben wollen, können Sie es nach dem Upgrade auf IBM Spectrum Protect Version 8.1.2 entfernen.
Wichtig: Das Entfernen von GSKit Version 7 kann sich auch auf andere Programme auf Ihrem System, die darauf angewiesen sind, auswirken.

Vorgehensweise

Gehen Sie wie folgt vor, um GSKit Version 7 zu entfernen:

1. Sichern Sie Ihre Registrierung.
   a. Klicken Sie auf Start und dann auf Ausführen.
   b. Geben Sie `Regedit` ein. Klicken Sie auf OK.
   c. Wählen Sie Datei > Exportieren aus, um eine Kopie Ihrer Registrierung zu speichern.
   d. Wenn Sie die Registrierung später wiederherstellen müssen, wählen Sie Datei > Importieren aus.
   Weitere Informationen finden Sie in der Windows-Dokumentation.
2. Suchen Sie das Verzeichnis, in dem GSKit installiert ist. Das Standardverzeichnis ist C:\Programme\IBM\gsk7\.
3. Entfernen Sie das GSKit-Installationsverzeichnis gsk7 und alle Subdateien und Unterverzeichnisse. Klicken Sie mit der rechten Maustaste auf den Ordner und mit der linken Maustaste auf Löschen.
4. Entfernen Sie den GSKit 7-Registrierungsschlüssel und alle Unterschlüssel und Werte.
   Wichtig: Wird der falsche Schlüssel entfernt, kann es zu Systemfehlern kommen. Es kann z. B. vorkommen, dass die Workstation nicht erneut gestartet werden kann.
   a. Klicken Sie auf Start und dann auf Ausführen.
   b. Geben Sie `Regedit` ein. Klicken Sie auf OK.

c. Der GSKit-Registrierungsschlüssel befindet sich in dem folgenden Verzeichnis: HKEY_LOCAL_MACHINE\SOFTWARE\IBM. Klicken Sie mit der rechten Maustaste auf den Registrierungsschlüssel HKEY_LOCAL_MACHINE\SOFTWARE\IBM\GSK7 und mit der linken Maustaste auf Löschen.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Operations Center installieren und Operations Center-Upgrade durchführen

Das IBM Spectrum Protect Operations Center ist die webbasierte Schnittstelle für die Verwaltung Ihrer Speicherumgebung.

Vorbereitende Schritte

Lesen Sie die folgenden Informationen, bevor Sie das Operations Center installieren und konfigurieren:

- Systemvoraussetzungen für das Operations Center
  - Voraussetzungen für den Computer des Operations Center
  - Voraussetzungen für Hub- und Peripherieserver
  - Betriebssystemvoraussetzungen
  - Voraussetzungen für den Web-Browser
  - Voraussetzungen für die Sprache
  - Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices
- Administrator-IDs, die für das Operations Center erforderlich sind
- IBM Installation Manager
- Prüfliste für die Installation
- Operations Center-Installationspaket abrufen

Informationen zu diesem Vorgang

In Tabelle 1 sind die Methoden für die Installation oder Deinstallation des Operations Center aufgelistet. Außerdem ist angegeben, wo Sie die zugehörigen Anweisungen finden.

Informationen zum Upgrade des Operations Center finden Sie in Upgrade des Operations Center.

Tabelle 1. Methoden für die Installation oder Deinstallation des Operations Center

Methode	Anweisungen
Grafisch orientierter Assistent	• Operations Center mit einem grafisch orientierten Assistenten installieren • Operations Center mit einem grafisch orientierten Assistenten deinstallieren
Konsolenmodus	• Operations Center im Konsolenmodus installieren • Operations Center im Konsolenmodus deinstallieren
Unbeaufsichtigter Modus	• Operations Center im unbeaufsichtigten Modus installieren • Operations Center im unbeaufsichtigten Modus deinstallieren

- Installation des Operations Center planen
  Vor der Installation des Operations Center müssen Sie die Systemvoraussetzungen, die Administrator-IDs, die das Operations Center benötigt, und die im Installationsprogramm anzugebenden Informationen kennen.
- Operations Center installieren
  Sie können das Operations Center mit jeder der folgenden Methoden installieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.
- Upgrade des Operations Center
  Sie können ein Upgrade des Operations Center mit jeder der folgenden Methoden durchführen: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.
- Erste Schritte mit dem Operations Center
  Bevor Sie das Operations Center für die Verwaltung Ihrer Speicherumgebung verwenden können, müssen Sie es konfigurieren.
- AIX-Betriebssysteme Linux-BetriebssystemeFehlerbehebung für die Operations Center-Installation
  Wenn bei der Installation des Operations Center ein Problem auftritt, das Sie nicht lösen können, können Sie in den Beschreibungen der bekannten Probleme nach einer Lösungsmöglichkeit suchen.
- Operations Center deinstallieren
  Sie können das Operations Center mit jeder der folgenden Methoden deinstallieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.
- Rollback zu einer vorherigen Version des Operations Center durchführen
  Standardmäßig speichert IBM Installation Manager ältere Versionen eines Pakets, damit ein Rollback ausgeführt werden kann, falls Probleme mit neueren Versionen von Updates, Fixes oder Paketen auftreten.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Installation des Operations Center planen

Vor der Installation des Operations Center müssen Sie die Systemvoraussetzungen, die Administrator-IDs, die das Operations Center benötigt, und die im Installationsprogramm anzugebenden Informationen kennen.

Informationen zu diesem Vorgang

Mithilfe des Operations Center können Sie die folgenden Hauptaspekte der Speicherumgebung verwalten:

- IBM Spectrum Protect-Server und -Clients
- Services wie Sichern und Zurückschreiben, Archivieren und Abrufen sowie Umlagern und Zurückrufen
- Speicherpool und Speichereinheiten

Das Operations Center verfügt über folgende Funktionen:

Benutzerschnittstelle für mehrere Server
: Sie können mit dem Operations Center mindestens einen IBM Spectrum Protect-Server verwalten.

  In einer Umgebung mit mehreren Servern können Sie einen Server als *Hub-Server* und die übrigen Server als *Peripherieserver* festlegen. Der Hub-Server kann Alerts und Statusinformationen von den Peripherieservern empfangen und in einer konsolidierten Sicht im Operations Center anzeigen.

Alertüberwachung
: Ein *Alert* ist eine Benachrichtigung über ein relevantes Problem auf dem Server und wird durch eine Servernachricht ausgelöst. Sie können definieren, welche Nachrichten Alerts auslösen, und nur diese Nachrichten werden als Alerts in der Operations Center oder in einer E-Mail aufgelistet.

  Diese Alertüberwachung kann Ihnen beim Erkennen und Verfolgen relevanter Probleme auf dem Server helfen.

Komfortable Befehlszeilenschnittstelle
: Das Operations Center verfügt über eine Befehlszeilenschnittstelle für erweiterte Funktionen und Konfiguration.

- Systemvoraussetzungen für das Operations Center
  Stellen Sie vor der Installation des Operations Center sicher, dass Ihr System die Mindestvoraussetzungen erfüllt.
- Administrator-IDs, die für das Operations Center erforderlich sind
  Ein Administrator muss für die Anmeldung beim Operations Center eine gültige ID und ein gültiges Kennwort auf dem Hub-Server haben. Eine Administrator-ID wird auch dem Operations Center zugeordnet, damit das Operations Center Server überwachen kann.
- IBM Installation Manager
  Das Operations Center verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.
- Prüfliste für die Installation
  Bevor Sie das Operations Center installieren, müssen Sie bestimmte Informationen überprüfen, z. B. die Berechtigungsnachweise für die Installation, und Sie müssen die Eingabedaten festlegen, die in IBM Installation Manager für die Installation angegeben werden sollen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Systemvoraussetzungen für das Operations Center

Stellen Sie vor der Installation des Operations Center sicher, dass Ihr System die Mindestvoraussetzungen erfüllt.

Mithilfe des Operations Center System Requirements Calculator können Sie die Systemvoraussetzungen für die Ausführung des Operations Center sowie der vom Operations Center überwachten Hub- und Peripherieserver schätzen.

Während der Installation überprüfte Voraussetzungen

Tabelle 1 enthält eine Auflistung der Voraussetzungen, die während der Installation überprüft werden, und Verweise auf weitere Informationen zu diesen Voraussetzungen.

Tabelle 1. Während der Installation überprüfte Voraussetzungen

Voraussetzungen	**Details**
Mindestspeicherbedarf	Voraussetzungen für den Computer des Operations Center
Betriebssystemvoraussetzungen	Betriebssystemvoraussetzungen
Hostnamen des Computers, auf dem das Operations Center installiert werden soll	Prüfliste für die Installation
Voraussetzungen für das Operations Center-Installationsverzeichnis	Prüfliste für die Installation

- Voraussetzungen für den Computer des Operations Center
  Sie können das Operations Center auf einem Computer installieren, auf dem auch der IBM Spectrum Protect-Server ausgeführt wird, oder

auf einem andere Computer. Wenn Sie das Operations Center zusammen mit einem Server auf demselben Computer installieren, muss dieser Computer die Systemvoraussetzungen für das Operations Center und für den Server erfüllen.

- Voraussetzungen für Hub- und Peripherieserver
  Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie das Operations Center einem einzelnen IBM Spectrum Protect-Server zuordnen, der als *Hub-Server* festgelegt ist. In einer Umgebung mit mehreren Servern können Sie die anderen Server, die als *Peripherieserver* bezeichnet werden, mit dem Hub-Server verbinden.
- Betriebssystemvoraussetzungen
  Das Operations Center ist für AIX-, Linux- und Windows-Systeme verfügbar.
- Voraussetzungen für den Web-Browser
  Das Operations Center kann in Apple-, Google-, Microsoft- und Mozilla-Web-Browsern ausgeführt werden.
- Voraussetzungen für die Sprache
  Standardmäßig verwendet das Operations Center dieselbe Sprache wie der Web-Browser. Beim Installationsprozess wird jedoch die Sprache des Betriebssystems verwendet. Überprüfen Sie, ob für den Web-Browser und das Betriebssystem die erforderliche Sprache definiert ist.
- Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices
  IBM Spectrum Protect-Clientverwaltungsservices ist eine Komponente, die Sie auf Clients für Sichern/Archivieren installieren, um Diagnoseinformationen (z. B. Clientprotokolldateien) zu erfassen. Bevor Sie den Clientverwaltungsservice auf Ihrem System installieren, müssen Sie die Voraussetzungen und Einschränkungen kennen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Voraussetzungen für den Computer des Operations Center

Sie können das Operations Center auf einem Computer installieren, auf dem auch der IBM Spectrum Protect-Server ausgeführt wird, oder auf einem andere Computer. Wenn Sie das Operations Center zusammen mit einem Server auf demselben Computer installieren, muss dieser Computer die Systemvoraussetzungen für das Operations Center und für den Server erfüllen.

Ressourcenanforderungen

Die folgenden Ressourcen sind für die Ausführung des Operations Center erforderlich:

- Ein Prozessorkern
- 4 GB Speicher
- 1 GB Plattenspeicherplatz

Für den Hub-Server und die Peripherieserver, die vom Operations Center überwacht werden, sind zusätzliche Ressourcen erforderlich (siehe Voraussetzungen für Hub- und Peripherieserver).

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Voraussetzungen für Hub- und Peripherieserver

Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie das Operations Center einem einzelnen IBM Spectrum Protect-Server zuordnen, der als *Hub-Server* festgelegt ist. In einer Umgebung mit mehreren Servern können Sie die anderen Server, die als *Peripherieserver* bezeichnet werden, mit dem Hub-Server verbinden.

Die Peripherieserver senden Alerts und Statusinformationen an den Hub-Server. Das Operations Center zeigt eine konsolidierte Sicht der Alerts und Statusinformationen für den Hub-Server und alle Peripherieserver an.

Wird nur ein einziger Server vom Operations Center überwacht, wird dieser Server als Hub-Server bezeichnet, obwohl keine Peripherieserver mit ihm verbunden sind.

In Tabelle 1 ist die Version des IBM Spectrum Protect-Servers aufgeführt, die auf dem Hub-Server und auf jedem vom Operations Center verwalteten Peripherieserver installiert sein muss.

Tabelle 1. Voraussetzungen bezüglich der IBM Spectrum Protect-Serverversion für Hub- und Peripherieserver

Operations Center	Version auf dem Hub-Server	Version auf jedem Peripherieserver
Version 8.1.2	Version 8.1.2	Version 6.3.4 oder höher Einschränkung: Für Server mit einer Version vor Version 8.1.2 sind einige Operations Center-Funktionen nicht verfügbar.

Anzahl Peripherieserver, die ein Hub-Server unterstützen kann

Die Anzahl der Peripherieserver, die ein Hub-Server unterstützen kann, ist von der Konfiguration und von der Version von IBM Spectrum Protect auf jedem Peripherieserver abhängig. Eine allgemeine Richtlinie ist jedoch, dass ein Hub-Server 10 - 20 Peripherieserver der Version 6.3.4, aber mehr Peripherieserver der Version 7.1 oder höher unterstützen kann.

- Tipps für das Entwerfen der Hub- und Peripherieserverkonfiguration
  Berücksichtigen Sie beim Entwurf der Hub- und Peripherieserverkonfiguration insbesondere die Ressourcenanforderungen für die Statusüberwachung. Überlegen Sie außerdem, wie Sie Hub- und Peripherieserver gruppieren und ob Sie mehrere Hub-Server verwenden wollen.
- Tipps für die Auswahl eines Hub-Servers
  Als Hub-Server müssen Sie einen Server auswählen, der über angemessene Ressourcen verfügt und sich an einem Standort befindet, der minimale Umlauflatenzzeit im Netz gewährleistet.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Tipps für das Entwerfen der Hub- und Peripherieserverkonfiguration

Berücksichtigen Sie beim Entwurf der Hub- und Peripherieserverkonfiguration insbesondere die Ressourcenanforderungen für die Statusüberwachung. Überlegen Sie außerdem, wie Sie Hub- und Peripherieserver gruppieren und ob Sie mehrere Hub-Server verwenden wollen.

Mithilfe des Operations Center System Requirements Calculator können Sie die Systemvoraussetzungen für die Ausführung des Operations Center sowie der vom Operations Center überwachten Hub- und Peripherieserver schätzen.

Primäre leistungsrelevante Faktoren

Die folgenden Faktoren haben den größten Einfluss auf die Leistung des Operations Center:

- Der Prozessor und Speicher auf dem Computer, auf dem das Operations Center installiert ist.
- Die Systemressourcen der Hub- und Peripherieserver, einschließlich des für die Hub-Serverdatenbank verwendeten Plattensystems.
- Die Anzahl der Clientknoten und Dateibereiche für virtuelle Maschinen, die von den Hub- und Peripherieservern verwaltet werden.
- Die Aktualisierungshäufigkeit der Daten im Operations Center.

Hub- und Peripherieserver gruppieren

Erwägen Sie die Gruppierung von Hub- und Peripherieservern nach Standort. Durch die Verwaltung der Server in demselben Rechenzentrum können beispielsweise Probleme vermieden werden, die durch Firewalls oder unzulängliche Netzbandbreite zwischen verschiedenen Standorten verursacht werden. Bei Bedarf können Sie die Server anhand der folgenden Merkmale weiter unterteilen:

- Administrator, der die Server verwaltet
- Organisationsentität, die die Server finanziert
- Serverbetriebssystem
- Sprache, mit der die Server ausgeführt werden.
  Tipp: Werden Hub- und Peripherieserver nicht mit derselben Sprache ausgeführt, könnte fehlerhafter Text im Operations Center angezeigt werden.

Hub- und Peripherieserver in einer unternehmensweiten Konfiguration gruppieren

In einer unternehmensweiten Konfiguration wird ein IBM Spectrum Protect-Servernetz als Gruppe verwaltet. Im *Konfigurationsmanager* vorgenommene Änderungen können automatisch an mindestens einen *verwalteten Server* im Netz verteilt werden.

Normalerweise registriert und verwaltet das Operations Center eine dedizierte Administrator-ID auf den Hub- und Peripherieservern. Dieser *Überwachungsadministrator* muss auf allen Servern immer dasselbe Kennwort haben.

Wenn Sie eine unternehmensweite Konfiguration verwenden, können Sie den Prozess, durch den die Administratorberechtigungsnachweise auf Peripherieservern synchronisiert werden, verbessern. Gehen Sie wie folgt vor, um die Leistung und Effizienz bei der Verwaltung der Überwachungsadministrator-ID zu verbessern:

1. Legen Sie den Konfigurationsmanagerserver als Hub-Server des Operations Center fest. Während der Hub-Server-Konfiguration wird die Überwachungsadministrator-ID 'IBM-OC-*Hub-Server-Name*' registriert.
2. Auf dem Hub-Server fügen Sie die Überwachungsadministrator-ID einem neuen oder vorhandenen Profil für die unternehmensweite Konfiguration hinzu. Geben Sie den Befehl NOTIFY SUBSCRIBERS aus, um das Profil an die verwalteten Server zu verteilen.
3. Fügen Sie mindestens einen der verwalteten Server als Peripherieserver des Operations Center hinzu.

Das Operations Center erkennt diese Konfiguration und gestattet dem Konfigurationsmanager, die Überwachungsadministrator-ID auf den Peripherienservern zu verteilen und zu aktualisieren.

Verwendung mehrerer Hub-Server

Sind mehr als 10 bis 20 Peripherieserver der Version 6.3.4 vorhanden oder muss die Umgebung aufgrund von Ressourceneinschränkungen partitioniert werden, können Sie mehrere Hub-Server konfigurieren und jeden Hub-Server mit einer Untergruppe der Peripherieserver verbinden. Einschränkungen:

- Derselbe Server kann nicht gleichzeitig Hub-Server und Peripherieserver sein.
- Jeder Peripherieserver kann nur einem einzigen Hub-Server zugeordnet sein.
- Für jeden Hub-Server ist eine separate Operations Center-Instanz mit einer separaten Webadresse erforderlich.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Tipps für die Auswahl eines Hub-Servers

Als Hub-Server müssen Sie einen Server auswählen, der über angemessene Ressourcen verfügt und sich an einem Standort befindet, der minimale Umlauflatenzzeit im Netz gewährleistet.

Achtung: Verwenden Sie nicht einen einzigen Server als Hub-Server für mehrere Operations Center.
Treffen Sie Ihre Entscheidung darüber, welcher Server als Hub-Server festgelegt werden soll, anhand der folgenden Richtlinien:

Wählen Sie einen Server mit geringer Auslastung
: Sie sollten einen Server mit einer geringen Auslastung für Operationen wie z. B. Clientsicherung und -archivierung auswählen. Ein Server mit geringer Auslastung ist auch eine gute Wahl als Hostsystem für das Operations Center.

  Stellen Sie sicher, dass der Server über die Ressourcen zur Bearbeitung sowohl seiner normalen Serverauslastung als auch der geschätzten Auslastung für seine Rolle als Hub-Server verfügt.

Positionieren Sie den Server so, dass minimale Umlauflatenzzeit im Netz entsteht
: Positionieren Sie den Hub-Server so, dass die Netzverbindung zwischen dem Hub-Server und den Peripherieservern eine Umlauflatenzzeit von maximal 5 ms aufweist. Diese Latenzzeit kann normalerweise erreicht werden, wenn sich die Server in demselben lokalen Netz (LAN) befinden.

  Netze, die schlecht eingestellt sind, von anderen Anwendungen stark genutzt werden oder eine Umlauflatenzzeit von sehr viel mehr als 5 ms haben, können die Kommunikation zwischen dem Hub-Server und den Peripherieservern verschlechtern. Umlauflatenzzeiten von 50 ms oder mehr können z. B. Überschreitungen des Kommunikationszeitlimits bewirken, die eine Trennung oder Wiederherstellung der Peripherieserververbindung zum Operations Center verursachen. Derartig lange Latenzzeiten können bei der Kommunikation im Weitverkehrsnetz (WAN) auftreten.

  Wenn der Abstand zwischen den Peripherieservern und dem Hub-Server sehr groß ist und häufige Trennungen der Peripherieserververbindung im Operations Center auftreten, können Sie den Wert der Option ADMINCOMMTIMEOUT auf jedem Server erhöhen, um das Problem zu verkleinern.

Stellen Sie sicher, dass der Hub-Server die Ressourcenanforderungen für die Statusüberwachung erfüllt
: Für die Statusüberwachung werden zusätzliche Ressourcen auf jedem Server benötigt, auf dem sie aktiviert ist. Der Ressourcenbedarf ist hauptsächlich von der Anzahl Clients abhängig, die von den Hub- und Peripherieservern verwaltet werden. Auf einem Hub-Server mit einem Peripherieserver der Version 7.1 oder höher werden weniger Ressourcen verwendet als auf einem Hub-Server mit einem Peripherieserver der Version 6.3.4.

  Stellen Sie sicher, dass der Hub-Server die Ressourcenanforderungen bezüglich der Prozessorauslastung, des Datenbankbereichs, des Speicherbereichs für das Archivprotokoll und der IOPS-Kapazität erfüllt (IOPS = E/A-Operationen pro Sekunde).

  Ein Hub-Server mit hoher IOPS-Kapazität kann ein hohes Volumen eingehender Statusdaten von Peripherieservern bearbeiten. Die Erfüllung dieser Kapazitätsanforderung kann durch die Verwendung der folgenden Speichereinheiten für die Hub-Server-Datenbank erleichtert werden:

  - Ein Solid-State-Laufwerk (SSD) auf Unternehmensebene
  - Eine externe SAN-Plattenspeichereinheit mit mehreren Datenträgern oder mehreren Spindeln unter jedem Datenträger

  In einer Umgebung mit weniger als 1000 Clients sollten Sie das Einrichten einer Basiskapazität von 1000 E/A-Operationen pro Sekunde für die Hub-Serverdatenbank in Betracht ziehen, wenn der Hub-Server Peripherieserver verwaltet.

Stellen Sie fest, ob in Ihrer Umgebung mehrere Hub-Server erforderlich sind
: Wenn eine aus einem Hub-Server und Peripherieservern bestehende Gruppe mehr als 10.000 bis 20.000 Clientknoten und Dateibereiche für virtuelle Maschinen verwaltet, könnte der Ressourcenbedarf die verfügbaren Ressourcen des Hub-Servers übersteigen, insbesondere, wenn es sich bei den Peripherieservern um Server der Version 6.3.4 handelt. In diesem Fall sollten Sie einen zweiten Server als Hub-Server angeben und zum Lastausgleich Peripherieserver zum neuen Hub-Server versetzen.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Betriebssystemvoraussetzungen

Das Operations Center ist für AIX-, Linux- und Windows-Systeme verfügbar.

Sie können das Operations Center auf den folgenden Systemen ausführen:

- AIX-BetriebssystemeAIX-Systeme:
  - IBM® AIX V7.1 (64 Bit) TL 4 und SP 2
  - IBM AIX V7.2 (64 Bit) TL 0 und SP 2
- Linux-BetriebssystemeLinux on x86_64-Systeme:
  - Red Hat Enterprise Linux 6.7
  - Red Hat Enterprise Linux 7.1

    - SUSE Linux Enterprise Server 11, Service-Pack 4 oder höher
    - SUSE Linux Enterprise Server 12
- Linux-BetriebssystemeLinux on System z-Systeme (s390x 64-Bit-Architektur):
    - Red Hat Enterprise Linux 7.1
    - SUSE Linux Enterprise Server 12
- Linux-BetriebssystemeLinux on Power Systems-Systeme (Little Endian):
    - Red Hat Enterprise Linux 7 mit PPC64LE-Architektur
- Windows-BetriebssystemeWindows-Systeme:
    - Microsoft Windows Server 2012: Standard, Enterprise oder Datacenter Edition (64-Bit)
    - Microsoft Windows Server 2012 R2 (64-Bit)
    - Microsoft Windows Server 2016

Aktuelle Informationen zu den Anforderungen finden Sie unter Software and Hardware Requirements.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Voraussetzungen für den Web-Browser

Das Operations Center kann in Apple-, Google-, Microsoft- und Mozilla-Web-Browsern ausgeführt werden.

Stellen Sie für eine optimale Anzeige des Operations Center im Web-Browser sicher, dass die Bildschirmauflösung für das System mindestens auf 1024 x 768 Pixel gesetzt ist.

Verwenden Sie einen Web-Browser mit guter JavaScript-Leistung und aktivieren Sie Browser-Caching, um eine optimale Leistung zu erzielen.

Das Operations Center kann in den folgenden Web-Browsern ausgeführt werden:

- Apple Safari auf dem iPad
  Einschränkung: Wird Apple Safari unter iOS 8.x oder iOS 9.x ausgeführt, können Sie ein selbst signiertes Zertifikat für die sichere Kommunikation mit dem Operations Center nur mit zusätzlicher Konfiguration des Zertifikats verwenden. Verwenden Sie ein Zertifikat einer Zertifizierungsstelle (CA-Zertifikat) oder konfigurieren Sie das selbst signierte Zertifikat nach Bedarf. Anweisungen finden Sie im technischen Hinweis (Technote) http://www.ibm.com/support/docview.wss?uid=swg21963153.
- Google Chrome 40 oder höher
- Microsoft Internet Explorer 11 oder höher
- Mozilla Firefox ESR 31 oder höher

Damit das Operations Center gemäß der Empfehlung von National Institute of Standards and Technology (NIST) Special Publications (SP) 800-131A ausgeführt werden kann, muss die Kommunikation zwischen dem Operations Center und dem Web-Browser mit dem TLS 1.2-Protokoll (TLS = Transport Layer Security) geschützt werden. Während der Installation geben Sie an, ob die Einhaltung von SP 800-131A erforderlich ist, sowie die Stufe der Einhaltung. Wenn während der Installation die strikte Einhaltung von SP 800-131A angegeben wird, muss der Web-Browser TLS 1.2 unterstützen und TLS 1.2 muss aktiviert sein.

Der Web-Browser zeigt einen SSL-Fehler an, wenn während der Installation die strikte Einhaltung von SP 800-131A angegeben wird, ohne dass der Web-Browser die vorangegangenen Voraussetzungen erfüllt.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Voraussetzungen für die Sprache

Standardmäßig verwendet das Operations Center dieselbe Sprache wie der Web-Browser. Beim Installationsprozess wird jedoch die Sprache des Betriebssystems verwendet. Überprüfen Sie, ob für den Web-Browser und das Betriebssystem die erforderliche Sprache definiert ist.

AIX-Betriebssysteme

Tabelle 1. Operations Center-Sprachwerte, die Sie auf AIX-Systemen verwenden können

Sprache	Wert für die Sprachoption
Chinesisch, vereinfacht	zh_CN
Chinesisch, vereinfacht (UTF-8)	ZH_CN
Chinesisch, traditionell (Big5)	Zh_TW
Chinesisch, traditionell (UTF-8)	ZH_TW
Chinesisch, traditionell (euc_tw)	zh_TW
Englisch	en_US
Englisch (UTF-8)	EN_US
Französisch	fr_FR

Sprache	Wert für die Sprachoption
Französisch (UTF-8)	FR_FR
Deutsch	de_DE
Deutsch (UTF-8)	DE_DE
Italienisch	it_IT
Italienisch (UTF-8)	IT_IT
Japanisch (EUC)	ja_JP
Japanisch (PC)	Ja_JP
Japanisch (UTF-8)	JA_JP
Koreanisch	ko_KR
Koreanisch (UTF-8)	KO_KR
Portugiesisch, Brasilianisches	pt_BR
Portugiesisch, Brasilianisches (UTF-8)	PT_BR
Russisch	ru_RU
Russisch (UTF-8)	RU_RU
Spanisch	es_ES
Spanisch (UTF-8)	ES_ES

Linux-Betriebssysteme

Tabelle 2. Operations Center-Sprachwerte, die Sie auf Linux-Systemen verwenden können

Sprache	Wert für die Sprachoption
Chinesisch, vereinfacht	zh_CN
Chinesisch, vereinfacht (GBK)	zh_CN.gb18030
Chinesisch, vereinfacht (UTF-8)	zh_CN.utf8
Chinesisch, traditionell (Big5)	Zh_TW
Chinesisch, traditionell (euc_tw)	zh_TW
Chinesisch, traditionell (UTF-8)	zh_TW.utf8
Englisch, Vereinigte Staaten	en_US
Englisch (UTF-8)	en_US.utf8
Französisch	fr_FR
Französisch (UTF-8)	fr_FR.utf8
Deutsch	de_DE
Deutsch (UTF-8)	de_DE.utf8
Italienisch	it_IT
Italienisch (UTF-8)	it_IT.utf8
Japanisch (EUC)	ja_JP
Japanisch (UTF-8)	ja_JP.utf8
Koreanisch	ko_KR
Koreanisch (UTF-8)	ko_KR.utf8
Portugiesisch, Brasilianisches	pt_BR
Portugiesisch, Brasilianisches (UTF-8)	pt_BR.utf8
Russisch	ru_RU
Russisch (UTF-8)	ru_RU.utf8
Spanisch	es_ES
Spanisch (UTF-8)	es_ES.utf8

Windows-Betriebssysteme

Tabelle 3. Operations Center-Sprachwerte, die Sie

auf Windows-Systemen verwenden können

Sprache	Wert für die Sprachoption
Chinesisch, vereinfacht	chs
Chinesisch, traditionell	cht
Englisch	ameng
Französisch	fra
Deutsch	deu
Italienisch	ita
Japanisch (Shift-JIS)	jpn
Koreanisch	kor
Portugiesisch, Brasilianisches	ptb
Russisch	rus
Spanisch	esp

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices

IBM Spectrum Protect-Clientverwaltungsservices ist eine Komponente, die Sie auf Clients für Sichern/Archivieren installieren, um Diagnoseinformationen (z. B. Clientprotokolldateien) zu erfassen. Bevor Sie den Clientverwaltungsservice auf Ihrem System installieren, müssen Sie die Voraussetzungen und Einschränkungen kennen.

In der Dokumentation für den Clientverwaltungsservice ist *Clientsystem* das System, in dem der Client für Sichern/Archivieren installiert ist.

Diagnoseinformationen können nur von Linux- und Windows-Clients erfasst werden. Administratoren können jedoch die Diagnoseinformationen unter AIX, Linux oder Windows im Operations Center anzeigen.

Voraussetzungen für den Clientverwaltungsservice

Lesen Sie die folgenden Informationen zu den Voraussetzungen, bevor Sie den Clientverwaltungsservice installieren:

- Für einen Fernzugriff auf den Client benötigt der Operations Center-Administrator Systemberechtigung oder eine der folgenden Clientberechtigungsstufen:
  - Maßnahmenberechtigung
  - Clienteignerberechtigung
  - Clientknotenzugriffsberechtigung
- Stellen Sie sicher, dass das Clientsystem die folgenden Voraussetzungen erfüllt:
  - Der Clientverwaltungsservice kann nur in Clientsystemen installiert werden, die mit Linux- oder Windows-Betriebssystemen ausgeführt werden:
    - Linux x86-64-Bit-Betriebssysteme, die für den Client für Sichern/Archivieren unterstützt werden.
    - Windows-32-Bit- und -64-Bit-Betriebssysteme, die für den Client für Sichern/Archivieren unterstützt werden.
  - Für die Datenübertragung zwischen dem Clientverwaltungsservice und dem Operations Center muss Transport Layer Security (TLS) 1.2 installiert sein. Es steht Basisauthentifizierung zur Verfügung und Daten sowie Authentifizierungsinformationen werden über den SSL-Kanal verschlüsselt. TLS 1.2 wird bei der Installation des Clientverwaltungsservice automatisch zusammen mit den erforderlichen SSL-Zertifikaten installiert.
- Auf Linux-Clientsystemen benötigen Sie Rootberechtigung für die Installation des Clientverwaltungsservice.
- Bei Clientsystemen, die mehrere Clientknoten haben können, z. B. Linux-Clientsysteme, muss jeder Knotenname im Clientsystem eindeutig sein.
  Tipp: Nach der Installation des Clientverwaltungsservice müssen Sie ihn nicht erneut installieren, weil der Service mehrere Clientoptionsdateien erkennen kann.

Einschränkungen des Clientverwaltungsservice

Der Clientverwaltungsservice stellt Basisservices für die Erfassung von Diagnoseinformationen aus den Clients für Sichern/Archivieren bereit. Für den Clientverwaltungsservice bestehen die folgenden Einschränkungen:

- Sie können den Clientverwaltungsservice nur auf Systemen mit Clients für Sichern/Archivieren installieren, einschließlich Clients für Sichern/Archivieren, die auf Knoten mit Einheiten zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware installiert sind.
- Sie können den Clientverwaltungsservice nicht auf anderen IBM Spectrum Protect-Clientkomponenten oder -Produkten installieren, die keine Clients für Sichern/Archivieren aufweisen.

- Wenn die Clients für Sichern/Archivieren durch eine Firewall geschützt sind, müssen Sie sicherstellen, dass das Operations Center durch die Firewall mithilfe des konfigurierten Anschlusses für den Clientverwaltungsservice eine Verbindung zu den Clients für Sichern/Archivieren herstellen kann. Der Standardanschluss ist 9028, der jedoch geändert werden kann.
- Der Clientverwaltungsservice überprüft alle Clientprotokolldateien auf Einträge für den vorhergehenden Zeitraum von 72 Stunden.
- Die Diagnoseseite im Operations Center enthält Basisinformationen zur Fehlerbehebung für Clients für Sichern/Archivieren. Bei einigen Sicherungsproblemen müssen Sie jedoch u. U. auf das Clientsystem zugreifen und weitere Diagnoseinformationen abrufen.
- Wenn die Clientfehlerprotokolldateien und die Planungsprotokolldateien in einem Clientsystem zusammen eine Größe von mehr als 500 MB haben, können beim Senden von Protokollsätzen an das Operations Center Verzögerungen auftreten. Sie können die Größe der Protokolldateien steuern, indem Sie eine Bereinigung oder einen Umlauf von Protokolldateien durch Angabe der Clientoption errorlogretention bzw. errorlogmax ermöglichen.
- Wenn Sie denselben Clientknotennamen verwenden, um eine Verbindung zu mehreren IBM Spectrum Protect-Servern herzustellen, die auf derselben Server-Hardware installiert sind, können Sie Protokolldateien für nur einen der Clientknoten anzeigen.

Aktualisierungen zum Clientverwaltungsservice, einschließlich Voraussetzungen, Einschränkungen und Dokumentationsaktualisierungen, finden Sie inTechnote 1963610.

Zugehörige Tasks:
Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen
 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Administrator-IDs, die für das Operations Center erforderlich sind

Ein Administrator muss für die Anmeldung beim Operations Center eine gültige ID und ein gültiges Kennwort auf dem Hub-Server haben. Eine Administrator-ID wird auch dem Operations Center zugeordnet, damit das Operations Center Server überwachen kann.

Für das Operations Center sind die folgenden IBM Spectrum Protect-Administrator-IDs erforderlich:

Auf dem Hub-Server registrierte Administrator-IDs
: Jede Administrator-ID, die auf dem Hub-Server registriert ist, kann für die Anmeldung beim Operations Center verwendet werden. Die Berechtigungsstufe der ID bestimmt die Tasks, die ausgeführt werden können. Sie können neue Administrator-IDs mit dem Befehl REGISTER ADMIN erstellen.
Einschränkung: Um eine Administrator-ID in einer serverübergreifenden Konfiguration verwenden zu können, muss die ID mit demselben Kennwort und derselben Berechtigungsstufe auf dem Hub-Server und den Peripherieservern registriert werden.
Die Authentifizierung für diese Server können Sie mit einer der folgenden Methoden verwalten:

  - Mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol).
  - Mit den Funktionen für die unternehmensweite Konfiguration, mit denen Änderungen an den Administratordefinitionen automatisch verteilt werden.

Überwachungsadministrator-ID
: Wenn Sie den Hub-Server anfänglich konfigurieren, wird eine Administrator-ID mit dem Namen IBM-OC-*Servername* mit Systemberechtigung auf dem Hub-Server registriert und dem von Ihnen angegebenen Anfangskennwort zugeordnet. Diese ID, die manchmal als *Überwachungsadministrator* bezeichnet wird, ist nur für die Verwendung durch das Operations Center bestimmt.

  Sie dürfen diese ID nicht löschen, sperren oder ändern. Dieselbe Administrator-ID mit demselben Kennwort wird auf den Peripherieservern registriert, die Sie hinzufügen. Das Kennwort wird automatisch alle 90 Tage auf dem Hub-Server und den Peripherieservern geändert. Sie müssen dieses Kennwort nicht verwenden oder verwalten.

  Einschränkung: Das Operations Center verwaltet die ID und das Kennwort des Überwachungsadministrators auf Peripherieservern, falls Sie diese Berechtigungsnachweise nicht mithilfe einer unternehmensweiten Konfiguration verwalten. Weitere Informationen zur Verwaltung der Berechtigungsnachweise mithilfe einer unternehmensweiten Konfiguration finden Sie in Tipps für das Entwerfen der Hub- und Peripherieserverkonfiguration.

Zugehörige Verweise:
REGISTER ADMIN (Administrator-ID registrieren)
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

IBM Installation Manager

Das Operations Center verwendet IBM® Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager nicht bereits installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie das Operations Center installieren. Die Software muss auf dem System installiert bleiben, damit das Operations Center später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

Angebot
: Eine installierbare Einheit eines Softwareprodukts.

Das Angebot 'Operations Center' enthält alle Datenträger, die IBM Installation Manager für die Installation des Operations Center benötigt.

Paket
: Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.
Das Operations Center-Paket enthält folgende Komponenten:

- Installationsprogramm von IBM Installation Manager
- Das Angebot 'Operations Center'

Paketgruppe
: Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

Repository
: Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

Das Operations Center-Paket wird in einem Repository in IBM Fix Central gespeichert.

Verzeichnis für gemeinsam genutzte Ressourcen
: Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version des Operations Center verwendet werden.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Prüfliste für die Installation

Bevor Sie das Operations Center installieren, müssen Sie bestimmte Informationen überprüfen, z. B. die Berechtigungsnachweise für die Installation, und Sie müssen die Eingabedaten festlegen, die in IBM® Installation Manager für die Installation angegeben werden sollen.

Die folgende Prüfliste enthält eine Zusammenfassung der Informationen, die Sie überprüfen bzw. festlegen müssen, bevor Sie das Operations Center installieren. In Tabelle 1 werden diese Informationen dann ausführlich beschrieben.

- ☐ Den Hostnamen des Computers überprüfen, auf dem das Operations Center installiert werden soll.
- ☐ Die Berechtigungsnachweise für die Installation überprüfen.
- ☐ Das Installationsverzeichnis für das Operations Center festlegen, wenn der Standardpfad nicht übernommen werden soll.
- ☐ Das Installationsverzeichnis für IBM Installation Manager festlegen, wenn der Standardpfad nicht übernommen werden soll.
- ☐ Die vom Operations Center zu verwendende Anschlussnummer festlegen, wenn die Standardanschlussnummer nicht übernommen werden soll.
- ☐ Das Kennwort für die sichere Kommunikation festlegen.
- ☐ Stellen Sie fest, ob die sichere Kommunikation der Empfehlung von National Institute of Standards and Technology (NIST) Special Publications (SP) 800-131A entsprechen muss.

Tabelle 1. Vor der Installation des Operations Center zu überprüfende bzw. festzulegende Informationen

Informationen	**Details**
Hostname des Computers, auf dem das Operations Center installiert werden soll.	Der Hostname muss die folgenden Kriterien erfüllen: • Der Name darf keine Zeichen aus Doppelbytezeichensätzen (DBCS) und keine Unterstreichungszeichen (_) enthalten. • Der Hostname darf zwar einen Bindestrich (–) enthalten, jedoch nicht als letztes Zeichen.
Berechtigungsnachweise für die Installation	Für die Installation des Operations Center müssen Sie das folgende Benutzerkonto verwenden: • AIX-BetriebssystemeLinux-BetriebssystemeRootbenutzer • Windows-BetriebssystemeAdministrator

Informationen	Details

Operations Center-Installationsverzeichnis	Das Operations Center wird im Unterverzeichnis ui des Installationsverzeichnisses installiert.
	
	Der folgende Pfad ist der Standardpfad für das Operations Center-Installationsverzeichnis:
	
	• AIX-BetriebssystemeLinux-Betriebssysteme/opt/tivoli/tsm
	Wenn Sie beispielsweise diesen Standardpfad verwenden, wird das Operations Center in dem folgenden Verzeichnis installiert:
	
	`/opt/tivoli/tsm/ui`
	
	• Windows-Betriebssystemec:\Programme\Tivoli\TSM
	Wenn Sie beispielsweise diesen Standardpfad verwenden, wird das Operations Center in dem folgenden Verzeichnis installiert:
	
	`c:\Programme\Tivoli\TSM\ui`
	
	Der Installationsverzeichnispfad muss die folgenden Kriterien erfüllen:
	
	• Der Pfad darf maximal 128 Zeichen enthalten.
	• Der Pfad darf nur ASCII-Zeichen enthalten.
	• Der Pfad darf keine nicht anzeigbaren Steuerzeichen enthalten.
	• Der Pfad darf keines der folgenden Zeichen enthalten:
	
	`% | < > ' " $ & ; *`

IBM Installation Manager-Installationsverzeichnis	Der folgende Pfad ist der Standardpfad für das IBM Installation Manager-Installationsverzeichnis: • AIX-BetriebssystemeLinux-Betriebssysteme/opt/IBM/InstallationManager • Windows-BetriebssystemeC:\Programme\IBM\Installation Manager
Vom Operations Center-Web-Server verwendete Anschlussnummer.	Der Wert für die sichere (HTTPS) Anschlussnummer muss die folgenden Kriterien erfüllen: • Die Nummer muss eine ganze Zahl im Bereich von 1024 bis 65535 sein. • Die Nummer darf nicht bereits im Gebrauch oder anderen Programmen zugeordnet sein. Wenn Sie keine Anschlussnummer angeben, lautet der Standardwert `11090`. Tipp: Wenn Sie sich später nicht mehr an die angegebene Anschlussnummer erinnern können, schauen Sie in der folgenden Datei nach (*Installationsverzeichnis* steht für das Verzeichnis, in dem das Operations Center installiert ist): • AIX-BetriebssystemeLinux-Betriebssysteme *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer/bootstrap.properties • Windows-Betriebssysteme *Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer\bootstrap.properties Die Datei bootstrap.properties enthält die Verbindungsdaten des IBM Spectrum Protect-Servers.

Informationen	Details
Kennwort für die sichere Kommunikation	Das Operations Center verwendet HTTPS (Hypertext Transfer Protocol Secure) für die Kommunikation mit Web-Browsern. Für das Operations Center ist die sichere Kommunikation zwischen dem Server und dem Operations Center erforderlich. Um die Kommunikation zu schützen, müssen Sie das TLS-Zertifikat des Hub-Servers zur Truststore-Datei des Operations Center hinzufügen (TLS = Transport Layer Security). Die Truststore-Datei des Operations Center enthält das Zertifikat, das das Operations Center für die HTTPS-Kommunikation mit Web-Browsern verwendet. Während der Installation des Operations Center erstellen Sie ein Kennwort für die Truststore-Datei. Wenn Sie die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server einrichten zu können, müssen Sie dasselbe Kennwort verwenden, um das Zertifikat des Hub-Servers der Truststore-Datei hinzuzufügen. Das Kennwort für die Truststore-Datei muss die folgenden Kriterien erfüllen: • Das Kennwort darf mindestens 6 Zeichen und maximal 64 Zeichen enthalten. • Das Kennwort muss mindestens die folgenden Zeichen enthalten: ◦ Einen Großbuchstaben (A – Z) ◦ Einen Kleinbuchstaben (a – z) ◦ Eine Ziffer (0 – 9) ◦ Zwei der nachfolgend aufgelisteten nicht alphanumerischen Zeichen: `~ ! @ # $ % ^ & * _ - + = ` |`  `( ) { } [ ] : ; < > , . ? /`

Zugehörige Tasks:
Sichere Kommunikation konfigurieren
Kennwort für die Truststore-Datei des Operations Center zurücksetzen
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Operations Center installieren

Sie können das Operations Center mit jeder der folgenden Methoden installieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

Vorbereitende Schritte

Sie können das Operations Center erst konfigurieren, nachdem Sie den IBM Spectrum Protect-Server installiert, konfiguriert und gestartet haben. Daher installieren Sie vor der Installation des Operations Center das entsprechende Serverpaket gemäß den in Voraussetzungen für Hub- und Peripherieserver aufgeführten Voraussetzungen bezüglich der Serverversion.

Sie können das Operations Center auf demselben Computer wie den IBM Spectrum Protect-Server oder auf einem separaten Computer installieren.

- Operations Center-Installationspaket abrufen
  Das Installationspaket kann von einer IBM® Download-Site heruntergeladen werden, z. B. IBM Passport Advantage oder IBM Fix Central.
- Operations Center mit einem grafisch orientierten Assistenten installieren
  Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM Installation Manager installieren oder aktualisieren.
- Operations Center im Konsolenmodus installieren
  Sie können das Operations Center mithilfe der Befehlszeile im Konsolenmodus installieren oder aktualisieren.
- Operations Center im unbeaufsichtigten Modus installieren
  Sie können das Operations Center im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Operations Center-Installationspaket abrufen

Das Installationspaket kann von einer IBM® Download-Site heruntergeladen werden, z. B. IBM Passport Advantage oder IBM Fix Central.

Informationen zu diesem Vorgang

Nachdem Sie das Paket von einer IBM Download-Site abgerufen haben, müssen Sie die Installationsdateien extrahieren.

Vorgehensweise

Gehen Sie wie folgt vor, um die Installationsdateien für das Operations Center zu extrahieren. In den folgenden Schritten müssen Sie *Versionsnummer* durch die zu installierende Version des Operations Center ersetzen.

AIX-BetriebssystemeAuf AIX-Systemen:

a. Laden Sie die folgende Paketdatei in ein beliebiges Verzeichnis herunter:

```
Versionsnummer.000
-IBM-SPOC-AIX.bin
```

b. Stellen Sie sicher, dass Sie über die Ausführberechtigung für die Paketdatei verfügen.
Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

```
chmod a+x Versionsnummer.000-IBM-SPOC-AIX.bin
```

c. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

```
./Versionsnummer.000-IBM-SPOC-AIX.bin
```

Die sich selbst entpackende Paketdatei wird in das Verzeichnis extrahiert.

Linux-BetriebssystemeAuf Linux-Systemen:

a. Laden Sie eine der folgenden Paketdateien in ein beliebiges Verzeichnis herunter:
   - *Versionsnummer*.000-IBM-SPOC-LinuxS390.bin
   - *Versionsnummer*.000-IBM-SPOC-Linuxx86_64.bin

b. Stellen Sie sicher, dass Sie über die Ausführberechtigung für die Paketdatei verfügen.
Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

```
chmod a+x Paketname.bin
```

c. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

```
./Paketname.bin
```

Die sich selbst entpackende Paketdatei wird in das Verzeichnis extrahiert.

Windows-BetriebssystemeAuf Windows-Systemen:

a. Laden Sie die folgende Paketdatei in ein beliebiges Verzeichnis herunter:

```
Versionsnummer.000-IBM-SPOC-WindowsX64.exe
```

b. Klicken Sie im Windows Explorer doppelt auf den Dateinamen, um die Installationsdateien zu extrahieren.

Die sich selbst entpackende Paketdatei wird in das Verzeichnis extrahiert.

AIX-Betriebssysteme
Linux-Betriebssysteme
Windows-Betriebssysteme

Operations Center mit einem grafisch orientierten Assistenten installieren

Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM® Installation Manager installieren oder aktualisieren.

AIX-Betriebssysteme

Vorbereitende Schritte

Wenn die folgenden RPM-Dateien auf dem Computer nicht installiert sind, installieren Sie sie. Anweisungen siehe RPM-Dateien für den grafisch orientierten Assistenten installieren.

- atk-1.12.3-2.aix5.2.ppc.rpm
- cairo-1.8.8-1.aix5.2.ppc.rpm
- expat-2.0.1-1.aix5.2.ppc.rpm
- fontconfig-2.4.2-1.aix5.2.ppc.rpm
- freetype2-2.3.9-1.aix5.2.ppc.rpm
- gettext-0.10.40-6.aix5.1.ppc.rpm
- glib2-2.12.4-2.aix5.2.ppc.rpm
- gtk2-2.10.6-4.aix5.2.ppc.rpm
- libjpeg-6b-6.aix5.1.ppc.rpm
- libpng-1.2.32-2.aix5.2.ppc.rpm
- libtiff-3.8.2-1.aix5.2.ppc.rpm
- pango-1.14.5-4.aix5.2.ppc.rpm
- pixman-0.12.0-3.aix5.2.ppc.rpm
- xcursor-1.1.7-3.aix5.2.ppc.rpm
- xft-2.1.6-5.aix5.1.ppc.rpm

- xrender-0.9.1-3.aix5.2.ppc.rpm
- zlib-1.2.3-3.aix5.1.ppc.rpm

Vorgehensweise

1. Geben Sie in dem Verzeichnis, in dem die Operations Center-Installationspaketdatei extrahiert wurde, den folgenden Befehl aus:
   - AIX-BetriebssystemeLinux-Betriebssysteme`./install.sh`
   - Windows-Betriebssysteme`install.bat`
2. Führen Sie die Installation der IBM Installation Manager- und Operations Center-Pakete gemäß den Anweisungen des Assistenten aus.
   AIX-BetriebssystemeWenn Ihre Ländereinstellung die UTF-8-Codierung verwendet, kann die folgende Nachricht angezeigt werden und der Installationsassistent kann langsam sein:

   ```
   Schriftartgruppe kann nicht erstellt werden
   ```

   Wird diese Nachricht angezeigt, führen Sie einen der folgenden Schritte aus:
   - Ersetzen Sie die Ländereinstellung durch eine, die keine UTF-8-Codierung verwendet. Informationen zu Sprachenoptionswerten, die keine UTF-8-Codierung verwenden, finden Sie in Voraussetzungen für die Sprache.
   - Installieren Sie das Operations Center mithilfe der Befehlszeile im Konsolenmodus.
   - Installieren Sie das Operations Center im unbeaufsichtigten Modus.

Nächste Schritte

Siehe Operations Center konfigurieren.

- AIX-BetriebssystemeRPM-Dateien für den grafisch orientierten Assistenten installieren
  Bevor Sie das Operations Center mit dem grafisch orientierten Assistenten von IBM Installation Manager installieren können, müssen bestimmte RPM-Dateien installiert werden.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Operations Center im Konsolenmodus installieren

Sie können das Operations Center mithilfe der Befehlszeile im Konsolenmodus installieren oder aktualisieren.

Vorgehensweise

1. Führen Sie in dem Verzeichnis, in dem die Installationspaketdatei extrahiert wurde, das folgende Programm aus:
   AIX-BetriebssystemeLinux-Betriebssysteme

   ```
   ./install.sh -c
   ```

   Windows-Betriebssysteme

   ```
   install.bat -c
   ```

2. Befolgen Sie die an der Konsole angezeigten Anweisungen, um die Pakete für Installation Manager und das Operations Center zu installieren.

Nächste Schritte

Siehe Operations Center konfigurieren.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Operations Center im unbeaufsichtigten Modus installieren

Sie können das Operations Center im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.

Vorbereitende Schritte

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis input zur Verfügung, in dem das Installationspaket extrahiert wird:

install_response_sample.xml
: Verwenden Sie diese Datei für die Installation des Operations Center.

update_response_sample.xml
: Verwenden Sie diese Datei für das Upgrade des Operations Center.

Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Erstellen Sie eine Antwortdatei. Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.
   Tipp: Zum Generieren einer Antwortdatei im Rahmen einer Installation im Konsolenmodus wählen Sie die Installationsoptionen im Konsolenmodus aus. Dann geben Sie in der Anzeige Zusammenfassung `G` ein, um die Antwortdatei entsprechend den zuvor ausgewählten Optionen zu generieren.
2. Erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.
   Wenn Sie die Datei install_response_sample.xml verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist *mein_Kennwort* das Kennwort:

   ```
   <variable name='ssl.password' value='mein_Kennwort' />
   ```

   Weitere Informationen zu diesem Kennwort finden Sie in Prüfliste für die Installation.
   Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei update_response_sample.xml aktualisieren.
3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.
   - AIX-Betriebssysteme Linux-Betriebssysteme

     ```
     ./install.sh -s -input Antwortdatei -acceptLicense
     ```

   - Windows-Betriebssysteme

     ```
     install.bat -s -input Antwortdatei -acceptLicense
     ```

Nächste Schritte

Siehe Operations Center konfigurieren.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Upgrade des Operations Center

Sie können ein Upgrade des Operations Center mit jeder der folgenden Methoden durchführen: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

Vorbereitende Schritte

Bevor Sie ein Upgrade des Operations Center durchführen, lesen Sie die Informationen zu den Systemvoraussetzungen und die Prüfliste für die Installation. Die Voraussetzungen und Anforderungen der neuen Version des Operations Center können von denen der momentan verwendeten Version abweichen.

Informationen zu diesem Vorgang

Die Anweisungen für das Upgrade des Operations Center sind mit Ausnahme der folgenden Punkte mit den Anweisungen für die Installation des Operations Center identisch:

- Sie verwenden nicht die Funktion Installieren von IBM® Installation Manager, sondern die Funktion Aktualisieren.
  Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.
- Wenn Sie ein Upgrade des Operations Center im unbeaufsichtigten Modus durchführen, können Sie den Schritt für die Erstellung eines Kennworts für die Truststore-Datei überspringen.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Erste Schritte mit dem Operations Center

Bevor Sie das Operations Center für die Verwaltung Ihrer Speicherumgebung verwenden können, müssen Sie es konfigurieren.

Informationen zu diesem Vorgang

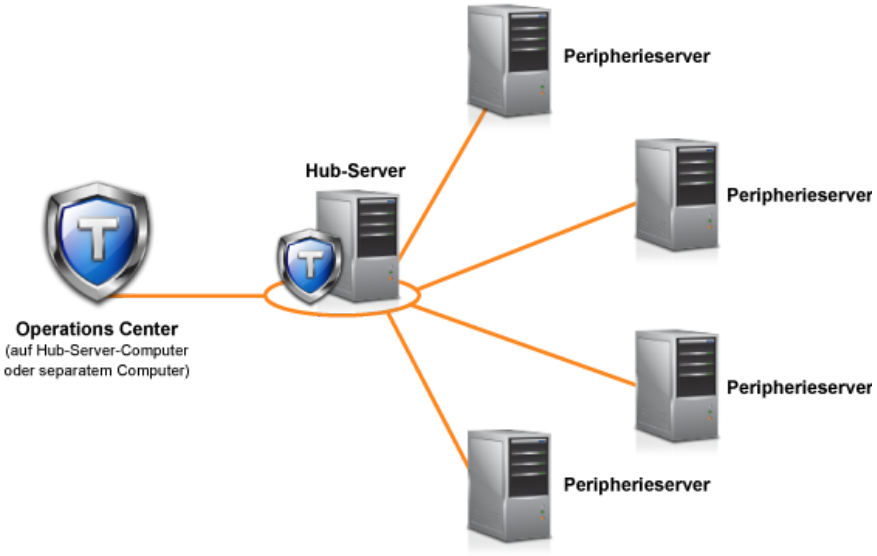
Führen Sie nach der Installation des Operations Center die folgenden Basiskonfigurationsschritte aus:

1. Legen Sie den Hub-Server fest.

2. Fügen Sie alle Peripherieserver hinzu.
3. Konfigurieren Sie wahlweise E-Mail-Alerts auf den Hub- und Peripherieservern.

Abbildung 1 veranschaulicht eine Operations Center-Konfiguration.

Abbildung 1. Beispiel einer Operations Center-Konfiguration mit Hub- und Peripherieservern



- Operations Center konfigurieren
  Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie es für die Verwaltung Ihrer Speicherumgebung konfigurieren. Sie müssen das Operations Center dem IBM Spectrum Protect-Server zuordnen, der als Hub-Server festgelegt ist. Anschließend können Sie weitere IBM Spectrum Protect-Server als Peripherieserver verbinden.
- Sichere Kommunikation konfigurieren
  Das Operations Center verwendet HTTPS (Hypertext Transfer Protocol Secure) für die Kommunikation mit Web-Browsern. Das TLS-Protokoll schützt die Kommunikation zwischen dem Operations Center und dem Hub-Server sowie zwischen dem Hub-Server und den zugeordneten Peripherieservern (TLS = Transport Layer Security).
- Web-Server starten und stoppen
  Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Das Stoppen und Starten des Web-Servers kann z. B. für Konfigurationsänderungen erforderlich sein.
- Operations Center öffnen
  Die Seite 'Übersicht' ist die Standardeingangssicht im Operations Center. In Ihrem Web-Browser können Sie jedoch für die Seite, die bei der Anmeldung beim Operations Center geöffnet werden soll, ein Lesezeichen setzen.
- Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen
  Der Clientverwaltungsservice erfasst Diagnoseinformationen über Clients für Sichern/Archivieren und stellt diese Informationen dem Operations Center für Basisüberwachungsfunktionen zur Verfügung.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Operations Center konfigurieren

Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie es für die Verwaltung Ihrer Speicherumgebung konfigurieren. Sie müssen das Operations Center dem IBM Spectrum Protect-Server zuordnen, der als Hub-Server festgelegt ist. Anschließend können Sie weitere IBM Spectrum Protect-Server als Peripherieserver verbinden.

- Hub-Server festlegen
  Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie angeben, welcher IBM Spectrum Protect-Server der Hub-Server ist.
- Peripherieserver hinzufügen
  Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server mindestens einen Peripherieserver hinzufügen.
- E-Mail-Alerts an Administratoren senden
  Ein Alert ist eine Benachrichtigung über ein relevantes Problem auf dem IBM Spectrum Protect-Server und wird durch eine Servernachricht ausgelöst. Alerts können im Operations Center angezeigt und vom Server per E-Mail an Administratoren gesendet werden.
- Angepassten Text in die Anmeldeanzeige einfügen
  Sie können angepassten Text, z. B. die Nutzungsbedingungen Ihres Unternehmens für die Software, zur Anmeldeanzeige des Operations Center hinzufügen, so dass die Benutzer des Operations Center den Text sehen, bevor sie ihren Benutzernamen und ihr Kennwort eingeben.
- REST-Services aktivieren
  Anwendungen, die REST-Services verwenden, können die Speicherumgebung abfragen und verwalten, indem eine Verbindung zum Operations Center hergestellt wird (REST = Representational State Transfer).

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Hub-Server festlegen

Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie angeben, welcher IBM Spectrum Protect-Server der Hub-Server ist.

Vorbereitende Schritte

Für das Operations Center ist die sichere Kommunikation zwischen dem Hub-Server und dem Operations Center erforderlich. Um die Kommunikation zu schützen, müssen Sie das TLS-Zertifikat des Hub-Servers zur Truststore-Datei des Operations Center hinzufügen (TLS = Transport Layer Security). Weitere Informationen finden Sie in Kommunikation zwischen Operations Center und Hub-Server schützen.

Vorgehensweise

Geben Sie die folgende Adresse in einem Web-Browser an. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist, und *sicherer_Anschluss* für die Anschlussnummer, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet:

```
https://Hostname:sicherer_Anschluss/oc
```

Tipps:

- Bei der URL muss die Groß-/Kleinschreibung beachtet werden. Achten Sie beispielsweise darauf, dass Sie "oc" wie gezeigt in Kleinbuchstaben eingeben.
- Weitere Informationen zu der Anschlussnummer finden Sie in Prüfliste für die Installation.
- Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie folgende Informationen angeben:
  - Verbindungsdaten für den Server, den Sie als Hub-Server festlegen wollen.
  - Berechtigungsnachweise zur Anmeldung für eine Administrator-ID, die für diesen Server definiert ist.
- Ist der Aufbewahrungszeitraum für Ereignisdatensätze des Servers kürzer als 14 Tage, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Hub-Server konfigurieren.

Nächste Schritte

Wenn Ihre Umgebung mehrere IBM Spectrum Protect-Server umfasst, fügen Sie die übrigen Server dem Hub-Server als Peripherieserver hinzu.

Achtung: Nachdem ein Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.
Zugehörige Konzepte:
Voraussetzungen für Hub- und Peripherieserver
Administrator-IDs, die für das Operations Center erforderlich sind
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Peripherieserver hinzufügen

Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server mindestens einen Peripherieserver hinzufügen.

Vorbereitende Schritte

Die Kommunikation zwischen dem Peripherieserver und dem Hub-Server muss mithilfe des TLS-Protokolls geschützt werden (TLS = Transport Layer Security). Um die Kommunikation zu schützen, müssen Sie das Zertifikat des Peripherieservers zur Truststore-Datei des Hub-Servers hinzufügen.

Vorgehensweise

1. Klicken Sie in der Menüleiste des Operations Center auf Server. Die Seite Server wird geöffnet.

   In der Tabelle auf der Seite Server kann ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass dieser Server zwar durch einen Administrator mit dem Befehl DEFINE SERVER für den Hub-Server definiert, aber noch nicht als Peripherieserver konfiguriert wurde.

2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
   - Wenn der Server, den Sie hinzufügen möchten, nicht in der Tabelle angezeigt wird und die sichere Kommunikation über SSL/TSL nicht erforderlich ist, klicken Sie auf + Peripherieserver in der Menüleiste der Tabelle.
3. Stellen Sie die erforderlichen Informationen bereit und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus. Tipp: Ist der Aufbewahrungszeitraum für Ereignisdatensätze des Servers kürzer als 14 Tage, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

Zugehörige Verweise:
DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

E-Mail-Alerts an Administratoren senden

Ein Alert ist eine Benachrichtigung über ein relevantes Problem auf dem IBM Spectrum Protect-Server und wird durch eine Servernachricht ausgelöst. Alerts können im Operations Center angezeigt und vom Server per E-Mail an Administratoren gesendet werden.

Vorbereitende Schritte

Bevor Sie die E-Mail-Benachrichtigung für Administratoren wegen Alerts konfigurieren, stellen Sie sicher, dass folgende Anforderungen erfüllt sind:

- Damit Alerts als E-Mail gesendet und empfangen werden können, ist ein SMTP-Server erforderlich und der Server, der die Alerts als E-Mail sendet, muss auf den SMTP-Server zugreifen können.
  Tipp: Wenn das Operations Center auf einem separaten Computer installiert ist, benötigt dieser Computer keinen Zugriff auf den SMTP-Server.
- Ein Administrator benötigt die Systemberechtigung, um die E-Mail-Benachrichtigung konfigurieren zu können.

Informationen zu diesem Vorgang

Eine E-Mail-Benachrichtigung wird nur für das erste Auftreten eines Alerts gesendet. Außerdem wird keine E-Mail-Benachrichtigung für einen Alert gesendet, wenn der Alert vor der Konfiguration der E-Mail-Benachrichtigung generiert wird.

Sie können die E-Mail-Benachrichtigung wie folgt konfigurieren:

- Benachrichtigung für einzelne Alerts senden
- Alertzusammenfassungen senden

Eine Alertzusammenfassung enthält Informationen zu aktuellen Alerts. Die Zusammenfassung beinhaltet die Gesamtzahl der Alerts, die Gesamtzahl der aktiven und inaktiven Alerts, den ältesten Alert, den neuesten Alert und den am häufigsten auftretenden Alert.

Sie können maximal drei Administratoren als Empfänger von Alertzusammenfassungen per E-Mail angeben. Alertzusammenfassungen werden ca. einmal stündlich gesendet.

Vorgehensweise

Gehen Sie auf jedem Hub- und Peripherieserver, von dem Sie E-Mail-Alerts erhalten wollen, wie folgt vor, um die E-Mail-Benachrichtigung für Administratoren wegen Alerts zu konfigurieren:

1. Geben Sie den folgenden Befehl aus, um zu überprüfen, dass die Alertüberwachung aktiviert ist:

   ```
   QUERY MONITORSETTINGS
   ```

2. Geben Sie den folgenden Befehl aus, wenn die Befehlsausgabe anzeigt, dass die Alertüberwachung inaktiviert ist. Andernfalls fahren Sie mit dem nächsten Schritt fort.

   ```
   SET ALERTMONITOR ON
   ```

3. Geben Sie den folgenden Befehl aus, um das Senden von E-Mail-Benachrichtigungen zu aktivieren:

   ```
   SET ALERTEMAIL ON
   ```

4. Geben Sie den folgenden Befehl aus, um den SMTP-Server zu definieren, der zum Senden von E-Mail-Benachrichtigungen verwendet wird:

   ```
   SET ALERTEMAILSMTPHOST Hostname
   ```

5. Geben Sie den folgenden Befehl aus, um die Anschlussnummer für den SMTP-Server anzugeben:

   ```
   SET ALERTEMAILSMTPPORT Anschlussnummer
   ```

   Die Standardanschlussnummer ist 25.

6. Geben Sie den folgenden Befehl aus, um die E-Mail-Adresse des Absenders der Alerts anzugeben:

   ```
   SET ALERTEMAILFROMADDR E-Mail-Adresse
   ```

7. Geben Sie für jede Administrator-ID, die E-Mail-Benachrichtigungen empfangen soll, einen der folgenden Befehle aus, um die E-Mail-Benachrichtigung zu aktivieren und um die E-Mail-Adresse anzugeben:

   ```
   REGISTER ADMIN Administratorname ALERT=YES EMAILADDRESS=E-Mail-Adresse
   ```

   ```
   UPDATE ADMIN Administratorname ALERT=YES EMAILADDRESS=E-Mail-Adresse
   ```

8. Wählen Sie eine oder beide der folgenden Optionen aus und geben Sie die Administrator-IDs an, die E-Mail-Benachrichtigungen empfangen sollen:
   - Benachrichtigung für einzelne Alerts senden
     Geben Sie einen der folgenden Befehle aus, um die Administrator-IDs anzugeben bzw. zu aktualisieren, die E-Mail-Benachrichtigungen für einen einzelnen Alert empfangen sollen:

     ```
     DEFINE ALERTTRIGGER Nachrichtennummer ADmin=Administratorname1,Administratorname2

     UPDATE ALERTTRIGGER Nachrichtennummer ADDadmin=Administratorname3 DELadmin=Administratorname1
     ```

     Tipp: Auf der Seite Alerts konfigurieren des Operations Center können Sie die Administratoren auswählen, die E-Mail-Benachrichtigungen erhalten sollen.
   - Alertzusammenfassungen senden
     Geben Sie den folgenden Befehl aus, um die Administrator-IDs anzugeben bzw. zu aktualisieren, die Alertzusammenfassungen per E-Mail erhalten sollen:

     ```
     SET ALERTSUMMARYTOADMINS Administratorname1,Administratorname2,Administratorname3
     ```

   Gehen Sie wie folgt vor, wenn Sie Alertzusammenfassungen, aber keine Benachrichtigungen über einzelne Alerts empfangen wollen:
   a. Setzen Sie die Benachrichtigung über einzelne Alerts wie in E-Mail-Alerts vorübergehend aussetzen beschrieben aus.
   b. Stellen Sie sicher, dass die betreffende Administrator-ID in dem folgenden Befehl aufgelistet ist:

      ```
      SET ALERTSUMMARYTOADMINS Administratorname1,Administratorname2,Administratorname3
      ```

E-Mail-Alerts an mehrere Administratoren senden

Das folgende Beispiel zeigt die Befehle, mit denen alle Alerts für Nachricht ANR1075E in einer E-Mail an die Administratoren `myadmin`, `djadmin` und `csadmin` gesendet werden:

```
SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin
```

- E-Mail-Alerts vorübergehend aussetzen
  E-Mail-Alerts können vorübergehend ausgesetzt werden, wenn bestimmte Situationen dies erforderlich machen. Sie möchten z. B. Alertzusammenfassungen erhalten, aber die Benachrichtigung über einzelne Alerts aussetzen oder Sie möchten die E-Mail-Benachrichtigung aussetzen, wenn ein Administrator im Urlaub ist.

Zugehörige Verweise:
DEFINE ALERTTRIGGER (Alertauslöser definieren)
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)
REGISTER ADMIN (Administrator-ID registrieren)
SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)
SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)
SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)
SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)
SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)
SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)
UPDATE ADMIN (Administrator aktualisieren)
UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)
 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Angepassten Text in die Anmeldeanzeige einfügen

Sie können angepassten Text, z. B. die Nutzungsbedingungen Ihres Unternehmens für die Software, zur Anmeldeanzeige des Operations Center hinzufügen, so dass die Benutzer des Operations Center den Text sehen, bevor sie ihren Benutzernamen und ihr Kennwort eingeben.

Vorgehensweise

Gehen Sie wie folgt vor, um angepassten Text zur Anmeldeanzeige hinzuzufügen:

1. Wechseln Sie auf dem Computer, auf dem das Operations Center installiert ist, in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):

    AIX-Betriebssysteme  Linux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer

   Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

2. Erstellen Sie in dem Verzeichnis eine Datei mit dem Namen loginText.html, die den Text enthält, den Sie zur Anmeldeanzeige hinzufügen wollen. Text mit Sonderzeichen, die keine ASCII-Zeichen sind, muss UTF-8-codiert sein.
   Tipp: Sie können den Text mit HTML-Tags formatieren.
3. Überprüfen Sie den hinzugefügten Text in der Anmeldeanzeige des Operations Center.
   Geben Sie die folgende Adresse in einem Web-Browser an, um das Operations Center zu öffnen. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist, und *sicherer_Anschluss* für die Anschlussnummer, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet:

   ```
   https://Hostname:sicherer_Anschluss/oc
   ```

REST-Services aktivieren

Anwendungen, die REST-Services verwenden, können die Speicherumgebung abfragen und verwalten, indem eine Verbindung zum Operations Center hergestellt wird (REST = Representational State Transfer).

Informationen zu diesem Vorgang

Aktivieren Sie dieses Feature, um REST-Services eine Interaktion mit Hub- und Peripherieservern zu ermöglichen. Dabei werden Aufrufe an die folgende Adresse gesendet:

```
https://OC-Hostname:Anschluss/oc/api
```

Hierbei steht *OC-Hostname* für den Netznamen oder die IP-Adresse des Hostsystems des Operations Center und *Anschluss* für die Anschlussnummer des Operations Center. Die Standardanschlussnummer ist 11090.
Informationen zu den für das Operations Center verfügbaren REST-Services finden Sie in Technote http://www.ibm.com/support/docview.wss?uid=swg21973011 oder geben Sie den folgenden REST-Aufruf aus:

```
https://OC-Hostname:Anschluss/oc/api/help
```

Vorgehensweise

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für die Einstellungen und klicken Sie auf Einstellungen.
2. Wählen Sie auf der Seite 'Allgemein' das Kontrollkästchen Verwaltungs-REST-API aktivieren aus.
3. Klicken Sie auf Speichern.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Sichere Kommunikation konfigurieren

Das Operations Center verwendet HTTPS (Hypertext Transfer Protocol Secure) für die Kommunikation mit Web-Browsern. Das TLS-Protokoll schützt die Kommunikation zwischen dem Operations Center und dem Hub-Server sowie zwischen dem Hub-Server und den zugeordneten Peripherieservern (TLS = Transport Layer Security).

Informationen zu diesem Vorgang

TLS 1.2 ist für die sichere Kommunikation zwischen dem IBM Spectrum Protect-Server und dem Operations Center sowie zwischen dem Hub-Server und den Peripherieservern erforderlich.

- Kommunikation zwischen Operations Center und Hub-Server schützen
  Um die Kommunikation zwischen dem Operations Center und dem Hub-Server zu schützen, müssen Sie das TLS-Zertifikat (Transport Layer Security) des Hub-Servers der Truststore-Datei des Operations Center hinzufügen.
- Kommunikation zwischen Hub-Server und Peripherieserver schützen
  Sie müssen das Zertifikat des Peripherieservers im Hub-Server definieren, um die Kommunikation zwischen dem Hub-Server und einem Peripherieserver mithilfe des TLS-Protokolls zu schützen (TLS = Transport Layer Security). Außerdem müssen Sie im Operations Center die Überwachung des Peripherieservers konfigurieren.
- Kennwort für die Truststore-Datei des Operations Center zurücksetzen
  Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server einrichten zu können, müssen Sie das Kennwort für die Truststore-Datei des Operations Center kennen. Sie erstellen dieses Kennwort während der Installation des Operations Center. Wenn Sie das Kennwort nicht kennen, können Sie es zurücksetzen.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Kommunikation zwischen Operations Center und Hub-Server schützen

Um die Kommunikation zwischen dem Operations Center und dem Hub-Server zu schützen, müssen Sie das TLS-Zertifikat (Transport Layer Security) des Hub-Servers der Truststore-Datei des Operations Center hinzufügen.

Vorbereitende Schritte

Die Truststore-Datei des Operations Center ist ein Container für Zertifikate, auf den das Operations Center zugreifen kann. Die Truststore-Datei enthält das Zertifikat, das das Operations Center für die HTTPS-Kommunikation mit Web-Browsern verwendet.

Während der Installation des Operations Center erstellen Sie ein Kennwort für die Truststore-Datei. Um die Kommunikation zwischen dem Operations Center und dem Hub-Server zu schützen, müssen Sie dasselbe Kennwort verwenden, um das Zertifikat des Hub-Servers der Truststore-Datei hinzuzufügen. Wenn Sie dieses Kennwort vergessen haben, können Sie es zurücksetzen. Siehe Kennwort für die Truststore-Datei des Operations Center zurücksetzen.

Vorgehensweise

1. Geben Sie das Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers an.

   Gehen Sie wie folgt vor, um cert256.arm als Standardzertifikat anzugeben:

   a. Geben Sie den folgenden Befehl im Verzeichnis der Hub-Server-Instanz aus:

   ```
   gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
    -label "TSM Server SelfSigned SHA Key"
   ```

   b. Starten Sie den Hub-Server erneut, damit er die Änderungen der Schlüsseldatenbankdatei übernehmen kann.
2. Geben Sie den folgenden Befehl aus, um zu überprüfen, ob das Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers definiert ist:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

3. Stoppen Sie den Web-Server des Operations Center.
4. Rufen Sie die Befehlszeile des Betriebssystems auf, auf dem das Operations Center installiert ist.
5. Verwenden Sie den Befehl iKeycmd oder iKeyman, um das Zertifikat der Truststore-Datei des Operations Center hinzuzufügen. Mit dem Befehl iKeyman wird die grafische Benutzerschnittstelle von IBM® Key Management geöffnet und iKeycmd ist eine Befehlszeilenschnittstelle.
   Geben Sie den Befehl iKeycmd aus, um das SSL-Zertifikat cert256.arm über die Befehlszeilenschnittstelle als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers hinzuzufügen:

   ```
   ikeycmd -cert -add
   -db /Installationsverzeichnis/Liberty/usr/servers/guiServer/gui-truststore.jks
   -file /fvt/comfrey/srv/cert256.arm
   -label 'Kennsatzbeschreibung'
   -pw 'Kennwort' -type jks -format ascii -trust enable
   ```

   Hierbei gilt Folgendes:

   Installationsverzeichnis
   : Das Verzeichnis, in dem das Operations Center installiert ist.

   Kennsatzbeschreibung
   : Die Beschreibung, die Sie dem Kennsatz zuordnen.

   Kennwort
   : Das Kennwort, das Sie bei der Installation des Operations Center erstellt haben. Wenn Sie das Kennwort zurücksetzen wollen, deinstallieren Sie das Operations Center, löschen Sie die Datei .jks und installieren Sie das Operations Center erneut.

   Gehen Sie wie folgt vor, um das Zertifikat mithilfe des Fensters 'IBM Key Management' hinzuzufügen:

   a. Wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):
      - AIX-BetriebssystemeLinux-Betriebssysteme*Installationsverzeichnis*/ui/jre/bin
      - Windows-Betriebssysteme*Installationsverzeichnis*\ui\jre\bin

   b. Geben Sie den folgenden Befehl aus, um das Fenster IBM Key Management zu öffnen:

   ```
   ikeyman
   ```

   c. Klicken Sie auf Schlüsseldatenbankdatei > Öffnen.
   d. Klicken Sie im Fenster Öffnen auf Durchsuchen und wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):
      - AIX-BetriebssystemeLinux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
      - Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

   e. Wählen Sie im Verzeichnis guiServer die Datei gui-truststore.jks aus.
   f. Klicken Sie auf Öffnen und dann auf OK.
   g. Geben Sie das Kennwort für die Truststore-Datei ein und klicken Sie auf OK.
   h. Klicken Sie im Bereich Schlüsseldatenbankinhalt des Fensters IBM Key Management auf den Pfeil und wählen Sie Zertifikate des Unterzeichners in der Liste aus.
   i. Klicken Sie auf Hinzufügen.
   j. Klicken Sie im Fenster Öffnen auf Durchsuchen und wechseln Sie in das Verzeichnis der Hub-Server-Instanz (siehe das folgende Beispiel).

- AIX-BetriebssystemeLinux-Betriebssysteme/opt/tivoli/tsm/server/bin
- Windows-Betriebssystemec:\Programme\Tivoli\TSM\server1

Das Verzeichnis enthält das Zertifikat cert256.arm.

Wenn Sie im Fenster Öffnen nicht auf das Verzeichnis der Hub-Server-Instanz zugreifen können, gehen Sie wie folgt vor:

i. Kopieren Sie die Datei cert256.arm mithilfe von FTP oder einer anderen Dateiübertragungsmethode vom Hub-Server in das folgende Verzeichnis auf dem Computer, auf dem das Operations Center installiert ist:
   - AIX-BetriebssystemeLinux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

ii. Wechseln Sie im Fenster Öffnen in das Verzeichnis guiServer.

k. Wählen Sie das Zertifikat cert256.arm aus.
Tipp: Das von Ihnen ausgewählte Zertifikat muss als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers definiert sein. Weitere Informationen finden Sie unter Schritt 1 und 2.

l. Klicken Sie auf Öffnen und dann auf OK.

m. Geben Sie eine Bezeichnung für das Zertifikat ein. Geben Sie beispielsweise den Namen des Hub-Servers ein.

n. Klicken Sie auf OK. Das SSL-Zertifikat des Hub-Servers wird der Truststore-Datei hinzugefügt und die Bezeichnung im Bereich Schlüsseldatenbankinhalt des Fensters IBM Key Management angezeigt.

o. Schließen Sie das Fenster IBM Key Management.

6. Starten Sie den Web-Server des Operations Center.
7. Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie die IP-Adresse oder den Netznamen des Hub-Servers und die Anschlussnummer für die Kommunikation mit dem Hub-Server angeben. Ist die Serveroption ADMINONCLIENTPORT für den IBM Spectrum Protect-Server aktiviert, geben Sie die durch die Serveroption TCPADMINPORT angegebene Anschlussnummer ein. Ist die Serveroption ADMINONCLIENTPORT nicht aktiviert, geben Sie die durch die Serveroption TCPPORT angegebene Anschlussnummer ein.
   Wenn das Operations Center bereits konfiguriert wurde, können Sie den Inhalt der Datei serverConnection.properties überprüfen, um die Verbindungsdaten zu verifizieren. Die Datei serverConnection.properties befindet sich in dem folgenden Verzeichnis auf dem Computer, auf dem das Operations Center installiert ist:
   - AIX-BetriebssystemeLinux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

Nächste Schritte

Informationen zur Konfiguration der SSL-Kommunikation zwischen dem Hub-Server und einem Peripherieserver finden Sie in Kommunikation zwischen Hub-Server und Peripherieserver schützen.

Zugehörige Verweise:
QUERY OPTION (Serveroptionen abfragen)
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Kommunikation zwischen Hub-Server und Peripherieserver schützen

Sie müssen das Zertifikat des Peripherieservers im Hub-Server definieren, um die Kommunikation zwischen dem Hub-Server und einem Peripherieserver mithilfe des TLS-Protokolls zu schützen (TLS = Transport Layer Security). Außerdem müssen Sie im Operations Center die Überwachung des Peripherieservers konfigurieren.

Vorgehensweise

1. Wechseln Sie auf dem Peripherieserver in das Verzeichnis der Peripherieserverinstanz.
2. Geben Sie das erforderliche Zertifikat cert256.arm als Standardzertifikat in der Schlüsseldatenbankdatei des Peripherieservers an. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed
 -label "TSM Server SelfSigned SHA Key"
```

3. Überprüfen Sie die Zertifikate in der Schlüsseldatenbankdatei des Peripherieservers. Geben Sie den folgenden Befehl aus:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

4. Übertragen Sie die Datei cert256.arm des Peripherieservers sicher an den Hub-Server.
5. Wechseln Sie auf dem Hub-Server in das Verzeichnis der Hub-Server-Instanz.
6. Definieren Sie das Zertifikat des Peripherieservers im Hub-Server. Geben Sie den folgenden Befehl im Verzeichnis der Hub-Server-Instanz aus. Hierbei steht *Peripherieservername* für den Namen des Peripherieservers und *Peripherie_cert256.arm* für den Dateinamen des Zertifikats des Peripherieservers.

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
 -label Peripherieservername -file Peripherie_cert256.arm
```

Der Peripherieserver benötigt nicht das Hub-Server-Zertifikat für die Kommunikation zwischen Hub-Server und Peripherieserver. In anderen Serverkonfigurationen, die Server mit Querdefinition benötigen, muss der Peripherieserver jedoch über das Hub-Server-Zertifikat verfügen.

7. Starten Sie den Hub-Server und den Peripherieserver neu.
8. Geben Sie für den Hub-Server den Befehl DEFINE SERVER gemäß dem folgenden Beispiel aus:

   ```
   DEFINE SERVER Peripherieservername HLA=Peripherieserveradresse
    LLA=spoke_SSLTCPADMINPort SERVERPA=Peripherieserverkennwort
   ```

   Tipp: Außer beim Senden oder Empfangen von Objektdaten durch den Server ist die Serverkommunikation standardmäßig verschlüsselt. Objektdaten werden mithilfe von TCP/IP gesendet und empfangen. Durch die Nichtverschlüsselung von Objektdaten entspricht die Serverleistung in etwa der Kommunikation über eine TCP/IP-Sitzung und die Sitzung ist sicher. Soll die gesamte Kommunikation mit dem angegebenen Server verschlüsselt werden, auch wenn der Server Objektdaten sendet und empfängt, müssen Sie im Befehl DEFINE SERVER den Parameter SSL=YES angeben.
9. Klicken Sie in der Menüleiste des Operations Center auf Server.

   In der Tabelle auf der Seite Server hat der in Schritt 8 definierte Peripherieserver normalerweise den Status 'Nicht überwacht'. Je nach Einstellung des Statusaktualisierungsintervalls wird der Peripherieserver möglicherweise nicht sofort angezeigt.

10. Klicken Sie auf den Peripherieserver, um den Eintrag hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.

Zugehörige Verweise:
DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
QUERY OPTION (Serveroptionen abfragen)
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Kennwort für die Truststore-Datei des Operations Center zurücksetzen

Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server einrichten zu können, müssen Sie das Kennwort für die Truststore-Datei des Operations Center kennen. Sie erstellen dieses Kennwort während der Installation des Operations Center. Wenn Sie das Kennwort nicht kennen, können Sie es zurücksetzen.

Informationen zu diesem Vorgang

Um das Kennwort zurückzusetzen, müssen Sie ein neues Kennwort erstellen, die Truststore-Datei des Operations Center löschen und den Web-Server des Operations Center erneut starten.

Vorgehensweise

1. Stoppen Sie den Web-Server des Operations Center.
2. Wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):
   - AIX-BetriebssystemeLinux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer
3. Öffnen Sie die Datei bootstrap.properties, die das Kennwort für die Truststore-Datei enthält. Wenn das Kennwort nicht verschlüsselt ist, können Sie damit die Truststore-Datei öffnen, ohne es zurücksetzen zu müssen.
   Die folgenden Beispiele zeigen den Unterschied zwischen einem verschlüsselten und einem nicht verschlüsselten Kennwort:

   Beispiel eines verschlüsselten Kennworts
   Verschlüsselte Kennwörter beginnen mit der Zeichenfolge `{xor}`.
   Das folgende Beispiel zeigt das verschlüsselte Kennwort als Wert des Parameters tsm.truststore.pswd:

   ```
   tsm.truststore.pswd={xor}MiYPPiwsKDAtOw==
   ```

   Beispiel eines nicht verschlüsselten Kennworts
   Das folgende Beispiel zeigt das nicht verschlüsselte Kennwort als Wert des Parameters tsm.truststore.pswd:

   ```
   tsm.truststore.pswd=J8b%^B
   ```

4. Sie setzen das Kennwort zurück, indem Sie das Kennwort in der Datei bootstrap.properties durch ein neues Kennwort ersetzen. Sie können das Kennwort durch ein verschlüsseltes Kennwort oder durch ein nicht verschlüsseltes Kennwort ersetzen. Merken Sie sich das nicht verschlüsselte Kennwort für eine spätere Verwendung.
   Gehen Sie wie folgt vor, um ein verschlüsseltes Kennwort zu erstellen:
   a. Erstellen Sie ein nicht verschlüsseltes Kennwort.
      Das Kennwort für die Truststore-Datei muss die folgenden Kriterien erfüllen:
      - Das Kennwort darf mindestens 6 Zeichen und maximal 64 Zeichen enthalten.
      - Das Kennwort muss mindestens die folgenden Zeichen enthalten:
        - Einen Großbuchstaben (A – Z)
        - Einen Kleinbuchstaben (a – z)
        - Eine Ziffer (0 – 9)
        - Zwei der nachfolgend aufgelisteten nicht alphanumerischen Zeichen:

          ```
          ~ ! @ # $ % ^ & * _ - + = ` |

          ( ) { } [ ] : ; < > , . ? /
          ```

b. Wechseln Sie über die Befehlszeile des Betriebssystems in das folgende Verzeichnis:
   - AIX-Betriebssysteme Linux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/bin
   - Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\bin

c. Geben Sie den folgenden Befehl aus, um das Kennwort zu verschlüsseln (`mein_Kennwort` ist das nicht verschlüsselte Kennwort):
   - AIX-Betriebssysteme Linux-Betriebssysteme`securityUtility encode mein_Kennwort`
   - Windows-Betriebssysteme`securityUtility.bat encode mein_Kennwort`

   Windows-BetriebssystemeDie folgende Nachricht könnte angezeigt werden:

   ```
   ! Der Befehl "java" ist entweder falsch geschrieben
   oder konnte nicht gefunden werden.
   ```

   Wenn diese Nachricht angezeigt wird, führen Sie folgende Schritte aus:

   i. Geben Sie den folgenden Befehl aus (`Installationsverzeichnis` ist das Verzeichnis, in dem das Operations Center installiert ist):

   ```
   set JAVA_HOME="Installationsverzeichnis\ui\jre"
   ```

   ii. Geben Sie den folgenden Befehl erneut aus, um das Kennwort zu verschlüsseln:

   ```
   securityUtility.bat encode mein_Kennwort
   ```

5. Schließen Sie die Datei bootstrap.properties.
6. Wechseln Sie in das folgende Verzeichnis:
   - AIX-Betriebssysteme Linux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer
7. Löschen Sie die Truststore-Datei gui-truststore.jks des Operations Center.
8. Starten Sie den Web-Server des Operations Center.

Ergebnisse

Eine neue Truststore-Datei wird automatisch für das Operations Center erstellt und das TLS-Zertifikat des Operations Center wird automatisch in die Truststore-Datei eingefügt.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Web-Server starten und stoppen

Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Das Stoppen und Starten des Web-Servers kann z. B. für Konfigurationsänderungen erforderlich sein.

Vorgehensweise

Stoppen Sie den Web-Server und starten Sie ihn erneut.

- AIX-BetriebssystemeGeben Sie im Verzeichnis /*Installationsverzeichnis*/ui/utils die folgenden Befehle aus (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):
  - Zum Stoppen des Servers:

    ```
    ./stopserver.sh
    ```

  - Zum Starten des Servers:

    ```
    ./startserver.sh
    ```

- Linux-BetriebssystemeGeben Sie die folgenden Befehle aus:
  - Zum Stoppen des Servers:

    ```
    service opscenter.rc stop
    ```

  - Zum Starten des Servers:

    ```
    service opscenter.rc start
    ```

  - Zum erneuten Starten des Servers:

    ```
    service opscenter.rc restart
    ```

  Geben Sie den folgenden Befehl aus, um festzustellen, ob der Server ausgeführt wird:

  ```
  service opscenter.rc status
  ```

- Windows-BetriebssystemeIm Fenster Dienste stoppen bzw. starten Sie den Dienst 'Operations Center'.

Operations Center öffnen

Die Seite 'Übersicht' ist die Standardeingangssicht im Operations Center. In Ihrem Web-Browser können Sie jedoch für die Seite, die bei der Anmeldung beim Operations Center geöffnet werden soll, ein Lesezeichen setzen.

Vorgehensweise

1. Geben Sie die folgende Adresse in einem Web-Browser an. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist, und *sicherer_Anschluss* für die Anschlussnummer, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet:

   `https://Hostname:sicherer_Anschluss/oc`

   Tipps:
   - Bei der URL muss die Groß-/Kleinschreibung beachtet werden. Achten Sie beispielsweise darauf, dass Sie "oc" wie gezeigt in Kleinbuchstaben eingeben.
   - Die Standardanschlussnummer für HTTPS-Kommunikation lautet 11090. Während der Installation des Operations Center kann jedoch eine andere Anschlussnummer angegeben werden.
2. Melden Sie sich unter Verwendung einer Administrator-ID an, die auf dem Hub-Server registriert ist.

   Auf der Seite 'Übersicht' können Sie Übersichtsdaten für Clients, Services, Server, Speicherpools und Speichereinheiten anzeigen. Sie können weitere Details anzeigen, indem Sie auf die Elemente klicken oder indem Sie die Menüleiste des Operations Center verwenden.

   Überwachung über eine mobile Einheit: Um die Speicherumgebung über Fernzugriff zu überwachen, können Sie die Seite 'Übersicht' des Operations Center im Web-Browser einer mobilen Einheit anzeigen. Das Operations Center unterstützt den Apple Safari-Web-Browser auf dem iPad. Es können auch andere mobile Einheiten verwendet werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen

Der Clientverwaltungsservice erfasst Diagnoseinformationen über Clients für Sichern/Archivieren und stellt diese Informationen dem Operations Center für Basisüberwachungsfunktionen zur Verfügung.

Informationen zu diesem Vorgang

Nach der Installation des Clientverwaltungsservice können Sie die Diagnoseseite im Operations Center aufrufen, um Fehlerbehebungsinformationen für Clients für Sichern/Archivieren anzuzeigen.

Diagnoseinformationen können nur von Linux- und Windows-Clients erfasst werden. Administratoren können jedoch die Diagnoseinformationen unter AIX, Linux oder Windows im Operations Center anzeigen.

Sie können den Clientverwaltungsservice auch auf Knoten mit Einheiten zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware installieren, um Diagnoseinformationen über die Einheiten zum Versetzen von Daten zu erfassen.

Tipp: In der Dokumentation für den Clientverwaltungsservice ist *Clientsystem* das System, in dem der Client für Sichern/Archivieren installiert ist.

- Clientverwaltungsservice mit einem grafisch orientierten Assistenten installieren
  Sie müssen den Clientverwaltungsservice auf den von Ihnen verwalteten Clientsystemen installieren, um Diagnoseinformationen über Clients für Sichern/Archivieren (z. B. Clientprotokolldateien) zu erfassen.
- Clientverwaltungsservice im unbeaufsichtigten Modus installieren
  Sie können den Clientverwaltungsservice im unbeaufsichtigten Modus installieren. Im unbeaufsichtigten Modus geben Sie die Installationswerte in einer Antwortdatei an und führen anschließend einen Installationsbefehl aus.
- Überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert wurde
  Bevor Sie Diagnoseinformationen über einen Client für Sichern/Archivieren mit dem Clientverwaltungsservice erfassen, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert wurde.
- Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren
  Wenn Sie nicht die Standardkonfiguration für den Clientverwaltungsservice verwenden, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.
- Clientverwaltungsservice starten und stoppen
  Der Clientverwaltungsservice wird nach seiner Installation auf dem Clientsystem automatisch gestartet. Sie müssen den Service in bestimmten Situationen möglicherweise stoppen und starten.
- Clientverwaltungsservice deinstallieren
  Wenn Sie keine Clientdiagnoseinformationen mehr erfassen müssen, können Sie den Clientverwaltungsservice im Clientsystem deinstallieren.
- Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren
  Der Clientverwaltungsservice verwendet Informationen in der Clientkonfigurationsdatei (client-configuration.xml), um Diagnoseinformationen zu erkennen. Wenn der Clientverwaltungsservice die Position der Protokolldateien nicht erkennen kann, müssen Sie das Dienstprogramm CmsConfig ausführen, um die Position der Protokolldateien zur Datei client-configuration.xml hinzuzufügen.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Clientverwaltungsservice mit einem grafisch orientierten Assistenten installieren

Sie müssen den Clientverwaltungsservice auf den von Ihnen verwalteten Clientsystemen installieren, um Diagnoseinformationen über Clients für Sichern/Archivieren (z. B. Clientprotokolldateien) zu erfassen.

Vorbereitende Schritte

Lesen Sie den Abschnitt Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices.

Informationen zu diesem Vorgang

Sie müssen den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren installieren.

Vorgehensweise

1. Laden Sie das Installationspaket für den Clientverwaltungsservice von einer IBM® Download-Site, z. B. IBM Passport Advantage oder IBM Fix Central, herunter. Suchen Sie nach einem Dateinamen, der etwa wie folgt lautet: `<Version>-IBM-SPCMS-<Betriebssystem>.bin`.

   Die folgende Tabelle enthält die Namen der Installationspakete.

Clientbetriebssystem	Installationspaketname
Linux x86 64-Bit	8.1.x.000-IBM-SPCMS-Linuxx64.bin
Windows 32-Bit	8.1.x.000-IBM-SPCMS-Windows32.exe
Windows 64-Bit	8.1.x.000-IBM-SPCMS-Windows64.exe

2. Erstellen Sie ein Verzeichnis auf dem Clientsystem, das Sie verwalten wollen, und kopieren Sie das Installationspaket dorthin.
3. Extrahieren Sie den Inhalt der Installationspaketdatei.
   - Gehen Sie in Linux-Clientsystemen wie folgt vor:
     a. Geben Sie den folgenden Befehl aus, um aus der Datei eine ausführbare Datei zu machen:

     ```
     chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

     b. Geben Sie den folgenden Befehl aus:

     ```
     ./8.1.x.000-IBM-SPCMS-Linuxx64.bin
     ```

   - In Windows-Clientsystemen klicken Sie doppelt auf den Namen des Installationspakets in Windows Explorer.

   Tipp: Wenn Sie das Paket zuvor bereits installiert und deinstalliert haben, wählen Sie bei der Aufforderung, die vorhandenen Installationsdateien zu ersetzen, Alle aus.
4. Führen Sie die Installationsstapeldatei in dem Verzeichnis aus, in dem Sie die Installationsdateien und zugehörige Dateien extrahiert haben. Dies ist das Verzeichnis, das Sie in Schritt 2 erstellt haben.
   - Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

     ```
     ./install.sh
     ```

   - In Windows-Clientsystemen klicken Sie doppelt auf install.bat.
5. Befolgen Sie die Anweisungen im Assistenten von IBM Installation Manager, um den Clientverwaltungsservice zu installieren.

   Ist IBM Installation Manager auf dem Clientsystem noch nicht installiert, müssen Sie sowohl IBM Installation Manager als auch IBM Spectrum Protect-Clientverwaltungsservices auswählen.

   Tipp: Sie können die Standardposition für das Verzeichnis für gemeinsam genutzte Ressourcen und für das Installationsverzeichnis von IBM Installation Manager übernehmen.

Nächste Schritte

Befolgen Sie die Anweisungen in Überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert wurde.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Clientverwaltungsservice im unbeaufsichtigten Modus installieren

Sie können den Clientverwaltungsservice im unbeaufsichtigten Modus installieren. Im unbeaufsichtigten Modus geben Sie die Installationswerte in einer Antwortdatei an und führen anschließend einen Installationsbefehl aus.

Vorbereitende Schritte

Lesen Sie den Abschnitt Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices.

Extrahieren Sie das Installationspaket gemäß den Anweisungen in Clientverwaltungsservice mit einem grafisch orientierten Assistenten installieren.

Informationen zu diesem Vorgang

Sie müssen den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren installieren.

Das Verzeichnis input, das sich in dem Verzeichnis befindet, in dem das Installationspaket extrahiert wird, enthält die folgende Musterantwortdatei:

install_response_sample.xml

Sie können die Musterdatei mit den Standardwerten verwenden oder diese Datei anpassen.

Tipp: Wenn Sie die Musterdatei anpassen wollen, müssen Sie eine Kopie der Musterdatei erstellen, die Kopie umbenennen und bearbeiten.

Vorgehensweise

1. Erstellen Sie eine auf der Musterdatei basierende Antwortdatei oder verwenden Sie die Musterdatei install_response_sample.xml.
   In beiden Fällen müssen Sie sicherstellen, dass in der Antwortdatei die Anschlussnummer für den Clientverwaltungsservice angegeben ist. Der Standardanschluss ist 9028. Beispiel:

   ```
   <variable name='port' value='9028'/>
   ```

2. Führen Sie den Installationsbefehl für den Clientverwaltungsservice aus und akzeptieren Sie die Lizenz. Geben Sie in dem Verzeichnis, in dem die Installationspaketdatei extrahiert wurde, den folgenden Befehl aus (*Antwordatei* steht für den Pfad der Antwortdatei einschließlich des Dateinamens):
   Auf einem Linux-Clientsystem:

   ```
   ./install.sh -s -input Antwortdatei -acceptLicense
   ```

   Beispiel:

   ```
   ./install.sh -s -input /cms_install/input/install_response.xml -acceptLicense
   ```

   Auf einem Windows-Clientsystem:

   ```
   install.bat -s -input Antwortdatei -acceptLicense
   ```

   Beispiel:

   ```
   install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
   ```

Nächste Schritte

Befolgen Sie die Anweisungen in Überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert wurde.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert wurde

Bevor Sie Diagnoseinformationen über einen Client für Sichern/Archivieren mit dem Clientverwaltungsservice erfassen, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert wurde.

Vorgehensweise

Geben Sie auf dem Clientsystem die folgenden Befehle in die Befehlszeile ein, um die Konfiguration des Clientverwaltungsservice anzuzeigen:

- Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

  ```
  Clientinstallationsverzeichnis/cms/bin/CmsConfig.sh list
  ```

  Clientinstallationsverzeichnis ist das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie bei einer Standardclientinstallation beispielsweise den folgenden Befehl aus:

  ```
  /opt/tivoli/tsm/cms/bin/CmsConfig.sh list
  ```

  Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

  ```
  CMS-Konfiguration auflisten

  server1.example.com:1500 NO_SSL HOSTNAME
            Funktionen: [LOG_QUERY]
  ```

```
    Optionsdateipfad: /opt/tivoli/tsm/client/ba/bin/dsm.sys

      Protokolldatei: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
      Protokolldatei: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
```

- Geben Sie auf Windows-Clientsystemen den folgenden Befehl aus:

  ```
  Clientinstallationsverzeichnis\cms\bin\CmsConfig.bat list
  ```

  Clientinstallationsverzeichnis ist das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie bei einer Standardclientinstallation beispielsweise den folgenden Befehl aus:

  ```
  C:\"Program Files"\Tivoli\TSM\cms\bin\CmsConfig.bat list
  ```

  Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

  ```
  CMS-Konfiguration auflisten

  server1.example.com:1500 NO_SSL HOSTNAME
            Funktionen: [LOG_QUERY]
      Optionsdateipfad: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

        Protokolldatei: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
        Protokolldatei: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  ```

Wenn der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist, zeigt die Ausgabe die Position der Fehlerprotokolldatei an. Der Ausgabetext wird aus der folgenden Konfigurationsdatei extrahiert:

- Auf Linux-Clientsystemen:

  ```
  Clientinstallationsverzeichnis/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
  ```

- Auf Windows-Clientsystemen:

  ```
  Clientinstallationsverzeichnis\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
  ```

Wenn die Ausgabe keine Einträge enthält, müssen Sie die Datei client-configuration.xml konfigurieren. Anweisungen zur Konfiguration dieser Datei finden Sie in Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren. Mit dem Befehl CmsConfig verify können Sie überprüfen, ob eine Knotendefinition in der Datei client-configuration.xml ordnungsgemäß erstellt wurde.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren

Wenn Sie nicht die Standardkonfiguration für den Clientverwaltungsservice verwenden, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

Vorbereitende Schritte

Stellen Sie sicher, dass der Clientverwaltungsservice auf dem Clientsystem installiert und gestartet wird.

Überprüfen Sie, ob die Standardkonfiguration verwendet wird. Die Standardkonfiguration wird nicht verwendet, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Clientverwaltungsservice verwendet nicht die Standardanschlussnummer 9028.
- Für den Zugriff auf den Client für Sichern/Archivieren wird nicht dieselbe IP-Adresse wie für das Clientsystem verwendet, in dem der Client für Sichern/Archivieren installiert ist. Eine andere IP-Adresse könnte beispielsweise in den folgenden Situationen verwendet werden:
  - Das Computersystem verfügt über zwei Netzkarten. Der Client für Sichern/Archivieren ist für die Kommunikation in einem Netz konfiguriert, während der Clientverwaltungsservice in dem anderen Netz kommuniziert.
  - Das Clientsystem ist mit DHCP (Dynamic Host Configuration Protocol) konfiguiert. Folglich wird dem Clientsystem eine IP-Adresse dynamisch zugeordnet, die während der vorherigen Operation des Clients für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gespeichert wird. Wenn das Clientsystem neu gestartet wird, kann ihm eine andere IP-Adresse zugeordnet werden. Um sicherzustellen, dass das Operations Center das Clientsystem immer finden kann, geben Sie einen vollständig qualifizierten Domänennamen an.

Vorgehensweise

Gehen Sie wie folgt vor, um das Operations Center für die Verwendung des Clientverwaltungsservice zu konfigurieren:

1. Wählen Sie auf der Seite Clients des Operations Center den Client aus.
2. Klicken Sie auf Details.
3. Klicken Sie auf die Registerkarte Eigenschaften.
4. Geben Sie im Feld URL für Ferndiagnose im Abschnitt Allgemein die URL für den Clientverwaltungsservice im Clientsystem an.

   Die Adresse muss mit `https` beginnen. Die folgende Tabelle enthält Beispiele der URL für Ferndiagnose.

URL-Typ	Beispiel
Mit DNS-Hostnamen und Standardanschluss 9028	`https://server.example.com`
Mit DNS-Hostnamen und ohne Standardanschluss	`https://server.example.com:1599`
Mit IP-Adresse und ohne Standardanschluss	`https://192.0.2.0:1599`

5. Klicken Sie auf Speichern.

Nächste Schritte

Auf Clientdiagnoseinformationen (z. B. Clientprotokolldateien) können Sie über die Registerkarte Diagnose im Operations Center zugreifen.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Clientverwaltungsservice starten und stoppen

Der Clientverwaltungsservice wird nach seiner Installation auf dem Clientsystem automatisch gestartet. Sie müssen den Service in bestimmten Situationen möglicherweise stoppen und starten.

Vorgehensweise

- Geben Sie die folgenden Befehle aus, um den Clientverwaltungsservice auf Linux-Clientsystemen zu stoppen, zu starten oder erneut zu starten:
  - Zum Stoppen des Service:

    ```
    service cms.rc stop
    ```

  - Zum Starten des Service:

    ```
    service cms.rc start
    ```

  - Zum erneuten Starten des Service:

    ```
    service cms.rc restart
    ```

- Auf Windows-Clientsystemen öffnen Sie das Fenster Dienste, wo Sie den Dienst 'IBM Spectrum Protect-Clientverwaltungsservices' stoppen, starten oder erneut starten können.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Clientverwaltungsservice deinstallieren

Wenn Sie keine Clientdiagnoseinformationen mehr erfassen müssen, können Sie den Clientverwaltungsservice im Clientsystem deinstallieren.

Informationen zu diesem Vorgang

Sie müssen den Clientverwaltungsservice mit IBM® Installation Manager deinstallieren. Falls nicht mehr benötigt, können Sie auch IBM Installation Manager deinstallieren.

Vorgehensweise

1. Deinstallieren Sie den Clientverwaltungsservice wie folgt auf dem Clientsystem:
   a. Öffnen Sie IBM Installation Manager:
      - Wechseln Sie im Linux-Clientsystem in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus:

        ```
        ./IBMIM
        ```

      - Im Windows-Clientsystem öffnen Sie IBM Installation Manager über das Menü Start.

   b. Klicken Sie auf Deinstallieren.
   c. Wählen Sie IBM Spectrum Protect-Clientverwaltungsservices aus und klicken Sie auf Weiter.
   d. Klicken Sie auf Deinstallieren und dann auf Fertigstellen.
   e. Schließen Sie das IBM Installation Manager-Fenster.

2. Falls Sie IBM Installation Manager nicht mehr benötigen, deinstallieren Sie es im Clientsystem:
    a. Öffnen Sie den Deinstallationsassistenten von IBM Installation Manager:
        - Wechseln Sie im Linux-Clientsystem in das Deinstallationsverzeichnis von IBM Installation Manager (z. B. /var/ibm/InstallationManager/uninstall) und geben Sie den folgenden Befehl aus:

          ```
          ./uninstall
          ```

        - Im Windows-Clientsystem klicken Sie auf Start > Systemsteuerung. Dann klicken Sie auf Programm deinstallieren > IBM Installation Manager > Deinstallieren.
    b. Wählen Sie IBM Installation Manager im Fenster IBM Installation Manager aus (falls noch nicht ausgewählt) und klicken Sie auf Weiter.
    c. Klicken Sie auf Deinstallieren und dann auf Fertigstellen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren

Der Clientverwaltungsservice verwendet Informationen in der Clientkonfigurationsdatei (client-configuration.xml), um Diagnoseinformationen zu erkennen. Wenn der Clientverwaltungsservice die Position der Protokolldateien nicht erkennen kann, müssen Sie das Dienstprogramm CmsConfig ausführen, um die Position der Protokolldateien zur Datei client-configuration.xml hinzuzufügen.

- Dienstprogramm CmsConfig
  Wenn Sie nicht die Standardclientkonfiguration verwenden, können Sie das Dienstprogramm CmsConfig auf dem Clientsystem ausführen, um die Position der Clientprotokolldateien zu erkennen und zur Datei client-configuration.xml hinzuzufügen. Nach Abschluss der Konfiguration kann der Clientverwaltungsservice auf die Clientprotokolldateien zugreifen und sie für Basisdiagnosefunktionen im Operations Center zur Verfügung stellen.

 AIX-Betriebssysteme  Linux-Betriebssysteme

Fehlerbehebung für die Operations Center-Installation

Wenn bei der Installation des Operations Center ein Problem auftritt, das Sie nicht lösen können, können Sie in den Beschreibungen der bekannten Probleme nach einer Lösungsmöglichkeit suchen.

-  AIX-BetriebssystemeGrafisch orientierter Installationsassistent kann auf einem AIX-System nicht gestartet werden
  Sie installieren das Operations Center auf einem AIX-System mithilfe des grafisch orientierten Assistenten und das Installationsprogramm startet nicht.
-  Linux-BetriebssystemeChinesische, japanische oder koreanische Schriftarten werden nicht ordnungsgemäß angezeigt
  Chinesische, japanische oder koreanische Schriftarten werden im Operations Center unter Red Hat Enterprise Linux 5 nicht ordnungsgemäß angezeigt.

 AIX-Betriebssysteme

Grafisch orientierter Installationsassistent kann auf einem AIX-System nicht gestartet werden

Sie installieren das Operations Center auf einem AIX-System mithilfe des grafisch orientierten Assistenten und das Installationsprogramm startet nicht.

Lösung

Die in Operations Center mit einem grafisch orientierten Assistenten installieren aufgelisteten RPM-Dateien müssen auf dem Computer installiert sein. Überprüfen Sie, ob die RPM-Dateien installiert sind.

 Linux-Betriebssysteme

Chinesische, japanische oder koreanische Schriftarten werden nicht ordnungsgemäß angezeigt

Chinesische, japanische oder koreanische Schriftarten werden im Operations Center unter Red Hat Enterprise Linux 5 nicht ordnungsgemäß angezeigt.

Lösung

Installieren Sie die folgenden Schriftartpakete, die von Red Hat verfügbar sind:

- fonts-chinese
- fonts-japanese
- fonts-korean

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Operations Center deinstallieren

Sie können das Operations Center mit jeder der folgenden Methoden deinstallieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

- Operations Center mit einem grafisch orientierten Assistenten deinstallieren
  Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM® Installation Manager deinstallieren.
- Operations Center im Konsolenmodus deinstallieren
  Zum Deinstallieren des Operations Center mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.
- Operations Center im unbeaufsichtigten Modus deinstallieren
  Zum Deinstallieren des Operations Center im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Operations Center mit einem grafisch orientierten Assistenten deinstallieren

Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM® Installation Manager deinstallieren.

Vorgehensweise

1. Öffnen Sie IBM Installation Manager.
   AIX-BetriebssystemeLinux-BetriebssystemeIn dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis eclipse (z. B. /opt/IBM/InstallationManager/eclipse) und geben Sie folgenden Befehl aus:

   ```
   ./IBMIM
   ```

   Windows-BetriebssystemeSie können IBM Installation Manager über das Menü Start öffnen.
2. Klicken Sie auf Deinstallieren.
3. Wählen Sie die Option für das Operations Center aus und klicken Sie auf Weiter.
4. Klicken Sie auf Deinstallieren.
5. Klicken Sie auf Fertigstellen.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Operations Center im Konsolenmodus deinstallieren

Zum Deinstallieren des Operations Center mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.

Vorgehensweise

1. In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
   - AIX-BetriebssystemeLinux-Betriebssystemeeclipse/tools
   - Windows-Betriebssystemeeclipse\tools

   Beispiel:

   - AIX-BetriebssystemeLinux-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
   - Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\eclipse\tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus:
   - AIX-BetriebssystemeLinux-Betriebssysteme`./imcl -c`
   - Windows-Betriebssysteme`imcl.exe -c`
3. Für die Deinstallation geben Sie `5` ein.
4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
5. Geben Sie `N` für 'Next' (Weiter) ein.
6. Wählen Sie die Deinstallation des Operations Center-Pakets aus.
7. Geben Sie `N` für 'Next' (Weiter) ein.
8. Geben Sie `U` für 'Uninstall' (Deinstallieren) ein.
9. Geben Sie `F` für 'Finish' (Fertigstellen) ein.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Operations Center im unbeaufsichtigten Modus deinstallieren

Zum Deinstallieren des Operations Center im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM® Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

Vorbereitende Schritte

Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation des Operations Center-Servers mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, uninstall_response_sample.xml, im Verzeichnis input, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie das Operations Center deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für den Operations Center-Eintrag in der Antwortdatei unverändert.

Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:
   - AIX-BetriebssystemeLinux-Betriebssystemeeclipse/tools
   - Windows-Betriebssystemeeclipse\tools

   Beispiel:

   - AIX-BetriebssystemeLinux-Betriebssysteme/opt/IBM/InstallationManager/eclipse/tools
   - Windows-BetriebssystemeC:\Programme\IBM\Installation Manager\eclipse\tools
2. Im Verzeichnis tools geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:
   - AIX-BetriebssystemeLinux-Betriebssysteme`./imcl -input Antwortdatei -silent`
   - Windows-Betriebssysteme`imcl.exe -input Antwortdatei -silent`

   Der folgende Befehl ist ein Beispiel:
   - AIX-BetriebssystemeLinux-Betriebssysteme`./imcl -input /tmp/input/uninstall_response.xml -silent`
   - Windows-Betriebssysteme`imcl.exe -input C:\tmp\input\uninstall_response.xml -silent`

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Rollback zu einer vorherigen Version des Operations Center durchführen

Standardmäßig speichert IBM® Installation Manager ältere Versionen eines Pakets, damit ein Rollback ausgeführt werden kann, falls Probleme mit neueren Versionen von Updates, Fixes oder Paketen auftreten.

Vorbereitende Schritte

Die Rollback-Funktion ist erst verfügbar, nachdem das Operations Center aktualisiert wurde.

Informationen zu diesem Vorgang

Wenn IBM Installation Manager ein Rollback zu einer vorherigen Version durchführt, wird die aktuelle Version der Paketdateien deinstalliert und die frühere Version erneut installiert.

Um ein Rollback zu einer vorherigen Version durchführen zu können, muss IBM Installation Manager auf Dateien für diese Version zugreifen. Diese Dateien werden standardmäßig während jeder aufeinanderfolgenden Installation gespeichert. Da die Anzahl der gespeicherten Dateien bei jeder installierten Version zunimmt, sollten Sie diese Dateien regelmäßig aus Ihrem System löschen. Wenn Sie die Dateien löschen, können Sie jedoch kein Rollback zu einer vorherigen Version durchführen.

Gehen Sie wie folgt vor, um gespeicherte Dateien zu löschen oder um Ihre Einstellung für die Speicherung dieser Dateien bei zukünftigen Installationen zu aktualisieren:

1. Klicken Sie in IBM Installation Manager auf Datei > Benutzervorgaben.
2. Klicken Sie auf der Seite mit den Benutzervorgaben auf Dateien für Rollback und geben Sie Ihre Vorgaben an.

Vorgehensweise

Wenn Sie ein Rollback zu einer vorherigen Version des Operations Center ausführen möchten, verwenden Sie die Funktion Rollback durchführen von IBM Installation Manager.

Server konfigurieren

Um Konfigurationstasks für den IBM Spectrum Protect-Server auszuführen, lesen Sie die verfügbare Dokumentation.

Informationen zu diesem Vorgang

Berücksichtigen Sie für eine bestehende Lösung die folgenden Aktionen.

Führen Sie zur Planung, Implementierung, Überwachung und Ausführung einer neuen Lösung die Anweisungen in IBM Spectrum Protect-Datenschutzlösungen aus.

Tipp: Ab IBM Spectrum Protect Version 7.1.3 ist das *Administratorhandbuch* veraltet.

Aktion	Details	Dokumentation
Überwachen einer Speicherlösung	Überwachen Sie die Speicherlösung, um vorhandene und potenzielle Probleme zu ermitteln. Auf diese Art und Weise können Sie Fehler beheben und die Systemleistung optimieren.	Speicherlösungen überwachen
Auswählen und Konfigurieren von Speicher	Wählen Sie Speicher auf der Basis Ihrer Geschäftsanforderungen aus und führen Sie dann die Tasks für die Konfiguration aus.	Speicher konfigurieren
Eliminieren doppelter Daten	Verwenden Sie die Datendeduplizierung, um redundante Daten in Speicherpools zu eliminieren. Die Datendeduplizierung reduziert den zum Aufbewahren der Daten erforderlichen Speicher. Es wird nur eine einzige Instanz der Daten in einem deduplizierten Speicherpool aufbewahrt. Ab IBM Spectrum Protect Version 7.1.3 können Sie die Inline-Datendeduplizierung verwenden.	Weitere Informationen zu den Unterschieden zwischen Inline-Datendeduplizierung und nachgeordneter Datendeduplizierung sowie Informationen zur Konfiguration der Best-Practice-Lösung für die Datendeduplizierung finden Sie in Datendeduplizierungsoptionen.
Replizieren von Daten	Sie können Clientknotendaten von einem Quellenreplikationsserver auf einen Zielreplikationsserver replizieren. Wenn ein Katastrophenfall eintritt und der Quellenserver vorübergehend nicht verfügbar ist, können Clientknoten ihre Daten vom Zielreplikationsserver wiederherstellen.	Informationen zur Implementierung einer Best-Practice-Lösung, die IBM Spectrum Protect-Replikation und automatische Übernahme verwendet, finden Sie in Plattenspeicherlösung für mehrere Standorte. Allgemeine Informationen zur Replikation, einschließlich Konfigurationsschritten, finden Sie in Clientdaten auf einen anderen Server replizieren.
Verwalten der Datenbank und des Wiederherstellungsprotokolls	Die Datenbank und das Wiederherstellungsprotokoll (der Serverbestand) speichern Informationen zu Clientdaten und sind für den Betrieb des Servers kritisch.	• Allgemeine Informationen zur Datenbank und zum Wiederherstellungsprotokoll finden Sie in Datenbank und Wiederherstellungsprotokoll verwalten (Version 7.1.1). • Informationen zum Optimieren der Index- und Tabellenreorganisation für die Serverdatenbank und zum Verhindern und Beheben von Problemen, die das Datenbankwachstum betreffen, und von Leistungsproblemen finden Sie in Technote 1683633.

Aktion	Details	Dokumentation
Server schützen	Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.	IBM Spectrum Protect-Server schützen
Konfigurieren von SSL für Lightweight Directory Access Protocol (LDAP)	Sie können SSL für LDAP-Verzeichnisserver konfigurieren und Kennwörter und Anmeldeverfahren verwalten.	Informationen zu LDAP finden Sie in: • Benutzer mithilfe eines LDAP-Servers authentifizieren • SSL oder TLS für LDAP-Verzeichnisserver konfigurieren (Version 7.1.1)
Informationen zu Maßnahmen für die Datenaufbewahrung und Konfigurieren dieser Maßnahmen	IBM Spectrum Protect-Maßnahmen definieren die Regeln zur Verwaltung Ihrer Daten.	Verwenden Sie das Operations Center, um Maßnahmen zu aktualisieren. Weitere Informationen zu Maßnahmen und zum Erstellen von Maßnahmen finden Sie in Maßnahmen anpassen.
Schützen des Servers und Wiederherstellen des Servers nach einem Katastrophenfall	Schützen Sie Ihre Systeminfrastruktur und Ihre Daten, damit eine Wiederherstellung nach einem Katastrophenfall möglich ist. Verwenden Sie die von IBM Spectrum Protect bereitgestellten Tools und Prozeduren zur Erstellung eines Plans zur Wiederherstellung nach einem Katastrophenfall.	Informationen zum Schützen und Wiederherstellen des Servers finden Sie in: • Datenbank und Infrastrukturkonfigurationsdateien schützen (Version 7.1.1) • Disaster Recovery Manager für Bandumgebungen verwenden (Version 7.1.1)
Schützen von NAS-Dateiservern	Sie können eine Sicherungsumgebung, die Ihren NAS-Dateiserver schützt, planen, konfigurieren und verwalten.	NAS-Dateiserver schützen
Konfigurieren einer Clusterumgebung	Konfigurieren Sie eine Clusterumgebung unter AIX, Linux oder Windows, um eine höhere Serververfügbarkeit und eine möglichst kurze Ausfallzeit zu gewährleisten.	Clusterumgebungen konfigurieren
Überprüfen der Lizenzeinhaltung	Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen.	Lizenzeinhaltung überprüfen

- IBM Spectrum Protect-Server schützen
  Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.
- Clientdaten auf einen anderen Server replizieren
  Mithilfe der Replikation von Clientdaten von einem Quellenserver auf einen anderen Server kann sichergestellt werden, dass gesicherte Clientdaten für die Wiederherstellung verfügbar sind, wenn der Quellenserver beschädigt. ist. Bei der Replikation werden Daten inkrementell vom Quellenserver auf den Zielserver kopiert, um Übernahme- und Rückübertragungsfunktionalität bereitzustellen.
- Clusterumgebungen konfigurieren
  Sie können den IBM Spectrum Protect-Server für das Clustering auf AIX-, Linux- oder Windows-Systemen konfigurieren.

IBM Spectrum Protect-Server schützen

Schützen Sie den IBM Spectrum Protect-Server und Daten, indem Sie den Zugriff auf Server und Clientknoten steuern, Daten verschlüsseln und sichere Zugriffsebenen und Kennwörter verwalten.

- Sicherheitskonzepte
  Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen

und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

- Administratoren verwalten
  Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.
- Kennwortanforderungen ändern
  Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.
- IBM Spectrum Protect auf dem System schützen
  Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.
- Kommunikation schützen
  Ihre Daten und Kennwörter sind sicherer, wenn Sie mithilfe von Secure Sockets Layer (SSL) oder Transport Layer Security (TLS), einer Form von SSL, geschützt werden.
- IBM Spectrum Protect-Benutzer mithilfe eines LDAP-Servers authentifizieren
  In einem IBM Spectrum Protect-System müssen sich Benutzer beim Server durch die Angabe einer Benutzer-ID und eines Kennworts authentifizieren. Wenn Ihr Unternehmen einen Lightweight Directory Access Protocol-Server (LDAP-Server) zur Verwaltung von Benutzer-IDs verwendet, können Sie den LDAP-Server für die Authentifizierung von IBM Spectrum Protect-Benutzer-IDs verwenden.

Sicherheitskonzepte

Sie können IBM Spectrum Protect vor Sicherheitsrisiken schützen, indem Sie Kommunikationsprotokolle verwenden, Kennwörter schützen und unterschiedliche Zugriffsebenen für Administratoren bereitstellen.

Transport Layer Security

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtsicherheit für eine sichere Verbindung zwischen Servern, Clients und Speicheragenten bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, verwenden Sie SSL oder TLS zum Verschlüsseln der Daten.

Tipp: In der gesamten IBM Spectrum Protect-Dokumentation gilt jede Angabe von "SSL" oder zum "Auswählen von SSL" für TLS.

SSL wird von Global Security Kit (GSKit) bereitgestellt, das zusammen mit dem IBM Spectrum Protect-Server installiert wird, der vom Server, vom Client und vom Speicheragenten verwendet wird.

Einschränkung: Sie dürfen die SSL- oder TLS-Protokolle nicht für die Kommunikation mit einer DB2-Datenbankinstanz verwenden, die von IBM Spectrum Protect-Servern verwendet wird.

Jeder Server, Client oder Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdiges selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle (CA) signiert ist. Sie können Ihre eigenen Zertifikate verwenden oder Zertifikate bei einer Zertifizierungsstelle (CA) kaufen. Jedes der Zertifikate muss installiert und der Schlüsseldatenbank auf dem IBM Spectrum Protect-Server, -Client oder -Speicheragenten hinzugefügt werden. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet. Einige CA-Zertifikate sind in der Schlüsseldatenbank standardmäßig vorinstalliert.

SSL wird auf dem IBM Spectrum Protect-Server, -Client und -Speicheragenten unabhängig voneinander konfiguriert.

Berechtigungsstufen

Für jeden IBM Spectrum Protect-Server sind verschiedene Administratorberechtigungsstufen verfügbar, die die Tasks festlegen, die ein Administrator ausführen kann.

Nach der Registrierung muss einem Administrator Berechtigung erteilt werden, indem ihm eine oder mehrere Administratorberechtigungsstufen zugeordnet werden. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen und anderen Administratoren über den Befehl GRANT AUTHORITY Berechtigungsstufen zuordnen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Ein Administrator kann andere Administrator-IDs registrieren, den IDs Berechtigungsstufen zuordnen, IDs umbenennen, IDs entfernen und IDs für den Server sperren oder entsperren.

Ein Administrator kann den Zugriff auf bestimmte Clientknoten für Rootbenutzer-IDs und Nicht-Rootbenutzer-IDs steuern. Standardmäßig kann eine Nicht-Rootbenutzer-ID keine Daten auf dem Knoten sichern. Ändern Sie mit dem Befehl UPDATE NODE die Knoteneinstellungen, um Sicherungen zu ermöglichen.

Kennwörter

Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer beim Zugriff auf den Server ein Kennwort eingeben.

Verwenden Sie LDAP (Lightweight Directory Access Protocol), um striktere Anforderungen für Kennwörter anzuwenden. Weitere Informationen finden Sie in Benutzer mithilfe eines LDAP-Servers authentifizieren.

Tabelle 1. Merkmale der Kennwortauthentifizierung

Merkmale	Weitere Informationen
Abhängigkeit von der Groß-/Kleinschreibung	Nicht von der Groß-/Kleinschreibung abhängig.
Standardwert für Kennwortablauf	90 Tage. Der Ablaufzeitraum beginnt mit der ersten Registrierung einer Administrator-ID oder eines Clientknotens beim Server. Wenn das Kennwort innerhalb dieses Zeitraums nicht geändert wird, muss das Kennwort beim nächsten Zugriff des Benutzers auf den Server geändert werden.
Ungültige Kennworteingabeversuche	Sie können einen Grenzwert für aufeinanderfolgende ungültige Kennworteingabeversuche für alle Clientknoten definieren. Wenn der Grenzwert überschritten wird, sperrt der Server den Knoten.
Kennwortlänge	Der Administrator kann eine Mindestlänge angeben.

Sitzungssicherheit

Die Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, -Verwaltungsclients und -Servern verwendet wird und mit dem Parameter SESSIONSECURITY festgelegt wird.

Der Parameter SESSIONSECURITY kann auf einen der folgenden Werte gesetzt werden:

- Mit dem Wert STRICT wird die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, -Knoten und -Administratoren durchgesetzt.
- Der Wert TRANSITIONAL gibt an, dass das vorhandene Kommunikationsprotokoll verwendet wird, wenn Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Wenn SESSIONSECURITY=TRANSITIONAL angegeben ist, werden strengere Sicherheitseinstellungen automatisch durchgesetzt, da höhere Versionen des TLS-Protokolls verwendet werden, wenn die Software auf Version 8.1.2 oder höher aktualisiert wird. Nachdem ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch in den Wert STRICT geändert und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder unter Verwendung früherer TLS-Protokolle authentifizieren.

Weitere Informationen zu den Werten für den Parameter SESSIONSECURITY enthalten die Beschreibungen der folgenden Befehle.

Tabelle 2. Befehle zum Festlegen des Parameters SESSIONSECURITY

Entität	Befehl
Clientknoten	• REGISTER NODE • UPDATE NODE
Administratoren	• REGISTER ADMIN • UPDATE ADMIN
Server	• DEFINE SERVER • UPDATE SERVER

Administratoren, die sich unter Verwendung des Befehls DSMADMC, des Befehls DSMC oder des Programms dsm authentifizieren, können sich nach der Authentifizierung unter Verwendung von Version 8.1.2 oder höher nicht unter Verwendung einer früheren Version authentifizieren. Die folgenden Tipps liefern Informationen zur Behebung von Authentifizierungsproblemen für Administratoren:
Tipps:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die das Administratorkonto für die Anmeldung verwendet, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto über mehrere Systeme anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf jedem System installiert ist.
- Nachdem sich ein Administrator bei einem Server der Version 8.1.2 oder höher unter Verwendung eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich der Administrator nur auf Clients oder Servern authentifizieren, die Version 8.1.2 oder höher verwenden. Ein Administratorbefehl kann von jedem beliebigen System ausgegeben werden.
- Erstellen Sie, falls erforderlich, ein separates Administratorkonto, das nur mit Clients und Servern verwendet wird, die Software der Version 8.1.1 oder früher verwenden.

Setzen Sie die höchste Sicherheitsstufe für die Kommunikation mit dem IBM Spectrum Protect-Server durch, indem Sie sicherstellen, dass alle Knoten, Administratoren und Server die Sitzungssicherheit STRICT verwenden. Mithilfe des Befehls SELECT können Sie feststellen, welche Server, Knoten und Administratoren die Sitzungssicherheit TRANSITIONAL verwenden und für die Verwendung der Sitzungssicherheit STRICT aktualisiert werden sollten.

Zugehörige Verweise:
Kommunikation schützen
SELECT (SQL-Abfrage für die Datenbank ausführen)

Administratoren verwalten

Ein Administrator mit Systemberechtigung kann jede Task für den IBM Spectrum Protect-Server ausführen, einschließlich der Zuordnung von Berechtigungsstufen zu anderen Administratoren. Zur Ausführung einiger Tasks muss Ihnen Berechtigung erteilt werden, indem Ihnen eine oder mehrere Berechtigungsstufen zugeordnet werden.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Administratoreinstellungen zu ändern.

Task	Prozedur

Administrator hinzufügen	Um einen Administrator, ADMIN1, mit Systemberechtigung hinzuzufügen und ein Kennwort anzugeben, führen Sie die folgenden Schritte aus:
	a. Registrieren Sie den Administrator und geben Sie Pa$#$twO als Kennwort an, indem Sie den folgenden Befehl ausgeben:
	`register admin admin1 Pa$#$twO`
	b. Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`

Administratorberechtigung ändern	Ändern Sie die Berechtigungsstufe für einen Administrator, ADMIN1.
	• Erteilen Sie dem Administrator Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`grant authority admin1 classes=system`
	• Entziehen Sie dem Administrator die Systemberechtigung, indem Sie den folgenden Befehl ausgeben:
	`revoke authority admin1 classes=system`

Administratoren entfernen	Entfernen Sie einen Administrator, ADMIN1, sodass er nicht mehr auf den IBM Spectrum Protect-Server zuzugreifen kann, indem Sie den folgenden Befehl ausgeben: `remove admin admin1`
Zugriff auf den Server vorübergehend verhindern	Sperren oder entsperren Sie einen Administrator, indem Sie den Befehl LOCK ADMIN bzw. UNLOCK ADMIN verwenden.

Kennwortanforderungen ändern

Sie können den Mindestwert für die Anzahl Anmeldeversuche, die Kennwortlänge und den Kennwortablauf ändern sowie die Authentifizierung für IBM Spectrum Protect aktivieren oder inaktivieren.

Informationen zu diesem Vorgang

Indem Sie die Kennwortauthentifizierung durchsetzen und Kennworteinschränkungen verwalten, können Sie Ihre Daten und Ihre Server vor möglichen Sicherheitsrisiken schützen.

Vorgehensweise

Führen Sie die folgenden Tasks aus, um Kennwortanforderungen für IBM Spectrum Protect-Server zu ändern.

Tabelle 1. Authentifizierungstasks für IBM Spectrum Protect-Server

Task	Prozedur

Task	Prozedur
Grenzwert für ungültige Kennworteingabeversuche festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl ungültiger Versuche im Feld Grenzwert für ungültige Anmeldeversuche an. Der Standardwert bei der Installation ist 0.
Mindestlänge für Kennwörter festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl Zeichen im Feld Mindestlänge für Kennwort an.
Ablaufzeitraum für Kennwörter festlegen	a. Wählen Sie auf der Seite Server im Operations Center den Server aus. b. Klicken Sie auf Details und dann auf die Registerkarte Merkmale. c. Geben Sie die Anzahl Tage im Feld Allgemeine Kennwortablaufdauer an.
Kennwortauthentifizierung inaktivieren	Standardmäßig verwendet der Server automatisch die Kennwortauthentifizierung. Bei der Kennwortauthentifizierung müssen alle Benutzer ein Kennwort eingeben, um auf den Server zugreifen zu können. Sie können die Kennwortauthentifizierung nur für Kennwörter inaktivieren, die mit dem Server (LOCAL) authentifiziert werden. Durch das Inaktivieren der Kennwortauthentifizierung erhöht sich das Sicherheitsrisiko für den Server.

Standardauthentifizierungsmethode festlegen	Geben Sie den Befehl SET DEFAULTAUTHENTICATION aus. Um beispielsweise den Server als die Standardauthentifizierungsmethode zu verwenden, geben Sie den folgenden Befehl aus:
	
	`set defaultauthentication local`
	
	Um einen Clientknoten für die Authentifizierung mit dem Server zu aktualisieren, schließen Sie `AUTHENTICATION=LOCAL` in den Befehl UPDATE NODE ein:
	
	`update node authentication=local`

IBM Spectrum Protect auf dem System schützen

Schützen Sie das System, auf dem der IBM Spectrum Protect-Server ausgeführt wird, um unbefugten Zugriff zu verhindern.

Vorgehensweise

Stellen Sie sicher, dass nicht berechtigte Benutzer nicht auf die Verzeichnisse für die Serverdatenbank und die Serverinstanz zugreifen können. Behalten Sie die Zugriffseinstellungen für diese Verzeichnisse bei, die Sie während der Implementierung konfiguriert haben.

- Benutzerzugriff auf den Server einschränken
  Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.
- Zugriff über Porteinschränkungen einschränken
  Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

Benutzerzugriff auf den Server einschränken

Berechtigungsstufen legen fest, welche Aktionen ein Administrator für den IBM Spectrum Protect-Server ausführen kann. Ein Administrator mit Systemberechtigung kann jede Task für den Server ausführen. Administratoren mit Maßnahmen-, Speicher- oder Bedienerberechtigung können Untergruppen von Tasks ausführen.

Vorgehensweise

1. Nachdem Sie einen Administrator mit dem Befehl REGISTER ADMIN registriert haben, legen Sie die Berechtigungsstufe des Administrators mithilfe des Befehls GRANT AUTHORITY fest. Ausführliche Informationen zum Festlegen und Ändern der Berechtigung finden Sie in Administratoren verwalten.
2. Um die Berechtigung eines Administrators zur Ausführung bestimmter Tasks zu steuern, verwenden Sie die beiden folgenden Serveroptionen:
   a. Über die Serveroption QUERYAUTH können Sie die Berechtigungsstufe auswählen, die ein Administrator haben muss, um Befehle QUERY und SELECT ausgeben zu können. Standardmäßig ist keine Berechtigungsstufe erforderlich. Sie können die Anforderung in eine der Berechtigungsstufen, einschließlich Systemberechtigung, ändern.
   b. Über die Serveroption REQSYSAUTHOUTFILE können Sie angeben, dass Systemberechtigung für Befehle erforderlich ist, die zur Folge haben, dass der Server Daten in eine externe Datei schreibt. Standardmäßig ist für diese Befehle Systemberechtigung erforderlich.
3. Sie können die Datensicherung auf einem Clientknoten ausschließlich auf Rootbenutzer-IDs oder berechtigte Benutzer beschränken. Um beispielsweise Sicherungen auf die Rootbenutzer-ID zu beschränken, geben Sie den Befehl REGISTER NODE oder UPDATE NODE unter Angabe des Parameters BACKUPINITIATION=root aus:

```
update node backupinitiation=root
```

Zugriff über Porteinschränkungen einschränken

Schränken Sie den Zugriff auf den Server ein, indem Sie Porteinschränkungen anwenden.

Informationen zu diesem Vorgang

Gegebenenfalls müssen Sie abhängig von Ihren Sicherheitsanforderungen den Zugriff auf bestimmte Server einschränken. Der IBM Spectrum Protect-Server kann so konfiguriert werden, dass er an vier TCP/IP-Ports empfangsbereit ist: zwei Ports, die für reguläre TCP/IP-Protokolle oder SSL-/TLS-Protokolle verwendet werden können, und zwei Ports, die nur für das SSL-/TLS-Protokoll verwendet werden können.

Vorgehensweise

Sie können die Serveroptionen wie in Tabelle 1 aufgeführt zur Angabe des erforderlichen Ports festlegen.

Tabelle 1. Serveroptionen und Portzugriff

Serveroption	Portzugriff
TCPPORT	Gibt die Nummer des Ports an, dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist 1500.
TCPADMINPORT	Gibt die Nummer des Ports an, an dem der TCP/IP-DFV-Treiber des Servers auf Anforderungen von anderen Sitzungen als Clientsitzungen warten soll. Dieser Port ist sowohl für TCP/IP- als auch für SSL-fähige Sitzungen empfangsbereit. Der Standardwert ist der Wert für TCPPORT. Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPPORT verwendet, zu trennen.
SSLTCPPORT	Gibt die SSL-TCP/-IP-Portadresse für einen Server an. Dieser Port ist nur für SSL-fähige Sitzungen empfangsbereit. Ein Standardwert für den Port ist nicht verfügbar.
SSLTCPADMINPORT	Gibt die Portadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen von SSL-fähigen Sitzungen wartet. Ein Standardwert für den Port ist nicht verfügbar. Verwenden Sie diese Option, um den Datenverkehr des Verwaltungsclients vom Datenverkehr des regulären Clients, der die Optionen TCPPORT und SSLTCPPORT verwendet, zu trennen.

Kommunikation schützen

Ihre Daten und Kennwörter sind sicherer, wenn Sie mithilfe von Secure Sockets Layer (SSL) oder Transport Layer Security (TLS), einer Form von SSL, geschützt werden.

SSL und TLS sind die Standardtechnologien zum Erstellen verschlüsselter Sitzungen zwischen Servern und Clients. SSL und TLS stellen einen sicheren Kanal für Server und Clients bereit, um über offene Kommunikationspfade zu kommunizieren. Bei SSL und TLS wird die Identität des Servers mithilfe digitaler Zertifikate geprüft. Clients, Server und Speicheragenten, die IBM Spectrum Protect-Software der Version 8.1.2 oder höher für die Kommunikation verwenden, werden automatisch für die Verwendung von TLS 1.2 konfiguriert.

Um die Systemleistung zu verbessern, verwenden Sie TLS für die Authentifizierung ohne die Verschlüsselung von Objektdaten. Informationen zur Angabe, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, finden Sie in der Beschreibung der Clientoption SSL für die Client/Server-Kommunikation und in der Beschreibung des Parameters SSL im Befehl UPDATE SERVER für die

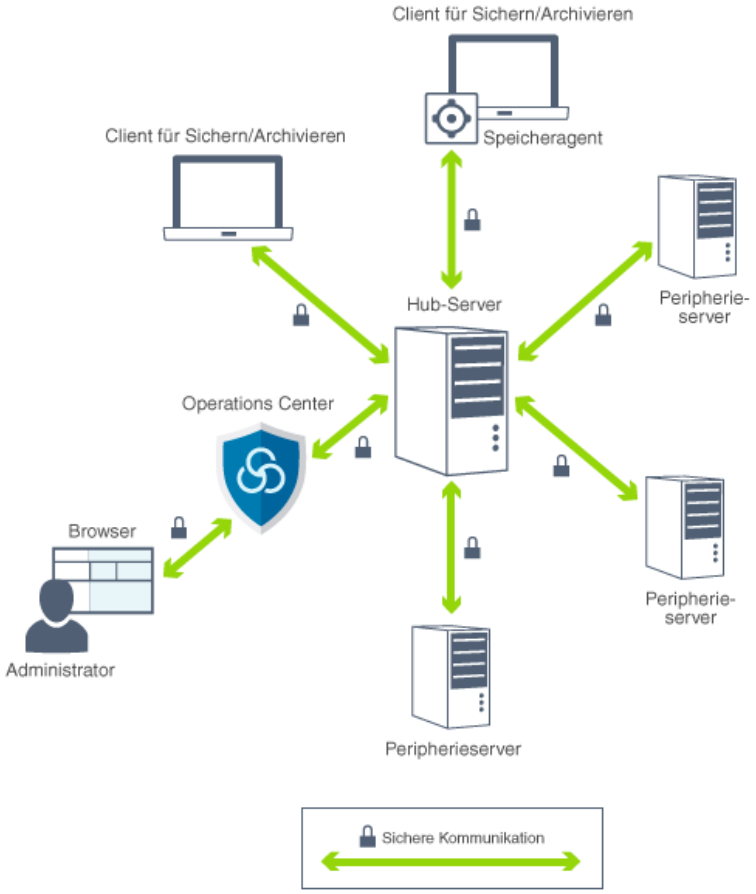
Kommunikation zwischen Servern. Wenn TLS für die Verschlüsselung von Objektdaten verwendet werden soll, fügen Sie gegebenenfalls weitere Prozessorressourcen auf dem IBM Spectrum Protect-Server hinzu, um den erhöhten Datenaustausch im Netz handhaben zu können.

Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, schützt TLS Kennwörter zwischen dem IBM Spectrum Protect-Server und dem LDAP-Server. TLS ist für die gesamte Kommunikation mit LDAP-Kennwort erforderlich.

- Kommunikation über Secure Sockets Layer und Transport Layer Security
  Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtsicherheit für eine sichere Verbindung zwischen IBM Spectrum Protect-Servern, -Clients, -Speicheragenten und dem Operations Center bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, wird SSL oder TLS zum Verschlüsseln der Daten verwendet.
- Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren
  Konfigurieren Sie Secure Sockets Layer (SSL) auf dem IBM Spectrum Protect-Server, dem Client für Sichern/Archivieren, dem Speicheragenten und im Operations Center, um sicherzustellen, dass Daten während der Kommunikation verschlüsselt werden.

Kommunikation über Secure Sockets Layer und Transport Layer Security

Mithilfe des Protokolls Secure Sockets Layer (SSL) oder Transport Layer Security (TLS) können Sie Transportschichtsicherheit für eine sichere Verbindung zwischen IBM Spectrum Protect-Servern, -Clients, -Speicheragenten und dem Operations Center bereitstellen. Wenn Sie Daten zwischen dem Server, dem Client und dem Speicheragenten austauschen, wird SSL oder TLS zum Verschlüsseln der Daten verwendet.



Einschränkung: Sie dürfen das SSL- oder TLS-Protokoll nicht für die Kommunikation mit einer IBM DB2-Datenbankinstanz verwenden, die vom IBM Spectrum Protect-Server verwendet wird.

Jeder Server oder Speicheragent verfügt über einen eindeutigen privaten Schlüssel und ein eindeutiges signiertes Zertifikat, mit dem SSL-Verbindungen ermöglicht werden. Wenn Sie selbst signierte Zertifikate verwenden, müssen Sie das selbst signierte Zertifikat für jeden Server oder Speicheragenten an alle Clients, Speicheragenten und Server verteilen, die TLS für die Kommunikation verwenden. Wenn Sie von einer Zertifizierungsstelle (CA) signierte Zertifikate verwenden, müssen Sie nur die CA-Zertifikate an alle Clients, Speicheragenten und Server verteilen, die TLS für die Kommunikation verwenden.

Wenn Sie ein Stammzertifikat von einer Zertifizierungsstelle verwenden, müssen Sie das Zertifikat in jeder Schlüsseldatenbank für den Client, den Server und den Speicheragenten installieren, der die SSL-Kommunikation einleitet. Ein *Stammzertifikat* ist ein Zertifikat, das die Stammzertifizierungsstelle angibt. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet.

Ab IBM Spectrum Protect Version 8.1.2 ist SSL standardmäßig für die Kommunikation zwischen Servern, Clients und Speicheragenten der Version 8.1.2 aktiviert.

Der IBM Spectrum Protect-Server, -Client oder -Speicheragent kann während der Kommunikation als SSL-Client fungieren. Ein SSL-Client ist die Komponente, die die Kommunikation einleitet und das Zertifikat für einen SSL-Server prüft. Wenn beispielsweise der IBM Spectrum Protect-Client die SSL-Kommunikation mit dem IBM Spectrum Protect-Server einleitet, ist der IBM Spectrum Protect-Client der SSL-Client und der Server der SSL-Server.

In Tabelle 1 sind die Komponenten aufgelistet, die ein SSL-Client oder SSL-Server sein können.

Tabelle 1. SSL-Clients und -Server in der IBM Spectrum Protect-Umgebung

SSL-Client	SSL-Server	Szenario
Client	Server	Der IBM Spectrum Protect-Client initiiert eine Kommunikationsanforderung mit dem IBM Spectrum Protect-Server. Der Client prüft das Zertifikat. Der Server stellt das Zertifikat bereit.
Server (wie beispielsweise ein Quellenserver)	Server (wie beispielsweise ein Zielserver)	Der IBM Spectrum Protect-Quellenserver initiiert eine Kommunikationsanforderung mit dem IBM Spectrum Protect-Zielserver. Der Quellenserver fungiert als SSL-Client und prüft das vom Zielserver bereitgestellte Zertifikat. Dieser Typ von Kommunikation ist während der Replikationsverarbeitung üblich.
Client über einen Speicheragenten	Server	Der Client überprüft jedes Zertifikat, wenn er die SSL-Kommunikation mit dem IBM Spectrum Protect-Server und dem Speicheragenten separat einleitet. Wenn der Speicheragent mit dem Server unter Verwendung des SSL-Kommunikationsprotokolls kommuniziert, fungiert der Speicheragent als SSL-Client und prüft das vom Server bereitgestellte Zertifikat. Der Speicheragent kann gleichzeitig SSL-Client und SSL-Provider sein.
Server	LDAP-Server	Der IBM Spectrum Protect-Server initiiert eine Kommunikationsanforderung mit dem LDAP-Server. Der IBM Spectrum Protect-Server fungiert als SSL-Client und prüft das vom LDAP-Server bereitgestellte Zertifikat.
Operations Center	Server	Das Operations Center initiiert eine Kommunikationsanforderung mit dem IBM Spectrum Protect-Server. Das Operations Center fungiert als SSL-Client und prüft das vom IBM Spectrum Protect-Server bereitgestellte Zertifikat.
Reporting	Server	Der Reporting-Agent initiiert eine Kommunikationsanforderung mit dem IBM Spectrum Protect-Server. Das Reporting-Feature fungiert als SSL-Client und prüft das vom IBM Spectrum Protect-Server bereitgestellte Zertifikat.

Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren

Konfigurieren Sie Secure Sockets Layer (SSL) auf dem IBM Spectrum Protect-Server, dem Client für Sichern/Archivieren, dem Speicheragenten und im Operations Center, um sicherzustellen, dass Daten während der Kommunikation verschlüsselt werden.

Mithilfe eines selbst signierten SSL-Zertifikats oder eines signierten Zertifikats einer unabhängigen Zertifizierungsstelle (CA) können Sie eine SSL-Kommunikationsanforderung zwischen dem Server, dem Client und dem Speicheragenten überprüfen. Jeder IBM Spectrum Protect-Server, -Client oder -Speicheragent, der SSL ermöglicht, muss ein vertrauenswürdiges selbst signiertes Zertifikat verwenden oder ein eindeutiges Zertifikat anfordern, das von einer Zertifizierungsstelle signiert ist.

Der Vorteil CA-signierter Zertifikate liegt darin, dass ein einziges CA-signiertes Zertifikat für alle Server verwendet werden kann und damit ein einzigen Zertifikat an Clients verteilt werden kann. Wenn Sie ein selbst signiertes Zertifikat verwenden, wird das Zertifikat automatisch für jeden Server und jeden Speicheragenten erstellt. Wenn Sie ein Stammzertifikat von einer Zertifizierungsstelle verwenden, muss das Zertifikat in jeder Schlüsseldatenbank für den Client, den Server und den Speicheragenten installiert werden, der die SSL-Kommunikation einleitet. Das Zertifikat wird von dem SSL-Client oder -Server geprüft, der die SSL-Kommunikation anfordert oder einleitet.

Einschränkung: Einige Zertifizierungsstellen (CAs) verwenden Zertifikate in einem Format, das von IBM Spectrum Protect nicht erkannt wird. Unter Umständen müssen Sie sich an Ihre Zertifizierungsstelle wenden, um das Zertifikat in ein Format zu konvertieren, das mit IBM Spectrum Protect verwendet werden kann.

- Server zum Akzeptieren von SSL-Verbindungen konfigurieren
  Konfigurieren Sie den Server zum Akzeptieren von SSL-Verbindungen, bevor Sie die SSL-Kommunikation vom Server zu einem Client, einem Speicheragenten oder einem anderen Server aktivieren.
- Speicheragenten für die Verwendung von SSL konfigurieren
  Um sicherzustellen, dass Daten für die Kommunikation zwischen dem Speicheragenten und dem Server sowie zwischen dem Speicheragenten und dem Client verschlüsselt werden, konfigurieren Sie die Speicheragenten für die Kommunikation unter Verwendung des SSL-Protokolls.
- Client für die Verbindung zu einem Speicheragenten unter Verwendung von SSL konfigurieren
  Um die Daten, die zwischen einem Client und einem Speicheragenten übertragen werden, zu schützen, konfigurieren Sie den Client so,

dass die Verbindung zum Speicheragenten unter Verwendung des SSL-Protokolls hergestellt wird.

Server zum Akzeptieren von SSL-Verbindungen konfigurieren

Konfigurieren Sie den Server zum Akzeptieren von SSL-Verbindungen, bevor Sie die SSL-Kommunikation vom Server zu einem Client, einem Speicheragenten oder einem anderen Server aktivieren.

Vorgehensweise

1. Geben Sie den Port an, an dem der Server auf die SSL-fähige Clientkommunikation wartet, oder akzeptieren Sie die Standardportnummer. Aktualisieren Sie wahlweise die Datei dsmserv.opt im Serverinstanzverzeichnis, indem Sie die Option TCPPORT und/oder die Option TCPADMINPORT angeben. Die Optionen SSLTCPPORT und SSLTCPADMINPORT können nur für Verbindungen, die ausschließlich für SSL gelten, verwendet werden.
2. Erstellen Sie die Serverschlüsseldatenbank, indem Sie den Server starten. Die Serverschlüsseldatenbankdatei, cert.kdb, wird im Serverinstanzverzeichnis gespeichert und der Standardzertifikatskennsatz wird automatisch als "TSM Server SelfSigned SHA Key" festgelegt. Das Zertifikat wird in die Datei cert256.arm exportiert.
3. Wenn Sie das selbst signierte Standardzertifikat verwenden, ist die Datei für das selbst signierte Standardzertifikat (cert256.arm) erforderlich, wenn Sie die Verbindung zum Server unter Verwendung von TLS herstellen.
4. Wenn Sie ein CA-signiertes Zertifikat importieren, führen Sie die folgenden Schritte aus:
   a. Importieren Sie ein eindeutiges Zertifikat, das von einer Zertifizierungsstelle signiert wurde, auf jeden Server, der SSL ermöglicht. Sie können sowohl ein CA-signiertes Stammzertifikat als auch ein CA-signiertes Zwischenzertifikat importieren. Für jeden Server wird dasselbe CA-signierte Zertifikat verwendet. Melden Sie sich am IBM Spectrum Protect-Serversystem mit der Instanzbenutzer-ID an und geben Sie im Instanzverzeichnis den folgenden Beispielbefehl aus:

      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed -label "CA-Stammzertifikat" -file ca.crt
      ```

   b. Um ein CA-signiertes Zwischenzertifikat zu importieren, geben Sie den folgenden Beispielbefehl aus:

      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed
      -label "CA-Zwischenzertifikat" -file intca.crt
      ```

   c. Das Stammzertifikat (ca.crt und das Zwischenzertifikat (intca.crt) sind erforderlich, wenn Sie die Verbindung zum Server unter Verwendung von TLS herstellen.
   d. Erstellen Sie auf dem Server eine Zertifikatsanforderung für die Unterzeichnung durch die CA, indem Sie einen ähnlichen Befehl wie in dem folgenden Beispiel ausgeben:

      ```
      gsk8capicmd_64 -certreq -create -db cert.kdb -stashed -label "CA-Zertifikat"
      -sigalg sha256 -size 2048 -ku "digitalSignature,keyEncipherment,keyAgreement "
      -eku "clientAuth,serverAuth" -dn "CN=tucson.example.com,OU=Spectrum Protect,O=IBM"
      -san_dnsname tucson.example.com -san_ipaddr 9.11.0.0 -file cert_request.csr
      ```

   e. Um das signierte Zertifikat zu erhalten und als Standardzertifikat für die Kommunikation mit Clients festzulegen, geben Sie den folgenden Beispielbefehl aus:

      ```
      gsk8capicmd_64 -cert -receive -db cert.kdb -stashed -file signiertes_Zertifikat.crt
      -default_cert yes
      ```

5. Wenn Änderungen durchgeführt wurden, starten Sie den Server erneut.

Nächste Schritte

Aktivieren Sie SSL-Kommunikation von einem Client, einem Speicheragenten oder einem anderen Server zu diesem Server. Um die folgenden Tasks ausführen zu können, müssen Ihnen das Zertifikat des Servers und die Portnummer, die für den Server definiert ist, zur Verfügung stehen.

1. Informationen zum Aktivieren der SSL-Kommunikation einem Client zum diesem Server finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
2. Informationen zum Aktivieren der SSL-Kommunikation von einem anderen Server zum diesem Server finden Sie in Server für die Verbindung zu einem anderen Server unter Verwendung von SSL konfigurieren.
3. Informationen zum Aktivieren der SSL-Kommunikation von einem Speicheragenten zu diesem Server finden Sie in Speicheragenten für die Verwendung von SSL konfigurieren.
4. Informationen zum Aktivieren der SSL-Kommunikation vom Operations Center zu diesem Server finden Sie in Operations Center für die Verbindung zum Hub-Server unter Verwendung von SSL konfigurieren.

- Clients für die Kommunikation mit dem Server unter Verwendung von SSL konfigurieren
  Um sicherzustellen, dass Daten während der Client/Server-Kommunikation verschlüsselt werden, konfigurieren Sie Clients für die Kommunikation mit dem Server unter Verwendung des SSL-Protokolls.
- Server für die Verbindung zu einem anderen Server unter Verwendung von SSL konfigurieren
  Um sicherzustellen, dass Daten während der Kommunikation zwischen Servern verschlüsselt werden, konfigurieren Sie Server für die Kommunikation mit Servern unter Verwendung des SSL-Protokolls.
- Operations Center für die Verbindung zum Hub-Server unter Verwendung von SSL konfigurieren
  Um sicherzustellen, dass Daten für die Kommunikation zwischen dem Operations Center und dem Hub-Server verschlüsselt werden, konfigurieren Sie das Operations Center für die Kommunikation mit dem Hub-Server unter Verwendung des SSL-Protokolls.

Zugehörige Verweise:
TCPPORT
TCPADMINPORT
QUERY SESSION (Clientsitzungen abfragen)

Clients für die Kommunikation mit dem Server unter Verwendung von SSL konfigurieren

Um sicherzustellen, dass Daten während der Client/Server-Kommunikation verschlüsselt werden, konfigurieren Sie Clients für die Kommunikation mit dem Server unter Verwendung des SSL-Protokolls.

Vorbereitende Schritte

Das Zertifikat des Servers und die Nummer des Ports, den der Server verwendet, müssen Ihnen zur Verfügung stehen. Weitere Informationen finden Sie in Server zum Akzeptieren von SSL-Verbindungen konfigurieren.

Vorgehensweise

Informationen zum Aktivieren der SSL-Kommunikation zwischen dem Server und Clients finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.

Server für die Verbindung zu einem anderen Server unter Verwendung von SSL konfigurieren

Um sicherzustellen, dass Daten während der Kommunikation zwischen Servern verschlüsselt werden, konfigurieren Sie Server für die Kommunikation mit Servern unter Verwendung des SSL-Protokolls.

Vorbereitende Schritte

Das Zertifikat und die Portnummer des Servers, zum dem die Verbindung hergestellt wird, müssen Ihnen zur Verfügung stehen. Weitere Informationen finden Sie in Server zum Akzeptieren von SSL-Verbindungen konfigurieren.

Informationen zu diesem Vorgang

Tipp: Wenn beide Server IBM Spectrum Protect-Software der Version 8.1.2 oder höher verwenden, wird SSL automatisch konfiguriert. Die manuelle Konfiguration wird empfohlen, ist aber nicht erforderlich. Wenn entweder der Server oder der Speicheragent IBM Spectrum Protect-Software vor Version 8.1.2 verwenden, müssen Sie SSL manuell konfigurieren.
In der Prozedur werden die folgenden Serveradressen als Beispiele verwendet:

- Die Adresse von ServerA (der Server, zu dem die Verbindung hergestellt wird) lautet `bfa.tucson.example.com`.
- Die Adresse von ServerB lautet `bfb.tucson.example.com`.

Vorgehensweise

1. Erstellen Sie die Serverschlüsseldatenbank, indem Sie den Server starten. Die Serverschlüsseldatenbankdatei, cert.kdb, wird im Serverinstanzverzeichnis gespeichert.
2. Importieren Sie für jeden Server die Datei cert256.arm oder die CA-Zertifikatsdateien des anderen Servers:

   ```
   gsk8capicmd_64 -cert -add -label Server-IP-Adresse -db cert.kdb -stashed
   -file cert256.arm
   ```

   Tipp: Verwenden Sie die IP-Adresse des Servers als den Kennsatznamen.
3. Auf jedem Server können Sie die Zertifikate in der Schlüsseldatenbank anzeigen, indem Sie den folgenden Befehl ausgeben:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

4. Starten Sie die Server erneut.
5. Geben Sie den Befehl DEFINE SERVER aus.
   a. Geben Sie für ServerA den folgenden Befehl aus:

      ```
      DEFINE SERVER BFB hla=bfb.tucson.example.com lla=1542
      serverpa=Kennwort_für_BFB SSL=YES
      ```

   b. Geben Sie für ServerB den folgenden Befehl aus:

      ```
      DEFINE SERVER BFA hla=bfa.tucson.example.com lla=1542
      serverpa=Kennwort_für_BFA SSL=YES
      ```

Zugehörige Verweise:
QUERY SESSION (Clientsitzungen abfragen)
TCPPORT
TCPADMINPORT
DEFINE SERVER (Server für Übertragung zwischen Servern definieren)

Operations Center für die Verbindung zum Hub-Server unter Verwendung von SSL konfigurieren

Um sicherzustellen, dass Daten für die Kommunikation zwischen dem Operations Center und dem Hub-Server verschlüsselt werden, konfigurieren Sie das Operations Center für die Kommunikation mit dem Hub-Server unter Verwendung des SSL-Protokolls.

Vorbereitende Schritte

Das Zertifikat des Hub-Servers und die Nummer des Ports, den der Server verwendet, müssen Ihnen zur Verfügung stehen. Weitere Informationen finden Sie in Server zum Akzeptieren von SSL-Verbindungen konfigurieren.

Vorgehensweise

Informationen zur Konfiguration der SSL-Kommunikation für das Operations Center finden Sie in Kommunikation zwischen dem Operations Center und dem Hub-Server schützen.

Speicheragenten für die Verwendung von SSL konfigurieren

Um sicherzustellen, dass Daten für die Kommunikation zwischen dem Speicheragenten und dem Server sowie zwischen dem Speicheragenten und dem Client verschlüsselt werden, konfigurieren Sie die Speicheragenten für die Kommunikation unter Verwendung des SSL-Protokolls.

Vorbereitende Schritte

Das Zertifikat des Servers und die Nummer des Ports, den der Server verwendet, müssen Ihnen zur Verfügung stehen. Weitere Informationen finden Sie in Server zum Akzeptieren von SSL-Verbindungen konfigurieren.

Vorgehensweise

1. Initialisieren Sie den Speicheragenten und fügen Sie der Einheitenkonfigurationsdatei und der Optionsdatei des Speicheragenten (dsmsta.opt) Kommunikationsinformationen hinzu, indem Sie den Befehl DSMSTA SETSTORAGESERVER ausgeben. Sie müssen die Parameter SSL=YES und STAKEYDBPW=Kennwort angeben, um die Schlüsseldatenbankdatei in dsmsta.opt zu erstellen. Alle Kennwörter in dsmsta.opt werden verschlüsselt.

   ```
   dsmsta setstorageserver myname=Name_des_Speicheragenten mypa=Kennwort_des_Speicheragenten
   myhla=IP-Adresse servername=Servername serverpa=Serverkennwort hla=IP-Adresse lla=SSL-Port
   STAKEYDBPW=Kennwort ssl=yes
   ```

2. Erstellen Sie das Schlüsseldatenbankzertifikat und die Standardzertifikate, indem Sie den Speicheragenten starten.
3. Importieren Sie für den Speicheragenten und den Server die Datei cert256.arm oder die CA-Zertifikatsdateien des jeweils anderen:

   ```
   gsk8capicmd_64 -cert -add -label IP-Adresse -db cert.kdb -stashed
   -file cert256.arm
   ```

   Tipp: Verwenden Sie die IP-Adresse als den Kennsatznamen.
4. Sie können die Zertifikate in der Schlüsseldatenbank anzeigen, indem Sie den folgenden Befehl ausgeben:

   ```
   gsk8capicmd_64 -cert -list -db cert.kdb -stashed
   ```

5. Starten Sie den Speicheragenten und den Server erneut.
6. Bauen Sie die Kommunikation zwischen dem Server und dem Speicheragenten auf, indem Sie den folgenden Befehl ausgeben:

   ```
   define server sta hla=IP-Adresse lla=Port serverpa=Kennwort ssl=yes
   ```

Zugehörige Verweise:
QUERY SESSION (Clientsitzungen abfragen)
TCPPORT
TCPADMINPORT
DEFINE SERVER (Server für Übertragung zwischen Servern definieren)

Client für die Verbindung zu einem Speicheragenten unter Verwendung von SSL konfigurieren

Um die Daten, die zwischen einem Client und einem Speicheragenten übertragen werden, zu schützen, konfigurieren Sie den Client so, dass die Verbindung zum Speicheragenten unter Verwendung des SSL-Protokolls hergestellt wird.

Vorbereitende Schritte

Das Zertifikat und die Portnummer für den Speicheragenten müssen Ihnen zur Verfügung stehen.

Informationen zu diesem Vorgang

Nachdem Sie einen Speicheragenten zum Akzeptieren von SSL-Verbindungen konfiguriert haben, konfigurieren Sie Clients für die Herstellung der Verbindung zu dem Speicheragenten unter Verwendung von SSL.

Vorgehensweise

Informationen zum Aktivieren der SSL-Kommunikation zwischen den Clients und dem Speicheragenten finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
Zugehörige Verweise:
TCPPORT
TCPADMINPORT

IBM Spectrum Protect-Benutzer mithilfe eines LDAP-Servers authentifizieren

In einem IBM Spectrum Protect-System müssen sich Benutzer beim Server durch die Angabe einer Benutzer-ID und eines Kennworts authentifizieren. Wenn Ihr Unternehmen einen Lightweight Directory Access Protocol-Server (LDAP-Server) zur Verwaltung von Benutzer-IDs verwendet, können Sie den LDAP-Server für die Authentifizierung von IBM Spectrum Protect-Benutzer-IDs verwenden.

Sie können eine der folgenden Methoden verwenden, um Benutzer mit einem LDAP-Server zu authentifizieren:

Methode, die für IBM Spectrum Protect-Server der Version 7.1.7 und höher bevorzugt wird
: Um diese Methode, die manchmal auch als *integrierter Modus* bezeichnet wird, verwenden zu können, müssen Benutzer-IDs in einer Active Directory-Datenbank auf einem LDAP-Server registriert werden. Anschließend registrieren Sie dieselben Benutzer beim IBM Spectrum Protect-Server. Wenn eine registrierte Benutzer-ID auf den IBM Spectrum Protect-Server zugreift, werden die Berechtigungsnachweise mithilfe der Active Directory-Datenbank authentifiziert.
Führen Sie zur Verwendung dieser Methode die Anweisungen in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren aus.

Methode, die für Server vor Version 7.1.7 und von Benutzern von IBM® Security Directory Server verwendet wird
: Um diese Methode verwenden zu können, müssen Benutzer-IDs in einer Active Directory-Datenbank auf einem LDAP-Server registriert werden. Benutzer-IDs können auch stattdessen in einer Datenbank von IBM Security Directory Server (zuvor IBM Tivoli Directory Server) auf einem LDAP-Server registriert werden. Bei dieser Methode können Sie nicht die Standardbenutzerkonten verwenden, die beim LDAP-Server registriert sind. Sie müssen separate Benutzerkonten erstellen, die einer bestimmten Organisationseinheit zugeordnet sind. Führen Sie zur Verwendung dieser Methode die Anweisungen in Kennwörter und Anmeldeverfahren verwalten (Version 7.1.1) aus. .

- Benutzer mithilfe einer Active Directory-Datenbank authentifizieren
  Sie können IBM Spectrum Protect-Benutzer mithilfe einer Active Directory-Datenbank auf einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifizieren. Bei dieser Methode verwenden Sie die Standardbenutzerkonten, die beim LDAP-Server registriert sind. Dieselbe Benutzer-ID kann zur Authentifizierung beim IBM Spectrum Protect-Server und LDAP-Server verwendet werden.

Clientdaten auf einen anderen Server replizieren

Mithilfe der Replikation von Clientdaten von einem Quellenserver auf einen anderen Server kann sichergestellt werden, dass gesicherte Clientdaten für die Wiederherstellung verfügbar sind, wenn der Quellenserver beschädigt. ist. Bei der Replikation werden Daten inkrementell vom Quellenserver auf den Zielserver kopiert, um Übernahme- und Rückübertragungsfunktionalität bereitzustellen.

Informationen zu diesem Vorgang

Wenn ein Katastrophenfall eintritt und der Quellenserver vorübergehend nicht verfügbar ist, können Clientknoten ihre Daten vom Zielserver wiederherstellen. Wenn eine Wiederherstellung des Quellenservers nicht möglich ist, können Sie Clientknotenkonfigurationen ändern, um Daten auf dem Zielserver zu speichern. Bei einem Ausfall kann für den Quellenserver automatisch eine Übernahme durch einen Zielserver zum Zweck der Datenwiederherstellung erfolgen.
Einschränkung: Ein Server kann Daten nur auf einen einzigen Zielserver replizieren.
Die Replikation kann für Daten, die in einem beliebigen Typ von Speicherpool gespeichert sind, ausgeführt werden. Der Speicherpooltyp auf dem Quellenreplikationsserver und der Speicherpooltyp dem Zielreplikationsserver können unterschiedlich sein. Die Replikation kann anhand des Typs der Clientknotendaten gesteuert werden:

- Gleichzeitig aktive und inaktive Sicherungsdaten oder nur aktive Sicherungsdaten
- Archivierungsdaten
- Daten, die von IBM Spectrum Protect for Space Management-Clients auf einen Quellenserver umgelagert wurden

Wenn Sie Daten in Verzeichniscontainerspeicherpools replizieren, verwenden Sie Speicherpoolschutz, um die Effizienz des Replikationsprozesses zu verbessern und die Reparatur von Daten zu ermöglichen. Wenn Sie Ihre Speicherpools mithilfe des Operations Center konfigurieren, werden Zeitpläne für den Schutz automatisch in Koordination mit dem Replikationszeitplan definiert.

Vorgehensweise

1. Stellen Sie sicher, dass Server kompatibel sind und über die Systemressourcen für die erfolgreiche Verwendung der Replikation verfügen.

   Es sind mehr Speicherkapazität und mehr Prozessorkerne erforderlich. Die Größe der Datenbank und der zugehörigen Protokolle müssen geändert werden, um sicherzustellen, dass Transaktionen ausgeführt werden können. Es ist ein dediziertes Netz mit ausreichender Bandbreite zur Verarbeitung des zu replizierenden Datenvolumens erforderlich.

   a. Stellen Sie sicher, dass die Quellen- und Zielserver für die Replikation kompatibel sind. Siehe Replikationskompatibilität.
   b. Stellen Sie sicher, dass der Server über die entsprechenden Ressourcen verfügt, um eine gute Leistung erzielen zu können. Ausführliche Informationen finden Sie in Prüfliste für Knotenreplikation.
2. Aktivieren Sie die Replikation. Siehe Knotenreplikation aktivieren.
3. Planen Sie die Replikation für den Quellenserver. Informationen zur Integration dieses Zeitplans in die Zeitpläne für die regelmäßige Serververwaltung finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren.
4. Planen Sie den Speicherpoolschutz für alle Verzeichniscontainerspeicherpools auf dem Quellenserver. Siehe Daten in Verzeichniscontainerspeicherpools schützen.
5. Überwachen Sie die Replikation mithilfe des Operations Center. Weitere Informationen finden Sie in Prüfliste für tägliche Überwachungstasks.

- Replikationskompatibilität
  Vor dem Konfigurieren von Replikationsoperationen mit IBM Spectrum Protect müssen Sie sicherstellen, dass die Quellen- und Zielreplikationsserver für die Replikation kompatibel sind.
- Knotenreplikation aktivieren
  Sie können die Knotenreplikation zum Schützen Ihrer Daten aktivieren.
- Daten in Verzeichniscontainerspeicherpools schützen
  Schützen Sie Daten in Verzeichniscontainerspeicherpools, um die Knotenreplikationszeit zu reduzieren und die Reparatur von Daten in Verzeichniscontainerspeicherpools zu ermöglichen.
- Replikationseinstellungen ändern
  Ändern Sie Replikationseinstellungen im Operations Center. Ändern Sie Einstellungen wie die Anzahl Replikationssitzungen, Replikationsregeln, die Daten, die repliziert werden sollen, den Replikationszeitplan und die Replikationsworkload.
- Unterschiedliche Aufbewahrungsmaßnahmen für den Quellenserver und den Zielserver festlegen
  Auf dem Zielreplikationsserver können Sie Maßnahmen festlegen, mit denen die replizierten Clientknotendaten anders als auf dem Quellenserver verwaltet werden. Beispielsweise können Sie auf dem Quellen- und dem Zielserver eine unterschiedliche Anzahl Versionen von Dateien aufbewahren.

Replikationskompatibilität

Vor dem Konfigurieren von Replikationsoperationen mit IBM Spectrum Protect müssen Sie sicherstellen, dass die Quellen- und Zielreplikationsserver für die Replikation kompatibel sind.

Tabelle 1. Replikationskompatibilität von Serverversionen

Version des Quellenreplikationsservers	Kompatible Versionen für den Zielreplikationsserver
Version 6.3.0 - Version 6.3.2	Version 6.3.0 - Version 6.3.2
Version 6.3.3	Version 6.3.3 oder höhere Stufen von Version 6.3
Version 6.3.4 oder höhere Stufen von Version 6.3	Version 6.3.4 oder höher
Version 7.1	Version 7.1 oder höher
Version 7.1.1	Version 7.1 oder höher
Version 7.1.3	Version 7.1.3 oder höher
Version 7.1.4	Version 7.1.3 oder höher
Version 7.1.5	Version 7.1.3 oder höher
Version 7.1.6	Version 7.1.3 oder höher
Version 7.1.7	Version 7.1.3 oder höher
Version 8.1	Version 7.1.3 oder höher
Version 8.1.1	Version 7.1.3 oder höher
Version 8.1.2	Version 7.1.3 oder höher

Knotenreplikation aktivieren

Sie können die Knotenreplikation zum Schützen Ihrer Daten aktivieren.

Vorbereitende Schritte

Stellen Sie sicher, dass die Quellen- und Zielserver für die Replikation kompatibel sind.

Informationen zu diesem Vorgang

Replizieren Sie den Clientknoten, um alle Clientdaten, einschließlich Metadaten, zu replizieren. Standardmäßig ist die Knotenreplikation inaktiviert, wenn Sie den Server zum ersten Mal starten.
Tipps:

- Um die Replikationsverarbeitungszeit zu reduzieren, schützen Sie den Speicherpool vor dem Replizieren von Clientknoten. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch den Speicherpoolschutz repliziert werden, übersprungen.
- Die Replikation erfordert mehr Speicherkapazität und genügend Bandbreite für die Ausführung der Verarbeitung. Ändern Sie die Größe der Datenbank und der zugehörigen Protokolle, um sicherzustellen, dass Transaktionen ausgeführt werden können.

Vorgehensweise

Um die Knotenreplikation zu aktivieren, führen Sie im Operations Center die folgenden Schritte aus:

a. Klicken Sie auf der Seite Server auf Details.
b. Klicken Sie auf der Seite Details auf Merkmale.
c. Wählen Sie im Abschnitt Replikation im Feld Abgehende Replikation die Option Aktiviert aus.
d. Klicken Sie auf Sichern.

Nächste Schritte

Führen Sie die folgenden Aktionen aus:

1. Informationen zur Überprüfung, ob die Replikation erfolgreich war, finden Sie in Prüfliste für tägliche Überwachungstasks.
2. Linux-BetriebssystemeWenn der IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Führen Sie die Anweisungen in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann aus.

Daten in Verzeichniscontainerspeicherpools schützen

Schützen Sie Daten in Verzeichniscontainerspeicherpools, um die Knotenreplikationszeit zu reduzieren und die Reparatur von Daten in Verzeichniscontainerspeicherpools zu ermöglichen.

Vorbereitende Schritte

Stellen Sie sicher, dass mindestens ein Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver vorhanden ist. Wenn Sie die Replikation im Operations Center aktivieren, können Sie den Speicherpoolschutz planen. Um die Replikation zu konfigurieren und den Speicherpoolschutz zu aktivieren, führen Sie die folgenden Schritte aus:

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über Speicher und klicken Sie auf Replikation.
2. Klicken Sie auf der Seite 'Replikation' auf Serverpaar.
3. Führen Sie die Schritte im Assistenten 'Serverpaar hinzufügen' aus.

Informationen zu diesem Vorgang

Durch das Schützen eines Verzeichniscontainerspeicherpools werden Datenbereiche in einem anderen Speicherpool gesichert und die Leistung bei der Knotenreplikation wird gegebenenfalls verbessert. Wenn die Knotenreplikation gestartet wird, werden die Datenbereiche, die bereits durch Speicherpoolschutz gesichert werden, übersprungen und die Replikationsverarbeitungszeit wird somit reduziert. Sie können den Schutz von Speicherpools mehrmals am Tag planen, um den Änderungen an Daten Rechnung zu tragen.

Indem ein Speicherpool geschützt wird, werden keine Ressourcen verwendet, die vorhandene Daten und Metadaten replizieren, wodurch die Serverleistung verbessert wird. Sie müssen Verzeichniscontainerspeicherpools verwenden, wenn nur der Speicherpool geschützt und gesichert werden soll.

Alternative Schutzstrategie: Als Alternative zur Verwendung der Replikation können Sie Daten in Verzeichniscontainerspeicherpools schützen, indem Sie die Daten in Containerkopienspeicherpools kopieren. Daten in Containerkopienspeicherpools werden auf Banddatenträgern gespeichert. Bandkopien, die an einem anderen Standort aufbewahrt werden, stellen zusätzlichen Schutz für die Wiederherstellung nach einem Katastrophenfall in einer replizierten Umgebung bereit.

Vorgehensweise

1. Um den Speicherpoolschutz zu aktivieren, können Sie auch stattdessen den Befehl PROTECT STGPOOL auf dem Quellenserver verwenden, um Datenbereiche in einem Verzeichniscontainerspeicherpool zu sichern. Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen POOL1 zu schützen, geben Sie den folgenden Befehl aus:

   ```
   protect stgpool pool1
   ```

   Im Rahmen der Ausführung des Befehls PROTECT STGPOOL werden beschädigte Speicherbereiche im Zielspeicherpool repariert. Eine Reparatur ist nur möglich, wenn die Speicherbereiche auf dem Zielserver bereits als beschädigt markiert sind. Beispielsweise kann vor der Ausgabe des Befehls PROTECT STGPOOL mit einem Befehl AUDIT CONTAINER eine Beschädigung im Zielspeicherpool identifiziert werden.
2. Optional: Wenn beschädigte Speicherbereiche im Zielspeicherpool repariert wurden und Sie mehrere Quellenspeicherpools in einem einzigen Zielspeicherpool schützen, führen Sie die folgenden Schritte aus, um eine vollständige Reparatur zu gewährleisten:
   a. Geben Sie den Befehl PROTECT STGPOOL für alle Quellenspeicherpools aus, um die Beschädigung möglichst vollständig zu reparieren.
   b. Geben Sie den Befehl PROTECT STGPOOL erneut für alle Quellenspeicherpools aus. Verwenden Sie bei dieser zweiten Operation den Parameter FORCERECONCILE=YES. Mit diesem Schritt wird sichergestellt, dass alle Reparaturen anderer Quellenpools korrekt für alle Quellenspeicherpools erkannt werden.

Ergebnisse

Wenn ein Verzeichniscontainerspeicherpool geschützt wird, können Sie den Speicherpool für den Fall, dass eine Beschädigung auftritt, mit dem Befehl REPAIR STGPOOL reparieren.
Einschränkung: Wenn Sie Clientknoten replizieren, den Verzeichniscontainerspeicherpool aber nicht schützen, können Sie den Speicherpool nicht reparieren.

Nächste Schritte

Führen Sie die folgenden Aktionen aus:

1. Um den Replikationsworkloadstatus anzuzeigen, führen Sie die Anweisungen in Prüfliste für tägliche Überwachungstasks aus.
2. Linux-BetriebssystemeWenn der IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Führen Sie die Anweisungen in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann aus.

Zugehörige Tasks:
Verzeichniscontainerspeicherpools auf Band kopieren
Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)
PROTECT STGPOOL (Speicherpooldaten schützen)

Replikationseinstellungen ändern

Ändern Sie Replikationseinstellungen im Operations Center. Ändern Sie Einstellungen wie die Anzahl Replikationssitzungen, Replikationsregeln, die Daten, die repliziert werden sollen, den Replikationszeitplan und die Replikationsworkload.

Informationen zu diesem Vorgang

In den folgenden Szenarios müssen Sie möglicherweise Ihre Replikationseinstellungen ändern:

- Änderungen an Datenprioritäten
- Änderungen an Replikationsregeln
- Erfordernis eines anderen Servers als Zielserver
- Geplante Prozesse, die sich negativ auf die Serverleistung auswirken

Vorgehensweise

Ändern Sie Replikationseinstellungen mithilfe des Operations Center.

Task	Prozedur
Ändern einer Replikationsregel	a. Klicken Sie auf der Seite Server auf Details. b. Klicken Sie auf der Seite Details auf Merkmale. c. Wählen Sie im Abschnitt Replikation die Replikationsregel aus, die angewendet werden soll: Standardregel für Archivierungsdaten, Standardregel für Sicherungsdaten oder Standardregel für speicherverwaltete Daten. d. Klicken Sie auf Sichern.

Task	Prozedur
Aufbewahrungsdauer für Replikationsdatensätze angeben	a. Klicken Sie auf der Seite Server auf Details. b. Klicken Sie auf der Seite Details auf Merkmale. c. Geben Sie im Abschnitt Replikation im Feld Replikationsprotokoll aufbewahren die Anzahl Tage ein, die Replikationsdatensätze beibehalten werden müssen. Sie können auch das Kontrollkästchen Nicht aufbewahren auswählen, wenn Replikationsdatensätze nicht erforderlich sind. d. Klicken Sie auf Sichern.
Zielreplikationsserver angeben	a. Klicken Sie auf der Seite Server auf Details. b. Klicken Sie auf der Seite Details auf Merkmale. c. Geben Sie im Abschnitt Replikation den Zielserver an. d. Klicken Sie auf Sichern.
Replikationsprozess abbrechen	a. Klicken Sie auf der Seite Server auf Aktive Tasks. b. Wählen Sie den Prozess oder die Sitzung aus, der bzw. die abgebrochen werden soll. c. Klicken Sie auf Abbrechen.

Unterschiedliche Aufbewahrungsmaßnahmen für den Quellenserver und den Zielserver festlegen

Auf dem Zielreplikationsserver können Sie Maßnahmen festlegen, mit denen die replizierten Clientknotendaten anders als auf dem Quellenserver verwaltet werden. Beispielsweise können Sie auf dem Quellen- und dem Zielserver eine unterschiedliche Anzahl Versionen von Dateien aufbewahren.

Vorgehensweise

1. Überprüfen Sie auf dem Quellenreplikationsserver die Replikationskonfiguration und stellen Sie sicher, dass der Quellenreplikationsserver mit dem Zielreplikationsserver kommunizieren kann, indem Sie den Befehl VALIDATE REPLICATION ausgeben. Überprüfen Sie beispielsweise die Konfiguration unter Angabe des Namens eines Clientknotens, der repliziert wird:

   ```
   validate replication node1 verifyconnection=yes
   ```

2. Geben Sie auf dem Quellenreplikationsserver den Befehl VALIDATE REPLPOLICY aus, um die Unterschiede zwischen den Maßnahmen auf dem Quellenreplikationsserver und den Maßnahmen auf dem Zielreplikationsserver zu überprüfen. Um beispielsweise die Unterschiede zwischen den Maßnahmen auf dem Quellenserver und den Maßnahmen auf dem Zielserver CVT_SRV2 anzuzeigen, geben Sie auf dem Quellenserver den folgenden Befehl aus:

   ```
   validate replpolicy cvt_srv2
   ```

3. Aktualisieren Sie die Maßnahmen auf dem Zielserver, falls erforderlich.
   Tipp: Mithilfe des Operations Center können Sie die Maßnahmen auf dem Zielserver ändern. Führen Sie die Anweisungen in Maßnahmen editieren aus.
   Um beispielsweise inaktive Dateiversionen auf dem Zielserver für einen kürzeren Zeitraum als auf dem Quellenserver aufzubewahren, reduzieren Sie die Einstellung Sicherungen in den Verwaltungsklassen, die für replizierte Clientdaten gelten.
4. Ermöglichen Sie dem Zielreplikationsserver die Verwendung seiner Maßnahmen zur Verwaltung der replizierten Clientknotendaten, indem Sie auf dem Quellenserver den Befehl SET DISSIMILARPOLICIES ausgeben. Um beispielsweise die Maßnahmen auf dem Zielreplikationsserver CVT_SRV2 zu aktivieren, geben Sie auf dem Quellenserver den folgenden Befehl aus:

   ```
   set dissimilarpolicies cvt_srv2 on
   ```

   Bei der nächsten Ausführung des Replikationsprozesses werden die Maßnahmen auf dem Zielreplikationsserver zur Verwaltung der replizierten Clientknotendaten verwendet.
   Tipp: Wenn Sie die Replikation mithilfe des Operations Center konfigurieren und die Maßnahmen auf dem Quellen- und dem Zielreplikationsserver nicht übereinstimmen, wird die für den Quellenreplikationsserver angegebene Maßnahme verwendet. Wenn die Maßnahmen auf dem Zielreplikationsserver mithilfe des Befehls SET DISSIMILARPOLICIES aktiviert wurden, wird die für den Zielreplikationsserver angegebene Maßnahme verwendet. Wenn der Zielreplikationsserver nicht über die von dem Knoten auf dem Quellenreplikationsserver verwendete Maßnahme verfügt, wird die Maßnahme STANDARD verwendet.

Zugehörige Verweise:
EXPORT POLICY (Maßnahmeninformationen exportieren)
SET DISSIMILARPOLICIES (Maßnahmen auf dem Zielreplikationsserver zum Verwalten replizierter Daten aktivieren)
VALIDATE REPLICATION (Replikation für einen Clientknoten überprüfen)
VALIDATE REPLPOLICY (Maßnahmen auf dem Zielreplikationsserver überprüfen)
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Clusterumgebungen konfigurieren

Sie können den IBM Spectrum Protect-Server für das Clustering auf AIX-, Linux- oder Windows-Systemen konfigurieren.

Eine Clusterumgebung kann für die folgenden Betriebssysteme verwendet werden:

- IBM® PowerHA SystemMirror for AIX
- IBM Tivoli System Automation for Multiplatforms for AIX and Linux
- Microsoft Failovercluster für Windows

Sie können andere Clusterprodukte zusammen mit IBM Spectrum Protect verwenden, es ist jedoch keine Dokumentation nur nur eingeschränkte Unterstützung verfügbar. Die neuesten Informationen zur Unterstützung für Clusterumgebungen finden Sie unter http://www.ibm.com/support/docview.wss?uid=swg21609772.

Bevor Sie ein anderes Clusterprodukt verwenden, müssen Sie sicherstellen, dass DB2 die erforderlichen Dateisysteme unterstützt. Weitere Informationen zu der von Ihnen verwendeten Version von DB2 finden Sie in der Produktinformation zu DB2, indem Sie nach empfohlenen Dateisystemen suchen.

- Übersicht über die Clusterumgebung
  Cluster bestehen aus vielen Komponenten, wie beispielsweise aus IBM Spectrum Protect-Servern, Hardware und Software. Mithilfe des Clustering können Sie zwei oder mehr Server oder Knoten über ein System mit gemeinsamer Plattennutzung verknüpfen.
- AIX-BetriebssystemeAIX-Umgebung für Clustering konfigurieren
  Sie können den IBM Spectrum Protect-Server für AIX-Clusterumgebungen mithilfe von IBM PowerHA SystemMirror for AIX oder IBM Tivoli System Automation for Multiplatforms konfigurieren.
- Linux-BetriebssystemeLinux-Umgebung für Clustering konfigurieren
  Sie können den IBM Spectrum Protect-Server unter Linux in einer Clusterumgebung mithilfe von IBM Tivoli System Automation for Multiplatforms Version 3.2.2 konfigurieren.
- Windows-BetriebssystemeWindows-Clusterumgebung konfigurieren
  Sie können einen IBM Spectrum Protect-Server für Windows in einer Microsoft-Failoverclusterumgebung konfigurieren. Windows-Clusterumgebungen bestehen aus Komponenten, wie beispielsweise IBM Spectrum Protect-Servern, Hardware und Software. Wenn diese Komponenten mit demselben Plattensystem verbunden sind, wird die Ausfallzeit auf ein Mindestmaß reduziert.

Zugehörige Informationen:
Upgrade für den Server in einer Clusterumgebung durchführen
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Übersicht über die Clusterumgebung

Cluster bestehen aus vielen Komponenten, wie beispielsweise aus IBM Spectrum Protect-Servern, Hardware und Software. Mithilfe des Clustering können Sie zwei oder mehr Server oder Knoten über ein System mit gemeinsamer Plattennutzung verknüpfen.

Diese Konfiguration ermöglicht es den Knoten, Daten gemeinsam zu nutzen, was eine höhere Serververfügbarkeit bewirkt und Ausfallzeiten minimiert. Beispiel:

- Sie können Anwendungen und Hardwarekomponenten, die in einem Cluster implementiert sind, konfigurieren, überwachen und steuern.
- Sie können eine Clusterverwaltungsschnittstelle und IBM Spectrum Protect verwenden, um Clusteranordnungen anzugeben und Übernahmemuster zu definieren. Der Server ist Teil des Clusters, das eine zusätzliche Sicherheitsstufe bereitstellt, indem sichergestellt wird, dass keine Transaktionen verloren gehen, da ein Server fehlgeschlagen ist. Durch das von Ihnen definierte Übernahmemuster werden zukünftige Fehler verhindert.
- Sie können Clustering auf den Knotenreplikationsprozess anwenden. Die Serververfügbarkeit ist damit höher als sie es wäre, wenn die Knotenreplikation als eigenständiger Prozess verwendet würde. Die Serververfügbarkeit ist höher, da die Wahrscheinlichkeit der Übernahme eines Clients durch einen anderen Server in einer Clusterumgebung geringer ist. Wenn Sie Daten von mehreren Quellenreplikationsservern auf einen einzigen Zielreplikationsserver replizieren, besteht ein hohes Maß an Abhängigkeit vom Zielreplikationsserver. Durch eine Clusterumgebung wird die Abhängigkeit vom Zielreplikationsserver verringert.

Komponenten in einem Server-Cluster werden als *Clusterobjekte* bezeichnet. Clusterobjekte sind einer Merkmalgruppe mit Datenwerten zugeordnet, die die Identität und das Verhalten eines Objekts im Cluster beschreiben. Clusterobjekte können die folgenden Komponenten umfassen:

- Knoten
- Speicher
- Dienste und Anwendungen
- Netze

Sie verwalten Clusterobjekte, indem Sie deren Merkmale bearbeiten; dies erfolgt normalerweise über eine Clusterverwaltungsanwendung.

- Clusterknoten
  Alle Knoten in einem Cluster haben ähnliche Merkmale; dadurch können sie gemeinsamen verwendet werden.

AIX-Betriebssysteme

AIX-Umgebung für Clustering konfigurieren

Sie können den IBM Spectrum Protect-Server für AIX-Clusterumgebungen mithilfe von IBM® PowerHA SystemMirror for AIX oder IBM Tivoli System Automation for Multiplatforms konfigurieren.

PowerHA SystemMirror SystemMirror for AIX und Tivoli System Automation erkennen Systemausfälle und steuern die Übernahme durch einen Wiederherstellungsprozessor mit einem minimalen Verlust an Benutzerzeit. Sie können den IBM Spectrum Protect-Server auf einem System in einem PowerHA- oder einem Tivoli System Automation-Cluster konfigurieren. Der IBM Spectrum Protect-Server kann dann bei einem Systemausfall auf einem anderen System im Cluster gestartet werden.

Sowohl bei der Übernahme als auch bei der Rückübertragung sieht es so aus, als würde der IBM Spectrum Protect-Server angehalten und dann erneut gestartet. Alle Transaktionen, die zum Zeitpunkt der Übernahme oder der Rückübertragung aktiv waren, werden rückgängig gemacht; alle abgeschlossenen Transaktionen bleiben abgeschlossen. IBM Spectrum Protect-Clients betrachten die Übernahme oder Rückübertragung als Kommunikationsfehler und versuchen, ihre Verbindungen wiederherzustellen.

Die folgenden Informationen enthalten Details zu diesen Clustering-Optionen.

- Konfigurieren Sie IBM Spectrum Protect for AIX für die Verwendung von IBM PowerHA SystemMirror for AIX in einer Clusterumgebung; lesen Sie dazu die folgenden Abschnitte.
- Konfigurieren Sie IBM Spectrum Protect for AIX für die Verwendung von Tivoli System Automation in einer Clusterumgebung; lesen Sie dazu die Informationen unter http://www.ibm.com/support/docview.wss?uid=swg27039780.
- Siehe die Produktinformation zu PowerHA SystemMirror.

- AIX-BetriebssystemeAnforderungen für einen PowerHA-Cluster
  IBM PowerHA SystemMirror for AIX erkennt Systemausfälle und steuert die Übernahme durch einen Wiederherstellungsprozessor mit einem minimalen Verlust an Benutzerzeit.
- AIX-BetriebssystemePowerHA-Übernahme und -Rückübertragung
  Wenn ein Knoten ausfällt, überträgt der Server-Cluster die vom Knoten gehosteten Gruppen auf andere Knoten im Cluster. Dieser Übertragungsprozess wird als *Übernahme* (Failover) bezeichnet. Der gegenteilige Prozess, *Rückübertragung* (Failback), findet statt, wenn der ausgefallene Knoten wieder aktiv wird und die Gruppen, die auf die anderen Knoten übertragen wurden, wieder auf den ursprünglichen Knoten zurückübertragen werden.
- AIX-BetriebssystemePowerHA SystemMirror for AIX installieren und konfigurieren
  Sie können den IBM Spectrum Protect-Server für AIX-Clusterumgebungen mithilfe von IBM PowerHA SystemMirror for AIX konfigurieren.
- AIX-BetriebssystemeIBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA installieren
  Installieren Sie den IBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA, um den Server für das Clustering konfigurieren zu können.
- AIX-BetriebssystemeIBM Spectrum Protect-Client auf einem Produktionsknoten für PowerHA installieren
  Sie müssen nur die Dateigruppe des Clients für Sichern/Archivieren installieren, die die Dateien des Clients für Sichern/Archivieren und den Verwaltungsbefehlszeilenclient enthält.
- AIX-BetriebssystemeKonfiguration des IBM Spectrum Protect-Servers für PowerHA überprüfen
  Wenn Sie den IBM Spectrum Protect-Server für die Verwendung von PowerHA konfigurieren, müssen Sie die Konfiguration überprüfen.
- AIX-BetriebssystemeStandby-Knoten für PowerHA konfigurieren
  Stellen Sie für PowerHA vor dem Konfigurieren des Standby-Knotens sicher, dass der IBM Spectrum Protect-Server nicht auf dem Produktionsknoten ausgeführt wird.
- AIX-BetriebssystemeSpeichereinheiten für austauschbare Datenträger für AIX for PowerHA definieren
  Für ein Betriebssystem AIX müssen Sie die Speichereinheiten für austauschbare Datenträger definieren, die von IBM Spectrum Protect auf den Produktions- und Standby-Knoten verwendet werden. Der Speicherarchivmanager überprüft, ob sich die Kassette, die die Speichereinheit für austauschbare Datenträger enthält, im korrekten Laufwerk befindet.
- AIX-BetriebssystemeCluster-Manager- und IBM Spectrum Protect-Konfigurationen ausführen
  Aktualisieren Sie die Konfiguration des Cluster-Managers, um den IBM Spectrum Protect-Server als eine Anwendung und eine Übernahmeressource des Standby-Knotens zu definieren. Der Produktionsknoten ist Eigner dieser Anwendung.
- AIX-BetriebssystemeFehlerbehebung in der PowerHA-Clusterumgebung
  Die folgende Liste enthält Informationen zur Behebung häufig auftretender Fehler. Die Informationen, die für IBM PowerHA SystemMirror for AIX bereitgestellt werden, repräsentieren nicht alle möglichen Szenarios.

AIX-Betriebssysteme

Anforderungen für einen PowerHA-Cluster

IBM PowerHA SystemMirror for AIX erkennt Systemausfälle und steuert die Übernahme durch einen Wiederherstellungsprozessor mit einem minimalen Verlust an Benutzerzeit.

Für die Konfiguration des IBM Spectrum Protect-Servers gelten die folgenden Hardwarevoraussetzungen:

- Eine Hardwarekonfiguration, die für PowerHA geeignet ist. Die Speichereinheiten für austauschbare Datenträger des IBM Spectrum Protect-Servers müssen physisch mit mindestens zwei Knoten des PowerHA-Clusters an einem gemeinsam genutzten Bus (einschließlich eines Speicherbereichsnetzes) verbunden sein.
- Ausreichend gemeinsam genutzter Plattenspeicherplatz zum Speichern der IBM Spectrum Protect-Datenbank, der Wiederherstellungsprotokolle, des Instanzverzeichnisses und der Plattenspeicherpools, die verwendet werden sollen. Informationen zur

Bestimmung, wie viel Speicherplatz für die Datenbank und das Wiederherstellungsprotokoll erforderlich ist, um die Verfügbarkeit der Datenbank und des Wiederherstellungsprotokolls sicherzustellen, finden Sie in Bestandskapazität verwalten.
- Ein TCP/IP-Netz

Tipp: Wenn ein IBM Spectrum Protect-Server Speichereinheiten für austauschbare Datenträger verwaltet, können Sie zwei IBM Spectrum Protect-Server konfigurieren, die auf verschiedenen Systemen in einem PowerHA-Cluster ausgeführt werden. Jedes System kann beide Server ausführen, wenn das andere System ausfällt. Um zwei IBM Spectrum Protect-Server für die Ausführung auf unterschiedlichen Systemen in einem PowerHA-Cluster zu konfigurieren, müssen Sie ein anderes Dateisystem verwenden, auf das beide Server zugreifen können.
AIX-Betriebssysteme

PowerHA-Übernahme und -Rückübertragung

Wenn ein Knoten ausfällt, überträgt der Server-Cluster die vom Knoten gehosteten Gruppen auf andere Knoten im Cluster. Dieser Übertragungsprozess wird als *Übernahme* (Failover) bezeichnet. Der gegenteilige Prozess, *Rückübertragung* (Failback), findet statt, wenn der ausgefallene Knoten wieder aktiv wird und die Gruppen, die auf die anderen Knoten übertragen wurden, wieder auf den ursprünglichen Knoten zurückübertragen werden.

Die Begriffe *Produktionsknoten* und *Standby-Knoten* beziehen sich auf die beiden PowerHA-Knoten, auf denen der IBM Spectrum Protect-Server ausgeführt wird.

PowerHA handhabt die Übernahme der TCP/IP-Adresse und das Laden des gemeinsam genutzten Dateisystems auf den Standby-Knoten bzw. auf den Produktionsknoten.

Wenn eine *Übernahme* oder eine *Rückübertragung* erfolgt, werden alle Transaktionen, die zu diesem Zeitpunkt gerade verarbeitet werden, rückgängig gemacht. Für IBM Spectrum Protect-Clients stellt die *Übernahme* oder *Rückübertragung* einen Kommunikationsfehler dar. Daher müssen Sie wieder eine Verbindung herstellen, die auf den Einstellungen für die Optionen COMMRESTARTDURATION und COMMRESTARTINTERVAL basiert.

In der Regel können Sie den Client für Sichern/Archivieren von der letzten festgeschriebenen Transaktion aus erneut starten. Wenn ein Clientzeitplan ausgeführt wird, wenn eine *Übernahme* erfolgt, schlägt die Clientoperation wahrscheinlich fehl. Wenn Sie Clientoperationen erneut starten können, muss dies ab dem Anfang der Verarbeitung erfolgen. Die Client- und Agentenoperationen werden so ausgeführt, wie dies normalerweise der Fall wäre, wenn der Server angehalten und erneut gestartet worden wäre, während der Client und die Agenten verbunden waren. Der einzige Unterschied besteht darin, dass der Server physisch auf anderer Hardware erneut gestartet wird.

Wenn keine automatische *Rückübertragung* erfolgen soll, können Sie die Ressource als kaskadierende Ressourcengruppe ohne *Rückübertragung* konfigurieren.

Zugehörige Informationen:
Produktinformation zu PowerHA SystemMirror

PowerHA SystemMirror for AIX installieren und konfigurieren

Sie können den IBM Spectrum Protect-Server für AIX-Clusterumgebungen mithilfe von IBM® PowerHA SystemMirror for AIX konfigurieren.

- AIX-BetriebssystemePowerHA-Cluster installieren und konfigurieren
  Möglicherweise treten Verarbeitungsfehler auf, wenn die Installation und Konfiguration von IBM PowerHA SystemMirror for AIX nicht ordnungsgemäß ausgeführt wird.
- AIX-BetriebssystemeIBM Spectrum Protect-Server auf dem Primärknoten für PowerHA konfigurieren
  Sie können eine IBM Spectrum Protect-Serverinstanz auf dem Primärknoten konfigurieren.
- AIX-BetriebssystemeIBM Spectrum Protect-Server auf einem Sekundärknoten für PowerHA mit einer gemeinsam genutzten DB2-Instanz konfigurieren
  Wenn das DB2-Instanzverzeichnis von den Knoten im PowerHA-Cluster gemeinsam genutzt wird, müssen Sie keine DB2-Instanz auf dem Sekundärknoten erstellen. Der Assistent dsmicfgx wird nicht ausgeführt.
- AIX-BetriebssystemeIBM Spectrum Protect-Server auf einem Sekundärknoten für PowerHA mit einer separaten DB2-Instanz konfigurieren
  Sie müssen eine DB2-Instanz auf jedem Sekundärknoten erstellen, wenn das DB2-Instanzverzeichnis (/home/tsminst1/sqllib) von den Knoten im PowerHA-Cluster nicht gemeinsam genutzt wird.

AIX-Betriebssysteme

PowerHA-Cluster installieren und konfigurieren

Möglicherweise treten Verarbeitungsfehler auf, wenn die Installation und Konfiguration von IBM PowerHA SystemMirror for AIX nicht ordnungsgemäß ausgeführt wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den PowerHA-Cluster zu installieren und zu konfigurieren:

1. Definieren Sie die gemeinsam genutzten Dateisysteme und logischen Datenträger, wenn sie benötigt werden. Möglicherweise sollen Dateien aufgrund von Integritäts- oder Leistungsaspekten in separate Dateisysteme oder auf separate physische Platten gestellt werden. Stellen Sie das Ausgangsverzeichnis der Benutzerinstanz nicht auf eine gemeinsam genutzte Platte. Spiegeln Sie die logischen Datenträger (einschließlich der zu Grunde liegenden Dateisysteme), um maximale Verfügbarkeit bereitzustellen. Die Dateisysteme, die definiert werden müssen, umfassen das Instanzverzeichnis des IBM Spectrum Protect-Servers, die Datenbank- und Protokollverzeichnisse, alle Verzeichnisse für Plattenspeicherpools und Verzeichnisse für Speicherpools des Einheitentyps FILE.
2. Konfigurieren Sie PowerHA derart, dass der Produktionsknoten Eigner der gemeinsam genutzten Datenträgergruppen ist und der Standby-Knoten die gemeinsam genutzten Datenträgergruppen übernimmt, wenn der Produktionsknoten ausfällt.
3. Konfigurieren Sie PowerHA derart, dass auch für die Dateisysteme eine Übernahme erfolgt.
4. Definieren Sie eine Service-IP-Adresse für den IBM Spectrum Protect-Server. Die Service-IP-Adresse darf nicht mit einer der Host-IP-Adressen übereinstimmen. Die Service-IP-Adresse und nicht die tatsächliche Host-IP-Adresse wird von Host zu Host versetzt.
5. Führen Sie eine Übernahme für die gemeinsam genutzte Datenbank und die Protokoll- und Instanzverzeichnisse auf den Standby-Knoten des PowerHA-Clusters durch.

Ergebnisse

Sie müssen die Speichereinheiten für austauschbare Datenträger für die Übernahme konfigurieren und den IBM Spectrum Protect-Server als Anwendung für PowerHA definieren.

AIX-Betriebssysteme

IBM Spectrum Protect-Server auf dem Primärknoten für PowerHA konfigurieren

Sie können eine IBM Spectrum Protect-Serverinstanz auf dem Primärknoten konfigurieren.

Vorgehensweise

1. Lesen Sie die Abschnitte in den Informationen zum Konfigurieren des IBM Spectrum Protect-Servers.
2. Nach dem Konfigurieren der IBM Spectrum Protect-Serverinstanz auf dem Primärknoten können Sie den IBM Spectrum Protect-Server auf einem Sekundärknoten konfigurieren.

Zugehörige Tasks:
IBM Spectrum Protect-Serverinstanz konfigurieren
AIX-Betriebssysteme

IBM Spectrum Protect-Server auf einem Sekundärknoten für PowerHA mit einer gemeinsam genutzten DB2-Instanz konfigurieren

Wenn das DB2-Instanzverzeichnis von den Knoten im PowerHA-Cluster gemeinsam genutzt wird, müssen Sie keine DB2-Instanz auf dem Sekundärknoten erstellen. Der Assistent dsmicfgx wird nicht ausgeführt.

Vorgehensweise

Um eine Serverinstanz auf dem Sekundärknoten mit einer gemeinsam genutzten DB2-Instanz zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Fügen Sie auf jedem Knoten im Cluster dem Script /opt/tivoli/tsm/server/bin/rc.dsmserv den folgenden Text hinzu:

```
DB2NODES_TEMP='/tmp/db2nodes.tmp'
DB2NODES=${homeDir}/sqllib/db2nodes.cfg
# Aktueller Hostname
HOSTNAME=$(/bin/Hostname)
# Hostname in db2nodes.cfg gespeichert
DB2_HOST=$(cat $DB2NODES | cut -d ' ' -f 2)
# Bei unterschiedlichen Namen die Datei aktualisieren
if [[ "$HOSTNAME" != "$DB2_HOST" ]]
then
  echo "Hostname in db2nodes.cfg wird aktualisiert"
  sed -e s_${DB2_HOST}_${HOSTNAME}_g $DB2NODES > $DB2NODES_TEMP
  cp $DB2NODES_TEMP $DB2NODES
fi
```

   Tipp: Wenn der Text nicht in das Script eingeschlossen wird, können Sie ihn vor der Ausgabe des Scripts /opt/tivoli/tsm/server/bin/rc.dsmserv einfügen.
2. Versetzen Sie alle gemeinsam genutzten Ressourcen auf den Sekundärknoten.
3. Aktualisieren Sie im Script /opt/tivoli/tsm/server/bin/startserver die folgenden Variablen unter Angabe dieser Werte:

Tabelle 1. Variablen im Script /opt/tivoli/tsm/server/bin/startserver

Beschreibung	Variable	Beispiel

Beschreibung	Variable	Beispiel
Setzen Sie INST_USER auf die Instanzbenutzer-ID.	INST_USER	INST_USER='tsmuser1'
Setzen Sie INST_DIR auf die Position des IBM Spectrum Protect-Instanzverzeichnisses. Dieses Verzeichnis enthält dsmserv.dbid und dsmserv.opt.	INST_DIR	INST_DIR='/home/tsmuser1/tsminst1'
Wählen Sie eine der folgenden Startoptionen aus: Option 1 - Instanz verwenden: $INST_USER, führen Sie den Server jedoch als Root (-U) aus. Option 2 - Instanz verwenden: $INST_USER und führen Sie den Server als $INST_USER (-u) aus.	INST_OPTION	Option 1: INST_OPTION='-U $INST_USER' Option 2: INST_OPTION='-u $INST_USER'

4. Starten Sie den Server, indem Sie das folgende Script ausgeben:

   ```
   /opt/tivoli/tsm/server/bin/startserver
   ```

5. Geben Sie nach dem Starten des Servers den Befehl BACKUP DB aus, um sicherzustellen, dass die Daten erfolgreich gesichert werden.

AIX-Betriebssysteme

IBM Spectrum Protect-Server auf einem Sekundärknoten für PowerHA mit einer separaten DB2-Instanz konfigurieren

Sie müssen eine DB2-Instanz auf jedem Sekundärknoten erstellen, wenn das DB2-Instanzverzeichnis (/home/tsminst1/sqllib) von den Knoten im PowerHA-Cluster nicht gemeinsam genutzt wird.

Informationen zu diesem Vorgang

Sie können den IBM Spectrum Protect-Server auf einem Sekundärknoten mithilfe des Assistenten dsmicfgx oder manuell konfigurieren.

Vorgehensweise

- Um eine DB2-Instanz auf einem Sekundärknoten mithilfe des Assistenten dsmicfgx zu erstellen, führen Sie die folgenden Schritte aus:
  1. Führen Sie den Assistenten dsmicfgx aus.
  2. Wählen Sie in der Anzeige Instanzverzeichnis das Kontrollkästchen Aktivieren, wenn Sie die Serverinstanz auf einem Sekundärknoten eines Clusters mit hoher Verfügbarkeit konfigurieren aus.
- Um eine DB2-Instanz manuell auf einem Sekundärknoten zu erstellen, führen Sie die folgenden Schritte aus:
  1. Versetzen Sie alle gemeinsam genutzten Ressourcen auf den Sekundärknoten.
  2. Erstellen Sie eine DB2-Instanz, indem Sie den folgenden Befehl db2icrt ausgeben:

     ```
     /opt/tivoli/tsm/db2/instance/db2icrt -s ese -u Instanzbenutzer Instanzbenutzer
     ```

     Dabei ist *Instanzbenutzer* derselbe Benutzer, der auch Eigner der DB2-Instanz auf dem Primärknoten ist.
  3. Melden Sie sich nach dem Erstellen der DB2-Instanz als Instanzbenutzer an oder geben Sie den Befehl su aus:

     ```
     su - <Instanzbenutzer>
     ```

  4. Geben Sie als Instanzbenutzer die folgenden Befehle aus:

     ```
     db2start
     db2 update dbm cfg using DFTDBPATH gemeinsam_genutzter_Datenbankpfad
     db2 catalog db TSMDB1
     db2stop
     ```

     Dabei ist *gemeinsam_genutzter_Datenbankpfad* das gemeinsam genutzte Datenbankverzeichnis. Das gemeinsam genutzte Datenbankverzeichnis ist normalerweise das Serverinstanzverzeichnis.
     Tipp: Um den Wert für *gemeinsam_genutzter_Datenbankpfad* zu bestimmen, geben Sie auf dem Primärknoten den folgenden Befehl aus:

     ```
     db2 get dbm cfg | grep DFTDBPATH
     ```

  5. Aktualisieren Sie im Script /opt/tivoli/tsm/server/bin/startserver die folgenden Variablen unter Angabe dieser Werte:

Tabelle 1. Variablen im Script /opt/tivoli/tsm/server/bin/startserver

Beschreibung	Variable	Beispiel

Beschreibung	Variable	Beispiel
Setzen Sie INST_USER auf die Instanzbenutzer-ID.	INST_USER	INST_USER='tsmuser1'
Setzen Sie INST_DIR auf die Position des IBM Spectrum Protect-Instanzverzeichnisses. Dieses Verzeichnis enthält dsmserv.dbid und dsmserv.opt.	INST_DIR	INST_DIR='/home/tsmuser1/tsminst1'
Wählen Sie eine der folgenden Startoptionen aus: Option 1 - Instanz verwenden: $INST_USER, führen Sie den Server jedoch als Root (-U) aus. Option 2 - Instanz verwenden: $INST_USER und führen Sie den Server als $INST_USER (-u) aus.	INST_OPTION	Option 1: INST_OPTION='-U $INST_USER' Option 2: INST_OPTION='-u $INST_USER'

6. Starten Sie den Server, indem Sie das folgende Script ausgeben:

   ```
   /opt/tivoli/tsm/server/bin/startserver
   ```

7. Geben Sie nach dem Starten des Servers den Befehl BACKUP DB aus, um sicherzustellen, dass die Daten erfolgreich gesichert werden.

AIX-Betriebssysteme

IBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA installieren

Installieren Sie den IBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA, um den Server für das Clustering konfigurieren zu können.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den IBM Spectrum Protect-Server auf dem Produktionsknoten zu installieren:

1. Installieren Sie IBM Spectrum Protect. Wählen Sie eine der folgenden Komponenten aus:
   - Den IBM Spectrum Protect-Server
   - Den IBM Spectrum Protect-Einheitentreiber, falls erforderlich
   - Die IBM Spectrum Protect-Lizenz

   Die ausführbaren Dateien werden normalerweise auf den internen Platten des Produktionsknotens installiert, nicht in dem gemeinsam genutzten IBM Spectrum Protect-Plattenspeicher. Die ausführbaren Dateien des IBM Spectrum Protect-Servers werden im Verzeichnis /opt/tivoli/tsm/server/bin installiert.

2. Konfigurieren Sie IBM Spectrum Protect für die Verwendung der TCP/IP-Übertragungsmethode. Anweisungen finden Sie in den Informationen zur Konfiguration einer Serverinstanz in AIX: Erste Schritte nach der Installation von IBM Spectrum Protect.
3. Definieren Sie eine neue Benutzer-ID als Eigner der IBM Spectrum Protect-Serverinstanz oder verwenden Sie eine vorhandene Benutzer-ID, die noch nicht Eigner einer IBM Spectrum Protect-Instanz ist. Während Sie mit der Instanzbenutzer-ID angemeldet sind, führen Sie die folgenden Schritte aus:
   a. Erstellen Sie mit dem Befehl mkdir ein Instanzverzeichnis in einem gemeinsam genutzten Dateisystem, für das die Übernahme durch das Standby-System möglich ist. Diese Platte muss für PowerHA definiert sein.
   b. Erstellen Sie mit dem Befehl mkdir die Datenbank- und Protokollverzeichnisse in gemeinsam genutzten Dateisystemen, für die eine Übernahme durch das Standby-System möglich ist. Diese Platten müssen auch für PowerHA für die Übernahme definiert sein.
   c. Schließen Sie die Konfiguration mithilfe des Assistenten dsmicfgx ab.

Zugehörige Tasks:
AIX: Server installieren
Upgrade für den Server durchführen
AIX-Betriebssysteme

IBM Spectrum Protect-Client auf einem Produktionsknoten für PowerHA installieren

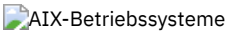
Sie müssen nur die Dateigruppe des Clients für Sichern/Archivieren installieren, die die Dateien des Clients für Sichern/Archivieren und den Verwaltungsbefehlszeilenclient enthält.

Vorgehensweise

Detaillierte Anweisungen zum Installieren des IBM Spectrum Protect-Clients finden Sie in IBM Spectrum Protect-Clients für Sichern/Archivieren installieren.

Führen Sie die folgenden Schritte aus, um den IBM Spectrum Protect-Client auf dem Produktionsknoten zu installieren.

1. Installieren Sie die ausführbaren Dateien des IBM Spectrum Protect-Clients im Verzeichnis /usr/tivoli/tsm/client/ba/bin. Diese Dateien werden normalerweise auf den internen Platten des Produktionsknotens installiert.
2. Damit der Client den Server finden kann, müssen Sie sicherstellen, dass die Clientoptionsdatei, dsm.sys, auf den IBM Spectrum Protect-Server verweist. Der Servername in dsm.sys wird nur im Parameter -servername des Befehls dsmadmc verwendet, um den Server anzugeben, auf den zugegriffen werden soll.



Konfiguration des IBM Spectrum Protect-Servers für PowerHA überprüfen

Wenn Sie den IBM Spectrum Protect-Server für die Verwendung von PowerHA konfigurieren, müssen Sie die Konfiguration überprüfen.

Informationen zu diesem Vorgang

Wenn Sie PowerHA verwenden, müssen sich alle Datenbank-, Protokoll-, Speicher- und Instanzverzeichnisse auf gemeinsam genutzten Platten befinden, die für die Übernahme durch PowerHA konfiguriert sind.

Vorgehensweise

Um die Verzeichnisse zu identifizieren, die sich auf gemeinsam genutzten Platten befinden, führen Sie die folgenden Schritte aus:

1. Melden Sie sich als der Instanzbenutzer an.
2. Führen Sie das Script /opt/tivoli/tsm/server/bin/dsmclustfs aus.
3. Prüfen Sie die Dateisysteme, die von dem Script zurückgemeldet werden, und stellen Sie sicher, dass sie sich auf gemeinsam genutzten Platten befinden. Das folgende Beispielscript zeigt, welchen Typ von Informationen Sie überprüfen müssen:

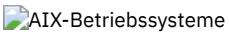
```
> su - tsminst1
$ /opt/tivoli/tsm/server/bin/dsmclustfs
SQL1026N Der Datenbankmanager ist bereits aktiv.
```

Die folgenden Datenbankverbindungsinformationen werden angezeigt, wenn der IBM Spectrum Protect-Server die Verbindung zur DB2-Datenbank herstellt:

```
DB20000I  Der Befehl START DATABASE MANAGER wurde erfolgreich ausgeführt.

   Datenbankverbindungsinformationen

 Datenbankserver                = DB2/AIX64 11.1.0
 SQL-Berechtigungs-ID           = TSMINST1
 Aliasname der lokalen Datenbank = TSMDB1

Dateisysteme, die für die DB2-Datenbank erforderlich sind: /TSMdbspace2 /TSMdbspace1
Dateisystem, das für die aktive Protokolldatei erforderlich ist: /TSMalog
Dateisystem, das für das Archivprotokoll erforderlich ist: /TSMarchlog
Spiegel der aktiven Protokolldatei für diese Datenbank nicht definiert
```

Das Script enthält die folgenden obligatorischen DB2-Dateisysteme:

```
 /TSMdb-1 /TSMalog-1 /TSMarchlog-1

Plattenbasierte TSM-Datenträger werden überprüft...
TSM-Daten sind in den folgenden Dateisystemen gespeichert: /TSMdisk-1 /TSMfile-1
```



Standby-Knoten für PowerHA konfigurieren

Stellen Sie für PowerHA vor dem Konfigurieren des Standby-Knotens sicher, dass der IBM Spectrum Protect-Server nicht auf dem Produktionsknoten ausgeführt wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Standby-Knoten zu konfigurieren:

1. Öffnen Sie auf dem Standby-Knoten die gemeinsam genutzte Datenträgergruppe und alle IBM Spectrum Protect-Dateisysteme.
2. Installieren Sie den IBM Spectrum Protect-Produktcode auf dem Standby-Knoten. Weitere Informationen finden Sie in IBM Spectrum Protect-Server auf einem Produktionsknoten für PowerHA installieren. Wenn die ausführbaren Dateien im gemeinsam genutzten

Plattenspeicher installiert werden, müssen Sie die Dateien möglicherweise auf dem Standby-Knoten installieren. IBM Spectrum Protect-Einheitentreiber, SMIT-Anzeigen und andere Dateien müssen in AIX-Systemverzeichnissen installiert werden.
3. Öffnen Sie den Assistenten dsmicfgx. Befolgen Sie die Anweisungen, um die Konfiguration abzuschließen. Wählen Sie das Kontrollkästchen aus, um anzugeben, dass es sich hierbei um einen Sekundärknoten im Cluster handelt.
4. Starten Sie den Server auf dem Standby-Knoten. Fragen Sie die Datenbank, das Wiederherstellungsprotokoll und die Speicherpooldatenträger ab, um zu prüfen, ob sie mit denen beim Starten des Servers auf dem Produktionsknoten übereinstimmen.
5. Installieren Sie den Client auf dem Standby-Knoten. Wenn die ausführbaren Dateien im gemeinsam genutzten Plattenspeicher installiert werden, müssen Sie die Dateien möglicherweise auf dem Standby-Knoten installieren. IBM Spectrum Protect, SMIT-Anzeigen und andere Dateien müssen in AIX-Systemverzeichnissen installiert werden. Verwenden Sie den AIX-Befehl RCP mit der Option -p, um die Datei dsm.sys vom Produktionsknoten auf den Standby-Knoten zu kopieren. Wird die Datei dsm.sys auf einem Knoten geändert, muss sie auf den anderen Knoten kopiert werden.

Ergebnisse

Tipp: Wird die Datei dsm.sys auf einem Knoten geändert, müssen Sie die Datei auf den anderen Knoten kopieren.
AIX-Betriebssysteme

Speichereinheiten für austauschbare Datenträger für AIX for PowerHA definieren

Für ein Betriebssystem AIX müssen Sie die Speichereinheiten für austauschbare Datenträger definieren, die von IBM Spectrum Protect auf den Produktions- und Standby-Knoten verwendet werden. Der Speicherarchivmanager überprüft, ob sich die Kassette, die die Speichereinheit für austauschbare Datenträger enthält, im korrekten Laufwerk befindet.

Informationen zu diesem Vorgang

Voraussetzung:

- Wenn Sie einen Speicherarchivmanagerserver definieren, der nicht gemeinsam mit dem IBM Spectrum Protect-Server genutzt wird, müssen Sie sicherstellen, dass der Parameter RESETDRIVES für den Befehl DEFINE LIBRARY oder den Befehl UPDATE LIBRARY YES lautet. Wenn Sie einen Speicherarchivmanagerserver definieren, der gemeinsam mit dem IBM Spectrum Protect-Server genutzt wird, muss die Option SANDISCOVERY in der IBM Spectrum Protect-Serveroptionsdatei dsmserv.opt auf ON gesetzt werden. Standardmäßig ist diese Option auf OFF gesetzt.
- Sie können den Befehl PERFORM LIBACTION für die Speicherarchivtypen SCSI und VTL ausgeben. Verwenden Sie diesen Befehl, um die Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt zu definieren.

Wenn die SAN-Einheitenzuordnung korrekt ist, fahren Sie mit Cluster-Manager- und IBM Spectrum Protect-Konfigurationen ausführen fort. Wenn die Einheitennamen auf dem primären und dem sekundären System nicht übereinstimmen, müssen Sie die SAN-Erkennung verwenden, damit der IBM Spectrum Protect-Server auf die Einheiten zugreifen kann.

Zugehörige Tasks:
Gemeinsame Speicherarchivnutzung konfigurieren (Version 7.1.1)
Zugehörige Verweise:
DEFINE LIBRARY (Speicherarchiv definieren)
UPDATE LIBRARY (Speicherarchiv aktualisieren)
PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Speicherarchiv definieren oder löschen)
SANDISCOVERY
Zugehörige Informationen:
Von IBM Spectrum Protect unterstützte Einheiten
AIX-Betriebssysteme

Cluster-Manager- und IBM Spectrum Protect-Konfigurationen ausführen

Aktualisieren Sie die Konfiguration des Cluster-Managers, um den IBM Spectrum Protect-Server als eine Anwendung und eine Übernahmeressource des Standby-Knotens zu definieren. Der Produktionsknoten ist Eigner dieser Anwendung.

Informationen zu diesem Vorgang

Sie können Befehle von IBM® PowerHA SystemMirror for AIX oder Tivoli System Automation ausgeben, um den Cluster zu konfigurieren. Fahren Sie mit der Konfiguration des IBM Spectrum Protect-Servers fort.

Zugehörige Informationen:
Produktinformation zu PowerHA SystemMirror
Produktinformation zu IBM Tivoli System Automation for Multiplatforms Version 3.2.2
AIX-Betriebssysteme

Fehlerbehebung in der PowerHA-Clusterumgebung

Die folgende Liste enthält Informationen zur Behebung häufig auftretender Fehler. Die Informationen, die für IBM® PowerHA SystemMirror for AIX bereitgestellt werden, repräsentieren nicht alle möglichen Szenarios.

Warnungen, die nach der Ausführung des Dienstprogramms clverify ausgegeben werden
: Sie können das PowerHA-Clusterprüfdienstprogramm clverify auf einem einzelnen Knoten ausführen, um die Clusterkonfiguration und die Zuordnung in den PowerHA-Ressourcen zu überprüfen. Wenn Sie das Dienstprogramm clverify nach der Definition des IBM Spectrum Protect-Servers als PowerHA-Anwendung ausführen, werden Warnungen ausgegeben.

  Warnungen werden angezeigt, da sich die Shell-Scripts, mit denen die IBM Spectrum Protect-Server gestartet und gestoppt werden, in einem gemeinsam genutzten Dateisystem befinden. Die Shell-Scripts können jeweils nur auf einem einzigen Knoten ausgeführt werden. Daher können die Shell-Scripts jeweils nur auf einem Knoten verfügbar sein. Sie können die Warnungen des Dienstprogramms clverify ignorieren. Kann ein gemeinsam genutztes Dateisystem nicht angehängt werden, kann der IBM Spectrum Protect-Server nicht gestartet werden.

IBM Spectrum Protect-Server wird nach dem Ausgeben des Scripts startserver nicht gestartet
: Wenn Sie das Shell-Script startserver verwenden und PowerHA den IBM Spectrum Protect-Server nicht starten kann, starten Sie ihn manuell an einem Terminal ohne Angabe der Option 'quiet'. Wenn der Server mit der Option 'quiet' ausgeführt werden soll, geben Sie den Befehl dsmserv -q aus.

Nachrichten, die dem Befehl tctl zugeordnet sind
: Wenn Sie den Befehl tctl -f/dev/rmt2 rewind ausgeben, kann die folgende Nachricht angezeigt werden:

  ```
  /dev/rmt2: A device is already mounted or cannot be unmounted
  ```

  Diese Nachricht gibt an, dass die E/A-Einheit mit einem Befehl SCSI RESERVE durch ein anderes System als das System gesperrt wird, auf dem der Befehl tctl ausgeführt wurde. Wenn Sie die persistente Reservierung verwenden, stellt der IBM Spectrum Protect-Server die Laufwerkreservierung standardmäßig zurück. Wenn der Einheitentreiber keine persistente Reservierung verwendet, führt der Server eine Zurücksetzung des Ziels aus.

Nachricht `ANS4329S Server hat keinen Datenspeicherbereich mehr`
: Wenn die Nachricht `ANS4329S Server hat keinen Datenspeicherbereich mehr` auf einem IBM Spectrum Protect-Client angezeigt wird, ist die Lizenz für den IBM Spectrum Protect-Server möglicherweise nicht konform. Geben Sie den Befehl QUERY LICENSE aus, um die Konformitätsinformationen für die Lizenz anzuzeigen. Wenn der Konformitätsstatus gültig ist, geben Sie den Befehl QUERY ACTLOG auf dem Server aus und überprüfen Sie die angezeigten Nachrichten, um das Problem zu bestimmen.

 Linux-Betriebssysteme

Linux-Umgebung für Clustering konfigurieren

Sie können den IBM Spectrum Protect-Server unter Linux in einer Clusterumgebung mithilfe von IBM® Tivoli System Automation for Multiplatforms Version 3.2.2 konfigurieren.

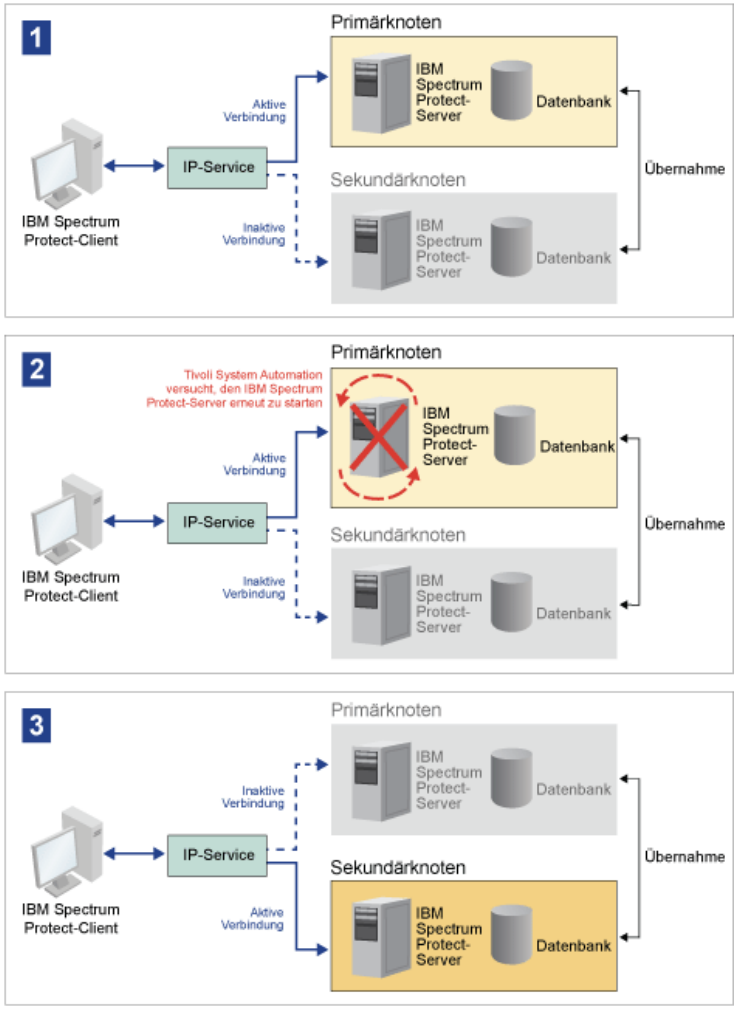
-  Linux-BetriebssystemeÜbersicht über einen IBM Spectrum Protect-Cluster mit zwei Knoten, der Tivoli System Automation verwendet
  Verwenden Sie den Tivoli System Automation-Cluster, um eine höherer Server- und Datenbankverfügbarkeit während eines Fehlers zu gewährleisten. Mithilfe der Übernahmefunktion von Tivoli System Automation können Serverkomponenten wie beispielsweise die Datenbank nach einem Fehler automatisch wiederhergestellt werden.
-  Linux-BetriebssystemeIBM Spectrum Protect-Cluster mit Tivoli System Automation konfigurieren
  Sie müssen den IBM Spectrum Protect-Cluster konfigurieren, um Tivoli System Automation verwenden zu können.
-  Linux-BetriebssystemeVoraussetzungen zum Konfigurieren einer Linux-Clusterumgebung mit Tivoli System Automation
  Bevor Sie IBM Spectrum Protect in einer Clusterumgebung mit Tivoli System Automation installieren und konfigurieren, müssen Sie die Voraussetzungen überprüfen.
-  Linux-BetriebssystemeIBM Spectrum Protect-Komponenten auf den Primär- und Sekundärknoten installieren und konfigurieren
  Sie müssen die IBM Spectrum Protect-Server- und -Datenbankkomponenten auf den Primär- und Sekundärknoten im Cluster installieren. Konfigurieren Sie anschließend zunächst den Primärknoten und dann den Sekundärknoten.
-  Linux-BetriebssystemeTivoli System Automation auf den Primär- und Sekundärknoten installieren
  Nachdem Sie IBM Spectrum Protect auf den Primär- und Sekundärknoten im Cluster installiert und konfiguriert haben, müssen Sie Tivoli System Automation auf diesen Knoten installieren und konfigurieren. Anschließend müssen Sie diese Knoten für die Domäne aktivieren, die Ressourcen konfigurieren und die Basismaßnahme aktivieren. Abschließend müssen Sie den IBM Spectrum Protect-Verzeichnissen die Mountpunkte hinzufügen.
-  Linux-BetriebssystemeSpeicherressourcen konfigurieren
  Verwenden Sie die Tivoli System Automation-Benutzerschnittstelle, oder -Befehlszeile, um Speicherressourcen hinzuzufügen oder zu löschen und um Mountpunkte, die nicht mehr benötigt werden, zu löschen. Wenn Sie dem Cluster einen Speicherpool hinzufügen, müssen Sie den Speicherpool der Ressourcengruppe hinzufügen. Wenn Sie einen Speicherpool aus dem Cluster entfernen, müssen Sie den Speicherpool auch aus der Ressourcengruppe löschen.
-  Linux-BetriebssystemeUpgrade für einen Server durchführen, der mit Tivoli System Automation konfiguriert ist
  Sie können ein Upgrade für einen Server der Version 6.3 oder Version 7.1 durchführen, der mit Tivoli System Automation konfiguriert ist.

 Linux-Betriebssysteme

Übersicht über einen IBM Spectrum Protect-Cluster mit zwei Knoten, der Tivoli System Automation verwendet

Verwenden Sie den Tivoli System Automation-Cluster, um eine höherer Server- und Datenbankverfügbarkeit während eines Fehlers zu gewährleisten. Mithilfe der Übernahmefunktion von Tivoli System Automation können Serverkomponenten wie beispielsweise die Datenbank nach einem Fehler automatisch wiederhergestellt werden.

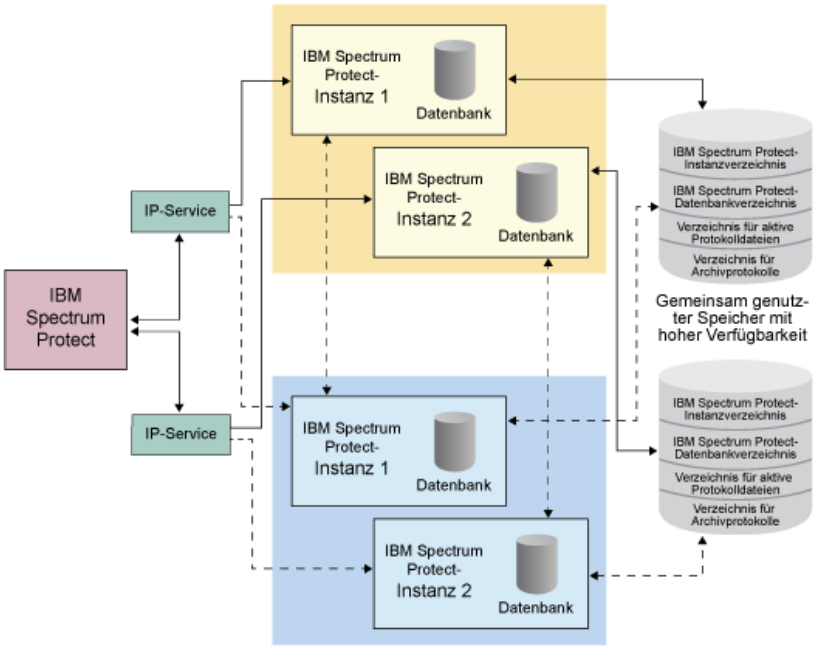
Der IBM Spectrum Protect-Server und die DB2-Datenbank sind die zu Grunde liegenden Serverkomponenten für diesen Cluster mit zwei Knoten. Der Server ist die Kernkomponente. Er ist für die Client- und Serveraktivität verantwortlich. Die DB2-Datenbank ist eine interne Komponente, die als Teil des Servers installiert wird. Der Server steuert die gesamte Datenbankaktivität, wie beispielsweise Start und Beendigung. Wenn der Server einen Fehler der Server- oder Datenbankkomponente erkennt, versucht er, die Datenbank erneut zu starten. Wenn der Neustart fehlschlägt, werden der Server und die Datenbank automatisch auf dem Primärknoten beendet und Tivoli System Automation startet diese Komponenten automatisch auf dem Sekundärknoten. Da die IBM Spectrum Protect-Funktionen sofort wiederhergestellt werden, ist die Server- und Datenbankverfügbarkeit höher.
Abbildung 1. Die Übernahmefunktion. Die Server- und Datenbankkomponenten schlagen auf dem Primärknoten fehl. Tivoli System Automation startet diese Komponenten auf dem Sekundärknoten.



Der Server und die Datenbank umfassen die folgenden Protokollverzeichnisse, die für die Speicherung verwendet werden:

- IBM Spectrum Protect-Instanzverzeichnis
- Verzeichnis für aktive Protokolldateien
- Verzeichnis für Archivprotokolle
- Datenbankverzeichnis

Die beiden Knoten in diesem Tivoli System Automation-Cluster sind für den Zugriff auf gemeinsam genutzten Speicher mit hoher Verfügbarkeit, der die Daten schützt, konfiguriert. Beispielsweise umfasst eine Zwei-Knoten-Topologie einen Primärknoten und einen Sekundärknoten. Diese Knoten befinden sich auf unterschiedlichen physischen Systemen, können aber unter Verwendung des gemeinsam genutzten Speicherbereichs auf dieselben Daten zugreifen.
Abbildung 2. Mehrere IBM Spectrum Protect-Serverinstanzen auf unterschiedlichen Knoten. Diese Serverinstanzen befinden sich auf unterschiedlichen physischen Systemen. Diese Instanzen können auf gemeinsam genutzten Speicher mit hoher Verfügbarkeit zugreifen.



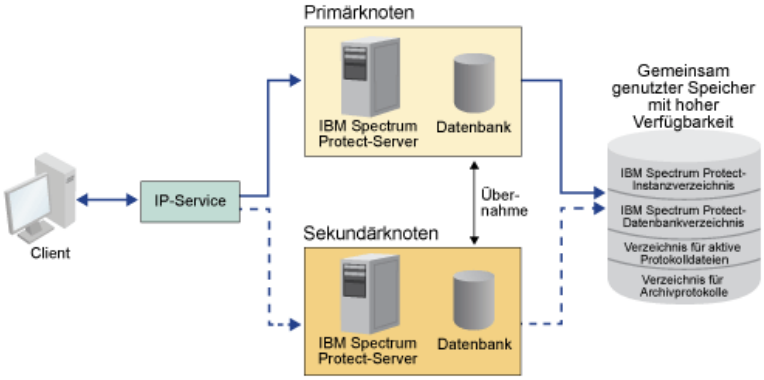
- Linux-BetriebssystemeZwei-Knoten-Topologie mit gemeinsam genutzter Platte
  Dieser Cluster verwendet eine Zwei-Knoten-Topologie mit gemeinsam genutzter Platte. Er umfasst einen Primärknoten und einen Sekundärknoten. Der Primärknoten hostet den IBM Spectrum Protect-Server, die Datenbank, die IBM Spectrum Protect-Instanz und die Daten. Der Sekundärknoten ist der Knoten, auf den die IBM Spectrum Protect-Ressourcen versetzt werden, wenn ein Fehler auftritt.
- Linux-BetriebssystemeTivoli System Automation-Ressourcengruppen
  Tivoli System Automation-Ressourcengruppen mit definierten Automatisierungsmaßnahmen ermöglichen Ihnen die Verwaltung der IBM Spectrum Protect-Komponenten für diesen Cluster. Die einzige Ausnahme ist die Datenbankserverinstanzressource, die vom IBM Spectrum Protect-Server verwaltet wird.

Linux-Betriebssysteme

Zwei-Knoten-Topologie mit gemeinsam genutzter Platte

Dieser Cluster verwendet eine Zwei-Knoten-Topologie mit gemeinsam genutzter Platte. Er umfasst einen Primärknoten und einen Sekundärknoten. Der Primärknoten hostet den IBM Spectrum Protect-Server, die Datenbank, die IBM Spectrum Protect-Instanz und die Daten. Der Sekundärknoten ist der Knoten, auf den die IBM Spectrum Protect-Ressourcen versetzt werden, wenn ein Fehler auftritt.

Die zwei Knoten in diesem Cluster sind über ein einzelnes öffentliches Netz miteinander verbunden und mit einem System mit *gemeinsam genutztem Plattenspeicher*, das immer verfügbar ist, über ein Festnetz verbunden. *Gemeinsam genutzter Plattenspeicher* bedeutet, dass ein oder mehrere Platten sowohl für den Primärknoten als auch für den Sekundärknoten verfügbar sind. Diese Platten werden jeweils nur einem einzigen Knoten, dem Primärknoten, bereitgestellt. Daten können von einem einzelnen Knoten als Eingabe an die gemeinsam genutzten Speicherplatten gesendet oder als Ausgabe von ihnen abgerufen werden. Die folgende Abbildung zeigt eine Zwei-Knoten-Topologie mit gemeinsam genutzter Platte, bei der die automatische Übernahme durch den Sekundärknoten erfolgt, wenn ein Fehler auftritt.



Linux-Betriebssysteme

Tivoli System Automation-Ressourcengruppen

Tivoli System Automation-Ressourcengruppen mit definierten Automatisierungsmaßnahmen ermöglichen Ihnen die Verwaltung der IBM Spectrum Protect-Komponenten für diesen Cluster. Die einzige Ausnahme ist die Datenbankserverinstanzressource, die vom IBM Spectrum

Protect-Server verwaltet wird.

Die gemeinsam genutzten Dateisysteme und IBM Spectrum Protect-Komponenten sind als Ressourcen definiert. Mehrere Ressourcen bilden eine Ressourcengruppe. Jede Ressource in einer Ressourcengruppe hat einen Ressourcentyp. Jede IBM Spectrum Protect-Instanz in einem Cluster umfasst eine einzelne Ressourcengruppe. Während geplanter Betriebsunterbrechungen können Ressourcengruppen manuell vom Primärknoten auf den Sekundärknoten versetzt werden.

Die IBM Spectrum Protect-Ressourcengruppe umfasst die folgenden Ressourcen. Die IBM Spectrum Protect-Ressourcengruppe hat den Namen SA-tsm-inst1-rg; dabei gibt 'inst1' den Instanznamen an. Die folgenden Ressourcen werden für unterschiedliche, aber obligatorische Funktionen in diesem Cluster verwendet.

Service-IP
: Die Service-IP-Ressource wird für die Kommunikation verwendet. Sie hat den Namen tsm-inst1-ip-rs; dabei gibt 'inst1' den Instanznamen an. Das Service-IP wird von Tivoli System Automation verwaltet. Dieses IP ist auf dem Knoten verfügbar, auf dem der IBM Spectrum Protect-Server ausgeführt wird. Sie müssen die logische Schnittstelle für das Service-IP auf derselben physischen Schnittstelle wie die Schnittstelle für das öffentliche Netz erstellen.

Ressource *Gemeinsam genutzter Plattenspeicher*
: Eine Ressource *Gemeinsam genutzter Plattenspeicher* ist eine physische Speichereinheit auf dem IBM Spectrum Protect-Server, auf der IBM Spectrum Protect- und DB2-Anwendungsdaten gespeichert werden. Sie müssen die folgenden Plattenspeicherressourcen erstellen:

  - Instanzverzeichnis - tsm-inst1-instdir-ag
  - DB2-Verzeichnis - tsm-inst1-db2dir-ag
  - Verzeichnis für aktive Protokolldateien - tsm-inst1-actlog-ag
  - Verzeichnis für Archivprotokolle - tsm-inst1-archlog-ag

Ressource *Gemeinsam genutzter Plattenspeicher* für Speicherpools
: Die Speicherpoolressource umfasst physische Speichereinheiten auf dem IBM Spectrum Protect-Server, auf denen Clientdaten gespeichert werden.

Datenträgergruppenressourcen
: Wenn Sie Ihren Speicher mithilfe von Datenträgergruppen konfigurieren, ist für die vorhergehenden Ressourcen *Gemeinsam genutzter Plattenspeicher* eine Datenträgergruppenressource verfügbar. Datenträgergruppenressourcen werden automatisch von Tivoli System Automation erstellt.

Anwendungsressourcen für die IBM Spectrum Protect-Serverinstanz
: Bei der IBM Spectrum Protect-Serverinstanzressource handelt es sich um die Serverressource, die die IBM Spectrum Protect-Anwendung verwaltet. Diese Ressource wird mithilfe von Tivoli System Automation-Steuerscripts verwaltet.

Tabelle 1. Tasks, die von den Tivoli System Automation-Steuerscripts ausgeführt werden

Tasks	Beschreibung	Beispielbefehle
Starten	Startet die IBM Spectrum Protect-Serverinstanz.	Mit dem Befehl /opt/tivoli/tsm/server/bin/rc.dsmserv -u db2inst1 –i /tsminst1 wird die Serverinstanz vom Benutzer db2inst1 im Verzeichnis /tsminst1 gestartet.
Stoppen	Stoppt die IBM Spectrum Protect-Serverinstanz.	kill –s SIGURG 345; dabei ist `345` die *PID*. Die *PID* ist in der Datei /tsminst1/dsmserv.v6lock angegeben.
Überwachen	Prüft, ob die Datei /tsminst1/dsmserv.v6lock vorhanden ist. Mithilfe der *PID* wird geprüft, ob der Prozess aktiv ist.	ps -ef | grep 345; dabei ist `345` die *PID*.

- Linux-BetriebssystemeRessourcengruppenabhängigkeiten
  Ressourcengruppenabhängigkeiten werden automatisch erstellt, um zu steuern, in welcher Reihenfolge Ressourcen gestartet werden. Diese Abhängigkeiten steuern auch, welche Ressourcen erneut gestartet oder beendet werden müssen, wenn die spezifische Ressource, von der diese Ressourcen abhängig sind, fehlschlägt.

Linux-Betriebssysteme

IBM Spectrum Protect-Cluster mit Tivoli System Automation konfigurieren

Sie müssen den IBM Spectrum Protect-Cluster konfigurieren, um Tivoli System Automation verwenden zu können.

Vorgehensweise

1. Installieren und konfigurieren Sie die IBM Spectrum Protect-Komponenten auf den Primär- und Sekundärknoten.
2. Installieren Sie Tivoli System Automation auf den Primär- und Sekundärknoten.
3. Konfigurieren Sie die Speicherressourcen.
4. Abhängig von der IBM Spectrum Protect-Version, die auf dem Server installiert ist, müssen Sie gegebenenfalls ein Upgrade des IBM Spectrum Protect-Servers für den Tivoli System Automation-Cluster durchführen.

5. Optional: Sie können die Variable *FILE_EXIT* im Cluster-Script tsmserverctrl definieren, um die Tivoli System Automation-Ereignisdaten in die IBM Spectrum Protect-Serverdatei FILEEXIT umzuleiten.
   Editieren Sie beispielsweise das Cluster-Script tsmserverctrl im Verzeichnis *<Serverinstallationsverzeichnis>*/tsam/controls und fügen Sie die folgende Zeile hinzu:

   ```
   FILE_EXIT="fileexittmp"
   ```

 Linux-Betriebssysteme

Voraussetzungen zum Konfigurieren einer Linux-Clusterumgebung mit Tivoli System Automation

Bevor Sie IBM Spectrum Protect in einer Clusterumgebung mit Tivoli System Automation installieren und konfigurieren, müssen Sie die Voraussetzungen überprüfen.

Überprüfen Sie, ob die folgenden Voraussetzungen erfüllt sind.

- Planen Sie die Installation des IBM Spectrum Protect-Servers.
- Überprüfen Sie nach der Installation von IBM Spectrum Protect Folgendes:
  - Stellen Sie sicher, dass die DB2-Datenbank auf demselben Knoten wie der Server installiert ist.
  - Stellen Sie sicher, dass der Server die Datenbankwiederherstellung steuern kann.
  - Stellen Sie sicher, dass gemeinsam genutzte Speichereinheiten verfügbar sind. IBM Spectrum Protect erfordert gemeinsam genutzte Speichereinheiten mit hoher Verfügbarkeit, um die Datenintegrität gewährleisten zu können.
  - Stellen Sie sicher, dass jeder Knoten im Cluster mehrere Instanzen des Servers enthalten kann.
- Bereiten Sie die Installation von Tivoli System Automation vor. Anweisungen finden Sie in der Tivoli System Automation-Produktdokumentation. Suchen Sie in der Veröffentlichung *Installation and Configuration Guide* nach *Preparing for installation*.
- Stellen Sie nach der Installation von Tivoli System Automation sicher, dass Tivoli System Automation die Übernahme, wie beispielsweise IP-Übernahme und Datenübernahme, für die Datenbank, die Instanzdaten, die aktive Protokolldatei und das Archivprotokoll sowie für Speicherpools verarbeiten kann.

Zugehörige Tasks:
Installation des IBM Spectrum Protect-Servers planen
Linux-Betriebssysteme

IBM Spectrum Protect-Komponenten auf den Primär- und Sekundärknoten installieren und konfigurieren

Sie müssen die IBM Spectrum Protect-Server- und -Datenbankkomponenten auf den Primär- und Sekundärknoten im Cluster installieren. Konfigurieren Sie anschließend zunächst den Primärknoten und dann den Sekundärknoten.

-  Linux-BetriebssystemeIBM Spectrum Protect-Serverkomponenten installieren
  Nachdem Sie die Voraussetzungen überprüft haben, müssen Sie die erforderlichen Komponenten auf den Primär- und Sekundärknoten auf dem System installieren.
-  Linux-BetriebssystemePrimärknoten konfigurieren
  Um die Zwei-Knoten-Topologie zu definieren, konfigurieren Sie die IBM Spectrum Protect-Komponenten auf beiden Knoten. Zunächst müssen Sie die IBM Spectrum Protect-Instanz auf dem Primärknoten konfigurieren.
-  Linux-BetriebssystemeSekundärknoten konfigurieren
  Nachdem Sie den Primärknoten konfiguriert haben, müssen Sie den Sekundärknoten konfigurieren, damit Tivoli System Automation die IBM Spectrum Protect-Serverkomponenten auf den Sekundärknoten versetzen kann, wenn der Server auf dem Primärknoten fehlschlägt.

 Linux-Betriebssysteme

IBM Spectrum Protect-Serverkomponenten installieren

Nachdem Sie die Voraussetzungen überprüft haben, müssen Sie die erforderlichen Komponenten auf den Primär- und Sekundärknoten auf dem System installieren.

Vorgehensweise

Lesen Sie die Abschnitte in den Informationen zum Installieren der IBM Spectrum Protect-Serverkomponenten.
Zugehörige Tasks:
IBM Spectrum Protect-Serverkomponenten installieren
 Linux-Betriebssysteme

Primärknoten konfigurieren

Um die Zwei-Knoten-Topologie zu definieren, konfigurieren Sie die IBM Spectrum Protect-Komponenten auf beiden Knoten. Zunächst müssen Sie die IBM Spectrum Protect-Instanz auf dem Primärknoten konfigurieren.

Vorbereitende Schritte

- Installieren Sie die IBM Spectrum Protect-Serverkomponenten.
- Stellen Sie sicher, dass der IBM Spectrum Protect-Instanzeigner für alle Knoten in der Clusterdomäne dieselbe Benutzer-ID und dieselbe Gruppen-ID hat.
- Stellen Sie sicher, dass der IBM Spectrum Protect-Instanzeigner für alle Clusterknoten dasselbe Kennwort hat.

Vorgehensweise

1. Detaillierte Anweisungen zum Erstellen der Verzeichnisse und der Benutzer-ID für die Serverinstanz finden Sie in Linux: Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen.
2. Stellen Sie sicher, dass der IBM Spectrum Protect-Server, die DB2-Instanz und die Verzeichnisse für die aktive Protokolldatei und das Archivprotokoll gemeinsam genutzt werden.
3. Definieren Sie die Mountpunkte, indem Sie der Datei /etc/fstab Einträge hinzufügen.

   Wenn Sie auf den Clusterknoten Mountpunkte hinzufügen, verwenden Sie die Option noauto, um zu verhindern, dass die Mountpunkte automatisch auf mehr als einem Knoten im Cluster bereitgestellt werden.

4. Definieren Sie für jeden der Mountpunkte die folgenden Berechtigungen:
   - 755. Beispielsweise wird mit dem folgenden Befehl die Berechtigung 755 für den Mountpunkt `/tsminst1` definiert.

     ```
     chmod -R 755 /tsminst1
     ```

   - IBM Spectrum Protect-Serverinstanzeigner. Beispielsweise werden mit dem folgenden Befehl die Berechtigungen für den Instanzeigner definiert.

     ```
     chown -R  tsminst1  /tsminst1
     ```

   - IBM Spectrum Protect-Servergruppe, zu der der Instanzeigner gehört. Beispielsweise werden mit dem folgenden Befehl die Berechtigungen für die Gruppe des Instanzeigners definiert.

     ```
     chgrp tsmsrv_1_group /tsminst1
     ```

5. Detaillierte Anweisungen zur Konfiguration des IBM Spectrum Protect-Servers mithilfe des Konfigurationsassistenten finden Sie in Linux: IBM Spectrum Protect mithilfe des Konfigurationsassistenten konfigurieren. Stellen Sie sicher, dass alle gemeinsam genutzten Verzeichnisse auf dem Primärknoten bereitgestellt werden.
6. Starten Sie die IBM Spectrum Protect-Serverinstanz auf dem Primärknoten mithilfe des Dienstprogramms DSMSERV. Beispielsweise wird mit dem folgenden Befehl der Server für den normalen Betrieb gestartet.

   ```
   /opt/tivoli/tsm/server/bin/dsmserv
   ```

7. Stellen Sie sicher, dass die IBM Spectrum Protect-Komponenten ohne Fehler gestartet werden.
8. Fahren Sie den IBM Spectrum Protect-Server herunter.
9. Heben Sie als Rootbenutzer die Bereitstellung der gemeinsam genutzten Laufwerke auf.

Linux-Betriebssysteme

Sekundärknoten konfigurieren

Nachdem Sie den Primärknoten konfiguriert haben, müssen Sie den Sekundärknoten konfigurieren, damit Tivoli System Automation die IBM Spectrum Protect-Serverkomponenten auf den Sekundärknoten versetzen kann, wenn der Server auf dem Primärknoten fehlschlägt.

Vorgehensweise

1. Um die Verzeichnisse und die Benutzer-ID für die Serverinstanz manuell zu erstellen, führen Sie die Anweisungen in Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen aus.
2. Stellen Sie sicher, dass der IBM Spectrum Protect-Server, die DB2-Instanz und die Verzeichnisse für die aktive Protokolldatei und das Archivprotokoll gemeinsam genutzt werden.
3. Definieren Sie die Mountpunkte, indem Sie in der Datei /etc/fstab Einträge hinzufügen.

   Wenn Sie auf den Clusterknoten Mountpunkte hinzufügen, verwenden Sie die Option noauto. Mit dieser Option wird verhindert, dass die Mountpunkte automatisch auf mehr als einem Knoten im Cluster bereitgestellt werden.

   Stellen Sie sicher, dass alle gemeinsam genutzten Verzeichnisse auf dem Sekundärknoten bereitgestellt werden.
4. Definieren Sie für jeden der Mountpunkte die folgenden Berechtigungen:
   - 755. Beispielsweise wird mit dem folgenden Befehl die Berechtigung 755 für den Mountpunkt `/tsminst1` definiert.

     ```
     chmod -R 755 /tsminst1
     ```

- IBM Spectrum Protect-Serverinstanzeigner. Beispielsweise werden mit dem folgenden Befehl die Berechtigungen für den Instanzeigner definiert.

  ```
  chown -R  tsminst1  /tsminst1
  ```

- IBM Spectrum Protect-Servergruppe, zu der der Instanzeigner gehört. Beispielsweise werden mit dem folgenden Befehl die Berechtigungen für die Gruppe des Instanzeigners definiert.

  ```
  chgrp tsmsrv_1_group /tsminst1
  ```

5. Erstellen Sie die IBM Spectrum Protect-Serverinstanz, indem Sie den Befehl db2icrt ausgeben. Anweisungen finden Sie in Serverinstanz erstellen.
   Hinweis: Sie müssen keine neue Serveroptionsdatei erstellen, da der Sekundärknoten die Datei dsmserv.opt des Primärknotens verwendet.
   Stellen Sie sicher, dass alle gemeinsam genutzten Verzeichnisse auf dem Sekundärknoten bereitgestellt werden.
6. Katalogisieren Sie die Datenbank, indem Sie den Befehl catalog db ausgeben. Beispielsweise wird mit dem folgenden Befehl die Datenbank `tsmdb1` katalogisiert.

   ```
   db2 catalog db tsmdb1
   ```

7. Bereiten Sie die Datenbank für die Sicherung vor. Anweisungen finden Sie in Datenbankmanager für die Datenbanksicherung vorbereiten.
8. Starten Sie den IBM Spectrum Protect-Server mithilfe des Dienstprogramms DSMSERV. Beispielsweise wird mit dem folgenden Befehl der Server für den normalen Betrieb gestartet.

   ```
   /opt/tivoli/tsm/server/bin/dsmserv
   ```

9. Stellen Sie sicher, dass die IBM Spectrum Protect-Komponenten ohne Fehler gestartet werden.
10. Fahren Sie auf dem Sekundärknoten den IBM Spectrum Protect-Server herunter und heben Sie die Bereitstellung der gemeinsam genutzten Verzeichnisse auf.

Linux-Betriebssysteme

Tivoli System Automation auf den Primär- und Sekundärknoten installieren

Nachdem Sie IBM Spectrum Protect auf den Primär- und Sekundärknoten im Cluster installiert und konfiguriert haben, müssen Sie Tivoli System Automation auf diesen Knoten installieren und konfigurieren. Anschließend müssen Sie diese Knoten für die Domäne aktivieren, die Ressourcen konfigurieren und die Basismaßnahme aktivieren. Abschließend müssen Sie den IBM Spectrum Protect-Verzeichnissen die Mountpunkte hinzufügen.

- Linux-BetriebssystemeKennsatz für die Mountpunkte erstellen
  Erstellen Sie für jeden Mountpunkt auf den Primär- und Sekundärknoten im Cluster einen Kennsatz.
- Linux-BetriebssystemeTivoli System Automation installieren und konfigurieren
  Sie müssen IBM Tivoli System Automation for Multiplatforms auf den Primär- und Sekundärknoten im System installieren.
- Linux-BetriebssystemeAktivierung der Clusterknoten für die Domäne vorbereiten
  Nachdem Sie Tivoli System Automation auf den Primär- und Sekundärknoten im Cluster installiert haben, müssen Sie diese Knoten vorbereiten, um den Cluster aktivieren und die Clusterdomäne starten zu können.
- Linux-BetriebssystemeDatenträgergruppenressourcen konfigurieren
  Wenn Sie Datenträgergruppen für Ihren Cluster erstellt haben, müssen Sie diese Ressourcen konfigurieren. Tivoli System Automation findet und definiert automatisch die Ressourcen für gemeinsam genutzte Plattendatenträger.
- Linux-BetriebssystemeRessourcen konfigurieren, die sich nicht in einer Datenträgergruppe befinden
  Wenn Sie Ihre Ressourcen *gemeinsam genutzter Plattenspeicher* unter Verwendung des Ressourcentyps ext2, ext3 oder reiserfs in einem der Knoten im Cluster erstellt haben, müssen Sie diese Ressourcen konfigurieren.
- Linux-BetriebssystemeBasismaßnahme aktivieren
  Nach dem Konfigurieren der Ressourcen müssen Sie die Maßnahme auf dem Primär- und Sekundärknoten aktivieren, um alle übrigen Ressourcen und die Ressourcengruppe zu erstellen.
- Linux-BetriebssystemeMountpunkte den IBM Spectrum Protect-Verzeichnissen hinzufügen
  Bevor Sie den Cluster starten können, müssen Sie die Mountpunkte hinzufügen, die für die IBM Spectrum Protect-Komponenten erstellt wurden.

Linux-Betriebssysteme

Kennsatz für die Mountpunkte erstellen

Erstellen Sie für jeden Mountpunkt auf den Primär- und Sekundärknoten im Cluster einen Kennsatz.

Vorgehensweise

1. Erstellen Sie für jeden der Datenträger, die Sie zuvor für die Mountpunkte für gemeinsam genutztes Verzeichnis erstellt haben, einen Kennsatz, indem Sie den Befehl e2label ausgeben. Beispielsweise wird mit dem folgenden Befehl der Kennsatz /tsminst1 erstellt, der über eine Partition /dev/tsmvg1/tsminst1LV verfügt.

```
e2label /dev/tsmvg1/tsminst1LV /tsminst1
```

2. Ersetzen Sie für jeden Knoten im Cluster die Einträge für die Mountpunkte, die Sie zuvor in der Datei /etc/fstab erstellt haben. Geben Sie beispielsweise für den vorherigen Beispielkennsatz den folgenden Befehl aus:

```
LABEL=/tsminst1 /tsminst1 ext3 defaults 0 0
```

Linux-Betriebssysteme

Tivoli System Automation installieren und konfigurieren

Sie müssen IBM® Tivoli System Automation for Multiplatforms auf den Primär- und Sekundärknoten im System installieren.

Vorgehensweise

1. Ausführliche Informationen zum Installieren und Konfigurieren von Tivoli System Automation finden Sie in der Veröffentlichung Tivoli System Automation Installation and Configuration Guide.
2. Laden Sie die Datei TSM-25072011-1015.zip über Integrated Service Management Library herunter. Extrahieren Sie die komprimierte Datei auf jedem Clusterknoten.
3. Überprüfen Sie nach dem Extrahieren der komprimierten Datei, ob das neue Tivoli System Automation-Verzeichnis, das während der Installation erstellt wurde, das Verzeichnis /TSM/HA und die zugehörigen Unterverzeichnisse umfasst.

Zugehörige Informationen:
Produktinformation zu IBM Tivoli System Automation for Multiplatforms Version 3.2.2
Linux-Betriebssysteme

Aktivierung der Clusterknoten für die Domäne vorbereiten

Nachdem Sie Tivoli System Automation auf den Primär- und Sekundärknoten im Cluster installiert haben, müssen Sie diese Knoten vorbereiten, um den Cluster aktivieren und die Clusterdomäne starten zu können.

Vorgehensweise

1. Bereiten Sie jeden Knoten für die Domäne vor, indem Sie den Befehl preprpnode ausgeben. Geben Sie diesen Befehl für alle Clusterknoten in der Domäne aus. Beispielsweise werden mit dem folgenden Befehl die Knoten HOST1.ibm.com und HOST2.ibm.com vorbereitet.

```
preprpnode HOST1.ibm.com HOST2.ibm.com
```

2. Erstellen Sie für jeden Knoten eine Domäne, indem Sie den Befehl mkrpdomain ausgeben. Beispielsweise wird mit dem folgenden Befehl die Domäne tsm_domain für die Knoten HOST1.ibm.com und HOST2.ibm.com erstellt.

```
mkrpdomain tsm_domain HOST1.ibm.com HOST2.ibm.com
```

3. Starten Sie die Domäne für jeden Knoten, indem Sie den Befehl startrpdomain ausgeben. Beispielsweise wird mit dem folgenden Befehl die Domäne tsm_domain gestartet.

```
startrpdomain tsm_domain
```

Linux-Betriebssysteme

Datenträgergruppenressourcen konfigurieren

Wenn Sie Datenträgergruppen für Ihren Cluster erstellt haben, müssen Sie diese Ressourcen konfigurieren. Tivoli System Automation findet und definiert automatisch die Ressourcen für gemeinsam genutzte Plattendatenträger.

Vorgehensweise

Um die Datenträgergruppenressourcen für die gemeinsam genutzten IBM Spectrum Protect-Verzeichnisse und -Mountpunkte, die Sie zuvor erstellt haben, zu konfigurieren, führen Sie die folgenden Schritte auf dem Primärknoten aus:

1. Importieren Sie die Datenträgergruppen. Verwenden Sie beispielsweise den Befehl vgimport X, um die X-Datenträgergruppen zu importieren.
2. Aktivieren Sie die Datenträgergruppen. Verwenden Sie beispielsweise den Befehl vgchange -ay X, um die X-Datenträgergruppen zu aktivieren.
3. Hängen Sie das Dateisystem an, indem Sie den Befehl mount ausgeben. In dem folgenden Beispiel wird das Dateisystem X angehängt.

```
mount X
```

4. Starten Sie die Domäne erneut, indem Sie die Befehle stoprpdomain und startrpdomain ausgeben. Beispielsweise wird mit den folgenden Befehlen die Domäne tsm_domain erneut gestartet.

```
stoprpdomain tsm_domain
startrpdomain tsm_domain
```

5. Hängen Sie das Dateisystem ab, indem Sie den Befehl umount ausgeben. Verwenden Sie beispielsweise den Befehl umount X, um das Dateisystem `X` abzuhängen.
6. Inaktivieren Sie die Datenträgergruppen. Verwenden Sie beispielsweise den Befehl vgchange -an X, um die `X`-Datenträgergruppen zu inaktivieren.
7. Überprüfen Sie, ob alle der IBM®.AgfileSystem-Speicherressourcen von Tivoli System Automation übernommen wurden, indem Sie den folgenden Befehl ausgeben:

```
lsrsrc –s “Name==’Ressourcenname' && ResourceType=1” IBM.AgFileSystem
```

Ressourcen konfigurieren, die sich nicht in einer Datenträgergruppe befinden

Wenn Sie Ihre Ressourcen *gemeinsam genutzter Plattenspeicher* unter Verwendung des Ressourcentyps ext2, ext3 oder reiserfs in einem der Knoten im Cluster erstellt haben, müssen Sie diese Ressourcen konfigurieren.

Vorgehensweise

Führen Sie auf dem Primärknoten die folgenden Schritte aus:

1. Hängen Sie das Dateisystem an, indem Sie den Befehl mount ausgeben. Beispielsweise wird mit dem folgenden Befehl das Dateisystem `X` angehängt.

   ```
   mount X
   ```

2. Starten Sie die Domäne erneut, indem Sie die Befehle stoprpdomain und startrpdomain ausgeben. Beispielsweise wird mit den folgenden Befehlen die Domäne tsm_domain erneut gestartet.

   ```
   stoprpdomain tsm_domain
   startrpdomain tsm_domain
   ```

3. Hängen Sie das Dateisystem ab, indem Sie den Befehl umount ausgeben. Beispielsweise wird mit dem folgenden Befehl das Dateisystem `X` abgehängt.

   ```
   umount X
   ```

4. Überprüfen Sie, ob alle der IBM®.AgfileSystem-Speicherressourcen von Tivoli System Automation übernommen wurden, indem Sie den folgenden Befehl ausgeben:

   ```
   lsrsc -s “Name==’Ressourcenname' && ResourceType=1” IBM.AgFileSystem
   ```

   Um beispielsweise die Ressource *tsmalog* zu prüfen, geben Sie den folgenden Befehl aus:

   ```
   lsrsrc -s "Name=='tsmalog' && ResourceType=1" IBM.AgFileSystem
         Resource Persistent Attributes for IBM.AgFileSystem resource 1:
         ResourceHandle= "0x2038 0xffff 0x6ad47197 0x256fc23d 0x9338a9950x263fa510"
         Name                = "tsmalog"
         ResourceType        = 1   <------------------------------
         MountPoint          = ""
         DeviceName          = ""
         Vfs                 = "ext3"
         AggregateResource   = "0x3fff 0xffff 0x00000000 0x00000000 0x00000000 0x00000000"
         ContainerResource   = "0x2036 0xffff 0x6ad47197 0x256fc23d 0x9338a995 0x25ffaa28"
         GhostDevice         = 0
         ResourceId          = "360050768019c021d30000000000005da"
         ProtectionMode      = 1
         UserControl         = 0
         SysMountPoint       = "/tsmalog"
         Label               = "/tsmalog"
         FSID                = "5792f887-8547-4c33-a519-9d0c50ab6882"
         PreOnlineMethod     = 0
         ContainerResourceId = "360050768019c021d30000000000005da"
         AutoMonitor         = 1
         Options             = "defaults,noauto"
         PreOfflineMethod    = 0
         ActivePeerDomain    = "TSM-Domäne"
         NodeNameList        = {"tsmlnode01.storage.tucson.ibm.com","tsmlnode02.storage.tucson.ibm.com"}
   ```

Basismaßnahme aktivieren

Nach dem Konfigurieren der Ressourcen müssen Sie die Maßnahme auf dem Primär- und Sekundärknoten aktivieren, um alle übrigen Ressourcen und die Ressourcengruppe zu erstellen.

Informationen zu diesem Vorgang

Um die Basismaßnahme zu aktivieren, müssen Sie die Service-IP-Ressource und IBM Spectrum Protect-Anwendungsressourcen für die IBM Spectrum Protect-Serverinstanz erstellen. Anschließend müssen Sie die Ressourcengruppe und die Maßnahmen zum Verwalten des Clusters erstellen.

Vorgehensweise

Führen Sie die folgenden Schritte zunächst auf dem Primärknoten und dann auf dem Sekundärknoten aus.

1. Wechseln Sie in das Verzeichnis, in das der Inhalt der Datei TSM-25072011-1015.zip extrahiert wurde.
2. Definieren Sie die Dateiberechtigungen für die Scripts im Verzeichnis bin, indem Sie den Befehl chmod ausgeben. Beispielsweise werden mit dem folgenden Befehl die Dateiberechtigungen für alle Scripts im Verzeichnis bin definiert. XXX ist der Name des extrahierten Ordners.

   ```
   chmod 755 /XXX/TSM/HA/bin/*
   ```

3. Wechseln Sie in das Verzeichnis bin, indem Sie den Befehl cd ausgeben.
4. Aktualisieren Sie die folgenden Variablen im Script base_cluster_variables.sh:
   - *NODE1* gibt den Hostnamen für Knoten 1 (Primärknoten) im Cluster an.
   - *NODE2* gibt den Hostnamen für Knoten 2 (Sekundärknoten) im Cluster an.
   - *IP_GATEWAY* gibt das Gateway des Service-IP an.
   - *SUBNET_MASK* gibt die Teilnetzmaske des Service-IP an.
   - *NET_INT* gibt den Namen der Netzschnittstelle eines bestimmten Knotens im Cluster an. Dieser Name muss für alle Knoten im Cluster identisch sein.
5. Führen Sie das Konfigurationsscript configureHA.sh aus, indem Sie den Befehl ./configureHA.sh auf allen Knoten im Cluster ausgeben. Wenn das Script configureHA.sh mit dem Fehler `-bash: ./configureHA.sh: /bin/bash^M: bad interpreter: No such file or directory` fehlschlägt, geben Sie den Befehl dos2unix für alle Scripts im Verzeichnis bin aus. Führen Sie beispielsweise für jedes Script den folgenden Befehl aus:

   ```
   dos2unix -o <Dateiname>
   ```

6. Überprüfen Sie, ob die Konfiguration erfolgreich ausgeführt wird, indem Sie überprüfen, ob das Konfigurationsscript erfolgreich ausgeführt wird.
7. Achtung: Führen Sie diesen Schritt nur auf dem Primärknoten aus!
   Führen Sie das Setup-Script aus, indem Sie den Befehl ./setup.sh ausgeben. Beispielsweise wird mit dem folgenden Befehl das Setup-Script für die IBM Spectrum Protect-Serverinstanz `inst1` für den Instanzbenutzer `dbinst1` im IBM Spectrum Protect-Serverinstanzverzeichnis `/tsminst1` mit `9.11.142.129` als Service-IP ausgeführt.

   ```
   ./setup.sh inst1 dbinst1 /tsminst1 9.11.142.129
   ```

8. Überprüfen Sie, ob das korrekte IP (Internet Protocol) verwendet wird, indem Sie den folgenden Befehl ausführen:

   ```
   lssam -V
   ```

9. Wiederholen Sie Schritt 5 für alle IBM Spectrum Protect-Instanzen in Ihrer IBM Spectrum Protect-Serverumgebung.
10. Führen Sie alle vorhergehenden Schritte auf dem Sekundärknoten aus.

Linux-Betriebssysteme

Mountpunkte den IBM Spectrum Protect-Verzeichnissen hinzufügen

Bevor Sie den Cluster starten können, müssen Sie die Mountpunkte hinzufügen, die für die IBM Spectrum Protect-Komponenten erstellt wurden.

Vorgehensweise

Um der Clusterressourcengruppe die Mountpunkte für gemeinsam genutzte Platten hinzuzufügen und den Cluster online zu schalten, führen Sie die folgenden Schritte aus:

1. Geben Sie Mountpunkte für die folgenden Verzeichnisse an:
   - Instanz
   - Datenbank
   - Aktive Protokolldatei
   - Archivprotokoll
   - Speicherpool
2. Fügen Sie jedem Mountpunkt Ressourcen hinzu:
   a. Überprüfen Sie, ob die Ressourcengruppe tsm-$INST_NAME-rg online ist, indem Sie den Befehl lssam ausgeben.
   b. Wenn die Ressourcengruppe tsm-$INST_NAME-rg online ist, schalten Sie sie offline, indem Sie den folgenden Befehl ausgeben:

```
chrg -o offline tsm-$INST_NAME-rg
```

c. Wechseln Sie in das Verzeichnis, in das der Inhalt der Datei TSM-25072011-1015.zip extrahiert wurde.
d. Wechseln Sie in das Verzeichnis 'bin', indem Sie den Befehl cd ausgeben.
e. Um jedem Mountpunkt gemeinsam genutzte Plattenressourcen hinzuzufügen, führen Sie das Script ./update_setup.sh aus. Beispielsweise wird mit dem folgenden Befehl der Mountpunkt `/tsminst1` der IBM Spectrum Protect-Serverinstanz `inst1` hinzugefügt.

```
./update_setup.sh inst1 /tsminst1
```

3. Schalten Sie die Ressourcengruppe tsm-$INST_NAME-rg online, indem Sie den folgenden Befehl ausgeben:

```
chrg -o online tsm-$INST_NAME-rg
```

4. Stellen Sie unter Verwendung des Service-Gateway-IP die Verbindung zum Server her, um zu überprüfen, ob die Konfiguration korrekt ist.

Linux-Betriebssysteme

Speicherressourcen konfigurieren

Verwenden Sie die Tivoli System Automation-Benutzerschnittstelle, oder -Befehlszeile, um Speicherressourcen hinzuzufügen oder zu löschen und um Mountpunkte, die nicht mehr benötigt werden, zu löschen. Wenn Sie dem Cluster einen Speicherpool hinzufügen, müssen Sie den Speicherpool der Ressourcengruppe hinzufügen. Wenn Sie einen Speicherpool aus dem Cluster entfernen, müssen Sie den Speicherpool auch aus der Ressourcengruppe löschen.

- Linux-BetriebssystemeSpeicherpool einer Ressourcengruppe hinzufügen
  Wenn bei Ihrer IBM Spectrum Protect-Konfiguration Daten auf Platten gespeichert werden, müssen Sie der Ressourcengruppe den Mountpunkt für gemeinsam genutzte Platten für den Speicherpool hinzufügen.
- Linux-BetriebssystemeSpeicherpool aus einer Ressourcengruppe löschen
  Sie können einen Speicherpool, der nicht mehr erforderlich ist, löschen. Wenn ein Speicherpool aus der IBM Spectrum Protect-Serverinstanz entfernt wird, muss er aus der Ressourcengruppe gelöscht werden.
- Linux-BetriebssystemeMountpunkt aus einer Ressourcengruppe löschen
  Sie können einen Mountpunkt, der nicht mehr erforderlich ist, bei Bedarf löschen.

Linux-Betriebssysteme

Speicherpool einer Ressourcengruppe hinzufügen

Wenn bei Ihrer IBM Spectrum Protect-Konfiguration Daten auf Platten gespeichert werden, müssen Sie der Ressourcengruppe den Mountpunkt für gemeinsam genutzte Platten für den Speicherpool hinzufügen.

Vorgehensweise

Um der Ressourcengruppe den Mountpunkt für gemeinsam genutzte Platten für den Speicherpool hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Sperren Sie die Ressourcengruppe, indem Sie den Befehl rgreq -o lock ausgeben. Beispielsweise wird mit dem folgenden Befehl die Ressourcengruppe `Beispielressourcengruppe_X` gesperrt.

```
rgreq -o lock Beispielressourcengruppe_X
```

2. Wechseln Sie in das Verzeichnis 'bin', indem Sie den Befehl cd ausgeben:
3. Um einer Ressourcengruppe eine Speicherpoolressource hinzuzufügen, führen Sie das Script update_setup.sh aus, indem Sie den Befehl ./update_setup.sh ausgeben. Beispielsweise wird mit dem folgenden Befehl der Speicherpoolmountpunkt `/inst1stg1` der IBM Spectrum Protect-Serverinstanz `inst1` hinzugefügt.

```
./update_setup.sh inst1 /inst1stg1
```

4. Entsperren Sie die Ressourcengruppe, indem Sie den Befehl rgreq -o unlock ausgeben. Beispielsweise wird mit dem folgenden Befehl die Ressourcengruppe `Beispielressourcengruppe_X` entsperrt.

```
rgreq -o unlock Beispielressourcengruppe_X
```

Linux-Betriebssysteme

Speicherpool aus einer Ressourcengruppe löschen

Sie können einen Speicherpool, der nicht mehr erforderlich ist, löschen. Wenn ein Speicherpool aus der IBM Spectrum Protect-Serverinstanz entfernt wird, muss er aus der Ressourcengruppe gelöscht werden.

Vorgehensweise

Um einen Speicherpool zu löschen, führen Sie die folgenden Schritte aus:

1. Sperren Sie die Ressourcengruppe, indem Sie den Befehl rgreq -o lock ausgeben. Beispielsweise wird mit dem folgenden Befehl die Ressourcengruppe `Beispielressourcengruppe_X` gesperrt.

   ```
   rgreq -o lock Beispielressourcengruppe_X
   ```

2. Wechseln Sie in das Verzeichnis bin, indem Sie den Befehl cd ausgeben.
3. Um eine Speicherpoolressource aus einer Ressourcengruppe zu löschen, führen Sie das Script delete_mount.sh aus, indem Sie den Befehl ./delete_mount.sh ausgeben. Beispielsweise wird mit dem folgenden Befehl der Mountpunkt `/inst1stg1` aus der IBM Spectrum Protect-Serverinstanz `inst1` gelöscht.

   ```
   ./delete_mount.sh /inst1stg1 inst1
   ```

4. Entsperren Sie die Ressourcengruppe, indem Sie den Befehl rgreq -o unlock ausgeben. Beispielsweise wird mit dem folgenden Befehl die Ressourcengruppe `Beispielressourcengruppe_X` entsperrt.

   ```
   rgreq -o unlock Beispielressourcengruppe_X
   ```

 Linux-Betriebssysteme

Mountpunkt aus einer Ressourcengruppe löschen

Sie können einen Mountpunkt, der nicht mehr erforderlich ist, bei Bedarf löschen.

Vorgehensweise

Um einen Mountpunkt zu löschen, führen Sie die folgenden Schritte aus:

1. Überprüfen Sie, ob die Ressourcengruppe tsm-$INST_NAME-rg online ist, indem Sie den Befehl lssam ausgeben.
2. Wenn die Ressourcengruppe tsm-$INST_NAME-rg online ist, schalten Sie die offline, indem Sie den folgenden Befehl ausgeben:

   ```
   chrg -o offline tsm-$INST_NAME-rg
   ```

3. Wechseln Sie in das Verzeichnis bin, indem Sie den Befehl cd ausgeben.
4. Um einen Mountpunkt zu löschen, führen Sie das Script delete_mount.sh aus. Beispielsweise wird mit dem folgenden Befehl der Mountpunkt `/tsminst1` aus der Ressourcengruppe der IBM Spectrum Protect-Serverinstanz `inst1` gelöscht.

   ```
   ./delete_mount.sh /tsminst1 inst1
   ```

5. Schalten Sie die Ressourcengruppe tsm-$INST_NAME-rg online, indem Sie den folgenden Befehl ausgeben:

   ```
   chrg -o online tsm-$INST_NAME-rg
   ```

 Linux-Betriebssysteme

Upgrade für einen Server durchführen, der mit Tivoli System Automation konfiguriert ist

Sie können ein Upgrade für einen Server der Version 6.3 oder Version 7.1 durchführen, der mit Tivoli System Automation konfiguriert ist.

Vorgehensweise

Um für den Server ein Upgrade auf jedem Knoten in dem Cluster durchzuführen, melden Sie sich bei dem Server an und führen Sie die folgenden Schritte aus. Mit diesen Schritten wird das Upgrade auf dem Primärknoten gestartet; später in dieser Prozedur wird dann das Upgrade für den Sekundärknoten durchgeführt.

1. Stoppen Sie die Serverressourcen, indem Sie den Befehl chrg -o Offline ausgeben. Beispielsweise werden mit dem folgenden Befehl die Ressourcen in der Ressourcengruppe tsm-tsminst1-rg gestoppt:

   ```
   chrg -o Offline tsm-tsminst1-rg
   ```

2. Stoppen Sie die Tivoli System Automation-Domäne, indem Sie den Befehl stoprpdomain ausgeben. Beispielsweise wird mit dem folgenden Befehl die Domäne tsm_domain gestoppt:

   ```
   stoprpdomain tsm_domain
   ```

3. Stellen Sie die Server-Mountpunkte auf dem Primärknoten bereit.
4. Informationen zur Durchführung eines Upgrades für den Server auf dem Primärknoten finden Sie in Upgrade für IBM Spectrum Protect durchführen.
5. Nachdem die Durchführung des Upgrades abgeschlossen ist, führen Sie die Schritte nach dem Upgrade aus, um sicherzustellen, dass das Upgrade auf dem Primärknoten erfolgreich durchgeführt wurde.

6. Stoppen Sie den Server und heben Sie die Bereitstellung der Server-Mountpunkte auf dem Primärknoten auf.
7. Stellen Sie die Server-Mountpunkte auf dem Sekundärknoten bereit.
8. Wenn Sie für einen Server ein Upgrade von Version 6 auf Version 7 durchführen, führen Sie die folgenden Schritte aus:
    a. Deinstallieren Sie den Server.

        Anweisungen finden Sie in Server der Version 6.2 deinstallieren.

    b. Installieren Sie den Server auf dem Sekundärknoten. Führen Sie die Anweisungen in Linux: Serverkomponenten installieren aus.
9. Informationen zur Durchführung eines Upgrades für den Server auf dem Sekundärknoten finden Sie in Upgrade für den Server durchführen.
10. Nachdem die Durchführung des Upgrades abgeschlossen ist, führen Sie die Schritte nach dem Upgrade aus, um sicherzustellen, dass das Upgrade auf dem Sekundärknoten erfolgreich durchgeführt wurde.
11. Heben Sie die Bereitstellung der Server-Mountpunkte auf dem Sekundärknoten auf.
12. Starten Sie die Tivoli System Automation-Domäne, indem Sie den Befehl startrpdomain ausgeben. Beispielsweise wird mit dem folgenden Befehl die Domäne tsa_domain gestartet:

    ```
    startrpdomain tsa_domain
    ```

13. Starten Sie die Serverressourcen, indem Sie den Befehl chrg -o Online ausgeben. Beispielsweise werden mit dem folgenden Befehl die Ressourcen in der Ressourcengruppe tsm-tsminst1-rg gestartet:

    ```
    chrg -o Online tsm-tsminst1-rg
    ```

Windows-Betriebssysteme

Windows-Clusterumgebung konfigurieren

Sie können einen IBM Spectrum Protect-Server für Windows in einer Microsoft-Failoverclusterumgebung konfigurieren. Windows-Clusterumgebungen bestehen aus Komponenten, wie beispielsweise IBM Spectrum Protect-Servern, Hardware und Software. Wenn diese Komponenten mit demselben Plattensystem verbunden sind, wird die Ausfallzeit auf ein Mindestmaß reduziert.

Microsoft-Software hilft beim Konfigurieren, Überwachen und Steuern von Anwendungen und Hardwarekomponenten, die in einem Windows-Cluster implementiert sind. Der Administrator verwendet die Microsoft-Cluster-Administratorschnittstelle und IBM Spectrum Protect, um Cluster-Aufteilungen zu kennzeichnen und um das Übernahmemuster zu definieren.

IBM Spectrum Protect unterstützt die Bandübernahme für eine Clusterumgebung unter Verwendung einer Fibre Channel- oder SCSI-Verbindung. Obwohl Microsoft-Failovercluster nicht die Übernahme von Bandeinheiten unterstützen, kann die Übernahmekonfiguration durch die Microsoft Cluster Administrator-Schnittstelle überwacht werden, nachdem sie über IBM Spectrum Protect konfiguriert wurde.

- Windows-BetriebssystemeÜbersicht über die Microsoft-Failoverclusterumgebung
  Mit einem Microsoft Failovercluster-Manager können Sie IBM Spectrum Protect-Server-Cluster-Ressourcen in eine Clustergruppe stellen. Die IBM Spectrum Protect-Clustergruppe verfügt über einen Netznamen, eine IP-Adresse, eine oder mehrere physische Platten, einen DB2-Server und einen IBM Spectrum Protect-Server-Service.
- Windows-BetriebssystemeBandübernahme für Knoten in einem Cluster
  Gruppen in einem Cluster können auf andere Knoten übertragen werden, wenn der Knoten, auf dem sich die Gruppen befinden, fehlschlägt.
- Windows-BetriebssystemePlanung für eine Clusterumgebung
  Die Konfiguration in einer Clusterumgebung bedarf einer sorgfältigen Planung, um die optimale Leistung Ihres Systems gewährleisten zu können. Ob Sie Ihr System für Cluster konfigurieren, hängt von Ihren Geschäftsanforderungen ab.
- Windows-BetriebssystemeIBM Spectrum Protect in einem Microsoft Failovercluster konfigurieren
  Sie müssen sicherstellen, dass Ihr Cluster korrekt installiert und konfiguriert ist, bevor Sie IBM Spectrum Protect installieren.
- Windows-BetriebssystemeClusterumgebung verwalten
  Nach der Konfiguration Ihres ersten Clusters oder Ihrer ersten Cluster ist der Verwaltungsaufwand minimal.

Windows-Betriebssysteme

Übersicht über die Microsoft-Failoverclusterumgebung

Mit einem Microsoft Failovercluster-Manager können Sie IBM Spectrum Protect-Server-Cluster-Ressourcen in eine Clustergruppe stellen. Die IBM Spectrum Protect-Clustergruppe verfügt über einen Netznamen, eine IP-Adresse, eine oder mehrere physische Platten, einen DB2-Server und einen IBM Spectrum Protect-Server-Service.

Der Netzname der IBM Spectrum Protect-Instanz ist unabhängig vom Namen des physischen Knotens, auf dem die IBM Spectrum Protect-Clustergruppe ausgeführt wird. Clients stellen die Verbindung zu einem IBM Spectrum Protect-Server nicht unter Verwendung des Windows-Knotennamens, sondern unter Verwendung des Netznamens der Instanz her. Der Netzname der Instanz ist einem Primär- oder Ausweichknoten zugeordnet. Die Zuordnung ist davon abhängig, welcher Knoten Eigner der Clustergruppe ist. Jeder Client, der Windows Internet Name Service (WINS) oder Verzeichnisservices zum Lokalisieren von Servern verwendet, kann den IBM Spectrum Protect-Cluster-Server automatisch verfolgen, wenn er zwischen den Knoten versetzt wird. Sie können den Cluster-Server automatisch verfolgen, ohne den Client ändern oder rekonfigurieren zu müssen.

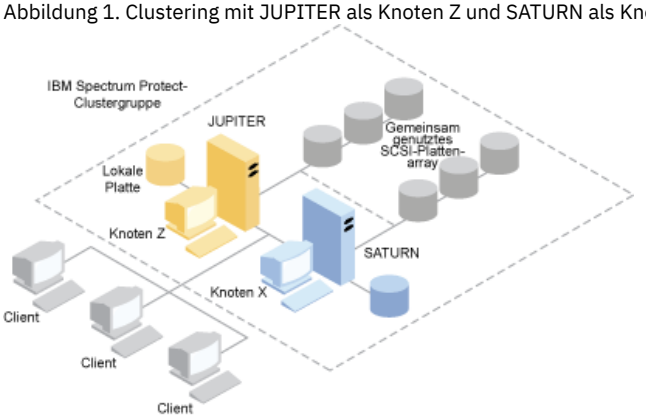
Jede IBM Spectrum Protect-Clustergruppe verfügt über ihre eigene Platte als Teil einer Clusterressourcengruppe. IBM Spectrum Protect-Clustergruppen können keine Daten zwischen Clustergruppen gemeinsam nutzen. Die Datenbank, die aktiven Protokolldateien und die Wiederherstellungsprotokolle sowie die Gruppe von Speicherpooldatenträgern sind für jeden IBM Spectrum Protect-Server, der in einer Clustergruppe konfiguriert ist, auf einer separaten Platte gespeichert. Die Clustergruppe, in der der Server konfiguriert ist, ist Eigner dieser Platte.

Hinweis: Microsoft Failovercluster-Manager unterstützt als Ressource nur eine IP-Adresse. Demzufolge muss jeder IBM Spectrum Protect-Server, der in einem Cluster ausgeführt wird, sein unterstütztes Kommunikationsverfahren ausschließlich auf TCP/IP beschränken. Jeder Client, der nicht TCP/IP als Kommunikationsverfahren verwendet, kann die IBM Spectrum Protect-Clustergruppe nicht erreichen, wenn eine Übernahme (Failover) durch den anderen Clusterknoten erfolgt.

Das folgende Beispiel zeigt, wie ein Microsoft Failovercluster-Manager für einen IBM Spectrum Protect-Cluster-Server funktioniert.

Angenommen, ein IBM Spectrum Protect-Cluster-Server mit dem Namen JUPITER wird auf dem Knoten Z ausgeführt und ein IBM Spectrum Protect-Cluster-Server mit dem Namen SATURN wird auf dem Knoten X ausgeführt. Clients stellen eine Verbindung zum IBM Spectrum Protect-Server JUPITER und zum IBM Spectrum Protect-Server SATURN her, ohne zu wissen, auf welchem Knoten sich ihr Server befindet.

Abbildung 1. Clustering mit JUPITER als Knoten Z und SATURN als Knoten X



Wenn in einer der Software- oder Hardwareressourcen ein Fehler auftritt, erfolgt eine Übernahme. Ressourcen, wie beispielsweise Anwendungen, Platten und eine IP-Adresse, werden von dem fehlerhaften Knoten in den verbleibenden Knoten versetzt. Der verbleibende Knoten führt Folgendes aus:

- Er übernimmt die IBM Spectrum Protect-Clustergruppe.
- Er schaltet die Plattenressourcen, die Netzressourcen und die DB2-Ressourcen online.
- Er startet den IBM Spectrum Protect-Service erneut.
- Er stellt Zugriff auf Administratoren und Clients bereit.

Wenn Knoten X ausfällt, übernimmt Knoten Z die Ausführung von SATURN. Für einen Client erscheint dies exakt so, als würde Knoten X ausgeschaltet und sofort wieder eingeschaltet. Clients verlieren alle Verbindungen zu SATURN, und alle aktiven Transaktionen werden rückgängig gemacht. Clients müssen die Verbindung zu SATURN wiederherstellen, nachdem die Verbindung verloren gegangen ist. Der Standort von SATURN ist für den Client nicht ersichtlich.

Windows-Betriebssysteme

Bandübernahme für Knoten in einem Cluster

Gruppen in einem Cluster können auf andere Knoten übertragen werden, wenn der Knoten, auf dem sich die Gruppen befinden, fehlschlägt.

Ein Knoten kann als Host für physische oder logische Einheiten, die als Ressourcen bezeichnet werden, dienen. Administratoren fassen diese Clusterressourcen in Funktionseinheiten zusammen, die als Gruppen bezeichnet werden, und ordnen diese Gruppen einzelnen Knoten zu. Wenn ein Knoten ausfällt, überträgt der Server-Cluster die vom Knoten gehosteten Gruppen auf andere Knoten im Cluster. Dieser Übertragungsprozess wird als *Übernahme* (Failover) bezeichnet. Der gegenteilige Prozess, *Rückübertragung* (Failback), findet statt, wenn der ausgefallene Knoten wieder aktiv wird und die Gruppen, die auf die anderen Knoten übertragen wurden, wieder auf den ursprünglichen Knoten zurückübertragen werden.

- Windows-BetriebssystemeFibre Channel-Bandübernahme
  IBM Spectrum Protect kann die Übernahme von direkt angeschlossenen Fibre Channel-Bandeinheiten und -Speicherarchiveinheiten auf einem Microsoft Windows-System in einer Clusterumgebung ohne zusätzliche Hardware handhaben.

Windows-Betriebssysteme

Planung für eine Clusterumgebung

Die Konfiguration in einer Clusterumgebung bedarf einer sorgfältigen Planung, um die optimale Leistung Ihres Systems gewährleisten zu können. Ob Sie Ihr System für Cluster konfigurieren, hängt von Ihren Geschäftsanforderungen ab.

Die Planung für eine Clusterkonfiguration muss gemäß Ihrer Umgebung erfolgen. Sie müssen sicherstellen, dass der korrekte Hardwaretyp und die geeignete Software verwendet werden. Darüber hinaus müssen Sie ein Übernahmemuster konfigurieren.

Wenn ein Knoten ausfällt oder offline geschaltet werden muss, welcher Knoten bzw. welche Knoten im Cluster übernimmt/übernehmen dann die Transaktionsverarbeitung? Bei einem Cluster mit zwei Knoten ist nur wenig Planung erforderlich. Bei einer komplexeren Anordnung sollten Sie darauf achten, wie Ihre Transaktionsverarbeitung am besten ausgeführt wird. Es muss eine Form des Lastausgleichs zwischen den Knoten vorliegen, damit die Spitzenleistung aufrecht erhalten wird. Es muss auch sichergestellt werden, dass Ihre Kunden keine Verzögerung und nur wenig Abfall der Produktivität wahrnehmen.

Für Microsoft Cluster Server und Microsoft Failovercluster benötigt jede IBM Spectrum Protect-Serverinstanz eine private Plattenressourcengruppe. Knoten können Plattenressourcen zwar gemeinsam nutzen, aber nur jeweils ein Knoten kann eine Platte aktiv steuern.

Achtung: Stellen Sie sicher, dass auf allen Computern im Cluster dieselbe Version von Windows (Windows 2012, Windows 2012 R2 und Windows 2016) installiert ist.

Ist eine Konfiguration besser als die andere? Um die optimale Installation zu ermitteln, müssen Sie einen Leistungs- und Kostenvergleich durchführen. Angenommen, es ist ein Cluster vorhanden, der dem IBM Spectrum Protect-Server zugeordnet ist und über Knoten mit vergleichbarer Leistung verfügt. Während der Übernahme kann die Leistung einer Konfiguration abnehmen, weil ein einziger Knoten beide IBM Spectrum Protect-Clusterinstanzen handhaben muss. Wenn jeder Knoten im Normalbetrieb 100 Clients bearbeitet, muss ein Knoten während eines Fehlers 200 Clients handhaben.

- Windows-BetriebssystemeArbeitsblatt für die Clusterkonfiguration
  Notieren Sie Ihre Antworten auf die folgenden Planungsfragen, bevor Sie die Clusterkonfiguration definieren.
- Windows-BetriebssystemeCluster-Hardware- und -Softwarekonfiguration planen
  Die Cluster-Hardware- und -Softwarekonfiguration wird während des Planungsstadiums und vor der eigentlichen Installation bestimmt.
- Windows-BetriebssystemeIBM Spectrum Protect im Microsoft Failovercluster konfigurieren
  Die IBM Spectrum Protect-Clusterkonfigurationsprozedur muss für die Gruppe von Knoten ausgeführt werden, die eine IBM Spectrum Protect-Clustergruppe hostet.

Zugehörige Informationen:
IBM Spectrum Protect Supported Operating Systems
Windows-Betriebssysteme

Arbeitsblatt für die Clusterkonfiguration

Notieren Sie Ihre Antworten auf die folgenden Planungsfragen, bevor Sie die Clusterkonfiguration definieren.

1. Welche Clusterlösung ist für Ihre Geschäftsanforderungen am besten geeignet?
2. Welchen Typ von Übernahmemuster benötigen Sie?

   Auch die Verwendung der Bandübernahmeunterstützung wirkt sich auf das Muster aus.

3. Wird Bandübernahmeunterstützung benötigt?

   Berücksichtigen Sie, wie Bandeinheiten von den IBM Spectrum Protect-Clusterinstanzen verwendet werden. Durch die Art und Weise, auf die Bandeinheiten von Clusterinstanzen verwendet werden, kann die Anzahl der Knoten im Übernahmemuster auf zwei begrenzt werden.

4. Welche Ressourcen sollen für IBM Spectrum Protect dediziert werden?

Ressourcentyp	Ressourcenname
Clusterressourcengruppe	
Ressourcen der physischen Platte	
IP-Adresse	
Teilnetzmaske	
Netz	
Netzname (Servername)	
Knoten	
Bandübernahme (optional): Einheitenname - beide Knoten	

Windows-Betriebssysteme

Cluster-Hardware- und -Softwarekonfiguration planen

Die Cluster-Hardware- und -Softwarekonfiguration wird während des Planungsstadiums und vor der eigentlichen Installation bestimmt.

Vorgehensweise

Anhand der folgenden Richtlinien kann bestimmt werden, welche Ressourcen für einen erfolgreichen IBM Spectrum Protect-Cluster benötigt werden:

1. Legen Sie die erforderliche Clusterkonfiguration für Server fest, die Platteneinheiten verwenden. Jede IBM Spectrum Protect-Clusterinstanz benötigt eine separate Gruppe von Plattenressourcen auf dem gemeinsamen Plattensubsystem. Unter Umständen können Probleme auftreten, wenn Sie das E/A-Subsystem als einen einzigen großen Bereich konfigurieren. Dies ist beispielsweise der Fall, wenn Sie einen Cluster mit zwei Servern konfigurieren und sich später für eine Erweiterung auf einen Cluster mit vier Servern entscheiden.
2. Identifizieren Sie die Datenträgerressourcen, die IBM Spectrum Protect zugeteilt werden sollen. Teilen Sie nicht eine gemeinsam genutzte Platte in mehrere Partitionen auf, wobei jede Partition einer anderen Anwendung und somit einer anderen Clustergruppe zugeordnet wird.

   Beispielsweise könnte Anwendung A, eine stabile Anwendung, aufgrund eines Softwareproblems mit Anwendung B zur Übernahme gezwungen werden. Diese Übernahme könnte erfolgen, wenn beide Anwendungen Partitionen verwenden, die Teil derselben physischen Platte sind. Dieses Problem hat zur Folge, dass die Cluster-Services Anwendung B und ihre zusätzlich erforderliche Plattenressource durch Übernahme übertragen. Da sich die Partitionen auf demselben physischen Laufwerk befinden, wird auch Anwendung A zur Übernahme gezwungen. Aus diesem Grund sollten Sie beim Installieren und Konfigurieren einer IBM Spectrum Protect-Anwendung eine gemeinsam genutzte Platte als Ressource zuordnen, für die, falls erforderlich, eine Übernahme erfolgen kann.

3. Stellen Sie sicher, dass für jede IBM Spectrum Protect-Serverinstanz, die Sie konfigurieren, eine IP-Adresse und ein Netzname angegeben werden. Für einen Cluster mit zwei IBM Spectrum Protect-Clusterinstanzen sind zwei Netznamen erforderlich.
4. Erstellen Sie eine Clusterressourcengruppe und versetzen Sie Plattenressourcen auf sie. Jede IBM Spectrum Protect-Serverinstanz erfordert eine Clusterressourcengruppe. Anfänglich darf die Gruppe nur Plattenressourcen enthalten. Sie können gegebenenfalls auch eine vorhandene Ressourcengruppe umbenennen, die lediglich Plattenressourcen enthält.
5. IBM Spectrum Protect wird auf jedem Knoten im Cluster auf einer lokalen Platte installiert. Legen Sie fest, welche Platte auf jedem Knoten verwendet werden soll. Verwenden Sie auf jedem System denselben Laufwerkbuchstaben. Wenn der IBM Spectrum Protect-Server in einer Clusterumgebung installiert wird, muss die Option SANDISCOVERY auf ON gesetzt werden. Standardmäßig ist diese Option auf OFF gesetzt.
6. Wenn Sie sich dafür entscheiden, die IBM Spectrum Protect-Bandübernahmeunterstützung nicht zu verwenden, können Sie Bandeinheiten mithilfe einer der folgenden Konfigurationen anschließen:

Konfiguration	**Vorteile und Nachteile**	**Erforderlicher Plattenspeicherplatz**	**Vorgehensweise zur Aktivierung der Umlagerung**	**Maßnahmen bei Auftreten einer Übernahme**
Anschluss an den Knoten, auf dem die IBM Spectrum Protect-Serverinstanz aktiv ist.	Diese Konfiguration ermöglicht leistungsfähige Sicherungs- und Zurückschreibungsoperationen. Sie ist jedoch nicht vollständig automatisiert, da ein Bedienereingriff erforderlich ist, um eine Übernahme zu handhaben, wenn Verzögerungen durch eine Reparatur auftreten.	Definieren Sie genügend Datenträgerspeicherplatz, für den Daten plattenbasiert sind, um Daten von durchschnittlich mehr als zwei Tagen aufbewahren zu können.	Definieren Sie eine Speicherpoolhierarchie, damit Daten effizient auf die Bandeinheit versetzt werden.	Trennen Sie die Bandeinheit manuell und schließen Sie sie wieder an den Knoten an, auf dem der Server aktiviert wurde.
Anschluss an ein drittes System ohne Clustering, auf dem eine weitere Instanz des IBM Spectrum Protect-Servers aktiv ist.	Diese Konfiguration ist unter Umständen in Installationen mit Übertragungen mit geringer Bandbreite zwischen den Servern im Cluster und dem Server mit dem Bandeinheitencontroller nicht durchführbar.	Definieren Sie genügend Datenträgerspeicherplatz, für den Daten plattenbasiert sind, um Daten von durchschnittlich mehr als zwei Tagen aufbewahren zu können.	Verwenden Sie die virtuellen Datenträger, um die Daten von den lokalen Plattendatenträgern auf die Bandeinheit zu versetzen.	Es ist keine Aktion erforderlich; der aktivierte Server verwendet weiterhin die virtuellen Datenträger.


Windows-Betriebssysteme

IBM Spectrum Protect im Microsoft Failovercluster konfigurieren

Die IBM Spectrum Protect-Clusterkonfigurationsprozedur muss für die Gruppe von Knoten ausgeführt werden, die eine IBM Spectrum Protect-Clustergruppe hostet.

Die Schritte für die Prozedur sind von dem Knoten abhängig, den Sie gerade konfigurieren. Wenn Sie den Primärknoten in der Gruppe konfigurieren, wird die IBM Spectrum Protect-Serverinstanz erstellt und konfiguriert. Wenn Sie die übrigen Knoten in der Gruppe konfigurieren, wird jeder Knoten mithilfe einer spezifischen Methode aktualisiert. Die Art und Weise, auf die der Knoten aktualisiert wird, ermöglicht es dem Knoten, die auf dem Primärknoten erstellte IBM Spectrum Protect-Serverinstanz zu hosten. Ein IBM Spectrum Protect-Server muss auf dem ersten Knoten in der Gruppe installiert und konfiguriert werden, bevor die übrigen Knoten in der Gruppe konfiguriert werden. Wird diese Bedingung nicht erfüllt, schlägt die Konfiguration fehl.

Wenn Sie mehrere IBM Spectrum Protect-Clustergruppen konfigurieren, müssen Sie sicherstellen, dass eine IBM Spectrum Protect-Clustergruppe vollständig konfiguriert wird, bevor Sie mit der nächsten Gruppe fortfahren. Da Sie separate IP-Adressen und Netznamen für jede IBM Spectrum Protect-Clustergruppe verwenden, verringern Sie die Fehlerwahrscheinlichkeit, indem Sie jede Clustergruppe separat konfigurieren.


Windows-Betriebssysteme

IBM Spectrum Protect in einem Microsoft Failovercluster konfigurieren

Sie müssen sicherstellen, dass Ihr Cluster korrekt installiert und konfiguriert ist, bevor Sie IBM Spectrum Protect installieren.

Vorgehensweise

Um IBM Spectrum Protect in einem Microsoft Failovercluster zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass das Windows-Betriebssystem auf allen Computern installiert ist, die zum Cluster gehören. Aktuelle Informationen zu unterstützten Windows-Betriebssystemen finden Sie in der Technote 1243309.
2. Melden Sie sich mit der Domänenbenutzer-ID an. Der Domänenbenutzer muss sich in derselben Domäne wie der IBM Spectrum Protect-Server befinden.
3. Stellen Sie sicher, dass der Failovercluster für alle Computer im Cluster installiert und konfiguriert ist.
   Wenn Sie planen, den IBM Spectrum Protect-Server unter dem Betriebssystem Windows Server 2012 zu installieren, installieren Sie zunächst den Server für Failoverclusterautomatisierung und die Failovercluster-Befehlsschnittstelle. Um diese Komponenten zu installieren, geben Sie in Windows 2.0 PowerShell die folgenden Befehle aus:

   ```
   Install-WindowsFeature -Name RSAT-Clustering-AutomationServer
   Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
   ```

4. Prüfen Sie, ob jeder Knoten und jede gemeinsam genutzte Platte im Cluster betriebsbereit ist.
5. Stellen Sie sicher, dass die gemeinsam genutzten Bandeinheiten betriebsbereit sind, wenn IBM Spectrum Protect-Bandübernahmeunterstützung verwendet wird.

- Windows-BetriebssystemeMicrosoft Failoverclustergruppe für einen virtuellen Basisserver vorbereiten
  Jede IBM Spectrum Protect-Serverinstanz erfordert eine Clusterressourcengruppe.
- Windows-BetriebssystemeIBM Spectrum Protect in einem Microsoft Failovercluster installieren
  Installieren Sie den IBM Spectrum Protect-Server auf jedem Knoten in dem Cluster, der einen IBM Spectrum Protect-Cluster-Server enthält.
- Windows-BetriebssystemeIBM Spectrum Protect-Server für einen Microsoft Failovercluster auf dem Primärknoten initialisieren
  Nachdem Sie IBM Spectrum Protect auf den Knoten im Cluster installiert haben, müssen Sie den Server auf dem Primärknoten initialisieren.
- Windows-BetriebssystemeKonfiguration von IBM Spectrum Protect in einem Microsoft Failovercluster überprüfen
  Nachdem Sie die Konfiguration von IBM Spectrum Protect in einem Microsoft Failovercluster beendet haben, können Sie das Zusammenfassungsfenster 'Failovercluster-Manager' überprüfen. Stellen Sie sicher, dass das Clustering erfolgreich ausgeführt wurde und der IBM Spectrum Protect-Server gestartet wurde.
- Windows-BetriebssystemeÜbernahmetest für Ihren Cluster ausführen
  Führen Sie nach Abschluss der Clusterkonfiguration einen Übernahmetest aus, um sicherzustellen, dass die Knoten ordnungsgemäß arbeiten.

Windows-Betriebssysteme

Microsoft Failoverclustergruppe für einen virtuellen Basisserver vorbereiten

Jede IBM Spectrum Protect-Serverinstanz erfordert eine Clusterressourcengruppe.

Vorbereitende Schritte

Verwenden Sie das Programm 'Failovercluster-Manager' auf dem Computer, der Eigner der gemeinsam genutzten Platte oder Bandressource ist, um Ihre Ressourcengruppe vorzubereiten. Anfänglich darf die Gruppe nur Plattenressourcen enthalten. Sie können eine Gruppe erstellen und Plattenressourcen auf sie versetzen. Sie können auch eine vorhandene Ressourcengruppe umbenennen, die nur Plattenressourcen enthält.

Bei der Erstellung Ihrer Ressourcengruppen müssen Sie Folgendes berücksichtigen:

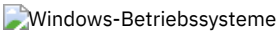
- Stellen Sie sicher, dass jede Ressourcengruppe über einen eindeutigen Namen verfügt. Ändern Sie die Namen nach der Erstellung der Gruppe nicht, da dies eine fehlerhafte Konfiguration zur Folge haben kann.
- Stellen Sie sicher, dass alle Knoten im Cluster online sind.
- Stellen Sie sicher, dass die Gruppe online ist und den Knoten als Eigner hat, auf dem die erste Serverinstanz installiert wird.

Vorgehensweise

Um eine Ressourcengruppe für die Clusterkonfiguration vorzubereiten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das Programm 'Failovercluster-Manager'. Klicken Sie mit der rechten Maustaste auf Dienste und Anwendungen und wählen Sie dann Weitere Aktionen > Leeren Dienst oder leere Anwendung erstellen aus.
2. Klicken Sie mit der rechten Maustaste auf Neuer Dienst oder neue Anwendung, wählen Sie Namen ändern aus und geben Sie einen neuen Namen, wie beispielsweise TSMGROUP, für die Ressourcengruppe an.
3. Klicken Sie mit der rechten Maustaste auf die Ressourcengruppe TSMGROUP und wählen Sie Speicherbereich hinzufügen aus.

4. Wählen Sie in der Anzeige 'Speicherbereich hinzufügen' den gemeinsam genutzten Datenträger oder die gemeinsam genutzten Datenträger für IBM Spectrum Protect aus und klicken Sie auf OK. Die Ressourcengruppe TSMGROUP, die die gerade hinzugefügten Plattendatenträger enthält, wird angezeigt.


Windows-Betriebssysteme

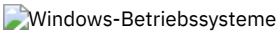
IBM Spectrum Protect in einem Microsoft Failovercluster installieren

Installieren Sie den IBM Spectrum Protect-Server auf jedem Knoten in dem Cluster, der einen IBM Spectrum Protect-Cluster-Server enthält.

Vorgehensweise

Führen Sie die folgenden Schritte für jeden Knoten in Ihrem Cluster aus, um den IBM Spectrum Protect-Server zu installieren:

1. Melden Sie sich mit einer Administrator-ID oder einer Domänenbenutzer-ID an. Der Domänenbenutzer muss ein Mitglied der Gruppe der Domänenadministratoren sein.
2. Installieren Sie den IBM Spectrum Protect-Server auf einer lokalen Platte auf jedem Knoten. Verwenden Sie für jeden Knoten denselben Laufwerkbuchstaben für die lokale Platte.
3. Starten Sie das System nach Beendigung der Serverinstallation erneut.

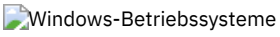

Windows-Betriebssysteme

IBM Spectrum Protect-Server für einen Microsoft Failovercluster auf dem Primärknoten initialisieren

Nachdem Sie IBM Spectrum Protect auf den Knoten im Cluster installiert haben, müssen Sie den Server auf dem Primärknoten initialisieren.

Vorgehensweise

1. Stellen Sie sicher, dass alle Systeme nach der Installation erneut gestartet werden. Stellen Sie sicher, dass alle Systeme korrekt ausgeführt werden.
2. Melden Sie sich mit einer Administrator-ID oder einer Domänenbenutzer-ID an. Der Domänenbenutzer muss sich in derselben Domäne wie der IBM Spectrum Protect-Server befinden.
3. Öffnen Sie das Programm Failovercluster-Manager und stellen Sie sicher, dass die Ressourcen online und für den Primärknoten verfügbar sind.
4. Beginnen Sie die Initialisierungsprozedur auf dem Primärknoten in Ihrem Cluster. Stellen Sie im Programm Failovercluster-Manager sicher, dass der Eigner der Ressourcengruppe der Primärknoten in Ihrem Cluster ist.
5. Klicken Sie im Menü Start auf Alle Programme > IBM Spectrum Protect-Server > Konfigurationsassistent.
6. Befolgen Sie die Anweisungen im Assistenten, indem Sie jeweils auf Weiter klicken, während Sie den Assistenten schrittweise durchlaufen. Wenn Sie zur Eingabe der Benutzer-ID aufgefordert werden, geben Sie den Namen des Domänenkontos ein, das dem Cluster zugeordnet werden soll.
7. Wenn die Initialisierung abgeschlossen ist, klicken Sie auf Fertig.


Windows-Betriebssysteme

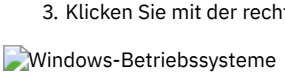
Konfiguration von IBM Spectrum Protect in einem Microsoft Failovercluster überprüfen

Nachdem Sie die Konfiguration von IBM Spectrum Protect in einem Microsoft Failovercluster beendet haben, können Sie das Zusammenfassungsfenster 'Failovercluster-Manager' überprüfen. Stellen Sie sicher, dass das Clustering erfolgreich ausgeführt wurde und der IBM Spectrum Protect-Server gestartet wurde.

Vorgehensweise

Um zu überprüfen, ob die IBM Spectrum Protect-Serverinstanz in einem Microsoft Failovercluster erstellt und korrekt konfiguriert wurde, führen Sie die folgenden Schritte aus:

1. Wählen Sie im Failovercluster-Manager die Serverinstanz aus. Der von Ihnen konfigurierte Netzname wird im Bereich 'Servername' angezeigt.
2. Stellen Sie sicher, dass die Serverinstanz und die IBM® DB2-Serverressource im Bereich 'Andere Ressourcen' angezeigt werden.
3. Klicken Sie mit der rechten Maustaste auf die IBM Spectrum Protect-Serverinstanz und wählen Sie Diese Ressource online schalten aus.


Windows-Betriebssysteme

Übernahmetest für Ihren Cluster ausführen

Führen Sie nach Abschluss der Clusterkonfiguration einen Übernahmetest aus, um sicherzustellen, dass die Knoten ordnungsgemäß arbeiten.

Vorgehensweise

1. Öffnen Sie Failovercluster-Manager. Klicken Sie unter 'Andere Ressourcen' mit der rechten Maustaste auf die Ressource für die IBM Spectrum Protect-Instanz(x). Wählen Sie Diese Ressource online schalten aus.
2. Um die Übernahme zu testen, klicken Sie mit der rechten Maustaste auf die IBM Spectrum Protect-Clusterressourcengruppe und wählen Sie Diesen Dienst oder diese Anwendung in einen anderen Knoten verschieben aus.
3. Prüfen Sie, ob die Übernahme vom zweiten Knoten auf den ersten Knoten erfolgreich ausgeführt wird.

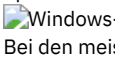
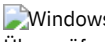
 Windows-Betriebssysteme

Clusterumgebung verwalten

Nach der Konfiguration Ihres ersten Clusters oder Ihrer ersten Cluster ist der Verwaltungsaufwand minimal.

Überprüfen Sie Ihr Windows-Ereignisprotokoll regelmäßig, wenn nicht sogar täglich, um die Aktivitäten der Knoten im Cluster zu überwachen. Überprüfen Sie mithilfe des Protokolls, ob ein Knoten fehlschlägt und Verwaltung erfordert.

Die folgenden Themen beschreiben Situationen, die Auswirkungen auf die Konfiguration oder das Format Ihres Clusters haben können, nachdem er betriebsbereit ist.

-  Windows-BetriebssystemeVorhandenen IBM Spectrum Protect-Server in einen Cluster umlagern
  Der Grund für das Versetzen von Clientdaten in einen Cluster ist mit dem Grund für das Hinzufügen eines Servers zu einem Cluster vergleichbar. Es dient der Verbesserung der Datenverfügbarkeit und -zuverlässigkeit für alle Benutzer. Da der Server Teil des Clusters ist, wird eine zusätzliche Sicherheitsstufe bereitgestellt, indem sichergestellt wird, dass keine Transaktionen aufgrund eines ausgefallenen Servers verloren gehen. Durch das von Ihnen definierte Übernahmemuster werden zukünftige Fehler verhindert.
-  Windows-BetriebssystemeIBM Spectrum Protect-Server mit Sicherung und Zurückschreibung hinzufügen
  Wenn Ihre Hardwareressourcen begrenzt sind, können Sie mit einer Sicherungs- und Zurückschreibungsprozedur einen vorhandenen IBM Spectrum Protect-Server einem Cluster hinzufügen.
-  Windows-BetriebssystemeVirtuellen IBM Spectrum Protect-Server in einem Cluster verwalten
  Bei den meisten Tasks können Sie einen virtuellen IBM Spectrum Protect-Server wie einen Server ohne Cluster verwalten. Zur Ausführung von Tasks, wie beispielsweise das Starten und Stoppen des Servers oder das Versetzen einer Ressourcengruppe auf einen anderen Knoten zur Ausführung der Systemwartung, müssen Sie die Microsoft Cluster Administrator-Schnittstelle verwenden.
-  Windows-BetriebssystemeBandübernahme in einem Cluster verwalten
  Überprüfen Sie im Rahmen Ihrer regelmäßigen Routinearbeiten das Ereignisprotokoll, um sicherzustellen, dass die Konfiguration ordnungsgemäß funktioniert. Wenn ein Serverfehler auftritt, wird der Fehler protokolliert. Das Protokoll liefert Ihnen Informationen, die erläutern, warum der Fehler aufgetreten ist.
-  Windows-BetriebssystemeFehlerbehebung mit dem IBM Spectrum Protect-Clusterprotokoll
  Die IBM Spectrum Protect-Clusterressourcen-DLL meldet Ereignisse und Fehler an das Clusterprotokoll. Das Clusterprotokoll ist ein nützliches Tool zur Fehlerbehebung. Wenn dieses Protokoll aktiviert ist, zeichnet es die Aktionen aller Komponenten des Cluster-Service (Clusterdienst) als Ergebnis der einzelnen Aktionen auf.

 Windows-Betriebssysteme

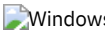
Vorhandenen IBM Spectrum Protect-Server in einen Cluster umlagern

Der Grund für das Versetzen von Clientdaten in einen Cluster ist mit dem Grund für das Hinzufügen eines Servers zu einem Cluster vergleichbar. Es dient der Verbesserung der Datenverfügbarkeit und -zuverlässigkeit für alle Benutzer. Da der Server Teil des Clusters ist, wird eine zusätzliche Sicherheitsstufe bereitgestellt, indem sichergestellt wird, dass keine Transaktionen aufgrund eines ausgefallenen Servers verloren gehen. Durch das von Ihnen definierte Übernahmemuster werden zukünftige Fehler verhindert.

Informationen zu diesem Vorgang

Um einen vorhandenen IBM Spectrum Protect-Server in einen Cluster umzulagern, können Sie entweder die Clients versetzen oder eine Sicherungs- und Zurückschreibungsprozedur ausführen. Ihre Auswahl hängt in erster Linie von der Verfügbarkeit und Kapazität der anderen IBM Spectrum Protect-Server-Computer an Ihrem Standort und Ihren Kenntnissen der Sicherungs- und Zurückschreibungsprozedur ab.

-  Windows-BetriebssystemeClients versetzen
  Wenn Sie Clients von einem IBM Spectrum Protect-Server-Computer ohne Clustering auf einen Computer mit Clustering versetzen, können Sie Ihre Benutzer ohne Serviceunterbrechung schrittweise auf das neue System versetzen. Sie müssen jedoch über die korrekte Hardware verfügen, die erforderlich ist, um zwei IBM Spectrum Protect-Server gleichzeitig auszuführen.

Zugehörige Tasks:
Server installieren und Upgrade für den Server durchführen
 Windows-Betriebssysteme

IBM Spectrum Protect-Server mit Sicherung und Zurückschreibung hinzufügen

Wenn Ihre Hardwareressourcen begrenzt sind, können Sie mit einer Sicherungs- und Zurückschreibungsprozedur einen vorhandenen IBM Spectrum Protect-Server einem Cluster hinzufügen.

Informationen zu diesem Vorgang

Angenommen, mit Ausnahme der beiden Serversysteme, die für das Clustering konfiguriert werden sollen, verfügen Sie über keine andere Hardware. Sie planen, den Computer, auf dem der IBM Spectrum Protect-Server ausgeführt wird, als Knoten zu verwenden. Führen Sie diese Prozedur aus, um IBM Spectrum Protect vom Computer zu entfernen und erneut im Cluster zu installieren:

Vorgehensweise

1. Sichern Sie alle Plattenspeicherpools in einem Kopienspeicherpool.
2. Sichern Sie die Datenbank des vorhandenen IBM Spectrum Protect-Servers.
3. Führen Sie die Installation und Konfiguration des Clusters durch.
4. Schreiben Sie die Datenbank auf den IBM Spectrum Protect-Cluster-Server zurück.
5. Schreiben Sie die Datenträger des Plattenspeicherpools vom Kopienspeicherpool zurück.
6. Löschen Sie den alten Server, nachdem Sie überprüft haben, ob alle Daten auf dem Cluster-Server vorhanden sind.

 Windows-Betriebssysteme

Virtuellen IBM Spectrum Protect-Server in einem Cluster verwalten

Bei den meisten Tasks können Sie einen virtuellen IBM Spectrum Protect-Server wie einen Server ohne Cluster verwalten. Zur Ausführung von Tasks, wie beispielsweise das Starten und Stoppen des Servers oder das Versetzen einer Ressourcengruppe auf einen anderen Knoten zur Ausführung der Systemwartung, müssen Sie die Microsoft Cluster Administrator-Schnittstelle verwenden.

Informationen zu diesem Vorgang

Die Microsoft Cluster Administrator-Schnittstelle ist über die Programmgruppe 'Verwaltung' verfügbar. Die Schnittstelle ist eine Detailsicht der Konfiguration eines virtuellen Servers. Die Konfiguration des virtuellen Servers umfasst Details wie die physischen Windows-Server, die Teil des Clusters sind, sowie ihre Ressourcen, ihre Netzverbindungen und ihren Status. Mithilfe dieser Schnittstelle können Sie die Komponenten der Konfiguration eines virtuellen Servers anzeigen und einen virtuellen Server starten oder stoppen oder ein Failback für den Server ausführen. Verwalten Sie einen virtuellen IBM Spectrum Protect-Server mithilfe der Microsoft Cluster Administrator-Schnittstelle, um Serverfehler und Fehlernachrichten zu verhindern. Wenn Sie beispielsweise den Windows-Dienststeuerungsmanager (Service Control Manager) zum Herunterfahren des Servers verwenden, empfangen Sie unter Umständen Nachrichten, die angeben, dass der Server fehlgeschlagen ist.

Falls gewünscht, können Sie einen virtuellen IBM Spectrum Protect-Server versetzen, wenn der Windows-Server als Primärknoten agiert und dieser Server eine Hardware- oder Systemwartung erfordert. Verwenden Sie die Microsoft Cluster Administrator-Schnittstelle, um die Verwaltung des virtuellen IBM Spectrum Protect-Servers auf den Sekundärknoten übertragen, bis die Wartung beendet ist.

 Windows-Betriebssysteme

Bandübernahme in einem Cluster verwalten

Überprüfen Sie im Rahmen Ihrer regelmäßigen Routinearbeiten das Ereignisprotokoll, um sicherzustellen, dass die Konfiguration ordnungsgemäß funktioniert. Wenn ein Serverfehler auftritt, wird der Fehler protokolliert. Das Protokoll liefert Ihnen Informationen, die erläutern, warum der Fehler aufgetreten ist.

Informationen zu diesem Vorgang

Manchmal muss ein Knoten wieder in den Cluster eingebunden werden, z. B. in den folgenden Fällen:

- Ein Knotenfehler ist aufgetreten.
- Eine neue Fibre Channel-HBA-Karte (Ausrüstungsänderungen) wird hinzugefügt.

Vorgehensweise

Führen Sie die folgenden Tasks in beliebiger Reihenfolge aus, um sicherzustellen, dass ein Knoten erfolgreich in den Cluster eingebunden werden kann:

- Aktualisieren Sie, falls erforderlich, das Laufwerk und das Speicherarchiv, die das IBM Spectrum Protect-Cluster-Tool verwenden.
- Schalten Sie den IBM Spectrum Protect-Server offline, bis der fehlerhafte Knoten wieder in den Cluster eingebunden wird. Mit dieser Aktion kann sichergestellt werden, dass der IBM Spectrum Protect-Server, der auf dem anderen Knoten ausgeführt wird, nicht betroffen ist.

 Windows-Betriebssysteme

Fehlerbehebung mit dem IBM Spectrum Protect-Clusterprotokoll

Die IBM Spectrum Protect-Clusterressourcen-DLL meldet Ereignisse und Fehler an das Clusterprotokoll. Das Clusterprotokoll ist ein nützliches Tool zur Fehlerbehebung. Wenn dieses Protokoll aktiviert ist, zeichnet es die Aktionen aller Komponenten des Cluster-Service (Clusterdienst) als Ergebnis der einzelnen Aktionen auf.

Im Vergleich zum Ereignisprotokoll von Microsoft Windows ist das Clusterprotokoll eine vollständige Aufzeichnung der Clusteraktivität. Das Clusterprotokoll zeichnet die Aktivität des Cluster-Service auf, die im Ereignisprotokoll aufgezeichnet wird. Das Ereignisprotokoll kann Sie zwar auf ein Problem aufmerksam machen, aber das Clusterprotokoll hilft Ihnen, das Problem zu lösen.

Das Clusterprotokoll ist in Windows standardmäßig aktiviert. Seine Ausgabe wird als Protokolldatei in %SystemRoot%\Cluster gedruckt. Weitere Informationen finden Sie in der Windows-Onlinehilfe.

Clients für Anwendungen, virtuelle Maschinen und Systeme konfigurieren

Der Server schützt Daten für Clients, die Anwendungen, virtuelle Maschinen und Systeme umfassen können. Um Clientdaten schützen zu können, müssen Sie den Clientknoten beim Server registrieren und einen Sicherungszeitplan zum Schützen der Clientdaten auswählen.

- Clients hinzufügen
  Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.
- Maßnahmen anpassen
  Die Ziele eines Unternehmens zum Schützen und Aufbewahren von Daten werden normalerweise durch Führungskräfte, Rechtsberater oder andere Personen in Führungspositionen definiert. *Maßnahmen* sind das Mittel, um den Einsatz von IBM Spectrum Protect und die Datenschutz- und Datenaufbewahrungsziele Ihres Unternehmens aufeinander abzustimmen.

Clients hinzufügen

Nach der Implementierung einer Datenschutzlösung mit IBM Spectrum Protect können Sie die Lösung durch Hinzufügen von Clients erweitern.

Informationen zu diesem Vorgang

Die Prozedur beschreibt grundlegende Schritte zum Hinzufügen eines Clients. Spezifischere Anweisungen zum Konfigurieren von Clients enthält die Dokumentation für das auf dem Clientknoten installierte Produkt. Folgende Typen von Clients können vorhanden sein:

Anwendungsclientknoten
: Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Systemclientknoten
: Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

VM-Clientknoten
: Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Vorgehensweise

Um einen Client hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie die Software aus, die auf dem Clientknoten installiert werden soll, und planen Sie die Installation. Führen Sie die Anweisungen in Client-Software auswählen und Installation planen aus.
2. Geben Sie an, wie Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Regeln zum Sichern und Archivieren von Clientdaten angeben aus.
3. Geben Sie an, wann Clientdaten gesichert und archiviert werden sollen. Führen Sie die Anweisungen in Sicherungs- und Archivierungsoperationen planen aus.
4. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, registrieren Sie den Client. Führen Sie die Anweisungen in Clients registrieren aus.
5. Um einen Clientknoten zu schützen, installieren und konfigurieren Sie die ausgewählte Software auf dem Clientknoten. Führen Sie die Anweisungen in Clients installieren und konfigurieren aus.

Client-Software auswählen und Installation planen

Unterschiedliche Typen von Daten erfordern unterschiedliche Typen von Schutz. Geben Sie den Typ der Daten an, die geschützt werden müssen, und wählen Sie die geeignete Software aus.

Informationen zu diesem Vorgang

Das bevorzugte Verfahren ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installieren, für das der Clientakzeptor keine Zeitpläne ausführt, müssen Sie die Konfigurationsanweisungen in der Produktdokumentation ausführen, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

Vorgehensweise

Wählen Sie abhängig von Ihrer Zielsetzung die zu installierenden Produkte aus und lesen Sie die Installationsanweisungen.
Tipp: Wenn Sie die Client-Software jetzt installieren, müssen Sie auch die in Clients installieren und konfigurieren beschriebenen Clientkonfigurationstasks ausführen, bevor Sie den Client verwenden können.

Ziel	Produkt und Beschreibung	Installationsanweisungen
Schutz eines Dateiservers oder einer Workstation	Der Client für Sichern/Archivieren sichert und archiviert Dateien und Verzeichnisse von Dateiservern und Workstations in Speicher. Es ist auch möglich, Sicherungsversionen und archivierte Kopien von Dateien zurückzuschreiben und abzurufen.	• Anforderungen für den Client für Sichern/Archivieren • UNIX- und Linux-Clients für Sichern/Archivieren installieren • Windows-Client für Sichern/Archivieren installieren
Schutz von Anwendungen mit Momentaufnahmesicherungs- und -zurückschreibungsfunktionalität	IBM Spectrum Protect Snapshot schützt Daten mit integrierter anwendungsgesteuerter Momentaufnahmesicherungs- und -zurückschreibungsfunktionalität. Sie können Daten schützen, die von IBM DB2-Datenbanksoftware sowie SAP-, Oracle-, Microsoft Exchange Server- und Microsoft SQL Server-Anwendungen gespeichert werden.	• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
Schutz einer E-Mail-Anwendung auf einem IBM Domino-Server	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass IBM Domino-Server heruntergefahren werden.	• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) • Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0)
Schutz einer E-Mail-Anwendung auf einem Server mit Microsoft Exchange Server	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatisiert den Datenschutz, sodass Sicherungen ausgeführt werden, ohne dass Server mit Microsoft Exchange Server heruntergefahren werden.	Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Schutz einer IBM DB2-Datenbank	Mithilfe der Anwendungsprogrammierschnittstelle (API) des Clients für Sichern/Archivieren können DB2-Daten auf dem IBM Spectrum Protect-Server gesichert werden.	IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Schutz einer IBM Informix-Datenbank	Mithilfe der API des Clients für Sichern/Archivieren können Informix-Daten auf dem IBM Spectrum Protect-Server gesichert werden.	IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Schutz einer Microsoft SQL-Datenbank	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server schützt Microsoft SQL-Daten.	Data Protection for SQL Server unter Windows Server Core installieren
Schutz einer Oracle-Datenbank	IBM Spectrum Protect for Databases: Data Protection for Oracle schützt Oracle-Daten.	Installation von Data Protection for Oracle

Ziel	Produkt und Beschreibung	Installationsanweisungen
Schutz einer SAP-Umgebung	IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP stellt Schutz bereit, der für SAP-Umgebungen angepasst ist. Das Produkt dient der Verbesserung der Verfügbarkeit von SAP-Datenbankservern und der Verringerung des Verwaltungsaufwands.	• IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren • IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren
Schutz einer virtuellen Maschine	IBM Spectrum Protect for Virtual Environments stellt Schutz bereit, der für virtuelle Microsoft Hyper-V- und VMware-Umgebungen angepasst ist. Mithilfe von IBM Spectrum Protect for Virtual Environments können Sie immer inkrementelle Sicherungen erstellen, die auf einem zentralen Server gespeichert werden, Sicherungsmaßnahmen erstellen und virtuelle Maschinen oder einzelne Dateien zurückschreiben. Sie können auch stattdessen den Client für Sichern/Archivieren zum Sichern und Zurückschreiben einer vollständigen virtuellen VMware- oder Microsoft Hyper-V-Maschine verwenden. Es ist auch möglich, Dateien oder Verzeichnisse von einer virtuellen VMware-Maschine zu sichern und zurückzuschreiben.	• Data Protection for Microsoft Hyper-V installieren • Installation und Upgrade für Data Protection for VMware durchführen • IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)

Tipp: Um den Client für die Speicherbereichsverwaltung zu verwenden, können Sie IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows installieren.

Regeln zum Sichern und Archivieren von Clientdaten angeben

Stellen Sie vor dem Hinzufügen eines Clients sicher, dass entsprechende Regeln zum Sichern und Archivieren der Clientdaten angegeben sind. Während des Clientregistrierungsprozesses ordnen Sie den Clientknoten einer Maßnahmendomäne zu, die die Regeln enthält, die die Regeln enthält, die steuern, wie und wann Clientdaten gespeichert werden.

Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Maßnahmen, die für Ihre Lösung konfiguriert sind, vertraut sind und wissen, dass für die Maßnahmen keine Änderungen erforderlich sind, fahren Sie mit Sicherungs- und Archivierungsoperationen planen fort.
- Wenn Sie mit den Maßnahmen nicht vertraut sind, führen Sie die Schritte in dieser Prozedur aus.

Informationen zu diesem Vorgang

Maßnahmen haben Auswirkungen auf das Datenvolumen, das im Laufe der Zeit gespeichert wird, und den Zeitraum, den Daten aufbewahrt werden und für die Zurückschreibung durch Clients verfügbar sind. Um Datenschutzziele zu erreichen, können Sie die Standardmaßnahme aktualisieren und eigene Maßnahmen erstellen. Eine Maßnahme umfasst die folgenden Regeln:

- Angabe, wie und wann Dateien in Serverspeicher gesichert und archiviert werden
- Anzahl Kopien einer Datei und Zeitraum, den Kopien im Serverspeicher aufbewahrt werden

Während des Clientregistrierungsprozesses ordnen Sie einen Client einer *Maßnahmendomäne* zu. Die Maßnahme für einen bestimmten Client wird durch die Regeln in der Maßnahmendomäne festgelegt, der der Client zugeordnet ist. In der Maßnahmendomäne befinden sich die Regeln, die wirksam sind, in der aktiven *Maßnahmengruppe*.

Wenn ein Client eine Datei sichert oder archiviert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Eine *Verwaltungsklasse* ist die wichtigste Gruppe von Regeln zur Verwaltung von Clientdaten. Die Sicherungs- und Archivierungsoperationen auf dem Client verwenden die Einstellungen in der Standardverwaltungsklasse der Maßnahmendomäne, es sei denn, Sie passen die Maßnahme weiter an. Eine Maßnahme kann angepasst werden, indem weitere Verwaltungsklassen definiert werden und ihre Verwendung über Clientoptionen zugeordnet wird.

Clientoptionen können in einer lokalen, editierbaren Datei auf dem Clientsystem und in einer Clientoptionsgruppe auf dem Server angegeben werden. Die Optionen in der Clientoptionsgruppe auf dem Server können die Optionen in der lokalen Clientoptionsdatei überschreiben oder den Optionen in der lokalen Clientoptionsdatei hinzugefügt werden.

Vorgehensweise

1. Überprüfen Sie die Maßnahmen, die für Ihre Lösung konfiguriert sind, indem Sie die Anweisungen in Maßnahmen anzeigen ausführen.
2. Wenn geringfügige Änderungen erforderlich sind, um die Datenaufbewahrungsanforderungen zu erfüllen, führen Sie die Anweisungen in Maßnahmen editieren aus.
3. Optional: Wenn Maßnahmendomänen erstellt oder umfangreiche Änderungen an Maßnahmen durchgeführt werden müssen, um Datenaufbewahrungsanforderungen zu erfüllen, lesen Sie die Informationen in Maßnahmen anpassen.

Maßnahmen anzeigen

Zeigen Sie Maßnahmen an, um zu bestimmen, ob die Maßnahmen zur Erfüllung Ihrer Anforderungen editiert werden müssen.

Vorgehensweise

1. Um die aktive Maßnahmengruppe für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
   a. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
   b. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.
2. Um inaktive Maßnahmengruppen für eine Maßnahmendomäne anzuzeigen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf der Seite Maßnahmengruppen auf die Umschaltfläche Konfigurieren. Jetzt können Sie die inaktiven Maßnahmengruppen anzeigen und editieren.
   b. Blättern Sie mithilfe der vorwärts und rückwärts gerichteten Pfeile durch die inaktiven Maßnahmengruppen. Wenn Sie eine inaktive Maßnahmengruppe anzeigen, sind die unterschiedlichen Einstellungen für die inaktive und aktive Maßnahmengruppe hervorgehoben.
   c. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.

Maßnahmen editieren

Um die Regeln zu ändern, die für eine Maßnahmendomäne gelten, editieren Sie die aktive Maßnahmengruppe für die Maßnahmendomäne. Sie können auch eine andere Maßnahmengruppe für eine Domäne aktivieren.

Vorbereitende Schritte

Änderungen an Maßnahmen können sich auf die Datenaufbewahrung auswirken. Stellen Sie sicher, dass weiterhin Daten gesichert werden, die für Ihr Unternehmen von entscheidender Bedeutung sind, sodass Sie diese Daten in einem Katastrophenfall zurückschreiben können. Stellen Sie außerdem sicher, dass Ihr System über genügend Speicherbereich für geplante Sicherungsoperationen verfügt.

Informationen zu diesem Vorgang

Sie editieren eine Maßnahmengruppe, indem Sie eine oder mehrere Verwaltungsklassen in der Maßnahmengruppe ändern. Wenn Sie die aktive Maßnahmengruppe editieren, stehen die Änderungen den Clients erst zur Verfügung, nachdem Sie die Maßnahmengruppe reaktiviert haben. Um die editierte Maßnahmengruppe Clients zur Verfügung zu stellen, aktivieren Sie die Maßnahmengruppe.

Obwohl Sie mehrere Maßnahmengruppen für eine Maßnahmendomäne definieren können, kann nur eine einzige Maßnahmengruppe aktiv sein. Wenn Sie eine andere Maßnahmengruppe aktivieren, ersetzt diese die momentan aktive Maßnahmengruppe.

Informationen zu bevorzugten Verfahren zum Definieren von Maßnahmen finden Sie in Maßnahmen anpassen.

Vorgehensweise

1. Wählen Sie auf der Seite Services im Operations Center eine Maßnahmendomäne aus und klicken Sie auf Details.
2. Klicken Sie auf der Seite Zusammenfassung für die Maßnahmendomäne auf die Registerkarte Maßnahmengruppen.

   Die Seite Maßnahmengruppen gibt den Namen der aktiven Maßnahmengruppe an und listet alle Verwaltungsklassen für diese Maßnahmengruppe auf.

3. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppe ist editierbar.
4. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
5. Editieren Sie die Maßnahmengruppe, indem Sie eine der folgenden Aktionen ausführen:

Option	Bezeichnung
Verwaltungsklasse hinzufügen	a. Klicken Sie in der Tabelle 'Maßnahmengruppen' auf + Verwaltungsklasse. b. Um die Regeln zum Sichern und Archivieren von Daten anzugeben, füllen Sie die Felder im Fenster Verwaltungsklasse hinzufügen aus. c. Um die Verwaltungsklasse als Standardverwaltungsklasse festzulegen, wählen Sie das Kontrollkästchen Als Standardwert definieren aus. d. Klicken Sie auf Hinzufügen.

Option	Bezeichnung
Verwaltungsklasse löschen	Klicken Sie in der Spalte 'Verwaltungsklasse' auf -. Tipp: Um die Standardverwaltungsklasse zu löschen, müssen Sie zunächst eine andere Verwaltungsklasse als Standardverwaltungsklasse zuordnen.
Legen Sie eine Verwaltungsklasse als Standardverwaltungsklasse fest.	Klicken Sie in der Spalte 'Standard' für die Verwaltungsklasse auf das Optionsfeld. Tipp: Die Standardverwaltungsklasse verwaltet Clientdateien, wenn einer Datei keine andere Verwaltungsklasse zugeordnet ist oder keine andere Verwaltungsklasse zur Verwaltung geeignet ist. Um sicherzustellen, dass Clients immer Dateien sichern und archivieren können, wählen Sie eine Standardverwaltungsklasse aus, die sowohl Regeln für das Sichern als auch für das Archivieren von Dateien enthält.
Verwaltungsklasse ändern	Um die Merkmale einer Verwaltungsklasse zu ändern, aktualisieren Sie die Felder in der Tabelle.

6. Klicken Sie auf Sichern.
   Achtung: Wenn Sie eine neue Maßnahmengruppe aktivieren, können Daten verloren gehen. Daten, die unter einer Maßnahmengruppe geschützt werden, werden möglicherweise unter einer anderen Maßnahmengruppe nicht geschützt. Daher müssen Sie vor dem Aktivieren einer Maßnahmengruppe sicherstellen, dass die Unterschiede zwischen der vorherigen Maßnahmengruppe und der neuen Maßnahmengruppe keinen Datenverlust zur Folge haben.
7. Klicken Sie auf Aktivieren. Es wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt. Stellen Sie sicher, dass die Änderungen in der neuen Maßnahmengruppe mit Ihren Datenaufbewahrungsanforderungen konsistent sind, indem Sie die folgenden Schritte ausführen:
   a. Überprüfen Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der aktiven Maßnahmengruppe gebunden sind, werden in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
   b. Ermitteln Sie Verwaltungsklassen in der aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben und wägen Sie die Konsequenzen für Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
   c. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden sollen, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.

Sicherungs- und Archivierungsoperationen planen

Bevor Sie einen neuen Client beim Server registrieren, müssen Sie sicherstellen, dass ein Zeitplan verfügbar ist, um anzugeben, wann Sicherungs- und Archivierungsoperationen ausgeführt werden. Während des Registrierungsprozesses können Sie dem Client einen Zeitplan zuordnen.

Vorbereitende Schritte

Legen Sie die weitere Vorgehensweise fest:

- Wenn Sie mit den Zeitplänen, die für die Lösung konfiguriert sind, vertraut sind und für die Zeitpläne keine Änderungen erforderlich sind, fahren Sie mit Clients registrieren fort.
- Wenn Sie mit den Zeitplänen nicht vertraut sind oder für die Zeitpläne Änderungen erforderlich sind, führen Sie die Schritte in dieser Prozedur aus.

Informationen zu diesem Vorgang

Normalerweise müssen Sicherungsoperationen für alle Clients täglich ausgeführt werden. Planen Sie Client- und Server-Workloads mit Bedacht, um die beste Leistung für Ihre Speicherumgebung zu erzielen. Um die Überschneidung von Client- und Serveroperationen zu verhindern, planen Sie die Ausführung von Clientsicherungs- und -archivierungsoperationen gegebenenfalls für die Nacht. Wenn sich Client- und Serveroperationen überschneiden oder ihnen nicht genügend Zeit und Ressourcen zur Verarbeitung zur Verfügung gestellt werden, können eine Verschlechterung der Systemleistung, fehlgeschlagene Operationen und andere Probleme die Folge sein.

Vorgehensweise

1. Überprüfen Sie die verfügbaren Zeitpläne, indem Sie den Mauszeiger in der Menüleiste des Operations Center über Clients bewegen. Klicken Sie auf Zeitpläne.
2. Optional: Ändern oder Erstellen Sie einen Zeitplan, indem Sie die folgenden Schritte ausführen:

Option	Bezeichnung
Zeitplan ändern	a. Wählen Sie in der Sicht Zeitpläne den Zeitplan aus und klicken Sie auf Details. b. Zeigen Sie auf der Seite Zeitplandetails Details an, indem Sie auf die blauen Pfeile am Anfang der Zeilen klicken. c. Ändern Sie die Einstellungen im Zeitplan und klicken Sie auf Sichern.
Zeitplan erstellen	Klicken Sie in der Sicht Zeitpläne auf +Zeitplan und führen Sie die Schritte zum Erstellen eines Zeitplans aus.

3. Optional: Verwenden Sie zum Konfigurieren von Zeitplaneinstellungen, die im Operations Center nicht sichtbar sind, einen Serverbefehl. Angenommen, Sie möchten eine Clientoperation planen, mit der ein bestimmtes Verzeichnis gesichert und einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zugeordnet wird.
   a. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.
   b. Geben Sie zum Erstellen eines Zeitplans den Befehl DEFINE SCHEDULE und zum Ändern eines Zeitplans den Befehl UPDATE SCHEDULE aus. Ausführliche Informationen zu den Befehlen finden Sie in DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren) bzw. UPDATE SCHEDULE (Clientzeitplan aktualisieren).

Zugehörige Tasks:
Zeitplan für tägliche Operationen optimieren

Clients registrieren

Registrieren Sie einen Client, um sicherzustellen, dass der Client die Verbindung zum Server herstellen und der Server Clientdaten schützen kann.

Vorbereitende Schritte

Bestimmen Sie, ob der Client eine Benutzer-ID mit Administratorberechtigung mit Clienteignerberechtigung für den Clientknoten erfordert. Informationen zum Bestimmen der Clients, die eine Benutzer-ID mit Administratorberechtigung erfordern, finden Sie in Technote 7048963. Einschränkung: Bei einigen Clienttypen müssen der Clientknotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Sie können diese Clients nicht mithilfe der in Version 7.1.7 eingeführten LDAP-Authentifizierungsmethode authentifizieren. Ausführliche Informationen zu dieser Authentifizierungsmethode, die manchmal als integrierter Modus bezeichnet wird, finden Sie in Benutzer mithilfe einer Active Directory-Datenbank authentifizieren.

Vorgehensweise

Um einen Client zu registrieren, führen Sie eine der folgenden Aktionen aus.

- Wenn der Client eine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Befehl REGISTER NODE unter Angabe des Parameters USERID:

  ```
  register node Knotenname Kennwort userid=Knotenname
  ```

  Dabei gibt *Knotenname* den Knotennamen und *Kennwort* das Knotenkennwort an. Ausführliche Informationen finden Sie in Knoten registrieren.
- Wenn der Client keine Benutzer-ID mit Administratorberechtigung erfordert, registrieren Sie den Client mit dem Assistenten 'Client hinzufügen' im Operations Center. Führen Sie die folgenden Schritte aus:
  a. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  b. Klicken Sie in der Tabelle 'Clients' auf + Client.
  c. Führen Sie die Schritte im Assistenten Client hinzufügen aus:
     i. Geben Sie an, dass redundante Daten sowohl auf dem Client als auch auf dem Server gelöscht werden können. Wählen Sie im Bereich 'Clientseitige Datendeduplizierung' das Kontrollkästchen Aktivieren aus.
     ii. Kopieren Sie im Fenster Konfiguration die Werte für die Optionen TCPSERVERADDRESS, TCPPORT, NODENAME und DEDUPLICATION.
     Tipp: Notieren Sie die Optionswerte und bewahren Sie die Unterlagen an einem sicheren Ort auf. Nachdem Sie die Clientregistrierung abgeschlossen und die Software auf dem Clientknoten installiert haben, verwenden Sie die Werte zum Konfigurieren des Clients.
     iii. Führen Sie die Anweisungen im Assistenten aus, um die Maßnahmendomäne, den Zeitplan und die Optionsgruppe anzugeben.
     iv. Legen Sie fest, wie Risiken für den Client angezeigt werden, indem Sie die Einstellung für die Gefährdung angeben.
     v. Klicken Sie auf Client hinzufügen.

Zugehörige Verweise:
DECOMMISSION NODE (Clientknoten stilllegen)
DECOMMISSION VM (Virtuelle Maschine stilllegen)
QUERY NODE (Knoten abfragen)
REMOVE REPLNODE (Clientknoten aus Replikation entfernen)

Clients installieren und konfigurieren

Bevor Sie einen Clientknoten schützen können, müssen Sie die ausgewählte Software installieren und konfigurieren.

Vorgehensweise

Wenn Sie die Software bereits installiert haben, starten Sie mit Schritt 2.

1. Führen Sie eine der folgenden Aktionen aus:

- Um Software auf einem Anwendungs- oder Clientknoten zu installieren, führen Sie die Anweisungen aus.

Software	Link zu Anweisungen
IBM Spectrum Protect-Client für Sichern/Archivieren	▪ UNIX- und Linux-Clients für Sichern/Archivieren installieren ▪ Windows-Client für Sichern/Archivieren installieren Informationen zur manuellen Implementierung von Clientaktualisierungen vom Server finden Sie in den folgenden Dokumenten: ▪ Für IBM Spectrum Protect-Server der Version 8.1.2 oder höher siehe Technote 2004596. ▪ Für IBM® Tivoli Storage Manager-Server der Version 7.1 und IBM Spectrum Protect-Server der Version 8.1.1 siehe Technote 1673299.
IBM Spectrum Protect for Databases	▪ Installation von Data Protection for Oracle ▪ Data Protection for SQL Server unter Windows Server Core installieren
IBM Spectrum Protect for Mail	▪ Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) ▪ Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0) ▪ Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect Snapshot	▪ Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen ▪ Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen ▪ Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
IBM Spectrum Protect for Enterprise Resource Planning	▪ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 installieren ▪ IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle installieren

- Um Software auf einem VM-Clientknoten zu installieren, führen Sie die Anweisungen für den ausgewählten Sicherungstyp aus.

Sicherungstyp	Link zu Anweisungen
Wenn Sie planen, VMware-Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie den IBM Spectrum Protect-Client für Sichern/Archivieren.	▪ UNIX- und Linux-Clients für Sichern/Archivieren installieren ▪ Windows-Client für Sichern/Archivieren installieren
Wenn Sie planen, immer inkrementelle Gesamtsicherungen virtueller Maschinen zu erstellen, installieren und konfigurieren Sie IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren auf demselben Clientknoten oder auf unterschiedlichen Clientknoten.	▪ IBM Spectrum Protect for Virtual Environments-Onlineproduktdokumentation Tipp: Die Software für IBM Spectrum Protect for Virtual Environments und den Client für Sichern/Archivieren sind im IBM Spectrum Protect for Virtual Environments-Installationspaket enthalten.

2. Um Clients das Herstellen einer Verbindung zum Server zu ermöglichen, fügen Sie die Werte für die Optionen TCPSERVERADDRESS, TCPPORT und NODENAME in der Clientoptionsdatei hinzu oder aktualisieren Sie diese. Verwenden Sie die Werte, die Sie beim Registrieren des Clients notiert haben (Clients registrieren).
   - Fügen Sie für Clients, die unter einem AIX-, Linux-, Mac OS X- oder Oracle Solaris-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.sys hinzu.
   - Fügen Sie für Clients, die unter einem Windows-Betriebssystem installiert sind, die Werte der Clientsystemoptionsdatei dsm.opt hinzu.

   Standardmäßig befinden sich die Optionsdateien im Installationsverzeichnis.
3. Wenn ein Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem installiert wurde, installieren Sie den Clientverwaltungsservice auf dem Client. Führen Sie die Anweisungen in Diagnoseinformationen mit Clientverwaltungsservices erfassen aus.
4. Konfigurieren Sie den Client für die Ausführung geplanter Operationen. Führen Sie die Anweisungen in Client für die Ausführung geplanter Operationen konfigurieren aus.
5. Optional: Konfigurieren Sie die Kommunikation durch eine Firewall. Führen Sie die Anweisungen in Client/Server-Kommunikation durch eine Firewall konfigurieren aus.
6. Führen Sie eine Testsicherung aus, um sicherzustellen, dass Daten wie geplant geschützt werden. Führen Sie beispielsweise für einen Client für Sichern/Archivieren die folgenden Schritte aus:
   a. Wählen Sie auf der Seite 'Clients' im Operations Center den Client aus, der gesichert werden soll, und klicken Sie auf Sichern.
   b. Überprüfen Sie, ob die Sicherung erfolgreich ausgeführt wird und keine Warnungen oder Fehlernachrichten vorhanden sind.
7. Überwachen Sie die Ergebnisse der geplanten Operationen für den Client im Operations Center.

Nächste Schritte

Wenn geändert werden muss, welche Daten vom Client gesichert werden, führen Sie die Anweisungen in Bereich einer Clientsicherung ändern aus.

Client für die Ausführung geplanter Operationen konfigurieren

Sie müssen einen Client-Scheduler auf dem Clientknoten konfigurieren und starten. Der Client-Scheduler ermöglicht die Kommunikation zwischen dem Client und dem Server, sodass geplante Operationen erfolgen können. Beispielsweise umfassen geplante Operationen normalerweise das Sichern von Dateien von einem Client.

Informationen zu diesem Vorgang

Die bevorzugte Methode ist die Installation des Clients für Sichern/Archivieren auf allen Clientknoten, sodass Sie den Clientakzeptor auf dem Clientknoten konfigurieren und starten können. Der Clientakzeptor ist für die effiziente Ausführung geplanter Operationen konzipiert. Der Clientakzeptor verwaltet den Client-Scheduler derart, dass der Scheduler nur in erforderlichen Fällen ausgeführt wird:

- Wenn der Zeitpunkt erreicht ist, an dem der Server nach der nächsten geplanten Operation abgefragt werden soll
- Wenn der Zeitpunkt erreicht ist, an dem die nächste geplante Operation gestartet werden soll

Durch die Verwendung des Clientakzeptors ist es möglich, die Anzahl Hintergrundprozesse auf dem Client zu reduzieren und Probleme in Bezug auf die Speicheraufbewahrungsdauer zu vermeiden.

Der Clientakzeptor führt Zeitpläne für die folgenden Produkte aus: Client für Sichern/Archivieren, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail und IBM Spectrum Protect for Virtual Environments. Wenn Sie ein Produkt installiert hatten, für das der Clientakzeptor keine Zeitpläne ausführt, führen Sie die Konfigurationsanweisungen in der Produktdokumentation aus, um sicherzustellen, dass geplante Operationen ausgeführt werden können.

Wenn Ihr Unternehmen standardmäßig ein Zeitplanungstool eines anderen Anbieters verwendet, können Sie statt des Clientakzeptors dieses Zeitplanungstool verwenden. Normalerweise starten Zeitplanungstools anderer Anbieter Clientprogramme direkt mithilfe von Betriebssystembefehlen. Informationen zum Konfigurieren eines Zeitplanungstools eines anderen Anbieters enthält die Produktdokumentation.

Vorgehensweise

Um den Client-Scheduler mithilfe des Clientakzeptors zu konfigurieren und zu starten, führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
b. Klicken Sie auf die Registerkarte Web-Client.
c. Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
d. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei dsm.sys die Option passwordaccess auf `generate`.
e. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkennwort ein:

   ```
   dsmc query sess
   ```

f. Starten Sie den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

   ```
   /usr/bin/dsmcad
   ```

g. Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie der Systemstartdatei (normalerweise /etc/inittab) den folgenden Eintrag hinzu:

   ```
   tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Clientakzeptordämon
   ```

Linux

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
b. Klicken Sie auf die Registerkarte Web-Client.
c. Klicken Sie im Feld Optionen für verwaltete Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beides.
d. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, setzen Sie in der Datei dsm.sys die Option passwordaccess auf `generate`.
e. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl aus und geben Sie auf Anforderung das Clientknotenkennwort ein:

   ```
   dsmc query sess
   ```

f. Starten Sie den Clientakzeptor, indem Sie sich mit der Rootbenutzer-ID anmelden und den folgenden Befehl ausgeben:

```
service dsmcad start
```

g. Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie den Service hinzu, indem Sie in einer Shelleingabeaufforderung den folgenden Befehl ausgeben:

```
# chkconfig --add dsmcad
```

MAC OS X

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
b. Um sicherzustellen, dass der Scheduler automatisch gestartet werden kann, klicken Sie auf Berechtigung, wählen Sie Kennwort generieren aus und klicken Sie auf Anwenden.
c. Um anzugeben, wie Services verwaltet werden, klicken Sie auf Web-Client, wählen Sie Zeitplan aus, klicken Sie auf Anwenden und dann auf OK.
d. Um sicherzustellen, dass das generierte Kennwort gespeichert wird, starten Sie den Client für Sichern/Archivieren erneut.
e. Starten Sie den Clientakzeptor mithilfe der Anwendung 'IBM Spectrum Protect Tools for Administrators'.

Windows

a. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Dienstprogramme > Setup-Assistent > Hilfe zum Konfigurieren des Client-Schedulers. Klicken Sie auf Weiter.
b. Lesen Sie die Informationen auf der Seite Schedulerassistent und klicken Sie auf Weiter.
c. Wählen Sie auf der Seite Scheduler-Task die Option Neuen oder zusätzlichen Scheduler installieren aus und klicken Sie auf Weiter.
d. Geben Sie auf der Seite Schedulername und -position einen Namen für den Client-Scheduler an, der hinzugefügt wird. Wählen Sie dann Scheduler mit Clientakzeptordämon (CAD) verwalten aus, um den Scheduler zu verwalten, und klicken Sie auf Weiter.
e. Geben Sie den Namen ein, der diesem Clientakzeptor zugeordnet werden soll. Der Standardname ist 'Clientakzeptor'. Klicken Sie auf Weiter.
f. Schließen Sie die Konfiguration ab, indem Sie den Assistenten durchlaufen.
g. Aktualisieren Sie die Clientoptionsdatei, dsm.opt, und setzen Sie die Option passwordaccess auf generate.
h. Um das Clientknotenkennwort zu speichern, geben Sie den folgenden Befehl in der Eingabeaufforderung aus:

```
dsmc query sess
```

Geben Sie auf Anforderung das Clientknotenkennwort ein.
i. Starten Sie den Clientakzeptorservice über die Seite Systemsteuerung. Wenn Sie beispielsweise den Standardnamen verwendet haben, starten Sie den Service 'Clientakzeptor'. Starten Sie nicht den Scheduler-Service, den Sie auf der Seite Schedulername und -position angegeben haben. Der Scheduler-Service wird wie erforderlich automatisch vom Clientakzeptorservice gestartet und gestoppt.

Client/Server-Kommunikation durch eine Firewall konfigurieren

Wenn ein Client durch eine Firewall mit einem Server kommunizieren muss, müssen Sie die Client/Server-Kommunikation durch die Firewall ermöglichen.

Vorbereitende Schritte

Wenn Sie den Assistenten 'Client hinzufügen' zum Registrieren eines Clients verwendet hatten, bestimmen Sie die Optionswerte in der Clientoptionsdatei, die während dieses Prozesses abgerufen wurden. Sie können die Werte zur Angabe von Ports verwenden.

Informationen zu diesem Vorgang

Achtung: Konfigurieren Sie eine Firewall nicht derart, dass dies eine Beendigung der Sitzungen zur Folge hätte, die von einem Server oder Speicheragenten verwendet werden. Die Beendigung einer gültigen Sitzung kann zu unvorhersehbaren Ergebnissen führen. Prozesse und Sitzungen scheinen unter Umständen aufgrund von Ein-/Ausgabefehlern gestoppt zu werden. Um das Ausschließen von Sitzungen von Zeitlimitbeschränkungen zu erleichtern, konfigurieren Sie bekannte Ports für IBM Spectrum Protect-Komponenten. Stellen Sie sicher, dass die Serveroption KEEPALIVE auf den Standardwert YES gesetzt bleibt. Auf diese Art und Weise kann sichergestellt werden, dass die Client/Server-Kommunikation unterbrechungsfrei erfolgt. Anweisungen zum Definieren der Serveroption KEEPALIVE finden Sie in KEEPALIVE.

Vorgehensweise

Öffnen Sie die folgenden Ports, um Zugriff durch die Firewall zu ermöglichen:

TCP/IP-Port für den Client für Sichern/Archivieren, den Verwaltungsbefehlszeilenclient und den Client-Scheduler
: Geben Sie den Port über die Option tcpport in der Clientoptionsdatei an. Die Option tcpport in der Clientoptionsdatei muss mit der Option TCPPORT in der Serveroptionsdatei übereinstimmen. Der Standardwert ist 1500. Wenn ein anderer Wert als der Standardwert verwendet werden soll, geben Sie eine Zahl zwischen 1024 und 32767 an.

HTTP-Port, um die Kommunikation zwischen dem Web-Client und fernen Workstations zu ermöglichen

Geben Sie den Port für die ferne Workstation an, indem Sie die Option httpport in der Clientoptionsdatei der fernen Workstation festlegen. Der Standardwert ist 1581.

TCP/IP-Ports für die ferne Workstation
: Der Standardwert von 0 (null) hat zur Folge, dass zwei freie Portnummern der fernen Workstation nach dem Zufallsprinzip zugeordnet werden. Wenn die Portnummern nicht nach dem Zufallsprinzip zugeordnet werden sollen, geben Sie über die Option webports in der Clientoptionsdatei der fernen Workstation Werte an.

TCP/IP-Port für Verwaltungssitzungen
: Geben Sie den Port an, an dem der Server auf Anforderungen von Verwaltungsclientsitzungen wartet. Der Wert der Clientoption tcpadminport muss mit dem Wert der Serveroption TCPADMINPORT übereinstimmen. Auf diese Art und Weise können Sie sichere Verwaltungssitzungen in einem privaten Netz gewährleisten.

Maßnahmen anpassen

Die Ziele eines Unternehmens zum Schützen und Aufbewahren von Daten werden normalerweise durch Führungskräfte, Rechtsberater oder andere Personen in Führungspositionen definiert. *Maßnahmen* sind das Mittel, um den Einsatz von IBM Spectrum Protect und die Datenschutz- und Datenaufbewahrungsziele Ihres Unternehmens aufeinander abzustimmen.

Informationen zu diesem Vorgang

Um Datenschutz und Datenaufbewahrung automatisch verwalten zu können, definieren Sie Maßnahmen; dies sind Regeln, die Sie auf dem Server festlegen. Maßnahmen haben Auswirkungen darauf, wie viele Daten im Laufe der Zeit gespeichert werden und wie lange Daten aufbewahrt werden und für die Zurückschreibung durch Clients verfügbar sind. Passen Sie Maßnahmen an, um die Datenschutzziele Ihres Unternehmens zu erreichen.

Die Auswahl der Maßnahme, mit der die Daten eines Clients verwaltet werden, erfolgt über die Zuordnung des Clients zu einer Maßnahmendomäne. Clients unterschiedlicher Typen haben unterschiedliche Aufbewahrungsanforderungen und die Anpassung und Erstellung von Maßnahmen ist normalerweise erforderlich.

Wenn ein Server installiert wird, verfügt er standardmäßig über exakt eine Maßnahme in exakt einer Maßnahmendomäne. Sie können diese Maßnahme anpassen und eigene Maßnahmen erstellen.

- Maßnahmenkonzepte
  Die Maßnahme für einen bestimmten Client wird durch die Einstellungen in der Maßnahmendomäne festgelegt, der ein Client hinzugefügt wird.
- Maßnahme anpassen
  Sie können vorhandene Maßnahmen anpassen, um neue oder überarbeitete Datenaufbewahrungsanforderungen Ihres Unternehmens zu erfüllen. Eine typische Möglichkeit zum Starten der Maßnahmenanpassung ist das Ändern einer Maßnahmendomäne oder das Kopieren einer vorhandenen Maßnahmendomäne.
- Maßnahme durch Kopieren einer vorhandenen Maßnahme erstellen
  Sie können neue Maßnahmen erstellen, indem Sie eine vorhandene Maßnahme kopieren und dann die Teile aktualisieren, die geändert werden sollen.
- Maßnahmendomäne erstellen
  Möglicherweise möchten Sie für jeden Typ von Client, der vom Server geschützt wird, eine neue Maßnahmendomäne erstellen. Möglicherweise möchten Sie auch die Zuständigkeit für Clients auf mehrere Administratoren verteilen, indem Sie Ihnen Berechtigung für bestimmte Maßnahmendomänen erteilen.
- Clientoperationen über Clientoptionsgruppen steuern
  Mithilfe von Clientoptionsgruppen können Sie die Verarbeitungsoptionen, die Clients für Operationen wie Sicherungen verwenden, zentral steuern. Mithilfe von Clientoptionsgruppen kann sichergestellt werden, dass Daten konsistent gemäß Ihren Anforderungen geschützt werden. Eine Clientoptionsgruppe kann Optionen in einer lokalen Clientoptionsdatei überschreiben oder Optionen hinzufügen, die unter Umständen nicht in der lokalen Clientoptionsdatei vorhanden sind.

Maßnahmenkonzepte

Die Maßnahme für einen bestimmten Client wird durch die Einstellungen in der Maßnahmendomäne festgelegt, der ein Client hinzugefügt wird.

Während des Clientregistrierungsprozesses ordnen Sie einen Client einer *Maßnahmendomäne* zu. Die Maßnahme für jeden Client wird durch die Regeln in der Maßnahmendomäne festgelegt, der der Client zugeordnet ist. In der Maßnahmendomäne befinden sich die Regeln, die wirksam sind, in der aktiven *Maßnahmengruppe*.

Wenn ein Client eine Datei sichert oder archiviert, wird die Datei an eine Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne gebunden. Eine *Verwaltungsklasse* ist die wichtigste Gruppe von Regeln zur Verwaltung von Clientdaten. Die Sicherungs- und Archivierungsoperationen auf dem Client verwenden die Einstellungen in der Standardverwaltungsklasse der Maßnahmendomäne, es sei denn, Sie passen die Maßnahme an.

Eine Maßnahme kann angepasst werden, indem weitere Verwaltungsklassen in der Maßnahmengruppe definiert werden, die Maßnahmengruppe aktiviert wird und die Verwendung der neuen Verwaltungsklassen über Clientoptionen zugeordnet wird.

Clientoptionen können in einer lokalen, editierbaren Datei auf dem Clientsystem und in einer Clientoptionsgruppe auf dem Server angegeben werden. Die Optionen in der Clientoptionsgruppe auf dem Server können die Optionen in der lokalen Clientoptionsdatei überschreiben oder den Optionen in der lokalen Clientoptionsdatei hinzugefügt werden.

Der Server verwendet die Maßnahme in Verwaltungsklassen, um Dateien abhängig davon, ob Dateiversionen aktiv oder inaktiv sind, zu verwalten. Die neueste Sicherungskopie oder archivierte Kopie einer Datei ist die *aktive Version*. Aktive Versionen werden nie aus dem Serverspeicher gelöscht.

Sicherungsversionen, die älter als die neueste Version sind, werden als *inaktive Versionen* bezeichnet. Eine aktive Version einer Datei wird inaktiv, wenn eines der folgenden Ereignisse eintritt:

- Die Datei wird erneut gesichert, wodurch eine neuere Version der Datei im Serverspeicher erstellt wird.
- Die Datei wird aus dem Speicher auf dem Clientknoten gelöscht und anschließend wird eine Teilsicherungsoperation ausgeführt. Bei einer *Teilsicherung*, der typischen Sicherungsoperation für einen Client, werden nur die Dateien gesichert, die sich seit der letzten Sicherung geändert haben.

Die Einstellungen in der Verwaltungsklasse, die an eine Datei gebunden ist, legen fest, wie lange und wie viele inaktive Versionen der Datei aufbewahrt werden.

Die *Verfallsverarbeitung* bestimmt mithilfe von Maßnahmen, wann inaktive Versionen nicht mehr benötigt werden, d. h., wann die Versionen verfallen. Der Verfallsprozess auf dem Server setzt Maßnahmen um, die Sie für die Datenaufbewahrung definieren; Sie müssen die regelmäßige Ausführung des Verfallsprozesses planen. Wenn beispielsweise eine Maßnahme die Aufbewahrung von maximal vier Versionen erfordert, verfällt die fünfte und älteste Version. Während der Verfallsverarbeitung entfernt der Server Einträge für verfallene Versionen aus der Datenbank, wodurch die Versionen tatsächlich aus dem Serverspeicher gelöscht werden.

- Aufbewahrung und Verfall von Sicherungsversionen
  Mehrere Versionen von Dateisicherungen sind wichtig, da Benutzer fortlaufend Dateien aktualisieren können und eine Datei möglicherweise mit dem Stand eines anderen Zeitpunkts zurückspeichern müssen. Richtlinieneinstellungen steuern die Sicherungsversionen, die der Server im Serverspeicher aufbewahrt, und haben Auswirkungen darauf, welche Daten Benutzer zurückschreiben können.
- Aktivierung der Maßnahme nach Aktualisierungen
  Wenn Sie Aktualisierungen an einer Maßnahme vornehmen, werden die Aktualisierungen erst wirksam, wenn Sie die aktualisierte Maßnahme aktivieren.

Zugehörige Konzepte:
Vollständige Teilsicherung und partielle Teilsicherung

Aufbewahrung und Verfall von Sicherungsversionen

Mehrere Versionen von Dateisicherungen sind wichtig, da Benutzer fortlaufend Dateien aktualisieren können und eine Datei möglicherweise mit dem Stand eines anderen Zeitpunkts zurückspeichern müssen. Richtlinieneinstellungen steuern die Sicherungsversionen, die der Server im Serverspeicher aufbewahrt, und haben Auswirkungen darauf, welche Daten Benutzer zurückschreiben können.

Mithilfe der Einstellungen in der Verwaltungsklasse können Sie die Versionen angeben, die der Server im Serverspeicher aufbewahrt:

- Geben Sie die Anzahl Tage für die Aufbewahrung von Sicherungsversionen an.
  Die Anzahl Tage für die Aufbewahrung von Sicherungsversionen wird über Einstellungen im Operations Center angegeben:
  - Zusätzliche Sicherungen aufbewahren; dies ist die Anzahl Tage für die Aufbewahrung inaktiver Sicherungsversionen. Die Tage werden ab dem Tag gezählt, an dem die Version inaktiv wird.

    Wenn Sie Befehle verwenden, verwenden Sie den Befehl DEFINE COPYGROUP mit dem Parameter RETEXTRA.

  - Gelöschte Sicherungen aufbewahren; dies ist die Anzahl Tage für die Aufbewahrung der letzten Sicherungsversion einer Datei, die aus dem Clientdateisystem gelöscht wurde.

    Wenn Sie Befehle verwenden, verwenden Sie den Befehl DEFINE COPYGROUP mit dem Parameter RETONLY.

- Geben Sie die Anzahl aufzubewahrender Versionen an.
  Die Anzahl aufzubewahrender Sicherungsversionen wird über Einstellungen im Operations Center angegeben:
  - Sicherungen; dies ist die Anzahl aufzubewahrender Versionen einer Datei, die noch auf dem Clientdateisystem vorhanden ist.

    Wenn Sie Befehle verwenden, verwenden Sie den Befehl DEFINE COPYGROUP mit dem Parameter VEREXISTS.

  - Gelöschte Sicherungen; dies ist die Anzahl aufzubewahrender Versionen einer Datei, die aus dem Clientdateisystem gelöscht wurde.

    Wenn Sie Befehle verwenden, verwenden Sie den Befehl DEFINE COPYGROUP mit dem Parameter VERDELETED.

- Geben Sie eine Kombination aus Anzahl Versionen und Anzahl Tage für deren Aufbewahrung an.
  Die Interaktion der Einstellungen legt fest, welche Sicherungsversionen der Server aufbewahrt. Sie müssen wissen, welche Einstellungen Vorrang haben und welche Interaktionen erfolgen können:

    - Wenn die Anzahl inaktiver Sicherungsversionen die Anzahl in den Einstellungen Sicherungen und Gelöschte Sicherungen überschreitet, verfällt die älteste Version und der Server löscht die Datei bei der nächsten Ausführung der Verfallsverarbeitung aus der Datenbank.
    - Die Anzahl inaktiver Versionen, die der Server aufbewahrt, wird auch von der Einstellung Zusätzliche Sicherungen aufbewahren beeinflusst. Inaktive Versionen verfallen, wenn die Anzahl Tage, die sie inaktiv sind, den Wert für die Aufbewahrung von Extraversionen überschreitet; dies ist selbst dann der Fall, wenn die zulässige Anzahl Versionen nicht überschritten wird.

- Dateiverfall und Verfallsverarbeitung
  Dateien verfallen, wenn sie die Aufbewahrungskriterien, die in der Maßnahme angegeben sind, nicht mehr erfüllen. Durch die Verfallsverarbeitung auf dem Server werden verfallene Dateien aus der Serverdatenbank entfernt und die Dateien aus dem Serverspeicher gelöscht.
- Beispiel: Aufbewahrung, wenn eine Maßnahme nur Zeitsteuerelemente verwendet
  Die einfachste Möglichkeit zur Verwaltung der Datenaufbewahrung besteht in der ausschließlichen Verwendung zeitbasierter Maßnahmen. Wenn die Maßnahme nur zeitbasierte Steuerelemente enthält, werden Dateiversionen auf der Basis der Anzahl Tage aufbewahrt, nachdem die Versionen inaktiv werden.
- Beispiel: Aufbewahrung, wenn eine Maßnahme sowohl Versions- als auch Zeitsteuerelemente verwendet
  Wenn sowohl die Versions- als auch die Zeitsteuerelemente in einer Maßnahme verwendet werden, ermöglicht dies Flexibilität bei der Handhabung der Datenaufbewahrung, hat jedoch auch Komplexität zur Folge. Studieren Sie zum besseren Verständnis der Interaktion zwischen Steuerelementen die Beispielmaßnahmen und ihre Auswirkungen auf die Aufbewahrung von Sicherungsversionen einer einzelnen Datei für die Dauer eines Monats.
- Interaktionen zwischen Maßnahmeneinstellungen
  Zeitbasierte und versionsbasierte Maßnahmeneinstellungen interagieren, wenn sie gemeinsam in einer Verwaltungsklasse für eine Maßnahme verwendet werden. Die Häufigkeit von Clientsicherungen wirkt sich auch auf die Sicherungsversionen aus, die für einen Client gespeichert werden.

Dateiverfall und Verfallsverarbeitung

Dateien verfallen, wenn sie die Aufbewahrungskriterien, die in der Maßnahme angegeben sind, nicht mehr erfüllen. Durch die Verfallsverarbeitung auf dem Server werden verfallene Dateien aus der Serverdatenbank entfernt und die Dateien aus dem Serverspeicher gelöscht.

Dateien verfallen unter folgenden Bedingungen:

- Benutzer löschen Dateibereiche von Clientknoten.
- Benutzer definieren Dateien mit dem Befehl EXPIRE auf dem Client als verfallen.
- Eine Sicherungsversion einer Datei erfüllt nicht mehr die Kriterien für die Aufbewahrung von Sicherungen (Aufbewahrungsdauer einer Datei und Anzahl inaktiver Versionen einer Datei, die aufbewahrt werden).
- Eine archivierte Datei erfüllt nicht mehr die Kriterien für die Aufbewahrung archivierter Dateien (Aufbewahrungsdauer archivierter Kopien).
- Eine Sicherungsgruppe überschreitet den Aufbewahrungszeitraum, der für die Sicherungsgruppe angegeben ist.

Der Server löscht verfallene Dateien nur während der Verfallsverarbeitung aus der Serverdatenbank. Nachdem verfallene Dateien aus der Datenbank gelöscht wurden, kann der Server den Speicherbereich in den Speicherpools, den die verfallenen Dateien belegten, wiederverwenden. Stellen Sie sicher, dass die Verfallsverarbeitung regelmäßig ausgeführt wird, damit der Server den Speicherbereich wiederverwenden kann.

Einschränkungen bei der Verfallsverarbeitung

Die Verwendung einiger Funktionen wirkt sich auf die Verfallsverarbeitung aus.

Replikation
: Wenn Sie ungleiche Maßnahmen auf dem Quellenserver und dem Zielserver verwenden, werden Dateien, die auf dem Quellenreplikationsserver für den sofortigen Verfall markiert sind, erst gelöscht, nachdem sie auf den Zielreplikationsserver repliziert wurden. Wenn Sie keine ungleichen Maßnahmen verwenden, werden Dateien, die auf dem Quellenreplikationsserver für den sofortigen Verfall markiert sind, sofort gelöscht.

  Auf dem Zielreplikationsserver werden Dateien, die als verfallen markiert sind, gelöscht, wenn der Zielreplikationsserver die Verfallsverarbeitung ausführt.

Ereignisgesteuerte Aufbewahrung für Archivierungsdaten
: Eine Archivierungsdatei kann nicht für die Verfallsverarbeitung ausgewählt werden, wenn die Datei den Status 'Löschen unzulässig' hat. Wenn eine Datei nicht den Status 'Löschen unzulässig' hat, wird sie gemäß der vorhandenen Verfallsverarbeitung verarbeitet.

Zugehörige Tasks:
Verfall/Löschen anhalten und freigeben

Beispiel: Aufbewahrung, wenn eine Maßnahme nur Zeitsteuerelemente verwendet

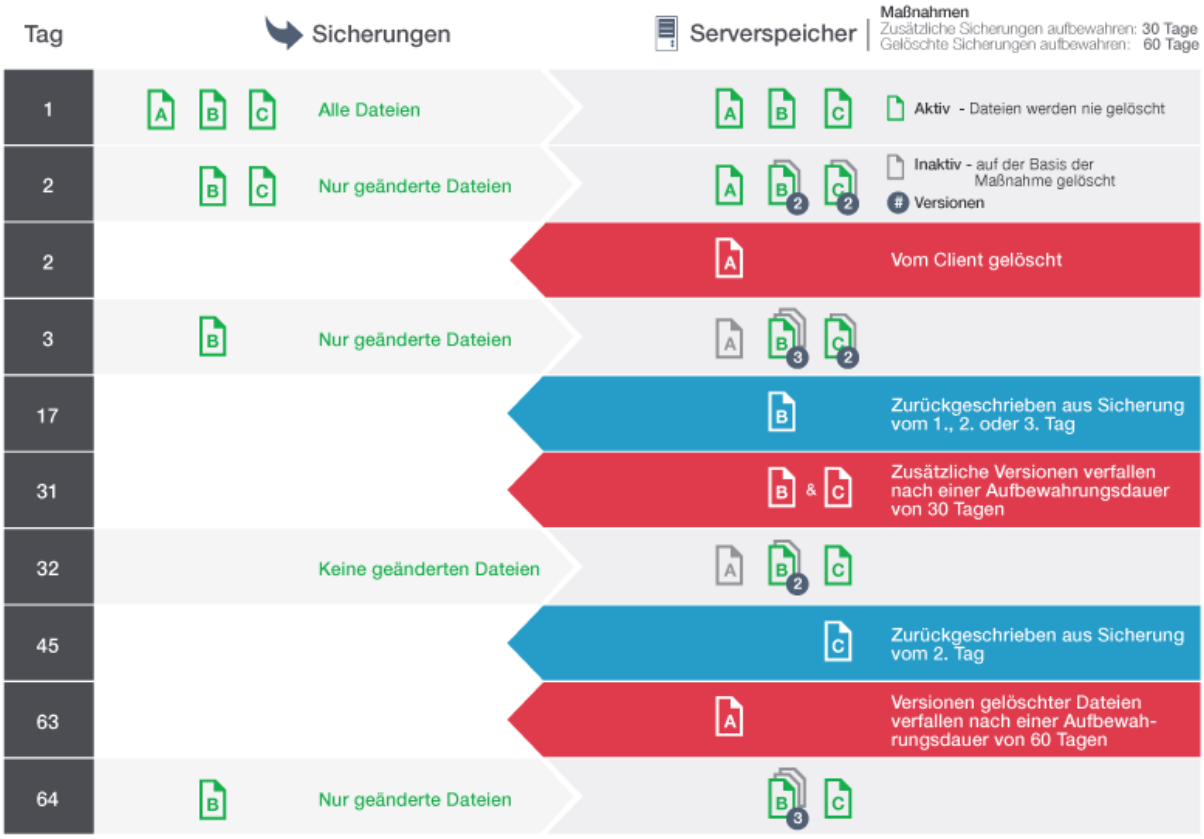
Die einfachste Möglichkeit zur Verwaltung der Datenaufbewahrung besteht in der ausschließlichen Verwendung zeitbasierter Maßnahmen. Wenn die Maßnahme nur zeitbasierte Steuerelemente enthält, werden Dateiversionen auf der Basis der Anzahl Tage aufbewahrt, nachdem die Versionen inaktiv werden.

Für eine Maßnahme, die nur auf der Zeit basiert, verwenden Sie die Steuerelemente Zusätzliche Sicherungen aufbewahren und Gelöschte Sicherungen aufbewahren. Mit diesem Typ von Maßnahme wird nicht die Anzahl Dateiversionen begrenzt. Wenn Clients häufig Sicherungen ausführen, stellen Sie sicher, dass der Serverspeicher die potenzielle Anzahl Dateiversionen handhaben kann.

Die folgende Abbildung zeigt die Handhabung von Dateien eines Clients durch den Server im Laufe der Zeit, wenn der Client täglich eine Teilsicherung ausführt.

In diesem Beispiel hat die Maßnahme die folgenden Merkmale:

- Die neueste Version einer Datei wird immer aufbewahrt, solange die Datei noch auf dem Clientsystem vorhanden ist. Die neueste Version ist die aktive Version. Dieses Merkmal ist Teil jeder Maßnahme auf dem Server.
- Die Einstellung Zusätzliche Sicherungen aufbewahren ist auf 30 Tage gesetzt. Wenn eine neuere Sicherung erstellt wird, wird eine Dateiversion inaktiv und im Serverspeicher 30 Tage lang aufbewahrt.
- Die Einstellung Gelöschte Sicherungen aufbewahren ist auf 60 Tage gesetzt. Wenn eine Datei aus dem Clientsystem gelöscht wird, werden alle Versionen der Datei im Serverspeicher inaktiv. Diese inaktiven Versionen werden 60 Tage lang aufbewahrt, nachdem die Dateiversionen inaktiv werden.



Beispiel: Aufbewahrung, wenn eine Maßnahme sowohl Versions- als auch Zeitsteuerelemente verwendet

Wenn sowohl die Versions- als auch die Zeitsteuerelemente in einer Maßnahme verwendet werden, ermöglicht dies Flexibilität bei der Handhabung der Datenaufbewahrung, hat jedoch auch Komplexität zur Folge. Studieren Sie zum besseren Verständnis der Interaktion zwischen Steuerelementen die Beispielmaßnahmen und ihre Auswirkungen auf die Aufbewahrung von Sicherungsversionen einer einzelnen Datei für die Dauer eines Monats.

Siehe Tabelle 1 und Abbildung 1. Ein Client sichert die Datei REPORT.TXT vier Mal in einem Monat (vom 23. März bis zum 23. April). Die Einstellungen in der Sicherungskopiengruppe der Verwaltungsklasse, an die REPORT.TXT gebunden ist, legen fest, wie der Server diese Sicherungsversionen handhabt. In Tabelle 2 wird gezeigt, wie sich unterschiedliche Kopiengruppeneinstellungen am 24. April (ein Tag, nachdem die Datei zuletzt gesichert wurde) auf die Versionen auswirken.

Tabelle 1. Status der Sicherungsversionen von REPORT.TXT am 24. April

Version	Erstellungsdatum	Tage seit die Version inaktiv wurde

Version	Erstellungsdatum	Tage seit die Version inaktiv wurde
Aktiv	23. April	(nicht zutreffend)
Inaktiv 1	13. April	1 (seit 13. April)
Inaktiv 2	31. März	11 (seit 13. April)
Inaktiv 3	23. März	24 (seit 31. März)

Abbildung 1. Aktive und inaktive Versionen von REPORT.TXT

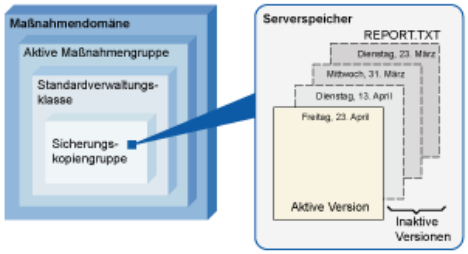


Tabelle 2. Auswirkungen der Maßnahme auf die Aufbewahrung von Sicherungsversionen für REPORT.TXT am 24. April

Sicherungen	Gelöschte Sicherungen	Zusätzliche Sicherungen aufbewahren	Gelöschte Sicherungen aufbewahren	Ergebnisse
4 Versionen	2 Versionen	60 Tage	180 Tage	Die Einstellungen Sicherungen und Zusätzliche Sicherungen aufbewahren steuern den Verfall der Versionen. Die am 23. März erstellte Version wird so lange beibehalten, bis die Datei erneut gesichert wird (und damit eine vierte inaktive Version erstellt wird) oder die Version eine Inaktivität von 60 Tagen erreicht. Wenn der Benutzer die Datei REPORT.TXT aus dem Clientdateisystem löscht, erkennt der Server die Löschung bei der nächsten vollständigen Teilsicherungsoperation durch den Client. Ab diesem Punkt sind die Einstellungen Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren auch für die Aufbewahrung wirksam. Alle Versionen sind jetzt inaktiv. Zwei der vier Versionen verfallen sofort (die Versionen vom 23. März und 31. März verfallen). Die Version vom 13. April verfällt nach einer Inaktivität von 60 Tagen (am 23. Juni). Der Server bewahrt die letzte noch verbleibende inaktive Version (die Version vom 23. April) 180 Tage lang auf, nachdem sie inaktiv wird.
Keine Begrenzung	2 Versionen	60 Tage	180 Tage	Die Einstellung Zusätzliche Sicherungen aufbewahren steuert den Verfall der Versionen. Die inaktiven Versionen (mit Ausnahme der letzten verbleibenden Version) verfallen nach einer Inaktivität von 60 Tagen. Wenn der Benutzer die Datei REPORT.TXT aus dem Clientknoten löscht, erkennt der Server die Löschung bei der nächsten vollständigen Teilsicherungsoperation durch den Client. Ab diesem Punkt sind die Einstellungen Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren auch für die Aufbewahrung wirksam. Alle Versionen sind jetzt inaktiv. Zwei der vier Versionen verfallen sofort (die Versionen vom 23. März und 31. März verfallen), da nur zwei Versionen zulässig sind. Die Version vom 13. April verfällt nach einer Inaktivität von 60 Tagen (am 22. Juni). Der Server bewahrt die letzte noch verbleibende inaktive Version (die Version vom 23. April) 180 Tage lang auf, nachdem sie inaktiv wird.

Sicherungen	Gelöschte Sicherungen	Zusätzliche Sicherungen aufbewahren	Gelöschte Sicherungen aufbewahren	Ergebnisse
Keine Begrenzung	Keine Begrenzung	60 Tage	180 Tage	Die Einstellung Zusätzliche Sicherungen aufbewahren steuert den Verfall der Versionen. Der Server lässt inaktive Versionen nicht aufgrund der maximalen Anzahl Sicherungskopien verfallen. Die inaktiven Versionen (mit Ausnahme der letzten verbleibenden Version) verfallen nach einer Inaktivität von 60 Tagen. Wenn der Benutzer die Datei REPORT.TXT aus dem Clientknoten löscht, erkennt der Server die Löschung bei der nächsten vollständigen Teilsicherungsoperation durch den Clientknoten. Ab diesem Punkt ist die Einstellung Gelöschte Sicherungen aufbewahren auch für die Aufbewahrung wirksam. Alle Versionen sind jetzt inaktiv. Drei der vier Versionen verfallen nach einer Inaktivität von jeweils 60 Tagen. Der Server bewahrt die letzte noch verbleibende inaktive Version (die Version vom 23. April) 180 Tage lang auf, nachdem sie inaktiv wird.
4 Versionen	2 Versionen	Keine Begrenzung	Keine Begrenzung	Die Einstellung Sicherungen steuert den Verfall der Versionen, bis ein Benutzer die Datei aus dem Clientknoten löscht. Der Server lässt inaktive Versionen nicht aufgrund ihres Alters verfallen. Wenn der Benutzer die Datei REPORT.TXT aus dem Clientknoten löscht, erkennt der Server die Löschung bei der nächsten vollständigen Teilsicherungsoperation durch den Clientknoten. Ab diesem Punkt steuert die Einstellung Gelöschte Sicherungen den Verfall. Alle Versionen sind jetzt inaktiv. Zwei der vier Versionen verfallen sofort (die Versionen vom 23. März und 31. März verfallen), da nur zwei Versionen zulässig sind. Der Server bewahrt die beiden verbleibenden inaktiven Versionen unbegrenzt auf.

Zugehörige Konzepte:
Vollständige Teilsicherung und partielle Teilsicherung

Interaktionen zwischen Maßnahmeneinstellungen

Zeitbasierte und versionsbasierte Maßnahmeneinstellungen interagieren, wenn sie gemeinsam in einer Verwaltungsklasse für eine Maßnahme verwendet werden. Die Häufigkeit von Clientsicherungen wirkt sich auch auf die Sicherungsversionen aus, die für einen Client gespeichert werden.

Betrachten Sie bei einem Clientsystem, für das zweimal am Tag eine Sicherung ausgeführt werden muss, die Auswirkungen der folgenden Auswahlangaben für die Maßnahme für eine Datei, die sich häufig ändert:

- Die Einstellung Zusätzliche Sicherungen aufbewahren wird auf 30 Tage gesetzt. Die Einstellung Sicherungen wird auf Keine Begrenzung gesetzt, sodass die Maßnahme die Anzahl Versionen nicht begrenzt. Nach 30 Tagen könnte der Server über 60 Sicherungsversionen der Datei verfügen, wenn sich die Datei zwischen jeder der beiden Sicherungsoperationen, die täglich ausgeführt werden, ändert. Für den Client kann wahlweise jede der 60 Versionen der vergangenen 30 Tage zurückgeschrieben werden.
- Die Einstellung Zusätzliche Sicherungen aufbewahren wird auf Keine Begrenzung und die Einstellung Sicherungen auf 30 Versionen gesetzt. Wenn sich die Datei zwischen jeder der beiden Sicherungsoperationen, die täglich ausgeführt werden, ändert, verfügt der Server nach 15 Tagen über 30 Sicherungsversionen. Nach 30 Tagen verfügt der Server immer noch nur über 30 Sicherungsversionen, da für die Anzahl Versionen eine Begrenzung festgelegt wurde. Wenn sich die Datei weiterhin zwischen jeder der beiden Sicherungsoperationen, die täglich ausgeführt werden, ändert, stammen die Sicherungsversionen unter Umständen nur aus den letzten 15 Tagen. Für den Client kann wahlweise eine der 30 Versionen, die möglicherweise nicht älter als 15 Tage sind, zurückgeschrieben werden.

Die Beispiele zeigen, dass unter der Voraussetzung, dass Sicherungsversionen für eine bestimmte Anzahl Tage verfügbar sein müssen, die einfachste Möglichkeit zur Implementierung dieser Voraussetzung in der Verwendung einer zeitbasierten Maßnahme besteht. Setzen Sie die Einstellung Zusätzliche Sicherungen aufbewahren auf die spezifische Anzahl Tage und die Einstellung Sicherungen auf Keine Begrenzung.

Die Auswirkungen des Werts Keine Begrenzung in den Maßnahmeneinstellungen sind von den anderen definierten Steuerelementen für die Maßnahme abhängig:

Zusätzliche Sicherungen aufbewahren

Wenn Sie Keine Begrenzung angeben, werden inaktive Sicherungsversionen auf der Basis der Einstellung Sicherungen oder Gelöschte Sicherungen gelöscht.

Um Clientknoten die Zurückschreibung von Dateien mit dem Stand eines bestimmten Zeitpunkts zu ermöglichen, setzen Sie die Einstellung Sicherungen oder Gelöschte Sicherungen auf Keine Begrenzung. Setzen Sie die Einstellung Zusätzliche Sicherungen aufbewahren auf die Anzahl Tage, für die Clients voraussichtlich Dateiversionen für eine mögliche Zurückschreibung nach Zeitpunkt

benötigen. Um beispielsweise Clients die Zurückschreibung von Dateien mit dem Stand eines Zeitpunkts zu ermöglichen, der 60 Tage in der Vergangenheit liegt, setzen Sie die Einstellung Zusätzliche Sicherungen aufbewahren auf 60.

Gelöschte Sicherungen aufbewahren

Wenn Sie Keine Begrenzung angeben, wird die letzte Version unbegrenzt aufbewahrt, es sei denn, die Datei wird von einem Benutzer oder einem Administrator aus dem Serverspeicher gelöscht.

Sicherungen

Wenn der Wert auf Keine Begrenzung gesetzt wird, ist möglicherweise mehr Speicher erforderlich; in einigen Situationen kann die Angabe dieses Werts jedoch erforderlich sein. Um beispielsweise Clientknoten die Zurückschreibung von Dateien mit dem Stand eines bestimmten Zeitpunkts zu ermöglichen, setzen Sie den Wert für Sicherungen auf Keine Begrenzung. Indem Versionen keine Begrenzung auferlegt wird, wird sichergestellt, dass der Server Versionen gemäß der Einstellung Zusätzliche Sicherungen aufbewahren aufbewahrt.

Gelöschte Sicherungen

Wenn der Wert auf Keine Begrenzung gesetzt wird, ist möglicherweise mehr Speicher erforderlich; in einigen Situationen kann die Angabe dieses Werts jedoch erforderlich sein. Setzen Sie beispielsweise den Wert für die Einstellung Gelöschte Sicherungen auf Keine Begrenzung, um Clients die Zurückschreibung von Dateien mit dem Stand eines bestimmten Zeitpunkts zu ermöglichen. Indem Versionen keine Begrenzung auferlegt wird, wird sichergestellt, dass der Server Versionen gemäß der Einstellung Zusätzliche Sicherungen aufbewahren aufbewahrt.

Querverweis für Felder des Operations Center und Serverbefehlsparameter

In der folgenden Tabelle sind die Felder des Operations Center mit den entsprechenden Parametern des Befehls `DEFINE COPYGROUP TYPE=BACKUP` aufgeführt.

Feldname in Sichten des Operations Center	**Parameter im Befehl `DEFINE COPYGROUP TYPE=BACKUP`**
Zusätzliche Sicherungen aufbewahren	RETEXTRA
Gelöschte Sicherungen aufbewahren	RETONLY
Sicherungen	VEREXISTS
Gelöschte Sicherungen	VERDELETED

Aktivierung der Maßnahme nach Aktualisierungen

Wenn Sie Aktualisierungen an einer Maßnahme vornehmen, werden die Aktualisierungen erst wirksam, wenn Sie die aktualisierte Maßnahme aktivieren.

Mit der Aktivierung der Maßnahmengruppe werden die durchgeführten Aktualisierungen wirksam. Beispielsweise werden die folgenden Aktualisierungstypen wirksam, wenn Sie die Maßnahmengruppe aktivieren:

- Sie definieren eine neue Maßnahmendomäne mit einer Maßnahmengruppe und einer oder mehreren Verwaltungsklassen.
- Sie fügen einer Maßnahmengruppe eine Verwaltungsklasse hinzu.
- Sie ändern die Einstellungen für die Aufbewahrung von Sicherungen in einer vorhandenen Verwaltungsklasse.

Prüfung der Maßnahmengruppe vor der Aktivierung

Im Operations Center ist die Prüfung kein separater Schritt. Wenn Sie Befehle verwenden, ist die Prüfung ein optionaler Befehl, der Ihnen die Gelegenheit gibt, eine Vorschau der Auswirkungen der Aktivierung einer geänderten Maßnahmengruppe anzuzeigen. Wenn Sie eine Maßnahmengruppe prüfen, meldet der Server Bedingungen zurück, die beim Aktivieren der Maßnahmengruppe Probleme verursachen können. Die Prüfung schlägt fehl, wenn die Maßnahmengruppe keine Standardverwaltungsklasse enthält. Die Prüfung hat Warnungen zur Folge, wenn eine der in Tabelle 1 aufgeführten Bedingungen erfüllt ist.

Tabelle 1. Bedingungen, die während der Prüfung der Maßnahmengruppe Warnungen zur Folge haben

Bedingung	**Grund für Warnung**
Die für Sicherungs-, Archivierungs- oder Umlagerungsoperationen angegebenen Speicherziele sind keine definierten Speicherpools.	Ein Speicherpool muss vorhanden sein, bevor er als Ziel angegeben werden kann.
Ein für Sicherungs-, Archivierungs- oder Umlagerungsoperationen angegebenes Speicherziel ist ein Kopienspeicherpool oder ein Pool für aktive Daten.	Das Speicherziel muss ein primärer Speicherpool sein.
Die Standardverwaltungsklasse enthält keine Sicherungs- oder Archivierungseinstellungen.	Wenn die Standardverwaltungsklasse keine Sicherungs- oder Archivierungseinstellungen enthält, werden alle Dateien, die an die Standardverwaltungsklasse gebunden sind, nicht gesichert oder archiviert.

Bedingung	Grund für Warnung
In der aktuellen aktiven Maßnahmengruppe ist eine Verwaltungsklasse angegeben, die in der Maßnahmengruppe, die geprüft wird, nicht definiert ist.	Wenn Sie Dateien sichern, die an eine Verwaltungsklasse gebunden wurden, die in der aktiven Maßnahmengruppe nicht mehr vorhandene ist, werden Sicherungsversionen erneut an die Standardverwaltungsklasse gebunden. Wenn die Verwaltungsklasse, an die eine Archivierungskopie gebunden ist, nicht mehr vorhanden ist und die Standardverwaltungsklasse keine Archivierungseinstellungen enthält, verwendet der Server für die Aufbewahrung der Archivierungskopie den Aufbewahrungszeitraum für Archivierung. Der Aufbewahrungszeitraum für Archivierung wird für eine Maßnahmendomäne definiert und diese Einstellung wird nur verwendet, wenn zur Verwaltung einer Archivierungskopie keine andere Maßnahmeneinstellung verfügbar ist.
Die aktuelle aktive Maßnahmengruppe enthält Sicherungseinstellungen, die in der Maßnahmengruppe, die geprüft wird, nicht definiert sind.	Wenn ein Client eine Datei sichert und die Verwaltungsklasse, an die die Datei gebunden ist, keine Sicherungseinstellungen mehr enthält, werden die Sicherungsversionen gemäß der Standardverwaltungsklasse verwaltet. Wenn die Standardverwaltungsklasse keine Sicherungseinstellungen enthält, verwendet der Server den Aufbewahrungszeitraum für Sicherung zur Verwaltung von Dateiversionen. Die Datei wird jedoch bei der nächsten Sicherungsoperation nicht gesichert. Der Aufbewahrungszeitraum für Sicherung wird für eine Maßnahmendomäne definiert und diese Einstellung wird nur verwendet, wenn zur Verwaltung einer Sicherungsversion keine andere Maßnahmeneinstellung verfügbar ist.
Eine Verwaltungsklasse gibt an, dass eine Sicherungsversion vorhanden sein muss, bevor eine Datei aus einem Clientknoten umgelagert werden kann, die Verwaltungsklasse enthält jedoch keine Sicherungseinstellungen.	Diese Warnung gilt nur, wenn Sie das Produkt IBM Spectrum Protect for Space Management verwenden. Die Konflikte innerhalb der Verwaltungsklasse können Probleme für IBM Spectrum Protect for Space Management-Clients zur Folge haben.

Aktivierung der Maßnahmengruppe

Wenn Sie eine Maßnahmengruppe aktivieren, prüft der Server den Inhalt der Maßnahmengruppe und kopiert die Maßnahmengruppe als aktive Maßnahmengruppe. Um den Inhalt der aktiven Maßnahmengruppe später ändern zu können, muss eine weitere Maßnahmengruppe erstellt oder geändert und anschließend aktiviert werden.

Einige Aktualisierungen an einer Maßnahme werden sofort wirksam, wenn die Maßnahme aktiviert wird, einige andere Aktualisierungen hingegen nicht:

- Aktualisierungen der Einstellungen Zusätzliche Sicherungen aufbewahren und Gelöschte Sicherungen aufbewahren werden sofort auf die Daten angewendet, die bereits im Serverspeicher vorhanden sind, sowie auf zukünftige Sicherungen.

  Bei der Verwendung von Befehlen betrifft dies die Parameter RETEXTRA und RETONLY für den Befehl DEFINE COPYGROUP oder UPDATE COPYGROUP.

- Aktualisierungen der Einstellungen Sicherungen und Gelöschte Sicherungen werden für Clientdaten erst wirksam, wenn die Clients die nächste Sicherungsoperation ausführen.

  Bei der Verwendung von Befehlen betrifft dies die Parameter VEREXISTS und VERDELETED für den Befehl DEFINE COPYGROUP oder UPDATE COPYGROUP.

Einschränkungen für Server, die die Funktion für den Datenaufbewahrungsschutz verwenden

Wenn die Funktion für den Datenaufbewahrungsschutz aktiv ist, gelten weitere Regeln, wenn Sie eine Maßnahmengruppe prüfen und aktivieren. Die Funktion für den Datenaufbewahrungsschutz wird aktiviert, indem der Befehl SET ARCHIVERETENTIONPROTECTION auf einem Server ausgegeben wird, der noch nicht über Clientdaten verfügt.

Wenn der Datenaufbewahrungsschutz für einen Server aktiv ist, müssen weitere Regeln erfüllt sein, bevor die Maßnahme aktiviert wird:

- Wenn eine Verwaltungsklasse in der aktiven Maßnahmengruppe vorhanden ist, muss eine Verwaltungsklasse mit demselben Namen in der Maßnahmengruppe vorhanden sein, die aktiviert wird.
- Alle Verwaltungsklassen in der Maßnahmengruppe, die aktiviert wird, müssen Einstellungen für den Aufbewahrungszeitraum für Archivierung enthalten.
- Wenn die aktive Maßnahmengruppe Einstellungen für den Aufbewahrungszeitraum für Archivierung in einer Verwaltungsklasse enthält, muss die Maßnahmengruppe, die aktiviert wird, Werte für den Aufbewahrungszeitraum für Archivierung enthalten, die mindestens so groß wie die entsprechenden Werte in der aktiven Maßnahmengruppe sind.

Wenn der Server ein verwalteter Server in einer unternehmensweiten Konfiguration ist, empfängt der Server möglicherweise Maßnahmenaktualisierungen von dem Server, der als Konfigurationsmanager definiert ist. Maßnahmenaktualisierungen, die der verwaltete Server vom Konfigurationsmanager empfängt, müssen ebenfalls die vorhergehenden Regeln erfüllen.

Zugehörige Konzepte:

Unternehmensweite Konfiguration (Version 7.1.1)

Zugehörige Verweise:

SET ARCHIVERETENTIONPROTECTION (Aufbewahrungsschutz für Daten aktivieren)

Maßnahme anpassen

Sie können vorhandene Maßnahmen anpassen, um neue oder überarbeitete Datenaufbewahrungsanforderungen Ihres Unternehmens zu erfüllen. Eine typische Möglichkeit zum Starten der Maßnahmenanpassung ist das Ändern einer Maßnahmendomäne oder das Kopieren einer vorhandenen Maßnahmendomäne.

Informationen zu diesem Vorgang

Die wichtigsten Maßnahmeneinstellungen befinden sich in Verwaltungsklassen. In Verwaltungsklassen können Sie sowohl die Anzahl Sicherungsversionen als auch die Anzahl Tage für die Aufbewahrung von Sicherungsversionen im Serverspeicher steuern. Wenn Sie beide Steuerungstypen verwenden, ist die Maßnahme komplexer. Wenn die Steuerung nur über die Anzahl Tage für die Aufbewahrung von Sicherungsversionen erfolgt, können Sie einfacher definieren, wie lange gesicherte Daten aufbewahrt werden.

Stellen Sie sicher, dass die Standardverwaltungsklasse in einer Maßnahmendomäne geeignete Datenaufbewahrungseinstellungen für die meisten oder alle Clients hat, die der Domäne zugeordnet sind. Die Aufbewahrungseinstellungen in der Standardverwaltungsklasse werden auf die Daten angewendet, wenn für Clientoperationen keine Verwaltungsklasse angegeben ist.

Sie können Aktualisierungen an einer Maßnahme durchführen und die Änderungen für einen späteren Zeitpunkt speichern. Wenn die Änderungen am Entwurf abgeschlossen sind, können Sie die aktualisierte Maßnahmengruppe aktivieren, damit die Änderungen wirksam werden.

Vorgehensweise

1. Klicken Sie auf der Seite Übersicht im Operations Center auf das Menü Services.
2. Wählen Sie die Maßnahmendomäne aus und klicken Sie auf Details. Klicken Sie auf Maßnahmengruppen.
3. Klicken Sie auf die Umschaltfläche Konfigurieren, um die Einstellungen aktualisieren zu können.
4. Passen Sie die Einstellungen in der Verwaltungsklasse an.
    a. Geben Sie Auswahlangaben für Sicherungsservices an. Aktualisieren Sie beispielsweise die folgenden Einträge, sodass inaktive Sicherungsversionen für die Clients 30 Tage lang aufbewahrt werden:
        - Sicherungen: Keine Begrenzung
        - Zusätzliche Sicherungen aufbewahren: 30 Tage
        - Gelöschte Sicherungen: 1
        - Gelöschte Sicherungen aufbewahren: Keine Begrenzung

    b. Optional: Geben Sie Auswahlangaben für Archivierungsservices an. Ändern Sie beispielsweise die Einstellung Archivierungen aufbewahren in 1 Jahr.
    c. Klicken Sie auf Sichern.
5. Optional: Klicken Sie auf +Verwaltungsklasse, um eine Verwaltungsklasse hinzuzufügen.
    a. Geben Sie Auswahlangaben für Basiseinstellungen an und klicken Sie auf Hinzufügen.
    b. Passen Sie weitere Einstellungen in der neuen Verwaltungsklasse an. Geben Sie für Sicherungsservices Auswahlangaben in den folgenden Spalten an: Sicherungsziel, Sicherungen, Zusätzliche Sicherungen aufbewahren, Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren. Geben Sie für Archivierungsservices Auswahlangaben in den Spalten Archivierungsziel und Archivierungen aufbewahren an.
    c. Klicken Sie auf Sichern.
6. Stellen Sie sicher, dass in der Spalte Standard eine entsprechende Verwaltungsklasse als Standardverwaltungsklasse ausgewählt ist. Die Aufbewahrungseinstellungen in der Standardverwaltungsklasse werden angewendet, wenn für Clientoperationen keine Verwaltungsklasse angegeben ist. Eine Verwaltungsklasse kann angegeben werden, wenn eine Clientoperation ausgeführt wird. Eine Verwaltungsklasse kann auch in einer Clientoptionsdatei auf dem Clientsystem oder in einer Clientoptionsgruppe, die auf dem Server definiert ist, angegeben werden.
7. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.
8. Ordnen Sie der neuen Maßnahmendomäne Clientknoten zu, indem Sie entweder vorhandene Clientknoten aktualisieren oder neue Knoten registrieren.
    - Um der Maßnahmendomäne neue Clients hinzuzufügen, klicken Sie auf +Client.
    - Um einen vorhandenen Client in die Maßnahmendomäne zu versetzen, wählen Sie den Client aus, klicken Sie auf Details und klicken Sie dann auf die Registerkarte Merkmale. Wählen Sie die neue Maßnahmendomäne aus und klicken Sie auf Sichern.

    Die Datenaufbewahrung für den Client, den Sie der Maßnahmendomäne zuordnen, wird jetzt durch diese Maßnahme gesteuert. Voraussetzung: Wenn ein Client bei der Zuordnung zu einer neuen Domäne aktiv ist, müssen Sie den Client stoppen und erneut starten, damit die Änderung wirksam wird.

Zugehörige Tasks:

Clientoperationen über Clientoptionsgruppen steuern

Maßnahme durch Kopieren einer vorhandenen Maßnahme erstellen

Sie können neue Maßnahmen erstellen, indem Sie eine vorhandene Maßnahme kopieren und dann die Teile aktualisieren, die geändert werden sollen.

Vorgehensweise

Sie können eine Maßnahme erstellen, indem Sie eine Maßnahmendomäne kopieren, die Verwaltungsklassen aktualisieren und dann der neuen Domäne Clients zuordnen.

1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder.
2. Kopieren Sie eine Maßnahmendomäne mit dem Befehl COPY DOMAIN. Kopieren Sie beispielsweise die Standardmaßnahmendomäne STANDARD in eine neue Maßnahmendomäne, NEWDOMAIN:

   ```
   copy domain standard newdomain
   ```

   Mit dieser Operation werden die Maßnahmendomäne und alle zugehörigen Maßnahmengruppen und Verwaltungsklassen kopiert. In diesem Beispiel werden mit der Operation die folgenden Elemente in die Maßnahmendomäne NEWDOMAIN kopiert:
   - Eine Maßnahmengruppe mit dem Namen STANDARD
   - Die Verwaltungsklasse mit dem Namen STANDARD, die sich in der Maßnahmengruppe STANDARD befindet
   - Die Kopiengruppen, die in der Verwaltungsklasse STANDARD enthalten sind:
     - Die Sicherungskopiengruppe mit dem Namen STANDARD
     - Die Archivierungskopiengruppe mit dem Namen STANDARD
3. Klicken Sie auf der Seite Übersicht im Operations Center auf das Menü Services.
4. Wählen Sie die neue Maßnahmendomäne aus und klicken Sie auf Details. Klicken Sie auf Maßnahmengruppen.
5. Klicken Sie auf die Umschaltfläche Konfigurieren, um die Einstellungen aktualisieren zu können.
6. Passen Sie die Einstellungen in den Verwaltungsklassen an.
   a. Geben Sie Auswahlangaben für Sicherungsservices an. Aktualisieren Sie beispielsweise die folgenden Einträge, sodass inaktive Sicherungsversionen für die Clients 30 Tage lang aufbewahrt werden:
      - Sicherungen: Keine Begrenzung
      - Zusätzliche Sicherungen aufbewahren: 30 Tage
      - Gelöschte Sicherungen: 1
      - Gelöschte Sicherungen aufbewahren: Keine Begrenzung

   b. Optional: Geben Sie Auswahlangaben für Archivierungsservices an. Ändern Sie beispielsweise die Einstellung Archivierungen aufbewahren in 1 Jahr.
   c. Klicken Sie auf Sichern.
7. Optional: Nehmen Sie weitere Aktualisierungen und Hinzufügungen vor, wie beispielsweise das Hinzufügen einer Verwaltungsklasse.
   a. Klicken Sie auf +Verwaltungsklasse, um eine Verwaltungsklasse hinzuzufügen. Geben Sie Auswahlangaben für Basiseinstellungen an und klicken Sie auf Hinzufügen.
   b. Passen Sie weitere Einstellungen in der neuen Verwaltungsklasse an. Geben Sie für Sicherungsservices Auswahlangaben in den folgenden Spalten an: Sicherungsziel, Sicherungen, Zusätzliche Sicherungen aufbewahren, Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren. Geben Sie für Archivierungsservices Auswahlangaben in den Spalten Archivierungsziel und Archivierungen aufbewahren an.
   c. Klicken Sie auf Sichern.
8. Wählen Sie in der Spalte Standard die Standardverwaltungsklasse aus, die von Clients verwendet wird. Klicken Sie auf Sichern. Die Aufbewahrungseinstellungen in der Standardverwaltungsklasse werden angewendet, wenn für Clientoperationen keine Verwaltungsklasse angegeben ist. Eine Verwaltungsklasse kann angegeben werden, wenn eine Clientoperation ausgeführt wird. Eine Verwaltungsklasse kann auch in einer Clientoptionsdatei auf dem Clientsystem oder in einer Clientoptionsgruppe, die auf dem Server definiert ist, angegeben werden.
9. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.
10. Ordnen Sie der neuen Maßnahmendomäne Clientknoten zu, indem Sie entweder vorhandene Clientknoten aktualisieren oder neue Knoten registrieren.
    - Um der Maßnahmendomäne neue Clients hinzuzufügen, klicken Sie auf +Client.
    - Um einen vorhandenen Client in die Maßnahmendomäne zu versetzen, wählen Sie den Client aus, klicken Sie auf Details und klicken Sie dann auf die Registerkarte Merkmale. Wählen Sie die neue Maßnahmendomäne aus und klicken Sie auf Sichern.

    Die Datenaufbewahrung für den Client, den Sie der Maßnahmendomäne zuordnen, wird jetzt durch diese Maßnahme gesteuert. Wenn Sie beispielsweise das Beispiel in Schritt 6 implementiert haben, werden inaktive Sicherungsversionen für die Clients standardmäßig 30 Tage lang aufbewahrt.
    Voraussetzung: Wenn ein Client bei der Zuordnung zu einer neuen Domäne aktiv ist, müssen Sie den Client stoppen und erneut starten, damit die Änderung wirksam wird.

Zugehörige Tasks:
Clientoperationen über Clientoptionsgruppen steuern

Maßnahmendomäne erstellen

Möglicherweise möchten Sie für jeden Typ von Client, der vom Server geschützt wird, eine neue Maßnahmendomäne erstellen. Möglicherweise möchten Sie auch die Zuständigkeit für Clients auf mehrere Administratoren verteilen, indem Sie Ihnen Berechtigung für bestimmte Maßnahmendomänen erteilen.

Informationen zu diesem Vorgang

Die Erstellung einer neuen Maßnahmendomäne kann unter den folgenden Umständen hilfreich sein:

- Anwendungen, Systeme oder virtuelle Maschinen erfordern unterschiedliche Datenaufbewahrungseinstellungen. Für jeden Clienttyp können Sie eine Maßnahmendomäne mit einer für diesen Typ geeigneten Standardmaßnahme erstellen.
- Administratoren sind für unterschiedliche Gruppen von Clients verantwortlich. Für jeden Administrator können Sie eine Maßnahmendomäne erstellen, der Sie die Clients zuordnen, die von diesem Administrator verwaltet werden sollen.

Vorgehensweise

Die folgenden Schritte sind eine Zusammenfassung der Vorgehensweise beim Erstellen einer Maßnahmendomäne.

1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder.
2. Definieren Sie eine Maßnahme mit dem Befehl DEFINE DOMAIN.
3. Definieren Sie eine Maßnahmengruppe für die Domäne mit dem Befehl DEFINE POLICYSET.
4. Klicken Sie auf der Seite Übersicht im Operations Center auf das Menü Services.
5. Wählen Sie die Maßnahmendomäne aus und klicken Sie auf Details. Klicken Sie auf Maßnahmengruppen.
6. Klicken Sie auf die Umschaltfläche Konfigurieren, um die Einstellungen aktualisieren zu können.
7. Klicken Sie auf +Verwaltungsklasse, um eine Verwaltungsklasse hinzuzufügen. Geben Sie Auswahlangaben für Basiseinstellungen an und klicken Sie auf Hinzufügen.
8. Optional: Passen Sie weitere Einstellungen in der neuen Verwaltungsklasse an:
    a. Geben Sie für Sicherungsservices Auswahlangaben in den folgenden Spalten an: Sicherungsziel, Sicherungen, Zusätzliche Sicherungen aufbewahren, Gelöschte Sicherungen und Gelöschte Sicherungen aufbewahren.
    b. Geben Sie für Archivierungsservices Auswahlangaben in den Spalten Archivierungsziel und Archivierungen aufbewahren an.
    c. Klicken Sie auf Sichern.
9. Optional: Klicken Sie auf +Verwaltungsklasse, um weitere Verwaltungsklassen hinzuzufügen.
10. Stellen Sie sicher, dass in der Spalte 'Standard' eine Standardverwaltungsklasse ausgewählt ist.
11. Aktivieren Sie die Maßnahmengruppe, indem Sie auf Aktivieren klicken.
12. Ordnen Sie der neuen Maßnahmendomäne Clients zu. Klicken Sie in der Menüleiste des Operations Center auf Clients.
    - Um der Maßnahmendomäne neue Clients hinzuzufügen, klicken Sie auf +Client.
    - Um einen vorhandenen Client in die Maßnahmendomäne zu versetzen, wählen Sie den Client aus, klicken Sie auf Details und klicken Sie dann auf die Registerkarte Merkmale. Wählen Sie die neue Maßnahmendomäne aus und klicken Sie auf Sichern.

Zugehörige Verweise:
DEFINE DOMAIN (Neue Maßnahmendomäne definieren)
DEFINE POLICYSET (Maßnahmengruppe definieren)

Clientoperationen über Clientoptionsgruppen steuern

Mithilfe von Clientoptionsgruppen können Sie die Verarbeitungsoptionen, die Clients für Operationen wie Sicherungen verwenden, zentral steuern. Mithilfe von Clientoptionsgruppen kann sichergestellt werden, dass Daten konsistent gemäß Ihren Anforderungen geschützt werden. Eine Clientoptionsgruppe kann Optionen in einer lokalen Clientoptionsdatei überschreiben oder Optionen hinzufügen, die unter Umständen nicht in der lokalen Clientoptionsdatei vorhanden sind.

Informationen zu diesem Vorgang

Indem Clientoptionsgruppen erstellt und zugeordnet werden, müssen Sie die lokale Clientoptionsdatei weniger häufig aktualisieren und der Aufwand für Sie bzw. Ihre Benutzer wird geringer.

Sie können beispielsweise eine Clientoptionsgruppe definieren, um eine Einschluss-/Ausschlussliste anzugeben, in der festgelegt ist, welche Daten gesichert werden, welche Daten von der Sicherung ausgeschlossen sind und welche Verwaltungsklassen zur Verwaltung der Datenaufbewahrung verwendet werden. Andere Clientoptionen, die gegebenenfalls für die zentrale Steuerung in einer Clientoptionsgruppe hilfreich sind, sind die Optionen compression und deduplication.

Sie können Clientoptionsgruppen für Clients mit ähnlichen Anforderungen erstellen, wie beispielsweise Clients unter demselben Betriebssystem, Clients, die dieselbe Software verwenden, oder Clients, die von einer bestimmten Abteilung verwendet werden. Sie können beispielsweise Clientoptionsgruppen für Windows-Workstations oder für die Lohnbuchhaltung erstellen. Nachdem die Clientoptionsgruppe erstellt wurde, ordnen Sie die Clientoptionsgruppe allen Clients desselben Typs zu.

In einer Clientoptionsgruppe auf dem Server können nicht alle Clientoptionen angegeben werden. Informationen dazu, welche Clientoptionen zentral in einer Clientoptionsgruppe gesteuert werden können, finden Sie in Clientoptionen, die vom Server definiert werden können.

Vorgehensweise

1. Definieren Sie eine Clientoptionsgruppe mit dem Befehl DEFINE CLOPTSET. Um beispielsweise eine Clientoptionsgruppe mit dem Namen PAYROLLBACKUP zu definieren, geben Sie den folgenden Befehl aus:

   ```
   define cloptset payrollbackup description='Sicherungsoptionen für die Lohnbuchhaltung'
   ```

2. Fügen Sie der Clientoptionsgruppe mit dem Befehl DEFINE CLIENTOPT Clientoptionen hinzu. Angenommen, die Optionen include und exclude sollen der Clientoptionsgruppe mit dem Namen PAYROLLBACKUP hinzugefügt werden, um die folgenden Ziele zu erreichen:
   - Temporäre Internetverzeichnisdateien von Sicherungsoperationen ausschließen
   - Alle Dateien im Verzeichnis C:\Data und die zugehörigen Unterverzeichnisse in eine Sicherung einschließen und die Dateien für die Datenaufbewahrung der Verwaltungsklasse PAYCLASS zuordnen

   Geben Sie die folgenden Befehle aus:

   ```
   define clientopt payrollbackup inclexcl "exclude.dir '*:\...\Temporäre Internet-Dateien'"
   define clientopt payrollbackup inclexcl "include C:\Data\...\* payclass"
   ```

3. Um einem Client eine Clientoptionsgruppe zuzuordnen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
   b. Wählen Sie einen Client aus und klicken Sie auf Details.
   c. Klicken Sie auf Merkmale.
   d. Wählen Sie im Bereich 'Allgemein' eine Optionsgruppe aus und klicken Sie auf Sichern.

Zugehörige Verweise:
DEFINE CLOPTSET (Clientoptionsgruppennamen definieren)
DEFINE CLIENTOPT (Option für eine Optionsgruppe definieren)
Clientoption 'compression'
Clientoption 'deduplication'

Speicher konfigurieren

Wählen Sie abhängig von der erforderlichen Speicherfunktionalität den korrekten Typ von Speichermedien aus. Optimieren und steuern Sie Ihre Speicherpools für verschiedene Typen von Daten.

- Speicherpooltypen
  Um den Speicherpooltyp bestimmen zu können, der Ihre Speicheranforderungen am besten erfüllt, sollten Sie die Merkmale jedes Speicherpooltyps bewerten.
- Datendeduplizierungsoptionen
  Verwenden Sie die Inline-Datendeduplizierung, um Daten gleichzeitig zu deduplizieren und in einen Containerspeicherpool zu schreiben. Verwenden Sie die nachgeordnete Datendeduplizierung, um doppelte Daten aus Speicherpools mit sequenziellem Zugriff (FILE) zu löschen.
- Speichereinheiten konfigurieren
  Konfigurieren Sie Speichereinheiten, indem Sie Einheiten anschließen, Einheitentreiber konfigurieren und die Objekte erstellen, die die Einheiten für den Server darstellen.
- Verzeichniscontainerspeicherpool für die Datenspeicherung konfigurieren
  Sie können Verzeichniscontainerspeicherpools für die Verwendung der Inline-Datendeduplizierung zum Speichern deduplizierter Daten konfigurieren.
- Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren
  Sie können deduplizierte Daten und nicht deduplizierte Daten in einem Cloud-Containerspeicherpool speichern und die Daten nach Bedarf zurückschreiben. Sie können Cloud-Containerspeicherpools für die Verwendung einer der folgenden Service-Provider und Protokolle konfigurieren: Amazon Web Services (AWS) mit Simple Storage Service (S3), IBM® Cloud Object Storage mit Swift oder S3 (und IBM SoftLayer), Microsoft Azure und OpenStack mit Swift unter Verwendung von Keystone Version 1 oder Version 2. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.
- Leistung für Cloudobjektspeicher optimieren
  Sie können IBM Spectrum Protect so konfigurieren, dass Daten während der Datenaufnahme vorübergehend in einem oder mehreren lokalen Speicherpoolverzeichnissen gespeichert werden. Die Daten werden dann aus dem lokalen Speicher in die Cloud übertragen. Auf diese Art und Weise können Sie die Datensicherungs- und -archivierungsleistung verbessern.
- Speicherbereich in Containerspeicherpools verwalten
  Nachdem Sie IBM Spectrum Protect konfiguriert und Speicherbereich hinzugefügt haben, müssen Sie Ihre Daten und Ihren Speicherbereich im Speicherpool effektiv verwalten, um die ordnungsgemäße Funktion zu gewährleisten. Maximieren Sie Ihren Speicherbereich und die Serverleistung mithilfe von Containerspeicherpools.
- Speicherpoolcontainer prüfen
  Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.
- Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten
  Für den IBM Spectrum Protect-Server können viele Typen von Speicher verwendet werden. Wenn Sie Plattenblockspeicher, Solid-State-Laufwerke (SSDs) oder an das Netz angeschlossene Dateisysteme als Serverspeicher verwenden, müssen Sie sicherstellen, dass der Speicher die Voraussetzungen erfüllt.

Speicherpooltypen

Um den Speicherpooltyp bestimmen zu können, der Ihre Speicheranforderungen am besten erfüllt, sollten Sie die Merkmale jedes Speicherpooltyps bewerten.

Bewerten Sie jeden Speicherpooltyp mithilfe der folgenden Tabelle.

Speicherpooltyp	Beschreibung	Verwendungen
Verzeichniscontainerspeicherpool	Ein primärer Speicherpool, der von einem Server zum Speichern von Daten verwendet wird. Daten, die in Verzeichniscontainerspeicherpools gespeichert werden, verwenden sowohl die Inline-Datendeduplizierung als auch die clientseitige Datendeduplizierung.	Verwenden Sie diesen Speicherpooltyp bei der Inline-Datendeduplizierung. Durch die Verwendung von Verzeichniscontainerspeicherpools entfällt die Notwendigkeit zur Datenträgerkonsolidierung, wodurch die Serverleistung verbessert und die Kosten der Speicherhardware gesenkt werden. Sie können diesen Speicherpooltyp nicht für Speicherpoolsicherungs-, Umlagerungs-, Konsolidierungs-, Import- oder Exportoperationen verwenden.
Cloud-Containerspeicherpool	Ein primärer Speicherpool, der von einem Server zum Speichern von Daten verwendet wird. Verwenden Sie Cloud-Containerspeicherpools, um Daten in einem objektspeicherbasierten Cloudspeicherprovider zu speichern. Daten, die in Cloud-Containerspeicherpools gespeichert werden, verwenden sowohl die Inline-Datendeduplizierung als auch die clientseitige Datendeduplizierung.	Das Speichern von Daten in Cloud-Containerspeicherpools ermöglicht es Ihnen, die von Clouds gebotenen Vorteile der Kosten pro Einheit zusammen mit der vom Cloudspeicher bereitgestellten Skalierungsfunktionalität zu nutzen. Sie können diesen Speicherpooltyp nicht für Speicherpoolsicherungs-, Umlagerungs-, Konsolidierungs-, Verschlüsselungs-, Import- oder Exportoperationen verwenden.
Speicherpool mit wahlfreiem Zugriff	Eine Gruppe von Datenträgern, die der Server zum Speichern von Sicherungsversionen von Dateien, Dateien, die Archivierungskopien sind, und Dateien, die aus Clientknoten umgelagert werden, verwendet. Dateien werden auf DISK-Einheiten gespeichert.	Verwenden Sie diesen Speicherpooltyp, um eine Kopie Ihrer Daten auf DISK-Einheiten aufzubewahren. Sie können Daten in diese Speicherpools und aus diesen Speicherpools umlagern.
Speicherpool mit sequenziellem Zugriff	Eine Gruppe von Datenträgern, die der Server zum Speichern von Sicherungsversionen von Dateien, Dateien, die Archivierungskopien sind, und Dateien, die aus Clientknoten umgelagert werden, verwendet. Dateien werden auf Band- oder FILE-Einheiten gespeichert. Daten, die in Speicherpools mit sequenziellem Zugriff gespeichert werden, verwenden sowohl die nachgeordnete Datendeduplizierung als auch die clientseitige Datendeduplizierung.	Verwenden Sie diesen Speicherpooltyp, um eine Kopie Ihrer Daten auf TAPE-Einheiten aufzubewahren. Sie können Daten in diesen Typ von Speicherpool umlagern.
Kopienspeicherpool	Eine benannte Gruppe von Datenträgern, die Kopien von Dateien enthalten, die in primären Speicherpools gespeichert sind. Kopienspeicherpools werden nur zum Sichern der Daten verwendet, die in primären Speicherpools gespeichert sind. Ein Kopienspeicherpool kann nicht als Ziel für eine Sicherungskopiengruppe, eine Archivierungskopiengruppe oder eine Verwaltungsklasse (für speicherverwaltete Dateien) verwendet werden.	Verwenden Sie Kopienspeicherpools, um über eine Kopie der aktiven und inaktiven Daten zu verfügen, die nach einem Katastrophenfall oder einem Ausfall in einen primären Speicherpool zurückgeschrieben werden kann. Sie können keine Inline-Datendeduplizierung, Komprimierung, Replikation oder Datendeduplizierung mit diesem Typ von Speicherpool verwenden.

Speicherpooltyp	Beschreibung	Verwendungen
Containerkopienspeicherpool	Eine Gruppe von Banddatenträgern, die eine Kopie der deduplizierten Speicherbereiche enthalten, die in einem Verzeichniscontainerspeicherpool gespeichert sind. Containerkopienspeicherpools werden nur zum Schützen der Daten verwendet, die in Verzeichniscontainerspeicherpools gespeichert sind. Containerkopienspeicherpools werden zum Reparieren einer Beschädigung in einem Verzeichniscontainerspeicherpool oder zum Zurückschreiben eines Verzeichniscontainerspeicherpools verwendet, wenn ein Katastrophenfall eintritt. Containerkopienspeicherpools sind auf sequenziellen Datenträgern gespeichert.	Verwenden Sie Containerkopienspeicherpools, um Kopien von Verzeichniscontainerspeicherpools vor Ort oder an einem anderen Standort aufzubewahren. Beschädigte Daten in Verzeichniscontainerspeicherpools können mithilfe der deduplizierten Speicherbereiche in einem Containerkopienspeicherpool repariert werden.
Speicherpool für aktive Daten	Eine benannte Gruppe von Speicherpooldatenträgern, die nur aktive Versionen von Clientsicherungsdaten enthalten.	Verwenden Sie Speicherpools für aktive Daten, um nach einem Katastrophenfall oder Ausfall nur aktive Daten in primäre Speicherpools zurückzuschreiben. Wenn nur aktive Daten zurückgeschrieben werden, können Sie Clientdaten schneller zurückschreiben und verwenden weniger Bandbreite. Sie können keine Inline-Datendeduplizierung, Komprimierung, Replikation oder Datendeduplizierung mit diesem Typ von Speicherpool verwenden.

Vergleichen Sie anhand der folgenden Tabelle die Speicherpoolfunktionalität und wählen Sie abhängig von Ihren Speicheranforderungen den Speicherpool aus, der Ihre Geschäftsanforderungen am besten erfüllt.

Benutzerziel	Verzeichniscontainerspeicherpool	Cloud-Containerspeicherpool	Speicherpool mit wahlfreiem Zugriff	Speicherpool mit sequenziellem Zugriff	Kopienspeicherpool	Containerkopienspeicherpool	Speicherpool für aktive Daten
Schützen von Speicherpooldaten mithilfe der Knotenreplikation	✓		✓	✓	✓		✓
Reduzieren des Speicherbedarfs mithilfe der Inline-Komprimierung	✓	✓					
Reduzieren des Speicherbedarfs mithilfe der Inline-Datendeduplizierung	✓	✓					
Reduzieren des Speicherbedarfs mithilfe der clientseitigen Datendeduplizierung	✓	✓		✓			
Reduzieren des Speicherbedarfs mithilfe der nachgeordneten Datendeduplizierung				✓			

Benutzerziel	Verzeichniscontainerspeicherpool	Cloud-Containerspeicherpool	Speicherpool mit wahlfreiem Zugriff	Speicherpool mit sequenziellem Zugriff	Kopienspeicherpool	Containerkopienspeicherpool	Speicherpool für aktive Daten
Schützen von Speicherpooldaten mithilfe von Speicherpoolschutz	✓					✓	
Sichern von Speicherpooldaten mithilfe von Kopienspeicherpools auf Platte oder Band			✓	✓			
Speichern von Daten in einer Cloud		✓					

Datendeduplizierungsoptionen

Verwenden Sie die Inline-Datendeduplizierung, um Daten gleichzeitig zu deduplizieren und in einen Containerspeicherpool zu schreiben. Verwenden Sie die nachgeordnete Datendeduplizierung, um doppelte Daten aus Speicherpools mit sequenziellem Zugriff (FILE) zu löschen.

Für die Inline-Datendeduplizierung müssen Verzeichniscontainerspeicherpools oder Cloud-Containerspeicherpools verwendet werden. Durch die Verwendung von Verzeichniscontainer- oder Cloud-Containerspeicherpools verringert sich die Notwendigkeit zur Offlinereorganisation, wodurch die Serverleistung verbessert wird und die Kosten der Speicherhardware gesenkt werden. Mit diesen Speicherpooltypen dürfen keine Einheitenklassen oder Datenträger verwendet werden.

Bei der nachgeordneten Datendeduplizierung identifiziert der Server zunächst die Daten und entfernt dann die doppelten Daten aus dem Speicherpool. Es wird nur eine einzige Instanz der Daten auf Speichermedien aufbewahrt. Andere Instanzen derselben Daten werden durch einen Zeiger auf die aufbewahrte Instanz ersetzt. Wenn Sie die doppelten Daten entfernen, können Sie Speicherbereich in dem Speicherpool konsolidieren.

Weitere Informationen zur nachgeordneten Datendeduplizierung finden Sie in Daten deduplizieren (Version 7.1.1).

Bei der clientseitigen Datendeduplizierung werden nur komprimierte, deduplizierte Daten an den Server gesendet. Die Verarbeitung während eines Sicherungsprozesses wird auf den Server und den Client verteilt.

Die folgende Tabelle enthält einen Vergleich der Datendeduplizierungsoptionen.

Typ der Datendeduplizierung	Vorteile	Nachteile
Nachgeordnet Einschränkung: Sie können die nachgeordnete Datendeduplizierung nur für Speicherpools mit sequenziellem Zugriff (FILE) verwenden.	• Nach der Datendeduplizierung können Sie den Speicherpool konsolidieren.	• Längere Verarbeitungszeiten, da die Daten zunächst identifiziert werden müssen, bevor die doppelten Daten aus dem Speicherpool entfernt werden.
Inline Einschränkung: Sie können die Inline-Datendeduplizierung nur für Verzeichniscontainer- und Cloud-Containerspeicherpools verwenden.	• Dedupliziert Daten, wenn die Daten in einen Containerspeicherpool geschrieben werden. • Verringert die Notwendigkeit zur Offlinereorganisation, wodurch die Serverleistung verbessert wird. • Geringere Kosten für Speicherhardware	• Höhere Prozessorauslastung durch den Server
Clientseite	• Die Verarbeitung während eines Sicherungsprozesses wird auf den Server und den Client verteilt.	• Höhere Prozessorauslastung durch den Client • Längere abgelaufene Zeit für Clientoperationen, wie beispielsweise Sicherungen • Nur komprimierte, deduplizierte Daten werden an den Server gesendet

Zugehörige Tasks:
Datendeduplizierung konfigurieren (Plattenspeicherlösung für mehrere Standorte)
Datendeduplizierung konfigurieren (Plattenspeicherlösung für einen einzelnen Standort)

Speicherpools vergleichen

Speichereinheiten konfigurieren

Konfigurieren Sie Speichereinheiten, indem Sie Einheiten anschließen, Einheitentreiber konfigurieren und die Objekte erstellen, die die Einheiten für den Server darstellen.

Informationen zu diesem Vorgang

Wenn Sie nicht die Plattenspeicherlösung für einen einzelnen Standort oder die Plattenspeicherlösung für mehrere Standorte verwenden, konfigurieren und verwalten Sie Speichereinheiten anhand der Anweisungen in der Dokumentation zu Version 7.1.1:

- AIX-BetriebssystemeLinux-BetriebssystemeSpeichereinheiten konfigurieren und verwalten
- Windows-BetriebssystemeSpeichereinheiten konfigurieren und verwalten

Verzeichniscontainerspeicherpool für die Datenspeicherung konfigurieren

Sie können Verzeichniscontainerspeicherpools für die Verwendung der Inline-Datendeduplizierung zum Speichern deduplizierter Daten konfigurieren.

Vorgehensweise

Um Daten in einem Verzeichniscontainerspeicherpool zu speichern, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Verzeichniscontainerspeicherpool, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie in der Menüleiste des Operations Center auf Speicher > Speicherpools.
   b. Klicken Sie auf der Seite Speicherpools auf + Speicherpool.
   c. Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus. Wählen Sie Verzeichnis als Typ des containerbasierten Speichers aus.
2. Aktualisieren Sie, nachdem der Speicherpool vom Assistenten erstellt wurde, Ihre Verwaltungsklassen und Maßnahmengruppen für die Verwendung des neuen Pools. Um eine Verwaltungsklasse für die Verwendung des neuen Pools zu aktualisieren, führen Sie die folgenden Schritte aus:
   a. Klicken Sie in der Menüleiste des Operations Center auf Services.
   b. Wählen Sie auf der Seite Maßnahmen eine Maßnahmendomäne aus und klicken Sie auf Details.
   c. Klicken Sie auf der Seite Details auf die Registerkarte Maßnahmengruppen.
   d. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind editierbar.
   e. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
   f. Aktualisieren Sie eine oder mehrere Verwaltungsklassen für die Verwendung des neuen Pools, indem Sie das Feld Sicherungsziel der Tabelle editieren.
   g. Klicken Sie auf Sichern.
3. Aktivieren Sie die geänderte Maßnahmengruppe, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie auf Aktivieren. Da das Ändern der aktiven Maßnahmengruppe unter Umständen einen Datenverlust zur Folge haben kann, wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt.
   b. Studieren Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Auswirkungen auf Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der derzeit aktiven Maßnahmengruppe gebunden sind, werden nach der Aktivierung in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
   c. Ermitteln Sie Verwaltungsklassen in der derzeit aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben, und wägen Sie die Auswirkungen auf Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden nach der Aktivierung von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
   d. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.
4. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.

Nächste Schritte

Um einen Verzeichniscontainerspeicherpool zu schützen, geben Sie den Befehl PROTECT STGPOOL aus. Anweisungen finden Sie in PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören) und Verzeichniscontainerspeicherpools auf Band kopieren.

Linux-BetriebssystemeWenn Sie einen Verzeichniscontainerspeicherpool schützen, indem Sie die Daten auf einen fernen Server kopieren, und Netzprobleme auftreten, lesen Sie in Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann nach.

- Verzeichniscontainerspeicherpools auf Band kopieren
  Sie können Daten in einem Verzeichniscontainerspeicherpool schützen, indem Sie die Daten in Containerkopienspeicherpools kopieren,

die durch Banddatenträger dargestellt werden. Die Bandkopie wird zur Reparatur von Beschädigungen an einem Verzeichniscontainerspeicherpool verwendet.
- Banddatenträger ohne Konfiguration von DRM im Rotationsprinzip auslagern
  Wenn Ihre Speicherlösung Containerkopienspeicherpools umfasst, die durch Banddatenträger dargestellt werden, die Funktion 'Disaster Recovery Manager' (DRM) jedoch nicht konfiguriert wurde, können Sie eine manuelle Prozedur verwenden, um die Banddatenträger im Rotationsprinzip auszulagern. Indem Sie Kopien von Daten in ausgelagerten Banddatenträgern aufbewahren, können Sie die Daten in einem Katastrophenfall zurückschreiben.
- Schwellenwert für Datenträgerkonsolidierung für Containerkopienspeicherpools ändern
  Standardmäßig ist die Konsolidierung von Banddatenträgern für Containerkopienspeicherpools aktiviert. Um sicherzustellen, dass Banddatenträger effizient verwendet werden, können Sie den Schwellenwert für Datenträgerkonsolidierung ändern.
- Banddatenträger in Containerkopienspeicherpools konsolidieren
  Sie können Banddatenträger in Containerkopienspeicherpools konsolidieren, ohne eine Schutzoperation auszuführen, wenn nicht ausreichend Zeit zur Verfügung steht, um sowohl Schutz- als auch Konsolidierungsoperationen zu ermöglichen.
- Bestimmen, ob Containerkopienspeicherpools für den Schutz vor Katastrophen verwendet werden können
  Bestimmen, ob Containerkopienspeicherpools Ihre Anforderungen für den Schutz vor Katastrophen erfüllen

Verzeichniscontainerspeicherpools auf Band kopieren

Sie können Daten in einem Verzeichniscontainerspeicherpool schützen, indem Sie die Daten in Containerkopienspeicherpools kopieren, die durch Banddatenträger dargestellt werden. Die Bandkopie wird zur Reparatur von Beschädigungen an einem Verzeichniscontainerspeicherpool verwendet.

Vorbereitende Schritte

Definieren Sie mit dem Befehl DEFINE LIBRARY mindestens ein Bandarchiv für den Server. Stellen Sie genügend Bandlaufwerke und Arbeitsdatenträger zur Erfüllung Ihrer Speicheranforderungen bereit. Weitere Informationen zur Verwaltung von Sicherungsdatenträgern und zur Konfiguration von Disaster Recovery Manager (DRM) finden Sie in Disaster Recovery Manager (Version 7.1.1).

Informationen zu diesem Vorgang

Um die Daten in Verzeichniscontainerspeicherpools auf Band zu kopieren, wird vom Operations Center ein Zeitplan zur Ausführung des Befehls PROTECT STGPOOL erstellt. Wenn der Zeitplan für den Schutz ausgeführt wird, wird eine einzelne Bandkopie erstellt. Wenn der Zeitplan für den Schutz ausgeführt wird, muss mindestens ein Datenträger verfügbar sein. Andernfalls schlägt die Operation fehl.

Sie können bis zu zwei Bandkopien erstellen, Sie müssen jedoch die Befehlszeilenschnittstelle verwenden, um einen zweiten Containerkopienspeicherpool zu erstellen. Eine Bandkopie kann an einen anderen Standort zur Wiederherstellung nach einem Katastrophenfall transportiert werden. Die andere Kopie kann vor Ort aufbewahrt werden, um eine schnelle Wiederherstellung bei weniger kritischen Fehlern zu ermöglichen.

Einschränkungen:

- Virtuelle Bandarchive werden, unabhängig davon, welcher Speicherarchivtyp definiert wird, nicht unterstützt. Es wird nur physisches Band unterstützt.
- Containerkopienspeicherpools können zum Reparieren geringfügiger bis moderater Beschädigungen an Speicherpools, einschließlich beschädigter Container oder Verzeichnisse, verwendet werden. Containerkopienspeicherpools können auch zum Schutz vor Katastrophen verwendet werden; Sie müssen jedoch sicherstellen, dass die Wiederherstellungszeiten Ihre Anforderungen erfüllen. Weitere Informationen finden Sie in Bestimmen, ob Containerkopienspeicherpools für den Schutz vor Katastrophen verwendet werden können.
- Die Replikation kann nicht für einen Containerkopienspeicherpool als Ziel verwendet werden.
  Tipp: Sie können eine Bandkopie der Daten im Verzeichniscontainerspeicherpool am Standort für die Wiederherstellung nach einem Katastrophenfall erstellen, indem Sie mithilfe dieser Prozedur einen Containerkopienspeicherpool auf dem Zielreplikationsserver erstellen. Planen Sie dann die Ausführung der Befehle PROTECT STGPOOL und REPLICATE NODE auf dem Quellenreplikationsserver, um Ihre Daten auf dem Zielreplikationsserver zu schützen.
- Die folgende Prozedur kann nicht verwendet werden, wenn dem Verzeichniscontainerspeicherpool bereits ein Containerkopienspeicherpool zugeordnet wurde. Um einen zweiten Containerkopienspeicherpool zu erstellen, führen Sie die Anweisungen in Schritt 5 aus.

Wenn Sie einen Containerkopienspeicherpool im Rahmen des Assistenten Speicherpool hinzufügen erstellt hatten, müssen Sie diese Prozedur nicht verwenden. Bei der Ausführung des Assistenten wurden vom Operations Center der Containerkopienspeicherpool und ein Zeitplan für den Schutz konfiguriert.

Vorgehensweise

Um Speicherpoolschutz für das Kopieren auf Band für einen vorhandenen Verzeichniscontainerspeicherpool zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Speicher > Speicherpools.
2. Wählen Sie auf der Seite Speicherpools den Verzeichniscontainerspeicherpool aus, der auf Band geschützt werden soll.
3. Klicken Sie auf Weitere > Containerkopienpool hinzufügen.
4. Führen Sie die Anweisungen im Fenster Containerkopienpool hinzufügen aus, um den Schutz für das Kopieren auf Band zu planen.

5. Nachdem Sie die vorherigen Schritte ausgeführt haben, können Sie mithilfe der Befehlszeilenschnittstelle einen zweiten Containerkopienspeicherpool hinzufügen. Führen Sie wahlweise die folgenden Schritte aus, um einen Containerkopienspeicherpool hinzuzufügen:
    a. Erstellen Sie einen Containerkopienspeicherpool, indem Sie den Befehl DEFINE STGPOOL ausgeben.
    b. Ordnen Sie den Containerkopienspeicherpool dem Verzeichniscontainerspeicherpool zu, indem Sie den Befehl UPDATE STGPOOL für den Verzeichniscontainerspeicherpool ausgeben.

Ergebnisse

Nachdem die Konfiguration abgeschlossen ist, werden die Daten in dem Verzeichniscontainerspeicherpool abhängig von dem definierten Zeitplan für den Schutz in einen Containerkopienspeicherpool kopiert.

Nächste Schritte

1. Wenn Sie eine Bandkopie für die Aufbewahrung an einem anderen Standort erstellt hatten, aktivieren Sie den Containerkopienspeicherpool an dem anderen Standort für DRM-Operationen, indem Sie den Befehl SET DRMCOPYCONTAINERSTGPOOL ausgeben. Stellen Sie sicher, dass die Banddatenträger Ihren Zeitplänen für die Rotation ausgelagerter Bänder hinzugefügt werden. Wenn DRM nicht konfiguriert ist, müssen Sie DRM konfigurieren oder eine Alternativmethode für die Auslagerung von Bändern im Rotationsprinzip verwenden. Anweisungen zu der Alternativmethode finden Sie in Banddatenträger ohne Konfiguration von DRM im Rotationsprinzip auslagern. Überprüfen Sie mithilfe des Befehls QUERY DRMSTATUS, ob Containerkopienspeicherpools an einem anderen Standort für DRM aktiviert sind.

   Anweisungen zur Konfiguration von DRM finden Sie in Disaster Recovery Manager (Version 7.1.1).

2. Bestätigen Sie, dass der Schwellenwert für Konsolidierung für Ihren Containerkopienspeicherpool Ihre Anforderungen erfüllt.

   Standardmäßig ist die Konsolidierung von Banddatenträgern für neue Containerkopienspeicherpools, die mit dem Operations Center erstellt werden, aktiviert. Eine Datenträgerkonsolidierung erfolgt, wenn der Schwellenwert für Konsolidierung für den Containerkopienspeicherpool unter 100 % liegt. Banddatenträger sind jedoch kein Kandidat für die Konsolidierung, bevor sie nicht zu 75 % gefüllt sind. Gehen Sie mit Vorsicht vor, wenn Sie die Konsolidierung mit Containerkopienspeicherpools verwenden, die über Datenträger an einem anderen Standort verfügen. Wenn ein Datenträger an einem anderen Standort für die Konsolidierung auswählbar wird, werden die Bereiche auf dem Datenträger vom Server an den Standort vor Ort zurückversetzt. Wenn vor Ort ein Katastrophenfall eintritt, kann der Server Bereiche von dem Datenträger an einem anderen Standort anfordern, wenn die zurückgeschriebene Datenbank auf Bereiche auf dem Datenträger an dem anderen Standort verweist. Um zu verhindern, dass Datenträger unmittelbar nach dem Löschen aller Bereiche erneut beschrieben werden, verwenden Sie den Parameter REUSEDELAY, um einen Wert größer als 0 anzugeben. Der Schwellenwert für Konsolidierung wird für Containerkopienspeicherpools vor Ort vom Operations Center auf 60 % gesetzt.

   Anweisungen zum Ändern des Schwellenwerts für Konsolidierung finden Sie in Schwellenwert für Datenträgerkonsolidierung für Containerkopienspeicherpools ändern.

3. Schützen Sie die Metadaten für Ihren Containerkopienspeicherpool.
   Wenn der Zeitplan für den Schutz ausgeführt wird, werden Datenbereiche in Containerkopienspeicherpools ohne die zugehörigen Metadaten auf Banddatenträger kopiert. Diese Metadaten sind zum Zurückschreiben der Bandkopien erforderlich. Um die Metadaten zu schützen, müssen Sie die Serverdatenbank zusammen mit dem Datenträgerprotokoll, den Serveroptionen und den Einheitenkonfigurationsdateien separat sichern. Wenn Sie die Konsolidierung mit Containerkopienspeicherpools verwenden, die über Datenträger an einem anderen Standort verfügen, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind, um Schutz für die Wiederherstellung nach einem Katastrophenfall bereitstellen zu können:
   - Datenbanksicherungsoperationen werden ausgeführt, nachdem Zeitpläne für den Schutz von Speicherpools und DRM-Versetzungszeitpläne beendet wurden.
   - Alle Datenbanksicherungsdatenträger und DRM-Datenträger werden zusammen ausgelagert.

   Anweisungen zum Sichern der Serverdatenbank und zugehöriger Dateien finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren.

4. Wahlweise können Sie den Zeitplan für den Schutz für einen Verzeichniscontainerspeicherpool, dem ein oder mehrere Containerkopienspeicherpools zugeordnet sind, ändern, indem Sie den Befehl UPDATE SCHEDULE verwenden. Der Zeitplan, der vom Operations Center erstellt wird, hat den Namen CONTAINER_COPY.

Zugehörige Konzepte:
Datenspeicher in Containerkopienspeicherpools
Zugehörige Tasks:
Bestimmen, ob Containerkopienspeicherpools für den Schutz vor Katastrophen verwendet werden können
Zugehörige Verweise:
DEFINE LIBRARY (Speicherarchiv definieren)
PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)
UPDATE SCHEDULE (Verwaltungszeitplan aktualisieren)
QUERY DRMSTATUS (Disaster Recovery Manager-Systemparameter abfragen)

Banddatenträger ohne Konfiguration von DRM im Rotationsprinzip auslagern

Wenn Ihre Speicherlösung Containerkopienspeicherpools umfasst, die durch Banddatenträger dargestellt werden, die Funktion 'Disaster Recovery Manager' (DRM) jedoch nicht konfiguriert wurde, können Sie eine manuelle Prozedur verwenden, um die Banddatenträger im Rotationsprinzip auszulagern. Indem Sie Kopien von Daten in ausgelagerten Banddatenträgern aufbewahren, können Sie die Daten in einem Katastrophenfall zurückschreiben.

Vorgehensweise

1. Entnehmen Sie den Speicherdatenträger, der im Rotationsprinzip ausgelagert werden muss, mithilfe des Befehls CHECKOUT LIBVOLUME.
2. Aktualisieren Sie den Datenträger, um anzugeben, dass er ausgelagert wird, mithilfe des Befehls UPDATE VOLUME unter Angabe von `ACCESS=UNAVAILABLE`. Geben Sie wahlweise den Standort für die Auslagerung mithilfe des Parameters LOCATION an. Geben Sie beispielsweise `LOCATION=SITE1` an.
3. Konsolidieren Sie Speicherbereich, indem Sie eine der folgenden Aktionen ausführen:
   - Um Speicherbereich zu konsolidieren, ohne den Speicherpool zu schützen, führen Sie den Befehl PROTECT STGPOOL unter Angabe von `TYPE=LOCAL` und `RECLAIM=ONLY` aus.
   - Um Speicherbereich zu konsolidieren, während der Speicherpool geschützt wird, führen Sie den Befehl PROTECT STGPOOL ohne Angabe von `RECLAIM=ONLY` aus.
4. Überwachen Sie den Datenträger mithilfe des Befehls QUERY VOLUME. Wenn der Datenträger als nicht verfügbar und leer angezeigt wird, bringen Sie den Datenträger wieder vor Ort und stellen Sie ihn mithilfe des Befehls CHECKIN LIBVOLUME in das Speicherarchiv zurück.
5. Aktualisieren Sie den Datenträger mithilfe des Befehls UPDATE VOLUME unter Angabe von `ACCESS=READWRITE`.

Zugehörige Verweise:
CHECKOUT LIBVOLUME (Speicherdatenträger aus einem Speicherarchiv entnehmen)
PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)
UPDATE VOLUME (Speicherpooldatenträger ändern)

Schwellenwert für Datenträgerkonsolidierung für Containerkopienspeicherpools ändern

Standardmäßig ist die Konsolidierung von Banddatenträgern für Containerkopienspeicherpools aktiviert. Um sicherzustellen, dass Banddatenträger effizient verwendet werden, können Sie den Schwellenwert für Datenträgerkonsolidierung ändern.

Vorgehensweise

1. Klicken Sie auf der Seite Übersicht im Operations Center auf Speicher > Speicherpools.
2. Wählen Sie den Speicherpool aus und klicken Sie auf Details und dann auf Merkmale.
3. Definieren Sie im Abschnitt Wiederherstellung den Prozentsatz der Konsolidierung und klicken Sie auf Sichern.
   Tipp: Es ist auch möglich, den Schwellenwert für Konsolidierung zu ändern, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters RECLAIM ausgeben. Ausführliche Informationen zum Parameter RECLAIM finden Sie in den Beschreibungen der Befehle zum Definieren und Aktualisieren von Containerkopienspeicherpools.
   Einschränkung: Sie können den Befehl RECLAIM STGPOOL nicht zum Konsolidieren von Datenträgern in Containerkopienspeicherpools verwenden. Ausführliche Informationen zum Konsolidieren von Datenträgern in Containerkopienspeicherpools finden Sie in der Beschreibung des Parameters RECLAIM im Befehl PROTECT STGPOOL.

Banddatenträger in Containerkopienspeicherpools konsolidieren

Sie können Banddatenträger in Containerkopienspeicherpools konsolidieren, ohne eine Schutzoperation auszuführen, wenn nicht ausreichend Zeit zur Verfügung steht, um sowohl Schutz- als auch Konsolidierungsoperationen zu ermöglichen.

Informationen zu diesem Vorgang

Wenn Sie den Befehl PROTECT STGPOOL ausgeben und es sich bei dem Zielspeicherpool um einen Containerkopienspeicherpool handelt, werden standardmäßig sowohl Schutz- als auch Konsolidierungsoperationen ausgeführt. Das bevorzugte Verfahren ist sowohl die Ausführung von Schutz- als auch von Konsolidierungsoperationen zu ermöglichen. Aus Gründen der Zeitersparnis können Sie jedoch nur die Speicherpoolschutzoperation oder nur die Konsolidierung ausführen oder die Anzahl Banddatenträger, die konsolidiert werden, einschränken. Verwenden Sie diese Prozedur nur, wenn Banddatenträger schnell konsolidiert werden müssen oder wenn eine begrenzte Anzahl Banddatenträger konsolidiert werden muss.

Vorgehensweise

Um Banddatenträger zu konsolidieren, ohne eine Speicherpoolschutzoperation auszuführen, führen Sie die folgenden Schritte aus:

1. Optional: Um den Umfang des Speicherbereichs, der konsolidiert wird, zu maximieren, starten Sie den Bestandsverfallsprozess, indem Sie den Befehl EXPIRE INVENTORY ausgeben.
2. Bestimmen Sie, ob die Konsolidierung bis zum Abschluss ausgeführt werden soll oder ob die Anzahl Banddatenträger, die konsolidiert werden, begrenzt werden soll.

3. Um die Konsolidierung bis zum Abschluss auszuführen, geben Sie den Befehl PROTECT STGPOOL unter Angabe der Parameter TYPE=LOCAL und RECLAIM=ONLY aus. Um beispielsweise Speicherbereich in einem lokalen Containerkopienspeicherpool zu konsolidieren, der als Zielschutzpool für SPOOL1 definiert ist, geben Sie den folgenden Befehl aus:

   ```
   protect stgpool spool1 type=local reclaim=only
   ```

4. Um eine begrenzte Anzahl Banddatenträger zu konsolidieren, führen Sie die folgenden Schritte aus:
   a. Legen Sie einen Konsolidierungsgrenzwert für den Containerkopienspeicherpool fest, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters RECLAIMLIMIT ausgeben. Mit diesem Parameter wird die Anzahl Datenträger in dem Containerkopienspeicherpool, die konsolidiert werden, begrenzt.
   b. Geben Sie den Befehl PROTECT STGPOOL unter Angabe des Parameters TYPE=LOCAL zusammen mit dem Parameter RECLAIM=YESLIMITED oder RECLAIM=ONLYLIMITED aus.
   Tipp: Wenn Sie RECLAIM=YESLIMITED angeben, werden sowohl Konsolidierungs- als auch Speicherpoolschutzoperationen ausgeführt, wenn der Befehl PROTECT STGPOOL ausgegeben wird. Wenn Sie RECLAIM=ONLYLIMITED angeben, wird nur die Konsolidierungsoperation ausgeführt. Wenn Sie einen dieser Werte angeben, wird die Konsolidierung nur so lange ausgeführt, bis der Konsolidierungsgrenzwert, der für den Containerkopienspeicherpool definiert ist, erreicht ist. Der Konsolidierungsgrenzwert wird mit dem Parameter RECLAIMLIMIT im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert.

   Um beispielsweise maximal fünf Banddatenträger in einem Containerkopienspeicherpool mit dem Namen CCPOOL1 zu konsolidieren, ohne eine Schutzoperation für den Quellenverzeichniscontainerspeicherpool mit dem Namen SPOOL1 auszuführen, geben Sie die folgenden Befehle aus:

   ```
   update stgpool ccpool1 reclaimlimit=5
   protect stgpool spool1 type=local reclaim=onlylimited
   ```

   Um beispielsweise einen Speicherpool mit dem Namen SPOOL1 zu schützen und maximal 10 Banddatenträger in dem zugehörigen Containerkopienspeicherpool zu konsolidieren, geben Sie die folgenden Befehle aus:

   ```
   update stgpool spool1 reclaimlimit=10
   protect stgpool spool1 type=local reclaim=yeslimited
   ```

Ergebnisse

Die Konsolidierungsverarbeitung für den Containerkopienspeicherpool ist abgeschlossen. Die Speicherpoolschutzoperation wurde nicht ausgeführt, sodass Daten im Verzeichniscontainerspeicherpool, die seit der letzten Schutzoperation aktualisiert wurden, nicht geschützt werden.

Nächste Schritte

1. Schützen Sie die Daten im Verzeichniscontainerspeicherpool in dem Containerkopienspeicherpool, indem Sie den Befehl PROTECT STGPOOL unter Angabe des Parameters TYPE=LOCAL ausgeben. Der Schutzprozess wird mit dem Standardparameter RECLAIM=YES ausgeführt. Die Schutzoperation nimmt weniger Zeit in Anspruch, da die Konsolidierung bereits ausgeführt wurde.
   Um beispielsweise die Daten in einem Verzeichniscontainerspeicherpool mit dem Namen SPOOL1 zu schützen, geben Sie den folgenden Befehl aus:

   ```
   protect stgpool spool1 type=local
   ```

   Es ist auch möglich, die Daten in einem Verzeichniscontainerspeicherpool mit dem Namen SPOOL1 zu schützen, ohne die Konsolidierung auszuführen, indem Sie den folgenden Befehl ausgeben:

   ```
   protect stgpool spool1 type=local reclaim=no
   ```

2. Sichern Sie die Serverdatenbank und führen Sie geplante Verwaltungsoperationen aus. Anweisungen finden Sie in Zeitpläne für Serververwaltungsaktivitäten definieren.

Zugehörige Verweise:
PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)
DEFINE STGPOOL (Containerkopienspeicherpool definieren)
UPDATE STGPOOL (Containerkopienspeicherpool aktualisieren)
EXPIRE INVENTORY (Bestandsverfallsverarbeitung manuell starten)

Bestimmen, ob Containerkopienspeicherpools für den Schutz vor Katastrophen verwendet werden können

Bestimmen, ob Containerkopienspeicherpools Ihre Anforderungen für den Schutz vor Katastrophen erfüllen

Informationen zu diesem Vorgang

Sie können eine ausgelagerte Kopie Ihres Containerkopienspeicherpools für den Schutz für die Wiederherstellung nach einem Katastrophenfall oder zur Erfüllung gesetzlicher Bestimmungen und Geschäftsanforderungen für ausgelagerte Bandkopien erstellen. Bevor Sie sich für die Verwendung ausgelagerter Bandkopien zum Schutz vor Katastrophen entscheiden, müssen Sie sorgfältig abwägen, ob die Lösung Ihre Zielsetzung für Wiederherstellungszeit erfüllt.

Die Verwendung von Containerkopienspeicherpools für die Wiederherstellung nach einem Katastrophenfall ist geeignet, wenn das Datenvolumen in Ihrer Umgebung kleiner-gleich den folgenden Werten ist:

- 200 TB verwaltete Daten insgesamt
- 50 TB Back-End-Daten
- 37 TB Front-End-Daten

Gesamtvolumen der verwalteten Daten
: Alle Daten, die in dem Verzeichniscontainerspeicherpool auf dem Server gespeichert sind. Dies umfasst aktive und inaktive Versionen der Daten. Die Anzahl Versionen wird durch Aufbewahrungsmaßnahmen bestimmt.

Back-End-Daten
: Alle Daten, die in dem Containerkopienspeicherpool gespeichert sind.

Front-End-Daten
: Die derzeit aktiven Daten, die in dem Containerkopienspeicherpool gespeichert sind. Dies sind die aktiven Daten, die zum Zurückschreiben von Daten auf Clientknoten verwendet werden. Bei einer Katastrophe sind alle Front-End-Daten oder ein Teil der Front-End-Daten zur Wiederaufnahme der Produktion erforderlich. Die Front-End-Daten sind ein Prozentsatz des Gesamtvolumens der verwalteten Daten; ihr Volumen ist abhängig von den aktiven Maßnahmeneinstellungen kleiner-gleich dem Gesamtvolumen der verwalteten Daten.

Um innerhalb von 48 Stunden nach einem Katastrophenfall eine Wiederherstellung ausführen zu können, muss die Systemumgebung am Wiederherstellungsstandort die Hardwaremindestvoraussetzungen für die Aktionen in der folgenden Tabelle erfüllen.

Aktion	Erforderlicher Zeitbedarf	Mindestvoraussetzungen
Konfigurieren Sie einen neuen IBM Spectrum Protect-Server am Standort für die Wiederherstellung nach einem Katastrophenfall. Um den neuen Server zu konfigurieren, müssen Sie die folgenden Schritte ausführen: 1. Stellen Sie Platten für den Server bereit. 2. Schreiben Sie den Server aus der Sicherung zurück. 3. Starten Sie den Server. 4. Aktualisieren Sie die Speicher- und Einheitenkonfigurationen.	Zeitbedarf zum Wiederherstellen des Servers: 6 Stunden	Verwenden Sie ein Solid-State-Laufwerk (SSD) für die Serverdatenbank, das die folgenden Voraussetzungen erfüllt: • Kombinierter Schreib-/Lesedurchsatz von mindestens 100 MB pro Sekunde im Durchschnitt • Mindestens 12.862 Ein-/Ausgabeoperationen pro Sekunde (IOPS) im Durchschnitt
Prüfen Sie den Verzeichniscontainerspeicherpool und reparieren Sie die Daten mithilfe von Bändern. Tipp: Wenn das System die Hardwaremindestvoraussetzungen erfüllt, können Sie bis zu 50 TB Back-End-Daten innerhalb von 48 Stunden reparieren.	Zeitbedarf zum Prüfen des Speicherpools: 2 Stunden Zeitbedarf zum Reparieren des Speicherpools mithilfe einer Bandkopie: 28 Stunden Anmerkung: Der geschätzte Zeitbedarf gilt für den Fall, dass maximal 200 TB verwaltete Daten insgesamt im Speicherpool vorhanden sind.	Verwenden Sie Nearline-SAS-Laufwerke (NL-SAS-Laufwerke) wie in einer mittelgroßen Blueprint-Serverkonfiguration mit einer Mindestschreibleistung von 700 MB pro Sekunde auf Speicherpoolplatte. Verwenden Sie Bandtechnologie einer neuen Generation, wie beispielsweise LTO-7 oder besser, mit mindestens sechs Laufwerken, um gleichzeitig ablaufende Leseoperationen von Banddatenträgern zu ermöglichen.
Schreiben Sie Daten auf Clientknoten zurück. Tipp: Wenn das System die Hardwaremindestvoraussetzungen erfüllt, können Sie bis zu 37 TB Front-End-Daten innerhalb von 48 Stunden zurückschreiben.	Zeitbedarf für Clientzurückschreibungsoperationen: 12 Stunden	Verwenden Sie Nearline-SAS-Laufwerke (NL-SAS-Laufwerke) wie in einer mittelgroßen Blueprint-Serverkonfiguration mit mindestens 10 Zurückschreibungssitzungen und einer Mindestschreibleistung von 3102 GB pro Stunde.

Vorgehensweise

1. Schätzen Sie die Wiederherstellungszeit nach einem Katastrophenfall für Ihre Umgebung mithilfe der folgenden Tabelle. Bestimmen Sie, ob die Wiederherstellungszeit Ihre Anforderungen erfüllt.

Tabelle 1. Geschätzte Wiederherstellungszeit für unterschiedliche Gesamtvolumina verwalteter Daten

Zielsetzung für Wiederherstellungszeit	Gesamtvolumen der verwalteten Daten (TB)	Anzahl Stunden zur Reparatur eines Verzeichniscontainerspeicherpools (erstes Byte zurückgeschrieben)	Stunden bis zur Zurückschreibung der Clientknoten (Wiederherstellung nach einem Katastrophenfall abgeschlossen)

Zielsetzung für Wiederherstellungszeit	Gesamtvolumen der verwalteten Daten (TB)	Anzahl Stunden zur Reparatur eines Verzeichniscontainerspeicherpools (erstes Byte zurückgeschrieben)	Stunden bis zur Zurückschreibung der Clientknoten (Wiederherstellung nach einem Katastrophenfall abgeschlossen)
Bis zu 1 Tag	25	10	12
	50	13	16
	75	17	22
Bis zu 2 Tage	100	20	26
	200	34	46
Bis zu 4 Tage	300	48	66
	400	62	86
Mehr als 4 Tage	500	76	106

Anmerkungen:

- Welche Geschwindigkeiten erzielt werden können, ist in hohem Maß von der Arbeitslast und der konfigurierten Umgebung abhängig.
- Der Prozentsatz an Front-End-Daten ist relativ zum Gesamtvolumen der verwalteten Daten. Eine Zunahme des Front-End-Datenvolumens hat eine Verlängerung der Wiederherstellungsgesamtzeit zur Folge. Eine Abnahme des Front-End-Datenvolumens hat eine Verkürzung der Wiederherstellungsgesamtzeit zur Folge.

2. Schätzen Sie die Wiederherstellungszeit für Ihre Umgebung mithilfe der folgenden Formel:
   - Schätzen Sie den Wert für **Stunden bis zur Reparatur eines Verzeichniscontainerspeicherpools (erstes Byte zurückgeschrieben)**:

     ```
     Zeitbedarf bis zur Zurückschreibung des ersten Byte auf dem Client =
     6 Stunden + 14 Stunden pro 100 TB verwalteter Daten insgesamt
     ```

   - Schätzen Sie den Wert für **Stunden bis zur Zurückschreibung der Clientknoten (Wiederherstellung nach einem Katastrophenfall abgeschlossen)**:

     ```
     Zeitbedarf bis zum Abschluss der Clientzurückschreibung =
     Zeitbedarf bis zur Zurückschreibung des ersten Byte auf dem Client + ((Gesamtvolumen der verwalteten
     Daten * Front-End-Daten) / Zurückschreibungsgeschwindigkeit)
     ```

   Zurückschreibungsgeschwindigkeit: Die Geschwindigkeit, mit der Clients Daten vom Server wieder auf ihren lokalen Computer oder ihre lokale Speichereinheit zurückschreiben können.

3. Führen Sie Testprozeduren für die Wiederherstellung nach einem Katastrophenfall aus, um sicherzustellen, dass Containerkopienspeicherpools zum Zurückschreiben Ihrer Umgebung innerhalb eines Zeitrahmens, der Ihre Anforderungen erfüllt, verwendet werden können.

Zugehörige Verweise:
Speicherpools nach einem Katastrophenfall reparieren

Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren

Sie können deduplizierte Daten und nicht deduplizierte Daten in einem Cloud-Containerspeicherpool speichern und die Daten nach Bedarf zurückschreiben. Sie können Cloud-Containerspeicherpools für die Verwendung einer der folgenden Service-Provider und Protokolle konfigurieren: Amazon Web Services (AWS) mit Simple Storage Service (S3), IBM® Cloud Object Storage mit Swift oder S3 (und IBM SoftLayer), Microsoft Azure und OpenStack mit Swift unter Verwendung von Keystone Version 1 oder Version 2. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.

Vorbereitende Schritte

Führen Sie die folgenden Schritte aus:

1. Rufen Sie die Konfigurationsinformationen für Ihren Cloud-Service-Provider ab:
   - Amazon mit S3 (Off-Premises)
   - Microsoft Azure
   - IBM Cloud Object Storage mit S3 (Off-Premises, mit IBM SoftLayer)
   - IBM Cloud Object Storage mit Swift (Off-Premises, mit IBM SoftLayer)
   - IBM Cloud Object Storage mit S3 (On-Premises)
   - OpenStack mit Swift (On-Premises oder Off-Premises)
2. Geben Sie eine Einheitenklasse an, die für Datenbanksicherungsoperationen verwendet werden soll. Wenn Sie Verschlüsselung für Cloud-Containerspeicherpools verwenden, wird der Masterverschlüsselungsschlüssel des Servers zum Schützen des Cloudverschlüsselungsschlüssels in einer Datenbanksicherung verwendet.
   a. Wählen Sie in der Menüleiste des Operations Center Server aus.
   b. Wählen Sie eine Serverzeile aus und klicken Sie auf Sichern.

c. Wählen Sie eine Einheitenklasse aus, die für Datenbanksicherungsoperationen verwendet werden soll, und klicken Sie auf Sichern.

Tipp: Sie können auch stattdessen den Befehl SET DBRECOVERY verwenden, um eine Einheitenklasse für die Datenbanksicherung anzugeben.

Vorgehensweise

Um Daten in einem Cloud-Containerspeicherpool zu speichern, führen Sie die folgenden Schritte aus:

1. Erstellen Sie einen Cloud-Containerspeicherpool. Sie müssen Konfigurationsinformationen zur Identifikation des Cloud-Service angeben.
   a. Klicken Sie in der Menüleiste des Operations Center auf Speicher > Speicherpools.
   b. Klicken Sie auf der Seite Speicherpools auf + Speicherpool.
   c. Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus. Wählen Sie On-Premises-Cloud oder Off-Premises-Cloud für den Typ des containerbasierten Speichers aus.
2. Aktualisieren Sie Ihre Verwaltungsklassen und Maßnahmengruppen für die Verwendung des neuen Speicherpools. Um eine Verwaltungsklasse für die Verwendung des neuen Speicherpools zu aktualisieren, führen Sie die folgenden Schritte aus:
   a. Klicken Sie in der Menüleiste des Operations Center auf Services.
   b. Wählen Sie auf der Seite Maßnahmen eine Maßnahmendomäne aus und klicken Sie auf Details.
   c. Klicken Sie auf der Seite Details auf die Registerkarte Maßnahmengruppen.
   d. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind editierbar.
   e. Optional: Um eine Maßnahmengruppe zu editieren, die nicht aktiv ist, klicken Sie auf die vorwärts und rückwärts gerichteten Pfeile, um die Maßnahmengruppe zu lokalisieren.
   f. Aktualisieren Sie eine oder mehrere Verwaltungsklassen für die Verwendung des neuen Speicherpools, indem Sie das Feld Sicherungsziel der Tabelle editieren.
   g. Klicken Sie auf Sichern.
3. Aktivieren Sie die geänderte Maßnahmengruppe, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie auf Aktivieren. Da das Ändern der aktiven Maßnahmengruppe unter Umständen einen Datenverlust zur Folge haben kann, wird eine Zusammenfassung der Unterschiede zwischen der aktiven Maßnahmengruppe und der neuen Maßnahmengruppe angezeigt.
   b. Studieren Sie die Unterschiede zwischen entsprechenden Verwaltungsklassen in den beiden Maßnahmengruppen und wägen Sie die Auswirkungen auf Clientdateien ab. Clientdateien, die an Verwaltungsklassen in der derzeit aktiven Maßnahmengruppe gebunden sind, werden nach der Aktivierung in der neuen Maßnahmengruppe an die Verwaltungsklassen mit denselben Namen gebunden.
   c. Ermitteln Sie Verwaltungsklassen in der derzeit aktiven Maßnahmengruppe, die in der neuen Maßnahmengruppe keine Entsprechung haben, und wägen Sie die Auswirkungen auf Clientdateien ab. Clientdateien, die an diese Verwaltungsklassen gebunden sind, werden nach der Aktivierung von der Standardverwaltungsklasse in der neuen Maßnahmengruppe verwaltet.
   d. Wenn die Änderungen, die durch die Maßnahmengruppe implementiert werden, akzeptabel sind, wählen Sie das Kontrollkästchen Ich weiß, dass diese Aktualisierungen zu einem Datenverlust führen können aus und klicken Sie auf Aktivieren.
4. Klicken Sie auf die Umschaltfläche Konfigurieren. Die Maßnahmengruppen sind nicht mehr editierbar.
5. Um die Vorteile von lokalem Speicher nutzen zu können, erstellen Sie mit dem Befehl DEFINE STGPOOLDIRECTORY ein Speicherpoolverzeichnis für diesen Speicherpool. Weitere Informationen finden Sie in Leistung für Cloudobjektspeicher optimieren.

Zugehörige Tasks:
Konfiguration von Cloud-Containerspeicherpools für AWS mit S3 vorbereiten (Off-Premises)
Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit S3 vorbereiten (On-Premises)
Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit S3 vorbereiten (Off-Premises)
Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit Swift vorbereiten (Off-Premises)
Konfiguration von Cloud-Containerspeicherpools für OpenStack mit Swift vorbereiten
Daten für Cloud-Containerspeicherpools verschlüsseln
Leistung für Cloudobjektspeicher optimieren
Zugehörige Verweise:
SET DBRECOVERY (Einheitenklasse für automatische Sicherungen definieren)

Konfiguration von Cloud-Containerspeicherpools für AWS mit S3 vorbereiten (Off-Premises)

Bevor Sie Cloud-Containerspeicherpools für die Off-Premises-Verwendung von Amazon Web Services (AWS) mit dem Protokoll 'Simple Storage Service' (S3) konfigurieren können, müssen Sie Informationen von Amazon abrufen, die für den Konfigurationsprozess erforderlich sind.

Informationen zu diesem Vorgang

AWS-Kontoberechtigungsnachweise unterscheiden sich von Amazon-Kontoberechtigungsnachweisen. Verwenden Sie die Berechtigungsnachweise für Ihr AWS-Konto, wenn Sie Speicherpools im Operations Center oder mit dem Befehl DEFINE STGPOOL konfigurieren.

AWS verwendet *Buckets* zum Speichern von Daten. AWS-Buckets werden auf dieselbe Art und Weise wie Container in einem Cloud-Containerspeicherpool verwendet. IBM Spectrum Protect erstellt für eine Instanz von IBM Spectrum Protect automatisch ein Bucket in Amazon, das von allen Pools für diese Instanz gemeinsam genutzt wird.

Einschränkung: Sie dürfen ein AWS-Bucket nur mit IBM Spectrum Protect editieren und die Daten in dem Bucket nicht ändern oder die Konfigurationseinstellungen für das Bucket nicht editieren.

Vorgehensweise

1. Melden Sie sich bei einem AWS-Konto an, indem Sie die Seite für Amazon S3 aufrufen und auf die Schaltfläche zum Erstellen eines AWS-Kontos klicken.
2. Rufen Sie Ihre AWS-Berechtigungsnachweise ab:
   a. Rufen Sie die Seite für Amazon S3 auf und klicken Sie auf die Schaltfläche zum Anmelden an der Konsole.
   b. Wählen Sie Ihren Namen und dann die Option für Sicherheitsberechtigungsnachweise aus.
   c. Rufen Sie den Abschnitt für Zugriffsschlüssel auf und lokalisieren Sie die Felder für die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel. Notieren Sie die Werte, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
3. Wenn Sie planen, Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
   - Cloudtyp: `Amazon - S3 API`
   - Zugriffsschlüssel-ID: *Zugriffsschlüssel-ID*
   - Geheimer Zugriffsschlüssel: *geheimer_Zugriffsschlüssel*
   - Region: Wählen Sie auf der Basis der Seite Regionen und Endpunkte von AWS den Regionsendpunkt aus, der für Ihren Standort am besten geeignet ist. Wenn Sie `Other` auswählen, geben Sie eine Regionsendpunkt-URL im Feld URL an und schließen Sie das Protokoll, in der Regel https://, ein. Normalerweise können Sie für den Parameter Region die Region verwenden, die Ihrem physischen Standort am nächsten liegt. Da ein Amazon-Bucket nur in einer einzigen Region vorhanden ist, können Sie nur eine einzige Endpunkt-URL für eine Region angeben. Wenn eine GovCloud-Region erforderlich ist, geben Sie eine der auf der Seite AWS GovCloud (US) Endpoints aufgelisteten URLs an.
     Warnung: Stellen Sie sicher, dass nur die AWS-Endpunkt-URL für den Regionswert verwendet wird, wie beispielsweise `https://s3-us-west-1.amazonaws.com`. Verwenden Sie für diesen Wert nicht die statische Website-Hosting-URL.
   - Bucketname: Verwenden Sie den vom Server generierten Standardbucketnamen oder geben Sie einen neuen Bucketnamen an.
4. Um einen Cloud-Containerspeicherpool zu definieren, geben Sie den Befehl DEFINE STGPOOL mit den folgenden Werten aus:
   - CLOUDTYPE: S3
   - IDENTITY: *Zugriffsschlüssel-ID*
   - PASSWORD: *geheimer_Zugriffsschlüssel*
   - CLOUDURL: Geben Sie auf der Basis der Seite Regionen und Endpunkte von AWS die Regionsendpunkt-URL an, die für Ihren Standort am besten geeignet ist.

     Normalerweise können Sie für den Parameter CLOUDURL die Region verwenden, die Ihrem physischen Standort am nächsten liegt. Wenn eine GovCloud-Region erforderlich ist, geben Sie eine der auf der Seite AWS GovCloud (US) Endpoints aufgelisteten URLs an.

     Warnung: Stellen Sie sicher, dass nur die AWS-Endpunkt-URL für den CLOUDURL-Wert verwendet wird, wie beispielsweise `https://s3-us-west-1.amazonaws.com`. Verwenden Sie für diesen Wert nicht die statische Website-Hosting-URL.

Nächste Schritte

Konfigurieren Sie Cloud-Containerspeicherpools für AWS, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

Amazon S3-kompatible Einheit als Cloud-Containerspeicherpool konfigurieren

Sie können eine Speichereinheit konfigurieren, die mit dem Protokoll Amazon Simple Storage Service (S3) kompatibel ist, um die Einheit als IBM Spectrum Protect-Cloud-Containerspeicherpool verwenden zu können.

Informationen zu diesem Vorgang

Amazon S3 verwendet *Buckets* zum Speichern von Daten. Sie müssen ein Bucket auf der S3-kompatiblen Speichereinheit für die Verwendung durch einen IBM Spectrum Protect-Server erstellen. Verwenden Sie nach dem Erstellen des Buckets die Berechtigungsnachweise des Kontos auf Ihrer Amazon S3-kompatiblen Cloudobjektspeichereinheit, wenn Sie Speicherpools mit dem Befehl DEFINE STGPOOL konfigurieren.

Einschränkung: Sie dürfen die Daten in dem Bucket nicht ändern oder die Konfigurationseinstellungen für das Bucket nicht editieren.

Vorgehensweise

1. Erstellen Sie ein Bucket in der Cloudobjektspeichereinheit. Führen Sie die Anweisungen in der Einheitendokumentation aus.
2. Erstellen Sie ein Benutzerkonto in der Cloudobjektspeichereinheit. Das Konto wird von IBM Spectrum Protect für den Zugriff auf die Einheit mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels verwendet. Stellen Sie sicher, dass das Konto über Berechtigungen zum Speichern von Daten in dem in Schritt 1 erstellten Bucket und zum Löschen von Daten aus diesem Bucket verfügt. Notieren Sie die Werte für die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
3. Geben Sie den URL-Wert an, der von IBM Spectrum Protect für den Zugriff auf die Cloudobjektspeichereinheit verwendet wird. Anweisungen finden Sie in in der Dokumentation zu Ihrer Cloudobjektspeichereinheit.
4. Um einen Cloud-Containerspeicherpool zu definieren, geben Sie den Befehl DEFINE STGPOOL mit den folgenden Werten aus:

- CLOUDTYPE: S3
- IDENTITY: *Zugriffsschlüssel-ID*
- PASSWORD: *geheimer_Zugriffsschlüssel*
- CLOUDURL: http://*IP-Adresse_des_Cloudobjektspeicherendpunkts* oder https://*IP-Adresse_des_Cloudobjektspeicherendpunkts*. Wenn Sie mehr als einen Endpunkt verwenden, listen Sie die IP-Adressen der Endpunkte wie in dem folgenden Beispiel gezeigt durch einen vertikalen Strich (|) ohne Leerzeichen voneinander getrennt auf:

  ```
  CLOUDURL=URL1_für_Endpunkt|URL2_für_Endpunkt|URL3_für_Endpunkt
  ```

- BUCKETNAME: *Name_des_Buckets_auf_der_Einheit*

  Um die Leistung zu optimieren, verwenden Sie mehrere Endpunkte oder eine Einrichtung für den Lastausgleich.

Nächste Schritte

Konfigurieren Sie Cloud-Containerspeicherpools auf ähnliche Weise wie einen Cloud-Containerspeicherpool für IBM Cloud Object Storage, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

Konfiguration von Cloud-Containerspeicherpools für Microsoft Azure vorbereiten (Off-Premises)

Bevor Sie Cloud-Containerspeicherpools für die Verwendung des Microsoft Azure-Cloud-Computing-Systems konfigurieren können, müssen Sie Informationen für den Konfigurationsprozess von Microsoft abrufen.

Informationen zu diesem Vorgang

IBM Spectrum Protect unterstützt die folgenden Azure-Speicherebenen:

- *Speicherebene 'Heiß' (Hot)* für Daten, auf die häufig zugegriffen wird
- *Speicherebene 'Kalt' (Cool)* für Daten, auf die weniger häufig zugegriffen wird

Eine Speicherebene 'Kalt' (Cool) kann für die kosteneffiziente langfristige Speicherung verwendet werden. Das Zurückschreiben von Daten aus einer Speicherebene 'Kalt' (Cool) ist jedoch kostenintensiver als die Zurückschreibung aus einer Speicherebene 'Heiß' (Hot).

Vorgehensweise

1. Melden Sie sich für ein Microsoft Azure-Konto an, indem Sie das Azure-Portal aufrufen und ein Konto erstellen.
2. Erstellen Sie ein Speicherkonto. In der Regel wählen Sie als Standort für das Speicherkonto den Standort aus, der Ihrem IBM Spectrum Protect-Server am nächsten liegt.
3. Rufen Sie Ihre Azure-Berechtigungsnachweise ab:
   a. Rufen Sie das Azure-Portal auf und klicken Sie auf Speicherkonten.
   b. Öffnen Sie das neue Speicherkonto, wechseln Sie zum Containerabschnitt im Bereich Blob-Dienst und notieren Sie den Wert für den Blob-Dienstendpunkt, damit Sie diesen beim Konfigurieren von Speicherpools verwenden können. Der Blob-Dienstendpunkt ähnelt den Werten in den folgenden Beispielen: https://*Name*.blob.core.windows.net und http://*Name*.blob.core.windows.net.
   c. Erstellen Sie ein SAS-Token (SAS = Shared Access Signature), indem Sie die Registerkarte für Shared Access Signature öffnen und die Felder ausfüllen. Stellen Sie sicher, dass der Bereich Zulässige Dienste 'Blob' umfasst und dass der Bereich für zulässige Ressourcentypen 'Container' und 'Objekt' umfasst. Stellen Sie sicher, dass das SAS-Token über Berechtigungen zum Lesen, Schreiben, Löschen, Auflisten, Hinzufügen und Erstellen verfügt. Klicken Sie auf SAS generieren.
   d. Notieren Sie den SAS-Tokenwert, damit Sie diesen beim Konfigurieren von Speicherpools verwenden können. Da IBM Spectrum Protect das Verfallsdatum des SAS-Tokens nicht überwacht, müssen Sie ein Datum auswählen, das Ihren Anforderungen am besten gerecht wird. Wenn das Token verfällt, geht der Zugriff des IBM Spectrum Protect-Servers auf das Speicherkonto verloren, bis Sie ein neues SAS-Token bereitstellen.
   Tipp: Wenn das SAS-Token seltener aktualisiert werden soll, legen Sie ein Verfallsdatum fest, das mehrere Jahre in der Zukunft liegt. Stellen Sie außerdem sicher, dass die Felder für das Startdatum und die Startzeit verifiziert werden.
4. Wenn Sie planen, Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
   - Cloudtyp: `Azure`
   - SAS-Token: *Wert_für_SAS-Token*. Suchen Sie nach einer ähnlichen Zeichenfolge wie in dem folgenden Beispiel:

     ```
     ?sv=2016-05-31&ss=b&srt=sco&sp=rwdlac&se=2017-04-05T18:26:
     12Z&st=2017-04-05T10:26:12Z&spr=https&sig=
     XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
     ```

   - Blob-Dienstendpunkt: Geben Sie den Blob-Dienstendpunkt für Ihr Azure-Speicherkonto an, beispielsweise https://*Name*.blob.core.windows.net oder http://*Name*.blob.core.windows.net.
5. Wenn Sie planen, Speicherpools mithilfe des Befehls DEFINE STGPOOL zu konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
   - CLOUDTYPE: Azure
   - PASSWORD: *Wert_für_SAS-Token*. Suchen Sie nach einer ähnlichen Zeichenfolge wie in dem folgenden Beispiel:

```
?sv=2016-05-31&ss=b&srt=sco&sp=rwdlac&se=2017-04-05T18:26:
12Z&st=2017-04-05T10:26:12Z&spr=https&sig=
XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
```

- CLOUDURL: Geben Sie den Blob-Dienstendpunkt für Ihr Azure-Speicherkonto an, beispielsweise https://*Name*.blob.core.windows.net oder http://*Name*.blob.core.windows.net.

Nächste Schritte

Konfigurieren Sie Cloud-Containerspeicherpools für Azure, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit Swift vorbereiten (Off-Premises)

Bevor Sie Cloud-Containerspeicherpools für die Off-Premises-Verwendung von IBM® Cloud Object Storage und IBM SoftLayer mit Swift konfigurieren können, müssen Sie Konfigurationsinformationen von der Seite 'Object Storage' in SoftLayer abrufen.

Informationen zu diesem Vorgang

Verwenden Sie die Berechtigungsnachweise Ihres IBM SoftLayer-Kontos, wenn Sie die Speicherpools im Operations Center oder mit dem Befehl DEFINE STGPOOL konfigurieren.

Vorgehensweise

1. Erstellen Sie ein SoftLayer-Konto, indem Sie die Anweisungen in der SoftLayer-Dokumentation ausführen.
2. Rufen Sie Ihre SoftLayer-Berechtigungsnachweise ab:
   a. Rufen Sie die Seite 'Object Storage' in SoftLayer auf und melden Sie sich mit Ihren Kontoberechtigungsnachweisen an.
   b. Wählen Sie das Konto und den Cluster für die Konfiguration aus.
   c. Klicken Sie im Abschnitt Account auf View Credentials.
   d. Lokalisieren Sie im Abschnitt Account Credentials die Felder Public Authentication Endpoint, Username und API Key. Notieren Sie die Werte in diesen Feldern, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
3. Wenn Sie planen, Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
   - Cloudtyp: `IBM Cloud Object Storage - Swift API (SoftLayer)`
   - Benutzername: *Benutzername*
   - Kennwort: *API-Schlüssel*
   - URL: *öffentlicher_Authentifizierungsendpunkt*
4. Wenn Sie planen, Speicherpools mithilfe des Befehls DEFINE STGPOOL zu konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
   - CLOUDTYPE: SOFTLAYER
   - IDENTITY: *Benutzername*
   - PASSWORD: *API-Schlüssel*
   - CLOUDURL: *öffentlicher_Authentifizierungsendpunkt*

Nächste Schritte

Konfigurieren Sie Cloud-Containerspeicherpools für IBM SoftLayer, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit S3 vorbereiten (Off-Premises)

Sie können Cloudspeicherpools für die Off-Premises-Verwendung von IBM® Cloud Object Storage mit dem Protokoll 'Simple Storage Service' (S3) konfigurieren.

Informationen zu diesem Vorgang

Die Off-Premises-Implementierung von IBM Cloud Object Storage wird über IBM SoftLayer oder IBM Bluemix verwaltet. Bei dieser Konfiguration kann nur der Eigner des SoftLayer- oder Bluemix-Kontos Buckets und Administratoren erstellen.

Verwenden Sie die Berechtigungsnachweise Ihres IBM SoftLayer- oder IBM Bluemix-Kontos, wenn Sie die Speicherpools im Operations Center oder mit dem Befehl DEFINE STGPOOL konfigurieren. Weitere Informationen finden Sie auf der Seite 'Objektspeicher' in SoftLayer. Um diese Konfiguration zu verwenden, wählen Sie Cloud Object Storage - S3 API auf der Seite 'Order Object Storage' in SoftLayer aus.

Vorgehensweise

1. Melden Sie sich beim SoftLayer-Kundenportal an.
2. Klicken Sie auf das Menü Storage und wählen Sie Object Storage aus.
3. Wählen Sie auf der Seite 'Object Storage' ein S3-Konto aus.
4. Klicken Sie auf der Seite 'Cloud Object Storage' auf Manage Buckets und anschließend auf das Symbol +, um das Bucket zu erstellen, das mit dem neuen Cloud-Containerspeicherpool verwendet werden soll.
5. Klicken Sie auf Show Credentials, um Administratorberechtigungsnachweise für Ihr neues Bucket zu erstellen.
6. Klicken Sie auf Add Credential.
7. Lokalisieren Sie die Zugriffsschlüssel-ID (Access Key ID), den geheimen Zugriffsschlüssel (Secret Access Key) und den öffentlichen Authentifizierungsendpunkt (Public Authentication Endpoint). Notieren Sie die Werte in diesen Feldern, damit Sie diese beim Konfigurieren von Speicherpools verwenden können. Innerhalb des SoftLayer-Netzes können Sie einen privaten Authentifizierungsendpunkt verwenden.
8. Um Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, wählen Sie Off-Premises-Cloud aus. Verwenden Sie für die Parameter die folgenden Werte:
   - Cloudtyp: `IBM Cloud Object Storage - S3 API (SoftLayer)`
   - Zugriffsschlüssel-ID: *Zugriffsschlüssel-ID*
   - Geheimer Zugriffsschlüssel: *geheimer_Zugriffsschlüssel*
   - Bucketname: *Bucketname* (aus Schritt 4)
   - URL: *us-geo-Authentifizierungsendpunkt*
     Anmerkung: Bei dieser Konfiguration ist nur ein einziger Cloud-Provider-Endpunkt erforderlich. Wenn sich alle Ihre Server innerhalb des SoftLayer-Netzes befinden, können Sie einen privaten Authentifizierungsendpunkt verwenden.
9. Wenn Sie Speicherpools mithilfe des Befehls DEFINE STGPOOL konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
   - CLOUDTYPE: S3
   - IDENTITY: *Zugriffsschlüssel-ID*
   - BUCKETNAME: *Bucketname* (aus Schritt 4)
   - PASSWORD: *geheimer_Zugriffsschlüssel*
   - CLOUDURL: *us-geo-Authentifizierungsendpunkt*
     Anmerkung: Bei dieser Konfiguration ist nur ein einziger Cloud-Provider-Endpunkt erforderlich. Wenn sich alle Ihre Server innerhalb des SoftLayer-Netzes befinden, können Sie einen privaten Authentifizierungsendpunkt verwenden.

Nächste Schritte

Konfigurieren Sie Cloud-Containerspeicherpools für IBM SoftLayer Cloud Object Storage, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

Konfiguration von Cloud-Containerspeicherpools für IBM Cloud Object Storage mit S3 vorbereiten (On-Premises)

Bevor Sie Cloud-Containerspeicherpools für die On-Premises-Verwendung von IBM® Cloud Object Storage mit S3 konfigurieren können, müssen Sie eine IBM Cloud Object Storage-Vaultvorlage und ein IBM Cloud Object Storage-Benutzerkonto definieren und dann Konfigurationsinformationen abrufen.

Informationen zu diesem Vorgang

IBM Cloud Object Storage-Vaults werden auf dieselbe Art und Weise wie Container in einem Cloud-Containerspeicherpool verwendet. Definieren Sie eine Vaultvorlage, um Vaults schnell mit Ihren bevorzugten Einstellungen erstellen zu können.

Verwenden Sie nach dem Erstellen einer Vaultvorlage die Berechtigungsnachweise Ihres IBM Cloud Object Storage-Benutzerkontos, um die Speicherpools im Operations Center oder mit dem Befehl DEFINE STGPOOL zu konfigurieren. IBM Spectrum Protect verwendet das Protokoll 'Simple Storage Service' (S3) für die Kommunikation mit IBM Cloud Object Storage.

Tipp: Sie können die ersten vier Schritte in der Prozedur überspringen, wenn eine Vault konfiguriert werden soll, die bereits vorhanden ist, indem Sie den Parameter BUCKETNAME im Befehl DEFINE STGPOOL oder UPDATE STGPOOL verwenden.

Vorgehensweise

1. Erstellen Sie eine Vaultvorlage:
   a. Melden Sie sich bei IBM Cloud Object Storage an und klicken Sie auf die Registerkarte Configure.
   b. Erweitern Sie im Navigationsfenster dsNet die Option Storage Pools.
   c. Wählen Sie den IBM Cloud Object Storage-Speicherpool aus, für den die Vaultvorlage erstellt werden soll, und klicken Sie auf den Link Storage Pool im Abschnitt General.
   d. Klicken Sie im Abschnitt Vault Templates auf Create Vault Template.
   e. Wählen Sie die Einstellungen für die Standardvaultvorlage aus. Unter Umständen können Sie die Leistung optimieren, indem Sie die Option Enable SecureSlice Technology oder Name Index Enabled nicht auswählen und die Option Recovery Listing Enabled auswählen.
   f. Wählen Sie im Abschnitt Deployment den oder die Zugriffspools aus, die für die Vorlage verwendet werden sollen, und klicken Sie auf Save.
2. Legen Sie die Vaultvorlage als Standardvaultvorlage für Ihr IBM Cloud Object Storage-dsNet fest:

a. Klicken Sie auf die Registerkarte Configure.
b. Klicken Sie im Abschnitt Default Vault Template Configuration auf Configure.
c. Wählen Sie eine Vaultvorlage aus, die als Standardvaultvorlage verwendet werden soll, und klicken Sie auf Update, um diese Vorlage als Standardvorlage festzulegen.

3. Wenn Sie zum ersten Mal eine Vaultvorlage konfigurieren, aktivieren Sie die Rolle für die Vaultbereitstellung, damit Sie neue Vaults erstellen können:
   a. Klicken Sie auf die Registerkarte Administration.
   b. Klicken Sie im Abschnitt Provisioning API Configuration auf Configure.
   c. Wählen Sie Create Only oder Create and Delete aus, damit Benutzer neue Vaults mithilfe der Bereitstellungs-API (Provisioning API) erstellen können.
   d. Klicken Sie auf Update, um die Einstellungen zu speichern.
4. Verwenden Sie ein IBM Cloud Object Storage-Konto mit Administratorberechtigung, um ein Benutzerkonto für die IBM Cloud Object Storage-Instanz in Ihrer Umgebung zu erstellen. Stellen Sie sicher, dass das neue Benutzerkonto über die Rolle Vault Provisioner verfügt.
5. Klicken Sie auf die Registerkarte Security und wählen Sie das neue Benutzerkonto aus.
6. Generieren Sie einen Zugriffsschlüssel für den neuen Benutzer:
   a. Klicken Sie im Abschnitt Access Key Authentication auf Change Keys.
   b. Klicken Sie auf der Seite Edit Access Key auf Generate New Access Key.
   c. Klicken Sie auf Back.
7. Lokalisieren Sie im Abschnitt Access Key Authentication die Werte für Access Key ID und Secret Access Key. Notieren Sie die Werte, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
8. Lokalisieren Sie den Wert für die URL:
   a. Klicken Sie auf die Registerkarte Configure.
   b. Erweitern Sie im Navigationsfenster dsNet die Abschnitte Devices und Accesser.
   c. Wählen Sie den IBM Cloud Object Storage-Accesser aus. Stellen Sie sicher, dass der Accesser zu einem Zugriffspool gehört, für den die Standardvaultvorlage implementiert ist.
   d. Notieren Sie den im Abschnitt Device Configuration für den Accesser angegebenen Wert für IP Address, damit Sie diesen beim Konfigurieren von Speicherpools verwenden können. Geben Sie `http://` vor dem Wert für die IP-Adresse an, um Zertifikatssicherheitsfehler zu verhindern.
9. Wenn Sie Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
   - Cloudtyp: `IBM Cloud Object Storage - S3 API`
   - Zugriffsschlüssel-ID: *Zugriffsschlüssel-ID*
   - Geheimer Zugriffsschlüssel: *geheimer_Zugriffsschlüssel*
   - Bucketname: Verwenden Sie den vom Server generierten Standardbucketnamen oder geben Sie einen neuen Bucketnamen an.
   - URL: `http://`*IP-Adresse_des_Cloud_Object_Storage-Accessers*
     Wichtig: Wenn mehr als ein Accesser verwendet wird, geben Sie die IP-Adresse eines Accessers ein und drücken Sie dann die Eingabetaste, um weitere IP-Adressen hinzuzufügen. Verwenden Sie zur Erzielung der optimalen Leistung mehrere Accesser oder eine Einrichtung für den Lastausgleich.
10. Wenn Sie Speicherpools mithilfe des Befehls DEFINE STGPOOL konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
    - CLOUDTYPE: S3
    - IDENTITY: *Zugriffsschlüssel-ID*
    - PASSWORD: *geheimer_Zugriffsschlüssel*
    - CLOUDURL: `http://`*IP-Adresse_des_Cloud_Object_Storage-Accessers*
      Wichtig: Wenn Sie mehr als einen Accesser verwenden, listen Sie die IP-Adressen der Accesser durch einen vertikalen Strich (|) ohne Leerzeichen voneinander getrennt auf. Beispiel: *CLOUDURL=<Accesser-URL1>|<Accesser-URL2>|<Accesser-URL3>*.
      Verwenden Sie zur Erzielung der optimalen Leistung mehrere Accesser oder eine Einrichtung für den Lastausgleich.

Nächste Schritte

Konfigurieren Sie Cloud-Containerspeicherpools für IBM Cloud Object Storage, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

Konfiguration von Cloud-Containerspeicherpools für OpenStack mit Swift vorbereiten

Bevor Sie Cloud-Containerspeicherpools für die On-Premises- oder Off-Premises-Verwendung von OpenStack mit Swift konfigurieren können, müssen Sie Konfigurationsinformationen vom OpenStack Swift-Computer abrufen.

Informationen zu diesem Vorgang

Verwenden Sie die Berechtigungsnachweise Ihres OpenStack Swift-Kontos, wenn Sie die Speicherpools mit dem Operations Center oder dem Befehl DEFINE STGPOOL konfigurieren.

Vorgehensweise

1. Erstellen Sie ein OpenStack Swift-Konto, indem Sie die Anweisungen in der OpenStack Swift-Dokumentation ausführen.

2. Rufen Sie Ihre OpenStack Swift-Berechtigungsnachweise ab:
   a. Geben Sie auf dem OpenStack Swift-Computer den folgenden Befehl ein:

      ```
      swift auth -v
      ```

   b. Lokalisieren Sie in der Ausgabe die Werte für `OS_AUTH_URL`, `OS_TENANT_NAME`, `OS_USERNAME` und `OS_PASSWORD`. Notieren Sie die Werte, damit Sie diese beim Konfigurieren von Speicherpools verwenden können.
3. Wenn Sie planen, Speicherpools mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center zu konfigurieren, verwenden Sie die folgenden Werte für die Parameter:
   - Cloudtyp: `OpenStack Swift`
   - Benutzername: *OS-Tenantname:OS-Benutzername*
   - Kennwort: *OS-Kennwort*
   - URL: *OS-Authentifizierungs-URL*
4. Wenn Sie planen, Speicherpools mithilfe des Befehls DEFINE STGPOOL zu konfigurieren, verwenden Sie die folgenden Werte für die Befehlsparameter:
   - CLOUDTYPE: SWIFT oder V1SWIFT
   - IDENTITY: *OS-Tenantname:OS-Benutzername*
   - PASSWORD: *OS-Kennwort*
   - CLOUDURL: *OS-Authentifizierungs-URL*
5. Wenn Sie planen, einen bestimmten Tenant- oder Benutzernamen zu verwenden, notieren Sie die Werte in folgendem Format: *Tenantname:Benutzername*.
6. Um einen Datenverlust zu verhindern, konfigurieren OpenStack Swift zum Erstellen von Replikaten der Daten, die in den OpenStack Swift-Objektspeicher geschrieben werden. Weitere Informationen enthält die OpenStack Swift-Dokumentation.

Nächste Schritte

Konfigurieren Sie Cloud-Containerspeicherpools für OpenStack Swift, indem Sie die Anweisungen in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren ausführen.

Daten für Cloud-Containerspeicherpools verschlüsseln

Daten, die in Off-Premises-Cloud-Container-Pools gespeichert werden, werden standardmäßig verschlüsselt. Daten in On-Premises-Cloud-Containerspeicherpools können wahlweise verschlüsselt werden.

Informationen zu diesem Vorgang

Informationen zum Verschlüsseln von Daten in Cloud-Containerspeicherpools und zu Leistungsaspekten bei der Verschlüsselung von Daten, finden Sie in der Technote 1963635.

Leistung für Cloudobjektspeicher optimieren

Sie können IBM Spectrum Protect so konfigurieren, dass Daten während der Datenaufnahme vorübergehend in einem oder mehreren lokalen Speicherpoolverzeichnissen gespeichert werden. Die Daten werden dann aus dem lokalen Speicher in die Cloud übertragen. Auf diese Art und Weise können Sie die Datensicherungs- und -archivierungsleistung verbessern.

Vorbereitende Schritte

Um die Sicherungs- und Archivierungsleistung zu optimieren, müssen Sie sicherstellen, dass IBM Spectrum Protect Version 8.1 installiert ist.

Informationen zu diesem Vorgang

Nachdem Sie ein Speicherpoolverzeichnis definiert haben, verwendet der IBM Spectrum Protect-Server dieses Verzeichnis als temporären Speicherplatz für die Daten, die Sie in den Cloudobjektspeicher übertragen. Der Server verwendet einen automatisierten Hintergrundprozess, um die Daten aus dem lokalen Speicher im Verzeichnis in den Cloudobjektspeicher zu übertragen. Sie müssen keine zusätzlichen Schritte ausführen, um diesen Übertragungsprozess zu starten oder zu verwalten. Nachdem der Server die Daten erfolgreich aus dem lokalen Speicher in den Cloudobjektspeicher übertragen hat, löscht der Server die Daten aus dem Verzeichnis und gibt Speicherbereich für weitere ankommende Daten frei.

Wenn Speicherpoolverzeichnisse keinen freien Speicherbereich mehr enthalten, werden Sicherungsoperationen vorzeitig gestoppt. Um diese Situation zu vermeiden, können Sie weitere Speicherpoolverzeichnisse zuordnen. Sie können auch warten, bis die Daten nach der Übertragung in die Cloud automatisch aus den lokalen Verzeichnissen entfernt werden. Die erforderliche Anzahl Speicherpoolverzeichnisse, die Sie definieren müssen, ist von Ihrer Plattenkonfiguration auf dem Server abhängig. Wenn die Erstsicherung erfolgt, verteilt der Server die Daten über alle definierten Verzeichnisse.

Der Umfang des Speicherbereichs, der für lokalen Speicher benötigt wird, basiert auf dem erwarteten Datenvolumen nach der Datendeduplizierung und Komprimierung, das täglich gesichert werden muss. Wenn Sie über eine stabile Netzverbindung zum Cloudobjektspeicher verfügen, entspricht der erforderliche Speicherbedarf in etwa dem für eine tägliche Sicherung erforderlichen Speicherbereich.

Zusätzliche Planungsinformationen finden Sie in dem Abschnitt für Ihr Betriebssystem:

- AIX: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools
- Linux: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools
- Windows: Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools

Vorgehensweise

1. Erstellen Sie einen Cloud-Containerspeicherpool mithilfe des Assistenten 'Speicherpool hinzufügen' im Operations Center. Es ist auch möglich, den Pool mithilfe des Befehls DEFINE STGPOOL zu erstellen.
2. Definieren Sie ein oder mehrere Speicherpoolverzeichnisse mithilfe des Befehls DEFINE STGPOOLDIRECTORY. Stellen Sie sicher, dass jedes Speicherpoolverzeichnis sein eigenes Dateisystem hat. Verwenden Sie auf Linux-Systemen das xfs- oder ext4-Dateisystem statt des ext3-Dateisystems, da das Löschen großer Dateien bei ext3 länger dauert. Stellen Sie sicher, dass die neuen Speicherpoolverzeichnisse weder das Stammdateisystem noch dieselben Dateisysteme gemeinsam nutzen, die von anderen IBM Spectrum Protect-Ressourcen, wie beispielsweise der Datenbank oder den Protokollen, verwendet werden.

Zugehörige Verweise:
DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Speicherbereich in Containerspeicherpools verwalten

Nachdem Sie IBM Spectrum Protect konfiguriert und Speicherbereich hinzugefügt haben, müssen Sie Ihre Daten und Ihren Speicherbereich im Speicherpool effektiv verwalten, um die ordnungsgemäße Funktion zu gewährleisten. Maximieren Sie Ihren Speicherbereich und die Serverleistung mithilfe von Containerspeicherpools.

Informationen zu diesem Vorgang

Containerspeicherpools sind primäre Speicherpools, die für Inline-Datendeduplizierung, Inline-Komprimierung und Cloudspeicher verwendet werden.
Einschränkung: Folgende Funktionen können bei Containerspeicherpools nicht verwendet werden:

- Umlagerung
- Konsolidierung
- Zusammenfassung
- Kollokation
- Export
- Import
- Gleichzeitiges Schreiben
- Speicherpoolsicherung
- Virtuelle Datenträger

Vorgehensweise

1. Erstellen Sie einen Verzeichniscontainerspeicherpool, indem Sie die folgenden Schritte ausführen:
   a. Öffnen Sie das Operations Center.
   b. Klicken Sie in der Menüleiste des Operations Center auf Speicher > Speicherpools.
   c. Klicken Sie auf +Speicherpool.
   d. Führen Sie die Schritte im Assistenten Speicherpool hinzufügen aus:
      - Um die Inline-Datendeduplizierung verwenden zu können, wählen Sie einen Speicherpool Verzeichnis unter dem containerbasierten Speicher aus.
      - Wenn Sie Verzeichnisse für den Verzeichniscontainerspeicherpool konfigurieren, geben Sie die Verzeichnispfade an, die während der Systemkonfiguration für Speicher erstellt wurden.
   e. Klicken Sie nach dem Konfigurieren des neuen Verzeichniscontainerspeicherpools auf Schließen & Maßnahmen anzeigen, um eine Verwaltungsklasse zu aktualisieren und mit der Verwendung des Speicherpools zu beginnen.
2. Um eine optimale Leistung bei Containerspeicherpools zu erzielen, führen Sie die folgenden Tasks aus:

Task	Prozedur	Weitere Informationen
Speicherpool schützen	Wenn Sie im Operations Center einen Verzeichniscontainerspeicherpool erstellen, können Sie Speicherpoolschutz in dem Zeitplan konfigurieren, den Sie dem Speicherpool zuordnen. Sie können auch stattdessen den Befehl PROTECT STGPOOL auf dem Quellenserver verwenden, um Datenbereiche in einem Verzeichniscontainerspeicherpool zu sichern.	○ Daten in Verzeichniscontainerspeicherpools schützen ○ PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)

	Indem ein Speicherpool geschützt wird, werden keine Ressourcen verwendet, die vorhandene Daten und Metadaten replizieren, wodurch die Serverleistung verbessert wird.	
Speicherpool reparieren	Wenn ein Speicherpool geschützt ist, können Sie beschädigte Datenbereiche mit dem Befehl REPAIR STGPOOL reparieren. Verwenden Sie den Befehl REPAIR STGPOOL, um einen Verzeichniscontainerspeicherpool zu reparieren. Einschränkung: Wenn Sie Clientknoten replizieren, den Verzeichniscontainerspeicherpool aber nicht schützen, können Sie den Speicherpool nicht reparieren.	◦ Speicherpools reparieren ◦ REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)
Container löschen	Container werden im Bestand gelöscht, wenn Dateidaten entfernt werden oder verfallen. Steuern Sie mithilfe des Befehls DEFINE STGPOOL unter Angabe des Parameters REUSEDELAY, wie lange deduplizierte Speicherbereiche einem Verzeichniscontainerspeicherpool zugeordnet bleiben, nachdem sie nicht mehr referenziert werden. Wenn ein Container beschädigt ist, verwenden Sie den Befehl AUDIT CONTAINER, um Daten wiederherzustellen oder zu entfernen.	◦ DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren) ◦ AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)
Einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, konvertieren	Sie können einen vorhandenen Speicherpool in einen Verzeichniscontainerspeicherpool konvertieren, indem Sie die Schritte in Primären Speicherpool in einen Containerspeicherpool konvertieren ausführen. Einschränkung: Die folgenden Speicherpooltypen können nicht konvertiert werden: ◦ Primäre Speicherpools, die Einheitenklassen für Einheiten mit wahlfreiem Zugriff (DISK) verwenden ◦ Kopienspeicherpools ◦ Speicherpools für aktive Daten	◦ CONVERT STGPOOL (Speicherpool in einen Containerspeicherpool konvertieren)
Containerspeicherpoolbelegung überwachen	Überwachen Sie die Speicherlösung, um vorhandene und potenzielle Probleme zu ermitteln. Weitere Informationen finden Sie in Speicherlösungen überwachen.	

- Primären Speicherpool in einen Containerspeicherpool konvertieren
  Konvertieren Sie einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Containerspeicherpool. Daten, die in einem Containerspeicherpool gespeichert sind, können sowohl die Inline-Datendeduplizierung als auch die Inline-Komprimierung verwenden.
- Daten in einem Quellenspeicherpool bereinigen
  Um einen Speicherpool in einen Verzeichniscontainerspeicherpool zu konvertieren, müssen Sie gegebenenfalls beschädigte Daten oder Dateien bereinigen, die sich im Quellenspeicherpool befinden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Primären Speicherpool in einen Containerspeicherpool konvertieren

Konvertieren Sie einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Containerspeicherpool. Daten, die in einem Containerspeicherpool gespeichert sind, können sowohl die

Inline-Datendeduplizierung als auch die Inline-Komprimierung verwenden.

Vorbereitende Schritte

Um sicherzustellen, dass Datenträger in einem Quellenspeicherpool und zugehörigen Kopienspeicherpools während eines Konvertierungsprozesses nicht wiederverwendet werden, geben Sie für den Parameter REUSEDELAY im Befehl UPDATE STGPOOL einen Wert an. Geben Sie für den Parameter REUSEDELAY einen Wert an, der größer als der Wert für die Konvertierungsdauer ist. Möglicherweise müssen Sie die Wiederverwendung von Datenträgern aus den folgenden Gründen verzögern:

- Die Daten werden während der Speicherpoolkonvertierung versehentlich gelöscht.
- Es ist Quellenspeicherpoolfunktionalität erforderlich, die in Containerspeicherpools nicht verfügbar ist.

Tipp: Wenn Sie den Parameter REUSEDELAY angeben, während eine Konvertierungsoperation in Bearbeitung ist, ist ein Teil des Speicherbereichs im Quellenspeicherpool erst wieder verfügbar, wenn die durch den Wert für den Parameter angegebene Zeit abläuft.
Erstellen Sie einen Containerspeicherpool, in den die Daten versetzt werden sollen, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf der Seite Speicherpools im Operations Center auf + Speicherpool.
2. Führen Sie die Schritte im Assistenten 'Speicherpool hinzufügen' aus. Wählen Sie den Typ des erforderlichen containerbasierten Speichers aus.

Informationen zu diesem Vorgang

Wenn Sie einen Speicherpool in einen Containerspeicherpool konvertieren, ist keine Datenträgerkonsolidierung erforderlich. Das Entfallen von Datenträgerkonsolidierungsoperationen kann dazu beitragen, die Serverleistung zu verbessern und den Umfang der erforderlichen Speicherhardware zu reduzieren.

Beim Konvertieren von Dateien werden alle in Kopienpools oder Pools für aktive Daten gespeicherten Kopien gelöscht.
Einschränkungen:

- Wenn der Quellenpool in einer aktiven Maßnahmengruppe als Sicherungs-, Archivierungs- oder Umlagerungsziel mit anstehenden Änderungen angegeben ist, müssen Sie diese Änderungen aktivieren, bevor Sie den Pool konvertieren können.
- Um sicherzustellen, dass das Ziel einen Speicherpool angibt, der nicht konvertiert wurde bzw. gerade konvertiert wird, müssen Sie alle Maßnahmen aktualisieren, die den Quellenspeicherpool referenzieren.
- Wenn der Quellenspeicherpool als nächster Speicherpool angegeben ist, müssen Sie den Parameter NEXTSTGPOOL im Befehl UPDATE STGPOOL aktualisieren, um einen Speicherpool mit wahlfreiem oder sequenziellem Zugriff anzugeben, der nicht gerade konvertiert wird.
- Die folgenden Datentypen sind für die Konvertierung nicht auswählbar: Sicherungen von Inhaltsverzeichnissen (TOC-Sicherungen), virtuelle Datenträger und Network Data Management Protocol-Daten (NDMP-Daten). Bevor Sie den Konvertierungsprozess starten, müssen Sie diese Datentypen manuell aus dem Speicherpool löschen und die Datentypen in einen anderen primären Speicherpool versetzen oder die Datentypen müssen auf der Basis von Maßnahmeneinstellungen verfallen können.
- Wenn Sie einen Speicherpool mit einer Einheitenklasse FILE in einen Verzeichniscontainerpool konvertieren, sollte der Zielspeicherpool ungefähr 30 % größer als der Quellenspeicherpool sein. Zusätzlicher Speicherbereich ist in der Regel nicht erforderlich, wenn Sie andere Speicherpooltypen konvertieren.

  Weitere Informationen zu Best Practices für die die Speicherpoolkonvertierung finden Sie in Best practices for IBM Spectrum Protect storage pool conversion.

- Wenn der Quellenspeicherpool zum Speichern von TOC-Sicherungen verwendet wird, stellen Sie sicher, dass ein weiterer primärer Speicherpool zum Speichern neuer TOC-Sicherungen verfügbar ist. Vorhandene TOC-Sicherungen werden im Rahmen der Konvertierung nicht versetzt.

  Der TOC-Pool muss das Datenformat NATIVE oder NONBLOCK und eine andere Einheitenklasse als Centera haben. Verwenden Sie die Einheitenklasse DISK oder FILE, um Mountverzögerungen zu verhindern.

Vorgehensweise

1. Wählen Sie auf der Seite Speicherpools im Operations Center einen Speicherpool aus, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet.
2. Klicken Sie auf Weitere > Konvertieren und führen Sie die Schritte im Assistenten 'Speicherpool konvertieren' aus.
   Tipp: Planen Sie für die Konvertierung eines Speicherpools, der eine Einheitenklasse FILE verwendet, mindestens 2 Stunden ein und für die Konvertierung eines Speicherpools, der ein VTL verwendet, mindestens 4 Stunden.

Nächste Schritte

Wenn der Konvertierungsprozess abgeschlossen ist, kann der Quellenspeicherpool unter Umständen beschädigte Daten oder Daten enthalten, die mit Containerspeicherpools inkompatibel sind. Bereinigen Sie den Quellenspeicherpool, indem Sie die Schritte in Objekte in einem Quellenspeicherpool bereinigen ausführen.

Zugehörige Tasks:
Datenbank zurückschreiben
 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Daten in einem Quellenspeicherpool bereinigen

Um einen Speicherpool in einen Verzeichniscontainerspeicherpool zu konvertieren, müssen Sie gegebenenfalls beschädigte Daten oder Dateien bereinigen, die sich im Quellenspeicherpool befinden.

Vorgehensweise

Verwenden Sie die folgenden Optionen, um beschädigte Daten wiederherzustellen oder zu reparieren.

- Stellen Sie eine unbeschädigte Version der Daten aus einem Kopienspeicherpool oder Speicherpool für aktive Daten wieder her, indem Sie den Befehl RESTORE STGPOOL ausgeben.
- Stellen Sie eine unbeschädigte Version der Daten von einem Zielreplikationsserver wieder her, indem Sie den Befehl REPLICATE NODE unter Angabe des Parameters RECOVERDAMAGED=YES ausgeben.
- Entfernen Sie Daten, die nicht repariert werden können, nach der Speicherpoolkonvertierung, indem Sie den Befehl REMOVE DAMAGED ausgeben.
  Mit dem Befehl REMOVE DAMAGED werden möglicherweise keine Datenträger entfernt, die im Quellenspeicherpool als dauerhaft beschädigt markiert sind. Um diese Datenträger zu entfernen, führen Sie die folgenden Schritte aus:
  a. Geben Sie den Befehl DELETE VOLUME unter Angabe des Parameters DISCARDDATA=YES aus.
  b. Geben Sie den Befehl CONVERT STGPOOL aus, um den Speicherpool erneut zu konvertieren.
  c. Wenn während der Speicherpoolkonvertierung beschädigte Daten erkannt werden, geben Sie den Befehl REMOVE DAMAGED erneut aus.
- Führen Sie die in der Technote 1666371 beschriebenen Analysetasks aus.

Nächste Schritte

Nachdem Sie die beschädigten Daten wiederhergestellt oder repariert haben, wiederholen Sie die Konvertierung, indem Sie den Befehl CONVERT STGPOOL ausgeben.
Um Informationen zu beschädigten Dateien anzuzeigen, die im Quellenspeicherpool verblieben sind, geben Sie den Befehl QUERY CLEANUP aus.
Tipp: Wenn für einen Speicherpool, der keine Daten enthält, ein Bereinigungsstatus angezeigt wird, können Sie den Speicherpool mit dem Befehl DELETE STGPOOL löschen.
Zugehörige Verweise:
DELETE VOLUME (Speicherpooldatenträger löschen)
QUERY CLEANUP (In einem Quellenspeicherpool erforderliche Bereinigung abfragen)
REMOVE DAMAGED (Beschädigte Daten aus einem Quellenspeicherpool entfernen)
REPLICATE NODE (Daten in Dateibereichen replizieren, die zu einem Clientknoten gehören)
RESTORE STGPOOL (Speicherpooldaten aus einem Kopienpool oder einem Pool für aktive Daten zurückschreiben)

Speicherpoolcontainer prüfen

Mit der Prüfung eines Speicherpoolcontainers wird auf Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Speicherpool geprüft.

Informationen zu diesem Vorgang

Sie prüfen einen Speicherpoolcontainer in den folgenden Situationen:

- Sie geben den Befehl QUERY DAMAGED aus und es wird ein Problem erkannt.
- Der Server zeigt Nachrichten zu beschädigten Datenbereichen an.
- Ihre Hardware meldet ein Problem und es werden Fehlernachrichten angezeigt, die sich auf den Speicherpoolcontainer beziehen.

Vorgehensweise

1. Um einen Speicherpoolcontainer zu prüfen, geben Sie den Befehl AUDIT CONTAINER aus. Geben Sie beispielsweise den folgenden Befehl aus, um den Container 000000000000076c.dcf zu prüfen:

   ```
   audit container c:\tsm-storage\07\000000000000076c.dcf
   ```

2. Überprüfen Sie die Ausgabe der Nachricht ANR4891I auf Informationen zu allen beschädigten Datenbereichen.

Nächste Schritte

Wenn Sie Probleme mit dem Speicherpoolcontainer erkennen, können Sie Daten auf der Basis Ihrer Konfiguration zurückschreiben. Sie können den Inhalt des Speicherpools mit dem Befehl REPAIR STGPOOL reparieren.
Einschränkung: Sie können den Inhalt des Speicherpools nur reparieren, wenn der Speicherpool mit dem Befehl PROTECT STGPOOL geschützt wurde.
Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainerspeicherpool prüfen)

QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool abfragen)

Speichersystemvoraussetzungen und Reduzierung des Risikos fehlerhafter Daten

Für den IBM Spectrum Protect-Server können viele Typen von Speicher verwendet werden. Wenn Sie Plattenblockspeicher, Solid-State-Laufwerke (SSDs) oder an das Netz angeschlossene Dateisysteme als Serverspeicher verwenden, müssen Sie sicherstellen, dass der Speicher die Voraussetzungen erfüllt.

Die folgenden Voraussetzungen gelten für Speicher für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll sowie für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden, und für Verzeichniscontainerspeicherpools.

Speicher kann mit jeder Methode, die für das Betriebssystem gültig ist, an das Serversystem angeschlossen werden. Beispielsweise kann der Speicher direkt angeschlossen werden oder unter Verwendung der Fibre Channel- oder iSCSI-Technologie.

Da viele Speichersysteme die Voraussetzungen für Serverspeicher erfüllen können, ist eine Liste derartiger Einheiten nicht verfügbar. Wenden Sie sich an den Hersteller, wenn Sie nicht wissen, ob ein System die IBM Spectrum Protect-Voraussetzungen erfüllt.

Ausführliche Informationen zu Dateisystemvoraussetzungen enthält die Technote 1902417. Ausführliche Informationen zu NFS-Voraussetzungen enthält die Technote 1470193.

Speicher- und Dateisysteme müssen Schreib- und Festschreibergebnisse synchron und korrekt an den IBM Spectrum Protect-Server zurückmelden. Nicht zurückgemeldete oder asynchron zurückgemeldete Schreibfehler, die zur Folge haben, dass Daten nicht permanent im Speichersystem festgeschrieben werden, können fehlerhafte Daten zur Folge haben. Fehlerhafte Daten können betriebsbezogene Fehler verursachen, einschließlich des Fehlschlagens, den Server starten zu können, und erfordern in der Regel eine Datenwiederherstellung.

Die folgenden Informationen enthalten Tipps, wie das Risiko fehlerhafter Daten verringert werden kann:

Schreibcache
: Plattensysteme verwenden Schreibcache zur Verbesserung der Systemleistung. Um das Risiko fehlerhafter Daten zu verringern, muss das Speichersystem die Daten im Schreibcache zuverlässig in permanentem Speicher festschreiben.

  Der Schreibcache verfügt normalerweise über eine Batterie, um den Verlust von Daten im Cache während eines kurzen Stromausfalls zu verhindern. Bei kritischen Systemen sollten Sie die Bereitstellung einer Notstromversorgung in Erwägung ziehen, um den Cache bei längeren Stromausfällen zu schützen.

Direkte E/A
: Die direkte E/A erfüllt die Anforderungen des Servers in Bezug auf das synchrone und korrekte Zurückmelden bei Schreib- und Festschreibungsoperationen für Daten.
  Achtung: Sie dürfen die direkte E/A nicht in Situationen inaktivieren, in denen das Schreibcaching einen Datenverlust zur Folge haben könnte. Das Inaktivieren der direkten E/A kann die Wahrscheinlichkeit eines Datenverlusts stark erhöhen, da zusätzlich zum Plattensystem mehr Daten vom Dateisystem zwischengespeichert werden.

Speicherreplikation
: Umgebungen, die IBM Spectrum Protect-Speicher replizieren, müssen Funktionen wie die Beibehaltung der Schreibreihenfolge zwischen der Quelle (dem lokalen Server) und dem Ziel (dem fernen Server) verwenden. Die Datenbank, die aktive Protokolldatei, die Archivprotokolle und die Speicherpools müssen zu einer Konsistenzgruppe gehören. Eine Konsistenzgruppe verwaltet Beziehungen zwischen Datenträgern, um die Schreibreihenfolge beizubehalten, damit eine Wiederherstellung der Datenträger möglich ist. Jede Ein-/Ausgabe für die Mitglieder der Zielkonsistenzgruppe muss in derselben Reihenfolge wie die der Quelle geschrieben werden und dieselben Volatilitätsmerkmale haben.

  Um die Synchronisation zwischen IBM Spectrum Protect-Servern am lokalen und fernen Standort zu gewährleisten, dürfen Sie einen Server am fernen Standort nur in einer Übernahmesituation starten. Überwachen Sie die Synchronisation der Daten am lokalen und fernen Standort. Wenn die Synchronisation verloren geht, müssen Sie den Server am fernen Standort mithilfe von IBM Spectrum Protect-Zurückschreibungsbefehlen für die Datenbank und Speicherpools zurückschreiben.

Tipps zur Speicherkonfiguration

Tipps zur Speicherkonfiguration zur Optimierung der Systemleistung liefern die folgenden Themen in der Produktdokumentation der Version 7.1.1. Die Informationen in den Prüflisten können auf höhere Releases angewendet werden.

- Prüfliste für Platten für die Serverdatenbank
- Prüfliste für Platten für das Serverwiederherstellungsprotokoll
- Prüfliste für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden

Speicherlösungen überwachen

Nach der Implementierung einer IBM Spectrum Protect-Lösung müssen Sie die Lösung überwachen, um sicherzustellen, dass sie ordnungsgemäß funktioniert. Indem die Lösung täglich und regelmäßig überwacht wird, können Sie bestehende und potenzielle Probleme erkennen. Die zusammengestellten Informationen können zur Fehlerbehebung und zur Optimierung der Systemleistung verwendet werden.

Informationen zu diesem Vorgang

Die bevorzugte Art und Weise zur Überwachung einer Lösung erfolgt über die Verwendung des Operations Center, das den Gesamtsystemstatus und den detaillierten Systemstatus in einer grafischen Benutzerschnittstelle bereitstellt. Darüber hinaus können Sie das Operations Center zum Generieren von E-Mail-Berichten mit einer Zusammenfassung des Systemstatus konfigurieren.

Vorgehensweise

1. Führen Sie tägliche Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für tägliche Überwachungstasks.
2. Führen Sie regelmäßige Überwachungstasks aus. Anweisungen finden Sie in Prüfliste für regelmäßige Überwachungstasks.
3. Um zu überprüfen, ob Ihr System Lizenzierungsvoraussetzungen erfüllt, führen Sie die Anweisungen in Lizenzeinhaltung überprüfen aus.
4. Optional: Konfigurieren Sie E-Mail-Berichte des Systemstatus. Anweisungen finden Sie in Systemstatus mithilfe von E-Mail-Berichten verfolgen.
5. Optional: In einigen Fällen möchten Sie vielleicht erweiterte Überwachungstools verwenden, um bestimmte Überwachungs- oder Fehlerbehebungstasks auszuführen. Informationen zum Auswählen und Konfigurieren erweiterter Überwachungstools finden Sie in Überwachungstools auswählen, konfigurieren und verwenden.

Nächste Schritte

Installieren Sie zur Unterstützung bei der Diagnose von Problemen bei Clients für Sichern/Archivieren die IBM Spectrum Protect-Clientverwaltungsservices auf den Systemen des Clients für Sichern/Archivieren, die diese unterstützen. Wenn der Clientverwaltungsservice auf einem System installiert ist, können Sie im Operations Center auf Diagnose klicken, um Hilfe bei der Diagnose von Problemen beim Client für Sichern/Archivieren anzufordern. Um den Clientverwaltungsservice zu installieren, führen Sie die Anweisungen in Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen aus.

Zugehörige Konzepte:

Leistung

Zugehörige Tasks:

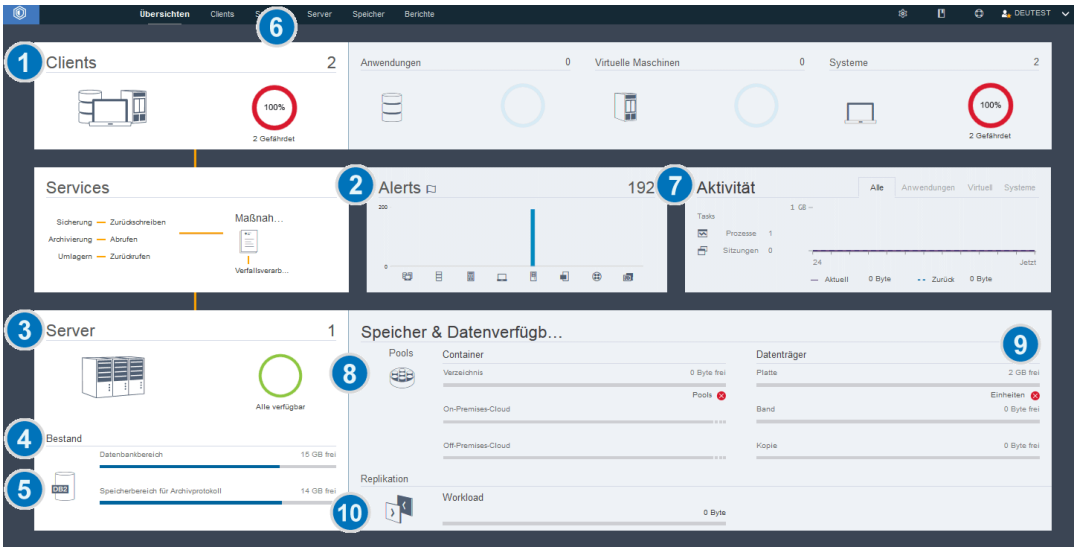
Fehlerbehebung

Prüfliste für tägliche Überwachungstasks

Überprüfen Sie die Prüfliste, um sicherzustellen, dass wichtige tägliche Überwachungstasks ausgeführt werden.

Führen Sie die täglichen Überwachungstasks über die Seite Übersicht im Operations Center aus. Sie können auf die Seite Übersicht zugreifen, indem Sie das Operations Center öffnen und auf Übersichten klicken.

Die folgende Abbildung zeigt die Position zur Ausführung der jeweiligen Task.



Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder.

In der folgenden Tabelle sind die täglichen Überwachungstasks sowie Anweisungen zur Ausführung jeder Task aufgeführt.

Tabelle 1. Tägliche Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
1 Bestimmen Sie, ob Clients vorhanden sind, bei denen die Gefahr besteht, dass sie aufgrund fehlgeschlagener oder versäumter Sicherungsoperationen ungeschützt sind.	Um zu überprüfen, ob Clients gefährdet sind, suchen Sie nach einem Hinweis Gefährdet. Um Details anzuzeigen, klicken Sie auf den Bereich 'Clients'. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie die Clientfehler- und -planungsprotokolle anzeigen, indem Sie die folgenden Schritte ausführen: 1. Wählen Sie in der Tabelle 'Clients' den Client aus und klicken Sie auf Details. 2. Um ein Problem zu diagnostizieren, klicken Sie auf Diagnose.	Greifen Sie bei Clients, für die der Clientverwaltungsservice nicht installiert ist, auf das Clientsystem zu, um die Clientfehlerprotokolle zu überprüfen.
2 Bestimmen Sie, ob clientbezogene oder serverbezogene Fehler einen Bedienereingriff erfordern.	Um die Bewertung jedes zurückgemeldeten Alerts zu bestimmen, bewegen Sie den Mauszeiger im Bereich 'Alerts' über die Spalten.	Um weitere Informationen zu Alerts anzuzeigen, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Alerts'. 2. Wählen Sie in der Tabelle 'Alerts' einen Alert aus. 3. Überprüfen Sie die Nachrichten im Fenster 'Aktivitätenprotokoll'. Im Fenster werden zugehörige Nachrichten angezeigt, die vor und nach dem Auftreten des ausgewählten Alerts ausgegeben wurden.
3 Bestimmen Sie, ob die vom Operations Center verwalteten Server verfügbar sind, um Datenschutzservices für Clients bereitzustellen.	1. Um zu überprüfen, ob Server gefährdet sind, suchen Sie im Bereich 'Server' nach einem Hinweis Nicht verfügbar. 2. Um zusätzliche Informationen anzuzeigen, klicken Sie auf den Bereich 'Server'. 3. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details.	Tipp: Wenn Sie ein Problem erkennen, das sich auf die Servermerkmale bezieht, aktualisieren Sie die Servermerkmale: 1. Wählen Sie in der Tabelle 'Server' einen Server aus und klicken Sie auf Details. 2. Um die Servermerkmale zu aktualisieren, klicken Sie auf Merkmale.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
4 Bestimmen Sie, ob für den Serverbestand, der aus der Serverdatenbank, der aktiven Protokolldatei und dem Archivprotokoll besteht, genügend Speicherbereich verfügbar ist.	1. Klicken Sie auf den Bereich 'Server'. 2. Zeigen Sie in der Spalte 'Status' der Tabelle den Status des Servers an und beheben Sie alle Probleme: ○ Normal Für die Serverdatenbank, die aktive Protokolldatei und das Archivprotokoll ist genügend Speicherbereich verfügbar. ○ Kritisch Für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll ist nicht genügend Speicherbereich verfügbar. Sie müssen unverzüglich Speicherbereich hinzufügen; andernfalls werden die vom Server bereitgestellten Datenschutzservices unterbrochen. ○ Warnung Der Der Speicherbereich für die Serverdatenbank, die aktive Protokolldatei oder das Archivprotokoll wird knapp. Wenn diese Bedingung bestehen bleibt, müssen Sie Speicherbereich hinzufügen. ○ Nicht verfügbar Der Status kann nicht abgerufen werden. Stellen Sie sicher, dass der Server aktiv ist und keine Netzprobleme vorliegen. Dieser Status wird auch angezeigt, wenn die Überwachungsadministrator-ID gesperrt ist oder aus anderen Gründen auf dem Server nicht verfügbar ist. Diese ID hat den Namen IBM-OC-Name_des_Hub-Servers. ○ Nicht überwacht Nicht überwachte Server sind für den Hub-Server definiert, aber nicht für die Verwaltung durch das Operations Center konfiguriert. Um einen nicht überwachten Server zu konfigurieren, wählen Sie den Server aus und klicken Sie auf Peripherieserver überwachen.	Sie können auch auf der Seite Alerts nach zugehörigen Alerts suchen. Weitere Anweisungen zur Fehlerbehebung finden Sie in Serverprobleme beheben.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
5 Überprüfen Sie Operationen zur Sicherung der Serverdatenbank.	Um zu bestimmen, ob ein Server kürzlich gesichert wurde, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf den Bereich 'Server'. 2. Überprüfen Sie in der Tabelle 'Server' die Spalte 'Letzte Datenbanksicherung'.	Um detaillierte Informationen zu Sicherungsoperationen abzurufen, führen Sie die folgenden Schritte aus: 1. Wählen Sie in der Tabelle 'Server' eine Zeile aus und klicken Sie auf Details. 2. Bewegen Sie im Bereich 'Datenbanksicherung' den Mauszeiger über die Häkchen, um Informationen zu Sicherungsoperation zu überprüfen. Wenn eine Datenbank nicht kürzlich (beispielsweise innerhalb der letzten 24 Stunden) gesichert wurde, können Sie eine Sicherungsoperation starten: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Server'. 2. Wählen Sie in der Tabelle einen Server aus und klicken Sie auf Sichern. Um zu bestimmen, ob die Serverdatenbank für automatische Sicherungsoperationen konfiguriert ist, führen Sie die folgenden Schritte aus: 1. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Geben Sie den Befehl QUERY DB aus: `query db f=d` 3. Überprüfen Sie in der Ausgabe das Feld `Einheitenklassenname für Gesamtsicherungen`. Wenn eine Einheitenklasse angegeben ist, ist der Server für automatische Datenbanksicherungen konfiguriert.
6 Überwachen Sie andere Serververwaltungstasks. Serververwaltungstasks können die Ausführung von Zeitplänen für Verwaltungsbefehle, Verwaltungsscripts und zugehörigen Befehlen umfassen.	Um nach Informationen zu Prozessen zu suchen, die aufgrund von Serverproblemen fehlgeschlagen sind, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf Server > Verwaltung. 2. Um das zwei Wochen umfassende Verlaufsprotokoll eines Prozesses abzurufen, zeigen Sie Spalte 'History' an. 3. Um weitere Informationen zu einem geplanten Prozess abzurufen, bewegen Sie den Mauszeiger über das Kontrollkästchen, das dem Prozess zugeordnet ist.	Weitere Informationen zum Überwachen von Prozessen und Beheben von Problemen, finden Sie in der Onlinehilfe des Operations Center.
7 Überprüfen Sie, ob das Datenvolumen, das kürzlich an Server bzw. von Servern gesendet wurde, innerhalb des erwarteten Bereichs liegt.	• Um eine Übersicht über die Aktivität der letzten 24 Stunden abzurufen, zeigen Sie den Bereich 'Aktivität' an. • Um die Aktivität der letzten 24 Stunden mit der Aktivität der vorherigen 24 Stunden zu vergleichen, studieren Sie die Zahlen in den Bereichen 'Aktuell' und 'Vorherig'.	• Wenn mehr Daten als erwartet an den Server gesendet wurden, bestimmen Sie die Clients, die mehr Daten sichern und ermitteln Sie die Ursache. Möglicherweise funktioniert die clientseitige Datendeduplizierung nicht ordnungsgemäß. • Wenn weniger Daten als erwartet an den Server gesendet wurden, überprüfen Sie, ob Clientsicherungsoperationen gemäß Zeitplan ausgeführt werden.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
8 Stellen Sie sicher, dass Speicherpools zum Sichern von Clientdaten verfügbar sind.	1. Wenn im Bereich 'Speicher & Datenverfügbarkeit' Probleme angezeigt werden, klicken Sie auf Pools, um die Details anzuzeigen: ○ Wenn der Status Kritisch angezeigt wird, ist in dem Speicherpool nicht genügend Speicherbereich verfügbar oder der Speicherpool hat den Zugriffsstatus UNAVAILABLE (Nicht verfügbar). ○ Wenn der Status Warnung angezeigt wird, wird der Speicherbereich für den Speicherpool knapp oder der Speicherpool hat den Zugriffsstatus READONLY (Lesezugriff). 2. Um den verwendeten Speicherbereich, den freien Speicherbereich und den Gesamtspeicherbereich für Ihren ausgewählten Speicherpool anzuzeigen, bewegen Sie den Mauszeiger über die Einträge in der Spalte 'Verwendete Kapazität'.	Um die Speicherpoolkapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie eine Zeile in der Tabelle 'Speicherpools' aus und klicken Sie auf Details.
9 Stellen Sie sicher, dass Speichereinheiten für Sicherungsoperationen verfügbar sind.	Überprüfen Sie im Bereich 'Speicher & Datenverfügbarkeit' im Abschnitt 'Datenträger' unterhalb der Balken für die Kapazität den Status, der neben Einheiten angegeben ist. Wenn der Status Kritisch oder Warnung für eine Einheit angezeigt wird, müssen Sie das Problem untersuchen. Um Details anzuzeigen, klicken Sie auf Einheiten.	Platteneinheiten können aus den folgenden Gründen den Status 'Kritisch' oder 'Warnung' haben: • Für Einheitenklassen DISK können Datenträger offline sein oder den Zugriffsstatus READONLY (Lesezugriff) haben. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Datenträger angezeigt. • Für nicht gemeinsam genutzte Einheitenklassen FILE können Verzeichnisse offline sein. Außerdem ist unter Umständen nicht genügend freier Speicherbereich für die Zuordnung von Arbeitsdatenträgern verfügbar. In der Spalte 'Plattenspeicher' der Tabelle 'Platteneinheiten' wird der Status der Verzeichnisse angezeigt. • Für gemeinsam genutzte Einheitenklassen FILE sind Laufwerke unter Umständen nicht verfügbar. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. In anderen Spalten der Tabelle 'Platteneinheiten' wird der Status der Laufwerke und Pfade angezeigt. Bandeinheiten können den Status 'Kritisch' haben, wenn Laufwerke nicht verfügbar sind. Ein Laufwerk ist nicht verfügbar, wenn es offline ist, während der Antwort an den Server gestoppt wurde oder sein Pfad offline ist. Eine Bandeinheit kann auch den Status 'Kritisch' haben, wenn das Speicherarchiv offline ist. In anderen Spalten der Tabelle 'Bandeinheiten' wird der Status der automatischen Einheiten im Speicherarchiv, der Laufwerke und der Pfade angezeigt. Stellen Sie für Bandsicherungsoperationen sicher, dass genügend Arbeitsbänder verfügbar sind. Wenn Sie sich nicht sicher sind, ob die Anzahl verfügbarer Arbeitsbänder ausreichend ist, öffnen Sie das Notizbuch 'Details', um die Bandnutzung sowie eine Schätzung der Verfügbarkeit von Arbeitsbändern anzuzeigen. Um das Notizbuch 'Details' zu öffnen, wählen Sie in der Tabelle ein Speicherarchiv aus und klicken Sie auf 'Details'.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebungsinformationen
10 Überwachen Sie Knotenreplikationsprozesse.	1. Um den Gesamtstatus der Knotenreplikationsprozesse abzurufen, zeigen Sie den Bereich 'Replikation' auf der Seite Übersicht im Operations Center an. 2. Um Informationen zu jedem replizierten Serverpaar anzuzeigen, klicken Sie auf den Bereich 'Replikation'. 3. Um das Datenvolumen, das im Laufe der letzten zwei Wochen repliziert wurde, und die Geschwindigkeit der Replikation anzuzeigen, wählen Sie ein Serverpaar aus und klicken Sie auf Details. 4. Um Replikationsinformationen für einen Client anzuzeigen, klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Studieren Sie die Informationen in der Spalte 'Replikationsworkload'.	Zeigen Sie für die erweiterte Überwachung mithilfe von Befehlen Informationen zu aktiven und beendeten Knotenreplikationsprozessen an: 1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Geben Sie den Befehl QUERY REPLICATION aus. Anweisungen finden Sie in QUERY REPLICATION (Knotenreplikationsprozesse abfragen). Wenn die Replikationsoperation erfolgreich ausgeführt wurde, stimmt der Wert für `Gesamtzahl der zu replizierenden Dateien` mit dem Wert für `Gesamtzahl der replizierten Dateien` überein. Um Nachrichten anzuzeigen, die sich auf einen Knotenreplikationsprozess auf einem Quellen- oder Zielreplikationsserver beziehen, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Server. 2. Wählen Sie den Quellen- oder Zielreplikationsserver aus und klicken Sie auf Details: ○ Um aktive Tasks anzuzeigen, klicken Sie auf Aktive Tasks, wählen die Task aus und überprüfen, ob der Status Aktiv angezeigt wird. Ausführliche Informationen enthalten die zugehörigen Aktivitätenprotokolle. ○ Um abgeschlossene Tasks anzuzeigen, klicken Sie auf Abgeschlossene Tasks, wählen die Task aus und überprüfen, ob der Status Abgeschlossen angezeigt wird. Ausführliche Informationen enthalten die zugehörigen Aktivitätenprotokolle.

Prüfliste für regelmäßige Überwachungstasks

Um sicherzustellen, dass Operationen ordnungsgemäß ausgeführt werden, führen Sie die Tasks in der Prüfliste für regelmäßige Überwachungstasks aus. Planen Sie regelmäßige Tasks häufig genug, sodass Sie potenzielle Probleme erkennen können, bevor diese wirklich problematisch werden.

Tipp: Um Verwaltungsbefehle für erweiterte Überwachungstasks auszuführen, verwenden Sie den Command Builder im Operations Center. Der Command Builder stellt eine Eingabepufferfunktion bereit, die Sie durch die Eingabe von Befehlen führt. Um den Command Builder zu öffnen, rufen Sie die Seite Übersicht im Operations Center auf. Bewegen Sie den Mauszeiger in der Menüleiste über das Symbol für Einstellungen und klicken Sie auf Command Builder.

Tabelle 1. Regelmäßige Überwachungstasks

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie die Systemleistung.	Bestimmen Sie den für Clientsicherungsoperationen erforderlichen Zeitraum: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. Suchen Sie den Server, der dem Client zugeordnet ist. 2. Klicken Sie auf Server. Wählen Sie den Server aus und klicken Sie auf Details. 3. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die in den letzten 24 Stunden abgeschlossenen wurden, klicken Sie auf Abgeschlossene Tasks. 4. Um den Zeitraum anzuzeigen, der für Tasks benötigt wurde, die vor mehr als 24 Stunden abgeschlossen wurden, verwenden Sie den Befehl QUERY ACTLOG. Führen Sie die Anweisungen in QUERY ACTLOG (Aktivitätenprotokoll abfragen) aus. 5. Wenn die Dauer von Clientsicherungsoperationen zunimmt, ohne dass ein offensichtlicher Grund erkennbar ist, überprüfen Sie Ursache. Wenn der Clientverwaltungsservice auf einem Client für Sichern/Archivieren installiert wurde, können Sie Leistungsprobleme für den Client für Sichern/Archivieren diagnostizieren, indem Sie die folgenden Schritte ausführen: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients. 2. Wählen Sie einen Client für Sichern/Archivieren aus und klicken Sie auf Details. 3. Um Clientprotokolle abzurufen, klicken Sie auf Diagnose.	Informationen zur Verkürzung der Zeit, die der Client zum Sichern von Daten auf dem Server benötigt, finden Sie in Häufig auftretende Clientleistungsprobleme lösen. Suchen Sie nach Leistungsengpässen. Anweisungen finden Sie in Leistungsengpässe identifizieren. Informationen zur Identifikation und Behebung anderer Leistungsprobleme finden Sie in Leistung.
Bestimmen Sie die Platteneinsparungen, die durch die Datendeduplizierung bereitgestellt werden.	1. Klicken Sie auf der Seite Übersicht im Operations Center auf Pools. 2. Wählen Sie einen Pool aus und klicken Sie auf Kurzübersicht. 3. Zeigen Sie im Bereich 'Datendeduplizierung' die Zeile 'Eingesparter Speicherbereich' an.	Um für die erweiterte Überwachung detaillierte Statistikdaten zu dem Datendeduplizierungsprozess für einen bestimmten Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abzurufen, führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen  und klicken Sie auf Command Builder. 2. Fordern Sie einen Statistikbericht an, indem Sie den Befehl GENERATE DEDUPSTATS ausgeben. Führen Sie die Anweisungen in GENERATE DEDUPSTATS (Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool generieren) aus. 3. Zeigen Sie den Statistikbericht an, indem Sie den Befehl QUERY DEDUPSTATS ausgeben. Führen Sie die Anweisungen in QUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen) aus.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Stellen Sie sicher, dass aktuelle Sicherungsdateien für Einheitenkonfigurations- und Datenträgerprotokolldaten gesichert werden.	Greifen Sie auf Ihre Speicherpositionen zu, um sicherzustellen, dass die Dateien verfügbar sind. Die bevorzugte Methode ist die Sicherung der Dateien an zwei Positionen.
	Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, führen Sie die folgenden Schritte aus:
	1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder.
	2. Um die Protokolldatei für Datenträger und die Einheitenkonfigurationsdatei zu lokalisieren, geben Sie die folgenden Befehle aus:
	`query option volhistory`
	`query option devconfig`
	3. Überprüfen Sie in der Ausgabe die Spalte 'Optionseinstellung', um die Dateipositionen zu finden.
	Wenn ein Katastrophenfall eintritt, sind sowohl die Protokolldatei für Datenträger als auch die Einheitenkonfigurationsdatei für die Zurückschreibung der Serverdatenbank erforderlich.	

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung

Bestimmen Sie, ob für das Instanzverzeichnisdateisystem genügend Speicherbereich verfügbar ist.	Stellen Sie sicher, dass im Instanzverzeichnisdateisystem mindestens 20 % freier Speicherbereich verfügbar ist. Führen Sie die für Ihr Betriebssystem zutreffende Aktion aus:
	• AIX-BetriebssystemeUm den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -g Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Linux-BetriebssystemeUm den verfügbaren Speicherbereich im Dateisystem anzuzeigen, geben Sie in der Betriebssystem-Befehlszeile den folgenden Befehl aus:
	`df -h Instanzverzeichnis`
	Dabei gibt *Instanzverzeichnis* das Instanzverzeichnis an.
	• Windows-BetriebssystemeKlicken Sie in Windows-Explorer mit der rechten Maustaste auf das Dateisystem und klicken Sie auf Eigenschaften. Zeigen Sie die Kapazitätsdaten an.
	Die bevorzugte Position des Instanzverzeichnisses ist von dem Betriebssystem abhängig, unter dem der Server installiert ist:
	• AIX-Betriebssysteme Linux-Betriebssysteme /home/tsminst1/tsminst1
	• Windows-Betriebssysteme C:\tsminst1
	Tipp: Wenn Sie ein Arbeitsblatt zur Planung ausgefüllt haben, ist die Position des Instanzverzeichnisses im Arbeitsblatt vermerkt.	

Ermitteln Sie nicht erwartete Clientaktivität.	Um im Rahmen der Überwachung der Clientaktivität zu bestimmen, ob das Datenvolumen das erwartete Volumen überschreitet, führen Sie die folgenden Schritte aus: 1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Clients'. 2. Um die Aktivität der vergangen zwei Wochen anzuzeigen, doppelklicken Sie auf einen beliebigen Client. 3. Um die Anzahl Byte anzuzeigen, die an den Client gesendet wurden, klicken Sie auf die Registerkarte Merkmale. 4. Zeigen Sie im Bereich 'Letzte Sitzung' die Zeile 'An Client gesendet' an.	Wenn Sie auf einen Client in der Tabelle 'Clients' doppelklicken, wird im Bereich Aktivität im Lauf von 2 Wochen das Datenvolumen angezeigt, das vom Client jeden Tag an den Server gesendet wurde.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Überwachen Sie das Speicherpoolwachstum im Laufe der Zeit.	1. Klicken Sie auf der Seite Übersicht im Operations Center auf den Bereich 'Pools'. 2. Um die Kapazität für die vergangenen zwei Wochen anzuzeigen, wählen Sie einen Pool aus und klicken Sie auf Details.	Tipps: • Um die Zeit anzugeben, die verstreichen muss, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool oder einem Cloud-Containerspeicherpool entfernt werden, nachdem sie nicht mehr vom Bestand referenziert werden, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus. 2. Klicken Sie auf Details > Merkmale. 3. Geben Sie im Feld `Verzögerungszeitraum für Containerwiederverwendung` den Zeitraum an. • Bestimmen Sie die Datendeduplizierungsleistung für Verzeichniscontainer- und Cloud-Containerspeicherpools mithilfe des Befehls GENERATE DEDUPSTATS. • Um Deduplizierungsstatistikdaten für einen Speicherpool anzuzeigen, führen Sie die folgenden Schritte aus: 1. Wählen Sie auf der Seite Speicherpools im Operations Center den Speicherpool aus. 2. Klicken Sie auf Details > Merkmale. Verwenden Sie dementsprechend den Befehl QUERY EXTENTUPDATES, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainer- oder Cloud-Containerspeicherpools anzuzeigen. Anhand der Befehlsausgabe können Sie die Datenbereiche bestimmen, die nicht mehr referenziert werden, sowie die Datenbereiche, die zum Löschen vom System auswählbar sind. Überwachen Sie in der Ausgabe die Anzahl Datenbereiche, die zum Löschen vom System auswählbar sind. Diese Messgröße steht in direkten Zusammenhang mit dem Umfang des freien Speicherbereichs in dem Containerspeicherpool. • Um den Umfang des physischen Speicherbereichs anzuzeigen, der von einem Dateibereich nach dem Entfernen der Datendeduplizierungseinsparungen belegt wird, verwenden Sie den Befehl select * from occupancy. Die Befehlsausgabe umfasst den Wert für LOGICAL_MB. LOGICAL_MB gibt an, wie viel Speicherbereich von diesem Dateibereich belegt wird.
Werten Sie das Timing von Clientzeitplänen aus. Stellen Sie sicher, dass die Start- und Endzeiten von Clientzeitplänen Ihre Geschäftsanforderungen erfüllen.	Klicken Sie auf der Seite Übersicht im Operations Center auf Clients > Zeitpläne. In der Tabelle 'Zeitpläne' wird in der Spalte 'Start' die konfigurierte Startzeit für die geplante Operation angezeigt. Um anzuzeigen, wann die letzte Operation gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	Tipp: Wenn die Ausführung einer Clientoperation länger als erwartet dauert, empfangen Sie unter Umständen eine Warnung. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite 'Übersicht' im Operations Center den Mauszeiger über Clients und klicken Sie auf Zeitpläne. 2. Wählen Sie einen Zeitplan aus und klicken Sie auf Details. 3. Zeigen Sie die Details eines Zeitplans an, indem Sie auf den blauen Pfeil neben der Zeile klicken. 4. Geben Sie im Feld Ausführungszeitalert die Uhrzeit an, zu der eine Warnung ausgegeben wird, wenn die geplante Operation nicht ausgeführt wird. 5. Klicken Sie auf Sichern.

Task	Basisprozeduren	Erweiterte Prozeduren und Fehlerbehebung
Werten Sie das Timing von Verwaltungstasks aus. Stellen Sie sicher, dass die Start- und Endzeiten von Verwaltungstasks Ihre Geschäftsanforderungen erfüllen.	Klicken Sie auf der Seite Übersicht im Operations Center auf Server > Verwaltung. Überprüfen Sie in der Tabelle 'Verwaltung' die Informationen in der Spalte 'Letzte Ausführungsdauer'. Um anzuzeigen, wann die letzte Verwaltungstask gestartet wurde, bewegen Sie den Mauszeiger über das Uhrsymbol.	Tipp: Wenn die Ausführung einer Verwaltungstask zu lange dauert, ändern Sie die Startzeit oder die maximale Ausführungszeit. Führen Sie die folgenden Schritte aus: 1. Bewegen Sie auf der Seite Übersicht im Operations Center den Mauszeiger über das Symbol für Einstellungen und klicken Sie auf Command Builder. 2. Um die Startzeit oder die maximale Ausführungszeit für eine Task zu ändern, geben Sie den Befehl UPDATE SCHEDULE aus. Anweisungen finden Sie in UPDATE SCHEDULE (Clientzeitplan aktualisieren).

Zugehörige Verweise:
QUERY ACTLOG (Aktivitätenprotokoll abfragen)
UPDATE STGPOOL (Speicherpool aktualisieren)
QUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)

Lizenzeinhaltung überprüfen

Stellen Sie sicher, dass die Bedingungen Ihrer Lizenzvereinbarung von Ihrer IBM Spectrum Protect-Lösung eingehalten werden. Indem die Einhaltung regelmäßig überprüft wird, können Sie Trends beim Datenwachstum oder der PVU-Nutzung verfolgen. Planen Sie anhand dieser Informationen den weiteren Kauf von Lizenzen.

Informationen zu diesem Vorgang

Die Methode zur Überprüfung der Einhaltung der Lizenzbedingungen durch Ihre Lösung variiert abhängig von den Bedingungen Ihrer IBM Spectrum Protect-Lizenzvereinbarung.

Front-End-Kapazitätslizenzierung
: Das Front-End-Modell bestimmt die Lizenzvoraussetzungen auf der Basis des zurückgemeldeten Volumens an primären Daten, das von Clients gesichert wird. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme.

Back-End-Kapazitätslizenzierung
: Das Back-End-Modell bestimmt Lizenzvoraussetzungen auf der Basis der Terabyte Daten, die in primären Speicherpools und Repositorys gespeichert werden.
Tipps:

- Um die Genauigkeit von Schätzungen der Front-End- und Back-End-Kapazität zu gewährleisten, installieren Sie die neueste Version der Client-Software auf jedem Clientknoten.
- Die Informationen zur Front-End- und Back-End-Kapazität im Operations Center dienen zum Zweck der Planung und Schätzung.

PVU-Lizenzierung
: Das PVU-Modell basiert auf der Nutzung von PVUs durch Servereinheiten.
Wichtig: Die von IBM Spectrum Protect bereitgestellten PVU-Berechnungen werden als Schätzungen betrachtet und sind nicht rechtsverbindlich. Die von IBM Spectrum Protect zurückgemeldeten PVU-Lizenzinformationen werden nicht als zulässiger Ersatz für das IBM® License Metric Tool angesehen.

Die neuesten Informationen zu Lizenzierungsmodellen finden Sie in den Informationen zu Produktdetails und Lizenzen auf der Website der IBM Spectrum Protect-Produktfamilie. Wenden Sie sich bei Fragen oder Problemstellungen zu Lizenzierungsanforderungen an Ihren IBM Spectrum Protect-Software-Provider.

Vorgehensweise

Führen Sie zur Überwachung der Lizenzeinhaltung die Schritte aus, die den Bedingungen Ihrer Lizenzvereinbarung entsprechen.
Tipp: Das Operations Center stellt einen E-Mail-Bericht bereit, in dem die Front-End- und Back-End-Kapazitätsnutzung zusammengefasst sind. Berichte können automatisch regelmäßig an einen oder mehrere Empfänger gesendet werden. Klicken Sie für die Konfiguration und Verwaltung von E-Mail-Berichten in der Menüleiste des Operations Center auf Berichte.

Option	Bezeichnung

Option	Bezeichnung
Front-End-Modell	a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen und klicken Sie auf Lizenzierung. Die Schätzung der Front-End-Kapazität wird auf der Seite 'Front-End-Nutzung' angezeigt. b. Wenn in der Spalte 'Keine Zurückmeldung' ein Wert angezeigt wird, klicken Sie auf die Zahl, um Clients zu identifizieren, von denen keine Kapazitätsnutzung zurückgemeldet wurde. c. Um die Kapazität für Clients zu schätzen, für die keine Kapazitätsnutzung zurückgemeldet wurde, rufen Sie die folgende FTP-Site auf, auf der Tools und Anweisungen zum Messen der Kapazität bereitgestellt werden: ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools Um die Front-End-Kapazität mithilfe eines Scripts zu messen, führen Sie die Anweisungen im aktuellen Lizenzierungshandbuch aus. d. Addieren Sie den Operations Center-Schätzwert und alle Schätzwerte, die Sie mithilfe eines Scripts ermittelt haben. e. Überprüfen Sie, ob die geschätzte Kapazität die Bedingungen Ihrer Lizenzvereinbarung einhält.
Back-End-Modell	Einschränkung: Wenn der Quellen- und der Zielreplikationsserver nicht dieselben Maßnahmeneinstellungen verwenden, können Sie das Operations Center nicht zur Überwachung der Back-End-Kapazitätsnutzung für replizierte Clients verwenden. Informationen zur Schätzung der Kapazitätsnutzung für diese Clients finden Sie in Technote 1656476. a. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für Einstellungen und klicken Sie auf Lizenzierung. b. Klicken Sie auf die Registerkarte Back-End. c. Überprüfen Sie, ob das geschätzte Datenvolumen die Bedingungen Ihrer Lizenzvereinbarung einhält.
PVU-Modell	Informationen zur Vorgehensweise beim Prüfen der Einhaltung der PVU-Lizenzbedingungen finden Sie in Einhaltung des PVU-Lizenzierungsmodells prüfen.

- Einhaltung des PVU-Lizenzierungsmodells prüfen
  Wenn Sie IBM Spectrum Protect unter dem Prozessor-Value-Unit-Lizenzierungsmodell (PVU-Lizenzierungsmodell) gekauft haben, stellen Sie sicher, dass Ihre Lösung die Lizenzbedingungen einhält. Überprüfen Sie die PVU-Schätzungen in regelmäßigen Abständen, um den weiteren Kauf von Lizenzen zu planen. Wenn sich beispielsweise PVU-Schätzungen erhöhen oder Sie die Installation weiterer Server planen, müssen Sie gegebenenfalls weitere Lizenzen kaufen.

Systemstatus mithilfe von E-Mail-Berichten verfolgen

Konfigurieren Sie das Operations Center für die Generierung von E-Mail-Berichten zur Zusammenfassung des Systemstatus. Sie können eine Mail-Server-Verbindung konfigurieren, Berichtseinstellungen ändern und wahlweise angepasste SQL-Berichte erstellen.

Vorbereitende Schritte

Bevor Sie E-Mail-Berichte konfigurieren, müssen Sie sicherstellen, dass die folgenden Voraussetzungen erfüllt sind:

- Es ist ein SMTP-Host-Server (SMTP = Simple Mail Transfer Protocol) verfügbar, um Berichte als E-Mail senden und empfangen zu können. Der SMTP-Server muss als offenes Mail-Relay konfiguriert sein. Außerdem müssen Sie sicherstellen, dass der IBM Spectrum Protect-Server, der E-Mail-Nachrichten sendet, Zugriff auf den SMTP-Server hat. Wenn das Operations Center auf einem anderen Computer installiert ist, ist für diesen Computer kein Zugriff auf den SMTP-Server erforderlich.
- Um E-Mail-Berichte konfigurieren zu können, müssen Sie über Systemberechtigung für den Server verfügen.
- Um die Empfänger anzugeben, können Sie eine oder mehrere E-Mail-Adressen oder Administrator-IDs eingeben. Wenn eine Administrator-ID eingegeben werden soll, muss die ID auf dem Hub-Server registriert sein und der ID muss eine E-Mail-Adresse zugeordnet sein. Eine E-Mail-Adresse für einen Administrator können Sie mithilfe des Parameters EMAILADDRESS im Befehl UPDATE ADMIN angeben.

Informationen zu diesem Vorgang

Sie können das Operations Center zum Senden eines Berichts über allgemeine Operationen, eines Lizenzeinhaltungsberichts und eines oder mehrerer angepasster Berichte, die SQL-Anweisungen SELECT zum Abfragen verwalteter Server verwenden, konfigurieren.

Vorgehensweise

Um E-Mail-Berichte zu konfigurieren und zu verwalten, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Berichte.
2. Wenn noch keine E-Mail-Server-Verbindung konfiguriert ist, klicken Sie auf Mail-Server konfigurieren und füllen Sie die Felder aus. Nach der Konfiguration des Mail-Servers sind der Bericht über allgemeine Operationen und der Lizenzeinhaltungsbericht aktiviert.
3. Um Berichtseinstellungen zu ändern, wählen Sie einen Bericht aus, klicken Sie auf Details und aktualisieren Sie das Formular.
4. Optional: Um einen angepassten SQL-Bericht hinzuzufügen, klicken Sie auf + Bericht und füllen Sie die Felder aus.
   Tipp: Um einen Bericht sofort auszuführen und zu senden, wählen Sie den Bericht aus und klicken Sie auf Senden.

Ergebnisse

Aktivierte Berichte werden gemäß den angegebenen Einstellungen gesendet.

Zugehörige Verweise:

UPDATE ADMIN (Administrator aktualisieren)

Zugehörige Informationen:

Beispiele für angepasste Berichte

Überwachungstools auswählen, konfigurieren und verwenden

Verwenden Sie das Operations Center, um eine Übersicht über den Systemstatus abzurufen und ein Drilldown zu detaillierten Informationen durchzuführen. In einigen Fällen möchten Sie vielleicht erweiterte Tools verwenden, um bestimmte Überwachungsdaten zu erfassen.

Vorgehensweise

Wählen Sie die für Ihre Lösung geeigneten Überwachungstools aus und konfigurieren Sie diese.

Tabelle 1. Überwachungstools

Tooltyp	Anwendungsfälle	Links zu weiteren Informationen
Operations Center	• Verwenden Sie die grafische Benutzerschnittstelle, um den Systemstatus zu überprüfen und Probleme zu diagnostizieren. • Konfigurieren Sie das Operations Center für das Senden täglicher E-Mail-Zusammenfassungsberichte. • Optional: Passen Sie die Alerts an, die im Operations Center angezeigt werden, und konfigurieren Sie E-Mail-Benachrichtigungen für die Alerts. • Optional: Überwachen Sie die Speicherumgebung über Fernzugriff, indem Sie die Seite Übersicht im Web-Browser einer mobilen Einheit anzeigen. Sie können beispielsweise den Apple Safari-Web-Browser auf einem Apple iPad-Gerät verwenden. Es können auch andere mobile Einheiten verwendet werden. Tipp: Wenn Sie IBM Spectrum Protect-Clientverwaltungsservices auf einem Client für Sichern/Archivieren installieren, können Sie mithilfe des Operations Center Fehlerbehebungsinformationen für den Client für Sichern/Archivieren abrufen. Der Clientverwaltungsservice kann nur unter Linux- oder Windows-Betriebssystemen installiert werden.	

Tooltyp	Anwendungsfälle	Links zu weiteren Informationen
IBM Spectrum Protect-Verwaltungsbefehle	Lesen Sie die ausführlichen Informationen. Verwenden Sie die für Ihre Lösung zutreffende Methode: • Um Nachrichten anzuzeigen, die vom Server und Client generiert wurden, verwenden Sie den Befehl QUERY ACTLOG. Tipp: Sie können Verwaltungsbefehle über den Command Builder von Operations Center ausführen. • Um Aktivitäten, wie beispielsweise Serverumlagerung und Clientanmeldungen, zu überwachen, verwenden Sie den Verwaltungsclient im Konsolenmodus. Führen Sie den Befehl dsmadmc -consolemode aus.	• Verwaltungsbefehle • QUERY ACTLOG (Aktivitätenprotokoll abfragen) • Serveraktivitäten über den Verwaltungsclient überwachen • Verwaltungsclientoptionen
Ereignisprotokollierung	Protokollieren Sie Servernachrichten und die meisten Clientnachrichten als Ereignisse in einem oder mehreren Repositorys, die als Empfänger bezeichnet werden.	AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeAnweisungen zur Verwendung der Ereignisprotokollierung zur Überwachung einer Lösung finden Sie in IBM Spectrum Protect-Ereignisse in Empfängern protokollieren (Version 7.1.1). Linux-BetriebssystemeAnweisungen zur Protokollierung von Ereignissen in einem Linux-Systemprotokoll finden Sie in Ereignisse im Linux-Systemprotokoll protokollieren (Version 7.1.4).
SQL-Abfragen	Erstellen und formatieren Sie angepasste Abfragen der Serverdatenbank. Sie können beispielsweise die SQL-Aktivitätsübersichtstabelle abfragen, um Statistikdaten zu Clientoperationen und Serverprozessen anzuzeigen. Um alle Informationen in der Übersichtstabelle anzuzeigen, geben Sie den folgenden Befehl über den Verwaltungsclient aus: `select * from summary`	Befehle SELECT verwenden (Version 7.1.1)
Betriebssystemtools	Überwachen und testen Sie die Systemleistung.	
Einheitenüberwachungstools	Überwachen Sie Einheiten auf Verfügbarkeit, Kapazität und Leistung. Verwenden Sie beispielsweise IBM Spectrum Control oder Tools, die Bestandteil der Einheitenhardwarepakete sind.	Um den Einheitengesamtstatus mithilfe von IBM Spectrum Control zu überwachen, führen Sie die Anweisungen in Status und Zustand von Ressourcen überwachen aus. Um die Leistung mithilfe von IBM Spectrum Control zu überwachen, führen Sie die Anweisungen in Leistung von Ressourcen überwachen aus.
IBM® Tivoli Monitoring for Tivoli Storage Manager	Überwachen Sie IBM Spectrum Protect-Server und erstellen Sie Langzeitberichte über Server- und Clientaktivitäten. Tipp: Das Operations Center ist das bevorzugte Tool für die Überwachung. Tivoli Monitoring for Tivoli Storage Manager ist jedoch für die Erstellung von Langzeitberichten, die auf der Technologie von IBM Cognos Business Intelligence basieren, geeignet.	Tivoli Monitoring for Tivoli Storage Manager

Operationen verwalten

Durch die effektive Verwaltung von Server- und Clientoperationen können Sie die Leistung Ihrer Speicherumgebung optimieren. Überwachen Sie als ersten Schritt die Umgebung mithilfe des Operations Center. Ergreifen Sie dann Maßnahmen, um potenzielle Probleme zu verhindern und die Leistung zu verbessern.

Informationen zu diesem Vorgang

- Serveroperationen verwalten
  Sie können den Server starten und stoppen, die Bestandskapazität verwalten sowie die Speichernutzung und Prozessorauslastung verwalten. Sie können auch die Datenübertragung zwischen Servern optimieren, ein Upgrade für den Server durchführen und geplante Aktivitäten optimieren.
- Clientoperationen verwalten
  Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.
- Operations Center verwalten
  Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.

Serveroperationen verwalten

Sie können den Server starten und stoppen, die Bestandskapazität verwalten sowie die Speichernutzung und Prozessorauslastung verwalten. Sie können auch die Datenübertragung zwischen Servern optimieren, ein Upgrade für den Server durchführen und geplante Aktivitäten optimieren.

- Server stoppen und starten
  Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.
- Bestandskapazität verwalten
  Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.
- Speichernutzung und Prozessorauslastung verwalten
  Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datendeduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.
- Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann
  Wenn Ihr IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert oder Speicherpools auf einem fernen Server schützt, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie die entsprechenden Lizenzen anfordern. Es sind sowohl Test- als auch Volllizenzen verfügbar.
- Durchführung eines Upgrades für den Server planen
  Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.
- Geplante Aktivitäten optimieren
  Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

Server stoppen und starten

Stoppen Sie vor der Ausführung von Verwaltungs- oder Rekonfigurationstasks den Server. Starten Sie dann den Server im Verwaltungsmodus. Wenn die Verwaltungs- oder Rekonfigurationstasks abgeschlossen sind, starten Sie den Server erneut im Produktionsmodus.

Vorbereitende Schritte

Um den IBM Spectrum Protect-Server stoppen und starten zu können, müssen Sie über System- oder Bedienerberechtigung verfügen.

- Server stoppen
  Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.
- Server für Verwaltungs- oder Rekonfigurationstasks starten
  Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

Server stoppen

Bereiten Sie das System vor, bevor Sie den Server stoppen, indem Sie sicherstellen, dass alle Datenbanksicherungsoperationen abgeschlossen und alle anderen Prozesse und Sitzungen beendet sind. So können Sie den Server sicher herunterfahren und gewährleisten, dass Daten geschützt sind.

Informationen zu diesem Vorgang

Wenn Sie den Befehl HALT zum Stoppen des Servers ausgeben, werden die folgenden Aktionen ausgeführt:

- Alle Prozesse und Clientknotensitzungen werden abgebrochen.
- Alle aktuellen Transaktionen werden gestoppt. (Die Transaktionen werden rückgängig gemacht, wenn der Server erneut gestartet wird.)

Vorgehensweise

Um das System vorzubereiten und den Server zu stoppen, führen Sie die folgenden Schritte aus:

1. Verhindern Sie, dass neue Clientknotensitzungen gestartet werden, indem Sie den Befehl DISABLE SESSIONS ausgeben:

   ```
   disable sessions all
   ```

2. Bestimmen Sie, ob Clientknotensitzungen oder -prozesse aktiv sind, indem Sie die folgenden Schritte ausführen:
   a. Rufen Sie die Seite Übersicht im Operations Center auf, auf der im Bereich Aktivität die Gesamtzahl Prozesse und Sitzungen angezeigt wird, die derzeit aktiv sind. Wenn die Zahlen erheblich von den Zahlen abweichen, die normalerweise während Ihrer täglichen Speicherverwaltungsroutine angezeigt werden, überprüfen Sie mithilfe weiterer Statusanzeiger im Operations Center, ob ein Problem vorliegt.
   b. Zeigen Sie das Diagramm im Bereich Aktivität an, um den Umfang des Datenaustauschs im Netz für die folgenden Perioden zu vergleichen:
      - Die laufende Periode, d. h. die letzte 24-Stunden-Periode
      - Die vorherige Periode, d. h. die 24 Stunden vor der laufenden Periode

      Wenn das Diagramm für die vorherige Periode den erwarteten Umfang des Datenaustauschs darstellt, können deutliche Abweichungen in dem Diagramm für die laufende Periode auf ein Problem hindeuten.
   c. Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details. Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, rufen Sie mithilfe von Verwaltungsbefehlen Informationen zu Prozessen ab. Geben Sie den Befehl QUERY PROCESS aus, um Prozesse abzufragen; geben Sie den Befehl QUERY SESSION aus, um Informationen zu Sitzungen abzurufen.
3. Warten Sie, bis die Clientknotensitzungen abgeschlossen sind oder brechen Sie diese ab. Um Prozesse und Sitzungen abzubrechen, führen Sie die folgenden Schritte aus:
   - Wählen Sie auf der Seite Server einen Server aus, für den Prozesse und Sitzungen angezeigt werden sollen, und klicken Sie auf Details.
   - Klicken Sie auf die Registerkarte Aktive Tasks und wählen Sie einen oder mehrere Prozesse und/oder eine oder mehrere Sitzungen aus, die abgebrochen werden sollen.
   - Klicken Sie auf Abbrechen.
   - Wenn der Server im Operations Center nicht als Hub- oder Peripherieserver registriert ist, brechen Sie Sitzungen mithilfe von Verwaltungsbefehlen ab. Geben Sie den Befehl CANCEL SESSION aus, um eine Sitzung abzubrechen; geben Sie den Befehl CANCEL PROCESS aus, um Prozesse abzubrechen.
     Tipp: Wenn der Prozess, der abgebrochen werden soll, auf die Bereitstellung eines Banddatenträgers wartet, wird die Mountanforderung abgebrochen. Wenn Sie beispielsweise einen Befehl EXPORT, IMPORT oder MOVE DATA ausgeben, leitet der Befehl möglicherweise einen Prozess ein, der die Bereitstellung eines Banddatenträgers erfordert. Wenn jedoch ein Banddatenträger durch ein automatisiertes Speicherarchiv bereitgestellt wird, wird die Abbruchoperation unter Umständen erst wirksam, wenn der Bereitstellungsprozess abgeschlossen ist. Abhängig von Ihrer Systemumgebung kann dies mehrere Minuten dauern.
4. Stoppen Sie den Server, indem Sie den Befehl HALT ausgeben:

   ```
   halt
   ```

Server für Verwaltungs- oder Rekonfigurationstasks starten

Bevor Sie mit der Ausführung von Serververwaltungs- und Rekonfigurationstasks beginnen, starten Sie den Server im Verwaltungsmodus. Wenn Sie den Server im Verwaltungsmodus starten, werden Operationen, die Ihre Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, inaktiviert.

Informationen zu diesem Vorgang

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm DSMSERV mit dem Parameter MAINTENANCE ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server

- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.
Tipps:

- Sie müssen die Serveroptionsdatei, dsmserv.opt, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung (-wiederherstellung), den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

Vorgehensweise

Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

```
dsmserv maintenance
```

Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann über Server im Verwaltungsmodus starten angezeigt werden.

Nächste Schritte

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl HALT ausgeben:

   ```
   halt
   ```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden. Führen Sie die Anweisungen für Ihr Betriebssystem aus:
   - AIX-BetriebssystemeServerinstanz starten
   - Linux-BetriebssystemeServerinstanz starten
   - Windows-BetriebssystemeServerinstanz starten

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

Bestandskapazität verwalten

Durch die Verwaltung der Kapazität der Datenbank, der aktiven Protokolldatei und von Archivprotokollen wird sichergestellt, dass die Größe des Bestands auf der Basis des Status der Protokolle für die Tasks entsprechend angepasst wird.

Vorbereitende Schritte

Die aktive Protokolldatei und das Archivprotokoll haben die folgenden Merkmale:

- Die Größe der aktiven Protokolldatei kann maximal 512 GB betragen. Weitere Informationen zum Festlegen der Größe der aktiven Protokolldatei für Ihr System finden Sie in Planung der Speicherarrays.
- Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist. Die Größe des Archivprotokolls ist im Gegensatz zur Größe der aktiven Protokolldatei nicht auf eine vordefinierte Größe festgelegt. Archivprotokolldateien werden automatisch gelöscht, wenn sie nicht mehr benötigt werden.

Als Best Practice können Sie wahlweise ein Archivübernahmeprotokoll erstellen, in dem Archivprotokolldateien gespeichert werden, wenn das Archivprotokollverzeichnis voll ist.

Bestimmen Sie über das Operations Center, welche Komponente des Bestands voll ist. Stellen Sie sicher, dass der Server gestoppt wird, bevor Sie eine der Bestandskomponenten vergrößern.

Vorgehensweise

- Um die Datenbank zu vergrößern, führen Sie die folgenden Schritte aus:
  - Erstellen Sie in unterschiedlichen Laufwerken oder Dateisystemen ein oder mehrere Verzeichnisse für die Datenbank.
  - Geben Sie den Befehl EXTEND DBSPACE aus, um der Datenbank das Verzeichnis oder die Verzeichnisse hinzuzufügen. Die Instanzbenutzer-ID des Datenbankmanagers muss Zugriff auf die Verzeichnisse haben. Standardmäßig erfolgt eine Neuverteilung der Daten auf alle Datenbankverzeichnisse und eine Konsolidierung des Speicherbereichs.
    Tipps:
    - Die Zeit, die für die vollständige Neuverteilung von Daten und die Konsolidierung von Speicherbereich erforderlich ist, variiert abhängig von der Größe Ihrer Datenbank. Stellen Sie sicher, dass Sie dies bei der Planung berücksichtigen.
    - Stellen Sie sicher, dass die Verzeichnisse, die Sie angeben, dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.
  - Stoppen Sie den Server und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig nutzen zu können.

- Reorganisieren Sie die Datenbank, falls erforderlich. Die Index- und Tabellenreorganisation für die Serverdatenbank kann dazu beitragen, unerwartetes Datenbankwachstum und Leistungsprobleme zu verhindern. Weitere Informationen zur Reorganisation der Datenbank finden Sie in Technote 1683633.

- Um die Datenbank für Server der Version 7.1 und höher zu verkleinern, geben Sie im Serverinstanzverzeichnis die folgenden DB2-Befehle aus:
  Einschränkung: Die Befehle können die E/A-Aktivität erhöhen und sich unter Umständen auf die Serverleistung auswirken. Um Leistungsprobleme auf ein Mindestmaß zu reduzieren, warten Sie, bis ein Befehl abgeschlossen ist, bevor Sie den nächsten Befehl ausgeben. Die DB2-Befehle können ausgegeben werden, wenn der Server aktiv ist.

  ```
  db2 connect to tsmdb1
  db2 set schema tsmdb1
  db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
  db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
  db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE1 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE2 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE3 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE4 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
  db2 ALTER TABLESPACE DEDUPIDXSPACE5 REDUCE MAX
  ```

- Um die aktive Protokolldatei zu vergrößern oder zu verkleinern, führen Sie die folgenden Schritte aus:
  1. Stellen Sie sicher, dass die Position für die aktive Protokolldatei über genügend Speicherbereich für die erhöhte Protokollgröße verfügt. Wenn ein Protokollspiegel vorhanden ist, muss auch die Position für den Spiegel über genügend Speicherbereich für die erhöhte Protokollgröße verfügen.
  2. Stoppen Sie den Server.
  3. Aktualisieren Sie in der Datei dsmserv.opt die Option ACTIVELOGSIZE mit der neuen Größe der aktiven Protokolldatei (angegeben in Megabyte).
     Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Die folgende Tabelle enthält Richtlinien für den Speicherbedarf:

     Tabelle 1. Schätzen des Speicherbedarfs für Datenträger und Dateibereiche

Wert für die Option ACTIVELOGSize	**Größe des im Verzeichnis für aktive Protokolldateien zu reservierender freier Speicherbereich zusätzlich zum Speicherbereich für ACTIVELOGSize**
16 GB bis 128 GB	5120 MB
129 GB bis 256 GB	10240 MB
257 GB bis 512 GB	20480 MB

     Um die Größe der aktiven Protokolldatei in die maximale Größe von 512 GB zu ändern, geben Sie die folgende Serveroption ein:

     ```
     activelogsize 524288
     ```

  4. Wenn Sie planen, ein neues Verzeichnis für aktive Protokolldateien zu verwenden, aktualisieren Sie den in der Serveroption ACTIVELOGDIRECTORY angegebenen Verzeichnisnamen. Das neue Verzeichnis muss leer sein und die Benutzer-ID des Datenbankmanagers muss Zugriff auf dieses Verzeichnis haben.
  5. Starten Sie den Server erneut.

- Komprimieren Sie die Archivprotokolle, um die Größe des Speicherbereichs, der zum Speichern benötigt wird, zu reduzieren. Aktivieren Sie die dynamische Komprimierung für das Archivprotokoll, indem Sie den folgenden Befehl ausgeben:

  ```
  setopt archlogcompress yes
  ```

  Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hohen Workloads aktivieren. Ein Aktivieren dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Dateisystem für Archivprotokolle haben. Diese Verzögerung kann zur Folge haben, dass der Speicherbereich im Dateisystem für aktive Protokolldateien knapp wird. Sie müssen den verfügbaren Speicherbereich im Dateisystem für aktive Protokolldateien überwachen, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn für das Dateisystem für das Verzeichnis für aktive Protokolldateien fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT können Sie die Komprimierung für das Archivprotokoll sofort inaktivieren, ohne den Server stoppen zu müssen.

Zugehörige Verweise:
Serveroption ACTIVELOGSIZE
EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)
SETOPT (Serveroption für dynamische Aktualisierung definieren)

Speichernutzung und Prozessorauslastung verwalten

Der Speicherbedarf und die Prozessorauslastung müssen verwaltet werden, um sicherzustellen, dass der Server Datenprozesse wie Sicherung und Datendeduplizierung ausführen kann. Berücksichtigen Sie die Auswirkung auf die Leistung, wenn Sie bestimmte Prozesse ausführen.

Vorbereitende Schritte

- Stellen Sie sicher, dass Ihre Konfiguration die erforderliche Hardware und Software verwendet. Weitere Informationen finden Sie in IBM Spectrum Protect Supported Operating Systems.
- Weitere Informationen zur Verwaltung von Ressourcen, wie beispielsweise Datenbank und Wiederherstellungsprotokoll, finden Sie in Planung der Speicherarrays.
- Fügen Sie zusätzlichen Systemspeicher hinzu, um festzustellen, ob sich die Leistung verbessert. Überwachen Sie die Speichernutzung regelmäßig, um zu bestimmen, ob weiterer Speicher erforderlich ist.

Vorgehensweise

1. Geben Sie, falls möglich, Speicherbereich aus dem Dateisystemcache frei.
2. Verwenden Sie zur Verwaltung des Systemspeichers, den jeder Server auf einem System verwendet, die Serveroption DBMEMPERCENT. Begrenzen Sie den Prozentsatz des Systemspeichers, der vom Datenbankmanager jedes Servers verwendet werden kann. Wenn alle Server gleich wichtig sind, verwenden Sie denselben Wert für jeden Server. Wenn ein Server der Produktionsserver ist und die anderen Server Testserver sind, definieren Sie für den Produktionsserver einen höheren Wert als für die Testserver.
3. Definieren Sie den Benutzerdatengrenzwert und den privaten Speicher für die Datenbank, um sicherzustellen, dass immer genügend privater Speicher verfügbar ist. Wenn der private Speicher knapp wird, kann dies Fehler, eine nicht optimale Leistung und Instabilität zur Folge haben.


Linux-Betriebssysteme

Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann

Wenn Ihr IBM Spectrum Protect-Server Knoten auf einen fernen Server repliziert oder Speicherpools auf einem fernen Server schützt, prüfen Sie, ob der Datendurchsatz an den fernen Server mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) verbessert werden kann. Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie die entsprechenden Lizenzen anfordern. Es sind sowohl Test- als auch Volllizenzen verfügbar.

Vorbereitende Schritte

Die Aspera FASP-Technologie wird zur Übertragung von Datenbereichen aus einem Containerspeicherpool auf einen fernen Server verwendet. Wenn die Aspera FASP-Technologie aktiviert ist, werden die Datenbereiche, unabhängig davon, ob das Protokoll Secure Sockets Layer (SSL) aktiviert ist, bei der Übertragung immer verschlüsselt. Soll jedoch die Netzverbindung geschützt werden, müssen Sie SSL aktivieren. Informationen zu SSL und zur Aktivierung von SSL finden Sie in Kommunikation über Secure Sockets Layer und Transport Layer Security.

Informationen zu diesem Vorgang

Einschränkungen:

- Verwenden Sie die Aspera FASP-Technologie, wenn Ihr Weitverkehrsnetz (WAN-Netz) Anzeichen großer Paketverluste und/oder Datenübertragungsverzögerungen zeigt, die durch eine Beeinträchtigung des Netzes verursacht werden. Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.
- Um die Aspera FASP-Technologie für Knotenreplikationsoperationen zu aktivieren, müssen die Daten in einem Verzeichniscontainerspeicherpool gespeichert sein.

Vorgehensweise

1. Bestimmen Sie, ob die Aspera FASP-Technologie für Ihre Systemumgebung geeignet ist. Wenn eine der folgenden Bedingungen erfüllt ist, aktivieren Sie die Aspera FASP-Technologie:
   - Durchschnittliche Verzögerungen bei Datenübertragungsoperationen überschreiten 50 Millisekunden.
   - Der Paketverlust ist größer als 0,01 %.

   Netzmerkmale können sehr unterschiedlich sein. Möglicherweise können Sie den Netzdurchsatz durch die Aktivierung der Aspera FASP-Technologie selbst dann verbessern, wenn die Datenübertragungsverzögerung weniger als 50 Millisekunden und der Paketverlust weniger als 0,01 % beträgt.

2. Fordern Sie die entsprechenden Lizenzen an und installieren Sie diese. Führen Sie eine der folgenden Aktionen aus:

   Testlizenzen anfordern und installieren

   Um Testlizenzen, die eine Ablaufdauer von 30 Tagen haben, anzufordern und zu installieren, führen Sie die folgenden Schritte aus:

   a. Fordern Sie die Lizenzen an, indem Sie eine E-Mail an alliances@asperasoft.com senden:
      - Geben Sie den Namen Ihres Unternehmens, Ihre Adresse, Ihre Telefonnummer und die E-Mail-Adresse des primären Ansprechpartners in Ihrem Unternehmen an.
      - Geben Sie an, dass eine Testlizenz mit einer Gültigkeit von 30 Tagen erforderlich ist.
      - Geben Sie die Anzahl erforderlicher Lizenzen an.

      Pro Server, der für die Datenübertragung mit der Aspera FASP-Technologie verwendet wird, ist jeweils eine Lizenz erforderlich. Wenn Sie beispielsweise einen Knoten von einem Quellenserver auf einen Zielserver replizieren, sind zwei Lizenzen erforderlich.

      Wenn die Lizenzanforderung genehmigt wird, empfängt der primäre Ansprechpartner in der Regel innerhalb von 24 Stunden eine E-Mail. Die E-Mail-Anlage umfasst Lizenzdateien, die gemäß der folgenden Konvention benannt sind:

      xxxxx-ConnectSrv-unlim.eval.aspera-license

      Dabei ist *xxxxx* eine eindeutige Zahl.

   b. Kopieren Sie eine der Lizenzdateien in das Verzeichnis server/bin des Quellenservers. Wählen Sie eine der beiden Lizenzdateien aus. Das Verzeichnis befindet sich standardmäßig an der folgenden Position:

      ```
      /opt/tivoli/tsm/server/bin
      ```

   c. Kopieren Sie die andere Lizenzdatei in das Verzeichnis bin auf dem Zielserver.
   d. Setzen Sie auf dem Quellen- und dem Zielserver die Berechtigungsstufe jeder Lizenzdatei auf 755. Wenn Sie beispielsweise das Standardinstallationsverzeichnis verwenden und die eindeutige Lizenznummer 47474 lautet, geben Sie den folgenden Befehl in einer einzigen Zeile aus:

      ```
      chmod 755 /opt/tivoli/tsm/server/bin/
      47474-ConnectSrv-unlim.eval.aspera-license
      ```

   Volllizenzen anfordern und installieren

   Um uneingeschränkte Volllizenzen ohne Ablaufdauer anzufordern und zu installieren, führen Sie die folgenden Schritte aus:

   a. Kaufen Sie das Produkt IBM Spectrum Protect High Speed Data Transfer. Die Produktidentifikationsnummer lautet 5725-Z10. Sie können das Produkt über Passport Advantage anfordern.

      Pro Server, der für die Datenübertragung mit der Aspera FASP-Technologie verwendet wird, ist eine Instanz von IBM Spectrum Protect High Speed Data Transfer erforderlich. Wenn Sie beispielsweise einen Knoten von einem Quellenserver auf einen Zielserver replizieren, sind zwei Instanzen von IBM Spectrum Protect High Speed Data Transfer erforderlich.

   b. Installieren Sie IBM Spectrum Protect High Speed Data Transfer mithilfe des Installationsassistenten auf jedem Server.

   Einschränkung: Wenn die erforderlichen Lizenzen fehlen oder abgelaufen sind, schlagen Operationen zum Replizieren von Knoten und Schützen von Speicherpools mithilfe der Aspera FASP-Technologie fehl.
3. Optional: Validieren Sie die Aspera FASP-Konfiguration, indem Sie den Befehl VALIDATE ASPERA ausgeben. Mit dem Befehl VALIDATE ASPERA können Sie sicherstellen, dass Ihre Systemumgebung für Aspera FASP korrekt konfiguriert ist und dass gültige Lizenzen installiert sind. Darüber hinaus können Sie mithilfe des Befehls die Geschwindigkeit des Netzdurchsatzes bei Verwendung der Aspera FASP-Technologie gegenüber der bei Verwendung der TCP/IP-Technologie vergleichen.

Nächste Schritte

Um die Aspera FASP-Technologie zu aktivieren, führen Sie die Schritte in Datenübertragung durch Aktivierung der Aspera FASP-Technologie optimieren aus.

- Datenübertragung durch Aktivierung der Aspera FASP-Technologie optimieren
  Wenn Sie einen fernen Server für den Speicherpoolschutz oder die Knotenreplikation verwenden und Netzprobleme auftreten, möchten Sie möglicherweise die Datenübertragung mithilfe der Technologie von Aspera Fast Adaptive Secure Protocol (FASP) optimieren.

Durchführung eines Upgrades für den Server planen

Wenn ein Fixpack oder ein vorläufiger Fix verfügbar wird, können Sie für den IBM Spectrum Protect-Server ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten erfolgen. Stellen Sie sicher, dass Sie vor der Durchführung eines Upgrades für den Server die Planungsschritte ausführen.

Informationen zu diesem Vorgang

Beachten Sie diese Richtlinien:

- Bei der bevorzugten Methode erfolgt das Upgrade für den Server mithilfe des Installationsassistenten. Nachdem Sie den Assistenten gestartet haben, klicken Sie im Fenster IBM Installation Manager auf das Symbol zum Aktualisieren; klicken Sie nicht auf das Symbol zum Installieren oder Ändern!
- Wenn sowohl für die Serverkomponente als auch für die Operations Center-Komponente Upgrades verfügbar sind, wählen Sie die Kontrollkästchen aus, um das Upgrade für beide Komponenten durchzuführen.

Vorgehensweise

1. Überprüfen Sie die Liste der Fixpacks und vorläufigen Fixes. Siehe Technote 1239415.
2. Studieren Sie die Produktverbesserungen, die in der Readme-Datei beschrieben sind.
   Tipp: Wenn Sie die Installationspaketdatei von der IBM Spectrum Protect-Unterstützungssite abrufen, können Sie auch auf die Readme-Datei zugreifen.
3. Stellen Sie sicher, dass die Version, auf die das Upgrade für Ihren Server durchgeführt wird, mit anderen Komponenten, wie beispielsweise Speicheragenten und Speicherarchivclients, kompatibel ist. Siehe Technote 1302789.
4. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden. Siehe Technote 1053218.
5. Lesen Sie die Upgradeanweisungen. Stellen Sie sicher, dass Sie die Serverdatenbank, die Einheitenkonfigurationsinformationen und die Protokolldatei für Datenträger sichern.

Nächste Schritte

Um ein Fixpack oder einen vorläufigen Fix zu installieren, führen Sie die Anweisungen für Ihr Betriebssystem aus:

- AIX-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
- Linux-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren
- Windows-BetriebssystemeIBM Spectrum Protect-Server-Fixpack installieren

Geplante Aktivitäten optimieren

Planen Sie täglich Verwaltungstasks, um sicherzustellen, dass Ihre Lösung ordnungsgemäß funktioniert. Indem Sie Ihre Lösung optimieren, können Sie Serverressourcen maximieren und verschiedene Funktionen, die in Ihrer Lösung verfügbar sind, effektiv nutzen.

Vorgehensweise

1. Überwachen Sie die Systemleistung regelmäßig, um sicherzustellen, dass Clientsicherungs- und Serververwaltungstasks erfolgreich ausgeführt werden. Führen Sie die Anweisungen in Speicherlösungen überwachen aus.
2. Optional: Wenn die Überwachungsdaten anzeigen, dass sich die Server-Workload erhöht hat, überprüfen Sie die Planungsinformationen. Überprüfen Sie, ob die Kapazität des Systems in den folgenden Fällen ausreichend ist:
   - Erhöhung der Anzahl Clients
   - Zunahme des Datenvolumens, das gesichert wird
   - Änderung des Zeitraums, der für Sicherungen verfügbar ist
3. Bestimmen Sie, ob Ihre Lösung auf dem von Ihnen erwarteten Niveau ausgeführt wird. Überprüfen Sie die Clientzeitpläne dahingehend, ob Tasks innerhalb des geplanten Zeitrahmens ausgeführt werden:
   a. Wählen Sie auf der Seite Clients im Operations Center den Client aus.
   b. Klicken Sie auf Details.
   c. Überprüfen Sie auf der Seite Zusammenfassung des Clients die für Gesichert und Repliziert angegebene Aktivität, um alle Risiken zu ermitteln.

   Passen Sie, falls erforderlich, den Zeitpunkt und die Häufigkeit für die Ausführung von Clientsicherungsoperationen an.
4. Planen Sie ausreichend Zeit ein, um die folgenden Verwaltungstasks innerhalb von 24 Stunden erfolgreich ausführen zu können:
   a. Schützen von Speicherpools
   b. Replizieren von Knotendaten
   c. Sichern der Datenbank
   d. Ausführen der Verfallsverarbeitung, um Clientsicherungen und Archivierungsdateikopien aus dem Serverspeicher zu entfernen

   Tipp: Planen Sie einen geeigneten Zeitpunkt für den Start von Verwaltungstasks und die Ausführung in der korrekten Reihenfolge. Planen Sie beispielsweise Replikationstasks im Anschluss an die erfolgreiche Ausführung von Clientsicherungen.

- Clients von einem Server auf einen anderen versetzen
  Um zu verhindern, dass der Speicherbereich auf einem Server knapp wird, oder um Workloadprobleme zu beheben, müssen Sie unter Umständen Clientknoten von einem Server auf einen anderen versetzen.

Zugehörige Konzepte:
Leistung
Zugehörige Tasks:
Daten deduplizieren (Version 7.1.1)

Clientoperationen verwalten

Sie können Fehler, die einen Client für Sichern/Archivieren betreffen, mithilfe des Operations Center, das Vorschläge zur Behebung von Fehlern bereitstellt, auswerten und beheben. Bei Fehlern für andere Typen von Clients müssen Sie die Fehlerprotokolle auf dem Client überprüfen und in der Produktdokumentation nachlesen.

Informationen zu diesem Vorgang

In einigen Fällen können Clientfehler behoben werden, indem der Clientakzeptor gestoppt und gestartet wird. Wenn Clientknoten oder Administrator-IDs gesperrt sind, können Sie das Problem beheben, indem Sie den Clientknoten bzw. die Administrator-ID entsperren und dann das Kennwort zurücksetzen.

Detaillierte Anweisungen zum Identifizieren und Beheben von Clientfehlern finden Sie in Clientprobleme lösen.

- Bereich einer Clientsicherung ändern
  Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.
- Fehler in Clientfehlerprotokollen auswerten
  Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.
- Clientakzeptor stoppen und erneut starten
  Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.
- Kennwörter zurücksetzen
  Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.
- Clientknoten stilllegen
  Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.
- Daten zum Freigeben von Speicherbereich inaktivieren
  In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegeben Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.
- Client-Upgrades verwalten
  Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

Bereich einer Clientsicherung ändern

Wenn Sie Clientsicherungsoperationen konfigurieren, ist das bevorzugte Verfahren das Ausschließen von Objekten, die nicht erforderlich sind. Angenommen, Sie möchten normalerweise temporäre Dateien von einer Sicherungsoperation ausschließen.

Informationen zu diesem Vorgang

Indem Sie nicht benötigte Objekte von Sicherungsoperationen ausschließen, können Sie die Größe des Speicherbereichs, der für Sicherungsoperationen erforderlich ist, und die Speicherkosten besser steuern. Abhängig von Ihrem Lizenzpaket ist es unter Umständen auch möglich, die Lizenzierungskosten zu begrenzen.

Vorgehensweise

Die Vorgehensweise beim Ändern des Bereichs von Sicherungsoperationen ist von dem Produkt abhängig, das auf dem Clientknoten installiert ist:

- Bei einem Client für Sichern/Archivieren können Sie eine Einschluss-/Ausschlussliste erstellen, um eine Datei, Dateigruppen oder Verzeichnisse in Sicherungsoperationen einzuschließen oder von Sicherungsoperationen auszuschließen. Um eine Einschluss-/Ausschlussliste zu erstellen, führen Sie die Anweisungen in Einschluss-/Ausschlussliste erstellen aus.

  Um die konsistente Verwendung einer Einschluss-/Ausschlussliste für alle Clients eines bestimmten Typs zu gewährleisten, können Sie auf dem Server eine Clientoptionsgruppe erstellen, die die erforderlichen Optionen enthält. Anschließend ordnen Sie die Clientoptionsgruppe jedem Client desselben Typs zu. Ausführliche Informationen finden Sie in Clientoperationen über Clientoptionsgruppen steuern.

- Für einen Client für Sichern/Archivieren können Sie die Objekte, die in eine Teilsicherungsoperation eingeschlossen werden sollen, mithilfe der Option domain angeben. Führen Sie die Anweisungen in Clientoption 'domain' aus.
- Führen Sie für andere Produkte die Anweisungen in der Produktdokumentation aus, um zu definieren, welche Objekte in Sicherungsoperationen eingeschlossen und von Sicherungsoperationen ausgeschlossen werden sollen.

Fehler in Clientfehlerprotokollen auswerten

Sie können Clientfehler beheben, indem Sie Vorschläge vom Operations Center anfordern oder die Fehlerprotokolle auf dem Client überprüfen.

Vorbereitende Schritte

Um Fehler in einem Client für Sichern/Archivieren unter einem Linux- oder Windows-Betriebssystem zu beheben, stellen Sie sicher, dass der Clientverwaltungsservice installiert und gestartet wurde. Installationsanweisungen finden Sie in Diagnoseinformationen mit Clientverwaltungsservices erfassen.

Vorgehensweise

Um Clientfehler zu diagnostizieren und zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn der Clientverwaltungsservice auf dem Clientknoten installiert ist, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Details.
  3. Klicken Sie auf der Seite 'Zusammenfassung' auf die Registerkarte Diagnose.
  4. Überprüfen Sie die abgerufenen Protokollnachrichten.
     Tipps:
     - Um das Fenster 'Clientprotokolle' ein- oder auszublenden, doppelklicken Sie auf den Rahmen des Fensters 'Clientprotokolle'.
     - Um die Größe des Fensters 'Clientprotokolle' zu ändern, klicken Sie auf den Rahmen des Fensters 'Clientprotokolle' und ziehen Sie den Rahmen.

     Wenn auf der Seite 'Diagnose' Vorschläge angezeigt werden, wählen Sie einen Vorschlag aus. Im Fenster 'Clientprotokolle' sind die Clientprotokollnachrichten, auf die sich der Vorschlag bezieht, hervorgehoben.
  5. Lösen Sie die in den Fehlernachrichten angegebenen Probleme mithilfe der Vorschläge.
     Tipp: Vorschläge werden nur für einen Teil der Clientnachrichten bereitgestellt.
- Wenn der Clientverwaltungsservice nicht auf dem Clientknoten installiert ist, überprüfen Sie die Fehlerprotokolle für den installierten Client.

Clientakzeptor stoppen und erneut starten

Wenn Sie die Konfiguration Ihrer Lösung ändern, müssen Sie den Clientakzeptor auf allen Clientknoten erneut starten, auf denen ein Client für Sichern/Archivieren installiert ist.

Informationen zu diesem Vorgang

In einigen Fällen können Clientzeitplanungsprobleme behoben werden, indem der Clientakzeptor gestoppt und erneut gestartet wird. Der Clientakzeptor muss aktiv sein, um sicherzustellen, dass geplante Operationen auf dem Client erfolgen können. Wenn Sie beispielsweise die IP-Adresse oder den Domänennamen des Servers ändern, müssen Sie den Clientakzeptor erneut starten.

Vorgehensweise

Führen Sie die Anweisungen für das Betriebssystem aus, das auf dem Clientknoten installiert ist:

AIX und Oracle Solaris

- Um den Clientakzeptor zu stoppen, führen Sie die folgenden Schritte aus:
  a. Bestimmen Sie die Prozess-ID für den Clientakzeptor, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

     ```
     ps -ef | grep dsmcad
     ```

     Überprüfen Sie die Ausgabe. In der folgenden Beispielausgabe lautet die Prozess-ID für den Clientakzeptor 6764:

     ```
     root  6764     1   0 16:26:35 ?           0:00 /usr/bin/dsmcad
     ```

  b. Geben Sie in der Befehlszeile den folgenden Befehl aus:

     ```
     kill -9 PID
     ```

     Dabei gibt *PID* die Prozess-ID für den Clientakzeptor an.
- Um den Clientakzeptor zu starten, geben Sie in der Befehlszeile den folgenden Befehl aus:

  ```
  /usr/bin/dsmcad
  ```

Linux

- Um den Clientakzeptor zu stoppen, ohne ihn erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad stop
```

- Um den Clientakzeptor zu stoppen und erneut zu starten, geben Sie den folgenden Befehl aus:

```
# service dsmcad restart
```

MAC OS X

Klicken Sie auf Applications > Utilities > Terminal.

- Um den Clientakzeptor zu stoppen, geben Sie den folgenden Befehl aus:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Um den Clientakzeptor zu starten, geben Sie den folgenden Befehl aus:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Um den Clientakzeptorservice zu stoppen, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf Start > Verwaltung > Dienste.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf Beenden und OK.
- Um den Clientakzeptorservice erneut zu starten, führen Sie die folgenden Schritte aus:
  a. Klicken Sie auf Start > Verwaltung > Dienste.
  b. Doppelklicken Sie auf den Clientakzeptorservice.
  c. Klicken Sie auf Starten und OK.

Zugehörige Verweise:
Fehler für Clientzeitplanung beheben

Kennwörter zurücksetzen

Wenn ein Kennwort für einen Clientknoten oder eine Administrator-ID verloren gegangen ist oder Sie das Kennwort vergessen haben, können Sie das Kennwort zurücksetzen. Mehrere Versuche, mit einem ungültigen Kennwort auf das System zuzugreifen, können zur Folge haben, dass ein Clientknoten oder eine Administrator-ID gesperrt wird. Zur Behebung des Problems können entsprechende Schritte ausgeführt werden.

Vorgehensweise

Um Kennwortprobleme zu beheben, führen Sie eine der folgenden Aktionen aus:

- Wenn ein Client für Sichern/Archivieren auf einem Clientknoten installiert ist und das Kennwort verloren gegangen ist oder Sie das Kennwort vergessen haben, führen Sie die folgenden Schritte aus:
  1. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Knotenname* den Clientknoten und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
  2. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.
     Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf `generate` gesetzt haben.
- Wenn ein Administrator aufgrund von Kennwortproblemen ausgesperrt ist, führen Sie die folgenden Schritte aus:
  1. Um dem Administrator den Zugriff auf den Server zu ermöglichen, geben Sie den Befehl UNLOCK ADMIN aus. Anweisungen finden Sie in UNLOCK ADMIN (Administrator entsperren).
  2. Legen Sie mit dem Befehl UPDATE ADMIN ein neues Kennwort fest:

     ```
     update admin Administratorname neues_Kennwort forcepwreset=yes
     ```

     Dabei gibt *Administratorname* den Namen des Administrators und *neues_Kennwort* das Kennwort an, das Sie zuordnen.
- Wenn ein Clientknoten gesperrt ist, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, warum der Clientknoten gesperrt ist und ob er entsperrt werden muss. Wenn beispielsweise der Clientknoten stillgelegt ist, wird der Clientknoten aus der Produktionsumgebung entfernt. Sie können die Stilllegungsoperation nicht zurücknehmen und der Clientknoten bleibt gesperrt. Ein Clientknoten kann auch gesperrt sein, wenn die Clientdaten Gegenstand einer rechtlichen Untersuchung sind.
  2. Verwenden Sie zum Entsperren eines Clientknotens den Befehl UNLOCK NODE. Anweisungen finden Sie in UNLOCK NODE (Clientknoten entsperren).
  3. Generieren Sie ein neues Kennwort, indem Sie den Befehl UPDATE NODE ausgeben:

     ```
     update node Knotenname neues_Kennwort forcepwreset=yes
     ```

Dabei gibt *Knotenname* den Namen des Knotens und *neues_Kennwort* das Kennwort an, das Sie zuordnen.

4. Informieren Sie den Eigner des Clientknotens über das geänderte Kennwort. Wenn sich der Eigner des Clientknotens mit dem angegebenen Kennwort anmeldet, wird automatisch ein neues Kennwort generiert. Dieses Kennwort ist Benutzern nicht bekannt, um die Sicherheit zu verbessern.
   Tipp: Das Kennwort wird automatisch generiert, wenn Sie zuvor die Option passwordaccess in der Clientoptionsdatei auf `generate` gesetzt haben.

Clientknoten stilllegen

Wenn ein Clientknoten nicht mehr erforderlich ist, können Sie einen Prozess starten, um ihn aus der Produktionsumgebung zu entfernen. Wenn beispielsweise Daten von einer Workstation auf dem IBM Spectrum Protect-Server gesichert wurden, die Workstation aber nicht mehr verwendet wird, können Sie die Workstation stilllegen.

Informationen zu diesem Vorgang

Wenn Sie den Stilllegungsprozess starten, sperrt der Server den Clientknoten, um zu verhindern, dass dieser auf den Server zugreift. Dateien, die zu dem Clientknoten gehören, werden nacheinander gelöscht; anschließend wird der Clientknoten gelöscht. Sie können die folgenden Typen von Clientknoten stilllegen:

Anwendungsclientknoten
: Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Systemclientknoten
: Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

VM-Clientknoten
: Clientknoten virtueller Maschinen bestehen aus einem einzelnen Gasthost in einem Hypervisor. Jede virtuelle Maschine wird als ein Dateibereich dargestellt.

Die einfachste Methode zur Stilllegung eines Clientknotens ist die Verwendung des Operations Center. Der Stilllegungsprozess wird im Hintergrund ausgeführt. Wenn der Client für die Replikation von Clientdaten konfiguriert ist, entfernt das Operations Center den Client automatisch aus der Replikation auf dem Quellen- und dem Zielreplikationsserver, bevor es den Client stilllegt.
Tipp: Sie können einen Clientknoten auch stilllegen, indem Sie den Befehl DECOMMISSION NODE oder DECOMMISSION VM ausgeben. Diese Methode kann beispielsweise in den folgenden Fällen verwendet werden:

- Um den Stilllegungsprozess für einen späteren Zeitpunkt zu planen oder eine Serie von Befehlen unter Verwendung eines Scripts auszuführen, geben Sie die Ausführung des Stilllegungsprozesses im Hintergrund an.
- Um den Stilllegungsprozess zu Zwecken der Fehlerbehebung zu überwachen, geben Sie die Ausführung des Stilllegungsprozesses im Vordergrund an. Wenn Sie den Prozess im Vordergrund ausführen, müssen Sie warten, bis der Prozess abgeschlossen ist, bevor Sie die Arbeit mit anderen Tasks fortsetzen können.

Vorgehensweise

Führen Sie eine der folgenden Aktionen aus:

- Um einen Client mithilfe des Operations Center im Hintergrund stillzulegen, führen Sie die folgenden Schritte aus:
  1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients und wählen Sie den Client aus.
  2. Klicken Sie auf Weitere > Stilllegen.
- Um einen Clientknoten mithilfe eines Verwaltungsbefehls stillzulegen, führen Sie die folgenden Schritte aus:
  1. Bestimmen Sie, ob der Clientknoten für die Knotenreplikation konfiguriert ist, indem Sie den Befehl QUERY NODE ausgeben. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, führen Sie den folgenden Befehl aus:

     ```
     query node austin format=detailed
     ```

     Überprüfen Sie das Ausgabefeld 'Replikationsstatus'.
  2. Wenn der Clientknoten für die Replikation konfiguriert ist, entfernen Sie den Clientknoten aus der Replikation, indem Sie den Befehl REMOVE REPLNODE ausgeben. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

     ```
     remove replnode austin
     ```

  3. Führen Sie eine der folgenden Aktionen aus:
     - Um einen Anwendungs- oder Systemclientknoten im Hintergrund stillzulegen, geben Sie den Befehl DECOMMISSION NODE aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

       ```
       decommission node austin
       ```

- Um einen Anwendungs- oder Systemclientknoten im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION NODE unter Angabe des Parameters `wait=yes` aus. Wenn beispielsweise der Clientknoten den Namen AUSTIN hat, geben Sie den folgenden Befehl aus:

  ```
  decommission node austin wait=yes
  ```

- Um eine virtuelle Maschine im Hintergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM aus. Wenn beispielsweise die virtuelle Maschine den Namen AUSTIN hat, der Dateibereich 7 ist und der Dateibereichsname über die Dateibereichs-ID angegeben wird, geben Sie den folgenden Befehl aus:

  ```
  decommission vm austin 7 nametype=fsid
  ```

  Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

  ```
  decommission vm "austin 2" 7 nametype=fsid
  ```

- Um eine virtuelle Maschine im Vordergrund stillzulegen, geben Sie den Befehl DECOMMISSION VM unter Angabe des Parameters `wait=yes` aus. Geben Sie beispielsweise den folgenden Befehl aus:

  ```
  decommission vm austin 7 nametype=fsid wait=yes
  ```

  Wenn der Name der virtuellen Maschine ein oder mehrere Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen ein. Beispiel:

  ```
  decommission vm "austin 2" 7 nametype=fsid wait=yes
  ```

Nächste Schritte

Achten Sie auf Fehlernachrichten, die unter Umständen in der Benutzerschnittstelle oder in der Befehlsausgabe unmittelbar nach der Ausführung des Prozesses angezeigt werden.

Um zu überprüfen, ob der Clientknoten stillgelegt wurde, gehen Sie wie folgt vor:

1. Klicken Sie auf der Seite Übersicht im Operations Center auf Clients.
2. Überprüfen Sie in der Tabelle 'Clients' in der Spalte 'Gefährdet' den Status:
   - Der Status 'Stillgelegt' (DECOMMISSIONED) gibt an, dass der Knoten stillgelegt wurde.
   - Ein Nullwert gibt an, dass der Knoten nicht stillgelegt wurde.
   - Der Status 'Anstehend' (PENDING) gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

   Tipp: Wenn der Status eines anstehenden Stilllegungsprozesses bestimmt werden soll, geben Sie den folgenden Befehl aus:

   ```
   query process
   ```

3. Überprüfen Sie die Befehlsausgabe:
   - Wenn für den Stilllegungsprozess ein Status angegeben ist, ist der Prozess in Bearbeitung. Beispiel:

     ```
     query process
      Prozess-     Prozessbeschreibung           Prozessstatus
      nummer
     --------     --------------------     -----------------------------------------
            3          DECOMMISSION NODE        Anzahl der für Knoten NODE1 inaktivierten
                                                 Sicherungsobjekte: 8 Objekte inaktiviert.
     ```

   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie keine Fehlernachricht empfangen haben, ist der Prozess unvollständig. Ein Prozess kann unvollständig sein, wenn Dateien, die dem Knoten zugeordnet sind, noch nicht inaktiviert wurden. Führen Sie nach der Inaktivierung der Dateien den Stilllegungsprozess erneut aus.
   - Wenn für den Stilllegungsprozess kein Status angegeben ist und Sie eine Fehlernachricht empfangen, ist der Prozess fehlgeschlagen. Führen Sie den Stilllegungsprozess erneut aus.

Zugehörige Verweise:
DECOMMISSION NODE (Clientknoten stilllegen)
DECOMMISSION VM (Virtuelle Maschine stilllegen)
QUERY NODE (Knoten abfragen)
REMOVE REPLNODE (Clientknoten aus Replikation entfernen)

Daten zum Freigeben von Speicherbereich inaktivieren

In einigen Fällen können Sie Daten, die auf dem IBM Spectrum Protect-Server gespeichert sind, inaktivieren. Wenn Sie den Inaktivierungsprozess ausführen, werden alle Sicherungsdaten, die vor dem angegeben Datum und vor der angegebenen Uhrzeit gespeichert wurden, inaktiviert und gelöscht, sobald sie verfallen. Auf diese Art und Weise können Sie Speicherbereich auf dem Server freigeben.

Informationen zu diesem Vorgang

Einige Anwendungsclients sichern Daten immer als aktive Sicherungsdaten auf dem Server. Da aktive Sicherungsdaten nicht durch die Bestandsverfallsmaßnahmen verwaltet werden, werden die Daten nicht automatisch gelöscht und belegen unbegrenzt Serverspeicher. Um den Speicherbereich freizugeben, der von veralteten Daten belegt wird, können Sie die Daten inaktivieren.

Wenn Sie den Inaktivierungsprozess ausführen, werden alle aktiven Sicherungsdaten, die vor dem angegeben Datum gespeichert wurden, inaktiv. Die Daten werden gelöscht, sobald sie verfallen, und können nicht zurückgeschrieben werden. Die Inaktivierungsfunktion gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

Vorgehensweise

1. Klicken Sie auf der Seite 'Übersicht' im Operations Center auf Clients.
2. Wählen Sie in der Tabelle 'Clients' einen oder mehrere Clients aus und klicken Sie auf Weitere > Bereinigen.
   Befehlszeilenmethode: Inaktivieren Sie Daten mit dem Befehl DEACTIVATE DATA.

Zugehörige Verweise:
DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)

Client-Upgrades verwalten

Wenn ein Fixpack oder ein vorläufiger Fix für einen Client verfügbar wird, können Sie für den Client ein Upgrade durchführen, um die Vorteile der Produktverbesserungen zu nutzen. Die Upgrades für Server und Clients können zu unterschiedlichen Zeiten und mit einigen Einschränkungen für verschiedene Versionen erfolgen.

Vorbereitende Schritte

1. Überprüfen Sie die Voraussetzungen für die Client/Server-Kompatibilität in Technote 1053218. Wenn Ihre Lösung Server oder Clients vor Version 7.1 umfasst, überprüfen Sie die Richtlinien, um sicherzustellen, dass Clientsicherungs- und Archivierungsoperationen nicht unterbrochen werden.
2. Überprüfen Sie die Systemvoraussetzungen für den Client in IBM Spectrum Protect Supported Operating Systems.
3. Wenn die Lösung Speicheragenten oder Speicherarchivclients umfasst, überprüfen Sie die Informationen zur Kompatibilität von Speicheragenten bzw. Speicherarchivclients mit Servern, die als Speicherarchivmanager konfiguriert sind. Siehe Technote 1302789.

   Wenn Sie planen, ein Upgrade für einen Speicherarchivmanager und einen Speicherarchivclient durchzuführen, müssen Sie zuerst das Upgrade für den Speicherarchivmanager durchführen.

Vorgehensweise

Um ein Software-Upgrade durchzuführen, führen Sie die in der folgenden Tabelle aufgelisteten Anweisungen aus.

Software	Link zu Anweisungen
IBM Spectrum Protect-Client für Sichern/Archivieren	• Upgrade des Clients für Sichern/Archivieren durchführen
IBM Spectrum Protect Snapshot	• Installation und Upgrade für IBM Spectrum Protect Snapshot for UNIX and Linux durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for VMware durchführen • Installation und Upgrade für IBM Spectrum Protect Snapshot for Windows durchführen
IBM Spectrum Protect for Databases	• Upgrade für Data Protection for SQL Server durchführen • Installation von Data Protection for Oracle • Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
IBM Spectrum Protect for Enterprise Resource Planning	• Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für DB2 durchführen • Upgrade für IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP für Oracle durchführen
IBM Spectrum Protect for Mail	• Installation von Data Protection for IBM Domino auf einem UNIX-, AIX- oder Linux-System (Version 7.1.0) • Installation von Data Protection for IBM Domino auf einem Windows-System (Version 7.1.0) • Installation, Upgrade und Migration für IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server

Software	Link zu Anweisungen
IBM Spectrum Protect for Virtual Environments	• Installation und Upgrade für Data Protection for VMware durchführen • Data Protection for Microsoft Hyper-V installieren

Operations Center verwalten

Das Operations Center stellt Webzugriff und mobilen Zugriff auf Statusinformationen zur IBM Spectrum Protect-Umgebung bereit. Mithilfe des Operations Center können Sie mehrere Server überwachen und einige Verwaltungstasks ausführen. Über das Operations Center wird auch der Webzugriff auf die IBM Spectrum Protect-Befehlszeile bereitgestellt.

- Peripherieserver hinzufügen und entfernen
  In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.
- Web-Server starten und stoppen
  Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Assistenten für die Erstkonfiguration erneut starten
  Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.
- Hub-Server ändern
  Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.
- Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben
  Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

Peripherieserver hinzufügen und entfernen

In einer Umgebung mit mehreren Servern können Sie dem Hub-Server die anderen Server, die als *Peripherieserver* bezeichnet werden, hinzufügen.

Informationen zu diesem Vorgang

Die Peripherieserver senden Alerts und Statusinformationen an den Hub-Server. Das Operations Center zeigt eine konsolidierte Sicht der Alerts und Statusinformationen für den Hub-Server und alle Peripherieserver.

- Peripherieserver hinzufügen
  Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.
- Peripherieserver entfernen
  Sie können einen Peripherieserver aus dem Operations Center entfernen.

Peripherieserver hinzufügen

Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.

Vorbereitende Schritte

Die Kommunikation zwischen dem Peripherieserver und dem Hub-Server muss unter Verwendung des Protokolls Transport Layer Security (TLS) geschützt werden. Um die Kommunikation zu schützen, fügen Sie das Zertifikat des Peripherieservers der Truststore-Datei des Hub-Servers hinzu.

Vorgehensweise

1. Klicken Sie in der Menüleiste des Operations Center auf Server. Die Seite Server wird geöffnet.

   In der Tabelle auf der Seite Server könnte ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass - obwohl ein Administrator diesen Server mit dem Befehl DEFINE SERVER für den Hub-Server definiert hat - der Server noch nicht als Peripherieserver konfiguriert ist.

2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf Peripherieserver überwachen.
   - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird und die sichere SSL-/TLS-Kommunikation nicht erforderlich ist, klicken Sie in der Menüleiste der Tabelle auf +Peripherieserver.

3. Geben Sie die erforderlichen Informationen an und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.
   Tipp: Wenn der Aufbewahrungszeitraum für Ereignissätze des Servers weniger als 14 Tage beträgt, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

Peripherieserver entfernen

Sie können einen Peripherieserver aus dem Operations Center entfernen.

Informationen zu diesem Vorgang

Unter Umständen müssen Sie einen Peripherieserver in den folgenden Situationen entfernen:

- Der Peripherieserver soll von einem Hub-Server auf einen anderen Hub-Server versetzt werden.
- Der Peripherieserver soll stillgelegt werden.

Vorgehensweise

Um den Peripherieserver aus der Gruppe der Server zu entfernen, die vom Hub-Server verwaltet werden, führen Sie die folgenden Schritte aus:

1. Geben Sie in der IBM Spectrum Protect-Befehlszeile auf dem Hub-Server den folgenden Befehl aus:

   ```
   QUERY MONITORSETTINGS
   ```

2. Kopieren Sie in der Ausgabe des Befehls den Namen im Feld Überwachte Gruppe.
3. Geben Sie auf dem Hub-Server den folgenden Befehl aus; dabei ist *Gruppenname* der Name der überwachten Gruppe und *Mitgliedsname* der Name des Peripherieservers:

   ```
   DELETE GRPMEMBER Gruppenname Mitgliedsname
   ```

4. Optional: Wenn der Peripherieserver von einem Hub-Server auf einen anderen Hub-Server versetzt werden soll, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Alertausgabe und Überwachung auf dem Peripherieserver inaktivieren, indem Sie auf dem Peripherieserver die folgenden Befehle ausgeben:

   ```
   SET STATUSMONITOR OFF
   SET ALERTMONITOR OFF
   ```

5. Optional: Wenn die Definition des Peripherieservers für andere Zwecke verwendet wird, wie beispielsweise unternehmensweite Konfiguration, Befehlsweiterleitung, Speichern virtueller Datenträger oder Speicherarchivverwaltung, dürfen Sie diesen Schritt **nicht** ausführen. Andernfalls können Sie die Definition des Peripherieservers auf dem Hub-Server löschen, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

   ```
   DELETE SERVER Name_des_Peripherieservers
   ```

Web-Server starten und stoppen

Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Unter Umständen müssen Sie den Web-Server stoppen und starten, um beispielsweise Konfigurationsänderungen durchzuführen.

Vorgehensweise

1. Stoppen Sie den Web-Server.
   - AIX-BetriebssystemeGeben Sie im Verzeichnis /*Installationsverzeichnis*/ui/utils (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:

     ```
     ./stopserver.sh
     ```

   - Linux-BetriebssystemeGeben Sie den folgenden Befehl aus:

     ```
     service opscenter.rc stop
     ```

   - Windows-BetriebssystemeStoppen Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.
2. Starten Sie den Web-Server.
   - AIX-BetriebssystemeGeben Sie im Verzeichnis /*Installationsverzeichnis*/ui/utils (dabei gibt *Installationsverzeichnis* das Verzeichnis an, in dem das Operations Center installiert ist) den folgenden Befehl aus:

     ```
     ./startserver.sh
     ```

   - Linux-BetriebssystemeGeben Sie die folgenden Befehle aus:

     Starten Sie den Server:

     ```
     service opscenter.rc start
     ```

Starten Sie den Server erneut:

```
service opscenter.rc restart
```

Bestimmen Sie, ob der Server aktiv ist:

```
service opscenter.rc status
```

- Windows-BetriebssystemeStarten Sie den Dienst IBM Spectrum Protect Operations Center im Fenster Dienste.

Assistenten für die Erstkonfiguration erneut starten

Unter Umständen müssen Sie den Assistenten für die Erstkonfiguration im Operations Center erneut starten, um beispielsweise Konfigurationsänderungen durchzuführen.

Vorbereitende Schritte

Um die folgenden Einstellungen zu ändern, verwenden Sie die Seite Einstellungen im Operations Center, anstatt den Assistenten für die Erstkonfiguration erneut zu starten:

- Häufigkeit, mit der Statusdaten aktualisiert werden
- Dauer, die Alerts aktiv, inaktiv oder geschlossen bleiben
- Bedingungen, die angeben, dass Clients gefährdet sind

Die Hilfe des Operations Center enthält weitere Informationen zum Ändern dieser Einstellungen.

Informationen zu diesem Vorgang

Um den Assistenten für die Erstkonfiguration erneut zu starten, müssen Sie eine Merkmaldatei löschen, die Informationen zur Hub-Server-Verbindung enthält. Alle für den Hub-Server konfigurierten Einstellungen für Alertausgabe, Überwachung oder Gefährdung bzw. serverübergreifenden Einstellungen werden nicht gelöscht. Diese Einstellungen werden als Standardeinstellungen im Konfigurationsassistenten verwendet, wenn der Assistent erneut gestartet wird.

Vorgehensweise

1. Stoppen Sie den Web-Server des Operations Center.
2. Wechseln Sie auf dem Computer, auf dem das Operations Center installiert ist, in das folgende Verzeichnis (dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist):
   - AIX-BetriebssystemeLinux-Betriebssysteme*Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssysteme*Installationsverzeichnis*\ui\Liberty\usr\servers\guiServer

   Beispiel:
   - AIX-BetriebssystemeLinux-Betriebssysteme/opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
   - Windows-Betriebssystemec:\Programme\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. Löschen Sie im Verzeichnis guiServer die Datei serverConnection.properties.
4. Starten Sie den Web-Server des Operations Center.
5. Öffnen Sie das Operations Center.
6. Rekonfigurieren Sie mithilfe des Konfigurationsassistenten das Operations Center. Geben Sie ein neues Kennwort für die Überwachungsadministrator-ID an.
7. Aktualisieren auf jedem Peripherieserver, der bereits zuvor mit dem Hub-Server verbunden war, das Kennwort für die Überwachungsadministrator-ID, indem Sie den folgenden Befehl in der IBM Spectrum Protect-Befehlszeilenschnittstelle ausgeben:

   ```
   UPDATE ADMIN IBM-OC-Name_des_Hub-Servers neues_Kennwort
   ```

   Einschränkung: Übernehmen Sie alle anderen Einstellungen für diese Administrator-ID unverändert. Nachdem Sie das Anfangskennwort angegeben haben, wird dieses Kennwort automatisch vom Operations Center verwaltet.

Hub-Server ändern

Mithilfe des Operations Center können Sie den Hub-Server von IBM Spectrum Protect entfernen und einen anderen Hub-Server konfigurieren.

Vorgehensweise

1. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut. Im Rahmen dieser Prozedur löschen Sie die bestehende Hub-Server-Verbindung.
2. Verwenden Sie den Assistenten, um das Operations Center für die Verbindung zu dem neuen Hub-Server zu konfigurieren.

Zugehörige Tasks:
Assistenten für die Erstkonfiguration erneut starten

Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben

Wenn bestimmte Probleme auftreten, möchten Sie möglicherweise die Operations Center-Konfiguration mit dem vorkonfigurierten Zustand zurückschreiben, bei dem die IBM Spectrum Protect-Server nicht als Hub- oder Peripherieserver definiert sind.

Vorgehensweise

Um die Konfiguration zurückzuschreiben, führen Sie die folgenden Schritte aus:

1. Stoppen Sie den Web-Server des Operations Center.
2. Dekonfigurieren Sie den Hub-Server, indem Sie die folgenden Schritte ausführen:
   a. Geben Sie auf dem Hub-Server die folgenden Befehle aus:

      ```
      SET MONITORINGADMIN ""
      SET MONITOREDSERVERGROUP ""
      SET STATUSMONITOR OFF
      SET ALERTMONITOR OFF
      REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
      ```

      Tipp: `IBM-OC-Name_des_Hub-Servers` ist die Überwachungsadministrator-ID, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.
   b. Setzen Sie das Kennwort für den Hub-Server zurück, indem Sie den folgenden Befehl auf dem Hub-Server ausgeben:

      ```
      SET SERVERPASSWORD ""
      ```

      Achtung: Führen Sie diesen Schritt nicht aus, wenn der Hub-Server für andere Server für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation konfiguriert ist.
3. Dekonfigurieren Sie alle Peripherieserver, indem Sie die folgenden Schritte ausführen:
   a. Um zu bestimmen, ob noch Peripherieserver vorhanden sind, die als Mitglieder der Servergruppe definiert sind, geben Sie auf dem Hub-Server den folgenden Befehl aus:

      ```
      QUERY SERVERGROUP IBM-OC-Name_des_Hub-Servers
      ```

      Tipp: `IBM-OC-Name_des_Hub-Servers` ist der Name der überwachten Servergruppe, die bei der Konfiguration des ersten Peripherieservers automatisch erstellt wurde. Dieser Servergruppenname stimmt auch mit der Überwachungsadministrator-ID überein, die bei der Erstkonfiguration des Hub-Servers automatisch erstellt wurde.
   b. Um Peripherieserver aus der Servergruppe zu löschen, geben Sie auf dem Hub-Server für jeden Peripherieserver den folgenden Befehl aus:

      ```
      DELETE GRPMEMBER IBM-OC-Name_des_Hub-Servers Name_des_Peripherieservers
      ```

   c. Nachdem alle Peripherieserver aus der Servergruppe gelöscht wurden, geben Sie auf dem Hub-Server die folgenden Befehle aus:

      ```
      DELETE SERVERGROUP IBM-OC-Name_des_Hub-Servers
      SET MONITOREDSERVERGROUP ""
      ```

   d. Geben Sie auf jedem Peripherieserver die folgenden Befehle aus:

      ```
      REMOVE ADMIN IBM-OC-Name_des_Hub-Servers
      SETOPT PUSHSTATUS NO
      SET ALERTMONITOR OFF
      SET STATUSMONITOR OFF
      ```

   e. Löschen Sie die Definition des Hub-Servers, indem Sie auf jedem Peripherieserver den folgenden Befehl ausgeben:

      ```
      DELETE SERVER Name_des_Hub-Servers
      ```

      Achtung: Führen Sie diesen Schritt nicht aus, wenn die Definition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.
   f. Löschen Sie die Definition jedes Peripherieservers, indem Sie auf dem Hub-Server den folgenden Befehl ausgeben:

      ```
      DELETE SERVER Name_des_Peripherieservers
      ```

      Achtung: Führen Sie diesen Schritt nicht aus, wenn die Serverdefinition für andere Zwecke wie gemeinsame Speicherarchivnutzung, Export und Import von Daten oder Knotenreplikation verwendet wird.
4. Schreiben Sie die Standardeinstellungen auf jeden Server zurück, indem Sie die folgenden Befehle ausgeben:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Starten Sie den Assistenten für die Erstkonfiguration des Operations Center erneut.

Zugehörige Tasks:
Assistenten für die Erstkonfiguration erneut starten
Web-Server starten und stoppen

Virtuelle Bandarchive konfigurieren

Ein virtuelles Bandarchiv (VTL) verwendet keine physischen Banddatenträger. Wenn Sie VTL-Speicher implementieren, kann die Kapazität eines physischen Bandarchivs überschritten werden. Aufgrund der Möglichkeit, viele Datenträger und Laufwerke definieren zu können, kann größere Flexibilität für die Speicherumgebung bereitgestellt werden.

- Hinweise zur Verwendung virtueller Bandarchive
  Beim Definieren eines Speicherarchivs als virtuelles Bandarchiv (VTL), einschließlich Erweiterungen zur Leistungsverbesserung und Konfiguration Ihrer Hardware, sind einige Hinweise zu beachten.
- Virtuelles Bandarchiv Ihrer Umgebung hinzufügen
  Definieren Sie ein virtuelles Bandarchiv (VTL), um die Vorteile der Mountleistung und Skalierbarkeit nutzen zu können.
- Alle Laufwerke und Pfade für ein einzelnes Speicherarchiv definieren
  Verwenden Sie den Befehl PERFORM LIBACTION, um ein einzelnes SCSI-Speicherarchiv oder ein einzelnes virtuelles Bandarchiv (VTL) in einem einzigen Schritt zu konfigurieren.
- AIX-Betriebssysteme Linux-BetriebssystemeBeispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurieren
  Konfigurieren Sie ein VTL oder ein SCSI-Speicherarchiv, das zwei LTO-Bandlaufwerke enthält.
- AIX-Betriebssysteme Linux-BetriebssystemeBeispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren
  Sie können ein Speicherarchiv mit mehreren Laufwerkeinheitentypen konfigurieren, beispielsweise ein StorageTek L40-Speicherarchiv, das ein DLT-Laufwerk und ein LTO Ultrium-Laufwerk enthält.

Hinweise zur Verwendung virtueller Bandarchive

Beim Definieren eines Speicherarchivs als virtuelles Bandarchiv (VTL), einschließlich Erweiterungen zur Leistungsverbesserung und Konfiguration Ihrer Hardware, sind einige Hinweise zu beachten.

Informationen zu diesem Vorgang

Das Definieren eines virtuellen Bandarchivs (VTL) für den IBM Spectrum Protect-Server kann zu einer Leistungsverbesserung führen, da der Server die Mountpunktverarbeitung für VTLs anders als bei realen Bandarchiven handhabt. Die physischen Einschränkungen für reale Bandhardware gelten nicht für ein VTL, das Optionen zur besseren Skalierbarkeit bietet.

Sie können ein VTL für jedes virtuelle Bandarchiv verwenden, wenn die folgenden Bedingungen erfüllt sind:

- Für das VTL werden keine gemischten Datenträger verwendet. In dem Speicherarchiv wird nur ein einziger Typ und eine einzige Generation von Laufwerk und Datenträger emuliert.
- Jeder Server und jeder Speicheragent mit Zugriff auf das VTL hat Pfade, die für alle Laufwerke in dem Bandarchiv definiert sind.

Ist eine dieser Bedingungen nicht erfüllt, kann der Vorteil in Bezug auf die Mountleistung, der durch das Definieren eines VTL-Speicherarchivs für den IBM Spectrum Protect-Server entsteht, geringer ausfallen oder negiert werden.

VTLs sind mit früheren Versionen von Speicherarchivclients und Speicheragenten kompatibel. Der Typ von Speicherarchiv, der für Speicher verwendet wird, hat keine Auswirkungen auf den Speicherarchivclient oder den Speicheragenten. Wenn die Bedingungen in Bezug auf gemischte Datenträger und Pfad für ein SCSI-Speicherarchiv erfüllt sind, kann es mit LIBTYPE=VTL definiert oder aktualisiert werden.

- Speicherkapazität für virtuelle Bandarchive
  Da virtuelle Bandarchive (VTLs) nicht den physischen Einschränkungen realer Bandhardware unterliegen, ist ihre Speicherkapazität flexibler.
- Laufwerkkonfiguration für virtuelle Bandarchive
  Abhängig von den Anforderungen Ihrer Umgebung ist die Laufwerkkonfiguration in einem virtuellen Bandarchiv (VTL) variabel.

Speicherkapazität für virtuelle Bandarchive

Da virtuelle Bandarchive (VTLs) nicht den physischen Einschränkungen realer Bandhardware unterliegen, ist ihre Speicherkapazität flexibler.

Das Konzept der Speicherkapazität in einem virtuellen Bandarchiv unterscheidet sich von dem in physischer Bandhardware. In einem physischen Bandarchiv hat jeder Datenträger eine definierte Kapazität und die Kapazität des Bandarchivs ist als Gesamtzahl Datenträger in dem Bandarchiv definiert. Die Kapazität eines virtuellen Bandarchivs hingegen, ist als insgesamt verfügbarer Plattenspeicherplatz definiert. Sie können die Anzahl und Größe der Datenträger auf der Platte erhöhen oder reduzieren.

Diese Variabilität hat Auswirkungen auf knappen Speicherbereich in einem virtuellen Bandarchiv. Beispielsweise kann auf einem Datenträger in einem virtuellen Bandarchiv der Speicherbereich knapp werden, bevor die zugeordnete Kapazität erreicht wird, wenn auf der zu Grunde liegenden Platte der Speicherbereich knapp wird. In dieser Situation kann der Server eine Datenträgerendenachricht empfangen, ohne dass eine Warnung ausgegeben würde, was Sicherungsfehler zur Folge hat.

Wenn Fehler aufgrund fehlenden Speicherbereichs oder Sicherungsfehler auftreten, ist in der Regel noch Plattenspeicherplatz in dem virtuellen Bandarchiv verfügbar. Er ist in Datenträgern verborgen, die nicht im Gebrauch sind. Beispielsweise werden Datenträger, die im IBM Spectrum Protect-Server logisch gelöscht oder wieder in den Arbeitsstatus versetzt werden, nur in der Serverdatenbank gelöscht. Das virtuelle Bandarchiv wird nicht benachrichtigt und verwaltet die vollständige Größe des Datenträgers gemäß der Kapazitätszuordnung.

Um zu verhindern, dass Fehler aufgrund fehlenden Speicherbereichs auftreten, müssen Sie sicherstellen, dass jedes SCSI-Speicherarchiv, das mit LIBTYPE=VTL aktualisiert wird, unter Angabe von YES für den Parameter RELABELSCRATCH aktualisiert wird. Die Option RELABELSCRATCH ermöglicht es dem Server, den Kennsatz für jeden gelöschten Datenträger zu überschreiben und im Speicherarchiv in den Arbeitsstatus zurückzuversetzen. Für den Parameter RELABELSCRATCH wird standardmäßig für jedes als VTL definierte Speicherarchiv YES angenommen.

Zugehörige Verweise:
UPDATE LIBRARY (Speicherarchiv aktualisieren)

Laufwerkkonfiguration für virtuelle Bandarchive

Abhängig von den Anforderungen Ihrer Umgebung ist die Laufwerkkonfiguration in einem virtuellen Bandarchiv (VTL) variabel.

Die meisten VTL-Umgebungen verwenden so viele Laufwerke wie möglich, um die Anzahl gleichzeitig ablaufender Bandoperationen zu maximieren. Ein einzelner Bandmount in einer VTL-Umgebung erfolgt in der Regel schneller ein physischer Bandmount. Werden jedoch viele Laufwerke verwendet, verlängert sich die Zeit, die der IBM Spectrum Protect-Server benötigt, wenn ein Mount angefordert wird. Der Auswahlprozess dauert länger, da sich die Anzahl Laufwerke, die in einem einzigen Speicherarchivobjekt definiert ist, erhöht. Virtuelle Bandmounts können abhängig von der Anzahl Laufwerke in dem VTL genauso lange oder länger als physische Bandmounts dauern.

Überprüfen Sie zusammen mit Ihrem VTL-Anbieter die einheitenspezifischen Empfehlungen, um die besten Ergebnisse beim Erstellen von Laufwerken zu erzielen. Sind mehr als 300-500 Laufwerke für jedes VTL erforderlich, können Sie das VTL logisch in mehrere Speicherarchive partitionieren und jedem Speicherarchiv Laufwerke zuordnen. Möglicherweise unterliegt die Anzahl Einheiten, die innerhalb des VTL-Speicherarchivs verwendet werden können, aufgrund des Betriebssystems und der SAN-Hardwarekonfiguration gewissen Einschränkungen.

Virtuelles Bandarchiv Ihrer Umgebung hinzufügen

Definieren Sie ein virtuelles Bandarchiv (VTL), um die Vorteile der Mountleistung und Skalierbarkeit nutzen zu können.

Informationen zu diesem Vorgang

VTLs werden mithilfe des Befehls DEFINE LIBRARY unter Angabe des Parameters LIBTYPE=VTL angegeben. Da ein VTL-Speicherarchiv funktional mit dem Server auf dieselbe Art und Weise wie ein SCSI-Speicherarchiv interagiert, können Sie den Befehl UPDATE LIBRARY verwenden, um den Speicherarchivtyp eines bereits definierten SCSI-Speicherarchivs zu ändern. Sie müssen das Speicherarchiv nicht erneut definieren.

Vorgehensweise

- Fügen Sie ein neues VTL-Speicherarchiv hinzu. Definieren Sie ein Speicherarchiv wie in dem folgenden Beispiel gezeigt als ein VTL für den Server:

  ```
  define library chester libtype=vtl
  ```

  Damit wird das neue VTL-Speicherarchiv konfiguriert und die Option RELABELSCRATCH aktiviert, damit Datenträgern, die gelöscht und wieder in den Arbeitsstatus versetzt wurden, ein neuer Kennsatz zugeordnet werden kann.

- Ändern Sie ein SCSI-Speicherarchiv in ein VTL. Wenn ein SCSI-Speicherarchiv vorhanden ist, das in ein VTL-Speicherarchiv geändert werden soll, verwenden Sie den Befehl UPDATE LIBRARY, um den Speicherarchivtyp zu ändern:

  ```
  update library calzone libtype=vtl
  ```

  Sie können diesen Befehl nur ausgeben, wenn das Speicherarchiv, das aktualisiert wird, mit dem Parameter LIBTYPE=SCSI definiert ist.

Zugehörige Verweise:
DEFINE LIBRARY (Speicherarchiv definieren)
UPDATE LIBRARY (Speicherarchiv aktualisieren)

Alle Laufwerke und Pfade für ein einzelnes Speicherarchiv definieren

Verwenden Sie den Befehl PERFORM LIBACTION, um ein einzelnes SCSI-Speicherarchiv oder ein einzelnes virtuelles Bandarchiv (VTL) in einem einzigen Schritt zu konfigurieren.

Informationen zu diesem Vorgang

Wenn Sie Ihre Hardwareumgebung konfigurieren oder ändern und eine große Anzahl Laufwerkdefinitionen erstellen oder ändern müssen, kann diese Task durch die Verwendung des Befehls PERFORM LIBACTION erheblich vereinfacht werden. Sie können ein neues Speicherarchiv definieren und dann alle Laufwerke und Pfade zu den Laufwerken definieren. Wenn ein vorhandenes Speicherarchiv gelöscht werden soll, können Sie alle vorhandenen Laufwerke und ihre zugehörigen Pfade auch in einem einzigen Schritt löschen.

Mit dem Parameter PREVIEW können Sie die Ausgabe der Befehle vor ihrer Verarbeitung anzeigen, um die Aktion, die ausgeführt werden soll, zu überprüfen. Wenn Sie ein Speicherarchiv definieren, muss bereits ein Pfad zu dem Speicherarchiv definiert sein, wenn der Parameter PREVIEW angegeben werden soll. Die Parameter PREVIEW und DEVICE können nicht zusammen verwendet werden.

Der Befehl PERFORM LIBACTION kann nur für SCSI- und VTL-Speicherarchive verwendet werden. Wenn Sie Laufwerke und Pfade für ein Speicherarchiv definieren, muss die Option SANDISCOVERY unterstützt werden und aktiviert sein. Das Bandarchiv muss die Zuordnung zwischen Laufwerkseriennummer und Laufwerkadresse zurückgeben können.

Vorgehensweise

Um ein VTL-Speicherarchiv mit dem Namen ODIN zu konfigurieren, führen Sie diese Schritte aus:

1. Definieren Sie das Speicherarchiv.

   ```
   define library odin libtype=vtl
   ```

2. Definieren Sie zwei Laufwerke und die zugehörigen Pfade für Ihr neues Speicherarchiv ODIN.
   AIX-Betriebssysteme

   ```
   perform libaction odin action=define device=/dev/lb3 prefix=dr
   ```

   Der Server gibt dann die folgenden Befehle aus:

   ```
   define path tsmserver odin srct=server destt=library device=/dev/
    lb3 define drive odin dr0
   define path tsmserver dr0 srct=server destt=drive library=odin
    device=/dev/mt1 define drive odin dr1
   define path tsmserver dr1 srct=server destt=drive library=odin
    device=/dev/mt2
   ```

   Linux-Betriebssysteme

   ```
   perform libaction odin action=define device=/dev/tsmscsi/lb3 prefix=dr
   ```

   Der Server gibt dann die folgenden Befehle aus:

   ```
   define path tsmserver odin srct=server destt=library device=/dev/tsmscsi/lb3
    define drive odin dr0
   define path tsmserver dr0 srct=server destt=drive library=odin
    device=/dev/tsmscsi/mt1 define drive odin dr1
   define path tsmserver dr1 srct=server destt=drive library=odin
    device=/dev/tsmscsi/mt2
   ```

   Windows-Betriebssysteme

   ```
   perform libaction odin action=define device=lb0.0.0.2 prefix=dr
   ```

   Der Server gibt dann die folgenden Befehle aus:

   ```
   define path tsmserver odin srct=server destt=library device=lb0.0.0.2
    define drive odin dr0
   define path tsmserver dr0 srct=server destt=drive library=odin
    device=mt0.1.0.2 define drive odin dr1
   define path tsmserver dr1 srct=server destt=drive library=odin
    device=mt0.2.0.2
   ```

Zugehörige Verweise:
DEFINE LIBRARY (Speicherarchiv definieren)
DEFINE PATH (Pfad definieren, wenn Ziel ein Laufwerk ist)
PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Speicherarchiv definieren oder löschen)

Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit einem einzigen Laufwerkeinheitentyp konfigurieren

Konfigurieren Sie ein VTL oder ein SCSI-Speicherarchiv, das zwei LTO-Bandlaufwerke enthält.

Informationen zu diesem Vorgang

Diese Prozedur ist ein Beispiel für die Konfiguration eines automatisierten SCSI-Speicherarchivs, das zwei Laufwerke enthält, für das Serversystem. Das Speicherarchiv wird nicht mit anderen IBM Spectrum Protect-Servern oder Speicheragenten gemeinsam genutzt und ist normalerweise über SCSI-Kabel an das Serversystem angeschlossen.

In dieser Konfiguration haben beide Laufwerke in dem Speicherarchiv denselben Einheitentyp. Definieren Sie exakt eine Einheitenklasse. Die Vorgehensweise ist bis auf den Schritt zum Definieren des Speicherarchivs für SCSI-Speicherarchive und VTLs identisch. Definieren Sie für SCSI-Speicherarchive das Speicherarchiv mit libtype=scsi. Definieren Sie für VTL-Speicherarchive das Speicherarchiv mit libtype=vtl.

Vorgehensweise

1. Definieren Sie ein SCSI-Speicherarchiv mit dem Namen AUTODLTLIB.

   ```
   define library autoltolib libtype=scsi
   ```

   Wenn das Speicherarchiv einen Barcodeleser hat und Bändern automatisch Kennsätze zugeordnet werden sollen, bevor sie zurückgestellt werden, können Sie den Parameter AUTOLABEL auf YES setzen. Beispiel:

   ```
   define library autoltolib libtype=scsi autolabel=yes
   ```

2. Definieren Sie einen Pfad vom Server zum Speicherarchiv.
    AIX-Betriebssysteme

   ```
   define path server1 autoltolib srctype=server desttype=library
   device=/dev/lb3
   ```

    Linux-Betriebssysteme

   ```
   define path server1 autoltolib srctype=server desttype=library
   device=/dev/tsmscsi/lb3
   ```

    Windows-Betriebssysteme

   ```
   define path server1 autoltolib srctype=server desttype=library
   device=lb0.0.0.3
   ```

3. Definieren Sie die Laufwerke im Speicherarchiv. Beide Laufwerke gehören zum Speicherarchiv AUTODLTLIB.

   ```
   define drive autoltolib drive01
   define drive autoltolib drive02
   ```

   Tipp: Mithilfe des Befehls PERFORM LIBACTION können Sie Laufwerke und Pfade für ein Speicherarchiv in einem einzigen Schritt definieren.
4. Definieren Sie einen Pfad vom Server zu jedem Laufwerk.
    AIX-Betriebssysteme

   ```
   define path server1 drive01 srctype=server desttype=drive
   library=autoltolib device=/dev/mt4
   define path server1 drive02 srctype=server desttype=drive
   library=autoltolib device=/dev/mt5
   ```

    Linux-Betriebssysteme

   ```
   define path server1 drive01 srctype=server desttype=drive
   library=autoltolib device=/dev/tsmscsi/mt4
   define path server1 drive02 srctype=server desttype=drive
   library=autoltolib device=/dev/tsmscsi/mt5
   ```

    Windows-Betriebssysteme

   ```
   define path server1 drive01 srctype=server desttype=drive
   library=autoltolib device=mt0.0.0.4
   define path server1 drive02 srctype=server desttype=drive
   library=autoltolib device=mt0.0.0.5
   ```

   Wurde die Elementadresse bei der Definition des Laufwerks nicht angegeben, fragt der Server jetzt das Speicherarchiv nach der Standardelementadresse des Laufwerks ab.

5. Definieren Sie eine Einheitenklasse mit dem Namen AUTODLT_CLASS für die beiden Laufwerke im Speicherarchiv AUTODLTLIB.

   ```
   define devclass autolto_class library=autodltlib devtype=lto
   ```

6. Definieren Sie einen Speicherpool mit dem Namen AUTOLTO_POOL, der der Einheitenklasse mit dem Namen AUTOLTO_CLASS zugeordnet ist.

   ```
   define stgpool autolto_pool autolto_class maxscratch=20
   ```

7. Ordnen Sie Datenträgern im Speicherarchiv Kennsätze zu und stellen Sie die Datenträger zurück.

   ```
   label libvolume autoltolib search=yes labelsource=barcode checkin=scratch
   ```

8. Überprüfen Sie Ihre Definitionen, indem Sie die folgenden Befehle ausgeben:

```
query library
query drive
query path
query devclass
query stgpool
query libvolume
```

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)
DEFINE LIBRARY (Speicherarchiv definieren)
DEFINE PATH (Pfad definieren, wenn Ziel ein Laufwerk ist)

Beispiel: SCSI-Speicherarchiv oder virtuelles Bandarchiv mit mehreren Laufwerkeinheitentypen konfigurieren

Sie können ein Speicherarchiv mit mehreren Laufwerkeinheitentypen konfigurieren, beispielsweise ein StorageTek L40-Speicherarchiv, das ein DLT-Laufwerk und ein LTO Ultrium-Laufwerk enthält.

Informationen zu diesem Vorgang

Diese Prozedur ist ein Beispiel für die Konfiguration eines automatisierten SCSI-Speicherarchivs, das zwei Laufwerke enthält, für das Serversystem. Das Speicherarchiv wird nicht mit anderen IBM Spectrum Protect-Servern oder Speicheragenten gemeinsam genutzt und ist normalerweise über SCSI-Kabel an das Serversystem angeschlossen.

In dieser Konfiguration haben die Laufwerke unterschiedliche Einheitentypen. Definieren Sie für jeden Laufwerkeinheitentyp eine Einheitenklasse. Laufwerke mit verschiedenen Einheitentypen werden in einem einzelnen Speicherarchiv unterstützt, wenn Sie für jeden Laufwerktyp eine Einheitenklasse definieren. Wenn die Konfiguration auf diese Art und Weise erfolgt, müssen Sie das spezifische Format für den Einheitentyp des Laufwerks einschließen, indem Sie den Parameter FORMAT mit einem anderen Wert als DRIVE verwenden.

Die Vorgehensweise ist bis auf den Schritt zum Definieren des Speicherarchivs für SCSI-Speicherarchive und VTLs identisch. Definieren Sie für SCSI-Speicherarchive das Speicherarchiv mit libtype=scsi. Definieren Sie für VTL-Speicherarchive das Speicherarchiv mit libtype=vtl.

Vorgehensweise

1. Definieren Sie ein SCSI-Speicherarchiv mit dem Namen MIXEDLIB.

```
define library mixedlib libtype=scsi
```

2. Definieren Sie einen Pfad vom Server zum Speicherarchiv.
   AIX-Betriebssysteme

```
define path server1 mixedlib srctype=server desttype=library
device=/dev/lb3
```

   Linux-Betriebssysteme

```
define path server1 mixedlib srctype=server desttype=library
device=/dev/tsmscsi/lb3
```

   Windows-Betriebssysteme

```
define path server1 mixedlib srctype=server desttype=library
device=lb0.0.0.3
```

3. Definieren Sie die Laufwerke im Speicherarchiv. Beide Laufwerke gehören zum Speicherarchiv MIXEDLIB.

```
define drive mixedlib dlt1
define drive mixedlib lto1
```

4. Definieren Sie einen Pfad vom Server zu jedem Laufwerk. Der Parameter DEVICE gibt den Namen des Einheitentreibers für das Laufwerk an; dabei handelt es sich um den Gerätedateinamen für die Einheit.
   AIX-Betriebssysteme

```
define path server1 dlt1 srctype=server desttype=drive
library=mixedlib device=/dev/mt4
define path server1 lto1 srctype=server desttype=drive
library=mixedlib device=/dev/mt5
```

   Linux-Betriebssysteme

```
define path server1 dlt1 srctype=server desttype=drive
library=mixedlib device=/dev/tsmscsi/mt4
```

```
define path server1 lto1 srctype=server desttype=drive
library=mixedlib device=/dev/tsmscsi/mt5
```

 Windows-Betriebssysteme

```
define path server1 drive01 srctype=server desttype=drive
library=autoltolib device=mt0.0.0.4
define path server1 drive02 srctype=server desttype=drive
library=autoltolib device=mt0.0.0.5
```

Wurde die Elementadresse bei der Definition des Laufwerks nicht angegeben, fragt der Server jetzt das Speicherarchiv nach der Elementadresse des Laufwerks ab.

5. Definieren Sie Einheitenklassen.
   Wichtig: Verwenden Sie nicht das Standardformat DRIVE. Da die Laufwerke verschiedene Typen haben, verwendet der Server die Formatspezifikation für die Auswahl eines Laufwerks. Das Ergebnis der Verwendung des Formats DRIVE in einem Speicherarchiv mit gemischten Datenträgern ist unvorhersehbar.

   ```
   define devclass dlt_class library=mixedlib devtype=dlt format=dlt40
   define devclass lto_class library=mixedlib devtype=lto format=ultriumc
   ```

6. Definieren Sie Speicherpools, die den Einheitenklassen zugeordnet sind.

   ```
   define stgpool lto_pool lto_class maxscratch=20
   define stgpool dlt_pool dlt_class maxscratch=20
   ```

7. Ordnen Sie Datenträgern im Speicherarchiv Kennsätze zu und stellen Sie die Datenträger zurück.

   ```
   label libvolume mixedlib search=yes labelsource=barcode checkin=scratch
   ```

8. Überprüfen Sie Ihre Definitionen, indem Sie die folgenden Befehle ausgeben:

   ```
   query library
   query drive
   query path
   query devclass
   query stgpool
   query libvolume
   ```

NAS-Dateiserver schützen

Sie können eine Sicherungsumgebung, die einen NAS-Dateiserver schützt, konfigurieren und verwalten.

Sie können den IBM Spectrum Protect-Server, den IBM Spectrum Protect-Client für Sichern/Archivieren oder IBM Spectrum Protect Snapshot wie in der folgenden Tabelle beschrieben zum Sichern und Zurückschreiben eines NAS-Dateiservers verwenden.

Produkt	Beschreibung
IBM Spectrum Protect-Server	Um NAS-Dateiserverdaten mithilfe des IBM Spectrum Protect-Servers sichern und zurückschreiben zu können, muss IBM Spectrum Protect Extended Edition installiert sein. Sie können den IBM Spectrum Protect-Server für die Verwendung von NDMP (Network Data Management Protocol) wie in den folgenden Themen in diesem Abschnitt beschrieben zum Sichern und Zurückschreiben von Daten konfigurieren. Um große NetApp-Dateisysteme zu schützen, können Sie auch stattdessen IBM Spectrum Protect für die Verwendung der NetApp-Funktion 'SnapMirror to Tape' (die auch als SMTape bekannt ist) konfigurieren. 'SnapMirror to Tape' verwendet eine Datenkopie auf Blockebene für die Sicherung, die schneller als eine traditionelle NDMP-Gesamtsicherung ist und verwendet werden kann, wenn NDMP-Gesamtsicherungen nicht geeignet sind. Informationen zur Verwendung der Funktion 'SnapMirror to Tape' zum Sichern und Zurückschreiben von Daten finden Sie in Sicherungs- und Zurückschreibungsoperationen mit der NetApp-Funktion 'SnapMirror to Tape'.
IBM Spectrum Protect-Client für Sichern/Archivieren	Sie können den -Client für Sichern/Archivieren zum Sichern und Zurückschreiben von Dateiserverdaten mithilfe des NFS-Protokolls (NFS = Network File System) oder des CIFS-Protokolls (CIFS = Common Internet File System) konfigurieren. Informationen zur Verwendung des Clients für Sichern/Archivieren zum Sichern und Zurückschreiben von Daten finden Sie in Daten mit Clients für Sichern/Archivieren sichern und zurückschreiben.
IBM Spectrum Protect Snapshot	Sie können IBM Spectrum Protect Snapshot zum Sichern und Zurückschreiben von Dateiserverdaten verwenden, indem Sie die erweiterten Momentaufnahmetechnologien der Speichersysteme verwenden. Informationen zur Verwendung von IBM Spectrum Protect Snapshot zum Sichern und Zurückschreiben von Daten finden Sie in Übersicht über IBM Spectrum Protect Snapshot for UNIX and Linux oder Übersicht über IBM Spectrum Protect Snapshot for VMware.

- NDMP-Anforderungen
  Um NDMP für Operationen mit NAS-Dateiservern verwenden zu können, muss IBM Spectrum Protect Extended Edition installiert sein und Ihre Dateiserverumgebung muss bestimmte Voraussetzungen erfüllen.
- Verwaltung von NDMP-Operationen
  Es gibt mehrere Administratoraktivitäten für NDMP-Operationen.
- IBM Spectrum Protect für NDMP-Operationen konfigurieren
  Sie können IBM Spectrum Protect zum Sichern und Wiederherstellen von Daten auf NAS-Dateiservern mithilfe von NDMP konfigurieren. Die Konfigurationsprozedur ist abhängig davon, ob Daten von einem NAS-Dateiserver ohne oder mit Clustering gesichert werden sollen, unterschiedlich.
- NAS-Dateiserver mithilfe von NDMP sichern und zurückschreiben
  Nach der Konfiguration von IBM Spectrum Protect für NDMP-Operationen können Sie mit der Verwendung von NDMP beginnen.
- Sicherung und Zurückschreibung auf Dateiebene für NDMP-Operationen
  Wenn Sie Daten mit NDMP sichern, können Sie angeben, dass der IBM Spectrum Protect-Server Informationen auf Dateiebene erfasst und in einem Inhaltsverzeichnis (TOC) speichert.
- Sicherungs- und Zurückschreibungsoperationen auf Verzeichnisebene
  Wenn Sie über ein großes NAS-Dateisystem verfügen, werden durch das Einleiten einer Sicherung auf Verzeichnisebene Sicherungs- und Zurückschreibungszeiten reduziert und größere Flexibilität beim Konfigurieren von NAS-Sicherungen bereitgestellt. Durch das Definieren virtueller Dateibereiche kann eine Dateisystemsicherung auf mehrere NDMP-Sicherungsoperationen und auf mehrere Bandlaufwerke verteilt werden. Sie können auch verschiedene Sicherungszeitpläne verwenden, um Unterverzeichnisstrukturen eines Dateisystems zu sichern.
- Sicherungs- und Zurückschreibungsoperationen mit der NetApp-Funktion 'SnapMirror to Tape'
  Sie können große NetApp-Dateisysteme mithilfe der NetApp-Funktion 'SnapMirror to Tape' (die auch als 'SMTape' bekannt ist) sichern. Durch die Verwendung einer Datenkopie auf Blockebene für die Sicherung ist die Methode 'SnapMirror to Tape' schneller als eine traditionelle NDMP-Gesamtsicherung und kann verwendet werden, wenn NDMP-Gesamtsicherungen nicht geeignet sind.
- NDMP-Sicherungsoperationen mithilfe von in Celerra-Dateiserver integrierten Prüfpunkten
  Wenn der IBM Spectrum Protect-Server eine NDMP-Sicherungsoperation auf einer Celerra-Einheit zum Versetzen von Daten einleitet, kann die Sicherung eines umfangreichen Dateisystems mehrere Stunden dauern. Ohne integrierte Celerra-Prüfpunkte werden alle auf dem Dateisystem vorgenommenen Änderungen in das Sicherungsimage geschrieben.
- NAS-Knoten replizieren
  Sie können einen NAS-Knoten, der NDMP für Sicherungsoperationen verwendet, replizieren. Machen Sie sich, bevor Sie die Replikationsoperation konfigurieren, mit den geltenden Einschränkungen vertraut.

NDMP-Anforderungen

Um NDMP für Operationen mit NAS-Dateiservern verwenden zu können, muss IBM Spectrum Protect Extended Edition installiert sein und Ihre Dateiserverumgebung muss bestimmte Voraussetzungen erfüllen.

NAS-Dateiserver
: Das Betriebssystem auf dem Dateiserver muss von IBM Spectrum Protect unterstützt werden. Informationen zu den unterstützten NAS-Dateiservern finden Sie in Technote 1054144.

  Die Kombination aus Dateiservermodell und Betriebssystem muss vom NAS-Dateiserver unterstützt werden. Weitere Spezifikationen enthält die Produktinformation für den NAS-Dateiserver.

Bandarchive
: Diese Anforderung gilt nur für eine Sicherung auf einer lokal angeschlossenen NAS-Einheit. Der IBM Spectrum Protect-Server unterstützt die folgenden Speicherarchivtypen für NDMP-Operationen:

  SCSI
  : Ein SCSI-Speicherarchiv kann direkt an den IBM Spectrum Protect-Server oder an den NAS-Dateiserver angeschlossen werden. Wenn das Speicherarchiv direkt an den IBM Spectrum Protect-Server angeschlossen wird, steuert dieser Server die Speicherarchivoperationen, indem die SCSI-Befehle direkt an das Speicherarchiv übergeben werden. Wenn das Speicherarchiv direkt an den NAS-Dateiserver angeschlossen wird, steuert der IBM Spectrum Protect-Server das Speicherarchiv, indem SCSI-Befehle über den NAS-Dateiserver an das Speicherarchiv übergeben werden.

  ACSLS
  : Ein ACSLS-Speicherarchiv kann direkt an den IBM Spectrum Protect-Server angeschlossen werden. Der IBM Spectrum Protect-Server steuert das Speicherarchiv, indem die Speicherarchivanforderung über TCP/IP an den Speicherarchivsteuerungsserver übergeben wird.
    Einschränkung: Der IBM Spectrum Protect-Server verfügt nicht über Unterstützung für externe Speicherarchive für das ACSLS-Speicherarchiv, wenn das Speicherarchiv für NDMP-Operationen verwendet wird.

  VTL
  : Ein virtuelles Bandarchiv (VTL) kann direkt an den IBM Spectrum Protect-Server oder an den NAS-Dateiserver angeschlossen werden. Ein virtuelles Bandarchiv ist im Grunde ein SCSI-Speicherarchiv, das aber gemäß den Merkmalen virtueller Bandarchive funktional erweitert wurde und eine bessere Mountleistung ermöglicht.
    Wenn Sie ein VTL definieren, darf Ihre Umgebung keine gemischten Datenträger umfassen. Pfade müssen zwischen allen Laufwerken in dem Speicherarchiv und allen definierten Servern, einschließlich Speicheragenten, die das Speicherarchiv verwenden, definiert sein. Wenn diese Bedingungen nicht erfüllt sind, kann sich die Gesamtleistung insbesondere während Zeiten mit hoher Belastung auf dieselbe Leistungsstufen wie bei Speicherarchiven des Typs SCSI verschlechtern.

  349X

Ein 349X-Speicherarchiv kann direkt nur an den IBM Spectrum Protect-Server angeschlossen werden. Der IBM Spectrum Protect-Server steuert das Speicherarchiv, indem die Speicherarchivanforderung über TCP/IP an den Speicherarchivmanager übergeben wird.

Gemeinsame Speicherarchivnutzung: Bei dem IBM Spectrum Protect-Server, der NDMP-Operationen ausführt, kann es sich um einen Speicherarchivmanager für ein ACSLS-, SCSI-, VTL- oder 349X-Speicherarchiv handeln, jedoch nicht um einen Speicherarchivclient. Der IBM Spectrum Protect-Server kann auch ein Speicherarchivclient sein; dies ist in einer Konfiguration der Fall, bei der der NAS-Dateiserver Daten unter Verwendung von TCP/IP an den Server und nicht an ein Bandarchiv sendet, das an den Dateiserver angeschlossen ist. Wenn der IBM Spectrum Protect-Server, der NDMP-Operationen ausführt, ein Speicherarchivmanager ist, muss dieser Server das Speicherarchiv direkt steuern und nicht durch die Übergabe von Befehlen über den NAS-Dateiserver.

Bandlaufwerke

Ein Bandlaufwerk ist nur für die Sicherung auf einer lokal angeschlossenen NAS-Einheit erforderlich. Der NAS-Dateiserver muss Zugriff auf die Laufwerke haben. Eine NAS-Einheit wird in einem Speicherarchiv mit gemischten Einheiten nicht unterstützt. Bei den Laufwerken muss Unterstützung für Bandsicherungsoperationen durch den NAS-Dateiserver und das dazugehörige Betriebssystem vorliegen. Die Produktdokumentation zum NAS-Dateiserver enthält ausführliche Informationen zur NDMP-Einheitenunterstützung.
Gemeinsame Laufwerknutzung: Die Bandlaufwerke können vom IBM Spectrum Protect-Server und einem oder mehreren NAS-Dateiservern gemeinsam genutzt werden. Wenn ein SCSI-, VTL- oder 349X-Speicherarchiv an den Server und nicht an den NAS-Dateiserver angeschlossen ist, können außerdem die Laufwerke mit einem oder mehreren NAS-Dateiservern gemeinsam genutzt werden. Die Laufwerke können auch von einem oder mehreren IBM Spectrum Protect-Speicherarchivclients und Speicheragenten gemeinsam genutzt werden.
Laufwerkreservierungen: Wenn Bandlaufwerke an NAS-Einheiten angeschlossen sind und der Parameter RESETDRIVES=YES für den Befehl DEFINE LIBRARY angegeben ist gelten die folgenden Einschränkungen:

- Wenn ein Bandlaufwerk von einem IBM Spectrum Protect-Server und einer NAS-Einheit gemeinsam genutzt wird, wird die Zurückstellung der Laufwerkreservierung unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve enthält die Dokumentation zu Ihrer NAS-Einheit.
- Wenn ein Bandlaufwerk nur an eine NAS-Einheit angeschlossen ist und nicht mit einem IBM Spectrum Protect-Server gemeinsam genutzt wird, wird die Zurückstellung der Laufwerkreservierung nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung durch die NAS-Einheit definiert, aber nie gelöscht wird, müssen Sie eine andere Methode zum Löschen der Reservierung verwenden.

Klären Sie die Kompatibilität bestimmter Kombinationen aus NAS-Dateiserver, Bandeinheiten und an ein SAN angeschlossener Einheiten mit dem Hersteller der Hardware ab.
Tipp: IBM Spectrum Protect unterstützt NDMP Version 4 für alle NDMP-Operationen. IBM Spectrum Protect unterstützt weiterhin alle NDMP-Sicherungs- und -Zurückschreibungsoperationen mit einer NAS-Einheit, auf der NDMP Version 3 ausgeführt wird. Der IBM Spectrum Protect-Server vereinbart mit dem NDMP-Server die höchste Protokollversion (entweder Version 3 oder Version 4), wenn er eine NDMP-Verbindung aufbaut. Treten bei Verwendung von Version 4 Probleme auf, können Sie versuchsweise Version 3 verwenden.

- Schnittstellen für NDMP-Operationen
  Sie können verschiedene Schnittstellen zur Ausführung von NDMP-Operationen verwenden. Sie können eine NDMP-Operation mit dem Befehl BACKUP NODE oder RESTORE NODE planen und einen Zeitplan für die Verarbeitung des Befehls erstellen.
- Datenformate für NDMP-Sicherungsoperationen
  Daten, die mithilfe von NDMP gesichert werden, haben nicht dasselbe Format wie die Daten, die für typische IBM Spectrum Protect-Sicherungsoperationen verwendet werden. Der NAS-Dateiserver steuert das Format der Sicherungsdaten.

Schnittstellen für NDMP-Operationen

Sie können verschiedene Schnittstellen zur Ausführung von NDMP-Operationen verwenden. Sie können eine NDMP-Operation mit dem Befehl BACKUP NODE oder RESTORE NODE planen und einen Zeitplan für die Verarbeitung des Befehls erstellen.

Clientschnittstellen:

- Befehlszeilenclient für Sichern/Archivieren (auf einem Windows, AIX (64-Bit) oder Oracle Solaris-System (64-Bit))
- Web-Client

Serverschnittstellen:

- Serverkonsole
- Befehlszeile auf dem Verwaltungsclient
  Tipp: Alle Beispiele für NDMP-Operationen verwenden Serverbefehle.

Bei der IBM Spectrum Protect-Web-Client-Schnittstelle, die mit dem Client für Sichern/Archivieren verfügbar ist, werden die Dateisysteme des NAS-Dateiservers in einer grafischen Sicht angezeigt. Die Clientfunktion ist nicht erforderlich, aber die Clientschnittstellen können für NDMP-Operationen verwendet werden. Die Clientfunktion ist die bevorzugte Methode für Zurückschreibungsoperationen auf Dateiebene. Weitere Informationen zu Zurückschreibungsoperationen auf Dateiebene finden Sie in Sicherung und Zurückschreibung auf Dateiebene für NDMP-Operationen.

IBM Spectrum Protect fordert Sie zur Eingabe einer Administrator-ID und des zugehörigen Kennworts auf, wenn Sie NDMP-Funktionen mit einer der Clientschnittstellen ausführen. Weitere Informationen zum Installieren und Aktivieren von Clientschnittstellen finden Sie in IBM Spectrum Protect-Clients für Sichern/Archivieren installieren.

Um den IBM Spectrum Protect-Client für Sichern/Archivieren oder den Web-Client für NAS-Operationen verwenden zu können, muss das erste Zeichen der Dateisystemnamen auf der NAS-Einheit ein Schrägstrich (/) sein. Diese Einschränkung hat keine Auswirkungen auf NAS-Operationen, die über die IBM Spectrum Protect-Serverbefehlszeile gestartet werden.

Datenformate für NDMP-Sicherungsoperationen

Daten, die mithilfe von NDMP gesichert werden, haben nicht dasselbe Format wie die Daten, die für typische IBM Spectrum Protect-Sicherungsoperationen verwendet werden. Der NAS-Dateiserver steuert das Format der Sicherungsdaten.

Daten, die in einem Speicherarchiv gesichert werden, das direkt an den Dateiserver angeschlossen ist, müssen in einen Speicherpool mit dem korrekten Datenformat übertragen werden. Wenn Sie einen Speicherpool für NDMP-Operationen definieren, geben Sie eines der folgenden Datenformate an:

- NETAPPDUMP, wenn der NAS-Dateiserver eine NetApp-Einheit oder eine IBM® System Storage N Series-Einheit ist
- CELERRADUMP, wenn der NAS-Dateiserver eine EMC Celerra-Einheit ist
- NDMPDUMP für alle anderen Einheiten

Daten, die über das Netz in der lokalen IBM Spectrum Protect-Hierarchie gesichert werden, können an jeden beliebigen primären Speicherpool mit wahlfreiem oder sequenziellem Zugriff übertragen werden. Das Format der Daten ändert sich jedoch nicht.

Verwaltung von NDMP-Operationen

Es gibt mehrere Administratoraktivitäten für NDMP-Operationen.

- NAS-Dateiserverknoten verwalten
  Sie können NAS-Dateiserverknoten abfragen, aktualisieren, umbenennen und entfernen.
- In NDMP-Operationen verwendete Einheiten zum Versetzen von Daten verwalten
  Sie können die für NAS-Dateiserver definierten Einheiten zum Versetzen von Daten abfragen, aktualisieren und löschen.
- IBM Spectrum Protect-Laufwerk für NDMP-Operationen dedizieren
  Wenn Sie bereits ein Laufwerk für IBM Spectrum Protect-Operationen verwenden, können Sie dieses Laufwerk für NDMP-Operationen dedizieren.
- Speicherpoolverwaltung für NDMP-Operationen
  Wenn NETAPPDUMP, CELERRADUMP oder NDMPDUMP als Speicherpooltyp angegeben wird, unterscheidet sich die Verwaltung von Speicherpools, die von NDMP-Operationen erstellt werden, von der Verwaltung von Speicherpools, die Datenträger für traditionelle IBM Spectrum Protect-Sicherungen enthalten.
- Inhaltsverzeichnisse verwalten
  Sie können mehrere Befehle für die Verwaltung unterschiedlicher Aspekte Ihres Dateninhalts verwenden.
- Schließen inaktiver NDMP-Verbindungen mit langer Laufzeit verhindern
  Um zu verhindern, dass Firewalls inaktive NDMP-Verbindungen mit langer Laufzeit schließen, können Sie den TCP-Keepalive-Mechanismus auf den NDMP-Steuerverbindungen aktivieren.

NAS-Dateiserverknoten verwalten

Sie können NAS-Dateiserverknoten abfragen, aktualisieren, umbenennen und entfernen.

Vorgehensweise

Verwenden Sie einen der folgenden Befehle, um NAS-Dateiserverknoten zu verwalten:

Befehl	Prozedur
QUERY NODE	Um einen Knoten abzufragen, geben Sie den Befehl QUERY NODE mit den entsprechenden Parametern aus. Wenn beispielsweise der NAS-Knoten NASNODE1 abgefragt werden soll, geben Sie den folgenden Befehl aus: `query node nasnode1 type=nas`
UPDATE NODE	Um einen Knoten zu aktualisieren, geben Sie den Befehl UPDATE NODE mit den entsprechenden Parametern aus. Wenn Sie beispielsweise eine neue Maßnahmendomäne mit dem Namen NASDOMAIN für NAS-Knoten erstellt haben und der Knoten NASNODE1 aktualisiert werden soll, um ihn in die neue Domäne einzuschließen, geben Sie den folgenden Befehl aus: `update node nasnode1 domain=nasdomain`

Befehl	Prozedur
RENAME NODE	Zum Umbenennen eines NAS-Knotens müssen Sie auch die zugehörige NAS-Einheit zum Versetzen von Daten umbenennen, da beide denselben Namen haben müssen. Um beispielsweise NASNODE1 in NAS1 umzubenennen, führen Sie die folgenden Schritte aus: 1. Löschen Sie alle Pfade zwischen der Einheit NASNODE1 zum Versetzen von Daten und den Speicherarchiven sowie zwischen der Einheit NASNODE1 zum Versetzen von Daten und den Laufwerken. 2. Löschen Sie die für den NAS-Knoten definierte Einheit zum Versetzen von Daten. 3. Geben Sie folgenden Befehl aus, um NASNODE1 in NAS1 umzubenennen: `rename node nasnode1 nas1` 4. Definieren Sie die Einheit zum Versetzen von Daten unter Verwendung des neuen Knotennamens. In diesem Beispiel müssen Sie eine neue Einheit zum Versetzen von Daten mit dem Namen NAS1 mit denselben Parametern definieren, die beim Definieren von NASNODE1 verwendet wurden. Wichtig: Wenn Sie eine neue Einheit zum Versetzen von Daten für einen umbenannten Knoten definieren, stellen Sie sicher, dass der Name der Einheit zum Versetzen von Daten mit dem neuen Knotennamen übereinstimmt. Stellen Sie außerdem sicher, dass die Parameter für die neue Einheit zum Versetzen von Daten mit den Parametern der ursprünglichen Einheit zum Versetzen von Daten identisch sind. Wenn der Knotenname nicht mit dem Namen der Einheit zum Versetzen von Daten übereinstimmt bzw. die Parameter der neuen Einheit zum Versetzen von Daten nicht identisch mit den Parametern der ursprünglichen Einheit zum Versetzen von Daten sind, kann unter Umständen keine Sitzung mit dem NAS-Dateiserver aufgebaut werden. 5. Definieren Sie für SCSI- oder 349X-Speicherarchive nur dann einen Pfad zwischen der NAS-Einheit zum Versetzen von Daten und einem Speicherarchiv, wenn das Bandarchiv physisch über eine Direktverbindung mit dem NAS-Dateiserver verbunden ist. 6. Definieren Sie Pfade zwischen der NAS-Einheit zum Versetzen von Daten und allen Laufwerken, die für NDMP-Operationen verwendet werden.
REMOVE NODE	Um einen Knoten zu entfernen, führen Sie die folgenden Schritte aus: 1. Löschen Sie alle Definitionen des virtuellen Dateibereichs für den Knoten. 2. Löschen Sie alle Pfade zwischen der Einheit zum Versetzen von Daten und den Speicherarchiven sowie zwischen der Einheit zum Versetzen von Daten und den Laufwerken. 3. Löschen Sie den Knoten. Wenn beispielsweise ein Knoten mit dem Namen NAS1 entfernt werden soll, geben Sie den folgenden Befehl aus: `remove node nas1`

Zugehörige Verweise:
QUERY NODE (Knoten abfragen)
UPDATE NODE (Knotenattribute aktualisieren)
RENAME NODE (Knoten umbenennen)
REMOVE NODE (Knoten oder zugeordneten Maschinenknoten löschen)

In NDMP-Operationen verwendete Einheiten zum Versetzen von Daten verwalten

Sie können die für NAS-Dateiserver definierten Einheiten zum Versetzen von Daten abfragen, aktualisieren und löschen.

Vorgehensweise

Verwenden Sie einen der folgenden Befehle, um Einheiten zum Versetzen von Daten zu verwalten:

Befehl	Prozedur
QUERY DATAMOVER	Um eine Einheit zum Versetzen von Daten abzufragen, geben Sie den Befehl QUERY DATAMOVER mit den entsprechenden Parametern aus. Wenn beispielsweise die Einheit zum Versetzen von Daten mit dem Namen NASNODE1 abgefragt werden soll, geben Sie den folgenden Befehl aus: `query datamover nasnode1`
UPDATE DATAMOVER	Um eine Einheit zum Versetzen von Daten zu aktualisieren, geben Sie den Befehl UPDATE DATAMOVER mit den entsprechenden Parametern aus. Wenn Sie beispielsweise einen NAS-Dateiserver zu Wartungszwecken herunterfahren und die Einheit zum Versetzen von Daten in den Offlinestatus versetzt werden soll, geben Sie den folgenden Befehl aus: `update datamover nasnode1 online=no`
DELETE DATAMOVER	Um eine Einheit zum Versetzen von Daten zu löschen, geben Sie den Befehl DELETE DATAMOVER aus. Wenn beispielsweise die Einheit zum Versetzen von Daten mit dem Namen NASNODE1 gelöscht werden soll, geben Sie den folgenden Befehl aus: `delete datamover nasnode1` Einschränkung: Wenn die Einheit zum Versetzen von Daten über einen Pfad zu einem Speicherarchiv verfügt und die Einheit zum Versetzen von Daten gelöscht bzw. in den Offlinestatus versetzt wird, inaktivieren Sie damit den Zugriff auf das Speicherarchiv.

Zugehörige Verweise:
QUERY DATAMOVER (Definitionen für Einheiten zum Versetzen von Daten anzeigen)
UPDATE DATAMOVER (Einheit zum Versetzen von Daten aktualisieren)
DELETE DATAMOVER (Einheit zum Versetzen von Daten löschen)

IBM Spectrum Protect-Laufwerk für NDMP-Operationen dedizieren

Wenn Sie bereits ein Laufwerk für IBM Spectrum Protect-Operationen verwenden, können Sie dieses Laufwerk für NDMP-Operationen dedizieren.

Vorgehensweise

Entfernen Sie den IBM Spectrum Protect-Serverzugriff, indem Sie die Pfaddefinition löschen. Wenn beispielsweise der Servername SERVER1 und der Laufwerkname NASDRIVE1 lautet, geben Sie den folgenden Befehl aus:

```
delete path server1 nasdrive1 srctype=server desttype=drive library=naslib
```

Speicherpoolverwaltung für NDMP-Operationen

Wenn NETAPPDUMP, CELERRADUMP oder NDMPDUMP als Speicherpooltyp angegeben wird, unterscheidet sich die Verwaltung von Speicherpools, die von NDMP-Operationen erstellt werden, von der Verwaltung von Speicherpools, die Datenträger für traditionelle IBM Spectrum Protect-Sicherungen enthalten.

Für Speicherpools des Typs NETAPPDUMP, CELERRADUMP und NDMPDUMP, die von NDMP-Operationen erstellt werden, gelten die folgenden Richtlinien und Einschränkungen:

- Sie können Speicherpools abfragen und aktualisieren, der Parameter DATAFORMAT kann jedoch nicht aktualisiert werden.
- Sie können keinen CENTERA-Speicherpool, Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool als Zielpool von NDMP-Operationen angeben.
- Unterschiedliche Speicherpools für Daten verschiedener NAS-Anbieter zu verwalten ist selbst dann das bevorzugte Verfahren, wenn beide das Datenformat NDMPDUMP haben.
- Die folgenden Parameter der Befehle DEFINE STGPOOL und UPDATE STGPOOL werden ignoriert, da Speicherpoolhierarchien, Konsolidierung und Umlagerung für diese Speicherpools nicht unterstützt werden:
  - MAXSIZE
  - NEXTSTGPOOL
  - LOWMIG
  - HIGHMIG
  - MIGDELAY
  - MIGCONTINUE

- RECLAIMSTGPOOL
- OVFLOCATION

Wichtig: Stellen Sie sicher, dass Sie Speicherpools, die für NDMP-Operationen definiert wurden, nicht versehentlich für traditionelle IBM Spectrum Protect-Operationen verwenden. Gehen Sie mit besonderer Sorgfalt vor, wenn Sie den Speicherpoolnamen als Wert für den Parameter DESTINATION im Befehl DEFINE COPYGROUP zuordnen. Wenn der Zielspeicherpool nicht das geeignete Datenformat aufweist, schlägt die Sicherung fehl.

Inhaltsverzeichnisse verwalten

Sie können mehrere Befehle für die Verwaltung unterschiedlicher Aspekte Ihres Dateninhalts verwenden.

Informationen zu diesem Vorgang

Mit dem Befehl SET TOCLOADRETENTION können Sie angeben, wie lange ungefähr (in Minuten) ein Inhaltsverzeichnis, auf das nicht verwiesen wird, in der IBM Spectrum Protect-Datenbank geladen bleibt. Der serverweite Wert für den Aufbewahrungszeitraum von Inhaltsverzeichnissen (TOC) in IBM Spectrum Protect legt fest, wie lange ein geladenes Inhaltsverzeichnis nach dem letzten Zugriff auf Informationen in dem Inhaltsverzeichnis in der Datenbank aufbewahrt wird.

Da die Inhaltsverzeichnisinformationen in temporäre Datenbanktabellen geladen werden, gehen diese Informationen verloren, wenn der Server angehalten wird, auch wenn der Aufbewahrungszeitraum für das Inhaltsverzeichnis noch nicht abgelaufen ist. Bei der Installation wird für den Aufbewahrungszeitraum der Wert 120 Minuten definiert. Sie können den Aufbewahrungszeitraum für das Inhaltsverzeichnis mit dem Befehl QUERY STATUS anzeigen.

Geben Sie den Befehl QUERY NASBACKUP aus, um Informationen zu den Dateisystemimageobjekten anzuzeigen, die für einen bestimmten NAS-Knoten und -Dateibereich gesichert wurden. Wenn Sie den Befehl ausgeben, wird eine Anzeige aller von NDMP generierten Sicherungsimages mit der Angabe, ob jedes Image über ein entsprechendes Inhaltsverzeichnis (TOC) verfügt, aufgerufen.
Tipp: Der IBM Spectrum Protect-Server kann zusätzlich zu der von Ihnen angegebenen Anzahl Versionen eine Gesamtsicherung speichern, wenn diese Gesamtsicherung über abhängige Differenzsicherungen verfügt. NAS-Gesamtsicherungen mit abhängigen Differenzsicherungen verhalten sich wie andere Basisdateien mit abhängigen Subdateien. Aufgrund des Aufbewahrungszeitraums, der in der Einstellung RETEXTRA angegeben ist, wird die NAS-Gesamtsicherung nicht als verfallen definiert und die Version wird in der Ausgabe eines Befehls QUERY NASBACKUP angezeigt. Informationen zum Definieren von Datenaufbewahrungsmaßnahmen finden Sie in Maßnahmen anpassen.

Zeigen Sie mit dem Befehl QUERY TOC Dateien und Verzeichnisse in einem mit NDMP generierten Sicherungsimage an. Durch Ausgabe des Serverbefehls QUERY TOC können Sie alle Verzeichnisse und Dateien in einem einzelnen angegebenen Inhaltsverzeichnis (TOC) anzeigen. Auf das angegebene Inhaltsverzeichnis wird bei jeder Ausgabe des Befehls QUERY TOC in einem Speicherpool zugegriffen, da dieser Befehl keine Inhaltsverzeichnisinformationen in die IBM Spectrum Protect-Datenbank lädt. Verwenden Sie dann den Befehl RESTORE NODE mit dem Parameter FILELIST, um einzelne Dateien zurückzuschreiben.

Schließen inaktiver NDMP-Verbindungen mit langer Laufzeit verhindern

Um zu verhindern, dass Firewalls inaktive NDMP-Verbindungen mit langer Laufzeit schließen, können Sie den TCP-Keepalive-Mechanismus auf den NDMP-Steuerverbindungen aktivieren.

Informationen zu diesem Vorgang

Der IBM Spectrum Protect-Server baut Steuerverbindungen zu NAS-Einheiten während NDMP-Sicherungs- oder -Zurückschreibungsoperationen auf. Es kann vorkommen, dass diese Steuerverbindungen für längere Zeit offen und inaktiv bleiben. Angenommen, zwei NDMP-Operationen werden für dieselbe NAS-Einheit gestartet. Die Steuerverbindung für eine NDMP-Operation kann offen, aber inaktiv bleiben, wenn die Operation eine Ressource erfordert, beispielsweise ein Bandlaufwerk oder einen sequenziellen Datenträger, der von der anderen NDMP-Operation verwendet wird.

Bestimmte Firewall-Software ist so konfiguriert, dass Netzverbindungen, die für eine bestimmte Dauer inaktiv sind, automatisch geschlossen werden. Wenn zwischen einem IBM Spectrum Protect-Server und einer NAS-Einheit eine Firewall vorhanden ist, kann es vorkommen, dass die Firewall NDMP-Steuerverbindungen wider Erwarten schließt und das Fehlschlagen der NDMP-Operation verursacht.

Der IBM Spectrum Protect-Server stellt einen Mechanismus, den TCP-Keepalive-Mechanismus, bereit, den Sie aktivieren können, um das Schließen inaktiver Verbindungen mit langer Laufzeit zu verhindern. Wenn der TCP-Keepalive-Mechanismus aktiviert ist, werden kleine Pakete in vordefinierten Intervallen über das Netz an den Verbindungspartner gesendet.

Einschränkung: Um Fehler zu vermeiden, dürfen Sie den TCP-Keepalive-Mechanismus in bestimmten Typen von Umgebungen nicht aktivieren. Ein Beispiel sind Umgebungen, die über keine Firewalls zwischen dem IBM Spectrum Protect-Server und einer NAS-Einheit verfügen. Ein anderes Beispiel sind Umgebungen mit Firewalls, die inaktive Verbindungen mit langer Laufzeit tolerieren. Das Aktivieren des TCP-Keepalive-Mechanismus in diesen Typen von Umgebungen kann zur Folge haben, dass eine inaktive Verbindung versehentlich geschlossen wird, wenn der Verbindungspartner vorübergehend nicht auf TCP-Keepalive-Pakete antwortet.

- TCP-Keepalive-Mechanismus aktivieren
  Um den TCP-Keepalive-Mechanismus, der verhindert, dass NDMP-Verbindungen geschlossen werden, zu aktivieren, verwenden Sie die Serveroption NDMPENABLEKEEPALIVE.

- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeInaktivitätsdauer für Verbindungen für den TCP-Keepalive-Mechanismus angeben
  Um die Inaktivitätsdauer für Verbindungen (in Minuten) anzugeben, bevor das erste TCP-Keepalive-Paket gesendet wird, verwenden Sie die Serveroption NDMPKEEPIDLEMINUTES.

TCP-Keepalive-Mechanismus aktivieren

Um den TCP-Keepalive-Mechanismus, der verhindert, dass NDMP-Verbindungen geschlossen werden, zu aktivieren, verwenden Sie die Serveroption NDMPENABLEKEEPALIVE.

Vorgehensweise

Fügen Sie die Option der Serveroptionsdatei dsmserv.opt hinzu:

```
ndmpenablekeepalive yes
```

Zugehörige Verweise:
NDMPENABLEKEEPALIVE
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Inaktivitätsdauer für Verbindungen für den TCP-Keepalive-Mechanismus angeben

Um die Inaktivitätsdauer für Verbindungen (in Minuten) anzugeben, bevor das erste TCP-Keepalive-Paket gesendet wird, verwenden Sie die Serveroption NDMPKEEPIDLEMINUTES.

Vorgehensweise

Fügen Sie die Option der Serveroptionsdatei dsmserv.opt hinzu:

```
ndmpkeepidleminutes Minuten
```

Zugehörige Verweise:
NDMPKEEPIDLEMINUTES

IBM Spectrum Protect für NDMP-Operationen konfigurieren

Sie können IBM Spectrum Protect zum Sichern und Wiederherstellen von Daten auf NAS-Dateiservern mithilfe von NDMP konfigurieren. Die Konfigurationsprozedur ist abhängig davon, ob Daten von einem NAS-Dateiserver ohne oder mit Clustering gesichert werden sollen, unterschiedlich.

- IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren
  Bevor Sie IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren, müssen Sie die erforderliche Lizenz registrieren.
- IBM Spectrum Protect für NDMP-Operationen in einer NetApp-Clusterumgebung konfigurieren
  Sie können Daten von einem NetApp-Cluster auf einer direkt angeschlossenen Bandeinheit oder einem IBM Spectrum Protect-Server sichern, der die Daten in einem Speicherpool speichert. Sie können den gesamten Cluster auf einem einzigen IBM Spectrum Protect-Knoten oder Teile des Clusters auf mehreren Knoten sichern.

IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren

Bevor Sie IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren, müssen Sie die erforderliche Lizenz registrieren.

Vorgehensweise

1. Definieren Sie das Bandarchiv und Datenträger. Siehe Bandarchiv für NDMP-Operationen konfigurieren; dort werden die folgenden Schritte ausführlicher erläutert.
   a. Schließen Sie das SCSI-Bandarchiv oder das virtuelle Bandarchiv (VTL = Virtual Tape Library) an den NAS-Dateiserver oder an den IBM Spectrum Protect-Server an oder schließen Sie das ACSLS-Speicherarchiv oder das 349X-Speicherarchiv an den IBM Spectrum Protect-Server an.
   b. Definieren Sie das Speicherarchiv mit dem Speicherarchivtyp SCSI, VTL, ACSLS oder 349X.
   c. Definieren Sie eine Einheitenklasse für die Bandlaufwerke.
   d. Definieren Sie einen Speicherpool für NAS-Sicherungsdatenträger.

e. Optional: Definieren Sie einen Speicherpool für die Speicherung eines Inhaltsverzeichnisses.

2. Konfigurieren Sie eine IBM Spectrum Protect-Maßnahme für die Verwaltung von NAS-Imagesicherungen. Siehe IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren.
3. Registrieren Sie einen NAS-Dateiserverknoten beim IBM Spectrum Protect-Server. Siehe NAS-Knoten im IBM Spectrum Protect-Server registrieren.
4. Definieren Sie eine Einheit zum Versetzen von Daten für den NAS-Dateiserver. Siehe Einheit zum Versetzen von Daten für einen NAS-Dateiserver definieren.
5. Einen Pfad vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver zum Bandarchiv definieren. Siehe Pfade zu Speicherarchiven für NDMP-Operationen definieren.
6. Bandlaufwerke für IBM Spectrum Protect definieren und Pfade zu den betreffenden Laufwerken vom NAS-Dateiserver und optional vom IBM Spectrum Protect-Server aus definieren. Siehe Pfade für NDMP-Operationen definieren.
7. Stellen Sie Bänder in das Speicherarchiv und ordnen Sie den Bändern Kennsätze zu.

    AIX-Betriebssysteme  Linux-BetriebssystemeBanddatenträgern müssen Kennsätze zugeordnet werden, bevor sie vom Server verwendet werden können. Dazu können Sie den Befehl LABEL LIBVOLUME verwenden oder die Befehle DEFINE LIBRARY und UPDATE LIBRARY unter Angabe des Parameters AUTOLABEL.

    Windows-BetriebssystemeAllen Datenträgern müssen Kennsätze zugeordnet werden. Um Datenträgern bei einem automatisierten Speicherarchiv Kennsätze zuzuordnen, müssen Sie die Datenträger in das Speicherarchiv zurückstellen. Um Datenträgern mit dem Befehl LABEL LIBVOLUME Kennsätze zuzuordnen, geben Sie den Parameter CHECKIN an. Um Banddatenträgern in SCSI-Speicherarchiven automatisch Kennsätze zuzuordnen, verwenden Sie den Parameter AUTOLABEL in den Befehlen DEFINE LIBRARY und UPDATE LIBRARY.

   Anweisungen finden Sie in den Beschreibungen der Befehle LABEL LIBVOLUME, DEFINE LIBRARY und UPDATE LIBRARY.

8. Optional: Definieren Sie geplante Sicherungen für NAS-Dateiserver. Siehe NDMP-Operationen planen.
9. Optional: Definieren Sie den Namen eines virtuellen Dateibereichs. Siehe Virtuelle Dateibereiche definieren.
10. Optional: Band-zu-Band-Kopie zum Sichern von Daten konfigurieren. Siehe Daten mit der Band-zu-Band-Kopierfunktion sichern.
11. Optional: Band-zu-Band-Kopie zum Versetzen von Daten in eine andere Bandtechnologie konfigurieren. Siehe Daten mit der Band-zu-Band-Kopierfunktion versetzen.

- IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren
  Mithilfe von Maßnahmen können Sie die Anzahl und den Aufbewahrungszeitraum von NDMP-Imagesicherungsversionen verwalten.
- Bandarchive und -laufwerke für NDMP-Operationen
  Der größte Teil der Planung für die Implementierung von Sicherungs- und Zurückschreibungsoperationen mit NDMP betrifft die Einheitenkonfiguration. Sie können auswählen, wie die Speicherarchive und Laufwerke angeschlossen und verwendet werden sollen.
- Greifarme des Bandarchivs für NAS-Speicherarchive anschließen
  Wenn Sie planen, NAS-Daten in einem Speicherarchiv zu sichern, das direkt a die NAS-Einheit angeschlossen ist, und wenn Sie ein SCSI-Bandarchiv verwenden, müssen Sie die Anschlussposition für das Speicherarchiv festlegen.
- NAS-Knoten im IBM Spectrum Protect-Server registrieren
  Registrieren Sie den NAS-Dateiserver unter Angabe von TYPE=NAS als einen IBM Spectrum Protect-Knoten. Anhand dieses Knotennamens werden die Imagesicherungen für den NAS-Dateiserver protokolliert.
- Einheit zum Versetzen von Daten für einen NAS-Dateiserver definieren
  Definieren Sie eine Einheit zum Versetzen von Daten für jeden NAS-Dateiserver unter Verwendung von NDMP-Operationen in Ihrer Umgebung. Der Name der Einheit zum Versetzen von Daten muss mit dem Knotennamen übereinstimmen, den Sie angegeben haben, als Sie den NAS-Knoten für den IBM Spectrum Protect-Server registriert haben.
- Pfade für NDMP-Operationen definieren
  Für NDMP-Operationen müssen Sie Pfade zu Laufwerken und Speicherarchiven erstellen.
- NDMP-Operationen planen
  Sie können Sicherungs- oder Zurückschreibungsoperationen für Images planen, die von NDMP-Operationen erstellt werden. Verwenden Sie Verwaltungszeitpläne, die den Verwaltungsbefehl BACKUP NODE oder RESTORE NODE verarbeiten.
- Virtuelle Dateibereiche definieren
  Verwenden Sie die Definition eines virtuellen Dateibereichs, um NAS-Sicherungen auf Verzeichnisebene auszuführen. Um die Sicherungs- und Zurückschreibungszeiten für große Dateisysteme zu reduzieren, ordnen Sie einen Verzeichnispfad von einem NAS-Dateiserver zum Namen eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server zu.
- Daten mit der Band-zu-Band-Kopierfunktion sichern
  Wenn Sie die NDMP-Band-zu-Band-Kopierfunktion zum Sichern von Daten verwenden, kann der Speicherarchivtyp SCSI, 349X oder ACSLS (Automated Cartridge System Library Software) sein. Laufwerke können von den NAS-Einheiten und dem IBM Spectrum Protect-Server gemeinsam genutzt werden.
- Daten mit der Band-zu-Band-Kopierfunktion versetzen
  Um Daten unter Verwendung der NDMP-Band-zu-Band-Kopieroperation von einer vorherigen Bandtechnologie in in eine neue Bandtechnologie zu versetzen, müssen Sie die Standardschritte in Ihrem Konfigurationssetup sowie weitere Schritte ausführen.

IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren

Mithilfe von Maßnahmen können Sie die Anzahl und den Aufbewahrungszeitraum von NDMP-Imagesicherungsversionen verwalten.

Informationen zu diesem Vorgang

Weitere Informationen finden Sie in Maßnahmen für Sicherungen, die von einem IBM Spectrum Protect-Server eingeleitet werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Maßnahme für NDMP-Operationen zu konfigurieren:

1. Erstellen Sie eine Maßnahmendomäne für NAS-Dateiserver (NAS = Network-attached Storage). Geben Sie beispielsweise folgenden Befehl ein, um die Maßnahmendomäne NASDOMAIN zu definieren:

   ```
   define domain nasdomain description='Maßnahmendomäne für NAS-Dateiserver'
   ```

2. Erstellen Sie eine Maßnahmengruppe in dieser Domäne. Um beispielsweise eine Maßnahmengruppe mit dem Namen STANDARD in der Maßnahmendomäne NASDOMAIN zu definieren, geben Sie den folgenden Befehl aus:

   ```
   define policyset nasdomain standard
   ```

3. Definieren Sie die Verwaltungsklasse und ordnen Sie dann die Verwaltungsklasse als Standardwert für die Maßnahmengruppe zu. Um beispielsweise eine Verwaltungsklasse mit dem Namen MC1 in der Maßnahmengruppe STANDARD zu definieren und anschließend als Standard zuzuordnen, geben Sie die folgenden Befehle aus:

   ```
   define mgmtclass nasdomain standard mc1

   assign defmgmtclass nasdomain standard mc1
   ```

4. Definieren Sie eine Sicherungskopiengruppe in der Standardverwaltungsklasse. Das Ziel muss der Speicherpool sein, den Sie für die durch NDMP-Operationen generierten Sicherungsimages erstellt hatten. Zusätzlich können Sie die Anzahl der Sicherungsversionen angeben, die aufbewahrt werden sollen. Um beispielsweise eine Sicherungskopiengruppe für die Verwaltungsklasse MC1 zu definieren und bis zu vier Versionen jedes Dateisystems im Speicherpool mit dem Namen NASPOOL aufzubewahren, geben Sie den folgenden Befehl aus:

   ```
   define copygroup nasdomain standard mc1 destination=naspool verexists=4
   ```

   Wenn ein Inhaltsverzeichnis (TOC) für Ihre Sicherungen erstellt werden soll, muss der Parameter TOCDESTINATION der Kopiengruppe den Namen des primären Speicherpools enthalten.

   ```
   define copygroup nasdomain standard mc1 destination=naspool
   tocdestination=tocpool verexists=4
   ```

   Wichtig: Wenn Sie eine Kopiengruppe für eine Verwaltungsklasse definieren, an die ein durch NDMP generiertes Dateisystemimage gebunden ist, müssen Sie sicherstellen, dass der Parameter DESTINATION den Namen eines Speicherpools angibt, der für NDMP-Operationen definiert ist. Wenn im Parameter DESTINATION ein ungültiger Speicherpool angegeben ist, schlagen Sicherungen mit NDMP fehl.
5. Aktivieren Sie die Maßnahmengruppe. Um beispielsweise die Maßnahmengruppe STANDARD in der Maßnahmendomäne NASDOMAIN zu aktivieren, geben Sie den folgenden Befehl aus:

   ```
   activate policyset nasdomain standard
   ```

   Die Maßnahme kann jetzt verwendet werden. Knoten werden bei ihrer Registrierung einer Maßnahme zugeordnet. Weitere Informationen finden Sie in NAS-Knoten im IBM Spectrum Protect-Server registrieren.

- Maßnahmen für Sicherungen, die von einem IBM Spectrum Protect-Server eingeleitet werden
  Sie können einen NAS-Dateiserver unter Verwendung von NDMP-Operationen als Knoten registrieren. Unter der Steuerung des IBM Spectrum Protect-Servers sichert der NAS-Dateiserver ein Dateisystem und Verzeichnisimages und schreibt diese in ein Bandarchiv zurück.
- Maßnahmen für Sicherungen, die mit der Clientschnittstelle eingeleitet werden
  Wenn ein Clientknoten eine Sicherung einleitet, hat die Optionsdatei für den betreffenden Clientknoten Auswirkungen auf die Maßnahme.
- Festlegung der NAS-Sicherungsposition
  Wenn IBM Spectrum Protect NDMP zum Schützen von NAS-Dateiservern verwendet, werden Operationen durch den IBM Spectrum Protect-Server gesteuert. Während dieser Zeit überträgt der NAS-Dateiserver die Daten entweder an ein angeschlossenes Speicherarchiv oder direkt an den IBM Spectrum Protect-Server.

Maßnahmen für Sicherungen, die von einem IBM Spectrum Protect-Server eingeleitet werden

Sie können einen NAS-Dateiserver unter Verwendung von NDMP-Operationen als Knoten registrieren. Unter der Steuerung des IBM Spectrum Protect-Servers sichert der NAS-Dateiserver ein Dateisystem und Verzeichnisimages und schreibt diese in ein Bandarchiv zurück.

Der IBM Spectrum Protect-Server leitet die Sicherung ein, ordnet ein Laufwerk zu, wählt die Datenträger aus und lädt sie. Der NAS-Dateiserver überträgt dann die Daten auf Band.

Da der NAS-Dateiserver die Daten sichert, werden die Daten im Format des NAS-Dateiservers gespeichert. Bei den meisten NAS-Dateiservern werden die Daten im Datenformat NDMPDUMP gespeichert. Bei NetApp-Dateiservern werden die Daten im Datenformat NETAPPDUMP gespeichert. Bei EMC-Dateiservern werden die Daten im Datenformat CELERRADUMP gespeichert. Zum Verwalten von Imagesicherungen des NAS-Dateiservers müssen Kopiengruppen für NAS-Knoten auf einen Speicherpool zeigen, der das Datenformat NDMPDUMP, NETAPPDUMP oder CELERRADUMP hat.

Die folgenden Attribute für Sicherungskopiengruppen werden für NAS-Images ignoriert:

- Häufigkeit
- Modus
- Einzige Version aufbewahren
- Durchnummerierung
- Versionen gelöschter Daten

Um die erforderliche Maßnahme für NAS-Knoten zu definieren, können Sie eine neue, separate Maßnahmendomäne definieren.

Wenn der IBM Spectrum Protect-Server ein Inhaltsverzeichnis erstellt, können Sie eine Sammlung einzelner Dateien und Verzeichnisse anzeigen, die unter Verwendung von NDMP gesichert werden. Anschließend können Sie die zurückzuschreibenden Dateien und Verzeichnisse auswählen. Um festzulegen, wohin Daten gesendet werden sollen und wo das Inhaltsverzeichnis gespeichert werden soll, definieren Sie die Maßnahme wie folgt:

- Stellen Sie sicher, dass Imagesicherungsdaten an einen Speicherpool mit dem Format NDMPDUMP, NETAPPDUMP oder CELERRADUMP gesendet werden.
- Stellen Sie sicher, dass das Inhaltsverzeichnis an einen Speicherpool mit dem Format NATIVE oder NONBLOCK gesendet wird.

Maßnahmen für Sicherungen, die mit der Clientschnittstelle eingeleitet werden

Wenn ein Clientknoten eine Sicherung einleitet, hat die Optionsdatei für den betreffenden Clientknoten Auswirkungen auf die Maßnahme.

Sie können die Verwaltungsklassen steuern, die auf Sicherungsimages angewendet werden, die durch NDMP-Operationen (NDMP = Network Data Management Protocol) generiert wurden, und zwar unabhängig davon, welcher Knoten die Sicherung einleitet. Sie können diese Task ausführen, indem Sie eine Gruppe von Optionen erstellen, die von den Clientknoten verwendet werden sollen. Die Optionsgruppe kann eine Anweisung `include.fs.nas` enthalten, um die Verwaltungsklasse für NAS-Dateiserversicherungen anzugeben.

Tipp: Sie können eine Optionsgruppe mit dem Befehl DEFINE CLOPTSET definieren. Fügen Sie dann der Optionsgruppe mit dem Befehl DEFINE CLIENTOPT eine Clientoption hinzu. Sie können einem Client eine Optionsgruppe zuordnen, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie die Seite Übersicht im Operations Center und klicken Sie auf Clients.
2. Doppelklicken Sie auf den Client und klicken Sie auf Merkmale.
3. Wählen Sie im Feld Optionsgruppe eine Option aus und klicken Sie auf Sichern.

Anweisungen zur Verwendung des Befehls DEFINE CLOPTSET finden Sie in DEFINE CLOPTSET (Clientoptionsgruppennamen definieren). Anweisungen zur Verwendung des Befehls DEFINE CLIENTOPT finden Sie in DEFINE CLIENTOPT (Option für eine Optionsgruppe definieren).

Festlegung der NAS-Sicherungsposition

Wenn IBM Spectrum Protect NDMP zum Schützen von NAS-Dateiservern verwendet, werden Operationen durch den IBM Spectrum Protect-Server gesteuert. Während dieser Zeit überträgt der NAS-Dateiserver die Daten entweder an ein angeschlossenes Speicherarchiv oder direkt an den IBM Spectrum Protect-Server.

Sie können auch einen Client für Sichern/Archivieren verwenden, um einen NAS-Dateiserver zu sichern, indem das NAS-Dateisystem auf dem Client-Computer bereitgestellt wird und dann die Sicherung wie gewohnt ausgeführt wird. Sie können entweder einen NFS-Mount oder eine CIFS-Map verwenden.

Eine Beschreibung der Methoden zur Sicherung und Zurückschreibung finden Sie in Tabelle 1.

Tipp: Sie können eine einzelne Methode oder eine Kombination der Methoden in Ihrer individuellen Speicherumgebung verwenden.

Tabelle 1. Vergleich der Methoden zum Sichern von NDMP-Daten

Merkmal	NDMP: Vom Dateiserver auf den Server	NDMP: Vom Dateiserver in ein angeschlossenes Speicherarchiv	Vom Client für Sichern/Archivieren auf den Server
Datenverkehr im Netz	Alle Sicherungsdaten werden über das LAN vom NAS-Dateiserver zum Server übertragen.	Der Server steuert Operationen über Remotezugriff, aber die NAS-Einheit versetzt die Daten lokal.	Alle Sicherungsdaten werden über das LAN von der NAS-Einheit zum Client und dann zum Server übertragen.
Dateiserververarbeitung während der Sicherung	Im Vergleich zur Sicherungsmethode mit dem Client für Sichern/Archivieren ist weniger Dateiserververarbeitung erforderlich, da bei der Sicherung keine Dateizugriffsprotokolle wie zum Beispiel NFS und CIFS verwendet werden.	Im Vergleich zur Sicherungsmethode mit dem Client für Sichern/Archivieren ist weniger Dateiserververarbeitung erforderlich, da bei der Sicherung keine Dateizugriffsprotokolle wie zum Beispiel NFS und CIFS verwendet werden.	Dateisicherungsoperationen erfordern mehr Serververarbeitungsressourcen für Dateizugriffsprotokolle wie NFS und CIFS.

Merkmal	NDMP: Vom Dateiserver auf den Server	NDMP: Vom Dateiserver in ein angeschlossenes Speicherarchiv	Vom Client für Sichern/Archivieren auf den Server
Entfernung zwischen Einheiten	Der IBM Spectrum Protect-Server muss sich innerhalb des SCSI- bzw. Fibre Channel-Bereichs des Bandarchivs befinden.	Der IBM Spectrum Protect-Server muss sich nicht lokal auf dem NAS-Dateiserver und nicht innerhalb des Bandarchivs befinden.	Der IBM Spectrum Protect-Server muss sich innerhalb des SCSI- bzw. Fibre Channel-Bereichs des Bandarchivs befinden.
Firewallaspekte	Strikter als bei der Übertragung zwischen Dateiserver und angeschlossenem Speicherarchiv, da die Übertragung entweder vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver eingeleitet werden kann.	Weniger strikt als bei der Übertragung zwischen Dateiserver und Server, da die Übertragung nur vom IBM Spectrum Protect-Server eingeleitet werden kann.	Clientkennwörter und -daten werden verschlüsselt.
Sicherheitsaspekte	Daten werden entschlüsselt von einem NAS-Dateiserver an einen IBM Spectrum Protect-Server gesendet.	Diese Methode muss in einer vertrauenswürdigen Umgebung verwendet werden, da Portnummern nicht sicher sind.	Die Portnummernkonfiguration ermöglicht sichere Verwaltungssitzungen in einem privaten Netz.
Last auf dem IBM Spectrum Protect-Server	Höhere CPU-Workload ist erforderlich, um alle Back-End-Datenprozesse zu verwalten (beispielsweise Umlagerung).	Die CPU-Workload verringert sich, da Umlagerung und Konsolidierung nicht unterstützt werden.	Höhere CPU-Workload ist erforderlich, um alle Back-End-Datenprozesse zu verwalten.
Sicherung von primären Speicherpools in Kopienspeicherpools	Daten können nur in Kopienspeicherpools gesichert werden, die das Datenformat NATIVE haben.	Daten können nur in Kopienspeicherpools gesichert werden, die dasselbe NDMP-Datenformat haben (NETAPPDUMP, CELERRADUMP oder NDMPDUMP).	Daten können nur in Kopienspeicherpools gesichert werden, die das Datenformat NATIVE haben.
Zurückschreibung von primären Speicherpools und Datenträgern aus Kopienspeicherpools	Daten können nur in Speicherpools und auf Datenträger zurückgeschrieben werden, die das Datenformat NATIVE haben.	Daten können nur in Speicherpools und auf Datenträger zurückgeschrieben werden, die dasselbe NDMP-Format haben.	Daten können nur in Speicherpools und auf Datenträger zurückgeschrieben werden, die das Datenformat NATIVE haben.
Versetzen von NDMP-Daten von Speicherpooldatenträgern	Daten können nur in einen anderen Speicherpool versetzt werden, wenn er das Datenformat NATIVE hat.	Daten können nur in einen anderen Speicherpool versetzt werden, wenn er dasselbe NDMP-Datenformat hat.	Daten können nur in einen anderen Speicherpool versetzt werden, wenn er das Datenformat NATIVE hat.
Umlagerung aus einem primären Speicherpool in einen anderen Speicherpool	Unterstützt	Nicht unterstützt	Unterstützt
Konsolidierung eines Speicherpools	Unterstützt	Nicht unterstützt	Unterstützt
Operationen für gleichzeitiges Schreiben während Sicherungen	Nicht unterstützt	Nicht unterstützt	Unterstützt
Export- und Importoperationen	Nicht unterstützt	Nicht unterstützt	Unterstützt
Generierung von Sicherungsgruppen	Nicht unterstützt	Nicht unterstützt	Unterstützt
Zyklische Blockprüfung (CRC), wenn Daten unter Verwendung von IBM Spectrum Protect-Prozessen versetzt werden	Unterstützt	Nicht unterstützt	Unterstützt
Prüfung unter Verwendung von IBM Spectrum Protect-Prüfbefehlen	Unterstützt	Nicht unterstützt	Unterstützt
Disaster Recovery Manager	Unterstützt	Unterstützt	Unterstützt

Bandarchive und -laufwerke für NDMP-Operationen

Der größte Teil der Planung für die Implementierung von Sicherungs- und Zurückschreibungsoperationen mit NDMP betrifft die Einheitenkonfiguration. Sie können auswählen, wie die Speicherarchive und Laufwerke angeschlossen und verwendet werden sollen.

Viele der Konfigurationsauswahlmöglichkeiten, die für Speicherarchive und Laufwerke zur Verfügung stehen, werden von den Hardware-Features Ihrer Speicherarchive bestimmt. Sie können NDMP-Operationen für alle unterstützten Speicherarchive und Laufwerke definieren. Je mehr Features jedoch für Ihr Speicherarchiv zur Verfügung stehen, desto flexibler lässt sich die Implementierung gestalten.

Zunächst sollten Sie folgende Fragen beantworten:

- Welcher Speicherarchivtyp (SCSI, ACSLS, 349X) wird verwendet?
- Bei Bei Verwendung eines SCSI-Speicherarchivs: Sollen die Greifarme des Bandarchivs an den IBM Spectrum Protect-Server oder den NAS-Dateiserver angeschlossen werden?
- Sollen Ihre NDMP-Daten auf Band versetzt werden?
- Wie sollen die Bandlaufwerke im Speicherarchiv verwendet werden?
    - Ordnen Sie alle Bandlaufwerke NDMP-Operationen zu.
    - Ordnen Sie einige Bandlaufwerke NDMP-Operationen und andere traditionellen IBM Spectrum Protect-Operationen zu.
    - Nutzen Sie Bandlaufwerke für NDMP-Operationen und traditionelle IBM Spectrum Protect-Operationen gemeinsam.
- Werden Daten für Funktionen zur Wiederherstellung nach einem Katastrophenfall von Band zu Band gesichert?
- Werden Sicherungsdaten an einen einzelnen IBM Spectrum Protect-Server gesendet, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen?
- Soll sich die gesamte Hardware auf dem IBM Spectrum Protect-Server befinden und sollen NDMP-Daten über das LAN gesendet werden?

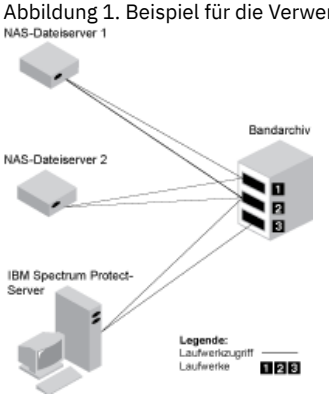
- Speicherarchivlaufwerknutzung bei der Sicherung auf NAS-Speicherarchiven bestimmen
  Laufwerke können aufgrund der bei IBM Spectrum Protect möglichen flexiblen Konfigurationen für vielfältige Zwecke eingesetzt werden. Für NDMP-Operationen muss der NAS-Dateiserver Zugriff auf das Laufwerk haben. Der IBM Spectrum Protect-Server kann ebenfalls Zugriff auf dasselbe Laufwerk haben, in Abhängigkeit von den vorliegenden Hardwareverbindungen und -einschränkungen.
- Bandarchiv für NDMP-Operationen konfigurieren
  Sie können ein Bandarchiv zum Sichern einer NAS-Einheit (NAS = Network-attached Storage) auf Band konfigurieren.

Speicherarchivlaufwerknutzung bei der Sicherung auf NAS-Speicherarchiven bestimmen

Laufwerke können aufgrund der bei IBM Spectrum Protect möglichen flexiblen Konfigurationen für vielfältige Zwecke eingesetzt werden. Für NDMP-Operationen muss der NAS-Dateiserver Zugriff auf das Laufwerk haben. Der IBM Spectrum Protect-Server kann ebenfalls Zugriff auf dasselbe Laufwerk haben, in Abhängigkeit von den vorliegenden Hardwareverbindungen und -einschränkungen.

Informationen zu diesem Vorgang

Alle Laufwerke werden für den IBM Spectrum Protect-Server definiert. Dasselbe Laufwerk kann jedoch sowohl für traditionelle IBM Spectrum Protect-Operationen als auch für NDMP-Operationen definiert werden. Abbildung 1 zeigt eine der möglichen Konfigurationen. Der IBM Spectrum Protect-Server hat Zugriff auf die Laufwerke 2 und 3, und jeder NAS-Dateiserver hat Zugriff auf die Laufwerke 1 und 2.
Abbildung 1. Beispiel für die Verwendung von IBM Spectrum Protect-Laufwerken



Um die in Abbildung 1 gezeigte Konfiguration zu erstellen, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Alle drei Laufwerke für IBM Spectrum Protect definieren.
2. Pfade vom IBM Spectrum Protect-Server zu den Laufwerken 2 und 3 definieren. Da der Server nicht auf Laufwerk 1 zugreift, wird kein Pfad zu diesem Laufwerk definiert.
3. Jeden NAS-Dateiserver als separate Einheit zum Versetzen von Daten definieren.
4. Pfade von jeder Einheit zum Versetzen von Daten zu Laufwerk 1 und 2 definieren.

Ergebnisse

Für die Verwendung der Back-End-Datenversetzungsoperationen in IBM Spectrum Protect erfordert der IBM Spectrum Protect-Server zwei verfügbare Laufwerkpfade von einer einzelnen NAS-Einheit zum Versetzen von Daten. Die Laufwerke können sich in verschiedenen Speicherarchiven befinden und können verschiedene Einheitentypen haben, die von NDMP unterstützt werden. Sie können Kopien zwischen zwei verschiedenen Bandeinheiten erstellen. Beispielsweise kann das Quellenbandlaufwerk ein DLT-Laufwerk in einem Speicherarchiv sein und das Ziellaufwerk ein LTO-Laufwerk in einem anderen Speicherarchiv.

Während der Back-End-Datenversetzungsoperationen in IBM Spectrum Protect sucht der IBM Spectrum Protect-Server eine NAS-Einheit zum Versetzen von Daten, die dasselbe Datenformat wie das Format der Daten unterstützt, aus denen kopiert wird, und die über zwei verfügbare Mountpunkte und Pfade zu den Laufwerken verfügt. Kann der IBM Spectrum Protect-Server eine solche Einheit zum Versetzen von Daten nicht finden, wird die angeforderte Datenversetzungsoperation nicht ausgeführt. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von den Mount-Limits der Einheitenklassen für die Speicherpools abhängig, die an den Back-End-Datenversetzungsoperationen beteiligt sind.

Unterstützt die Back-End-Datenversetzungsfunktion den Mehrprozessorbetrieb, erfordert jeder gleichzeitig ablaufende Back-End-Datenversetzungsprozess in IBM Spectrum Protect zwei verfügbare Mountpunkte und zwei verfügbare Laufwerke. Um zwei IBM Spectrum Protect-Prozesse gleichzeitig auszuführen, müssen mindestens vier Mountpunkte und vier Laufwerke verfügbar sein.

Weitere Informationen finden Sie in Pfade für NDMP-Operationen definieren.

Bandarchiv für NDMP-Operationen konfigurieren

Sie können ein Bandarchiv zum Sichern einer NAS-Einheit (NAS = Network-attached Storage) auf Band konfigurieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Bandarchive für NDMP-Operationen zu konfigurieren:

1. Schließen Sie das Bandarchiv und die Laufwerke, die für NDMP-Operationen verwendet werden sollen, an.
   a. Schließen Sie das SCSI-Bandarchiv an. Legen Sie, bevor Sie ein SCSI-Bandarchiv für NDMP-Operationen definieren, fest, ob die Steuerung für die Greifarme des Speicherarchivs an den IBM Spectrum Protect-Server oder den NAS-Dateiserver angeschlossen werden soll. Siehe Bandarchive und -laufwerke für NDMP-Operationen. Schließen Sie die Greifarme des SCSI-Bandarchivs an den IBM Spectrum Protect-Server oder an den NAS-Dateiserver an. Anweisungen finden Sie in der Dokumentation des Einheitenherstellers.

      Wenn das Speicherarchiv an den IBM Spectrum Protect-Server angeschlossen ist, stellen Sie eine SCSI- oder Fibre Channel-Verbindung zwischen dem IBM Spectrum Protect-Server und dem Steueranschluss für die Greifarme des Speicherarchivs her. Schließen Sie dann den NAS-Dateiserver an die Laufwerke an.

      Wenn das Speicherarchiv an den NAS-Dateiserver angeschlossen ist, stellen Sie eine SCSI- oder Fibre Channel-Verbindung zwischen dem NAS-Dateiserver und den Greifarmen des Speicherarchivs und den Laufwerken her.

   b. Schließen Sie das ACSLS-Speicherarchiv an. Schließen Sie das ACSLS-Bandarchiv an den IBM Spectrum Protect-Server an.
   c. Schließen Sie das 349X-Speicherarchiv an. Schließen Sie das 349X-Bandarchiv an den IBM Spectrum Protect-Server an.
2. Definieren Sie das Speicherarchiv für Ihre Speicherarchiveinheit, indem Sie den Befehl DEFINE LIBRARY ausgeben. Das Speicherarchiv darf keine gemischte Einheitentypen haben, sondern muss einen einzelnen Einheitentyp haben. Geben Sie einen der folgenden Befehle aus, um das Speicherarchiv abhängig vom Typ der Einheit, die Sie konfigurieren, zu definieren:

   SCSI-Speicherarchiv

   ```
   define library tsmlib libtype=scsi
   ```

   ACSLS-Speicherarchiv

   ```
   define library acslib libtype=acsls acsid=1
   ```

   349X-Speicherarchiv

   ```
   define library tsmlib libtype=349x
   ```

3. Definieren Sie eine Einheitenklasse für Ihre NDMP-Einheit, indem Sie den Befehl DEFINE DEVCLASS ausgeben.
   Tipp: Eine Einheitenklasse, die mit dem Einheitentyp NAS definiert ist, ist nicht explizit einem bestimmten Laufwerktyp, wie beispielsweise LTO, zugeordnet. Das bevorzugte Verfahren ist jedoch, für unterschiedliche Laufwerktypen jeweils eine andere Einheitenklasse zu definieren.
   Verwenden Sie im Befehl DEFINE DEVCLASS die folgenden Parameter und Werte:
   - Geben Sie `DEVTYPE=NAS` an.
   - Geben Sie `MOUNTRETENTION=0` an. Diese Angabe ist für NDMP-Operationen erforderlich.
   - Geben Sie einen Wert für den Parameter ESTCAPACITY an.

   Um beispielsweise eine Einheitenklasse mit dem Namen NASCLASS für ein Speicherarchiv mit dem Namen NASLIB mit einer geschätzten Kapazität von 40 GB für die Datenträger zu definieren, geben Sie den folgenden Befehl aus:

   ```
   define devclass nasclass devtype=nas library=naslib mountretention=0
    estcapacity=40g
   ```

4. Definieren Sie einen Speicherpool für NDMP-Datenträger, indem Sie den Befehl DEFINE STGPOOL ausgeben. Wenn NETAPPDUMP, CELERRADUMP oder NDMPDUMP als Speicherpooltyp angegeben wird, unterscheidet sich die Verwaltung von Speicherpools, die von NDMP-Operationen erstellt werden, von der Verwaltung von Speicherpools, die Datenträger für traditionelle IBM Spectrum Protect-Sicherungen enthalten. IBM Spectrum Protect-Operationen verwenden Speicherpools, die mit dem Datenformat NATIVE oder NONBLOCK definiert sind. Wenn Sie NETAPPDUMP, CELERRADUMP oder NDMPDUMP auswählen, erfordern NDMP-Operationen Speicherpools mit einem Datenformat, das dem NAS-Dateiserver und der ausgewählten Sicherungsmethode entspricht. Unterschiedliche Speicherpools für Daten verschiedener NAS-Anbieter zu verwalten ist selbst dann optimal, wenn beide das Datenformat NDMPDUMP haben. Um beispielsweise einen Speicherpool mit dem Namen NDMPPOOL für einen Dateiserver zu definieren, der kein NetApp- oder kein Celerra-Dateiserver ist, geben Sie den folgenden Befehl aus:

   ```
   define stgpool ndmppool nasclass maxscratch=10 dataformat=ndmpdump
   ```

   Um einen Speicherpool mit dem Namen NASPOOL für einen NetApp-Dateiserver zu definieren, geben Sie den folgenden Befehl aus:

   ```
   define stgpool naspool nasclass maxscratch=10 dataformat=netappdump
   ```

   Um einen Speicherpool mit dem Namen CELERRAPOOL für einen EMC Celerra-Dateiserver zu definieren, geben Sie den folgenden Befehl aus:

   ```
   define stgpool celerrapool nasclass maxscratch=10 dataformat=celerradump
   ```

   Achtung: Stellen Sie sicher, dass Sie Speicherpools, die für NDMP-Operationen definiert sind, nicht versehentlich für traditionelle IBM Spectrum Protect-Operationen verwenden. Gehen Sie mit besonderer Sorgfalt vor, wenn Sie den Speicherpoolnamen als Wert für den Parameter DESTINATION im Befehl DEFINE COPYGROUP zuordnen. Wenn der Zielspeicherpool nicht das geeignete Datenformat aufweist, kann die Sicherung fehlschlagen.
5. Optional: Definieren Sie einen Speicherpool für ein Inhaltsverzeichnis. Wenn Sie planen, ein Inhaltsverzeichnis zu erstellen, müssen Sie auch einen Plattenspeicherpool zum Speichern des Inhaltsverzeichnisses definieren. Sie müssen die Maßnahme so definieren, dass der IBM Spectrum Protect-Server das Inhaltsverzeichnis in einem anderen Speicherpool speichert als das Sicherungsimage. Das Inhaltsverzeichnis wird wie jedes andere Objekt in diesem Speicherpool behandelt. Um beispielsweise einen Speicherpool mit dem Namen TOCPOOL für eine Einheitenklasse DISK zu definieren, geben Sie den folgenden Befehl aus:

   ```
   define stgpool tocpool disk
   ```

   Definieren Sie dann Datenträger für den Speicherpool.

   AIX-BetriebssysteLinux-BetriebssystemeWeitere Informationen zum Definieren von Datenträgern befinden sich in Datenträger mit wahlfreiem Zugriff auf Platteneinheiten konfigurieren (Version 7.1.1).

   Windows-BetriebssystemeWeitere Informationen zum Definieren von Datenträgern befinden sich in Datenträger mit wahlfreiem Zugriff auf Platteneinheiten konfigurieren (Version 7.1.1).

   AIX-BetriebssysteLinux-BetriebssystemeWeitere Informationen zum Konfigurieren von Speicherarchiven finden Sie in Speicherarchive für die Verwendung durch einen Server konfigurieren.

Zugehörige Verweise:
DEFINE DEVCLASS (Einheitenklasse definieren)

Greifarme des Bandarchivs für NAS-Speicherarchive anschließen

Wenn Sie planen, NAS-Daten in einem Speicherarchiv zu sichern, das direkt a die NAS-Einheit angeschlossen ist, und wenn Sie ein SCSI-Bandarchiv verwenden, müssen Sie die Anschlussposition für das Speicherarchiv festlegen.

Informationen zu diesem Vorgang

Sie müssen festlegen, ob die Greifarme des Speicherarchivs an den IBM Spectrum Protect-Server oder den NAS-Dateiserver angeschlossen werden sollen. Unabhängig davon, wo die Greifarme des Speicherarchivs angeschlossen werden, müssen die Bandlaufwerke für NDMP-Operationen immer an den NAS-Dateiserver angeschlossen werden.

Berücksichtigt werden müssen auch die Entfernung und die verfügbaren Hardwareverbindungen für SCSI-Speicherarchive. Wenn das Speicherarchiv keine separaten Ports für die Greifarmsteuerung und den Laufwerkzugriff hat, muss das Speicherarchiv an den NAS-Dateiserver angeschlossen werden, da der NAS-Dateiserver Zugriff auf die Laufwerke haben muss. Wenn Ihr SCSI-Speicherarchiv über separate Ports für die Greifarmsteuerung und den Laufwerkzugriff verfügt, können Sie wählen, ob die Greifarme des Speicherarchivs an den IBM Spectrum Protect-Server oder den NAS-Dateiserver angeschlossen werden sollen. Wenn sich der NAS-Dateiserver an einem anderen Standort befindet als der IBM Spectrum Protect-Server, kann dies bedeuten, dass Sie das Speicherarchiv an den NAS-Dateiserver anschließen müssen.

Unabhängig davon, ob Sie ein SCSI-, ACSLS- oder 349X-Speicherarchiv verwenden, haben Sie die Wahl, das Speicherarchiv NDMP-Operationen zuzuordnen oder das Speicherarchiv für NDMP-Operationen zu verwenden. Sie können das Speicherarchiv auch für die meisten traditionellen IBM Spectrum Protect-Operationen verwenden.

Tabelle 1. Zusammenfassung der Konfigurationen für NDMP-Operationen

Konfiguration	Entfernung zwischen IBM Spectrum Protect-Server und Speicherarchiv	Gemeinsame Speicherarchivnutzung	Gemeinsame Laufwerknutzung zwischen IBM Spectrum Protect und NAS-Dateiserver	Gemeinsame Laufwerknutzung zwischen NAS-Dateiservern	Gemeinsame Laufwerknutzung zwischen Speicheragent und NAS-Dateiserver
Konfiguration 1(An den IBM Spectrum Protect-Server angeschlossenes SCSI-Speicherarchiv)	Begrenzt durch SCSI- oder FC-Verbindung	Unterstützt	Unterstützt	Unterstützt	Unterstützt
Konfiguration 2 (An den NAS-Dateiserver angeschlossenes SCSI-Speicherarchiv)	Keine Begrenzung	Nicht unterstützt	Unterstützt	Unterstützt	Nicht unterstützt
Konfiguration 3 (349X-Speicherarchiv)	Kann durch 349X-Verbindung begrenzt sein	Unterstützt	Unterstützt	Unterstützt	Unterstützt
AIX-Betriebssysteme Windows-Betriebssysteme Konfiguration 4 (ACSLS-Speicherarchiv)	AIX-Betriebssysteme Windows-Betriebssysteme Kann durch ACSLS-Verbindung begrenzt sein	AIX-Betriebssysteme Windows-Betriebssysteme Unterstützt	AIX-Betriebssysteme Windows-Betriebssysteme Unterstützt	AIX-Betriebssysteme Windows-Betriebssysteme Unterstützt	AIX-Betriebssysteme Windows-Betriebssysteme Unterstützt

- Konfiguration 1: An den IBM Spectrum Protect-Server angeschlossenes SCSI-Speicherarchiv
  Bei dieser Konfiguration muss das Bandarchiv über separate Ports für die Greifarmsteuerung und den Laufwerkzugriff verfügen. Außerdem muss sich das Speicherarchiv innerhalb des Fibre Channel-Bereichs oder SCSI-Bus-Bereichs sowohl des IBM Spectrum Protect-Servers als auch des NAS-Dateiservers befinden.
- Konfiguration 2: An den NAS-Dateiserver angeschlossenes SCSI-Speicherarchiv
  Bei dieser Konfiguration müssen die Greifarme des Speicherarchivs und die Laufwerke physisch über eine Direktverbindung an den NAS-Dateiserver angeschlossen werden. Pfade müssen von der NAS-Einheit zum Versetzen von Daten zum Speicherarchiv und zu den Laufwerken definiert werden. Es ist keine physische Verbindung zwischen dem IBM Spectrum Protect-Server und dem SCSI-Speicherarchiv erforderlich.
- Konfiguration 3: An den IBM Spectrum Protect-Server angeschlossenes 349x-Speicherarchiv
  Bei dieser Konfiguration schließen Sie das Bandarchiv wie für herkömmliche Operationen an das System an.
- Konfiguration 4: An den IBM Spectrum Protect-Server angeschlossenes ACSLS-Speicherarchiv
  Bei dieser Konfiguration schließen Sie das Bandarchiv wie für herkömmliche IBM Spectrum Protect-Operationen an das System an.

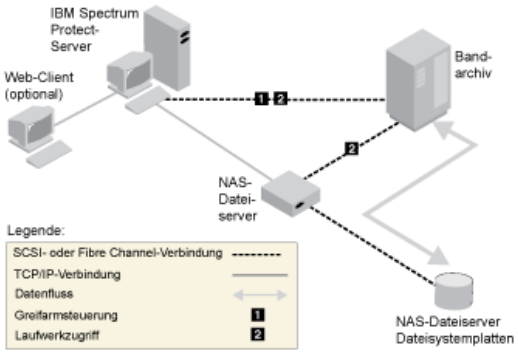
Konfiguration 1: An den IBM Spectrum Protect-Server angeschlossenes SCSI-Speicherarchiv

Bei dieser Konfiguration muss das Bandarchiv über separate Ports für die Greifarmsteuerung und den Laufwerkzugriff verfügen. Außerdem muss sich das Speicherarchiv innerhalb des Fibre Channel-Bereichs oder SCSI-Bus-Bereichs sowohl des IBM Spectrum Protect-Servers als auch des NAS-Dateiservers befinden.

Bei dieser Konfiguration steuert der IBM Spectrum Protect-Server das SCSI-Speicherarchiv über eine direkte physische Verbindung zum Steueranschluss für die Greifarme des Speicherarchivs. Für NDMP-Operationen werden die Laufwerke im Speicherarchiv direkt an den NAS-Dateiserver angeschlossen; außerdem muss ein Pfad von der NAS-Einheit zum Versetzen von Daten zu jedem Laufwerk, das verwendet werden soll, definiert werden. Der NAS-Dateiserver überträgt auf Anforderung des IBM Spectrum Protect-Servers Daten zum Bandlaufwerk. Um die Laufwerke auch für IBM Spectrum Protect-Operationen verwenden zu können, verbinden Sie den IBM Spectrum Protect-Server mit den Bandlaufwerken und definieren Sie Pfade vom Server zu den Bandlaufwerken.

Diese Konfiguration unterstützt außerdem einen IBM Spectrum Protect-Speicheragenten, der für seine LAN-unabhängigen Operationen Zugriff auf die Laufwerke hat; der IBM Spectrum Protect-Server kann dabei auch ein Speicherarchivmanager sein.

Abbildung 1. Konfiguration 1: An den IBM Spectrum Protect-Server angeschlossenes SCSI-Speicherarchiv

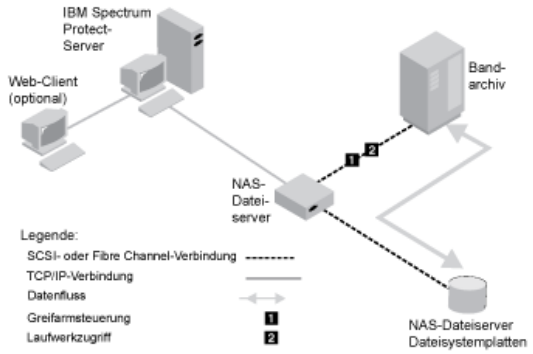


Konfiguration 2: An den NAS-Dateiserver angeschlossenes SCSI-Speicherarchiv

Bei dieser Konfiguration müssen die Greifarme des Speicherarchivs und die Laufwerke physisch über eine Direktverbindung an den NAS-Dateiserver angeschlossen werden. Pfade müssen von der NAS-Einheit zum Versetzen von Daten zum Speicherarchiv und zu den Laufwerken definiert werden. Es ist keine physische Verbindung zwischen dem IBM Spectrum Protect-Server und dem SCSI-Speicherarchiv erforderlich.

Der IBM Spectrum Protect-Server steuert die Greifarme, indem er Speicherarchivbefehle über das Netz an den NAS-Dateiserver sendet. Der NAS-Dateiserver übergibt die Befehle an das Bandarchiv. Alle vom Speicherarchiv generierten Antworten werden an den NAS-Dateiserver gesendet und über das Netz zurück an den IBM Spectrum Protect-Server übergeben. Diese Konfiguration unterstützt einen IBM Spectrum Protect-Server und einen NAS-Dateiserver, die physisch voneinander getrennt sind. Der IBM Spectrum Protect-Server kann sich beispielsweise in einer anderen Stadt befinden als der NAS-Dateiserver und das Bandarchiv.

Abbildung 1. Konfiguration 2: An den NAS-Dateiserver angeschlossenes SCSI-Speicherarchiv



Konfiguration 3: An den IBM Spectrum Protect-Server angeschlossenes 349x-Speicherarchiv

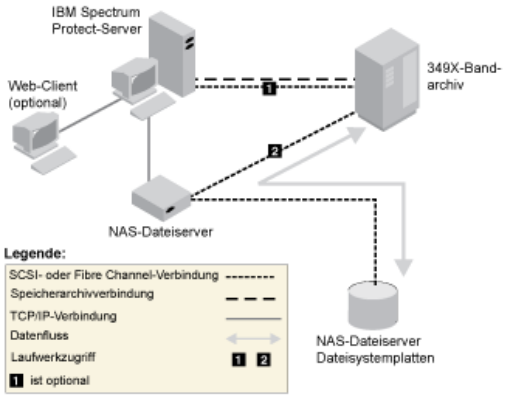
Bei dieser Konfiguration schließen Sie das Bandarchiv wie für herkömmliche Operationen an das System an.

Bei dieser Konfiguration wird das 349X-Bandarchiv durch den IBM Spectrum Protect-Server gesteuert. Der IBM Spectrum Protect-Server steuert das Speicherarchiv, indem die Anforderung über TCP/IP an den 349X-Speicherarchivmanager übergeben wird.

Um NAS-Sicherungs- oder -Zurückschreibungsoperationen auszuführen, muss der NAS-Dateiserver auf ein oder mehrere Bandlaufwerke im 349X-Speicherarchiv zugreifen können. Alle für NAS-Operationen verwendeten Bandlaufwerke müssen physisch an den NAS-Dateiserver angeschlossen sein. Es müssen Pfade von der NAS-Einheit zum Versetzen von Daten zu den Laufwerken definiert werden. Der NAS-Dateiserver überträgt auf Anforderung des IBM Spectrum Protect-Servers Daten zum Bandlaufwerk. Für den Anschluss der Einheit an das Serversystem sind die Anweisungen des Herstellers zu befolgen.

Diese Konfiguration unterstützt einen IBM Spectrum Protect-Server und einen NAS-Dateiserver, die physisch voneinander getrennt sind. Der IBM Spectrum Protect-Server könnte sich beispielsweise in einer anderen Stadt befinden als der NAS-Dateiserver und das Bandarchiv.

Abbildung 1. Konfiguration 3: An den IBM Spectrum Protect-Server angeschlossenes 349x-Speicherarchiv



Zugehörige Tasks:
Einheiten für den Server anschließen (Version 7.1.1)

Konfiguration 4: An den IBM Spectrum Protect-Server angeschlossenes ACSLS-Speicherarchiv

Bei dieser Konfiguration schließen Sie das Bandarchiv wie für herkömmliche IBM Spectrum Protect-Operationen an das System an.

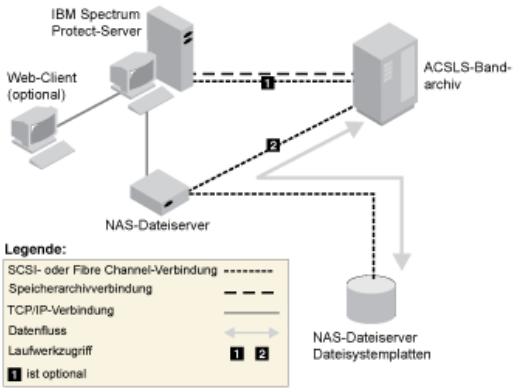
Das ACSLS-Bandarchiv (ACSLS = Automated Cartridge System Library Software) wird durch den IBM Spectrum Protect-Server gesteuert. Der IBM Spectrum Protect-Server steuert das Speicherarchiv, indem die Anforderung über TCP/IP an den ACSLS-Speicherarchivserver übergeben wird. Das ACSLS-Speicherarchiv unterstützt die gemeinsame Nutzung von Speicherarchiven und LAN-unabhängige Operationen.
Windows-BetriebssystemeEinschränkung: Um ACSLS-Funktionen verwenden zu können, muss StorageTek Library Attach-Software installiert sein. Weitere Informationen finden Sie in ACSLS-verwaltete Speicherarchive (Version 7.1.1).

Um NAS-Sicherungs- oder -Zurückschreibungsoperationen auszuführen, muss der NAS-Dateiserver auf ein oder mehrere Bandlaufwerke im ACSLS-Speicherarchiv zugreifen können. Alle für NAS-Operationen verwendeten Bandlaufwerke müssen physisch an den NAS-Dateiserver angeschlossen sein und alle Pfade von der NAS-Einheit zum Versetzen von Daten zu den Laufwerken müssen definiert werden. Der NAS-Dateiserver überträgt auf Anforderung des IBM Spectrum Protect-Servers Daten zum Bandlaufwerk. Für den Anschluss der Einheit an das Serversystem sind die Anweisungen des Herstellers zu befolgen.

Diese Konfiguration unterstützt einen IBM Spectrum Protect-Server und einen NAS-Dateiserver, die physisch voneinander getrennt sind. Der IBM Spectrum Protect-Server könnte sich beispielsweise in einer anderen Stadt befinden als der NAS-Dateiserver und das Bandarchiv.

Um die Laufwerke auch für IBM Spectrum Protect-Operationen verwenden zu können, müssen Sie den IBM Spectrum Protect-Server mit den Bandlaufwerken verbinden und Pfade vom IBM Spectrum Protect-Server zu den Bandlaufwerken definieren.

Abbildung 1. Konfiguration 4: An den IBM Spectrum Protect-Server angeschlossenes ACSLS-Speicherarchiv



Zugehörige Tasks:
Einheiten für den Server anschließen (Version 7.1.1)

NAS-Knoten im IBM Spectrum Protect-Server registrieren

Registrieren Sie den NAS-Dateiserver unter Angabe von TYPE=NAS als einen IBM Spectrum Protect-Knoten. Anhand dieses Knotennamens werden die Imagesicherungen für den NAS-Dateiserver protokolliert.

Vorgehensweise

Geben Sie folgenden Beispielbefehl aus, um einen NAS-Dateiserver als Knoten mit dem Namen NASNODE1 mit dem Kennwort NASPWD1 in einer Maßnahmendomäne mit dem Namen NASDOMAIN zu registrieren:

```
register node nasnode1 naspwd1 domain=nasdomain type=nas
```

Wenn Sie eine Clientoptionsgruppe verwenden, geben Sie die Optionsgruppe beim Registrieren des Knotens an.
Sie können prüfen, ob dieser Knoten registriert wurde, indem Sie folgenden Befehl ausgeben:

```
query node type=nas
```

Hinweis: Sie müssen TYPE=NAS angeben, damit nur NAS-Knoten angezeigt werden.

Einheit zum Versetzen von Daten für einen NAS-Dateiserver definieren

Definieren Sie eine Einheit zum Versetzen von Daten für jeden NAS-Dateiserver unter Verwendung von NDMP-Operationen in Ihrer Umgebung. Der Name der Einheit zum Versetzen von Daten muss mit dem Knotennamen übereinstimmen, den Sie angegeben haben, als Sie den NAS-Knoten für den IBM Spectrum Protect-Server registriert haben.

Informationen zu diesem Vorgang

IBM Spectrum Protect unterstützt zwei Arten von Einheiten zum Versetzen von Daten:

- Bei NDMP-Operationen handelt es sich bei den Einheiten zum Versetzen von Daten um NAS-Dateiserver. Die Definition für eine NAS-Einheit zum Versetzen von Daten enthält die Netzadresse, die Berechtigung sowie Datenformate, die für NDMP-Operationen erforderlich sind. Eine Einheit zum Versetzen von Daten aktiviert die Übertragung und stellt die Berechtigung für NDMP-Operationen zwischen dem IBM Spectrum Protect-Server und dem NAS-Dateiserver sicher.
- Bei der serverunabhängigen Datenversetzung handelt es sich bei den Einheiten zum Versetzen von Daten um Einheiten wie IBM® SAN Data Gateway, die Daten zwischen Platteinheiten und Bandeinheiten im SAN übertragen.

Vorgehensweise

Um eine Einheit zum Versetzen von Daten zu definieren, verwenden Sie den Befehl DEFINE DATAMOVER.

Beispiel

Definieren Sie beispielsweise eine Einheit zum Versetzen von Daten mit den folgenden Parametern:

- Der NAS-Knoten hat den Namen NASNODE1.
- Die Adresse der oberen Ebene ist eine IP-Adresse für den NAS-Dateiserver, und zwar entweder eine numerische Adresse oder ein Hostname.
- Die Adresse der unteren Ebene ist der IP-Port für NDMP-Sitzungen mit dem NAS-Dateiserver. Die Standardportnummer ist 10000.
- Die Benutzer-ID ist die für den NAS-Dateiserver definierte ID, die die Berechtigung für eine NDMP-Sitzung mit dem NAS-Dateiserver bereitstellt. In diesem Beispiel ist die Benutzer-ID die Verwaltungs-ID für den NetApp-Dateiserver.
- Der Kennwortparameter ist ein gültiges Kennwort für die Authentifizierung bei einer NDMP-Sitzung mit dem NAS-Dateiserver.
- Das Datenformat ist NETAPPDUMP. Dieses Datenformat wird vom NetApp-Dateiserver für Bandsicherungen verwendet. Dieses Datenformat muss mit dem Datenformat des Zielspeicherpools übereinstimmen.

Geben Sie den folgenden Befehl ein:

```
define datamover nasnode1 type=nas hladdress=netapp2 lladdress=10000 userid=root
password=admin dataformat=netappdump
```

Zugehörige Verweise:
DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren)

Pfade für NDMP-Operationen definieren

Für NDMP-Operationen müssen Sie Pfade zu Laufwerken und Speicherarchiven erstellen.

- Pfade zu Laufwerken für NDMP-Operationen definieren
  Welche Methode Sie für das Erstellen von Pfaden zu Laufwerken auswählen, ist davon abhängig, ob der Zugriff auf die Laufwerke über einen NAS-Dateiserver und den IBM Spectrum Protect-Server oder ausschließlich über einen NAS-Dateiserver erfolgt.
- Pfade zu Speicherarchiven für NDMP-Operationen definieren
  Definieren Sie entweder vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver einen Pfad zu dem SCSI-Speicherarchiv.

Pfade zu Laufwerken für NDMP-Operationen definieren

Welche Methode Sie für das Erstellen von Pfaden zu Laufwerken auswählen, ist davon abhängig, ob der Zugriff auf die Laufwerke über einen NAS-Dateiserver und den IBM Spectrum Protect-Server oder ausschließlich über einen NAS-Dateiserver erfolgt.

- Pfade für an einen NAS-Dateiserver und an den IBM Spectrum Protect-Server angeschlossene Laufwerke definieren
  Wenn der Zugriff auf ein Bandlaufwerk über einen NAS-Dateiserver und den IBM Spectrum Protect-Server erfolgen muss, müssen Sie zwei Pfade erstellen. Ein Pfad ist zwischen dem Bandlaufwerk und dem NAS-Dateiserver vorhanden. Der andere Pfad ist zwischen dem Bandlaufwerk und dem IBM Spectrum Protect-Server vorhanden.
- Pfade für nur an NAS-Dateiserver angeschlossene Laufwerke definieren
  Wenn der Zugriff auf ein Bandlaufwerk ausschließlich über einen NAS-Dateiserver und nicht über den IBM Spectrum Protect-Server erfolgen muss, ist nur ein einziger Pfad zwischen dem Bandlaufwerk und dem NAS-Dateiserver erforderlich.
- Namen für an NAS-Dateiserver angeschlossene Einheiten abrufen
  Für Pfade von einer NAS-Einheit zum Versetzen von Daten ist der Wert des Parameters DEVICE im Befehl DEFINE PATH der Name, unter dem der NAS-Dateiserver ein Speicherarchiv oder ein Laufwerk kennt.

Pfade für an einen NAS-Dateiserver und an den IBM Spectrum Protect-Server angeschlossene Laufwerke definieren

Wenn der Zugriff auf ein Bandlaufwerk über einen NAS-Dateiserver und den IBM Spectrum Protect-Server erfolgen muss, müssen Sie zwei Pfade erstellen. Ein Pfad ist zwischen dem Bandlaufwerk und dem NAS-Dateiserver vorhanden. Der andere Pfad ist zwischen dem Bandlaufwerk und dem IBM Spectrum Protect-Server vorhanden.

Vorgehensweise

Führen Sie die folgenden Schritte aus:

1. Wenn das Laufwerk für den IBM Spectrum Protect-Server nicht definiert ist, erstellen Sie die Laufwerkdefinition. Um beispielsweise das Laufwerk NASDRIVE1 für das Speicherarchiv NASLIB zu definieren, geben Sie den folgenden Befehl aus:

   ```
   define drive naslib nasdrive1 element=autodetect
   ```

   Hinweis: Wenn das Laufwerk an den IBM Spectrum Protect-Server angeschlossen ist, wird die Elementadresse automatisch erkannt.
2. Ordnen Sie den NAS-Laufwerknamen der entsprechenden Laufwerkdefinition auf dem IBM Spectrum Protect-Server zu:
   - Geben Sie auf dem IBM Spectrum Protect-Server den Befehl QUERY DRIVE FORMAT=DETAILED aus, um den weltweiten Namen (WWN) und die Seriennummer für das Laufwerk abzurufen, das an den NAS-Dateiserver angeschlossen wird.
   - Rufen Sie auf der NAS-Einheit den Bandeinheitennamen, die Seriennummer und den weltweiten Namen für das Laufwerk ab.

   Wenn der weltweite Name oder die Seriennummer übereinstimmen, ist das Laufwerk auf dem NAS-Dateiserver mit dem Laufwerk auf dem IBM Spectrum Protect-Server identisch.
3. Definieren Sie unter Verwendung des Laufwerknamens jeweils einen Pfad vom NAS-Dateiserver und vom IBM Spectrum Protect-Server zu dem Laufwerk.
   - Um beispielsweise einen Pfad zwischen einem Bandlaufwerk mit dem Einheitennamen rst01 und einem NetApp-Dateiserver zu definieren, geben Sie den folgenden Befehl aus:

     ```
     define path nasnode1 nasdrive1 srctype=datamover desttype=drive
       library=naslib device=rst01
     ```

   - Um einen Pfad zwischen dem Bandlaufwerk und dem IBM Spectrum Protect-Server zu definieren, geben Sie den folgenden Befehl aus:

     
     AIX-Betriebssysteme

     ```
     define path server1 nasdrive1 srctype=server desttype=drive
      library=naslib device=/dev/rmt0
     ```

     
     Linux-Betriebssysteme

     ```
     define path server1 nasdrive1 srctype=server desttype=drive
      library=naslib device=/dev/tsmscsi/mt0
     ```

     
     Windows-Betriebssysteme

     ```
     define path server1 nasdrive1 srctype=server desttype=drive
      library=naslib device=mt3.0.0.2
     ```

Pfade für nur an NAS-Dateiserver angeschlossene Laufwerke definieren

Wenn der Zugriff auf ein Bandlaufwerk ausschließlich über einen NAS-Dateiserver und nicht über den IBM Spectrum Protect-Server erfolgen muss, ist nur ein einziger Pfad zwischen dem Bandlaufwerk und dem NAS-Dateiserver erforderlich.

Vorgehensweise

Führen Sie die folgenden Schritte aus:

1. Rufen Sie die SCSI-Elementadresse, den weltweiten Name (WWN, worldwide name) und die Seriennummer für das Laufwerk ab, das an den NAS-Dateiserver angeschlossen werden soll.
   Einschränkung: Wenn das SCSI-Laufwerk nur an einen NAS-Dateiserver angeschlossen ist, wird die Elementadresse nicht automatisch erkannt, sodass Sie die Adresse angeben müssen. Wenn ein Speicherarchiv über mehrere Laufwerke verfügt, müssen Sie eine Elementadresse für jedes Laufwerk angeben.
   Um eine SCSI-Elementadresse abzurufen, rufen Sie die folgenden Websites für die Einheitenunterstützung auf:
   - AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
   - Linux-BetriebssystemeSupported devices for Linux

   Die Elementnummernzuordnung und Zuordnungen weltweiter Namen für Einheiten werden auch von den Herstellern der Bandarchiveinheiten zur Verfügung gestellt.
2. Erstellen Sie Laufwerkdefinitionen, indem Sie die im vorherigen Schritt identifizierte Elementadresse angeben. Geben Sie die Elementadresse im Parameter ELEMENT des Befehls DEFINE DRIVE an. Um beispielsweise das Laufwerk NASDRIVE1 mit der Elementadresse 82 für das Speicherarchiv NASLIB zu definieren, geben Sie den folgenden Befehl aus:

   ```
   define drive naslib nasdrive1 element=82
   ```

   Achtung: Für ein Laufwerk, das an den NAS-Dateiserver angeschlossen ist, dürfen Sie nicht ASNEEDED als Wert für den Parameter CLEANFREQUENCY im Befehl DEFINE DRIVE angeben.
3. Rufen Sie den Einheitennamen, die Seriennummer und den weltweiten Name für das Laufwerk auf der NAS-Einheit ab.
4. Ordnen Sie mithilfe der in den Schritten 1 und 3 abgerufenen Informationen den Namen der NAS-Einheit der Elementadresse in der Laufwerkdefinition auf dem IBM Spectrum Protect-Server zu.
5. Definieren Sie einen Pfad zwischen dem Bandlaufwerk und dem NAS-Dateiserver. Um beispielsweise eine Pfad zwischen einem NetApp-Dateiserver und einem Bandlaufwerk mit dem Einheitennamen rst01 zu definieren, geben Sie den folgenden Befehl aus:

   ```
   define path nasnode1 nasdrive1 srctype=datamover desttype=drive
    library=naslib device=rst01
   ```

Namen für an NAS-Dateiserver angeschlossene Einheiten abrufen

Für Pfade von einer NAS-Einheit zum Versetzen von Daten ist der Wert des Parameters DEVICE im Befehl DEFINE PATH der Name, unter dem der NAS-Dateiserver ein Speicherarchiv oder ein Laufwerk kennt.

Informationen zu diesem Vorgang

Sie können diese Einheitennamen, die auch als *Gerätedateinamen* bezeichnet werden, können durch Abfragen des NAS-Dateiservers abrufen. Informationen zum Abrufen der Namen von Einheiten, die mit einem NAS-Dateiserver verbunden sind, finden Sie in der Produktinformation zum Dateiserver.

Vorgehensweise

- Um die Einheitennamen für Bandarchive auf einem Dateiserver unter NetApp Release ONTAP 10.0 GX oder höher abzurufen, stellen Sie mithilfe von Telnet die Verbindung zum Dateiserver her und geben Sie den Befehl SYSTEM HARDWARE TAPE LIBRARY SHOW aus. Um die Einheitennamen für Bandlaufwerke auf einem Dateiserver unter NetApp Release ONTAP 10.0 GX oder höher abzurufen, stellen Sie mithilfe von Telnet die Verbindung zum Dateiserver her und geben Sie den Befehl SYSTEM HARDWARE TAPE DRIVE SHOW aus. Ausführliche Informationen zu diesen Befehlen finden Sie in der Produktdokumentation des NetApp ONTAP GX-Dateiservers.
- Verwenden Sie für Releases vor NetApp Release ONTAP 10.0 GX weiterhin den Befehl SYSCONFIG. Um beispielsweise die Einheitennamen für Bandarchive anzuzeigen, stellen Sie mithilfe von Telnet die Verbindung zum Dateiserver her und geben Sie den folgenden Befehl aus:

  ```
  sysconfig -m
  ```

  Geben Sie folgenden Befehl aus, um die Einheitennamen für Bandlaufwerke anzuzeigen:

  ```
  sysconfig -t
  ```

- Führen Sie für Laufwerke, die über Fibre Channel angeschlossen sind, und die Celerra-Einheit zum Versetzen von Daten die folgenden Schritte aus:
  1. Melden Sie sich bei der EMC Celerra-Steuerworkstation mit einer Verwaltungs-ID an. Geben Sie den folgenden Befehl aus:

     ```
     server_devconfig server_1 -l -s -n
     ```

     Tipp: Mit der Option -l für diesen Befehl werden nur die Einheitendaten aufgelistet, die in der Datenbank der Einheit zum Versetzen von Daten gespeichert wurden. Mit dem Befehl und der Option werden keine Änderungen an der Einheitenkonfiguration angezeigt, die nach der letzten Datenbankaktualisierung auf der Einheit zum Versetzen von Daten durchgeführt wurden. Ausführliche Informationen zum Abrufen der neuesten Einheitenkonfiguration für Ihre Einheit zum Versetzen von Daten enthält die EMC Celerra-Dokumentation.
     Die Ausgabe für den Befehl server_devconfig umfasst die Einheitennamen für die Einheiten, die an die Einheit zum Versetzen von Daten angeschlossen sind. Die Einheitennamen sind in der Spalte *addr* aufgeführt, z. B.:

     ```
     server_1:
     SCSI-Einheitentabelle
     name        addr      type    info
     ```

```
tape1       c64t0l0   tape   IBM ULT3580-TD2 53Y2
ttape1      c96t0l0   tape   IBM ULT3580-TD2 53Y2
```

2. Ordnen Sie den Celerra-Einheitennamen dem weltweiten Namen (WWN, wordwide name) der Einheit zu:
   a. Um den weltweiten Namen aufzulisten, melden Sie sich bei der EMC Celerra-Steuerworkstation an und geben Sie den folgenden Befehl aus. Beachten Sie, dass Sie in diesem Befehl als erstes Zeichen einen Punkt (.) angeben müssen.

      ```
      .server_config server_# -v "fcp bind show"
      ```

      Die Ausgabe für diesen Befehl umfasst den weltweiten Namen (WWN), z. B.:

      ```
      Chain 0064: WWN 500507630f418e29 HBA 2 N_PORT Bound
      Chain 0096: WWN 500507630f418e18 HBA 2 N_PORT Bound
      ```

      Tipp: Der Befehl .server_config ist ein EMC Celerra-Befehl, der nicht dokumentiert ist. Weitere Informationen zur Verwendung dieses Befehls erhalten Sie von EMC.
   b. Identifizieren Sie die Bandeinheit, die in der Ausgabe des Befehls server_devconfig aufgelistet war und denselben weltweiten Namen (WWN) hat mithilfe der Kettennummer, z. B.:

Bandeinheitenname	Kettennummer	WWN
c64t0l0	0064	500507630f418e29
c96t0l0	0096	500507630f418e18

Das Verhalten von Celerra-Befehlen kann auf verschiedenen EMC Celerra-Systemen und Betriebssystemversionen variieren. Um ausführliche Informationen zu erhalten, lesen Sie in der EMC Celerra-Dokumentation nach oder wenden Sie sich an EMC.

Pfade zu Speicherarchiven für NDMP-Operationen definieren

Definieren Sie entweder vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver einen Pfad zu dem SCSI-Speicherarchiv.

Vorgehensweise

1. Geben Sie für ein SCSI-Speicherarchiv, das mit IBM Spectrum Protect verbunden ist, den folgenden Beispielbefehl aus, um einen Pfad von dem Server mit dem Namen SERVER1 zu dem SCSI-Speicherarchiv mit dem Namen TSMLIB zu definieren:

    AIX-Betriebssysteme

   ```
   define path server1 tsmlib srctype=server desttype=library
           device=/dev/lb1
   ```

    Linux-Betriebssysteme

   ```
   define path server1 tsmlib srctype=server desttype=library
           device=/dev/tsmscsi/lb1
   ```

    Windows-Betriebssysteme

   ```
   define path server1 tsmlib srctype=server desttype=library
          device=lb0.0.0.2
   ```

2. Geben Sie für ein SCSI-Speicherarchiv, das mit einem NAS-Dateiserver verbunden ist, den folgenden Beispielbefehl aus, um einen Pfad zwischen einer NetApp-NAS-Einheit zum Versetzen von Daten mit dem Namen NASNODE1 und einem Speicherarchiv mit dem Namen NASLIB zu definieren:

   ```
   define path nasnode1 naslib srctype=datamover desttype=library device=mc0
   ```

3. Definieren Sie für ein 349X-Speicherarchiv einen Pfad vom IBM Spectrum Protect-Server zum Speicherarchiv. Geben Sie beispielsweise den folgenden Befehl ein, um einen Pfad vom Server mit dem Namen SERVER1 zum 349X-Speicherarchiv mit dem Namen TSMLIB zu definieren:

    AIX-Betriebssysteme

   ```
   define path server1 tsmlib srctype=server desttype=library
           device=/dev/lmcp0
   ```

    Linux-Betriebssysteme  Windows-Betriebssysteme

   ```
   define path server1 tsmlib srctype=server desttype=library
    device=library1
   ```

   Tipp: Der Befehl DEFINE PATH ist für ein ACSLS-Speicherarchiv nicht erforderlich.

NDMP-Operationen planen

Sie können Sicherungs- oder Zurückschreibungsoperationen für Images planen, die von NDMP-Operationen erstellt werden. Verwenden Sie Verwaltungszeitpläne, die den Verwaltungsbefehl BACKUP NODE oder RESTORE NODE verarbeiten.

Vorgehensweise

Erstellen Sie einen Verwaltungszeitplan mit dem Befehl DEFINE SCHEDULE. Um beispielsweise einen Verwaltungszeitplan mit dem Namen NASSCHED zu erstellen, um alle Dateisysteme für den Knoten NASNODE1 zu sichern, geben Sie den folgenden Befehl ein:

```
define schedule nassched type=administrative cmd='backup node nasnode1' active=yes
starttime=20:00 period=1 perunits=days
```

Der Zeitplan ist aktiv und wird jeden Tag um 20 Uhr ausgeführt.
Einschränkung: Die Befehle BACKUP NODE und RESTORE NODE können nur für Knoten mit TYPE=NAS verwendet werden.
Zugehörige Tasks:
Zeitplan für tägliche Operationen optimieren
Zugehörige Verweise:
BACKUP NODE (NAS-Knoten sichern)
RESTORE NODE (NAS-Knoten zurückschreiben)
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

Virtuelle Dateibereiche definieren

Verwenden Sie die Definition eines virtuellen Dateibereichs, um NAS-Sicherungen auf Verzeichnisebene auszuführen. Um die Sicherungs- und Zurückschreibungszeiten für große Dateisysteme zu reduzieren, ordnen Sie einen Verzeichnispfad von einem NAS-Dateiserver zum Namen eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server zu.

Vorgehensweise

Um den Namen eines virtuellen Dateibereichs für den Verzeichnispfad auf der NAS-Einheit zu erstellen, geben Sie den Befehl DEFINE VIRTUALFSMAPPING aus:

```
define virtualfsmapping nas1 /mikesdir /vol/vol1 /mikes
```

Mit diesem Befehl wird der Name des virtuellen Dateibereichs /MIKESDIR auf dem Server definiert, der den Verzeichnispfad /VOL/VOL1/MIKES auf dem NAS-Dateiserver darstellt, der durch Knoten NAS1 dargestellt wird. Weitere Informationen finden Sie in Sicherung und Zurückschreibung auf Verzeichnisebene für NDMP-Operationen.

Daten mit der Band-zu-Band-Kopierfunktion sichern

Wenn Sie die NDMP-Band-zu-Band-Kopierfunktion zum Sichern von Daten verwenden, kann der Speicherarchivtyp SCSI, 349X oder ACSLS (Automated Cartridge System Library Software) sein. Laufwerke können von den NAS-Einheiten und dem IBM Spectrum Protect-Server gemeinsam genutzt werden.

Informationen zu diesem Vorgang

Wenn Sie die NDMP-Band-zu-Band-Kopierfunktion verwenden, könnte Ihr Konfigurationssetup Auswirkungen auf die Leistung bei der Back-End-Datenversetzung in IBM Spectrum Protect haben.

Vorgehensweise

Um eine einzelne NAS-Einheit mit Pfaden zu vier Laufwerken in einem Speicherarchiv zu definieren, verwenden Sie den Befehl MOVE DATA, nachdem Sie Ihr Konfigurationssetup abgeschlossen haben. Damit werden Daten auf dem Datenträger VOL1 auf alle verfügbaren Datenträger in demselben Speicherpool wie VOL1 versetzt:

```
move data vol1
```

Daten mit der Band-zu-Band-Kopierfunktion versetzen

Um Daten unter Verwendung der NDMP-Band-zu-Band-Kopieroperation von einer vorherigen Bandtechnologie in in eine neue Bandtechnologie zu versetzen, müssen Sie die Standardschritte in Ihrem Konfigurationssetup sowie weitere Schritte ausführen.

Informationen zu diesem Vorgang

Wenn Sie die NDMP-Band-zu-Band-Kopierfunktion verwenden, könnte Ihr Konfigurationssetup Auswirkungen auf die Leistung bei der Back-End-Datenversetzung in IBM Spectrum Protect haben.

Vorgehensweise

Führen Sie zusätzlich zu den Standardschritten in Ihrem Konfigurationssetup die folgenden Schritte aus:

1. Definieren Sie ein einzelnes Laufwerk in dem Speicherarchiv lib1, das über die vorherige Bandtechnologie verfügt:

   ```
   define drive lib1 drv1 element=1035
   ```

2. Definieren Sie ein Laufwerk in dem Speicherarchiv lib2, das über die neue Bandtechnologie verfügt:

   ```
   define drive lib2 drv1 element=1036
   ```

3. Definieren Sie Pfade vom NAS-Dateiserver zu jedem Laufwerk:

   ```
   define path nas1 drv1 sourcetype=datamover desttype=drive library=lib1 device=rst1l
   define path nas1 drv1 sourcetype=datamover desttype=drive library=lib2 device=rst2l
   ```

4. Versetzen Sie Daten auf dem Datenträger vol1 in dem primären Speicherpool auf die Datenträger in einem anderen primären Speicherpool nasprimpool2:

   ```
   move data vol1 stgpool=nasprimpool2
   ```

IBM Spectrum Protect für NDMP-Operationen in einer NetApp-Clusterumgebung konfigurieren

Sie können Daten von einem NetApp-Cluster auf einer direkt angeschlossenen Bandeinheit oder einem IBM Spectrum Protect-Server sichern, der die Daten in einem Speicherpool speichert. Sie können den gesamten Cluster auf einem einzigen IBM Spectrum Protect-Knoten oder Teile des Clusters auf mehreren Knoten sichern.

Vorbereitende Schritte

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

Informationen zu diesem Vorgang

Sie können Daten in einer NetApp-Clusterumgebung auf den folgenden Speichermedien sichern:

Bandeinheit, die direkt an einen NAS-Dateiserver angeschlossen ist
: Sie können Daten auf einer Bandeinheit sichern, die direkt an einen NAS-Dateiserver angeschlossen ist. Dies ist die bevorzugte Methode. In der Regel erfolgt die Sicherung von Daten auf einer direkt angeschlossenen Bandeinheit schneller als die Sicherung von Daten in einem IBM Spectrum Protect-Speicherpool mithilfe einer Netzverbindung.

Speicherpool in der lokalen IBM Spectrum Protect-Hierarchie
: Sie können Daten auf einem IBM Spectrum Protect-Server sichern, der die Daten in einem Speicherpool des Typs DISK, FILE oder Band speichert. Das Speichern von Daten in einem Speicherpool hat den Vorteil, dass Sie die Daten replizieren können, um den Datenschutz zu verbessern. Sie können vorhandene Speicherpools verwenden oder Speicherpools erstellen. Zwischen dem NAS-Dateiserver und dem IBM Spectrum Protect-Server muss eine Netzverbindung vorhanden sein. Die Netzverbindung muss über genügend Bandbreite für die Übertragung der NAS-Sicherungsdaten verfügen.
  Tipp: Dieser Sicherungstyp wird manchmal auch als 'Sicherung vom Dateiserver auf den Server' bezeichnet.

Sie können eine der folgenden Sicherungsmethoden verwenden:

Clustergesamtsicherung
: Wenn Sie diese Methode anwenden, ist ein einzelner IBM Spectrum Protect-Knoten Eigner der Sicherungsdaten des gesamten Clusters. Selbst wenn die Datenträger innerhalb des Clusters verschoben werden, werden Clustergesamtsicherungsoperationen fortgesetzt und Sie müssen Sicherungsoperationen nicht rekonfigurieren. Dies ist die bevorzugte Methode.

Clusterteilsicherung
: Wenn Sie diese Methode anwenden, geben Sie eine NetApp Storage Virtual Machine (SVM) an, die den Bereich der Sicherungsoperation angibt. Die SVM ist ein virtueller Server, der Zugriff auf einen Teil eines Clusters bereitstellt. Sie können angeben, dass jede SVM in dem Cluster Daten auf einem anderen IBM Spectrum Protect-Knoten sichert. Diese Methode erfordert eine umfangreichere Konfiguration als die Clustergesamtsicherungsmethode sowie eine Netzverbindung für die Übertragung von Daten von der SVM auf den IBM Spectrum Protect-Knoten.
  Einschränkung: Sie können diese Methode nicht verwenden, um Daten auf einer Bandeinheit zu sichern, da SVMs keinen direkten Zugriff auf Bandeinheiten haben.

Vorgehensweise

1. Wählen Sie die Speichermedien auf der Basis der folgenden Fragen aus:

Frage	Speichermedien

Frage	Speichermedien
Ist es aufgrund Ihrer Geschäftsanforderungen erforderlich, Daten auf einer lokalen Bandeinheit zu sichern?	Lautet die Antwort 'Ja', verwenden Sie eine direkt angeschlossene Bandeinheit. Lautet die Antwort 'Nein', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool.
Sind für Ihr Unternehmen Hochgeschwindigkeitssicherungsoperationen erforderlich?	Lautet die Antwort 'Ja', verwenden Sie eine direkt angeschlossene Bandeinheit. Lautet die Antwort 'Nein', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool.
Verfügt Ihr Unternehmen über genügend Netzbandbreite für NAS-Sicherungsdaten?	Lautet die Antwort 'Ja', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool. Lautet die Antwort 'Nein', verwenden Sie eine direkt angeschlossene Bandeinheit.
Möchte Ihr Unternehmen mithilfe der Replikation den Datenschutz verbessern?	Lautet die Antwort 'Ja', verwenden Sie einen lokalen IBM Spectrum Protect-Speicherpool. Lautet die Antwort 'Nein', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool.
Befinden sich Ihre NAS-Dateiserver an fernen Standorten ohne Zugriff auf direkt angeschlossene Bandarchive?	Lautet die Antwort 'Ja', verwenden Sie einen lokalen IBM Spectrum Protect-Speicherpool. Lautet die Antwort 'Nein', verwenden Sie entweder eine direkt angeschlossene Bandeinheit oder einen lokalen IBM Spectrum Protect-Speicherpool.

2. Wählen Sie eine Sicherungsmethode auf der Basis der folgenden Fragen aus:

Frage	Sicherungsmethode
Ist es aufgrund Ihrer Geschäftsanforderungen erforderlich, Daten auf einer direkt angeschlossenen Bandeinheit zu sichern?	Lautet die Antwort 'Ja', verwenden Sie die Gesamtsicherungsmethode. Lautet die Antwort 'Nein', verwenden Sie entweder die Gesamt- oder die Teilsicherungsmethode.
Verfügt Ihr System über genügend Netzbandbreite, um mehrere SVMs ohne Auswirkungen auf die Netzleistung sichern zu können?	Lautet die Antwort 'Ja', verwenden Sie entweder die Gesamt- oder die Teilsicherungsmethode. Lautet die Antwort 'Nein', verwenden Sie die Gesamtsicherungsmethode. Die Teilsicherungsmethode kann sich unter Umständen negativ auf die Systemleistung auswirken.
Sind die SVMs über mehrere Unternehmen verteilt? Werden beispielsweise SVMs durch Dritte wie Cloudplattformprovider gesteuert?	Lautet die Antwort 'Ja', verwenden Sie die Teilsicherungsmethode, da SVM-Eigner Sicherungsoperationen für einzelne SVMs steuern können. Wenn ein SVM-Eigner auch Eigner eines IBM Spectrum Protect-Servers ist, kann der Eigner Sicherungsoperationen von der SVM zu einem Serverknoten konfigurieren. Auf diese Art und Weise kann der Eigner den End-to-End-Prozess steuern. Lautet die Antwort 'Nein', verwenden Sie entweder die Gesamt- oder die Teilsicherungsmethode.

3. Konfigurieren Sie die Systemumgebung auf der Basis der ausgewählten Speichermedien und der ausgewählten Sicherungsmethode. Führen Sie die Anweisungen für die von Ihnen ausgewählte Methode aus:
   - Clustergesamtsicherungen auf direkt angeschlossene Bandeinheiten konfigurieren
   - Clustergesamtsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren
   - Clusterteilsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren

   Tipp: Wenn Sie IBM Spectrum Protect zum Sichern von NetApp-Clustern mithilfe von NDMP auf Knotenebene konfiguriert haben, ziehen Sie die Rekonfiguration von IBM Spectrum Protect für die Verwendung von NDMP Cluster Aware Backup (CAB) in Erwägung. Auf diese Art und Weise können Sie Sicherungsoperationen für NetApp-Cluster optimieren. Führen Sie die Anweisungen in IBM Spectrum Protect für die Optimierung von Clustersicherungen rekonfigurieren aus.

- Clustergesamtsicherungen auf direkt angeschlossene Bandeinheiten konfigurieren
  Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster auf eine direkt angeschlossene Bandeinheit konfigurieren.
- Clustergesamtsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren
  Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster mit einem IBM Spectrum Protect-Server als Ziel konfigurieren, der die Daten in einem Speicherpool speichert. Selbst wenn Datenträger innerhalb des Clusters verschoben werden, werden Sicherungsoperationen fortgesetzt und es ist keine Rekonfiguration erforderlich.
- Clusterteilsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren
  Sie können IBM Spectrum Protect für die Ausführung einer Teilsicherung eines NetApp-Clusters konfigurieren. Diese Methode ist geeignet, wenn mehrere Unternehmen Eigner von Daten in dem Cluster sind. Jedes Unternehmen kann Sicherungsoperationen für seine Daten verwalten.
- IBM Spectrum Protect für die Optimierung von Clustersicherungen rekonfigurieren
  Wenn Sie IBM Spectrum Protect zum Sichern von NetApp-Clustern mithilfe von NDMP auf Knotenebene konfiguriert haben, können Sie

IBM Spectrum Protect für die Verwendung von NDMP Cluster Aware Backup (CAB) rekonfigurieren. Auf diese Art und Weise können Sie Sicherungsoperationen für NetApp-Cluster optimieren.

Clustergesamtsicherungen auf direkt angeschlossene Bandeinheiten konfigurieren

Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster auf eine direkt angeschlossene Bandeinheit konfigurieren.

Vorbereitende Schritte

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher auf Ihrem NetApp-Dateiserver installiert ist, verwenden Sie die folgende Prozedur. Nach der Konfiguration Ihres NetApp-Dateiservers für den gemeinsamen Einsatz mit IBM Spectrum Protect können Sie die Erweiterung NetApp Cluster Aware Backup (CAB) zum Sichern aller Datenträger verwenden.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher nicht auf Ihrem NetApp-Dateiserver installiert ist, sichern Sie Daten anhand der Anweisungen in IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren.

Informationen zu diesem Vorgang

Die bevorzugte Methode ist das Sichern des gesamten Clusters unter Verwendung eines Knotens und einer Einheit zum Versetzen von Daten, die dem clusterweiten Netz zugeordnet sind. Auf diese Art und Weise wird sichergestellt, dass ein einzelner IBM Spectrum Protect-Knoten Eigner der Sicherungsdaten ist. Selbst wenn Datenträger innerhalb des Clusters verschoben werden, werden Sicherungsoperationen fortgesetzt und es ist keine Rekonfiguration erforderlich.

Vorgehensweise

Um Clustergesamtsicherungsoperationen auf eine direkt angeschlossene Bandeinheit zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass IBM Spectrum Protect Extended Edition installiert und die Lizenz registriert ist. Wenn die Lizenz nicht registriert ist, geben Sie den folgenden IBM Spectrum Protect-Befehl aus:

   ```
   register license file=tsmee.lic
   ```

2. Fordern Sie Clusteradministratorberechtigungen für den NetApp-Dateiserver an. Dieser Schritt ist für den Zugriff auf die Clusterkonsole erforderlich.
3. Aktivieren Sie auf dem NetApp-Dateiserver die Verwendung von NDMP, indem Sie die Anweisungen in der Veröffentlichung *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide* ausführen. Führen Sie die folgenden Schritte aus:
   a. Aktivieren Sie auf Clusterebene NDMP-Sicherungsoperationen auf SVM-Ebene. Auf diese Art und Weise inaktivieren Sie auf dem NAS-Dateiserver NDMP-Sicherungsoperationen auf Knotenebene. Stellen Sie sicher, dass die Option node-scoped-ndmp auf dem NAS-Dateiserver auf OFF gesetzt ist.
   b. Erstellen Sie eine Sicherungsbenutzer-ID für NDMP-Operationen.
   c. Konfigurieren Sie eine Netzschnittstelle für NDMP-Steuerverbindungen auf Clusterebene.
4. Registrieren Sie den IBM Spectrum Protect-Knoten, der Eigner aller Sicherungsdaten für den Cluster werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl REGISTER NODE aus:

   ```
   register node Knotenname Kennwort domain=NAS-Domäne type=nas
   ```

   Dabei gibt *Knotenname* den Knotennamen, *Kennwort* das Knotenkennwort und *NAS-Domäne* die Domäne des Knotens an. Ordnen Sie den Knoten einer Domäne zu, die über eine Maßnahme zum Sichern von Daten in einem entsprechenden Speicherpool verfügt.
5. Bestimmen Sie die IP-Adresse der NetApp-Cluster-Managementschnittstelle auf dem NAS-Dateiserver. Die Schnittstelle stellt Zugriff auf den gesamten Cluster bereit. Geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Betriebssystembefehl aus:

   ```
   network interface show -role cluster-mgmt
   ```

   Die IP-Adresse, die in der Befehlsausgabe angezeigt wird, ist erforderlich, wenn Sie den Parameter HLADDRESS in Schritt 6 angeben.
6. Definieren Sie eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Knoten, der Eigner der Sicherungsdaten werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl DEFINE DATAMOVER in einer einzigen Zeile aus:

   ```
   define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nascluster
   hladdress=Cluster-Managementschnittstelle lladdress=Port
   USER=Benutzername password=Kennwort dataformat=netappdump
   ```

   Dabei ist *Cluster-Managementschnittstelle* der Wert aus Schritt 5 und *Name_der_Einheit_zum_Versetzen_von_Daten* der in Schritt 4 registrierte Knotenname. Informationen zur Angabe der anderen Parameter finden Sie in DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren).

Tipp: Nach dem Definieren der Einheit zum Versetzen von Daten werden weitere Einheiten zum Versetzen von Daten automatisch für jeden Knoten in dem Cluster definiert. Der Name der jeweiligen Einheit zum Versetzen von Daten stimmt mit dem Namen des physischen Knotens in dem Cluster überein. Diese Einheiten zum Versetzen von Daten werden beim Definieren von Pfaden zu Bandlaufwerken in Schritt 3 in Bandeinheiten für Clustergesamtsicherungen konfigurieren verwendet.

Nächste Schritte

Um die Bandeinheit für die Clustergesamtsicherung zu konfigurieren, führen Sie die Anweisungen in Bandeinheiten für Clustergesamtsicherungen konfigurieren aus.

- Bandeinheiten für Clustergesamtsicherungen konfigurieren
  Wenn Sie planen, alle Datenträger in einem NetApp-Cluster auf einer direkt angeschlossenen Bandeinheit zu sichern, müssen Sie die Bandeinheit konfigurieren.

Zugehörige Verweise:
REGISTER NODE (Knoten registrieren)

Clustergesamtsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren

Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster mit einem IBM Spectrum Protect-Server als Ziel konfigurieren, der die Daten in einem Speicherpool speichert. Selbst wenn Datenträger innerhalb des Clusters verschoben werden, werden Sicherungsoperationen fortgesetzt und es ist keine Rekonfiguration erforderlich.

Vorbereitende Schritte

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher auf Ihrem NetApp-Dateiserver installiert ist, verwenden Sie die folgende Prozedur. Nach der Konfiguration Ihres NetApp-Dateiservers für den gemeinsamen Einsatz mit IBM Spectrum Protect können Sie die Erweiterung NetApp Cluster Aware Backup (CAB) zum Sichern aller Datenträger in dem Cluster verwenden. Ein einzelner IBM Spectrum Protect-Knoten wird zum Eigner aller gesicherten Daten.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher nicht auf Ihrem NetApp-Dateiserver installiert ist, sichern Sie Daten anhand der Anweisungen in IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren.

Vorgehensweise

1. Stellen Sie sicher, dass IBM Spectrum Protect Extended Edition installiert und die Lizenz registriert ist. Wenn die Lizenz nicht registriert ist, geben Sie den folgenden IBM Spectrum Protect-Befehl aus:

   ```
   register license file=tsmee.lic
   ```

2. Fordern Sie Clusteradministratorberechtigungen für den NetApp-Dateiserver an. Dieser Schritt ist für den Zugriff auf die Clusterkonsole erforderlich.
3. Aktivieren Sie die Verwendung von NDMP, indem Sie die Anweisungen in der Veröffentlichung *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide* ausführen. Führen Sie die folgenden Schritte aus:
   a. Aktivieren Sie NetApp SVM, um NDMP-Sicherungsoperationen auf Clusterebene steuern zu können.
   b. Erstellen Sie eine Sicherungsbenutzer-ID für NDMP-Operationen.
   c. Konfigurieren Sie eine Netzschnittstelle für NDMP-Steuerverbindungen auf Clusterebene.
4. Registrieren Sie den IBM Spectrum Protect-Knoten, der Eigner aller Sicherungsdaten für den Cluster werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl REGISTER NODE aus:

   ```
   register node Knotenname Kennwort domain=NAS-Domäne type=nas
   ```

   Dabei gibt *Knotenname* den Knotennamen, *Kennwort* das Knotenkennwort und *NAS-Domäne* die Domäne des Knotens an.
5. Bestimmen Sie die numerische IP-Adresse oder den Domänennamen für den Zugriff auf den NAS-Dateiserver. Die Schnittstelle stellt Zugriff auf den gesamten Cluster bereit. Geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Betriebssystembefehl aus:

   ```
   network interface show -role cluster-mgmt
   ```

   Die IP-Adresse in der Ausgabe ist erforderlich, wenn Sie einen Wert für den Parameter HLADDRESS in Schritt 6 angeben.
6. Definieren Sie eine Einheit zum Versetzen von Daten für den Knoten, indem Sie den Befehl DEFINE DATAMOVER unter Angabe von `TYPE=NASCLUSTER` ausgeben. Geben Sie auf dem IBM Spectrum Protect-Server den folgenden Befehl in einer einzigen Zeile aus:

   ```
   define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nascluster
   hladdress=Cluster-Managementschnittstelle lladdress=Port
   USER=Benutzername password=Kennwort dataformat=netappdump
   ```

Dabei ist *Cluster-Managementschnittstelle* der Wert aus Schritt 5 und *Name_der_Einheit_zum_Versetzen_von_Daten* der in Schritt 4 registrierte Knotenname. Informationen zur Angabe der anderen Parameter finden Sie in DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren).

7. Konfigurieren Sie eine IBM Spectrum Protect-Maßnahme für die Verwaltung von NAS-Imagesicherungen. Führen Sie die Anweisungen in IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren aus.
8. Aktualisieren Sie den in Schritt 4 registrierten Clusterknoten für die in Schritt 7 konfigurierte Domäne. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl UPDATE NODE aus:

   ```
   update node Knotenname domain=Domänenname
   ```

9. Optional: Ermitteln Sie die Datenträger in dem Cluster und planen Sie Sicherungen für die Datenträger:
   a. Ermitteln Sie auf dem NAS-Dateiserver die Datenträger in dem Cluster, indem Sie den folgenden Data ONTAP-Befehl ausgeben:

      ```
      volume show
      ```

   b. Planen Sie Sicherungsoperationen, indem Sie die Anweisungen in NDMP-Operationen planen ausführen.

Nächste Schritte

Die folgenden Tasks sind optional:

- Um zu überprüfen, ob die Datenträger in dem NetApp-Cluster gesichert wurden, führen Sie die folgenden Schritte aus:
  1. Klicken Sie in der Menüleiste des Operations Center auf Clients.
  2. Klicken Sie doppelt auf einen NAS-Einheitenclient und klicken Sie auf Datenträger.
  3. Um zu bestimmen, wann die letzte Datenträgergesamtsicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Gesamtsicherung'. Um zu bestimmen, wann die letzte Differenzsicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Differenzsicherung'.
- Um Kopienspeicherpools für verbesserten Datenschutz zu konfigurieren, konfigurieren Sie die Band-zu-Band-Kopierfunktion zum Sichern von Daten. Anweisungen finden Sie in Daten mit der Band-zu-Band-Kopierfunktion sichern.

Zugehörige Verweise:
REGISTER NODE (Knoten registrieren)

Clusterteilsicherungen mit einem IBM Spectrum Protect-Server als Ziel konfigurieren

Sie können IBM Spectrum Protect für die Ausführung einer Teilsicherung eines NetApp-Clusters konfigurieren. Diese Methode ist geeignet, wenn mehrere Unternehmen Eigner von Daten in dem Cluster sind. Jedes Unternehmen kann Sicherungsoperationen für seine Daten verwalten.

Vorbereitende Schritte

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher auf Ihrem NetApp-Dateiserver installiert ist, verwenden Sie die folgende Prozedur. Nach der Konfiguration Ihres NetApp-Dateiservers für den gemeinsamen Einsatz mit IBM Spectrum Protect können Sie die Erweiterung NetApp Cluster Aware Backup (CAB) zum Sichern eines Teils eines Clusters verwenden. Wenn Sie eine Clusterteilsicherung konfigurieren, legen Sie den Bereich der Sicherung fest, indem Sie einen virtuellen Server, die NetApp Storage Virtual Machine (SVM), angeben. Die SVM stellt Zugriff auf einen Teil eines Clusters bereit.

Wenn das Betriebssystem NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher nicht auf Ihrem NetApp-Dateiserver installiert ist, sichern Sie Daten anhand der Anweisungen in IBM Spectrum Protect für NDMP-Operationen in einer Umgebung ohne Clustering konfigurieren.

Vorgehensweise

1. Stellen Sie sicher, dass IBM Spectrum Protect Extended Edition installiert und die Lizenz registriert ist. Wenn die Lizenz nicht registriert ist, geben Sie den folgenden IBM Spectrum Protect-Befehl aus:

   ```
   register license file=tsmee.lic
   ```

2. Fordern Sie Clusteradministratorberechtigungen für den NetApp-Dateiserver an. Dieser Schritt ist für den Zugriff auf die Clusterkonsole erforderlich.
3. Aktivieren Sie auf dem NetApp-Dateiserver die Verwendung von NDMP, indem Sie die Anweisungen in der Veröffentlichung *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide* ausführen. Führen Sie die folgenden Schritte aus:
   a. Aktivieren Sie NetApp SVM, um NDMP-Sicherungsoperationen steuern zu können.
   b. Erstellen Sie eine Sicherungsbenutzer-ID für NDMP-Operationen.
   c. Konfigurieren Sie eine Netzschnittstelle für NDMP-Steuerverbindungen auf SVM-Ebene.
4. Registrieren Sie den IBM Spectrum Protect-Knoten, der Eigner der gesicherten Daten werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl REGISTER NODE aus:

```
register node Knotenname Kennwort domain=NAS-Domäne type=nas
```

Dabei gibt *Knotenname* den Knotennamen, *Kennwort* das Knotenkennwort und *NAS-Domäne* die Domäne des Knotens an.

5. Bestimmen Sie die numerische IP-Adresse oder den Domänennamen der Clusterschnittstelle, die von der SVM verwendet wird. Um den Wert zu bestimmen, geben Sie auf dem NAS-Dateiserver den folgenden ONTAP-Betriebssystembefehl aus:

   ```
   network interface show -vserver Vserver-Name -role data
   ```

   Dabei gibt *Vserver-Name* den Namen der SVM an. Dieser Wert ist in Schritt 6 erforderlich.
6. Definieren Sie eine zugehörige Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Knoten, indem Sie den Befehl DEFINE DATAMOVER unter Angabe von `TYPE=NASVSERVER` ausgeben. Geben Sie auf dem IBM Spectrum Protect-Server den folgenden Befehl in einer einzigen Zeile aus:

   ```
   define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nasvserver
   hladdress=SVM-Datenschnittstelle lladdress=Port
   USER=Benutzername password=Kennwort dataformat=netappdump
   ```

   Dabei ist *SVM-Datenschnittstelle* der Wert aus Schritt 5 und *Name_der_Einheit_zum_Versetzen_von_Daten* der Name des in Schritt 4 registrierten Knotens.

   Informationen zur Angabe der anderen Parameter finden Sie in DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren).

7. Konfigurieren Sie eine IBM Spectrum Protect-Maßnahme für die Verwaltung von NAS-Imagesicherungen. Führen Sie die Anweisungen in IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren aus.
8. Aktualisieren Sie den in Schritt 4 registrierten Knoten für die in Schritt 7 konfigurierte Domäne. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl UPDATE NODE aus:

   ```
   update node Knotenname domain=Domänenname
   ```

9. Optional: Ermitteln Sie die Datenträger in dem Cluster und planen Sie Sicherungsoperationen. Führen Sie die folgenden Schritte aus:
   a. Ermitteln Sie auf dem NAS-Dateiserver die Datenträger in dem Cluster, indem Sie den folgenden Data ONTAP-Befehl ausgeben:

      ```
      volume show -vserver Vserver-Name
      ```

      Dabei gibt *Vserver-Name* den Namen der SVM an.
   b. Planen Sie Sicherungsoperationen, indem Sie die Anweisungen in NDMP-Operationen planen ausführen.

Nächste Schritte

Um zu überprüfen, ob die Datenträger in dem NetApp-Cluster gesichert wurden, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Clients.
2. Klicken Sie doppelt auf einen NAS-Einheitenclient und klicken Sie auf Datenträger.
3. Um zu bestimmen, wann die letzte Datenträgergesamtsicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Gesamtsicherung'. Um zu bestimmen, wann die letzte Differenzsicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Differenzsicherung'.

Zugehörige Verweise:
REGISTER NODE (Knoten registrieren)

IBM Spectrum Protect für die Optimierung von Clustersicherungen rekonfigurieren

Wenn Sie IBM Spectrum Protect zum Sichern von NetApp-Clustern mithilfe von NDMP auf Knotenebene konfiguriert haben, können Sie IBM Spectrum Protect für die Verwendung von NDMP Cluster Aware Backup (CAB) rekonfigurieren. Auf diese Art und Weise können Sie Sicherungsoperationen für NetApp-Cluster optimieren.

Vorbereitende Schritte

Eine Übersicht über die NDMP-Funktionalität in IBM Spectrum Protect- und NetApp-Dateiservern finden Sie in der Technote 7046965. In dieser Technote sind auch die Systemvoraussetzungen aufgelistet.

Informationen zu diesem Vorgang

Wenn Sie IBM Spectrum Protect für die Verwendung von CAB rekonfigurieren, können Sie Sicherungsoperationen wie folgt optimieren:

- Sie können IBM Spectrum Protect für die Sicherung aller Datenträger in einem NetApp-Cluster auf eine direkt angeschlossene Bandeinheit oder auf einen IBM Spectrum Protect-Server konfigurieren. In beiden Fällen ist ein einzelner IBM Spectrum Protect-Knoten Eigner der Daten. Selbst wenn Datenträger innerhalb des Clusters verschoben werden, werden Sicherungsoperationen fortgesetzt und es ist keine Rekonfiguration erforderlich.

- Sie können eine Teilsicherung eines NetApp-Clusters auf einen IBM Spectrum Protect-Server ausführen. Diese Methode ist geeignet, wenn mehrere Unternehmen Eigner von Daten in dem Cluster sind. Jedes Unternehmen kann Sicherungsoperationen für seine Daten verwalten. Sie legen den Bereich einer Teilsicherung fest, indem Sie eine NetApp Storage Virtual Machine (SVM) angeben, die Zugriff auf einen Teil eines Clusters bereitstellt.

Um IBM Spectrum Protect für die Verwendung von CAB zu rekonfigurieren, müssen Sie einen neuen IBM Spectrum Protect-Knoten und eine neue Einheit zum Versetzen von Daten definieren.

Vorgehensweise

1. Stellen Sie sicher, dass NetApp Clustered Data ONTAP 8.2 oder höher oder 9.1 oder höher auf dem NetApp-Dateiserver installiert ist.
2. Aktivieren Sie die Verwendung von NDMP, indem Sie die Anweisungen in der Veröffentlichung *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide* ausführen. Führen Sie eine der folgenden Aktionen aus:

   Für eine Clustergesamtsicherung
   Führen Sie die folgenden Schritte aus:
   a. Aktivieren Sie auf Clusterebene NDMP-Sicherungsoperationen auf SVM-Ebene. Auf diese Art und Weise inaktivieren Sie auf dem NAS-Dateiserver NDMP-Sicherungsoperationen auf Knotenebene. Stellen Sie sicher, dass die Option node-scoped-ndmp auf dem NAS-Dateiserver auf OFF gesetzt ist.
   b. Erstellen Sie eine Sicherungsbenutzer-ID für NDMP-Operationen.
   c. Konfigurieren Sie eine Netzschnittstelle für NDMP-Steuerverbindungen auf Clusterebene.

   Für eine Clusterteilsicherung
   Führen Sie die folgenden Schritte aus:
   a. Aktivieren Sie NDMP auf SVM-Ebene, um NDMP-Sicherungsoperationen steuern zu können.
   b. Erstellen Sie eine Sicherungsbenutzer-ID für NDMP-Operationen.
   c. Konfigurieren Sie eine Netzschnittstelle für NDMP-Steuerverbindungen auf SVM-Ebene.

3. Registrieren Sie den IBM Spectrum Protect-Knoten, der Eigner der Sicherungsdaten werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl REGISTER NODE aus:

   ```
   register node Knotenname Kennwort domain=NAS-Domäne type=nas
   ```

   Dabei gibt *Knotenname* den Knotennamen, *Kennwort* das Knotenkennwort und *NAS-Domäne* die Domäne des Knotens an.
4. Wenn Sie planen, einen gesamten Cluster zu sichern, bestimmen Sie die IP-Adresse der NetApp-Cluster-Managementschnittstelle auf dem NAS-Dateiserver. Die Schnittstelle stellt Zugriff auf den gesamten Cluster bereit. Geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Betriebssystembefehl aus:

   ```
   network interface show -role cluster-mgmt
   ```

   Die IP-Adresse in der Ausgabe ist erforderlich, wenn Sie den Parameter HLADDRESS in Schritt 6 angeben.
5. Wenn Sie planen, einen Teil eines Clusters zu sichern, bestimmen Sie die numerische IP-Adresse oder den Domänennamen der Clusterschnittstelle, die von der SVM verwendet wird. Um den Wert zu bestimmen, geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Betriebssystembefehl aus:

   ```
   network interface show -vserver Vserver-Name -role data
   ```

   Dabei gibt *Vserver-Name* den Namen der SVM an. Der abgerufene Wert ist in Schritt 6 erforderlich.
6. Definieren Sie eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Knoten. Führen Sie eine der folgenden Aktionen aus:

   Für eine Clustergesamtsicherung
   Definieren Sie eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Knoten, der Eigner der Sicherungsdaten werden soll. Geben Sie auf dem IBM Spectrum Protect-Server den Befehl DEFINE DATAMOVER in einer einzigen Zeile aus:

   ```
   define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nascluster
   hladdress=Cluster-Managementschnittstelle lladdress=Port
   USER=Benutzername password=Kennwort dataformat=netappdump
   ```

   Dabei ist *Cluster-Managementschnittstelle* der Wert aus Schritt 4 und *Name_der_Einheit_zum_Versetzen_von_Daten* der in Schritt 3 registrierte Knotenname.
   Tipp: Nach dem Definieren der Einheit zum Versetzen von Daten werden weitere Einheiten zum Versetzen von Daten automatisch für jeden Knoten in dem Cluster definiert. Der Name der jeweiligen Einheit zum Versetzen von Daten stimmt mit dem Namen des physischen Knotens in dem Cluster überein. Diese Einheiten zum Versetzen von Daten werden beim Definieren von Pfaden zu Bandlaufwerken verwendet, die an den Cluster angeschlossen sind.

   Für eine Clusterteilsicherung
   Definieren Sie eine Einheit zum Versetzen von Daten für den Knoten, indem Sie den Befehl DEFINE DATAMOVER unter Angabe von `TYPE=NASVSERVER` ausgeben. Geben Sie auf dem IBM Spectrum Protect-Server den folgenden Befehl in einer einzigen Zeile aus:

   ```
   define datamover Name_der_Einheit_zum_Versetzen_von_Daten type=nasvserver
   hladdress=SVM-Datenschnittstelle lladdress=Port
   USER=Benutzername password=Kennwort dataformat=netappdump
   ```

   Dabei ist *SVM-Datenschnittstelle* der Wert aus Schritt 5 und *Name_der_Einheit_zum_Versetzen_von_Daten* der in Schritt 3 registrierte Knotenname.

Informationen zur Angabe der anderen Parameter im Befehl DEFINE DATAMOVER finden Sie in DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren).

7. Um Daten auf eine direkt angeschlossene Bandeinheit zu sichern, ermitteln Sie für jedes Bandlaufwerk, das an den Cluster angeschlossen ist, den Einheitennamen und den physischen Knoten, an den das Laufwerk angeschlossen ist:
   a. Geben Sie auf dem NAS-Dateiserver den folgenden Data ONTAP-Befehl aus:

      ```
      storage tape show-tape-drive
      ```

   b. Prüfen Sie die Ausgabe, um die Seriennummer des Bandlaufwerks und den Knoten des Clusters, an den das Laufwerk angeschlossen ist, zu finden. Dieselbe Zeilengruppe umfasst den Einheitennamen, beispielsweise `st1`, `st2` oder `st3`.
8. Um eine Clustergesamtsicherung auf eine direkt angeschlossene Bandeinheit zu konfigurieren, führen Sie die Anweisungen in Bandeinheiten für Clustergesamtsicherungen konfigurieren aus.
9. Um eine Clustergesamt- oder Clusterteilsicherung auf einen IBM Spectrum Protect-Server zu konfigurieren, konfigurieren Sie eine Maßnahme für die Verwaltung von NAS-Imagesicherungen. Führen Sie die Anweisungen in IBM Spectrum Protect-Maßnahme für NDMP-Operationen konfigurieren aus.
10. Inaktivieren Sie geplante Sicherungsoperationen für alle Knoten, die zuvor zum Sichern des NetApp-Clusters verwendet wurden.
11. Ermitteln Sie die Datenträger in dem Cluster und planen Sie wahlweise Sicherungsoperationen für die Datenträger. Führen Sie eine der folgenden Aktionen aus:

    Für eine Clustergesamtsicherung
    a. Ermitteln Sie auf dem NAS-Dateiserver die Datenträger in dem Cluster, indem Sie den folgenden Data ONTAP-Befehl verwenden:

       ```
       volume show
       ```

    b. Führen Sie eine Gesamtsicherung des gesamten Clusters aus.
    c. Optional: Um Sicherungsoperationen zu planen, führen Sie die Anweisungen in NDMP-Operationen planen aus.

    Für eine Clusterteilsicherung
    a. Ermitteln Sie auf dem NAS-Dateiserver die Datenträger in dem Cluster, indem Sie den folgenden Data ONTAP-Befehl verwenden:

       ```
       volume show -vserver Vserver-Name
       ```

       Dabei gibt *Vserver-Name* den Namen der SVM an.
    b. Führen Sie eine Gesamtsicherung für einen Teil des Clusters aus.
    c. Optional: Um Sicherungsoperationen zu planen, führen Sie die Anweisungen in NDMP-Operationen planen aus.

Nächste Schritte

Um zu überprüfen, ob die Datenträger in dem NetApp-Cluster gesichert wurden, führen Sie die folgenden Schritte aus:

1. Klicken Sie in der Menüleiste des Operations Center auf Clients.
2. Klicken Sie doppelt auf einen NAS-Einheitenclient und klicken Sie auf Datenträger.
3. Um zu bestimmen, wann die letzte Datenträgergesamtsicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Gesamtsicherung'. Um zu bestimmen, wann die letzte Differenzsicherung ausgeführt wurde, überprüfen Sie die Informationen in der Spalte 'Letzte Differenzsicherung'.

Zugehörige Verweise:
DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren)
DEFINE PATH (Pfad definieren, wenn Ziel ein Laufwerk ist)
REGISTER NODE (Knoten registrieren)

NAS-Dateiserver mithilfe von NDMP sichern und zurückschreiben

Nach der Konfiguration von IBM Spectrum Protect für NDMP-Operationen können Sie mit der Verwendung von NDMP beginnen.

Vorgehensweise

Verwenden Sie entweder eine Clientschnittstelle oder eine Verwaltungsschnittstelle, um eine Dateisystemimagesicherung auszuführen. Um beispielsweise die Schnittstelle des Windows-Clients für Sichern/Archivieren zu verwenden, um ein Dateisystem mit dem Namen /vol/vol1 auf einem NAS-Dateiserver mit dem Namen NAS1 zu verwenden, geben Sie den folgenden Befehl aus:

```
dsmc backup nas -nasnodename=nas1 {/vol/vol1}
```

Weitere Informationen zu dem Befehl finden Sie in Sicherungsimage.
Tipp: Jedes Mal, wenn Sie die Clientschnittstelle verwenden, werden Sie aufgefordert, sich als IBM Spectrum Protect-Administrator zu authentifizieren, bevor die Operation beginnen kann. Die Administrator-ID muss mindestens über Clienteignerberechtigung für den NAS-Knoten verfügen.
Sie können dieselbe Sicherungsoperation auch mit einer Serverschnittstelle ausführen. Sichern Sie beispielsweise über den Verwaltungsbefehlszeilenclient das Dateisystem mit dem Namen /vol/vol1 auf einem NAS-Dateiserver mit dem Namen NAS1, indem Sie den folgenden Befehl ausgeben:

```
backup node nas1 /vol/vol1
```

Einschränkung: Die Befehle BACKUP NAS und BACKUP NODE schließen keine Momentaufnahmen ein. Informationen zum Sichern von Momentaufnahmen finden Sie in Mit Momentaufnahmen sichern und zurückschreiben.
Sie können das Image mit jeder der beiden Schnittstellen zurückschreiben. Sicherungen sind, unabhängig davon, ob sie mit einer Clientschnittstelle oder einer Serverschnittstelle gesichert werden, identisch. Angenommen, das in den vorherigen Beispielen gesicherte Image soll zurückgeschrieben werden. In diesem Beispiel wird das Dateisystem mit dem Namen /vol/vol1 in /vol/vol2 zurückgeschrieben. Schreiben Sie das Dateisystem mit dem folgenden Befehl, der von einer Schnittstelle des Windows-Clients für Sichern/Archivieren ausgegeben wird, zurück:

```
dsmc restore nas -nasnodename=nas1 {/vol/vol1} {/vol/vol2}
```

Sie können das Dateisystem wahlweise mithilfe einer Serverschnittstelle zurückschreiben. Um beispielsweise das Dateisystem mit dem Namen /vol/vol1 in das Dateisystem /vol/vol2 für einen NAS-Dateiserver mit dem Namen NAS1 zurückzuschreiben, geben Sie den folgenden Befehl ein:

```
restore node nas1 /vol/vol1 /vol/vol2
```

Sie können Daten von einem NAS-Anbietersystem auf ein anderes NAS-Anbietersystem zurückschreiben, wenn Sie das NDMPDUMP-Datenformat verwenden. Sie müssen jedoch entweder die Kompatibilität zwischen den Systemen überprüfen oder einen separaten Speicherpool für jeden NAS-Anbieter verwalten.

- NAS-Dateiserver: Sicherungen auf einem einzelnen IBM Spectrum Protect-Server
  Wenn mehrere NAS-Dateiserver an verschiedenen Standorten vorhanden sind, möchten Sie die Sicherungsdaten möglicherweise eher an einen einzelnen IBM Spectrum Protect-Server senden, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen.
- NDMP-Dateiserver auf einem IBM Spectrum Protect-Server sichern
  Sie können Daten auf einem einzelnen IBM Spectrum Protect-Server sichern, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen.

NAS-Dateiserver: Sicherungen auf einem einzelnen IBM Spectrum Protect-Server

Wenn mehrere NAS-Dateiserver an verschiedenen Standorten vorhanden sind, möchten Sie die Sicherungsdaten möglicherweise eher an einen einzelnen IBM Spectrum Protect-Server senden, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen.

Wenn Sie NAS-Sicherungsdaten in der Speicherhierarchie des IBM Spectrum Protect-Servers speichern, können Sie IBM Spectrum Protect-Back-End-Datenverwaltungsfunktionen anwenden. Auf diese Art und Weise können Sie die Vorteile der Umlagerung, Konsolidierung, Wiederherstellung nach einem Katastrophenfall und anderer Funktionen nutzen.

Um eine NAS-Einheit in einem nativen IBM Spectrum Protect-Speicherpool zu sichern, definieren Sie den Zielspeicherpool in der Kopiengruppe so, dass er auf den gewünschten nativen Speicherpool verweist. Der Zielspeicherpool stellt die Informationen zu dem Speicherarchiv und den Laufwerken zur Verfügung, die für die Sicherung und Zurückschreibung verwendet werden. Sie müssen sicherstellen, dass genügend Speicherbereich in Ihrem Zielspeicherpool verfügbar ist, um die NAS-Daten zu speichern, die auf sequenziellen Einheiten, Platten- oder Dateieinheiten gesichert werden können. Das Definieren einer separaten Einheitenklasse ist nicht erforderlich.

Wenn Sie ein Inhaltsverzeichnis erstellen, muss eine Verwaltungsklasse mit dem Parameter TOCDESTINATION in den Befehlen DEFINE und UPDATE COPYGROUP angegeben werden. Wenn Sie einen NAS-Dateiserver in nativen IBM Spectrum Protect-Pools sichern, kann TOCDESTINATION mit dem Ziel der Daten, die unter Verwendung von NDMP gesichert werden, identisch sein.

Firewallaspekte sind strikter als bei der Übertragung zwischen Dateiserver und angeschlossenem Speicherarchiv, da die Übertragung entweder vom IBM Spectrum Protect-Server oder vom NAS-Dateiserver eingeleitet werden kann. NDMP-Bandserver werden als Threads innerhalb des IBM Spectrum Protect-Servers ausgeführt und der Bandserver akzeptiert Verbindungen an Port 10001. Diese Portnummer kann mit der folgenden Option in der IBM Spectrum Protect-Serveroptionsdatei geändert werden: NDMPPORTRANGE untere_Portnummer, obere_Portnummer.

Während NDMP-Sicherungsoperationen vom Dateiserver auf den Server können Sie mit der Option NDMPPREFDATAINTERFACE angeben, welche Netzschnittstelle der IBM Spectrum Protect-Server verwendet, um Sicherungsdaten zu empfangen. Der Wert für diese Option ist ein Hostname oder eine IPv4-Adresse, die einer der aktiven Netzschnittstellen des Systems zugeordnet ist, auf dem der IBM Spectrum Protect-Server ausgeführt wird. Diese Schnittstelle muss IPv4-fähig sein.

Bevor Sie diese Option verwenden, überprüfen Sie, ob Ihre NAS-Einheit NDMP-Operationen unterstützt, die eine andere Netzschnittstelle für NDMP-Steuer- und NDMP-Datenverbindungen verwenden. NDMP-Steuerverbindungen werden von IBM Spectrum Protect zur Authentifizierung mit einem NDMP-Server und zur Überwachung einer NDMP-Operation verwendet, wohingegen NDMP-Datenverbindungen für die Übertragung und den Empfang von Sicherungsdaten während NDMP-Operationen verwendet werden. Sie müssen dennoch Ihre NAS-Einheit konfigurieren, damit Sicherungs- und Zurückschreibungsdaten an die entsprechende Netzschnittstelle weitergeleitet werden.

Wenn die Option NDMPPREFDATAINTERFACE aktiviert ist, wirkt sie sich auf alle nachfolgenden NDMP-Operationen zwischen Dateiserver und Server aus. Sie hat aber hat keine Auswirkungen auf NDMP-Steuerverbindungen, da diese die Standardnetzschnittstelle des Systems verwenden. Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server stoppen und erneut starten zu müssen.

NetApp-Dateiserver stellen eine NDMP-Option (ndmpd.preferred_interface) zur Verfügung, um die für NDMP-Datenverbindungen verwendete Schnittstelle zu ändern. Weitere Informationen enthält die Dokumentation zu Ihrer NAS-Einheit.

Anweisungen zur Ausführung von NDMP-Sicherungsoperationen vom Dateiserver auf den Server finden Sie in NDMP-Dateiserver auf einem IBM Spectrum Protect-Server sichern.

Informationen zu Serveroptionen finden Sie in Serveroptionen.

NDMP-Dateiserver auf einem IBM Spectrum Protect-Server sichern

Sie können Daten auf einem einzelnen IBM Spectrum Protect-Server sichern, anstatt ein Bandarchiv an jede NAS-Einheit anzuschließen.

Vorgehensweise

Um einen Server in einem NAS-Dateisystem zu sichern, führen Sie die folgenden Schritte aus:

1. Wählen Sie einen vorhandenen Speicherpool aus oder konfigurieren Sie einen Speicherpool für NAS-Daten, indem Sie den folgenden Befehl ausgeben:

   ```
   define stgpool naspool disk
   ```

2. Definieren Sie Datenträger, die dem Speicherpool hinzugefügt werden sollen. Definieren Sie beispielsweise einen Datenträger mit dem Namen naspool_volAB:

   ```
   define volume naspool /usr/storage/naspool_volAB formatsize=100
   ```

3. Setzen Sie das Kopienziel auf den zuvor definierten Speicherpool und aktivieren Sie die zugehörige Maßnahmengruppe.

   ```
   update copygroup standard standard standard destination=naspool
     tocdestination=naspool
   activate policyset standard standard
   ```

   Das Ziel für NAS-Daten wird durch das Ziel in der Kopiengruppe bestimmt. Bei der Schätzung der Speichergröße für NAS-Differenzsicherungen wird die Belegung des Dateibereichs verwendet - derselbe Wert, der für eine Gesamtsicherung verwendet wird. Sie können diese Größenschätzung als einen der Aspekte bei der Auswahl eines Speicherpools verwenden. Eines der Attribute eines Speicherpools ist der Wert für MAXSIZE, mit dem angegeben wird, dass Daten an den nächsten Speicherpool gesendet werden, wenn der Wert für MAXSIZE durch die geschätzte Größe überschritten wird. Da NAS-Differenzsicherungen in native IBM Spectrum Protect-Speicherpools die Belegungsgröße des Basisdateibereichs als geschätzte Speichergröße verwenden, werden Differenzsicherungen in demselben Speicherpool wie die Gesamtsicherung gespeichert. Abhängig von den Kollokationseinstellungen können Differenzsicherungen auf denselben Datenträgern wie die Gesamtsicherung gespeichert werden.
4. Definieren Sie einen Knoten und eine Einheit zum Versetzen von Daten für die NAS-Einheit. Das Datenformat gibt an, dass die von dieser NAS-Einheit erstellten Sicherungsimages ein Dump-Typ des Sicherungsimages in einem NetApp-spezifischen Format sind.

   ```
   register node nas1 nas1 type=nas domain=standard
   define datamover nas1 type=nas hla=nas1 user=root
   password=***** dataformat=netappdump
   ```

   Die NAS-Einheit kann jetzt in einem IBM Spectrum Protect-Serverspeicherpool gesichert werden. Pfade zu lokalen Laufwerken können definiert werden, das von der Verwaltungsklasse angegebene Ziel bestimmt jedoch die Zielposition für diese Sicherungsoperation.
5. Sichern Sie die NAS-Einheit in den IBM Spectrum Protect-Speicherpool, indem Sie den folgenden Befehl ausgeben:

   ```
   backup node nas1 /vol/vol0
   ```

6. Schreiben Sie eine NAS-Einheit aus dem IBM Spectrum Protect-Speicherpool zurück, indem Sie den folgenden Befehl ausgeben:

   ```
   restore node nas1 /vol/vol0
   ```

Sicherung und Zurückschreibung auf Dateiebene für NDMP-Operationen

Wenn Sie Daten mit NDMP sichern, können Sie angeben, dass der IBM Spectrum Protect-Server Informationen auf Dateiebene erfasst und in einem Inhaltsverzeichnis (TOC) speichert.

Wenn Sie diese Option während der Sicherung angeben, können Sie später das Inhaltsverzeichnis (TOC) des Sicherungsimages anzeigen. Mithilfe des Web-Clients für Sichern/Archivieren können Sie einzelne Dateien oder Verzeichnisse auswählen, um diese direkt aus den generierten Sicherungsimages zurückzuschreiben.

Die Erfassung von Informationen auf Dateiebene erfordert zusätzliche Verarbeitungszeit, Netzressourcen, Speicherpoolbereich, temporären Datenbankbereich und möglicherweise zusätzliche Speichereinheiteninteraktion. Anweisungen zum Konfigurieren von Speichereinheiten finden Sie in Speichereinheiten konfigurieren. Gegebenenfalls müssen Sie der IBM Spectrum Protect-Serverdatenbank mehr Speicherbereich zuordnen. Sie müssen die Maßnahme so konfigurieren, dass der IBM Spectrum Protect-Server das Inhaltsverzeichnis (TOC) in einem anderen Speicherpool als das Sicherungsimage speichert. Das Inhaltsverzeichnis (TOC) wird wie jedes andere Objekt in diesem Speicherpool behandelt.

Sie können auch eine Sicherung mit NDMP ausführen, ohne Zurückschreibungsinformationen auf Dateiebene zu erfassen.

Um die Erstellung eines Inhaltsverzeichnisses (TOC) für eine Sicherung mit NDMP zu ermöglichen, müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsimage gebunden ist. Sie können keinen Kopienspeicherpool oder Pool für aktive Daten als Ziel angeben. Der von Ihnen angegebene Speicherpool für das Ziel des Inhaltsverzeichnisses (TOCDESTINATION) muss das Datenformat NATIVE oder NONBLOCK haben und darf daher nicht der für das Sicherungsimage verwendete Bandspeicherpool sein.

Wenn Informationen auf Dateiebene erfasst werden sollen, geben Sie den Parameter TOC im Serverbefehl BACKUP NODE an. Wenn Sie Ihre Sicherung mithilfe des Clients einleiten, können Sie die Option TOC in der Clientoptionsdatei, in der Clientoptionsgruppe oder in der Clientbefehlszeile angeben. Sie können NO, PREFERRED oder YES angeben. Wenn Sie PREFERRED oder YES angeben, speichert der IBM Spectrum Protect-Server Dateiinformationen für eine einzelne NDMP-gesteuerte Sicherung in einem Inhaltsverzeichnis (TOC). Das Inhaltsverzeichnis (TOC) wird in einen Speicherpool gestellt. Danach kann der IBM Spectrum Protect-Server auf das Inhaltsverzeichnis (TOC) zugreifen, sodass Datei- und Verzeichnisinformationen vom Server oder Client abgefragt werden können. Die Verwendung des Parameters TOC ermöglicht es, ein Inhaltsverzeichnis (TOC) für einige Images zu generieren und für andere nicht, ohne dass verschiedene Verwaltungsklassen für die Images erforderlich sind.

Weitere Informationen zum Befehl BACKUP NODE finden Sie in BACKUP NODE (NAS-Knoten sichern).

Verwenden Sie Speicherpools mit wahlfreiem Zugriff (Einheitenklasse DISK) als Ziel für das Inhaltsverzeichnis (TOC), um Mountverzögerungen zu vermeiden und ausreichenden Speicherbereich zu gewährleisten. Bei Speicherpools mit sequenziellem Zugriff ist keine Kennzeichnung oder andere Datenträgervorbereitung erforderlich, wenn Arbeitsdatenträger zulässig sind.

Weitere Informationen finden Sie in Inhaltsverzeichnisse verwalten.

- Schnittstellen für Zurückschreibungsoperationen auf Dateiebene
  Wenn Sie einzelne Dateien und Verzeichnisse zurückschreiben, haben Sie die Möglichkeit, eine von zwei Schnittstellen zu verwenden, um die Zurückschreibung einzuleiten: den Web-Client für Sichern/Archivieren oder die Serverschnittstelle.
- Zeichen des internationalen Zeichensatzes für NetApp-Dateiserver
  Alle Systeme, die Daten auf einem bestimmten Datenträger des NAS-Dateiservers erstellen oder auf diese zugreifen, müssen dafür eine Methode verwenden, die mit der Spracheinstellung des Datenträgers kompatibel ist.
- Zurückschreibungsoperationen auf Dateiebene aus einem Sicherungsimage auf Verzeichnisebene
  Zurückschreibungsoperationen auf Dateiebene werden für Sicherungsimages auf Verzeichnisebene unterstützt.

Schnittstellen für Zurückschreibungsoperationen auf Dateiebene

Wenn Sie einzelne Dateien und Verzeichnisse zurückschreiben, haben Sie die Möglichkeit, eine von zwei Schnittstellen zu verwenden, um die Zurückschreibung einzuleiten: den Web-Client für Sichern/Archivieren oder die Serverschnittstelle.

Zurückschreibungsoperationen mithilfe des Web-Clients für Sichern/Archivieren
: Für den Web-Client für Sichern/Archivieren muss ein Inhaltsverzeichnis (TOC) vorhanden sein, um Dateien und Verzeichnisse zurückschreiben zu können. Der Web-Client muss sich auf einem Windows-System befinden. Der IBM Spectrum Protect-Server greift auf das Inhaltsverzeichnis (TOC) im Speicherpool zu und lädt TOC-Informationen in eine temporäre Datenbanktabelle. Dann können Sie mithilfe des Web-Clients für Sichern/Archivieren Verzeichnisse und Dateien in einem oder mehreren Dateisystemimages überprüfen und einzelne Dateien oder Verzeichnisse zum direkten Zurückschreiben aus den generierten Sicherungsimages auswählen.

Zurückschreibungsoperationen mithilfe der Serverschnittstelle

- Wenn ein Inhaltsverzeichnis (TOC) vorhanden ist, verwenden Sie den Befehl QUERY NASBACKUP, um Informationen zu den von NDMP generierten Sicherungsimages aufzurufen und anzuzeigen, welche Images über ein entsprechendes Inhaltsverzeichnis (TOC) verfügen. Verwenden Sie dann den Befehl RESTORE NODE mit dem Parameter FILELIST.
- Wenn kein Inhaltsverzeichnis (TOC) erstellt wurde, kann der Inhalt des Sicherungsimages nicht angezeigt werden. Sie können einzelne Dateien und/oder Verzeichnisse zurückschreiben, wenn Sie den Namen der Datei bzw. des Verzeichnisses kennen, und wenn Sie wissen, in welchem Image sich die Sicherung befindet. Verwenden Sie den Befehl RESTORE NODE mit dem Parameter FILELIST.

Zeichen des internationalen Zeichensatzes für NetApp-Dateiserver

Alle Systeme, die Daten auf einem bestimmten Datenträger des NAS-Dateiservers erstellen oder auf diese zugreifen, müssen dafür eine Methode verwenden, die mit der Spracheinstellung des Datenträgers kompatibel ist.

Sie müssen Data ONTAP 6.4.1 oder höher (falls verfügbar) auf Ihrem NetApp-NAS-Dateiserver installieren, um vollständige Unterstützung für Zeichen des internationalen Zeichensatzes in Datei- und Verzeichnisnamen zu erhalten.

Wenn Ihre Version von Data ONTAP älter als 6.4.1 ist, benötigen Sie eine der beiden folgenden Konfigurationen, um Informationen auf Dateiebene erfassen und zurückschreiben zu können. Bei anderen Konfigurationen als den beiden aufgeführten sind die Ergebnisse unvorhersehbar. Der IBM Spectrum Protect-Server gibt eine Warnung (ANR4946W) während Sicherungsoperationen aus. Die Nachricht gibt an, dass die Zeichencodierung der NDMP-Dateiprotokollnachrichten unbekannt ist und UTF-8 angenommen wird, um ein Inhaltsverzeichnis zu erstellen. Diese Nachricht kann nur in den beiden folgenden Konfigurationen ohne Bedenken ignoriert werden.

- Ihre Daten enthalten Verzeichnis- und Dateinamen, die nur aus Zeichen des englischen Zeichensatzes (7-Bit ASCII) bestehen.
- Ihre Daten enthalten Verzeichnis- und Dateinamen, die aus Zeichen bestehen, die nicht zum englischen Zeichensatz gehören, und als Datenträgersprache ist die UTF-8-Version der entsprechenden Ländereinstellung definiert (beispielsweise `de.UTF-8` für Deutsch).

Wenn Ihre Version von Data ONTAP 6.4.1 oder höher ist, benötigen Sie eine der drei folgenden Konfigurationen, um Informationen auf Dateiebene erfassen und zurückschreiben zu können. Bei anderen Konfigurationen als den drei aufgeführten sind die Ergebnisse unvorhersehbar.

- Ihre Daten enthalten Verzeichnis- und Dateinamen, die nur aus Zeichen des englischen Zeichensatzes (7-Bit ASCII) bestehen, und die Datenträgersprache ist entweder nicht definiert oder mit einem der folgenden Werte definiert:

    - C (POSIX)
    - en
    - en_US
    - en.UTF-8
    - en_US.UTF-8
- Ihre Daten enthalten Verzeichnis- und Dateinamen, die aus Zeichen bestehen, die nicht zum englischen Zeichensatz gehören, und als Datenträgersprache ist die entsprechende Ländereinstellung definiert (beispielsweise `de.UTF-8` oder `de` für Deutsch).
  Tipp: Die Verwendung der UTF-8-Version der Spracheinstellung des Datenträgers ist in Bezug auf die IBM Spectrum Protect-Serververarbeitung und den Speicherbereich des Inhaltsverzeichnisses effizienter.
- Sie verwenden CIFS nur, um Ihre Daten zu erstellen und auf sie zuzugreifen.

Zurückschreibungsoperationen auf Dateiebene aus einem Sicherungsimage auf Verzeichnisebene

Zurückschreibungsoperationen auf Dateiebene werden für Sicherungsimages auf Verzeichnisebene unterstützt.

Wie bei einer NAS-Dateisystemsicherung wird während einer Sicherung auf Verzeichnisebene ein Inhaltsverzeichnis erstellt und Sie können die Dateien in dem Image mit dem Web-Client durchsuchen. Standardmäßig werden die Dateien an die ursprüngliche Position zurückgeschrieben. Während einer Zurückschreibung auf Dateiebene aus einer Sicherung auf Verzeichnisebene können Sie jedoch entweder ein anderes Dateisystem oder einen anderen virtuellen Dateibereichsnamen als Ziel auswählen.

Für ein Inhaltsverzeichnis (TOC) eines Sicherungsimage auf Verzeichnisebene beziehen sich die Pfadnamen für alle Dateien auf das Verzeichnis, das in der Definition des virtuellen Dateibereichs angegeben wurde, und nicht auf das Stammverzeichnis des Dateisystems.

Sicherungs- und Zurückschreibungsoperationen auf Verzeichnisebene

Wenn Sie über ein großes NAS-Dateisystem verfügen, werden durch das Einleiten einer Sicherung auf Verzeichnisebene Sicherungs- und Zurückschreibungszeiten reduziert und größere Flexibilität beim Konfigurieren von NAS-Sicherungen bereitgestellt. Durch das Definieren virtueller Dateibereiche kann eine Dateisystemsicherung auf mehrere NDMP-Sicherungsoperationen und auf mehrere Bandlaufwerke verteilt werden. Sie können auch verschiedene Sicherungszeitpläne verwenden, um Unterverzeichnisstrukturen eines Dateisystems zu sichern.

Der Name des virtuellen Dateibereichs darf nicht mit einem Dateisystem auf dem NAS-Knoten übereinstimmen. Wird auf der NAS-Einheit ein Dateisystem erstellt, das denselben Namen wie ein virtuelles Dateisystem hat, tritt eine Namensunverträglichkeit auf dem IBM Spectrum Protect-Server auf, wenn der neue Dateibereich gesichert wird. Anweisungen zur Ausgabe von Befehlen zur Zuordnung virtueller Dateibereiche finden Sie in DEFINE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs definieren).
Einschränkung: Zuordnungen virtueller Dateibereiche werden nur für NAS-Knoten unterstützt.

- Sicherung und Zurückschreibung auf Verzeichnisebene für NDMP-Operationen
  Mit dem Befehl DEFINE VIRTUALFSMAPPING wird ein Verzeichnispfad eines NAS-Dateiservers dem Namen eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server zugeordnet. Nachdem eine Zuordnung definiert wurde, können Sie NAS-Operationen, wie beispielsweise BACKUP NODE und RESTORE NODE, unter Verwendung der Namen der virtuellen Dateibereiche so ausführen, als würde es sich um tatsächliche NAS-Dateibereiche handeln.
- Mit Momentaufnahmen sichern und zurückschreiben
  NDMP-Sicherungsoperationen auf Verzeichnisebene ermöglichen es Ihnen, benutzererstellte Momentaufnahmen eines NAS-Dateisystems zu sichern. Diese Momentaufnahmen werden dann als Unterverzeichnisse gespeichert. Die Momentaufnahmen können zu beliebiger Zeit erstellt werden, und die Sicherung auf Band kann bis zu einem geeigneten Zeitpunkt verzögert werden.

Sicherung und Zurückschreibung auf Verzeichnisebene für NDMP-Operationen

Mit dem Befehl DEFINE VIRTUALFSMAPPING wird ein Verzeichnispfad eines NAS-Dateiservers dem Namen eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server zugeordnet. Nachdem eine Zuordnung definiert wurde, können Sie NAS-Operationen, wie beispielsweise BACKUP NODE und RESTORE NODE, unter Verwendung der Namen der virtuellen Dateibereiche so ausführen, als würde es sich um tatsächliche NAS-Dateibereiche handeln.

Um eine Sicherung des Verzeichnisses zu starten, geben Sie den Befehl BACKUP NODE mit dem Namen des virtuellen Dateibereichs anstelle eines Dateibereichsnamens aus. Um die Unterverzeichnisstruktur des Verzeichnisses an die ursprüngliche Position zurückzuschreiben, führen Sie den Befehl RESTORE NODE aus und geben Sie den Namen des virtuellen Dateibereichs an.

Definitionen für den virtuellen Dateibereich können ebenfalls als Ziel in einem Befehl RESTORE NODE angegeben werden. Auf diese Art und Weise können Sie Sicherungsimages (Dateisystem oder Verzeichnis) in ein Verzeichnis in einem beliebigen Dateisystem der NAS-Einheit zurückschreiben.

Mit dem Web-Client können Sie Dateien für die Zurückschreibung aus einem Sicherungsimage auf Verzeichnisebene auswählen, da der IBM Spectrum Protect-Client die Namen der virtuellen Dateibereiche als NAS-Dateibereiche behandelt.

Mit Momentaufnahmen sichern und zurückschreiben

NDMP-Sicherungsoperationen auf Verzeichnisebene ermöglichen es Ihnen, benutzererstellte Momentaufnahmen eines NAS-Dateisystems zu sichern. Diese Momentaufnahmen werden dann als Unterverzeichnisse gespeichert. Die Momentaufnahmen können zu beliebiger Zeit erstellt werden, und die Sicherung auf Band kann bis zu einem geeigneten Zeitpunkt verzögert werden.

Vorgehensweise

Um beispielsweise eine Momentaufnahme, die für ein NetApp-Dateisystem erstellt wird, zu sichern, führen Sie die folgenden Schritte aus:

1. Geben Sie an der Konsole für die NAS-Einheit den Befehl zum Erstellen der Momentaufnahme aus. SNAP CREATE lautet der Befehl für eine NetApp-Einheit.

   ```
   snap create vol2 february17
   ```

   In diesem Beispiel wird eine Momentaufnahme mit dem Namen FEBRUARY 17 des Dateisystems /vol/vol2 erstellt. Die physische Position für die Momentaufnahmedaten befindet sich in dem Verzeichnis /vol/vol2/.snapshot/february17. Die Speicherposition für die Momentaufnahmedaten ist von der Implementierung durch den NAS-Anbieter abhängig. Für NetApp kann der Befehl SNAP LIST verwendet werden, um alle Momentaufnahmen für ein Dateisystem anzuzeigen.
2. Erstellen Sie eine Definition für die Zuordnung eines virtuellen Dateibereichs auf dem IBM Spectrum Protect-Server für die im vorherigen Schritt erstellten Momentaufnahmedaten.

   ```
   define virtualfsmapping  nas1 /feb17snapshot  /vol/vol2  /.snapshot/february17
   ```

   In diesem Beispiel wird die Definition /feb17snapshot für die Zuordnung eines virtuellen Dateibereichs erstellt.
3. Sichern Sie die Zuordnung des virtuellen Dateibereichs.

   ```
   backup node nas1 /feb17snapshot mode=full toc=yes
   ```

4. Nachdem die Sicherung erstellt wurde, können Sie entweder das gesamte Momentaufnahmeimage oder eine einzelne Datei zurückschreiben. Vor dem Zurückschreiben der Daten können Sie einen Namen für die Zuordnung des virtuellen Dateibereichs für das Zielverzeichnis erstellen. Sie können einen beliebigen Dateisystemnamen als Ziel auswählen. Die Zielposition in diesem Beispiel ist das Verzeichnis /feb17snaprestore im Dateisystem /vol/vol1.

   ```
   define virtualfsmapping  nas1 /feb17snaprestore  /vol/vol1  /feb17snaprestore
   ```

5. Schreiben Sie das Momentaufnahmesicherungsimage zurück.

   ```
   restore node nas1 /feb17snapshot /feb17snaprestore
   ```

   In diesem Beispiel wird eine Kopie des Dateisystems /vol/vol2 in das Verzeichnis /vol/vol1/feb17snaprestore in demselben Zustand wie bei der Erstellung der Momentaufnahme im ersten Schritt zurückgeschrieben.

Sicherungs- und Zurückschreibungsoperationen mit der NetApp-Funktion 'SnapMirror to Tape'

Sie können große NetApp-Dateisysteme mithilfe der NetApp-Funktion 'SnapMirror to Tape' (die auch als 'SMTape' bekannt ist) sichern. Durch die Verwendung einer Datenkopie auf Blockebene für die Sicherung ist die Methode 'SnapMirror to Tape' schneller als eine traditionelle NDMP-Gesamtsicherung und kann verwendet werden, wenn NDMP-Gesamtsicherungen nicht geeignet sind.

Verwenden Sie die NDMP-Funktion 'SnapMirror to Tape' als Option zur Wiederherstellung nach einem Katastrophenfall für das Kopieren großer NetApp-Dateisysteme in Zusatzspeicher. Verwenden Sie für die meisten NetApp-Dateisysteme die standardmäßige NDMP-Gesamt- oder Differenzsicherungsmethode.

Die Angabe eines Parameters in den Befehlen BACKUP NODE und RESTORE NODE ermöglicht Ihnen das Sichern und Zurückschreiben von Dateisystemen mithilfe der Funktion 'SnapMirror to Tape'. In Bezug auf die Verwendungsmöglichkeiten von SnapMirror-Images gibt es verschiedene Einschränkungen. Beachten Sie die folgenden Richtlinien, bevor Sie die Funktion als Sicherungsmethode verwenden:

- Wenn NetApp ONTAP 8.2 oder höher installiert wurde, müssen Sie eine Einheit des Typs NASCLUSTER oder NASVSERVER zum Versetzen von Daten für 'SnapMirror to Tape'-Operationen definieren.
- Eine Sicherungs- oder Zurückschreibungsoperation mit 'SnapMirror to Tape' kann nicht vom IBM Spectrum Protect Operations Center, Web-Client oder Befehlszeilenclient eingeleitet werden.
- Differenzsicherungen von SnapMirror-Images können nicht ausgeführt werden.
- Eine Sicherung auf Verzeichnisebene mithilfe der Funktion 'SnapMirror to Tape' kann nicht ausgeführt werden. Demzufolge erlaubt IBM Spectrum Protect keine Sicherungsoperationen mit 'SnapMirror to Tape' für einen virtuellen Serverdateibereich.
- Eine NDMP-Zurückschreibungsoperation auf Dateiebene aus 'SnapMirror to Tape'-Images kann nicht ausgeführt werden. Daher wird bei Imagesicherungen mit 'SnapMirror to Tape' nie ein Inhaltsverzeichnis erstellt.
- Zu Beginn einer Kopieroperation mit 'SnapMirror to Tape' generiert der Dateiserver eine Momentaufnahme des Dateisystems. NetApp stellt eine NDMP-Umgebungsvariable zur Verfügung, um zu steuern, ob diese Momentaufnahme am Ende der 'SnapMirror to Tape'-Operation entfernt wird. Diese Variable wird von IBM Spectrum Protect immer so gesetzt, dass die Momentaufnahme entfernt wird.
- Nachdem ein 'SnapMirror to Tape'-Image abgerufen und in ein NetApp-Dateisystem kopiert wurde, bleibt das Zieldateisystem als SnapMirror-Partner konfiguriert. NetApp stellt eine NDMP-Umgebungsvariable zur Verfügung, um zu steuern, ob diese SnapMirror-Beziehung abgebrochen werden soll. IBM Spectrum Protect bricht immer die SnapMirror-Beziehung während des Abrufs ab. Nach

Abschluss der Zurückschreibungsoperation befindet sich das Zieldateisystem in demselben Status wie das ursprüngliche Dateisystem zum Zeitpunkt der Sicherung.

Weitere Informationen zur Funktion 'SnapMirror to Tape' finden Sie in BACKUP NODE (NAS-Knoten sichern) und RESTORE NODE (NAS-Knoten zurückschreiben).

NDMP-Sicherungsoperationen mithilfe von in Celerra-Dateiserver integrierten Prüfpunkten

Wenn der IBM Spectrum Protect-Server eine NDMP-Sicherungsoperation auf einer Celerra-Einheit zum Versetzen von Daten einleitet, kann die Sicherung eines umfangreichen Dateisystems mehrere Stunden dauern. Ohne integrierte Celerra-Prüfpunkte werden alle auf dem Dateisystem vorgenommenen Änderungen in das Sicherungsimage geschrieben.

Demzufolge enthält das Sicherungsimage Änderungen, die während der gesamten Sicherungsoperation an dem Dateisystem vorgenommen wurden. Das Sicherungsimage ist kein echtes Zeitpunktimage des Dateisystems.

Wenn Sie NDMP-Sicherungsoperationen für Celerra-Dateiserver ausführen, führen Sie ein Upgrade für das Betriebssystem auf Ihrer Einheit zum Versetzen von Daten auf Celerra-Dateiserver Version T5.5.25.1 oder höher durch. Diese Betriebssystemversion ermöglicht die Aktivierung der integrierten Prüfpunkte für alle NDMP-Sicherungsoperationen von der Celerra-Steuerworkstation aus. Durch die Aktivierung dieses Features stellen Sie sicher, dass die Sicherungsdaten echte Zeitpunktimages des Dateisystems darstellen, das gesichert wird.

Anweisungen zum Aktivieren von integrierten Prüfpunkten während aller NDMP-Sicherungsoperationen enthält die Dokumentation zum Celerra-Dateiserver.

Wenn das Betriebssystem auf Ihrem Celerra-Dateiserver eine frühere Version als T5.5.25.1 hat und Sie NDMP zum Sichern von Celerra-Einheiten zum Versetzen von Daten verwenden, generieren Sie manuell eine Momentaufnahme des Dateisystems mithilfe der Celerra-Befehlszeilenfunktion für Prüfpunkte. Leiten Sie anschließend eine NDMP-Sicherungsoperation für das Prüfpunktdateisystem anstelle einer NDMP-Sicherungsoperation für das ursprüngliche Dateisystem ein.

Anweisungen zum Erstellen und Planen von Prüfpunkten von der Celerra-Steuerworkstation enthält die Dokumentation zum Celerra-Dateiserver.

NAS-Knoten replizieren

Sie können einen NAS-Knoten, der NDMP für Sicherungsoperationen verwendet, replizieren. Machen Sie sich, bevor Sie die Replikationsoperation konfigurieren, mit den geltenden Einschränkungen vertraut.

Informationen zu diesem Vorgang

Einschränkungen:

- Die Sicherungsdaten müssen sich in einem Speicherpool mit dem Datenformat NATIVE befinden. Sicherungsdaten in Speicherpools mit den folgenden Datenformaten können nicht repliziert werden:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
- Eine Differenzsicherung kann nur repliziert werden, wenn die zugehörige Gesamtsicherung repliziert wurde.

Vorgehensweise

1. Aktivieren Sie den NAS-Knoten für die Replikation, indem Sie den Befehl UPDATE NODE ausgeben:

   ```
   update node Knotenname replstate=enabled
   ```

   Dabei gibt *Knotenname* den Namen des NAS-Knotens an.
2. Replizieren Sie den Knoten, indem Sie den Befehl REPLICATE NODE ausgeben:

   ```
   replicate node Knotenname
   ```

   Dabei gibt *Knotenname* den Namen des NAS-Knotens an.
3. Um sicherzustellen, dass die replizierten Daten zurückgeschrieben werden können, definieren Sie eine Einheit zum Versetzen von Daten auf dem Zielserver für den Knoten, indem Sie den Befehl DEFINE DATAMOVER ausgeben:

   ```
   define datamover Knotenname type=nas hladdress=Adresse_der_höheren_Ebene
   lladdress=Adresse_der_unteren_Ebene
       userid=Benutzer-ID password=Benutzerkennwort dataformat=netappdump
   ```

   Erläuterungen:

   Knotenname
   : Gibt den Namen des NAS-Knotens an.

Adresse_der_höheren_Ebene
Gibt entweder die numerische IP-Adresse oder den Domänennamen für den Zugriff auf den NAS-Dateiserver an.
Adresse_der_unteren_Ebene
Gibt die TCP-Portnummer für den Zugriff auf die NAS-Einheit für NDMP-Sitzungen an.
Benutzer-ID
Gibt die ID eines Benutzers an, der zum Einleiten einer NDMP-Sitzung mit dem NAS-Dateiserver berechtigt ist.
Benutzerkennwort
Gibt das Kennwort des Benutzers an, der zum Einleiten einer NDMP-Sitzung mit dem NAS-Dateiserver berechtigt ist.

Ergebnisse

Das Format der Sicherungsdaten ändert sich während des Replikationsprozesses nicht. Wenn Sicherungsdaten repliziert werden, wird auch das zugehörige Inhaltsverzeichnis repliziert.

Datenschutz mithilfe des lizenzierten NetApp-Features SnapLock

Sie können das lizenzierte NetApp-Feature SnapLock verwenden, um die strengen gesetzlichen Bestimmungen für archivierte Daten einzuhalten. Wenn Sie das Feature SnapLock aktivieren, können Sie mithilfe von IBM Spectrum Protect ein Datum für das Ende des Aufbewahrungszeitraums für Dateien festlegen und eine Datei im WORM-Status (WORM = Write Once Read Many) festschreiben.

Daten, die mit einem Datum für das Ende des Aufbewahrungszeitraums gespeichert werden, können erst aus dem Dateisystem gelöscht werden, wenn der Aufbewahrungszeitraum abgelaufen ist. Das Feature SnapLock kann nur von IBM Spectrum Protect-Servern verwendet werden, wenn für die Server der Aufbewahrungsschutz für Daten aktiviert ist.

Daten, die auf Servern mit aktiviertem Aufbewahrungsschutz für Daten archiviert und auf NetApp-NAS-Dateiservern gespeichert werden, werden als IBM Spectrum Protect-FILE-Datenträger gespeichert. Am Ende einer Schreibtransaktion wird ein Datum für das Ende des Aufbewahrungszeitraums für den FILE-Datenträger über die SnapLock-Schnittstelle definiert. Dieses Datum wird mithilfe der Parameter RETVER und RETMIN der Archivierungskopiengruppe berechnet, die beim Archivieren der Daten verwendet wird. Indem dem FILE-Datenträger ein Datum für das Ende des Aufbewahrungszeitraums zugeordnet wird, wird verhindert, dass die Daten des FILE-Datenträgers gelöscht oder überschrieben werden, bevor der Aufbewahrungszeitraum abläuft. Diese FILE-Datenträger werden als WORM-FILE-Datenträger bezeichnet. Nachdem ein Datum für das Ende des Aufbewahrungszeitraums festgelegt wurde, kann der WORM-FILE-Datenträger erst gelöscht werden, nachdem das Datum für das Ende des Aufbewahrungszeitraums überschritten wurde. IBM Spectrum Protect for Data Retention stellt zusammen mit der WORM-FILE-Datenträgerkonsolidierung den Schutz der Daten während ihres Lebenszyklus sicher.

Speicherpools können entweder nach Schwellenwert oder nach Datenaufbewahrungszeitraum verwaltet werden. Der Speicherpoolparameter RECLAMATIONTYPE gibt an, dass ein Speicherpool auf der Basis eines Datenaufbewahrungszeitraums verwaltet wird. Wird ein traditioneller Speicherpool mit dem Parameter FORMAT=DETAILED abgefragt, wird diese Ausgabe angezeigt:

```
Konsolidierungstyp: THRESHOLD
```

Wenn ein IBM Spectrum Protect-Server mit Aufbewahrungsschutz für Daten über IBM Spectrum Protect for Data Retention aktiviert ist und der Server Zugriff auf einen NetApp-Dateiserver mit dem lizenzierten Feature SnapLock hat, können Sie einen Speicherpool definieren, für den der Parameter RECLAMATIONTYPE auf SNAPLOCK gesetzt ist. Dies bedeutet, dass Daten, die auf Datenträgern in diesem Speicherpool erstellt werden, anhand des Datums für das Ende des Aufbewahrungszeitraums verwaltet werden. Wenn ein SnapLock-Speicherpool mit dem Parameter FORMAT=DETAILED abgefragt wird, gibt die Ausgabe an, dass die Speicherpools anhand des Datenaufbewahrungszeitraums verwaltet werden:

```
 Konsolidierungstyp: SNAPLOCK
```

Weitere Informationen zum SnapLock-Dateiserver enthält die NetApp-Dokumentation *Data ONTAP Archive and Compliance Management Guide for 7-Mode*.

Achtung: Verwenden Sie dieses Feature nicht zum Schützen von Daten mit einem Aufbewahrungszeitraum von weniger als drei Monaten.

- Wiederherstellung und das Feature SnapLock
  Um sicherzustellen, dass Daten immer geschützt werden, setzen Sie den NetApp-Standardaufbewahrungszeitraum auf 30 Tage, damit er mit dem Standardkonsolidierungszeitraum des WORM-FILE-Datenträgers übereinstimmt. IBM Spectrum Protect konsolidiert alle verbleibenden Daten auf einem WORM-FILE-Datenträger unmittelbar vor dem Ablauf des Aufbewahrungszeitraums.
- Aufbewahrungszeiträume
  IBM Spectrum Protect-Maßnahmen steuern den Aufbewahrungszeitraum für den WORM-FILE-Datenträger. Die Aufbewahrungsdauer einiger Dateien kann unter Umständen den Aufbewahrungszeitraum für den WORM-FILE-Datenträger, auf dem sie gespeichert sind, überschreiten. Möglicherweise müssen Sie einige Dateien auf einen anderen Datenträger versetzen, um sicherzustellen, dass die Dateien auf WORM-Datenträgern gespeichert werden.
- Konfiguration des Features SnapLock für die ereignisgesteuerte Aufbewahrung
  Auf SnapLock-Datenträgern gespeicherte Daten, die durch IBM Spectrum Protect for Data Retention und ereignisgesteuerte Aufbewahrung verwaltet werden, können zu exzessiver Konsolidierung führen, was Leistungseinbußen auf dem Server zur Folge hat.
- Unterbrechungsfreier Datenschutz mit dem SnapLock-Feature
  Wenn Daten auf einem Datenträger mit aktiviertem SnapLock-Feature gespeichert sind und die Daten auf einen Datenträger, auf dem das SnapLock-Feature nicht aktiviert ist, versetzt oder kopiert werden, verlieren die Daten den einzigartigen Hardwareschutz, der durch NetApp-WORM-Datenträger zur Verfügung gestellt wird.

- SnapLock-Datenträger als IBM Spectrum Protect-WORM-FILE-Datenträger konfigurieren
  Um die strengen Anforderungen für archivierte Daten zu erfüllen, aktivieren Sie das NetApp-Feature SnapLock.

Wiederherstellung und das Feature SnapLock

Um sicherzustellen, dass Daten immer geschützt werden, setzen Sie den NetApp-Standardaufbewahrungszeitraum auf 30 Tage, damit er mit dem Standardkonsolidierungszeitraum des WORM-FILE-Datenträgers übereinstimmt. IBM Spectrum Protect konsolidiert alle verbleibenden Daten auf einem WORM-FILE-Datenträger unmittelbar vor dem Ablauf des Aufbewahrungszeitraums.

Mit der Konsolidierung eines WORM-FILE-Datenträgers auf einem anderen WORM-FILE-Datenträger vor dem Ablauf des Aufbewahrungszeitraums wird sichergestellt, dass Daten immer durch das Feature SnapLock geschützt werden.

Da dieser Schutz auf der IBM Spectrum Protect-Datenträgerebene stattfindet, können die Daten auf den Datenträgern durch IBM Spectrum Protect-Maßnahmen verwaltet werden, unabhängig davon, wo die Daten gespeichert werden. Daten, die auf WORM-FILE-Datenträgern gespeichert werden, werden sowohl durch den Aufbewahrungsschutz von Daten als auch durch den Aufbewahrungszeitraum geschützt, der mit der physischen Datei auf dem SnapLock-Datenträger gespeichert wird. Wenn ein IBM Spectrum Protect-Administrator einen Befehl zum Löschen der Daten ausgibt, schlägt der Befehl fehl. Wenn ein Benutzer versucht, die Datei mithilfe einer Reihe von Netzdateisystemaufrufen zu löschen, verhindert das Feature SnapLock das Löschen der Daten.

Während der Konsolidierungsverarbeitung wird eine Warnung ausgegeben, wenn der IBM Spectrum Protect-Server keine Daten von einem SnapLock-Datenträger, der verfällt, auf einen neuen SnapLock-Datenträger versetzen kann.

Aufbewahrungszeiträume

IBM Spectrum Protect-Maßnahmen steuern den Aufbewahrungszeitraum für den WORM-FILE-Datenträger. Die Aufbewahrungsdauer einiger Dateien kann unter Umständen den Aufbewahrungszeitraum für den WORM-FILE-Datenträger, auf dem sie gespeichert sind, überschreiten. Möglicherweise müssen Sie einige Dateien auf einen anderen Datenträger versetzen, um sicherzustellen, dass die Dateien auf WORM-Datenträgern gespeichert werden.

Einige Objekte auf dem Datenträger müssen möglicherweise länger als andere Objekte auf dem Datenträger aufbewahrt werden, da:

- Die Objekte an Verwaltungsklassen mit unterschiedlichen Aufbewahrungszeiträumen gebunden sind.
- Die Objekte aufgrund des Status 'Löschen unzulässig' nicht entfernt werden können.
- Die Objekte auf das Eintreten eines Ereignisses vor dem Verfall warten.
- Der Aufbewahrungszeitraum für eine Kopiengruppe verlängert wird und damit ein längerer Aufbewahrungszeitraum als der Aufbewahrungszeitraum erforderlich wird, der im Feature SnapLock beim Festschreiben des WORM-FILE-Datenträgers angegeben wurde.

Um einen WORM-FILE-Datenträger nach Aufbewahrungszeitraum zu verwalten, müssen Sie den Befehl DEFINE STGPOOL unter Angabe von RECLAMATIONTYPE=SNAPLOCK ausgeben. Auf diese Art und Weise definieren Sie einen Speicherpool als SnapLock-Speicherpool. Anschließend können Sie den Parameter RECLAMATIONTYPE nicht mit dem Wert THRESHOLD aktualisieren. Wenn Sie einen SnapLock-Speicherpool definieren, prüft das System, ob die angegebenen Verzeichnisse in der Einheitenklasse SnapLock-WORM-Datenträger sind. Wenn eine Dateiklasse definiert wird und Speicherpools mit dem Konsolidierungstyp SNAPLOCK erstellt werden, müssen alle Datenträger WORM-Datenträger sein; andernfalls schlägt die Operation fehl. Wenn eine Einheitenklasse aktualisiert wird, um zusätzliche Verzeichnisse zu enthalten, und wenn der Einheitenklasse SnapLock-Speicherpools zugeordnet werden, erfolgt dieselbe Prüfung, um sicherzustellen, dass alle Verzeichnisse SnapLock-WORM-Datenträger sind.

Für das NetApp-Feature SnapLock sind drei Aufbewahrungszeiträume verfügbar. Die Aufbewahrungszeiträume müssen korrekt konfiguriert werden, damit der IBM Spectrum Protect-Server WORM-Daten, die auf SnapLock-Datenträgern gespeichert werden, ordnungsgemäß verwalten kann. Der IBM Spectrum Protect-Server legt den Aufbewahrungszeitraum für Daten, die auf NetApp SnapLock-Datenträgern gespeichert werden, auf der Basis der Werte in der Kopiengruppe für die Daten fest, die archiviert werden. Der NetApp-Dateiserver darf nicht mit der Fähigkeit des IBM Spectrum Protect-Servers den Aufbewahrungszeitraum festlegen zu können, im Konflikt stehen. Die bevorzugte Methode ist die Konfiguration der folgenden Einstellungen für Aufbewahrungszeiträume im NetApp-Dateiserver:

- Minimaler Aufbewahrungszeitraum. Definieren Sie den höheren Wert: entweder 30 Tage oder die minimale Anzahl Tage, die von einer beliebigen Kopiengruppe (unter Verwendung eines NetApp SnapLock-Dateiservers für WORM-FILE-Speicher) für den Aufbewahrungszeitraum für Daten angegeben wird. Bei der Kopiengruppe handelt es sich um die Kopiengruppe, die zum Speichern von Daten auf NetApp SnapLock-Datenträgern verwendet wird.
- Maximaler Aufbewahrungszeitraum. Übernehmen Sie den Standardwert von 30 Jahren. Dieser Aufbewahrungszeitraum ermöglicht es dem IBM Spectrum Protect-Server, den tatsächlichen Datenträgeraufbewahrungszeitraum auf der Basis der Einstellungen in der Archivierungskopiengruppe festzulegen.
- Standardaufbewahrungszeitraum. Legen Sie diesen Zeitraum mit 30 Tagen fest. Wenn Sie diesen Wert und den maximalen Aufbewahrungszeitraum nicht festlegen, wird der Aufbewahrungszeitraum jedes Datenträgers auf 30 Jahre gesetzt. In diesem Fall kann der IBM Spectrum Protect-Server den Verfall und die Wiederverwendung von NetApp SnapLock-Datenträgern nicht steuern. Dies hat zur Folge, dass für die Dauer von 30 Jahren kein Datenträger wiederverwendet werden kann.

Wenn die NetApp SnapLock-Aufbewahrungszeiträume festgelegt werden, kann IBM Spectrum Protect die Daten in SnapLock-Speicherpools mit maximaler Effizienz verwalten. Für jeden Datenträger in einem SnapLock-Speicherpool wird ein IBM Spectrum Protect-Konsolidierungszeitraum erstellt. Der IBM Spectrum Protect-Konsolidierungszeitraum hat ein Startdatum (BEGIN RECLAIM PERIOD) und ein Enddatum (END RECLAIM

PERIOD). Sie können diese Datumsangaben anzeigen, indem Sie den Befehl QUERY VOLUME unter Angabe des Parameters FORMAT=DETAILED für einen SnapLock-Datenträger ausgeben. Die Ausgabe ähnelt der in dem folgenden Beispiel:

```
Anfang des Konsolidierungszeitraums: 05.09.2017
  Ende des Konsolidierungszeitraums: 06.10.2017
```

Wenn IBM Spectrum Protect Dateien auf einem SnapLock-Datenträger archiviert, verfolgt der Server das späteste Verfallsdatum dieser Dateien und der Wert für BEGIN RECLAIM PERIOD wird auf dieses späteste Verfallsdatum gesetzt. Wenn dem SnapLock-Datenträger weitere Dateien hinzugefügt werden, wird das Startdatum auf dieses spätere Datum gesetzt, wenn eine Datei mit einem späteren Verfallsdatum als das einer derzeit auf dem Datenträger gespeicherten Datei vorhanden ist. Das Startdatum wird für jede Datei auf diesem Datenträger auf das letzte Verfallsdatum gesetzt. Es wird davon ausgegangen, dass alle Dateien auf diesem Datenträger entweder bereits verfallen sind oder an diesem Tag verfallen. Am folgenden Tag sind keine gültigen Daten mehr auf diesem Datenträger vorhanden.

Das Ende des Konsolidierungszeitraums (END RECLAIM PERIOD) wird auf das Datum einen Monat nach dem Anfang des Konsolidierungszeitraums (BEGIN RECLAIM PERIOD) gesetzt. Das Datum für das Ende des Aufbewahrungszeitraums, das auf dem NetApp-Dateiserver für diesen Datenträger festgelegt ist, wird auf das Datum für END RECLAIM PERIOD gesetzt. Der NetApp-Dateiserver verhindert das Löschen dieses Datenträgers, bis das Datum für END RECLAIM PERIOD erreicht wird. Dieses Datum liegt ungefähr einen Monat nach dem Verfall der Daten auf dem IBM Spectrum Protect-Server. Wenn der IBM Spectrum Protect-Server ein Datum für END RECLAIM PERIOD für einen Datenträger berechnet und das Datum nach dem aktuellen Datum für END RECLAIM PERIOD liegt, wird das Datum auf dem NetApp-Dateiserver für diesen Datenträger auf das spätere Datum zurückgesetzt. Indem das Datum auf ein späteres Datum zurückgesetzt wird, wird sichergestellt, dass der IBM Spectrum Protect-WORM-FILE-Datenträger erst gelöscht wird, nachdem alle Daten auf dem Datenträger verfallen sind oder die Daten auf einen anderen SnapLock-Datenträger versetzt wurden.

Der IBM Spectrum Protect-Konsolidierungszeitraum ist der Zeitraum zwischen dem Anfangsdatum und dem Enddatum. Während des Konsolidierungszeitraums löscht der IBM Spectrum Protect-Server Datenträger, auf denen alle Daten verfallen sind, oder versetzt Dateien, die nicht verfallen sind und sich auf SnapLock-Datenträgern befinden, die verfallen, auf neue SnapLock-Datenträger mit neuen Datumsangaben. Dieser Monat ist entscheidend dafür, wie der Server die Daten auf WORM-FILE-Datenträgern sicher und effizient verwaltet. Daten auf einem SnapLock-Datenträger verfallen normalerweise, wenn das Anfangsdatum erreicht wird; außerdem muss der Datenträger leer sein. Wenn das Enddatum erreicht wird, kann der Datenträger gefahrlos aus dem IBM Spectrum Protect-Bestand und auf dem SnapLock-Dateiserver gelöscht werden.

Einige Ereignisse können jedoch zur Folge haben, dass sich gültige Daten auf einem SnapLock-Datenträger befinden:

- Die Verfallsverarbeitung auf dem IBM Spectrum Protect-Server für diesen Datenträger wurde möglicherweise verzögert oder ist nicht abgeschlossen.
- Die Aufbewahrungsparameter in der Kopiengruppe oder in den zugeordneten Verwaltungsklassen wurden möglicherweise für eine Datei nach deren Archivierung geändert und diese Datei wird für einige Zeit nicht verfallen.
- Einer oder mehreren Dateien auf dem Datenträger wurde möglicherweise der Status 'Löschen unzulässig' zugeordnet.
- Die Konsolidierungsverarbeitung ist entweder inaktiviert oder während der Konsolidierungsverarbeitung treten beim Versetzen von Daten auf neue SnapLock-Datenträger in einem SnapLock-Speicherpool Fehler auf.
- Eine Datei wartet auf das Eintreten eines Ereignisses, bevor der IBM Spectrum Protect-Server den Verfall der Datei starten kann.

Wenn das Anfangsdatum erreicht wird und Dateien auf einem SnapLock-Datenträger vorhanden sind, die nicht verfallen sind, müssen die Dateien auf einen neuen SnapLock-Datenträger mit einem neuen Anfangs- und Enddatum versetzt werden. Wenn sich die Verfallsverarbeitung auf dem IBM Spectrum Protect-Server jedoch verzögert und diese Dateien verfallen, wenn die Verfallsverarbeitung auf dem IBM Spectrum Protect-Server ausgeführt wird, ist es ineffizient, diese Dateien auf einen neuen SnapLock-Datenträger zu versetzen. Um sicherzustellen, dass keine unnötige Datenversetzung für Dateien stattfindet, die verfallen werden, wird das Versetzen von Dateien auf SnapLock-Datenträger, die verfallen, um einige Tage nach dem Datum für BEGIN RECLAIM PERIOD verzögert. Da die Daten auf dem SnapLock-Dateiserver bis zum Datum für END RECLAIM PERIOD geschützt sind, sind die Daten durch die Verzögerung dieser Versetzung nicht gefährdet. Damit kann die IBM Spectrum Protect-Verfallsverarbeitung beendet werden. Wenn nach dieser Anzahl Tage gültige Daten auf einem SnapLock-Datenträger, der verfällt, vorhanden sind, werden die Daten auf einen neuen SnapLock-Datenträger versetzt und die Daten bleiben demzufolge geschützt.

Seit dem ersten Archivieren der Daten wurden möglicherweise Änderungen an den Aufbewahrungsparametern für diese Daten vorgenommen (beispielsweise Änderungen an den Verwaltungsklassen- oder Kopienpoolparametern) oder diese Daten haben möglicherweise den Status 'Löschen unzulässig'. Die Daten auf diesem Datenträger werden jedoch von SnapLock nur bis zum Datum für END RECLAIM PERIOD geschützt. Daten, die nicht verfallen sind, werden während des IBM Spectrum Protect-Konsolidierungszeitraums auf neue SnapLock-Datenträger versetzt. Wenn beim Versetzen von Daten auf einen neuen SnapLock-Datenträger Fehler auftreten, wird eine Warnung ausgegeben, die angibt, dass die Daten bald nicht mehr geschützt sind. Wenn der Fehler bestehen bleibt, geben Sie einen Befehl MOVE DATA für den betreffenden Datenträger aus.

Achtung: Inaktivieren Sie die Konsolidierungsverarbeitung für einen SnapLock-Speicherpool nicht. Nach der Inaktivierung der Verarbeitung hat der IBM Spectrum Protect-Server keine Möglichkeit, Warnungen auszugeben, die angeben, dass die Daten bald nicht mehr geschützt sind. Diese Situation kann auch auftreten, wenn Konsolidierung und Umlagerung für den gesamten Server inaktiviert werden (wenn beispielsweise NOMIGRRECL in der Serveroptionsdatei definiert wird). Stellen Sie sicher, das Ihre Daten geschützt sind, wenn Sie SnapLock-Speicherpools verwalten.

Konfiguration des Features SnapLock für die ereignisgesteuerte Aufbewahrung

Auf SnapLock-Datenträgern gespeicherte Daten, die durch IBM Spectrum Protect for Data Retention und ereignisgesteuerte Aufbewahrung verwaltet werden, können zu exzessiver Konsolidierung führen, was Leistungseinbußen auf dem Server zur Folge hat.

Wenn Daten durch die ereignisgesteuerte Aufbewahrung verwaltet werden, setzt IBM Spectrum Protect anfänglich den Aufbewahrungszeitraum auf den größeren der beiden Werte für RETVER und RETMIN für die Archivierungskopiengruppe. Wenn der Konsolidierungszeitraum für den Datenträger beginnt und Daten, die auf dem Datenträger verbleiben, versetzt werden, wird der Aufbewahrungszeitraum für den Zieldatenträger auf den verbleibenden Aufbewahrungszeitraum der Daten gesetzt, der normalerweise 0 ist. Für den neuen Datenträger beginnt dann der Konsolidierungszeitraum kurz nachdem der Datenträger die Daten empfängt, was die Konsolidierung von Datenträgern zur Folge hat, die gerade erstellt wurden.

Sie können diese Situation durch Verwendung der Serveroption RETENTIONEXTENSION vermeiden. Mit dieser Option kann der Server das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers festlegen oder erweitern. Sie können einen Wert im Bereich von 30 bis 9999 Tagen angeben. Der Standardwert ist 365 Tage.

Wenn Sie Datenträger in einem SnapLock-Speicherpool für die Konsolidierung auswählen, prüft der Server, ob sich der Datenträger innerhalb des Konsolidierungszeitraums befindet:

- Wenn sich der Datenträger nicht innerhalb des Konsolidierungszeitraums befindet, wird keine Aktion ausgeführt. Der Datenträger wird nicht konsolidiert und das Ende des Aufbewahrungszeitraums bleibt unverändert.
- Wenn sich der Datenträger innerhalb des Konsolidierungszeitraums befindet, prüft der Server, ob der Prozentsatz des konsolidierbaren Speicherbereichs auf dem Datenträger größer als der Konsolidierungsschwellenwert des Speicherpools oder größer als der Prozentsatz für den Schwellenwert ist, der im Parameter THRESHOLD eines Befehls RECLAIM STGPOOL übergeben wurde:
  - Wenn der konsolidierbare Speicherbereich größer als der Schwellenwert ist, konsolidiert der Server den Datenträger und setzt das den Wert für das Ende des Aufbewahrungszeitraums des Zieldatenträgers auf den größeren der folgenden Werte:
    - Der verbleibende Aufbewahrungszeitraum der Daten plus 30 Tage für den Konsolidierungszeitraum.
    - Der Wert für RETENTIONEXTENSION plus 30 Tage für den Konsolidierungszeitraum.
  - Wenn der konsolidierbare Speicherbereich nicht größer als der Schwellenwert ist, ändert der Server den Wert für das Ende des Aufbewahrungszeitraums des Datenträgers gemäß dem in der Option RETENTIONEXTENSION angegebenen Wert. Der neue Aufbewahrungszeitraum wird berechnet, indem die angegebene Anzahl Tage zum aktuellen Datum addiert wird.

In den folgenden Beispielen befindet sich der SnapLock-Datenträger VolumeA in einem Speicherpool, dessen Konsolidierungsschwellenwert auf 60 % gesetzt ist. Die Serveroption RETENTIONEXTENSION ist auf 365 Tage gesetzt. Der Aufbewahrungszeitraum für VolumeA liegt innerhalb des Konsolidierungszeitraums. Die folgenden Situationen zeigen die Auswirkungen auf den Aufbewahrungszeitraum:

- Der konsolidierbare Speicherbereich auf VolumeA liegt unter 60 %. Das Ende des Aufbewahrungszeitraums von VolumeA wird um 365 Tage verlängert.
- Der konsolidierbare Speicherbereich auf VolumeA ist größer als 60 % und der verbleibende Aufbewahrungszeitraum der Daten beträgt mehr als 365 Tage. VolumeA wird konsolidiert und das Ende des Aufbewahrungszeitraums des Zieldatenträgers wird auf der Basis des verbleibenden Aufbewahrungszeitraums der Daten plus 30 Tage für den Konsolidierungszeitraum gesetzt.
- Der konsolidierbare Speicherbereich auf VolumeA ist größer als 60 % und der Aufbewahrungszeitraum der Daten beträgt weniger als 365 Tage. VolumeA wird konsolidiert und das Ende des Aufbewahrungszeitraums für VolumeA wird auf 365 Tage, den Wert für RETENTIONEXTENTION, plus 30 Tage für den Konsolidierungszeitraum gesetzt.

Unterbrechungsfreier Datenschutz mit dem SnapLock-Feature

Wenn Daten auf einem Datenträger mit aktiviertem SnapLock-Feature gespeichert sind und die Daten auf einen Datenträger, auf dem das SnapLock-Feature nicht aktiviert ist, versetzt oder kopiert werden, verlieren die Daten den einzigartigen Hardwareschutz, der durch NetApp-WORM-Datenträger zur Verfügung gestellt wird.

Der IBM Spectrum Protect-Server erlaubt diesen Typ der Versetzung. Wenn die Daten jedoch von einem WORM-FILE-Datenträger auf einen anderen Typ von Datenträger versetzt werden, sind die Daten möglicherweise nicht mehr vor unbeabsichtigtem oder böswilligem Löschen geschützt. Wenn sich diese Daten zur Erfüllung von Datenaufbewahrungs- und Datenschutzanforderungen aus rechtlichen Gründen auf WORM-Datenträgern befinden und auf andere Datenträger versetzt werden, erfüllen die Daten möglicherweise nicht mehr diese Anforderungen. Sie müssen Ihre Speicherpools so konfigurieren, dass dieser Typ von Daten in Speicherpools aufbewahrt wird, die während des gesamten Datenaufbewahrungszeitraums aus SnapLock-WORM-Datenträgern bestehen.

SnapLock-Datenträger als IBM Spectrum Protect-WORM-FILE-Datenträger konfigurieren

Um die strengen Anforderungen für archivierte Daten zu erfüllen, aktivieren Sie das NetApp-Feature SnapLock.

Informationen zu diesem Vorgang

Wenn Sie Konfigurationen, die SnapLock-Speicherpools einbeziehen, definieren oder aktualisieren, müssen Sie sicherstellen, dass die Option RECLAMATIONTYPE=SNAPLOCK für die Speicherpools, die für die Parameter NEXTSTGPOOL, RECLAIMSTGPOOL und COPYSTGPOOLS ausgewählt wurden, angegeben ist.

Indem Sie die Speicherpools auf diese Art und Weise konfigurieren, kann sichergestellt werden, dass Ihre Daten ordnungsgemäß geschützt sind. Wenn Sie einen nächsten Speicherpool, einen Konsolidierungsspeicherpool, einen Kopienspeicherpool oder einen Pool für aktive Daten definieren, ohne die Option RECLAMATIONTYPE=SNAPLOCK auszuwählen, ist der Speicherpool nicht geschützt. Der Befehl wird zwar erfolgreich ausgeführt, es wird jedoch eine Warnung ausgegeben.

Vorgehensweise

Um einen SnapLock-Datenträger für die Verwendung als IBM Spectrum Protect-WORM-FILE-Datenträger zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Installieren und konfigurieren Sie SnapLock auf dem NetApp-Dateiserver. Stellen Sie sicher, dass Sie den minimalen, den maximalen und den Standardaufbewahrungszeitraum konfigurieren. Anweisungen finden Sie in der NetApp-Dokumentation.
2. Installieren und konfigurieren Sie einen IBM Spectrum Protect-Server.
3. Aktivieren Sie den Aufbewahrungsschutz für Archivierungsdaten, indem Sie den Befehl SET ARCHIVERETENTIONPROTECTION ausgeben:

   ```
   set archiveretentionprotection on
   ```

4. Konfigurieren Sie die Maßnahme mithilfe des Befehls DEFINE COPYGROUP. Wählen Sie für RETVER und RETMIN in der Archivierungskopiengruppe Werte aus, die Ihre Anforderungen zum Schützen dieser Daten im WORM-Speicher erfüllen. Wenn für RETVER oder RETMIN keine Werte angegeben werden, werden die Werte der Standardverwaltungsklasse verwendet.
5. Konfigurieren Sie Speicher mithilfe des Befehls DEFINE DEVCLASS.
   - Verwenden Sie die Einheitenklasse FILE.
   - Geben Sie den Parameter DIRECTORY an, um auf das Verzeichnis oder die Verzeichnisse auf den SnapLock-Datenträgern zu verweisen.
6. Definieren Sie einen Speicherpool unter Verwendung der Einheitenklasse, die in Schritt 5 definiert wurde, indem Sie den Befehl DEFINE STGPOOL unter Angabe des Parameters RECLAMATIONTYPE=SNAPLOCK ausgeben.
7. Aktualisieren Sie die Kopiengruppe so, dass sie auf den Speicherpool verweist, indem Sie den Befehl UPDATE COPYGROUP ausgeben.
8. Verwenden Sie die IBM Spectrum Protect-API zum Archivieren Ihrer Objekte im SnapLock-Speicherpool. Dieses Feature ist in IBM Spectrum Protect-Standardclients für Sichern/Archivieren nicht verfügbar.

Daten in Verzeichniscontainerspeicherpools reparieren und wiederherstellen

Sie können beschädigte Datenbereiche in Verzeichniscontainerspeicherpools reparierenund verloren gegangene Daten nach einem Katastrophenfall wiederherstellen.

Datenbereiche gehören zu einer Datei, die während des Datendeduplizierungsprozesses erstellt wird. Bereiche werden mit anderen Dateibereichen verglichen, um doppelte Daten zu identifizieren. Wenn in Ihren Verzeichniscontainerspeicherpools beschädigte Dateien oder Verzeichnisse vorhanden sind, können Sie deduplizierte Datenbereiche mithilfe des Zielreplikationsservers, des Quellenreplikationsservers oder mithilfe von Banddatenträgern in Containerkopienspeicherpools reparieren.

- Speicherpools mithilfe eines Zielreplikationsservers reparieren
  Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenreplikationsserver beschädigt sind, können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver mithilfe eines Zielreplikationsservers reparieren.
- Speicherpools mithilfe von Datenträgern in Containerkopienspeicherpools reparieren
  Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenserver reparieren, indem Sie die deduplizierten Datenbereiche von Banddatenträgern in Containerkopienspeicherpools, die sich vor Ort oder an einem anderen Standort befinden, abrufen.
- Speicherpools in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopienspeicherpools reparieren
  Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver reparieren, indem Sie die deduplizierten Datenbereiche vom Zielreplikationsserver oder von Banddatenträgern in Containerkopienspeicherpools abrufen.
- Speicherpools auf einem Zielreplikationsserver reparieren
  Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Zielreplikationsserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver reparieren, indem Sie die deduplizierten Datenbereiche vom Quellenreplikationsserver abrufen.
- Speicherpools nach einem Katastrophenfall reparieren
  Nach einem Katastrophenfall können Sie Verzeichniscontainerspeicherpools reparieren und die zugehörigen verloren gegangenen Daten wiederherstellen.
- Beschädigten Banddatenträger im Containerkopienspeicherpool ersetzen
  Wenn ein Banddatenträger, der eine Kopie deduplizierter Datenbereiche in einem Containerkopienspeicherpool speichert, beschädigt wird, können Sie den Datenträger ersetzen.

Zugehörige Konzepte:
Strategien zum Schutz vor Katastrophen
Zugehörige Tasks:
Datenschutzlösungen
Wiederherstellung nach einem Datenverlust oder Systemausfall

Speicherpools mithilfe eines Zielreplikationsservers reparieren

Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenreplikationsserver beschädigt sind, können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver mithilfe eines Zielreplikationsservers reparieren.

Vorbereitende Schritte

Evaluieren Sie Ihre Speicherumgebung, um festzustellen, ob Ausfälle, Netzprobleme oder Hardwarefehler zu einer Beschädigung an Daten führen oder zur Folge haben, dass die Daten beschädigt zu sein scheinen. Wenn Probleme in Ihrer Umgebung zu einer Beschädigung an Daten führen, ermitteln und beheben Sie die Probleme.

Stellen Sie sicher, dass in dem Verzeichniscontainerspeicherpool genügend Speicherbereich für die wiederhergestellten Daten verfügbar ist. Der Parameter PREVIEW=YES im Befehl REPAIR STGPOOL gibt an, welches Datenvolumen repariert wird. Wenn nicht genügend Speicherbereich vorhanden ist, stellen Sie mithilfe des Befehls DEFINE STGPOOLDIRECTORY Speicherbereich bereit.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um die folgenden Typen von Beschädigungen zu reparieren:

- Geringfügige Beschädigung, die durch das versehentliche Löschen von Dateien oder Verzeichnissen, überschriebene Dateien, versehentliche Änderungen an Dateiberechtigungen oder Plattenfehler aufgrund von Hardwareproblemen verursacht werden.
- Moderate Beschädigung, die durch Plattenfehler oder Datenträgermountfehler verursacht wird. Dieser Typ von Beschädigung hat den Verlust einer oder mehrerer Verzeichnisse zur Folge, aber nicht den Verlust des gesamten Speicherpools.

Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die auf dem Zielreplikationsserver geschützt wurden.
Einschränkung: Sie können den Befehl REPAIR STGPOOL für einen angegebenen Speicherpool nur ausgeben, wenn die Daten mit dem Befehl PROTECT STGPOOL bereits in einen anderen Speicherpool auf einem Zielreplikationsserver kopiert wurden.
Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe eines Replikationsservers reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Zielreplikationsserver ist nicht verfügbar.
- Der Zielspeicherpool ist beschädigt.
- Es tritt ein Netzausfall auf.

Vorgehensweise

1. Wenn Sie eine geringfügige Beschädigung vermuten, geben Sie den Befehl AUDIT CONTAINER für den Containerspeicherpool auf Verzeichnisebene aus, um Inkonsistenzen zwischen der Datenbank und dem Verzeichniscontainerspeicherpool zu identifizieren. Indem Sie beschädigte Datenbereiche im Verzeichniscontainerspeicherpool identifizieren, können Sie die zu reparierenden Datenbereiche bestimmen. Um Zeit und Ressourcen einzusparen, prüfen Sie nur Container, bei denen Sie eine Beschädigung vermuten. Wenn Sie vermuten, dass Ihr Verzeichniscontainerspeicherpool eine schwerwiegendere Beschädigung aufweist, geben Sie den Befehl AUDIT CONTAINER auf Speicherpoolebene aus.
   Um beispielsweise ein Verzeichnis, n:\pooldir, in einem Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

   ```
   audit container stgpool=stgpool1 stgpooldirectory=n:\pooldir
   ```

   Um einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

   ```
   audit container stgpool=stgpool1
   ```

   Die Ausführung des Prüfprozesses kann mehrere Stunden dauern.

2. Um einen Verzeichniscontainerspeicherpool zu reparieren, geben Sie den Befehl REPAIR STGPOOL unter Angabe des Parameters SRCLOCATION=REPLSERVER aus. Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 mithilfe eines Replikationsservers zu reparieren, geben Sie den folgenden Befehl aus:

   ```
   repair stgpool stgpool1 srclocation=replserver
   ```

   Wenn Sie den Befehl REPAIR STGPOOL ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter REUSEDELAY angegebenen Wert beibehalten.

3. Identifizieren Sie alle weiteren beschädigten Bereiche, indem Sie den Befehl QUERY DAMAGED ausgeben.
4. Wenn eine Beschädigung erkannt wird und deduplizierte Speicherbereiche nicht mithilfe des Replikationsservers repariert werden können, ist eine Reparatur dennoch möglich. In einigen Fällen sendet der Clientknoten Daten im Rahmen einer Sicherungsoperation erneut und die beschädigten Bereiche werden repariert. Warten Sie für die Dauer von zwei Sicherungszyklen, um die Ausführung von Clientsicherungsoperationen zu ermöglichen. Führen Sie im Anschluss an zwei Sicherungszyklen die folgenden Schritte aus:
   a. Um zu prüfen, ob die Beschädigung repariert wurde, geben Sie den Befehl QUERY DAMAGED erneut aus.
   b. Wenn ein vollständiges Speicherpoolverzeichnis beschädigt ist, erstellen Sie ein neues Speicherpoolersatzverzeichnis mithilfe des Befehls DEFINE STGPOOLDIRECTORY.
   c. Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus.
      Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 zu prüfen und beschädigte Objekte zu entfernen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=removedamaged
```

d. Wahlweise können Sie den Befehl DELETE STGPOOLDIRECTORY ausgeben, um das leere Speicherpoolverzeichnis, das Sie in Schritt 4.b durch ein neues Verzeichnis ersetzt hatten, zu löschen.

Nächste Schritte

Wenn Sie im Laufe der Zeit immer wieder beschädigte Daten erkennen, geben Sie den Befehl AUDIT CONTAINER für den Verzeichniscontainerspeicherpool aus, um festzustellen, ob eine umfangreichere Beschädigung vorliegt. Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1
```

Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)
QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)
PROTECT STGPOOL (Speicherpooldaten schützen)
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)
DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)
DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)

Speicherpools mithilfe von Datenträgern in Containerkopienspeicherpools reparieren

Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenserver reparieren, indem Sie die deduplizierten Datenbereiche von Banddatenträgern in Containerkopienspeicherpools, die sich vor Ort oder an einem anderen Standort befinden, abrufen.

Vorbereitende Schritte

Evaluieren Sie Ihre Speicherumgebung, um festzustellen, ob Ausfälle, Netzprobleme oder Hardwarefehler zu einer Beschädigung an Daten führen oder zur Folge haben, dass die Daten beschädigt zu sein scheinen. Wenn Probleme in Ihrer Umgebung zu einer Beschädigung an Daten führen, ermitteln und beheben Sie die Probleme.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um die folgenden Typen von Beschädigungen zu reparieren:

- Geringfügige Beschädigung, die durch das versehentliche Löschen von Dateien oder Verzeichnissen, überschriebene Dateien, versehentliche Änderungen an Dateiberechtigungen oder Plattenfehler aufgrund von Hardwareproblemen verursacht werden.
- Moderate Beschädigung, die durch Plattenfehler oder Datenträgermountfehler verursacht wird. Dieser Typ von Beschädigung hat den Verlust einer oder mehrerer Verzeichnisse zur Folge, aber nicht den Verlust des gesamten Speicherpools.

Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die in Containerkopienspeicherpools geschützt wurden.
Einschränkung: Sie können den Befehl REPAIR STGPOOL für einen angegebenen Speicherpool nur ausgeben, wenn die Daten mit dem Befehl PROTECT STGPOOL bereits in Containerkopienspeicherpools kopiert wurden.
Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe von Containerkopienpools reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Containerkopienspeicherpool ist nicht verfügbar.
- Der Containerkopienspeicherpool ist beschädigt.
- Die Datenträger in Containerkopienspeicherpools sind nicht verfügbar oder beschädigt.

Vorgehensweise

1. Wenn Sie eine geringfügige Beschädigung vermuten, geben Sie den Befehl AUDIT CONTAINER für den Containerspeicherpool auf Verzeichnisebene aus, um Inkonsistenzen zwischen der Datenbank und dem Verzeichniscontainerspeicherpool zu identifizieren. Indem Sie beschädigte Datenbereiche im Verzeichniscontainerspeicherpool identifizieren, können Sie die zu reparierenden Datenbereiche bestimmen. Um Zeit und Ressourcen einzusparen, prüfen Sie nur Container, bei denen Sie eine Beschädigung vermuten. Wenn Sie vermuten, dass Ihr Containerspeicherpool eine schwerwiegendere Beschädigung aufweist, geben Sie den Befehl AUDIT CONTAINER auf Speicherpoolebene aus. Um beispielsweise ein Verzeichnis, n:\pooldir, in einem Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

   ```
   audit container stgpool=stgpool1 stgpooldirectory=n:\pooldir
   ```

   Um einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

   ```
   audit container stgpool=stgpool1
   ```

Die Ausführung des Prüfprozesses kann mehrere Stunden dauern.

Während der Reparaturoperation fordert der Server von Ihnen die erforderlichen Datenträger an. In Schritt 3 werden die Datenträger wieder vor Ort gebracht und in das Speicherarchiv zurückgestellt. Die erforderlichen Datenträger müssen vor Ort gebracht und in das Speicherarchiv zurückgestellt werden.

2. Um eine Voranzeige der Reparaturoperation aufzurufen und die Liste der für die Reparaturoperation erforderlichen Banddatenträger zu generieren, geben Sie den Befehl REPAIR STGPOOL unter Angabe der Parameter SRCLOCATION=LOCAL und PREVIEW=YES aus.
   Um beispielsweise für einen Speicherpool mit dem Namen STGPOOL1 eine Voranzeige der Reparaturoperation mithilfe von Containerkopienspeicherpools aufzurufen, geben Sie den folgenden Befehl aus:

   ```
   repair stgpool stgpool1 srclocation=local preview=yes
   ```

   Die Ausführung des Voranzeigeprozesses kann einige Zeit in Anspruch nehmen.

3. Wenn sich einige der erforderlichen Datenträger an einen anderen Standort befinden, führen Sie die folgenden Schritte aus:
   a. Bestimmen Sie mithilfe der Liste der Voranzeigeoperation, welche Datenträger vor Ort gebracht werden müssen.
   b. Wenn sich die Datenträger wieder vor Ort befinden, stellen Sie diese in das Speicherarchiv zurück, indem Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters STATUS=PRIVATE ausgeben.
   c. Aktualisieren Sie den Status der Datenträger, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters ACCESS=READWRITE ausgeben.

   Detaillierte Anweisungen zur Funktion Disaster Recovery Manager (DRM) finden Sie in Disaster Recovery Manager für Bandumgebungen verwenden (Version 7.1.1).
4. Stellen Sie auf der Basis der Informationen, die während der Voranzeigeoperation abgerufen wurden, sicher, dass der Speicherpool über genügend Speicherbereich für die wiederhergestellten Daten verfügt. Wenn nicht genügend Speicherbereich vorhanden ist, stellen Sie mithilfe des Befehls DEFINE STGPOOLDIRECTORY Speicherbereich bereit.
5. Um den Verzeichniscontainerspeicherpool zu reparieren, geben Sie den Befehl REPAIR STGPOOL unter Angabe des Parameters SRCLOCATION=LOCAL aus.
   Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 mithilfe eines Containerkopienspeicherpools zu reparieren, geben Sie den folgenden Befehl aus:

   ```
   repair stgpool stgpool1 srclocation=local
   ```

   Wenn Sie den Befehl REPAIR STGPOOL ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter REUSEDELAY angegebenen Wert beibehalten.

6. Identifizieren Sie alle weiteren beschädigten Bereiche, indem Sie den Befehl QUERY DAMAGED ausgeben.
7. Wenn eine Beschädigung erkannt wird und deduplizierte Speicherbereiche nicht mithilfe der Containerkopienspeicherpools repariert werden können, ist eine Reparatur dennoch möglich. In einigen Fällen sendet der Clientknoten Daten im Rahmen einer Sicherungsoperation erneut und die beschädigten Bereiche werden repariert. Warten Sie für die Dauer von zwei Sicherungszyklen, um die Ausführung von Clientsicherungsoperationen zu ermöglichen. Führen Sie im Anschluss an zwei Sicherungszyklen die folgenden Schritte aus:
   a. Um zu prüfen, ob die Beschädigung repariert wurde, geben Sie den Befehl QUERY DAMAGED erneut aus.
   b. Wenn ein vollständiges Speicherpoolverzeichnis beschädigt ist, erstellen Sie ein neues Speicherpoolersatzverzeichnis mithilfe des Befehls DEFINE STGPOOLDIRECTORY.
   c. Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus.
      Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 zu prüfen und beschädigte Objekte zu entfernen, geben Sie den folgenden Befehl aus:

      ```
      audit container stgpool=stgpool1 action=removedamaged
      ```

   d. Wahlweise können Sie den Befehl DELETE STGPOOLDIRECTORY ausgeben, um das leere Speicherpoolverzeichnis, das Sie in Schritt 7.b durch ein neues Verzeichnis ersetzt hatten, zu löschen.
8. Wenn ein vollständiges Speicherpoolverzeichnis repariert wurde, löschen Sie das ursprüngliche Verzeichnis, das leer ist und durch ein neues Verzeichnis ersetzt wurde. Löschen Sie das ursprüngliche Verzeichnis, indem Sie den Befehl DELETE STGPOOLDIRECTORY ausgeben.

Nächste Schritte

Wenn Sie im Laufe der Zeit immer wieder beschädigte Daten erkennen, geben Sie den Befehl AUDIT CONTAINER für den Verzeichniscontainerspeicherpool aus, um festzustellen, ob eine umfangreichere Beschädigung vorliegt. Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1
```

Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)
QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)
PROTECT STGPOOL (Speicherpooldaten schützen)
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)

DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)
DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)

Speicherpools in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopienspeicherpools reparieren

Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Quellenserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver reparieren, indem Sie die deduplizierten Datenbereiche vom Zielreplikationsserver oder von Banddatenträgern in Containerkopienspeicherpools abrufen.

Vorbereitende Schritte

Evaluieren Sie Ihre Speicherumgebung, um festzustellen, ob Ausfälle, Netzprobleme oder Hardwarefehler zu einer Beschädigung an Daten führen oder zur Folge haben, dass die Daten beschädigt zu sein scheinen. Wenn Probleme in Ihrer Umgebung zu einer Beschädigung an Daten führen, ermitteln und beheben Sie die Probleme.

Stellen Sie sicher, dass in dem Verzeichniscontainerspeicherpool genügend Speicherbereich für die wiederhergestellten Daten verfügbar ist. Der Parameter PREVIEW=YES im Befehl REPAIR STGPOOL gibt an, welches Datenvolumen repariert wird. Wenn nicht genügend Speicherbereich vorhanden ist, stellen Sie mithilfe des Befehls DEFINE STGPOOLDIRECTORY Speicherbereich bereit.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um die folgenden Typen von Beschädigungen zu reparieren:

- Geringfügige Beschädigung, die durch das versehentliche Löschen von Dateien oder Verzeichnissen, überschriebene Dateien, versehentliche Änderungen an Dateiberechtigungen oder Plattenfehler aufgrund von Hardwareproblemen verursacht werden.
- Moderate Beschädigung, die durch Plattenfehler oder Datenträgermountfehler verursacht wird. Dieser Typ von Beschädigung hat den Verlust einer oder mehrerer Verzeichnisse zur Folge, aber nicht den Verlust des gesamten Speicherpools.

Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die auf dem Zielreplikationsserver oder in Containerkopienspeicherpools auf einem Quellenserver geschützt wurden.
Einschränkung: Sie können den Befehl REPAIR STGPOOL für einen angegebenen Speicherpool nur ausgeben, wenn die Daten mit dem Befehl PROTECT STGPOOL bereits in einen anderen Speicherpool auf einem Zielreplikationsserver oder in Containerkopienspeicherpools kopiert wurden.
Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Zielreplikationsserver ist nicht verfügbar.
- Der Zielspeicherpool ist beschädigt.
- Es tritt ein Netzausfall auf.

Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe von Containerkopienpools reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Containerkopienspeicherpool ist nicht verfügbar.
- Der Containerkopienspeicherpool ist beschädigt.
- Die Datenträger in Containerkopienspeicherpools sind nicht verfügbar oder beschädigt.

Vorgehensweise

1. Versuchen Sie, den Speicherpool mithilfe des Zielreplikationsservers zu reparieren, indem Sie die Schritte in Speicherpools mithilfe eines Zielreplikationsservers reparieren ausführen.
2. Wenn die beschädigten Bereiche nicht mithilfe des Zielreplikationsservers repariert werden können, reparieren Sie die beschädigten Bereiche mithilfe von Containerkopienspeicherpools, indem Sie die Schritte in Speicherpools mithilfe von Datenträgern in Containerkopienspeicherpools reparieren ausführen.
3. Wenn Sie beschädigte Bereiche mithilfe von Containerkopienspeicherpools repariert hatten, geben Sie den Befehl PROTECT STGPOOL unter Angabe des Parameters TYPE=REPLSERVER für die Speicherpools auf dem Quellenreplikationsserver aus.

Nächste Schritte

Wenn Sie im Laufe der Zeit immer wieder beschädigte Daten erkennen, geben Sie den Befehl AUDIT CONTAINER für den Verzeichniscontainerspeicherpool aus, um festzustellen, ob eine umfangreichere Beschädigung vorliegt. Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1
```

Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)
PROTECT STGPOOL (Speicherpooldaten schützen)
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)
DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)
DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)

Speicherpools auf einem Zielreplikationsserver reparieren

Wenn Dateien, Verzeichnisse oder Speicherpools auf einem Zielreplikationsserver beschädigt sind, können Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver reparieren, indem Sie die deduplizierten Datenbereiche vom Quellenreplikationsserver abrufen.

Vorbereitende Schritte

Evaluieren Sie Ihre Speicherumgebung, um festzustellen, ob Ausfälle, Netzprobleme oder Hardwarefehler zu einer Beschädigung an Daten führen oder zur Folge haben, dass die Daten beschädigt zu sein scheinen. Wenn Probleme in Ihrer Umgebung zu einer Beschädigung an Daten führen, ermitteln und beheben Sie die Probleme.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um die folgenden Typen von Beschädigungen zu reparieren:

- Geringfügige Beschädigung, die durch das versehentliche Löschen von Dateien oder Verzeichnissen, überschriebene Dateien, versehentliche Änderungen an Dateiberechtigungen oder Plattenfehler aufgrund von Hardwareproblemen verursacht werden.
- Moderate Beschädigung, die durch Plattenfehler oder Datenträgermountfehler verursacht wird. Dieser Typ von Beschädigung hat den Verlust einer oder mehrerer Verzeichnisse zur Folge, aber nicht den Verlust des gesamten Speicherpools.

Im Rahmen der Ausführung des Befehls PROTECT STGPOOL werden beschädigte Speicherbereiche im Zielspeicherpool repariert. Eine Reparatur ist nur möglich, wenn die Speicherbereiche auf dem Zielserver bereits als beschädigt markiert sind. Beispielsweise kann vor der Ausgabe des Befehls PROTECT STGPOOL mit einem Befehl AUDIT CONTAINER eine Beschädigung im Zielspeicherpool identifiziert werden.

Vorgehensweise

1. Schützen Sie Datenbereiche in einem Verzeichniscontainerspeicherpool auf einem Quellenserver, indem Sie den Befehl PROTECT STGPOOL ausgeben.
   Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen POOL1 zu schützen, geben Sie den folgenden Befehl aus:

   ```
   protect stgpool pool1
   ```

   Warten Sie, bis der Prozess zum Schützen beendet ist.

2. Um die beschädigten Datenbereiche in dem Verzeichniscontainerspeicherpool auf dem Zielserver zu identifizieren, geben Sie den Befehl AUDIT CONTAINER aus.
   Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen, geben Sie den folgenden Befehl aus:

   ```
   audit container stgpool=stgpool1
   ```

3. Reparieren Sie beschädigte Bereiche in dem Zielspeicherpool, indem Sie den Befehl PROTECT STGPOOL auf dem Quellenserver erneut ausgeben. Die beschädigten Bereiche im Zielspeicherpool werden als beschädigt markiert und repariert.
4. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl QUERY DAMAGED ausgeben.

Zugehörige Verweise:
AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)
DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)
QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)
PROTECT STGPOOL (Speicherpooldaten schützen)
REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)
DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)
DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)

Speicherpools nach einem Katastrophenfall reparieren

Nach einem Katastrophenfall können Sie Verzeichniscontainerspeicherpools reparieren und die zugehörigen verloren gegangenen Daten wiederherstellen.

Wenn ein Katastrophenfall eintritt und Ihr primärer Standort nicht mehr verfügbar ist, können Sie Ihre Verzeichniscontainerspeicherpools reparieren, indem Sie diese an Ihrem Wiederherstellungsstandort auf einen neuen Zielserver zurückschreiben.

- Speicherpools mithilfe von Datenträgern in Containerkopienspeicherpools nach einem Katastrophenfall reparieren
  Bei einem Katastrophenfall auf einem Quellenserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool

mithilfe von ausgelagerten Banddatenträgern in Containerkopienspeicherpools reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielserver am Wiederherstellungsstandort repariert.

- Speicherpools mithilfe eines Zielreplikationsservers nach einem Katastrophenfall reparieren
  Bei einem Katastrophenfall auf einem Quellenreplikationsserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielserver am Wiederherstellungsstandort repariert.
- Speicherpools in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopienspeicherpools nach einem Katastrophenfall reparieren
  Bei einem Katastrophenfall auf einem Quellenserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers oder mithilfe von ausgelagerten Banddatenträgern in Containerkopienspeicherpools reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielserver am Wiederherstellungsstandort repariert.

Zugehörige Verweise:
Bestimmen, ob Containerkopienspeicherpools für den Schutz vor Katastrophen verwendet werden können

Speicherpools mithilfe von Datenträgern in Containerkopienspeicherpools nach einem Katastrophenfall reparieren

Bei einem Katastrophenfall auf einem Quellenserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe von ausgelagerten Banddatenträgern in Containerkopienspeicherpools reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielserver am Wiederherstellungsstandort repariert.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um die folgenden Typen schwerwiegender Beschädigungen zu reparieren:

- Vollständiger Verlust aller Containerspeicherpools auf dem Quellenserver
- Vollständiger Verlust des primären Standorts

Für dieses Wiederherstellungsszenario gelten die folgenden Voraussetzungen:

- Sie hatten den Befehl PROTECT STGPOOL verwendet, um Daten von einem Quellenserver in Containerkopienspeicherpools an einem anderen Standort zu sichern. Sie hatten die ausgelagerten Banddatenträger abgerufen, sodass diese am Wiederherstellungsstandort vorhanden sind.
- Sie hatten nicht den Befehl PROTECT STGPOOL verwendet, um Daten auf einen Zielreplikationsserver zu sichern.
- Sie hatten die IBM Spectrum Protect-Blueprints verwendet, um den IBM Spectrum Protect-Quellenserver zu konfigurieren; außerdem hatten Sie die Blueprint-Konfigurationsscripts verwendet, um die Umgebung zurückzuschreiben, indem am Wiederherstellungsstandort ein neuer Zielserver konfiguriert wurde. Mit den Scripts wurden Sicherungsversionen der IBM Spectrum Protect-Datenbank, der Serveroptionsdatei (dsmserv.opt), der Protokolldatei für Datenträger (volhist.out) und der Einheitenkonfigurationsdatei (devconfig.out) an ihre ursprünglichen Positionen auf dem Wiederherstellungsserver kopiert. Nach der Ausführung der Scripts werden die neu erstellten, leeren Verzeichnisse auf dem Wiederherstellungsserver angezeigt.

Wenn Sie versuchen, einen Verzeichniscontainerspeicherpool mithilfe von Containerkopienpools zu reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Containerkopienspeicherpool ist nicht verfügbar.
- Der Containerkopienspeicherpool ist beschädigt.
- Die Datenträger in Containerkopienspeicherpools sind nicht verfügbar oder beschädigt.

Vorgehensweise

1. Markieren Sie alle Datenbereiche in dem Containerspeicherpool als beschädigt, indem Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=MARKDAMAGED für den Containerspeicherpool auf Speicherpoolebene ausgeben.
   Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen und als beschädigt zu markieren, geben Sie den folgenden Befehl aus:

   ```
   audit container stgpool=stgpool1 action=markdamaged
   ```

2. Wenn Sie den Verzeichniscontainerspeicherpool sowohl mit Containerkopienspeicherpools vor Ort als auch mit Containerkopienspeicherpools an einem anderen Standort geschützt hatten, geben Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters ACCESS=UNAVAILABLE für die Kopie des Containerkopienspeicherpools vor Ort aus.
3. Wenn sich die ausgelagerten Datenträger in Containerkopienspeicherpools wieder vor Ort befinden, stellen Sie diese in das Speicherarchiv zurück, indem Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters STATUS=PRIVATE ausgeben.
4. Aktualisieren Sie den Status der Datenträger, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters ACCESS=READWRITE ausgeben.
5. Reparieren Sie den Speicherpool, indem Sie den Befehl REPAIR STGPOOL unter Angabe des Parameters SRCLOCATION=LOCAL ausgeben.
   Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 mithilfe von Containerkopienspeicherpools an einem anderen Standort zu reparieren, geben Sie den folgenden Befehl aus:

```
repair stgpool stgpool1 srclocation=local
```

Wenn Sie den Befehl REPAIR STGPOOL ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter REUSEDELAY angegebenen Wert beibehalten.

6. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl QUERY DAMAGED ausgeben.
7. Wiederholen Sie diese Prozedur, um alle Ihre Speicherpools zu reparieren.

Speicherpools mithilfe eines Zielreplikationsservers nach einem Katastrophenfall reparieren

Bei einem Katastrophenfall auf einem Quellenreplikationsserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielserver am Wiederherstellungsstandort repariert.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um die folgenden Typen schwerwiegender Beschädigungen zu reparieren:

- Vollständiger Verlust aller Containerspeicherpools auf dem Quellenreplikationsserver
- Vollständiger Verlust des primären Standorts

Für dieses Wiederherstellungsszenario gelten die folgenden Voraussetzungen:

- Sie hatten den Befehl PROTECT STGPOOL verwendet, um Daten von einem Quellenreplikationsserver auf einen Zielreplikationsserver zu sichern. Der Zielreplikationsserver wird an Ihrem Wiederherstellungsstandort ausgeführt.
- Sie hatten nicht den Befehl PROTECT STGPOOL verwendet, um Daten in Containerkopienspeicherpools an einem anderen Standort zu sichern.
- Sie hatten die IBM Spectrum Protect-Blueprints verwendet, um den IBM Spectrum Protect-Quellenserver zu konfigurieren; außerdem hatten Sie die Blueprint-Konfigurationsscripts verwendet, um die Umgebung zurückzuschreiben, indem am Wiederherstellungsstandort ein neuer Zielserver konfiguriert wurde. Mit den Scripts wurden Sicherungsversionen der IBM Spectrum Protect-Datenbank, der Serveroptionsdatei (dsmserv.opt), der Protokolldatei für Datenträger (volhist.out) und der Einheitenkonfigurationsdatei (devconfig.out) an ihre ursprünglichen Positionen auf dem Wiederherstellungsserver kopiert. Nach der Ausführung der Scripts werden die neu erstellten, leeren Verzeichnisse auf dem Wiederherstellungsserver angezeigt.

Wenn Sie versuchen, einen Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers zu reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Zielreplikationsserver ist nicht verfügbar.
- Der Zielspeicherpool ist beschädigt.
- Es tritt ein Netzausfall auf.

Vorgehensweise

1. Markieren Sie alle Datenbereiche in dem Containerspeicherpool als beschädigt, indem Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=MARKDAMAGED für den Containerspeicherpool auf Speicherpoolebene ausgeben.
   Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen und als beschädigt zu markieren, geben Sie den folgenden Befehl aus:

   ```
   audit container stgpool=stgpool1 action=markdamaged
   ```

2. Reparieren Sie den Speicherpool, indem Sie den Befehl REPAIR STGPOOL unter Angabe des Parameters SRCLOCATION=REPLSERVER ausgeben.
   Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 mithilfe eines Zielreplikationsservers zu reparieren, geben Sie den folgenden Befehl aus:

   ```
   repair stgpool stgpool1 srclocation=replserver
   ```

   Wenn Sie den Befehl REPAIR STGPOOL ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter REUSEDELAY angegebenen Wert beibehalten.

3. Wenn Sie nicht die Blueprint-Konfigurationsscripts für die Konfiguration Ihres Zielreplikationsservers verwendet hatten, stimmt die Dateistruktur auf dem Zielreplikationsserver möglicherweise nicht mit den in der Datenbank gespeicherten Informationen überein. Entfernen Sie wahlweise die Speicherpoolverzeichnisse, die auf dem Zielreplikationsserver nicht vorhanden sind, indem Sie den Befehl DELETE STGPOOLDIRECTORY ausgeben.
4. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl QUERY DAMAGED ausgeben.
5. Wenn eine Beschädigung erkannt wird und deduplizierte Speicherbereiche nicht mithilfe des Replikationsservers repariert werden können, ist eine Reparatur dennoch möglich. In einigen Fällen sendet der Clientknoten Daten im Rahmen einer Sicherungsoperation erneut und die beschädigten Bereiche werden repariert. Warten Sie für die Dauer von zwei Sicherungszyklen, um die Ausführung von Clientsicherungsoperationen zu ermöglichen. Führen Sie im Anschluss an zwei Sicherungszyklen die folgenden Schritte aus:

a. Um zu prüfen, ob die Beschädigung repariert wurde, geben Sie den Befehl QUERY DAMAGED erneut aus.
b. Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus.
Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 zu prüfen und beschädigte Objekte zu entfernen, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=removedamaged
```

6. Wiederholen Sie diese Prozedur, um alle Ihre Speicherpools zu reparieren.

Zugehörige Verweise:
QUERY DAMAGED (Beschädigte Speicherpooldaten abfragen)

Speicherpools in einer Umgebung mithilfe eines Replikationsservers und mithilfe von Datenträgern in Containerkopienspeicherpools nach einem Katastrophenfall reparieren

Bei einem Katastrophenfall auf einem Quellenserver können Sie deduplizierte Datenbereiche in einem Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers oder mithilfe von ausgelagerten Banddatenträgern in Containerkopienspeicherpools reparieren. Der Verzeichniscontainerspeicherpool wird auf einem Zielserver am Wiederherstellungsstandort repariert.

Informationen zu diesem Vorgang

Verwenden Sie die folgende Prozedur, um die folgenden Typen schwerwiegender Beschädigungen zu reparieren:

- Vollständiger Verlust aller Containerspeicherpools auf dem Quellenserver
- Vollständiger Verlust des primären Standorts

Für dieses Wiederherstellungsszenario gelten die folgenden Voraussetzungen:

- Sie hatten den Befehl PROTECT STGPOOL verwendet, um Daten von einem Quellenreplikationsserver auf einen Zielreplikationsserver zu sichern. Der Zielreplikationsserver wird an Ihrem Wiederherstellungsstandort ausgeführt.
- Sie hatten den Befehl PROTECT STGPOOL verwendet, um Daten in Containerkopienspeicherpools an einem anderen Standort zu sichern.
- Sie hatten die IBM Spectrum Protect-Blueprints verwendet, um den IBM Spectrum Protect-Quellenserver zu konfigurieren; außerdem hatten Sie die Blueprint-Konfigurationsscripts verwendet, um die Umgebung zurückzuschreiben, indem am Wiederherstellungsstandort ein neuer Zielserver konfiguriert wurde. Mit den Scripts wurden Sicherungsversionen der IBM Spectrum Protect-Datenbank, der Serveroptionsdatei (dsmserv.opt), der Protokolldatei für Datenträger (volhist.out) und der Einheitenkonfigurationsdatei (devconfig.out) an ihre ursprünglichen Positionen auf dem Wiederherstellungsserver kopiert. Nach der Ausführung der Scripts werden die neu erstellten, leeren Verzeichnisse auf dem Wiederherstellungsserver angezeigt.

Wenn Sie versuchen, einen Verzeichniscontainerspeicherpool mithilfe eines Zielreplikationsservers zu reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Zielreplikationsserver ist nicht verfügbar.
- Der Zielspeicherpool ist beschädigt.
- Es tritt ein Netzausfall auf.

Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe von Containerkopienpools reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:

- Der Containerkopienspeicherpool ist nicht verfügbar.
- Der Containerkopienspeicherpool ist beschädigt.
- Die Datenträger in Containerkopienspeicherpools sind nicht verfügbar oder beschädigt.

Vorgehensweise

1. Markieren Sie alle Datenbereiche in dem Containerspeicherpool als beschädigt, indem Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=MARKDAMAGED für den Containerspeicherpool auf Speicherpoolebene ausgeben.
Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 zu prüfen und als beschädigt zu markieren, geben Sie den folgenden Befehl aus:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Wenn Sie den Verzeichniscontainerspeicherpool sowohl mit Containerkopienspeicherpools vor Ort als auch mit Containerkopienspeicherpools an einem anderen Standort geschützt hatten, geben Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters ACCESS=UNAVAILABLE für die Kopie des Containerkopienspeicherpools vor Ort aus.
3. Wenn sich die ausgelagerten Datenträger in Containerkopienspeicherpools wieder vor Ort befinden, stellen Sie diese in das Speicherarchiv zurück, indem Sie den Befehl CHECKIN LIBVOLUME unter Angabe des Parameters STATUS=PRIVATE ausgeben. Wenn die Banddatenträger jetzt vor Ort transportiert werden, sind Sie für die Reparatur beschädigter Bereiche mithilfe der Banddatenträger in

Containerkopienspeicherpools vorbereitet, falls die beschädigten Bereiche nicht mithilfe des Zielreplikationsservers repariert werden können.

4. Aktualisieren Sie den Status der Datenträger, indem Sie den Befehl UPDATE STGPOOL unter Angabe des Parameters ACCESS=READWRITE ausgeben.
5. Reparieren Sie den Speicherpool, indem Sie den Befehl REPAIR STGPOOL unter Angabe des Parameters SRCLOCATION=REPLSERVER ausgeben.
   Um beispielsweise einen Speicherpool mit dem Namen STGPOOL1 mithilfe eines Zielreplikationsservers zu reparieren, geben Sie den folgenden Befehl aus:

   ```
   repair stgpool stgpool1 srclocation=replserver
   ```

   Wenn Sie den Befehl REPAIR STGPOOL ausgeben, werden die beschädigten Bereiche unmittelbar nach der Reparatur von dem Datenträger gelöscht. Die beschädigten Bereiche werden nicht gemäß dem im Parameter REUSEDELAY angegebenen Wert beibehalten.
6. Wenn Sie nicht die Blueprint-Konfigurationsscripts für die Konfiguration Ihres Zielreplikationsservers verwendet hatten, stimmt die Dateistruktur auf dem Zielreplikationsserver möglicherweise nicht mit den in der Datenbank gespeicherten Informationen überein. Entfernen Sie wahlweise die Speicherpoolverzeichnisse, die auf dem Zielreplikationsserver nicht vorhanden sind. Geben Sie den Befehl DELETE STGPOOLDIRECTORY aus, um Verzeichnisse zu löschen, die auf dem Zielreplikationsserver nicht vorhanden sind.
7. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl QUERY DAMAGED ausgeben.
8. Wenn die beschädigten Bereiche nicht mithilfe des Zielreplikationsservers repariert werden können, können Sie die beschädigten Bereiche mithilfe von ausgelagerten Containerkopienspeicherpools reparieren. Anweisungen finden Sie in Speicherpools mithilfe von Datenträgern in Containerkopienspeicherpools nach einem Katastrophenfall reparieren.
9. Stellen Sie sicher, dass keine weiteren beschädigten Bereiche vorhanden sind, indem Sie den Befehl QUERY DAMAGED erneut ausgeben.
10. Wenn eine Beschädigung erkannt wird und deduplizierte Speicherbereiche nicht mithilfe des Replikationsservers repariert werden können, ist eine Reparatur dennoch möglich. In einigen Fällen sendet der Clientknoten Daten im Rahmen einer Sicherungsoperation erneut und die beschädigten Bereiche werden repariert. Warten Sie für die Dauer von zwei Sicherungszyklen, um die Ausführung von Clientsicherungen zu ermöglichen. Führen Sie im Anschluss an zwei Sicherungszyklen die folgenden Schritte aus:
    a. Um zu prüfen, ob die Beschädigung repariert wurde, geben Sie den Befehl QUERY DAMAGED erneut aus.
    b. Um Objekte zu entfernen, die sich auf beschädigte Daten beziehen, geben Sie den Befehl AUDIT CONTAINER unter Angabe des Parameters ACTION=REMOVEDAMAGED aus.
       Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 zu prüfen und beschädigte Objekte zu entfernen, geben Sie den folgenden Befehl aus:

       ```
       audit container stgpool=stgpool1 action=removedamaged
       ```
11. Wiederholen Sie diese Prozedur, um alle Ihre Speicherpools zu reparieren.

Beschädigten Banddatenträger im Containerkopienspeicherpool ersetzen

Wenn ein Banddatenträger, der eine Kopie deduplizierter Datenbereiche in einem Containerkopienspeicherpool speichert, beschädigt wird, können Sie den Datenträger ersetzen.

Vorgehensweise

1. Löschen Sie den beschädigten Banddatenträger, indem Sie den Befehl DELETE VOLUME unter Angabe des Parameters DISCARDDATA=YES ausgeben.
   Um beispielsweise einen Datenträger mit dem Namen VOLUME1 zu löschen, geben Sie den folgenden Befehl aus:

   ```
   delete volume volume1 discarddata=yes
   ```
2. Schützen Sie Datenbereiche im Verzeichniscontainerspeicherpool, indem Sie die Daten auf vorhandene Datenträger im Containerkopienspeicherpool kopieren. Geben Sie auf dem Quellenserver den Befehl PROTECT STGPOOL aus.
   Um beispielsweise einen Verzeichniscontainerspeicherpool mit dem Namen POOL1 zu schützen, geben Sie den folgenden Befehl aus:

   ```
   protect stgpool pool1 type=local
   ```

Zugehörige Verweise:
PROTECT STGPOOL (Speicherpooldaten schützen)
DELETE VOLUME (Speicherpooldatenträger löschen)

Serverbefehle, -optionen und -dienstprogramme

Verwenden Sie Befehle, um den Server zu verwalten und zu konfigurieren, Optionen, um den Server anzupassen, und Dienstprogramme, um spezielle Tasks auszuführen, wenn der Server nicht aktiv ist.

- Server von der Befehlszeile aus verwalten
  IBM Spectrum Protect stellt mehrere verschiedene Befehlszeilenschnittstellen für die Verwaltung von IBM Spectrum Protect-Servern zur Verfügung.
- Verwaltungsbefehle
  Verwaltungsbefehle sind zum Verwalten und Konfigurieren des Servers verfügbar.

- Serveroptionen
  Bei der Installation stellt IBM Spectrum Protect eine Serveroptionsdatei zur Verfügung, die eine Reihe von Standardoptionen zum Starten des Servers enthält.
- Serverdienstprogramme
  Verwenden Sie Serverdienstprogramme, um spezielle Tasks auf dem Server auszuführen, während der Server nicht aktiv ist.
- Rückkehrcodes für die Verwendung in IBM Spectrum Protect-Scripts
  Sie können IBM Spectrum Protect-Scripts schreiben, die Rückkehrcodes verwenden, um den Fortschritt der Scriptverarbeitung zu bestimmen. Die Rückkehrcodes können eine von drei Wertigkeiten haben: OK, WARNING, ERROR.
- Einheitendienstprogramme
  Für Tasks, die sich auf das Konfigurieren von Speichereinheiten für den IBM Spectrum Protect-Server beziehen, können Einheitendienstprogramme verwendet werden.
- Server-Scripts und Makros für die Automatisierung
  Allgemeine Verwaltungstasks können durch das Erstellen von IBM Spectrum Protect-Server-Scripts oder Makros des Verwaltungsclients automatisiert werden. Server-Scripts werden in der Serverdatenbank gespeichert; ihre Ausführung kann mithilfe eines Befehls für Verwaltungszeitpläne geplant werden. Makros des Verwaltungsclients werden als Dateien auf dem Verwaltungsclient gespeichert.

Server von der Befehlszeile aus verwalten

IBM Spectrum Protect stellt mehrere verschiedene Befehlszeilenschnittstellen für die Verwaltung von IBM Spectrum Protect-Servern zur Verfügung.

Informationen zu diesem Vorgang

Die folgenden Befehlszeilenschnittstellen sind verfügbar:

Verwaltungsbefehlszeilenclient
: Der Verwaltungsbefehlszeilenclient ist ein Programm, das auf einem Dateiserver, einer Workstation oder einem Großrechner ausgeführt werden kann. Er wird im Rahmen des IBM Spectrum Protect-Serverinstallationsprozesses installiert. Auf den Verwaltungsclient kann über Remotezugriff zugegriffen werden.

  Auf dem Verwaltungsclient können Sie alle Serverbefehle ausgeben.

Serverkonsole
: Die Serverkonsole ist ein Befehlszeilenfenster auf dem System, auf dem der Server installiert ist. Daher müssen Sie sich am physischen Standort des Serversystems befinden, um die Serverkonsole zu verwenden.

  Im Vergleich zum Verwaltungsclient ist die Funktionalität der Serverkonsole begrenzt. Sie können bestimmte Befehle nicht an der Serverkonsole ausgeben und Sie können Befehle nicht an andere Server weiterleiten. Außerdem können Sie nicht angeben, dass bestimmte Befehle verarbeitet werden, bevor andere Befehle ausgegeben werden können. Diese Einschränkung kann jedoch nützlich sein, wenn Sie beispielsweise zwei Befehle in schneller Aufeinanderfolge ausführen möchten.

Operations Center-Befehlszeile
: Sie können über das Operations Center auf die IBM Spectrum Protect-Befehlszeile zugreifen. Möglicherweise möchten Sie diese Befehlszeile verwenden, um Serverbefehle für die Ausführung bestimmter IBM Spectrum Protect-Tasks auszugeben, die im Operations Center nicht unterstützt werden.

Mit Server-Scripts können allgemeine Verwaltungstasks automatisiert werden. Ein Makro ist eine Datei, die IBM Spectrum Protect-Verwaltungsbefehle enthält. Wenn Sie den Befehl MACRO ausgeben, verarbeitet der Server alle Befehle in der Makrodatei in Folge, einschließlich der Befehle, die in allen verschachtelten Makros enthalten sind.

- Befehle mit dem Verwaltungsclient ausgeben
  Der Verwaltungsbefehlszeilenclient ist ein Programm, das auf einem Dateiserver, einer Workstation oder einem Großrechner ausgeführt werden kann.
- Befehle im Operations Center ausgeben
  In der Operations Center-Befehlszeilenschnittstelle können Sie Befehle ausgeben, um IBM Spectrum Protect-Server zu verwalten, die als Hub-Server oder Peripherieserver konfiguriert sind.
- Befehle von der Serverkonsole ausgeben
  IBM Spectrum Protect stellt eine Benutzer-ID mit dem Namen SERVER_CONSOLE zur Verfügung, mit der Sie Befehle ausgeben und den Server von der Serverkonsole aus verwalten können, nachdem IBM Spectrum Protect installiert wurde. Bei der Installation wird SERVER_CONSOLE automatisch als Administrator registriert und erhält die Systemberechtigung.
- Verwaltungsbefehle eingeben
  Befehle bestehen aus Befehlsnamen und normalerweise aus Parametern und Variablen. Syntaxdiagramme zeigen die Regeln, die bei der Eingabe von Befehlen zu befolgen sind.
- Befehlsverarbeitung steuern
  Einige IBM Spectrum Protect-Befehle können nacheinander oder gleichzeitig mit anderen Befehlen ausgeführt werden. Sie können auch Befehle von einem Server an andere Server für die Verarbeitung weiterleiten.
- Tasks gleichzeitig auf mehreren Servern ausführen
  Mit der Befehlsweiterleitung können Sie Befehle an einen oder an mehrere Server zur Verarbeitung weiterleiten und dann die Ausgabe von diesen Servern sammeln.

- Berechtigungsklassen für Befehle
  Die einem Administrator über die Berechtigungsklasse erteilte Berechtigung bestimmt, welche Verwaltungsbefehle der Administrator ausgeben kann.

Zugehörige Konzepte:
Server-Scripts
Zugehörige Verweise:
Makros des Verwaltungsclients

Befehle mit dem Verwaltungsclient ausgeben

Der Verwaltungsbefehlszeilenclient ist ein Programm, das auf einem Dateiserver, einer Workstation oder einem Großrechner ausgeführt werden kann.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass Ihr Verwaltungsclient und Ihr Server in kompatiblen Sprachen ausgeführt werden. Weitere Informationen zu Optionen für Sprache und Locale befinden sich in LANGUAGE. Verwenden Ihr Client und Ihr Server unterschiedliche Sprachen, können die von IBM Spectrum Protect generierten Nachrichten unverständlich sein.

Tipp: Textzeichenfolgen, die vom Client an den Server gesendet werden, sind nicht von der Einstellung der Serversprache abhängig. Der Text wird ordnungsgemäß angezeigt, wenn der Verwaltungsclient beim Senden der Zeichenfolge und beim Empfangen der Zeichenfolge in derselben Locale ausgeführt wird.

Beispiel: Angenommen, Sie aktualisieren ein Knotenkontaktfeld mit einem Wert, der nationale Sonderzeichen enthält (`update node myNode contact=NLcontact_info`), und fragen später den Knoten ab (`query node myNode format=detailed`). Wenn der Client bei der Aktualisierung und bei der Abfrage in derselben Locale ausgeführt wird, wird *NLcontact_info* korrekt angezeigt. Wird der Client in einer Locale ausgeführt, wenn Sie das Knotenkontaktfeld aktualisieren, und wird der Client in einer anderen Locale ausgeführt, wenn der Knoten abgefragt wird, wird *NLcontact_info* möglicherweise nicht korrekt angezeigt.

- Verwaltungsclient starten und stoppen
  Verwenden Sie den Befehl DSMADMC, um eine Verwaltungsclientsitzung zu starten.
- Serveraktivitäten über den Verwaltungsclient überwachen
  Um IBM Spectrum Protect-Aktivitäten, wie beispielsweise die Serverumlagerung und Clientanmeldungen, zu überwachen, führen Sie den Verwaltungsclient im Konsolenmodus aus. Im Konsolenmodus können keine Verwaltungsbefehle eingegeben werden.
- Mounts für austauschbare Datenträger über den Verwaltungsclient überwachen
  Um die Bereitstellung und das Aufheben der Bereitstellung austauschbarer Datenträger zu überwachen, führen Sie den Verwaltungsclient im Mountmodus aus. Wenn der Client im Mountmodus ausgeführt wird, können keine Verwaltungsbefehle eingegeben werden.
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten
  Den Stapelbetrieb verwenden, um einen einzelnen Verwaltungsbefehl einzugeben. Die Verwaltungsclientsitzung wird automatisch beendet, wenn der Befehl verarbeitet wurde.
- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
  Sie können den interaktiven Modus verwenden, um eine Serie von Verwaltungsbefehlen zu verarbeiten.
- Ausgabe von Befehlen formatieren
  IBM Spectrum Protect formatiert die Befehlsverarbeitungsausgabe entsprechend der Anzeigen- oder Fensterbreite.
- Befehlsausgabe an einer angegebenen Position sichern
  Die häufigste Verwendung der Ausgabeumleitung ist das Sichern der Ausgabe von Abfragebefehlen in einer angegebenen Datei oder in einem Programm. Sie können dann den Inhalt der Datei durchsuchen oder in manchen Fällen den Inhalt drucken.
- Verwaltungsclientoptionen
  In allen Verwaltungsclientmodi können Sie Optionen verwenden, um die Antworten der Verwaltungsclientsitzungen zu ändern.

Verwaltungsclient starten und stoppen

Verwenden Sie den Befehl DSMADMC, um eine Verwaltungsclientsitzung zu starten.

Informationen zu diesem Vorgang

Der IBM Spectrum Protect-Server muss aktiv sein, bevor ein Verwaltungsclient eine Verbindung herstellen kann.

Vorgehensweise

- Um eine Verwaltungsclientsitzung im Befehlszeilenmodus zu starten, geben Sie diesen Befehl an Ihrer Workstation ein:

  ```
  dsmadmc -id=admin -password=admin -dataonly=yes
  ```

  Wenn der Befehl DSMADMC mit den Optionen -ID und -PASSWORD (siehe oben) eingegeben wird, werden Sie nicht zur Eingabe einer Benutzer-ID und eines Kennworts aufgefordert.

- Um eine Verwaltungsclientsitzung im Befehlszeilenmodus zu stoppen, geben Sie den folgenden Befehl ein:

```
quit
```

- Um einen Befehl DSMADMC zu unterbrechen, bevor seine Verarbeitung durch den IBM Spectrum Protect-Server beendet wird, verwenden Sie den UNIX-Befehl `kill -9` in einer verfügbaren Befehlszeile. Drücken Sie nicht `Strg+C`, da dies während der Beendigung der Sitzung zu nicht erwarteten Ergebnissen führen kann.

Serveraktivitäten über den Verwaltungsclient überwachen

Um IBM Spectrum Protect-Aktivitäten, wie beispielsweise die Serverumlagerung und Clientanmeldungen, zu überwachen, führen Sie den Verwaltungsclient im Konsolenmodus aus. Im Konsolenmodus können keine Verwaltungsbefehle eingegeben werden.

Vorgehensweise

- Um eine Verwaltungsclientsitzung im Konsolenmodus zu starten, geben Sie den folgenden Befehl ein:

  ```
  dsmadmc -consolemode
  ```

  Wenn die Authentifizierung für den Server aktiviert ist, muss ein Kennwort eingegeben werden. Soll keine Eingabeaufforderung für Benutzer-ID und Kennwort erfolgen, geben Sie den Befehl DSMADMC mit den Optionen -ID und -PASSWORD ein.

- Um eine Verwaltungsclientsitzung im Konsolenmodus zu beenden, verwenden Sie eine Tastaturunterbrechungsfolge.

Betriebssystem	Unterbrechungsfolge
UNIX- und Linux-Clients	Strg+C
Windows-Clients	Strg+C oder Strg+Unterbrechungstaste

Mounts für austauschbare Datenträger über den Verwaltungsclient überwachen

Um die Bereitstellung und das Aufheben der Bereitstellung austauschbarer Datenträger zu überwachen, führen Sie den Verwaltungsclient im Mountmodus aus. Wenn der Client im Mountmodus ausgeführt wird, können keine Verwaltungsbefehle eingegeben werden.

Vorgehensweise

- Um eine Verwaltungsclientsitzung im Mountmodus zu starten, geben Sie den folgenden Befehl ein:

  ```
  dsmadmc -mountmode
  ```

  Wenn die Authentifizierung für den Server aktiviert ist, muss ein Kennwort eingegeben werden. Soll keine Eingabeaufforderung für Benutzer-ID und Kennwort erfolgen, geben Sie den Befehl DSMADMC mit den Optionen -ID und -PASSWORD ein.

- Um eine Verwaltungsclientsitzung im Mountmodus zu beenden, verwenden Sie eine Tastaturunterbrechungsfolge.

Betriebssystem	Unterbrechungsfolge
UNIX- und Linux-Clients	Strg+C
Windows-Clients	Strg+C oder Strg+Unterbrechungstaste

Einzelne Befehle mit dem Verwaltungsclient verarbeiten

Den Stapelbetrieb verwenden, um einen einzelnen Verwaltungsbefehl einzugeben. Die Verwaltungsclientsitzung wird automatisch beendet, wenn der Befehl verarbeitet wurde.

Vorgehensweise

Um eine Verwaltungsclientsitzung im Stapelmodus zu starten, verwenden Sie den folgenden Befehl: `dsmadmc *Serverbefehl*`

Soll keine Eingabeaufforderung für Benutzer-ID und Kennwort erfolgen, können Sie den Befehl DSMADMC mit den Optionen -ID und -PASSWORD eingeben.

Im Stapelbetrieb muss der vollständige Befehl in einer Zeile eingegeben werden. Passt ein Befehl nicht in eine Zeile, ist er mit Hilfe eines Makros oder einer Prozedur einzugeben. Wird im Stapelbetrieb ein Parameter mit einer Zeichenfolge angegeben, muss die Zeichenfolge in einfache Anführungszeichen (' ') in dem Makro eingeschlossen werden. Verwenden Sie keine Anführungszeichen für Befehle im Stapelbetrieb, da Ihr Betriebssystem die Anführungszeichen möglicherweise nicht korrekt syntaktisch analysiert.

 Windows-BetriebssystemeSie können diese Einschränkung bezüglich der Anführungszeichen im Stapelbetrieb für Windows-Clients umgehen, indem Sie das Backslash-(\)-Escapezeichen verwenden. Für den Parameter OBJECTS des Befehls DEFINE CLIENTACTION könnten Sie beispielsweise die Zeichenfolge mit dem Zeichen \ vor den Anführungszeichen in dem Befehl eingeben.

```
dsmadmc -id=admin -password=admin define clientaction test_node domain=test_dom
action=restore objects='\"C:\program files\test\*\"'
```

Eine Serie von Befehlen des Verwaltungsclients verarbeiten

Sie können den interaktiven Modus verwenden, um eine Serie von Verwaltungsbefehlen zu verarbeiten.

Informationen zu diesem Vorgang

Um eine Verwaltungsclientsitzung im interaktiven Modus zu starten, muss eine Serversitzung verfügbar sein. Um die Verfügbarkeit von Serversitzungen für Verwaltungssitzungen und Clientknotensitzungen sicherzustellen, wird der interaktive Modus des Verwaltungsclients unterbrochen, wenn eine (oder mehrere) der folgenden Bedingungen zutrifft:

- Der Server wurde mit dem Befehl HALT gestoppt.
- Während der mit der Serveroption IDLETIMEOUT angegebenen Zeitspanne wurden keine Befehle von der Verwaltungsclientsitzung ausgegeben.
- Die Verwaltungsclientsitzung wurde mit dem Befehl CANCEL SESSION abgebrochen.

Vorgehensweise

Um eine Verwaltungssitzung im interaktiven Modus zu starten, verwenden Sie den folgenden Befehl: `dsmadmc`

Bei der Verwendung des interaktiven Modus können Fortsetzungszeichen verwendet werden. Weitere Informationen befinden sich in Fortsetzungszeichen für die Eingabe langer Befehle verwenden.

Die Verwaltungsclientsitzung kann automatisch erneut gestartet werden, indem jedesmal ein anderer Befehl eingegeben wird, wenn die Bedienerführung `tsm: Servername >` angezeigt wird.

Geben Sie einen Serverbefehl nicht mit dem Befehl DSMADMC ein. Der Verwaltungsclient würde dann im Stapelbetrieb und nicht im interaktiven Modus gestartet. Geben Sie zum Beispiel Folgendes nicht ein:

```
dsmadmc Serverbefehl
```

Ausgabe von Befehlen formatieren

IBM Spectrum Protect formatiert die Befehlsverarbeitungsausgabe entsprechend der Anzeigen- oder Fensterbreite.

Vorgehensweise

- Reicht die Anzeigen- oder Fensterbreite für eine horizontale Anzeige der Ausgabe nicht aus, zeigt IBM Spectrum Protect die Informationen vertikal angeordnet an.
- Sie können die Ausgabe von QUERY-Befehlen mit den Verwaltungsclientoptionen DISPLAYMODE und OUTFILE formatieren.

Befehlsausgabe an einer angegebenen Position sichern

Die häufigste Verwendung der Ausgabeumleitung ist das Sichern der Ausgabe von Abfragebefehlen in einer angegebenen Datei oder in einem Programm. Sie können dann den Inhalt der Datei durchsuchen oder in manchen Fällen den Inhalt drucken.

Informationen zu diesem Vorgang

Auf einigen Betriebssystemen können Sie die Ausgabe eines Befehls mithilfe von Sonderzeichen wie z. B. >, >> und | umleiten. Umleitungszeichen leiten die Ausgabe eines Befehls in eine angegebene Datei oder an ein angegebenes Programm und nicht an den Bildschirm. Die Ausgabe eines Befehls kann durch Eingabe von Umleitungszeichen am Ende des Befehls gesichert werden. Um die Ausgabe umzuleiten, lassen Sie ein Leerzeichen zwischen dem Umleitungszeichen und dem Datei- oder Programmnamen. Siehe die nachfolgenden Beispiele.

Bei der Umleitung der Ausgabe sind die Namenskonventionen des Betriebssystems zu beachten, auf dem der Verwaltungsclient ausgeführt wird.

Vorgehensweise

Die Beispiele in der folgenden Tabelle zeigen, wie die Befehlsausgabe umgeleitet wird.

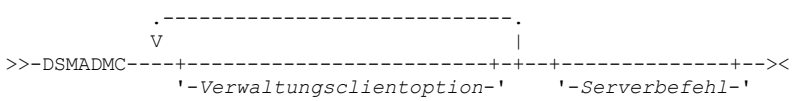
Task	Prozedur
Die Ausgabe eines Befehls QUERY DOMAIN im Stapelbetrieb oder im interaktiven Modus in eine neue Datei umleiten.	Verwenden Sie ein einzelnes Größer-als-Zeichen (>), um die Ausgabe in eine neue Datei umzuleiten oder eine vorhandene Datei zu überschreiben: `dsmadmc -id=xxx -pa=xxx query domain acctg > dominfo.acc`
Die Ausgabe eines Befehls QUERY DOMAIN im Stapelbetrieb oder im interaktiven Modus an das Ende einer vorhandenen Datei anhängen.	Verwenden Sie zwei aufeinanderfolgende Größer-als-Zeichen (>>), um die Ausgabe an das Ende einer vorhandenen Datei anzuhängen: `dsmadmc -id=xxx -pa=xxx query domain acctg >> dominfo.acc`

Task	Prozedur
Die gesamte Ausgabe von einer Verwaltungsclientsitzung im Konsolenmodus an ein Programm mit dem Namen filter.exe umleiten.	Verwenden Sie den vertikalen Balken (|), um die gesamte Ausgabe für eine Sitzung an ein Programm umzuleiten: `dsmadmc -console -id=admin -password=xxx | filter.exe` Das Programm kann so konfiguriert werden, dass es die Ausgabe auf einzelne Nachrichten überprüft und die entsprechende Aktion ausführt, wie beispielsweise das Senden von Post an einen anderen Benutzer.
Die gesamte Ausgabe im Konsolenmodus an eine Datei umleiten	Geben Sie die Option -OUTFILE mit einem Zieldateinamen an. Mit dem folgenden Befehl wird beispielsweise die gesamte Ausgabe an die Datei save.out umgeleitet: `dsmadmc -id=sullivan -password=secret -consolemode -outfile=save.out`

Verwaltungsclientoptionen

In allen Verwaltungsclientmodi können Sie Optionen verwenden, um die Antworten der Verwaltungsclientsitzungen zu ändern.

Syntax



Beispiel für die Verwendung von Verwaltungsclientoptionen

Sie können den Befehl DSMADMC mit Ihrer Benutzer-ID und Ihrem Kennwort eingeben, indem Sie die Optionen -ID und -PASSWORD verwenden, sodass Sie nicht zur Eingabe dieser Informationen aufgefordert werden. Soll IBM Spectrum Protect die gesamte Ausgabe in eine Datei umleiten, die Option -OUTFILE mit einem Zieldateinamen angeben. Soll beispielsweise der Befehl QUERY NODE im Stapelbetrieb ausgegeben werden und soll die Ausgabe in die Datei SAVE.OUT umgeleitet werden, Folgendes eingeben:

```
dsmadmc -id=sullivan -password=secret -outfile=save.out query node
```

Optionen

Verwaltungsclientoptionen können mit dem Befehl DSMADMC angegeben werden und sind nur in einer Verwaltungsclientsitzung gültig. Die Option kann in Großbuchstaben, Kleinbuchstaben oder in einer beliebigen Kombination aus beidem eingegeben werden. Großbuchstaben kennzeichnen die kürzeste zulässige Abkürzung. Steht eine Option nur in Großbuchstaben, kann sie nicht abgekürzt werden.

-ALWAYSPrompt
: Gibt an, dass eine Eingabeaufforderung angezeigt wird, wenn die Eingabe über die Tastatur erfolgt oder wenn sie umgeleitet wird (zum Beispiel aus einer Datei). Wird diese Option nicht angegeben und wird die Eingabe umgeleitet, wird die Eingabeaufforderung nicht geschrieben.

  Wird die Eingabe umgeleitet, wird nur die Befehlsausgabe angezeigt. Wird diese Option angegeben, werden die Eingabeaufforderung und die Befehlsausgabe angezeigt.

-CHECKAliashalt
: Ermöglicht es dem Verwaltungsclient, einen Aliasnamen für den Befehl HALT zu erkennen, der in der Serveroption ALIASHALT definiert ist. Für ausführliche Informationen siehe ALIASHALT.

-COMMAdelimited
: Gibt an, dass Ausgabe einer Serverabfrage in Tabellenform als Zeichenfolgen formatiert werden soll, die durch Kommas getrennt werden, und nicht im lesbaren Format. Diese Option soll hauptsächlich für die Umleitung der Ausgabe einer SQL-Abfrage (Befehl SELECT) verwendet werden. Das Format mit Kommatrennzeichen ist ein Standarddatenformat, das von vielen produktübergreifenden Programmen verarbeitet werden kann, einschließlich Tabellenkalkulationen, Datenbanken und Berichtsgeneratoren.

-CONsolemode
: Gibt an, dass IBM Spectrum Protect im Konsolenmodus ausgeführt wird. Der größte Teil der Ausgabe der Serverkonsole wird am Bildschirm angezeigt. Die Ausnahme sind Elemente, wie beispielsweise Antworten auf Abfragebefehle, die an der Konsole ausgegeben werden, Traceausgabe oder alle Systemnachrichten, die an der Konsole angezeigt werden.

-DATAONLY=NO oder YES
: Gibt an, ob Informationen zur Produktversion und Ausgabespaltenüberschriften mit der Ausgabe angezeigt werden. Der Standardwert ist NO.

  NO
  : Gibt an, dass Informationen zur Produktversion und Ausgabespaltenüberschriften angezeigt werden.

  YES

Gibt an, dass Informationen zur Produktversion und Ausgabespaltenüberschriften nicht angezeigt werden.

-DISPLaymode=LISt oder TABle
Sie können die QUERY-Ausgabe im Tabellen- oder Listenformat erzwingen, unabhängig von der Spaltenbreite des Befehlszeilenfensters.

Wird die Option -DISPLAYMODE verwendet und soll die Ausgabe in eine Datei gestellt werden, geben Sie nicht die Option -OUTFILE an. Verwenden Sie die Umleitung, um in die Datei zu schreiben.

-ID=Benutzer-ID
Gibt die Benutzer-ID des Administrators an.

-Itemcommit
Gibt an, dass IBM Spectrum Protect Befehle in einer Prozedur oder in einem Makro festschreibt, sobald die einzelnen Befehle verarbeitet werden.

-MOUNTmode
Gibt an, dass IBM Spectrum Protect im Lademodus aktiv ist. Alle Serverladenachrichten für austauschbare Datenträger werden angezeigt.

-NEWLINEAFTERPrompt
Gibt an, dass ein Zeilenvorschubzeichen nach der Eingabeaufforderung geschrieben wird, und Befehle, die über die Tastatur eingegeben werden, unter der Bedienerführung angezeigt werden. Wird diese Option nicht angegeben, werden die über die Tastatur eingegebenen Befehle rechts neben der Eingabeaufforderung angezeigt.

-NOConfirm
Gibt an, dass IBM Spectrum Protect vor der Verarbeitung von Befehlen, die sich auf die Verfügbarkeit des Servers oder die vom Server verwalteten Daten auswirken, keine Bestätigung anfordern soll.

-OUTfile
Gibt an, dass die Ausgabe von einer Serverabfrage in einer Zeile angezeigt wird. Wenn die Ausgabe in einer Zeile die Spaltenbreite überschreitet, die vom Server definiert ist, wird die Ausgabe in mehreren Zeilen angezeigt. Diese Option ist nur im Stapelbetrieb verfügbar.

-OUTfile=Dateiname
Gibt an, dass die Ausgabe von einer Serverabfrage in eine angegebene Datei umgeleitet wird. Im Stapelbetrieb wird die Ausgabe in eine angegebene Datei umgeleitet und das Format der Ausgabe entspricht dem Format der Ausgabe auf dem Bildschirm.

In Sitzungen, die im interaktiven Modus, Konsolenmodus oder Mountmodus ausgeführt werden, wird die Ausgabe am Bildschirm angezeigt.

-PAssword=Kennwort
Gibt das Kennwort des Administrators an.

-Quiet
Gibt an, dass IBM Spectrum Protect keine Standardausgabenachrichten anzeigt. Bei Verwendung dieser Option werden bestimmte Fehlernachrichten weiterhin angezeigt.

AIX-BetriebssystemeLinux-Betriebssysteme-SErveraddress
AIX-BetriebssystemeLinux-BetriebssystemeGibt die Serverzeilengruppe in der Datei dsm.sys an. Der Client verwendet die Serverzeilengruppe, um den Server zu bestimmen, zu dem die Verbindung hergestellt wird. Die Option SERVERADDRESS wird nur von Verwaltungsclients unterstützt, die unter den Betriebssystemen UNIX, Linux und Macintosh ausgeführt werden.

-TABdelimited
Gibt an, dass Ausgabe einer Serverabfrage in Tabellenform als Zeichenfolgen formatiert werden soll, die durch Tabulatoren getrennt werden, und nicht im lesbaren Format. Diese Option soll hauptsächlich für die Umleitung der Ausgabe einer SQL-Abfrage (Befehl SELECT) verwendet werden. Das Format mit Tabulatortrennzeichen ist ein Standarddatenformat, das von vielen produktübergreifenden Programmen verarbeitet werden kann, einschließlich Tabellenkalkulationen, Datenbanken und Berichtsgeneratoren.

-TCPPort
Gibt eine TCP/IP-Anschlussadresse für einen IBM Spectrum Protect-Server an. Die Option TCPPORT wird nur von Verwaltungsclients unterstützt, die unter Windows-Betriebssystemen ausgeführt werden, und ist in der Befehlszeile des Windows-Verwaltungsclients gültig.

-TCPServeraddress
Gibt eine TCP/IP-Serveradresse für einen IBM Spectrum Protect-Server an. Die Option TCPSERVERADDRESS wird nur von Verwaltungsclients unterstützt, die unter Windows-Betriebssystemen ausgeführt werden, und ist in der Befehlszeile des Windows-Verwaltungsclients gültig.

Zusätzlich zu den hier aufgeführten Optionen können auch alle Optionen in der Clientoptionsdatei angegeben werden. Jede Option muss mit einem Silbentrennungsstrich beginnen und durch ein Leerzeichen begrenzt werden.

Befehle im Operations Center ausgeben

In der Operations Center-Befehlszeilenschnittstelle können Sie Befehle ausgeben, um IBM Spectrum Protect-Server zu verwalten, die als Hub-Server oder Peripherieserver konfiguriert sind.

Vorgehensweise

Um die Befehlszeilenschnittstelle zu öffnen, bewegen Sie den Mauszeiger über das Globussymbol in der Operations Center-Menüleiste und klicken Sie auf Command Builder.

Befehle von der Serverkonsole ausgeben

IBM Spectrum Protect stellt eine Benutzer-ID mit dem Namen SERVER_CONSOLE zur Verfügung, mit der Sie Befehle ausgeben und den Server von der Serverkonsole aus verwalten können, nachdem IBM Spectrum Protect installiert wurde. Bei der Installation wird SERVER_CONSOLE automatisch als Administrator registriert und erhält die Systemberechtigung.

Informationen zu diesem Vorgang

Wenn Sie über Systemberechtigung verfügen, können Sie neue Berechtigungen für die Benutzer-ID SERVER_CONSOLE entziehen oder erteilen. Sie können keine der folgenden Aktionen ausführen:

- Benutzer-ID SERVER_CONSOLE registrieren oder aktualisieren
- Benutzer-ID SERVER_CONSOLE sperren oder entsperren
- Benutzer-ID SERVER_CONSOLE umbenennen
- Benutzer-ID SERVER_CONSOLE löschen
- Befehle von der Benutzer-ID SERVER_CONSOLE weiterleiten

Nicht alle IBM Spectrum Protect-Befehle werden von der Serverkonsole unterstützt. Sie können den Parameter WAIT nicht von der Serverkonsole aus angeben.

Verwaltungsbefehle eingeben

Befehle bestehen aus Befehlsnamen und normalerweise aus Parametern und Variablen. Syntaxdiagramme zeigen die Regeln, die bei der Eingabe von Befehlen zu befolgen sind.

Informationen zu diesem Vorgang

Um die Hilfe für Befehlszeile für Serverbefehle anzuzeigen, die eindeutige Namen haben, können Sie `help` *`Befehlsname`* eingeben, wobei *Befehlsname* der Name des Serverbefehls ist, für den Informationen angezeigt werden sollen. Soll beispielsweise Hilfe für den Befehl REGISTER NODE angezeigt werden, geben Sie `help` *`register node`* ein. Die Befehlssyntax und die Parameterbeschreibungen werden in der Ausgabe angezeigt.

Sie können auch `help`, gefolgt von der Nummer des Hilfethemas für den Befehl eingeben. Die Nummern der Hilfethemen sind im Inhaltsverzeichnis für die Befehlszeilenhilfe aufgelistet. Beispiel:

```
3.0 Verwaltungsbefehle
  3.46 REGISTER
     3.46.1 REGISTER ADMIN (Administrator registrieren)
     3.46.2 REGISTER LICENSE (Neue Lizenz registrieren)
     3.46.3 REGISTER NODE (Knoten registrieren)
```

Soll Hilfe für den Befehl REGISTER NODE angezeigt werden, geben Sie Folgendes ein:

```
help 3.46.3
```

Verwenden Sie die Nummern der Hilfethemen, um die Befehlszeilenhilfe für Unterbefehle anzuzeigen. DEFINE DEVCLASS ist ein Beispiel eines Befehls, der Unterbefehle hat. Sie können beispielsweise den Befehl DEFINE DEVCLASS für die Einheitenklasse 3590 und für die Einheitenklasse 3592 angeben:

```
3.0 Verwaltungsbefehle
  ...
  3.13.10 DEFINE DEVCLASS (Einheitenklasse definieren)
      3.13.10.1 DEFINE DEVCLASS (Einheitenklasse 3590 definieren)
      3.13.10.2 DEFINE DEVCLASS (Einheitenklasse 3592 definieren)
      ...
```

Soll Hilfe für den Befehl DEFINE DEVCLASS für die Einheitenklasse 3590 angezeigt werden, geben Sie Folgendes ein:

```
help 3.13.10.1
```

- Syntaxdiagramme lesen
  Zum Lesen eines Syntaxdiagramms für die Eingabe eines Befehls ist dem Pfad der Zeile zu folgen. Gelesen wird von links nach rechts und von oben nach unten.
- Fortsetzungszeichen für die Eingabe langer Befehle verwenden
  Fortsetzungszeichen sind nützlich, wenn ein Befehl verarbeitet werden soll, dessen Länge die Anzeigen- oder Fensterbreite überschreitet. Im interaktiven Modus des Verwaltungsclients können Fortsetzungszeichen verwendet werden.
- IBM Spectrum Protect-Objekte benennen
  IBM Spectrum Protect schränkt die Anzahl und die Art der Zeichen ein, die zum Benennen von Objekten verwendet werden können.
- Platzhalterzeichen zur Angabe von Objektnamen verwenden
  In einigen Befehlen (z. B. Abfragebefehle) kann mit Hilfe von Platzhalterzeichen eine Suchmusterzeichenfolge erstellt werden, die mehrere Objekte angibt. Platzhalterzeichen erleichtern die Anpassung eines Befehls an individuelle Anforderungen.
- Beschreibungen in Schlüsselwortparametern angeben
  Wenn eine Beschreibung (eine Zeichenfolge) eines Parameters mit einem einfachen oder doppelten Anführungszeichen beginnt oder eingebettete Leerzeichen oder Gleichheitszeichen enthält, muss der Wert in einfache (') oder doppelte Anführungszeichen (") eingeschlossen werden.

Syntaxdiagramme lesen

Zum Lesen eines Syntaxdiagramms für die Eingabe eines Befehls ist dem Pfad der Zeile zu folgen. Gelesen wird von links nach rechts und von oben nach unten.

- Das Symbol >>--- kennzeichnet den Anfang eines Syntaxdiagramms.
- Das Symbol ---> am Ende einer Zeile gibt an, dass das Syntaxdiagramm in der nächsten Zeile fortgesetzt wird.
- Das Symbol >--- am Anfang einer Zeile gibt an, dass ein in der vorherigen Zeile begonnenes Syntaxdiagramm fortgesetzt wird.
- Das Symbol --->< kennzeichnet das Ende eines Syntaxdiagramms.

Befehlsnamen

Der Befehlsname kann aus einem einzelnen Aktionswort bestehen, wie beispielsweise HALT, oder aus einem Aktionswort und einem Objekt für die Aktion, wie beispielsweise DEFINE DOMAIN. Sie können den Befehl in eine beliebige Spalte der Eingabezeile eingeben.

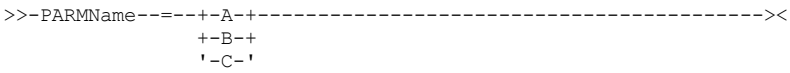
Geben Sie den vollständigen Befehlsnamen oder die in dem Syntaxdiagramm des Befehls angegebene Abkürzung ein. Großbuchstaben kennzeichnen die kürzeste zulässige Abkürzung. Steht ein Befehl nur in Großbuchstaben, kann er nicht abgekürzt werden. Der Befehl kann in Großbuchstaben, Kleinbuchstaben oder in einer beliebigen Kombination aus beidem eingegeben werden. In diesem Beispiel kann CMDNA, CMDNAM oder CMDNAME in einer beliebigen Kombination aus Groß- und Kleinbuchstaben eingegeben werden.

Anmerkung: Befehlsnamen im beschreibenden Text werden immer in Großbuchstaben angezeigt.

Erforderliche Parameter

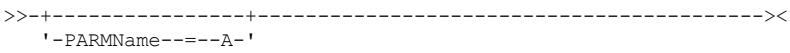
Befindet sich ein Parameter auf derselben Zeile wie der Befehlsname, ist der Parameter erforderlich. Werden zwei oder mehr Parameterwerte als Stapel angezeigt und befindet sich einer davon auf der Zeile, *muss* ein Wert angegeben werden.

In diesem Beispiel müssen Sie PARMNAME=A, PARMNAME=B oder PARMNAME=C eingeben. Direkt vor und hinter dem Gleichheitszeichen (=) dürfen sich keine Leerzeichen befinden.



Optionale Parameter

Steht ein Parameter unterhalb der Zeile, ist der Parameter optional. In diesem Beispiel können Sie PARMNAME=A eingeben oder keine Eingabe vornehmen. Direkt vor und hinter dem Gleichheitszeichen (=) dürfen sich keine Leerzeichen befinden.

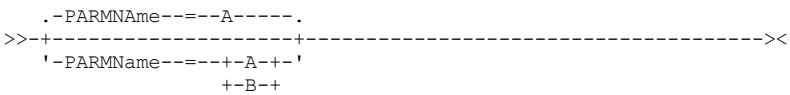


Werden zwei oder mehr Parameterwerte als Stapel unterhalb der Zeile angezeigt, sind alle Parameterwerte optional. In diesem Beispiel können Sie PARMNAME=A, PARMNAME=B oder PARMNAME=C eingeben oder keine Eingabe vornehmen. Direkt vor und hinter dem Gleichheitszeichen (=) dürfen sich keine Leerzeichen befinden.

Standardwerte

Standardwerte werden oberhalb der Zeile angezeigt. Das System verwendet die Standardwerte, sofern sie nicht vom Benutzer überschrieben werden. Der Standardwert kann durch Eingabe einer Option aus dem Stapel unterhalb der Zeile überschrieben werden.

In diesem Beispiel ist PARMNAME=A der Standardwert. Sie können auch PARMNAME=A, PARMNAME=B oder PARMNAME=C eingeben. Direkt vor oder direkt nach dem Gleichheitszeichen (=) dürfen keine Leerzeichen stehen.



```
                '-C-'
```

Variablen

Kursiv hervorgehobene Elemente (wie hier) kennzeichnen Variablen. In diesen Beispielen stellt Variablenname Variablen dar:

```
>>-CMDNAme--Variablenname---------------------------------------><


>>-+---------------------------+-------------------------------><
   '-PARMname--=--Variablenname-'
```

Sonderzeichen

Diese Symbole müssen exakt so eingegeben werden, wie sie im Syntaxdiagramm erscheinen.

*
: Stern

:
: Doppelpunkt

,
: Komma

=
: Gleichheitszeichen

-
: Silbentrennungsstrich

( )
: Runde Klammer

.
: Punkt

Werte wiederholen

Ein nach links zurücklaufender Pfeil bedeutet, daß das Element wiederholt eingegeben werden kann. Ein Zeichen innerhalb des Pfeils gibt an, dass die Elemente, die wiederholt werden, durch dieses Zeichen voneinander getrennt werden müssen.

```
   .-,---------.
   V           |
>>---Dateiname-+-------------------------------------------------><
```

Wiederholbare Auswahlangaben

Ein Stapel von Werten gefolgt von einem nach links zurücklaufenden Pfeil bedeutet, dass mehrere Werte ausgewählt werden können oder, wenn zulässig, ein einzelner Wert wiederholt werden kann. In diesem Beispiel kann mehr als ein Wert angegeben werden, wobei die einzelnen Namen durch Komma getrennt werden müssen. Direkt vor oder direkt nach dem Gleichheitszeichen (=) dürfen keine Leerzeichen stehen.

```
                .-,---------.
                V           |
>>-PARMNAme--=----+-Wert1-+-+---------------------------------><
                  +-Wert2-+
                  '-Wert3-'
```

Fußnoten

Fußnoten sind in runden Klammern eingeschlossen.

```
   .-,---------------.
   V  (1)            |
>>---------Dateiname-+-----------------------------------------><
```

Anmerkungen:

1. Sie können bis zu fünf Dateinamen angeben.

Parameter eingeben

Die Reihenfolge, in der Sie Parameter eingeben, kann wichtig sein. Das folgende Beispiel zeigt einen Teil des Befehls zum Definieren eines Kopienspeicherpools:

```
>>-DEFine STGpool--Poolname--Einheitenklassenname--------------->

>--POoltype--=--COpy--+-----------------------------+---------->
                      '-DESCription--=--Beschreibung-'

   .-RECLaim--=--100-----.
>--+---------------------+-------------------------------------><
   '-RECLaim--=--Prozent-'
```

Die ersten beiden Parameter in diesem Befehl (*Poolname* und *Einheitenklassenname* sind erforderliche Parameter. *Poolname* und *Einheitenklassenname* sind außerdem positionsgebunden. Das bedeutet, dass sie in der angezeigten Reihenfolge direkt nach dem Befehlsnamen eingegeben werden müssen. Der Parameter POOLTYPE ist ein erforderlicher Schlüsselwortparameter. DESCRIPTION und RECLAIM sind optionale Schlüsselwortparameter. Schlüsselwortparameter werden durch ein Gleichheitszeichen identifiziert, das einen bestimmten Wert oder eine Variable angibt. Schlüsselwortparameter müssen auf positionsgebundene Parameter in einem Befehl folgen.

Die folgenden Befehlseingaben, in denen die Schlüsselwortparameter unterschiedlich angeordnet sind, werden akzeptiert:

```
define stgpool mycopypool mydeviceclass pooltype=copy description=engineering
   reclaim=50
define stgpool mycopypool mydeviceclass description=engineering pooltype=copy
   reclaim=50
```

Das folgende Beispiel, in dem einer der positionsgebundenen Parameter auf einen Schlüsselwortparameter folgt, wird nicht akzeptiert:

```
define stgpool mycopypool pooltype=copy mydeviceclass description=engineering
   reclaim=50
```

Syntaxfragmente

Einige Diagramme müssen aufgrund ihrer Länge Teile der Syntax mit Fragmenten anzeigen. Der Fragmentname erscheint zwischen vertikalen Balken im Diagramm.

Das erweiterte Fragment erscheint im Diagramm nach allen anderen Parametern oder ganz unten im Diagramm. Das erweiterte Fragment wird durch eine Überschrift mit dem Fragmentnamen gekennzeichnet. Befehle, die direkt auf der Linie stehen, müssen eingegeben werden.

In diesem Beispiel hat das Fragment den Namen "Fragment".

```
>>-| Fragment |-------------------------------------------------><

Fragment

   .-A-.
|--+---+-------------------------------------------------------|
   +-B-+
   '-C-'
```

Fortsetzungszeichen für die Eingabe langer Befehle verwenden

Fortsetzungszeichen sind nützlich, wenn ein Befehl verarbeitet werden soll, dessen Länge die Anzeigen- oder Fensterbreite überschreitet. Im interaktiven Modus des Verwaltungsclients können Fortsetzungszeichen verwendet werden.

Informationen zu diesem Vorgang

Ohne Fortsetzungszeichen können maximal 256 Zeichen eingegeben werden. Mit Fortsetzungszeichen können maximal 1500 Zeichen eingegeben werden.

Anmerkung: Im Befehl MACRO gelten die Höchstwerte nach dem Anwenden von Substitutionsvariablen.
Mit Fortsetzungszeichen kann folgendes ausgeführt werden:

- Einen Bindestrich am Ende der fortzusetzenden Zeile eingeben.
  Beispiel:

  ```
  register admin pease mypasswd -
  contact="david, ext1234"
  ```

- Eine Werteliste wird fortgesetzt, indem ein Bindestrich oder ein umgekehrter Schrägstrich ohne vorangehende Leerstellen hinter dem letzten Komma der in der ersten Zeile eingegebenen Liste eingegeben wird. Dann werden die übrigen Elemente der Liste auf der nächsten Zeile ohne vorangehende Leerstellen eingegeben. Beispiel:

  ```
  stgpools=stg1,stg2,stg3,-
  stg4,stg5,stg6
  ```

- Um eine in Anführungszeichen eingeschlossene Wertefolge fortzusetzen, muss der erste Abschnitt der Folge zwischen Anführungszeichen eingegeben und mit einem Bindestrich oder einem umgekehrten Schrägstrich am Zeilenende abgeschlossen werden. Dann wird der Rest der Wertefolge zwischen derselben Art von Anführungszeichen auf der nächsten Zeile eingegeben.
  Beispiel:

  ```
  contact="david pease, bldg. 100, room 2b, san jose,"-
  "ext. 1234, alternate contact-norm pass,ext 2345"
  ```

  IBM Spectrum Protect verknüpft die beiden Zeichenfolgen ohne dazwischenliegende Leerzeichen. Es darf nur diese Methode zur Fortsetzung einer Zeichenfolge in Anführungszeichen über mehrere Zeilen verwendet werden.

IBM Spectrum Protect-Objekte benennen

IBM Spectrum Protect schränkt die Anzahl und die Art der Zeichen ein, die zum Benennen von Objekten verwendet werden können.

Informationen zu diesem Vorgang

Folgende Zeichen können für die Definition von Objektnamen verwendet werden.

Zeichen	Beschreibung
A–Z	Alle Buchstaben von A bis Z
0–9	Alle Zahlen von 0 bis 9
_	Unterstreichung
.	Punkt
-	Silbentrennungsstrich
+	Plus
&	Et-Zeichen

Die folgende Tabelle zeigt die maximal zulässige Länge von Zeichen für die Benennung von Objekten.

Art des Namens	Maximale Länge
Administratoren, Clientoptionsgruppen, Clientknoten, Kennwörter, Servergruppen, Server, Namen, Namen virtueller Dateibereiche	64
IDs wiederanlauffähiger Exporte	64
TCP/IP-Adressen (IPv4 oder IPv6) der höheren und unteren Ebene	64
Einheitenklassen, Laufwerke, Kassettenarchive, Verwaltungsklassen, Maßnahmendomänen, Profile, Zeitpläne, Scripts, Sicherungsgruppen, Speicherpools	30

Folgende Zeichen können für die Definition von Kennwörtern verwendet werden:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Kennwörter, die als "LOCAL" betrachtet werden, sind die Kennwörter, die mit dem IBM Spectrum Protect-Server authentifiziert werden. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden. Sobald ein Knoten oder Administrator für die Verwendung des Parameters SESSIONSECURITY=STRICT aktualisiert wird, muss beim Kennwort die Groß-/Kleinschreibung beachtet werden, wenn das Kennwort das nächste Mal geändert wird. Kennwörter, die als "LDAP" betrachtet werden, sind die Kennwörter, die mit einem LDAP-Verzeichnisserver authentifiziert werden. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung beachtet werden.

Wenn Sie Befehle DEFINE verwenden, um Datenbank-, Wiederherstellungsprotokoll- und Speicherpooldatenträger zu definieren, ist die Namenskonvention für den Datenträgernamen abhängig vom verwendeten Typ des Datenträgers mit sequenziellem Zugriff oder mit wahlfreiem Zugriff. Ausführliche Informationen befinden sich unter dem jeweiligen VOLUME-Befehl.

Platzhalterzeichen zur Angabe von Objektnamen verwenden

In einigen Befehlen (z. B. Abfragebefehle) kann mit Hilfe von Platzhalterzeichen eine Suchmusterzeichenfolge erstellt werden, die mehrere Objekte angibt. Platzhalterzeichen erleichtern die Anpassung eines Befehls an individuelle Anforderungen.

Informationen zu diesem Vorgang

Welche Platzhalterzeichen verwendet werden, ist abhängig von dem Betriebssystem, über das die Befehle ausgegeben werden. Mögliche Platzhalterzeichen sind beispielsweise ein Stern (*), der beliebigen (0 oder mehr) Zeichen entspricht, und ein Fragezeichen (?) oder ein Prozentzeichen (%), die exakt einem Zeichen entsprechen.

Tabelle 1 enthält Referenzen für Platzhalterzeichen einiger Betriebssysteme. Die für das verwendete System geeigneten Platzhalterzeichen sind zu verwenden.

Tabelle 1. Platzhalterzeichen nach Betriebssystem

Betriebssystem	Beliebige Entsprechung	Exakte Entsprechung
AIX, Linux, Windows	*	?
TSO	*	%

Sollen beispielsweise alle Verwaltungsklassen, deren Namen mit DEV beginnen, in allen Maßnahmengruppen in DOMAIN1 abgefragt werden und verwendet das System einen Stern als Zeichen für eine *beliebige Entsprechung*, kann folgendes eingegeben werden:

```
query mgmtclass domain1 * dev*
```

Verwendet das System ein Fragezeichen als Zeichen für eine *exakte Entsprechung* und sollen die Verwaltungsklassen in POLICYSET1 in DOMAIN1 abgefragt werden, kann Folgendes eingegeben werden:

```
query mgmtclass domain1 policyset1 mc?
```

IBM Spectrum Protect zeigt Informationen über Verwaltungsklassen mit den Namen MC an.

Tabelle 2 zeigt weitere Beispiele der Verwendung von Platzhalterzeichen für beliebige Entsprechungen.

Tabelle 2. Zeichen für beliebige Entsprechung

Muster	Entspricht	Entspricht nicht
ab*	ab, abb, abxxx	a, b, aa, bb
ab*rs	abrs, abtrs, abrsrs	ars, aabrs, abrss
ab*ef*rs	abefrs, abefghrs	abefr, abers

Tabelle 3 zeigt weitere Beispiele der Verwendung von Platzhalterzeichen für exakte Entsprechungen. Das Fragezeichen (?) kann durch ein Prozentzeichen (%) ersetzt werden, wenn die Plattform dieses Zeichen anstelle von ? verwendet.

Tabelle 3. Exakte Entsprechung

Muster	Entspricht	Entspricht nicht
ab?	abc	ab, abab, abzzzz
ab?rs	abfrs	abrs, abllrs
ab?ef?rs	abdefjrs	abefrs, abdefrs, abefjrs
ab??rs	abcdrs, abzzrs	abrs, abjrs, abkkkrs

Beschreibungen in Schlüsselwortparametern angeben

Wenn eine Beschreibung (eine Zeichenfolge) eines Parameters mit einem einfachen oder doppelten Anführungszeichen beginnt oder eingebettete Leerzeichen oder Gleichheitszeichen enthält, muss der Wert in einfache (') oder doppelte Anführungszeichen (") eingeschlossen werden.

Informationen zu diesem Vorgang

Das Anfangsanführungszeichen und das abschließende Anführungszeichen müssen von derselben Art sein. Wenn das Anfangsanführungszeichen ein einfaches Anführungszeichen ist, muß das abschließende Anführungszeichen auch ein einfaches Anführungszeichen sein.

Soll beispielsweise der neue Client-Knoten Louie mit dem Kennwort secret und seinem Titel als Kontaktinformationen registriert werden, folgendes eingeben:

```
register node louie secret contact="manager of dept. 61f"
```

Die folgende Tabelle zeigt die Eingabemöglichkeiten für eine Beschreibung für den Parameter CONTACT. Der Wert darf Anführungszeichen, eingebettete Leerzeichen und Gleichheitszeichen enthalten.

Für diese Beschreibung	Folgendes eingeben

Für diese Beschreibung	Folgendes eingeben
manager	contact=manager
manager's	contact="manager's" *oder* contact='manager"s'
"manager"	contact='"manager"' *oder* contact="""manager"""
manager's report	contact="manager's report" *oder* contact='manager''s report'
manager's "report"	contact='manager''s "report"'
manager=dept. 61f	contact='manager=dept. 61f'
manager reports to dept. 61f	contact='manager reports to dept. 61f' *oder* contact="manager reports to dept. 61f"

Befehlsverarbeitung steuern

Einige IBM Spectrum Protect-Befehle können nacheinander oder gleichzeitig mit anderen Befehlen ausgeführt werden. Sie können auch Befehle von einem Server an andere Server für die Verarbeitung weiterleiten.

Informationen zu diesem Vorgang

- Serverbefehlsverarbeitung
  IBM Spectrum Protect verarbeitet Verwaltungsbefehle im Vordergrund oder im Hintergrund. Im Vordergrund verarbeitete Befehle müssen beendet sein, bevor Sie einen weiteren Befehl ausgeben können. Werden Befehle im Hintergrund verarbeitet, können Sie jederzeit zusätzliche Befehle ausgeben.
- Hintergrundprozesse stoppen
  Mit dem Befehl CANCEL PROCESS können Befehle abgebrochen werden, die Hintergrundprozesse generieren.

Serverbefehlsverarbeitung

IBM Spectrum Protect verarbeitet Verwaltungsbefehle im Vordergrund oder im Hintergrund. Im Vordergrund verarbeitete Befehle müssen beendet sein, bevor Sie einen weiteren Befehl ausgeben können. Werden Befehle im Hintergrund verarbeitet, können Sie jederzeit zusätzliche Befehle ausgeben.

Die meisten IBM Spectrum Protect-Befehle werden im Vordergrund verarbeitet. Bei einigen Befehlen, die normalerweise im Hintergrund verarbeitet werden (z. B. BACKUP DB), können Sie den Parameter WAIT (WAIT=YES) mit dem Befehl angeben, so dass der Befehl im Vordergrund verarbeitet wird. Möglicherweise soll aus einem der folgenden Gründe ein Befehl im Vordergrund und nicht im Hintergrund verarbeitet werden:

- Um schnell zu bestimmen, ob ein Befehl erfolgreich ausgeführt wurde. Wenn Sie einen Befehl eingeben, der im Vordergrund verarbeitet wird, sendet IBM Spectrum Protect eine Bestätigungsnachricht, die die erfolgreiche Ausführung des Befehls anzeigt. Wird der Befehl im Hintergrund verarbeitet, müssen Sie das Feature 'Berichte zum Betrieb' (Operational Reporting) öffnen oder das Aktivitätenprotokoll abfragen, um zu bestimmen, ob der Befehl erfolgreich ausgeführt wurde.
- Zur Überwachung von Serveraktivitäten (z. B. Nachrichten) auf dem Verwaltungsclient während der Verarbeitung eines Befehls. Das ist unter Umständen dem Durchsuchen eines langen Aktivitätenprotokolls nach Beendigung des Befehls vorzuziehen.
- Damit ein anderer Prozess unmittelbar nach Beendigung des Befehls gestartet werden kann. Sie können beispielsweise WAIT=YES für einen Befehl angeben, dessen Verarbeitung nur kurze Zeit dauert, so dass Sie nach Beendigung der Verarbeitung sofort die Verarbeitung eines anderen Befehls starten können.
- Zum Serialisieren von Befehlen in einem Verwaltungsscript, wenn es darauf ankommt, dass ein Befehl beendet wird, bevor ein anderer beginnt.

Überprüfen Sie die jeweilige Befehlsbeschreibung, um zu bestimmen, ob ein Befehl über einen Parameter WAIT verfügt.

Sie können im Vordergrund verarbeitete Befehle über die Serverkonsole oder eine andere Verwaltungsclientsitzung abbrechen.

Jedem Hintergrundprozess wird eine Prozessnummer zugeordnet. Mit dem Befehl QUERY PROCESS können der Status und die Prozessnummer eines Hintergrundprozesses abgefragt werden.

Anmerkung:

- Wenn Sie einen Zeitplan mit einem Befehl definieren, in dem WAIT=NO (Standardwert) angegeben ist, und Sie QUERY EVENT ausgeben, um den Status Ihrer geplanten Operation festzustellen, haben fehlgeschlagene Operationen den Ereignisstatus COMPLETED mit dem Rückgabewert OK. Damit in der Ausgabe von QUERY EVENT der Fehlerstatus angezeigt wird, muss für den Parameter WAIT der Wert YES angegeben werden. Dadurch wird die geplante Operation im Vordergrund ausgeführt, und Sie werden nach ihrer Beendigung über den Status informiert.
- Von der Serverkonsole aus können Sie keine Befehle im Vordergrund verarbeiten.

Hintergrundprozesse stoppen

Mit dem Befehl CANCEL PROCESS können Befehle abgebrochen werden, die Hintergrundprozesse generieren.

Informationen zu diesem Vorgang

Mit dem Befehl QUERY PROCESS können der Status und die Prozessnummer eines Hintergrundprozesses abgefragt werden. Ist ein Hintergrundprozess bei seinem Abbruch aktiv, stoppt der Server den Prozess. Nicht festgeschriebene Änderungen werden rückgängig gemacht. Festgeschriebene Änderungen werden jedoch nicht rückgängig gemacht.

Wenn ein QUERY-Befehl über den Verwaltungsclient ausgegeben wird, können mehrere Ausgabeanzeigen generiert werden. In diesem Fall kann die Anzeige der Ausgabe an der Client-Workstation abgebrochen werden, wenn keine zusätzliche Ausgabe benötigt wird. Die Verarbeitung des Befehls wird dabei nicht beendet.

Tasks gleichzeitig auf mehreren Servern ausführen

Mit der Befehlsweiterleitung können Sie Befehle an einen oder an mehrere Server zur Verarbeitung weiterleiten und dann die Ausgabe von diesen Servern sammeln.

Informationen zu diesem Vorgang

Um Befehle an andere Server weiterzuleiten, müssen Sie auf jedem Server, an den der Befehl weitergeleitet wird, dieselbe Administrator-ID und dasselbe Kennwort sowie die erforderliche Administratorberechtigung haben. Sie können von der Serverkonsole aus keine Befehle an andere Server weiterleiten.

Nachdem die Verarbeitung des Befehls auf allen Servern beendet wurde, wird die vollständige Ausgabe für jeden Server angezeigt. Beispielsweise wird die Ausgabe von SERVER_A vollständig angezeigt, dann die Ausgabe von SERVER_B. Die Ausgabe beinhaltet Übersichtsnachrichten für jeden einzelnen Server und zeigt an, welcher Server die Ausgabe verarbeitet hat. Rückkehrcodes zeigen an, ob die Befehle erfolgreich auf den Servern verarbeitet wurden. Diese Rückkehrcodes zeigen drei Bewertungen an: 0, ERROR oder WARNING.

Jeder Server, der als Ziel eines weitergeleiteten Befehls angegeben wird, muss zuerst mit dem Befehl DEFINE SERVER definiert werden. Der Befehl wird automatisch an alle Server weitergeleitet, die als Teil einer Servergruppe angegeben sind, oder an einzelne Server, die mit dem Befehl angegeben werden.

Die folgenden Beispiele beschreiben das Weiterleiten des Befehls QUERY STGPOOL an einen Server, an mehrere Server, an eine Servergruppe, an mehrere Servergruppen oder an eine Kombination von Servern und Servergruppen. Die einzelnen Server oder Servergruppen in einer Liste müssen ohne Leerzeichen durch ein Komma voneinander getrennt werden.

Befehle an einen einzelnen Server weiterleiten

Vorgehensweise

Soll der Befehl QUERY STGPOOL an den Server ASTRO weitergeleitet werden, Folgendes eingeben:

```
astro: query stgpool
```

Der Doppelpunkt hinter dem Server-Namen zeigt das Ende der Leitweginformationen an. Dies wird auch als *Serverpräfix* bezeichnet. Eine andere Möglichkeit, das Ende der Leitweginformationen anzugeben, ist die Verwendung von runden Klammern, die den Server-Namen einschließen, zum Beispiel:

```
(astro) query stgpool
```

Befehle an mehrere Server weiterleiten

Informationen zu diesem Vorgang

Vorgehensweise

Soll der Befehl QUERY STGPOOL an die Server HD_QTR, MIDAS, SATURN weitergeleitet werden, Folgendes eingeben:

```
hd_qtr,midas,saturn: query stgpool
```

Wenn der erste Server nicht für IBM Spectrum Protect definiert wurde, wird der Befehl an den nächsten definierten Server in der Server-Liste weitergeleitet.

Sie können den Befehl auch wie folgt eingeben:

```
(hd_qtr,midas,saturn) query stgpool
```

Befehle an eine Servergruppe weiterleiten

Informationen zu diesem Vorgang

In diesem Beispiel sind in der Servergruppe ADMIN die Server SECURITY, PAYROLL, PERSONNEL als Gruppenteile definiert. Der Befehl wird an jeden dieser Server weitergeleitet.

Vorgehensweise

Soll der Befehl QUERY STGPOOL an die Servergruppe ADMIN weitergeleitet werden, Folgendes eingeben:

```
admin: query stgpool
```

Sie können den Befehl auch wie folgt eingeben:

```
(admin) query stgpool
```

Befehle an Servergruppen weiterleiten

Informationen zu diesem Vorgang

In diesem Beispiel sind in der Servergruppe ADMIN2 die Server SERVER_A, SERVER_B und SERVER_C und in der Servergruppe ADMIN3 die Server ASTRO, GUMBY und CRUSTY als Gruppenteile definiert. Der Befehl wird an die Server SERVER_A, SERVER_B, SERVER_C, ASTRO, GUMBY und CRUSTY weitergeleitet.

Vorgehensweise

Soll der Befehl QUERY STGPOOL an die beiden Servergruppen ADMIN2 und ADMIN3 weitergeleitet werden, Folgendes eingeben:

```
admin2,admin3: query stgpool
```

Sie können den Befehl auch wie folgt eingeben:

```
(admin2,admin3) query stgpool
```

Befehle an zwei Server und eine Servergruppe weiterleiten

Informationen zu diesem Vorgang

In diesem Beispiel sind in der Servergruppe DEV_GROUP die Server SALES, MARKETING und STAFF als Gruppenteile definiert. Der Befehl wird an die Server SALES, MARKETING, STAFF, MERCURY und JUPITER weitergeleitet.

Vorgehensweise

Soll der Befehl QUERY STGPOOL an die Servergruppe DEV_GROUP und an die Server MERCURY und JUPITER weitergeleitet werden, Folgendes eingeben:

```
dev_group,mercury,jupiter: query stgpool
```

Sie können den Befehl auch wie folgt eingeben:

```
(dev_group,mercury,jupiter) query stgpool
```

Befehle innerhalb von Prozeduren weiterleiten

Informationen zu diesem Vorgang

Werden Befehle innerhalb von Prozeduren weitergeleitet, muß der Server oder die Server-Gruppe in runde Klammern eingeschlossen und der Doppelpunkt übergangen werden. Andernfalls wird der Befehl bei Ausgabe des Befehls RUN nicht weitergeleitet und nur auf dem Server ausgeführt, auf dem der Befehl RUN ausgegeben wird.

Soll beispielsweise der Befehl QUERY STGPOOL innerhalb einer Prozedur weitergeleitet werden, wie folgt vorgehen:

Vorgehensweise

1. Die Prozedur QU_STG definieren, um sie an die Servergruppe DEV_GROUP weiterzuleiten.

   ```
   define script qu_stg "(dev_group) query stgpool"
   ```

2. Die Prozedur QU_STG ausführen:

   ```
   run qu_stg
   ```

Ergebnisse

In diesem Beispiel sind in der Servergruppe DEV_GROUP die Server SALES, MARKETING und STAFF als Gruppenteile definiert. Der Befehl QUERY STGPOOL wird an diese Server weitergeleitet.

Berechtigungsklassen für Befehle

Die einem Administrator über die Berechtigungsklasse erteilte Berechtigung bestimmt, welche Verwaltungsbefehle der Administrator ausgeben kann.

Es gibt vier Administratorberechtigungsklassen in IBM Spectrum Protect:

- Systemberechtigung
- Maßnahmenberechtigung
- Speicherberechtigung
- Bedienerberechtigung

Wenn ein Administrator mit Hilfe des Befehls REGISTER ADMIN registriert wurde, kann er eine beschränkte Befehlsgruppe, einschließlich aller Abfragebefehle, ausgeben. Wenn Sie IBM Spectrum Protect installieren, wird die Serverkonsole als Systemadministrator mit dem Namen SERVER_CONSOLE definiert und erhält die Systemberechtigung.

- Befehle, die die Systemberechtigung erfordern
  Ein Administrator mit Systemberechtigung verfügt über die höchste Berechtigungsstufe für den Server. Mit Systemberechtigung kann ein Administrator alle Verwaltungsbefehle ausgeben und hat die Berechtigung, alle Maßnahmendomänen und alle Speicherpools zu verwalten.
- Befehle, die die Maßnahmenberechtigung erfordern
  Ein Administrator mit Maßnahmenberechtigung kann Befehle für Maßnahmenverwaltungsobjekte ausgeben, wie z. B. Maßnahmendomänen, Maßnahmengruppen, Verwaltungsklassen, Kopiengruppen und Zeitpläne. Die Maßnahmenberechtigung kann uneingeschränkt sein oder kann auf bestimmte Maßnahmendomänen beschränkt werden.
- Befehle, die die Speicherberechtigung erfordern
  Ein Administrator mit Speicherberechtigung kann Befehle ausgeben, die Speicherressourcen für den Server zuordnen und steuern. Die Speicherberechtigung kann uneingeschränkt sein oder kann auf bestimmte Speicherpools beschränkt werden.
- Befehle, die die Bedienerberechtigung erfordern
  Ein Administrator mit Bedienerberechtigung kann Befehle ausgeben, die den direkten Betrieb des Servers und die Verfügbarkeit von Speicherdatenträgern steuern.
- Befehle, die jeder Administrator ausgeben kann
  Eine begrenzte Anzahl von Befehlen kann von jedem Administrator verwendet werden, auch wenn er über keine speziellen Administratorberechtigungen verfügt.

Befehle, die die Systemberechtigung erfordern

Ein Administrator mit Systemberechtigung verfügt über die höchste Berechtigungsstufe für den Server. Mit Systemberechtigung kann ein Administrator alle Verwaltungsbefehle ausgeben und hat die Berechtigung, alle Maßnahmendomänen und alle Speicherpools zu verwalten.

Tabelle 1 enthält die Befehle, die Administratoren mit Systemberechtigung ausgeben können. In einigen Fällen können Administratoren mit niedrigeren Berechtigungsstufen, beispielsweise mit uneingeschränkter Speicherberechtigung ebenfalls diese Befehle ausgeben. Außerdem kann mit der Serveroption REQSYSAUTHOUTFILE angegeben werden, dass bestimmte Befehle die Systemberechtigung erfordern, wenn sie bewirken, dass der Server in eine externe Datei schreibt. Weitere Informationen zu dieser Serveroption finden Sie in REQSYSAUTHOUTFILE.

Tabelle 1. Systemberechtigungsbefehle

Befehlsname	Befehlsname

Befehlsname	Befehlsname
• AUDIT LDAPDIRECTORY • AUDIT LICENSES • ACCEPT DATE • BEGIN EVENTLOGGING • CANCEL EXPIRATION • CANCEL PROCESS • CANCEL REPLICATION • CANCEL REQUEST • CANCEL RESTORE • CLEAN DRIVE • COPY ACTIVEDATA • COPY DOMAIN • COPY POLICYSET • COPY PROFILE • COPY SCHEDULE (Siehe Anmerkung.) • COPY SCRIPT • COPY SERVERGROUP • DEFINE BACKUPSET • DEFINE CLIENTACTION • DEFINE CLIENTOPT • DEFINE CLOPTSET • DEFINE COLLOCGROUP • DEFINE COLLOCMEMBER • DEFINE DEVCLASS • DEFINE DOMAIN • DEFINE DRIVE • DEFINE EVENTSERVER • DEFINE GRPMEMBER • DEFINE LIBRARY • DEFINE MACHINE • DEFINE MACHNODEASSOCIATION • DEFINE NODEGROUP • DEFINE NODEGROUPMEMBER • DEFINE PATH • DEFINE PROFASSOCIATION • DEFINE PROFILE • DEFINE RECMEDMACHASSOCIATION • DEFINE RECOVERYMEDIA • DEFINE SCHEDULE (Siehe Anmerkung.) • DEFINE SCRIPT • DEFINE SERVER • DEFINE SERVERGROUP	• DEFINE SPACETRIGGER • DEFINE STGPOOL • DEFINE SUBSCRIPTION • DEFINE VIRTUALFSMAPPING • DEFINE VOLUME • DELETE BACKUPSET • DELETE CLIENTOPT • DELETE CLOPTSET • DEFINE COLLOCGROUP • DEFINE COLLOCMEMBER • DELETE DOMAIN • DELETE DRIVE • DELETE EVENTSERVER • DELETE GRPMEMBER • DELETE LIBRARY • DELETE MACHINE • DELETE MACHNODEASSOCIATION • DELETE NODEGROUP • DELETE NODEGROUPMEMBER • DELETE PROFASSOCIATION • DELETE PROFILE • DELETE RECMEDMACHASSOCIATION • DELETE RECOVERYMEDIA • DELETE SCHEDULE (Siehe Anmerkung.) • DELETE SCRIPT • DELETE SERVER • DELETE SERVERGROUP • DELETE SPACETRIGGER • DELETE STGPOOL • DELETE SUBSCRIBER • DELETE SUBSCRIPTION • DELETE VIRTUALFSMAPPING • DISABLE EVENTS • ENABLE EVENTS • END EVENTLOGGING • EXPIRE INVENTORY • EXPORT ADMIN • EXPORT NODE • EXPORT POLICY • EXPORT SERVER • GENERATE BACKUPSET • GRANT AUTHORITY

Befehlsname	Befehlsname
• GRANT PROXYNODE • IDENTIFY DUPLICATES • IMPORT NODE • IMPORT POLICY • IMPORT SERVER • INSERT MACHINE • LABEL LIBVOLUME • LOCK ADMIN • LOCK PROFILE • MIGRATE STGPOOL • MOVE DRMEDIA • MOVE MEDIA • MOVE GRPMEMBER • NOTIFY SUBSCRIBERS • PERFORM LIBACTION • PING SERVER • PREPARE • QUERY BACKUPSETCONTENTS • QUERY MEDIA • QUERY RPFCONTENT • QUERY TOC • RECLAIM STGPOOL • RECONCILE VOLUMES • REGISTER ADMIN • REGISTER LICENSE • REMOVE ADMIN • REMOVE REPLNODE • RENAME ADMIN • RENAME SCRIPT • RENAME SERVERGROUP • RENAME STGPOOL • REPLICATE NODE • RESET PASSEXP • RESTORE NODE • REVOKE AUTHORITY • REVOKE PROXYNODE • RUN • SET ACCOUNTING • SET ACTLOGRETENTION • SET ARCHIVERETENTIONPROTECTION • SET ARREPLRULEDEFAULT • SET BKREPLRULEDEFAULT • SET CLIENTACTDURATION	• SET CONFIGMANAGER • SET CONFIGREFRESH • SET CONTEXTMESSAGING • SET CROSSDEFINE • SET DBRECOVERY • SET DEFAULTAUTHENTICATION • SET DRMACTIVEDATASTGPOOL • SET DRMCHECKLABEL • SET DRMCMDFILENAME • SET DRMCOPYCONTAINERSTGPOOL • SET DRMCOPYSTGPOOL • SET DRMCOURIERNAME • SET DRMDBBACKUPEXPIREDAYS • SET DRMFILEPROCESS • SET DRMINSTRPREFIX • SET DRMNOTMOUNTABLENAME • SET DRMPLANPREFIX • SET DRMPLANVPOSTFIX • SET DRMPRIMSTGPOOL • SET DRMRPFEXPIREDAYS • SET DRMVAULTNAME • SET EVENTRETENTION • SET INVALIDPWLIMIT • SET LDAPPASSWORD • SET LDAPUSER • SET LICENSEAUDITPERIOD • SET MAXCMDRETRIES • SET MAXSCHEDSESSIONS • SET MINPWLENGTH • SET PASSEXP • SET QUERYSCHEDPERIOD • SET RANDOMIZE • SET REPLRETENTION • SET REPLSERVER • SET RETRYPERIOD • SET SCHEDMODES • SET SERVERHLADDRESS • SET SERVERLLADDRESS • SET SERVERNAME • SET SERVERPASSWORD • SET SPREPLRULEDEFAULT • SET SUBFILE • SET TOCLOADRETENTION
• SETOPT • UNLOCK ADMIN • UNLOCK PROFILE • UPDATE ADMIN • UPDATE BACKUPSET • UPDATE CLIENTOPT • UPDATE CLOPTSET • UPDATE COLLOCGROUP • UPDATE DEVCLASS • UPDATE DRIVE • UPDATE LIBRARY • UPDATE LIBVOLUME • UPDATE MACHINE	• UPDATE NODEGROUP • UPDATE PATH • UPDATE PROFILE • UPDATE RECOVERYMEDIA • UPDATE REPLRULE • UPDATE SCHEDULE (Siehe Anmerkung.) • UPDATE SCRIPT • UPDATE SERVER • UPDATE SERVERGROUP • UPDATE SPACETRIGGER • UPDATE VIRTUALFSMAPPING • UPDATE VOLHISTORY • VALIDATE LANFREE • VALIDATE REPLICATION
Anmerkung: Dieser Befehl ist durch die Berechtigung eingeschränkt, die einem Administrator erteilt wird. Die Systemberechtigung ist nur für Verwaltungsbefehlszeitpläne erforderlich. Die System- oder Maßnahmenberechtigung ist für Clientoperationszeitpläne erforderlich.	

Befehle, die die Maßnahmenberechtigung erfordern

Ein Administrator mit Maßnahmenberechtigung kann Befehle für Maßnahmenverwaltungsobjekte ausgeben, wie z. B. Maßnahmendomänen, Maßnahmengruppen, Verwaltungsklassen, Kopiengruppen und Zeitpläne. Die Maßnahmenberechtigung kann uneingeschränkt sein oder kann auf bestimmte Maßnahmendomänen beschränkt werden.

Mit der uneingeschränkten Maßnahmenberechtigung können Sie alle Administratorbefehle ausgeben, für die die Maßnahmenberechtigung erforderlich ist. Es können Befehle ausgegeben werden, die alle vorhandenen Maßnahmendomänen sowie alle Maßnahmendomänen betreffen, die in Zukunft definiert werden. Ein Administrator mit uneingeschränkter Maßnahmenberechtigung kann keine Maßnahmendomänen definieren, löschen oder kopieren.

Mit der eingeschränkten Maßnahmenberechtigung können Sie Administratorbefehle ausgeben, die eine oder mehrere Maßnahmendomänen betreffen, für die die Berechtigung erteilt wird. Für den Befehl DELETE MGMTCLASS ist beispielsweise die Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Verwaltungsklasse gehört.

Tabelle 1 enthält die Befehle, die ein Administrator mit Maßnahmenberechtigung ausgeben kann.

Tabelle 1. Maßnahmenberechtigungsbefehle

Befehlsname	**Befehlsname**
• ACTIVATE POLICYSET • ASSIGN DEFMGMTCLASS • CLEAN DRIVE • BACKUP NODE • COPY MGMTCLASS • COPY POLICYSET • COPY SCHEDULE (Siehe Anmerkung 2.) • DEFINE ASSOCIATION • DEFINE BACKUPSET • DEFINE COPYGROUP • DEFINE CLIENTACTION • DEFINE CLIENTOPT • DEFINE MGMTCLASS • DEFINE NODEGROUP • DEFINE NODEGROUPMEMBER • DEFINE POLICYSET • DEFINE SCHEDULE • DELETE ASSOCIATION • DELETE BACKUPSET • DELETE COPYGROUP • DELETE EVENT (Siehe Anmerkung 1.) • DELETE FILESPACE • DELETE MGMTCLASS • DELETE NODEGROUP • DELETE NODEGROUPMEMBER	• DELETE POLICYSET • DELETE PATH • DELETE SCHEDULE (Siehe Anmerkung 2.) • GENERATE BACKUPSET • LOCK NODE • QUERY BACKUPSETCONTENTS • REGISTER NODE • REMOVE NODE • RENAME FILESPACE • RENAME NODE • SET SUMMARYRETENTION • RESTORE NODE • QUERY TOC • UNLOCK NODE • UPDATE BACKUPSET • UPDATE COPYGROUP • UPDATE DOMAIN • UPDATE MGMTCLASS • UPDATE NODE • UPDATE NODEGROUP • UPDATE POLICYSET • UPDATE SCHEDULE (Siehe Anmerkung 2.) • VALIDATE POLICYSET
Anmerkungen: 1. Dieser Befehl kann durch die Maßnahmendomäne eingeschränkt werden. Ein Administrator mit uneingeschränkter Maßnahmenberechtigung oder eingeschränkter Maßnahmenberechtigung für eine angegebene Maßnahmendomäne kann diesen Befehl ausgeben. 2. Dieser Befehl ist durch die Berechtigung eingeschränkt, die einem Administrator erteilt wird. Die Systemberechtigung ist nur für Verwaltungsbefehlszeitpläne erforderlich. Die System- oder Maßnahmenberechtigung ist für Clientoperationszeitpläne erforderlich.	

Befehle, die die Speicherberechtigung erfordern

Ein Administrator mit Speicherberechtigung kann Befehle ausgeben, die Speicherressourcen für den Server zuordnen und steuern. Die Speicherberechtigung kann uneingeschränkt sein oder kann auf bestimmte Speicherpools beschränkt werden.

Mit der uneingeschränkten Speicherberechtigung können alle Administratorbefehle ausgegeben werden, für die Speicherberechtigung erforderlich ist. Es können Befehle ausgegeben werden, die alle vorhandenen Speicherpools sowie alle Speicherpools betreffen, die in Zukunft definiert werden. Außerdem können Befehle ausgegeben werden, die die Datenbank und das Wiederherstellungsprotokoll betreffen. Ein Administrator mit uneingeschränkter Speicherberechtigung kann Speicherpools nicht definieren oder löschen.

Mit der eingeschränkten Speicherberechtigung können Administratorbefehle ausgegeben werden, die nur einen Speicherpool betreffen, für den eine Berechtigung erteilt wurde. Der Befehl DELETE VOLUME betrifft beispielsweise nur einen Datenträger aus dem Speicherpool, der für einen bestimmten Speicherpool definiert ist.

Tabelle 1 enthält die Befehle, die ein Administrator mit Speicherberechtigung ausgeben kann.

Tabelle 1. Speicherberechtigungsbefehle

Befehlsname	Befehlsname
• AUDIT LIBRARY • AUDIT VOLUME (Siehe Anmerkung.) • BACKUP DB • BACKUP DEVCONFIG • BACKUP STGPOOL • BACKUP VOLHISTORY • CHECKIN LIBVOLUME • CHECKOUT LIBVOLUME • COPY ACTIVEDATA (Siehe Anmerkung.) • DEFINE COLLOCGROUP • DEFINE COLLOCMEMBER • DEFINE DATAMOVER • DEFINE DEVCLASS • DEFINE DRIVE • DEFINE LIBRARY • DEFINE PATH • DEFINE VIRTUALFSMAPPING • DEFINE VOLUME (Siehe Anmerkung.) • DEFINE SPACETRIGGER • DELETE COLLOCGROUP • DELETE COLLOCMEMBER • DELETE DATAMOVER • DELETE DEVCLASS • DELETE DRIVE • DELETE LIBRARY • DELETE PATH	• DELETE SPACETRIGGER • DELETE VIRTUALFSMAPPING • DELETE VOLHISTORY • DELETE VOLUME (Siehe Anmerkung.) • GRANT PROXYNODE • LABEL LIBVOLUME • MIGRATE STGPOOL • MOVE DATA (Siehe Anmerkung.) • MOVE MEDIA • QUERY TAPEALERTMSG • RECLAIM STGPOOL • RESTORE STGPOOL • RESTORE VOLUME • REVOKE PROXYNODE • SET TAPEALERTMSG • UPDATE COLLOCGROUP • UPDATE DATAMOVER • UPDATE DEVCLASS • UPDATE DRIVE • UPDATE LIBRARY • UPDATE PATH • UPDATE SPACETRIGGER • UPDATE STGPOOL (Siehe Anmerkung.) • UPDATE VIRTUALFSMAPPING
Anmerkung: Dieser Befehl kann durch den Speicherpool eingeschränkt werden. Ein Administrator mit uneingeschränkter Speicherberechtigung oder eingeschränkter Speicherberechtigung für einen angegebenen Speicherpool kann diesen Befehl ausgeben.	

Befehle, die die Bedienerberechtigung erfordern

Ein Administrator mit Bedienerberechtigung kann Befehle ausgeben, die den direkten Betrieb des Servers und die Verfügbarkeit von Speicherdatenträgern steuern.

Tabelle 1 enthält die Befehle, die ein Administrator mit Bedienerberechtigung ausgeben kann.

Tabelle 1. Bedienerberechtigungsbefehle

Befehlsname	Befehlsname
• CANCEL SESSION • DISABLE SESSIONS • DISMOUNT VOLUME • ENABLE SESSIONS • HALT	• MOVE DRMEDIA • MOVE MEDIA • QUERY MEDIA • REPLY • UPDATE VOLUME • VARY

Befehle, die jeder Administrator ausgeben kann

Eine begrenzte Anzahl von Befehlen kann von jedem Administrator verwendet werden, auch wenn er über keine speziellen Administratorberechtigungen verfügt.

Tabelle 1 enthält die Befehle, die jeder registrierte Administrator ausgeben kann.

Tabelle 1. Befehle, die von allen Administratoren ausgegeben werden

Befehlsname	Befehlsname

Befehlsname	Befehlsname
• COMMIT • HELP • ISSUE MESSAGE • MACRO • PARALLEL • QUERY ACTLOG • QUERY ADMIN • QUERY ASSOCIATION • QUERY AUDITOCCUPANCY • QUERY BACKUPSET • QUERY CLOPTSET • QUERY COLLOCGROUP • QUERY CONTENT • QUERY COPYGROUP • QUERY DATAMOVER • QUERY DB • QUERY DBSPACE • QUERY DEVCLASS • QUERY DIRSPACE • QUERY DOMAIN • QUERY DRIVE • QUERY DRMEDIA • QUERY DRMSTATUS • QUERY ENABLED • QUERY EVENT • QUERY EVENTRULES • QUERY EVENTSERVER • QUERY FILESPACE • QUERY LIBRARY • QUERY LIBVOLUME • QUERY LICENSE • QUERY LOG • QUERY MACHINE • QUERY MGMTCLASS • QUERY MOUNT • QUERY NASBACKUP	• QUERY NODE • QUERY NODEDATA • QUERY NODEGROUP • QUERY OCCUPANCY • QUERY OPTION • QUERY PATH • QUERY POLICYSET • QUERY PROCESS • QUERY PROFILE • QUERY PROXYNODE • QUERY RECOVERYMEDIA • QUERY REPLICATION • QUERY REPLNODE • QUERY REPLRULE • QUERY REQUEST • QUERY RESTORE • QUERY RPFILE • QUERY SCHEDULE • QUERY SCRIPT • QUERY SERVER • QUERY SERVERGROUP • QUERY SESSION • QUERY SPACETRIGGER • QUERY STATUS • QUERY STGPOOL • QUERY SUBSCRIBER • QUERY SUBSCRIPTION • QUERY SYSTEM • QUERY VIRTUALFSMAPPING • QUERY VOLHISTORY • QUERY VOLUME • QUIT • ROLLBACK • SELECT • SERIAL

Verwaltungsbefehle

Verwaltungsbefehle sind zum Verwalten und Konfigurieren des Servers verfügbar.

Die Informationen zu jedem Befehl beinhalten

- eine Beschreibung der Tasks, die ein Befehl ausführt.
- die für den Befehl erforderliche Administrator-Berechtigungsklasse.
- ein Syntaxdiagramm, das die erforderlichen und wahlfreien Parameter für den Befehl kennzeichnet.
- Beschreibungen jedes Befehlsparameters.
- Beispiele für die Verwendung eines Befehls.
- eine Liste der zugehörigen Befehle.

- ACCEPT DATE (Aktuelles Systemdatum akzeptieren)
  Mit diesem Befehl können Sie den Server mit der normalen Verarbeitung beginnen lassen, wenn der Server aufgrund einer Abweichung zwischen dem Serverdatum und dem aktuellen Systemdatum die normale Verarbeitung nicht startet.
- ACTIVATE POLICYSET (Neue Maßnahmengruppe aktivieren)
  Mit diesem Befehl kann der Inhalt einer Maßnahmengruppe in die AKTIVE Maßnahmengruppe für die Domäne kopiert werden. Der Server verwendet die Regeln in der AKTIVEN Maßnahmengruppe, um Clientoperationen in der Domäne zu verwalten. Für eine Maßnahmendomäne können mehrere Maßnahmengruppen definiert werden, aber es kann nur eine Maßnahmengruppe aktiv sein. Die aktuelle AKTIVE Maßnahmengruppe wird durch die Maßnahmengruppe ersetzt, die bei Ausgabe dieses Befehls angegeben wird. Die AKTIVE Maßnahmengruppe kann nur geändert werden, indem eine andere Maßnahmengruppe aktiviert wird.
- ASSIGN DEFMGMTCLASS (Standardverwaltungsklasse zuordnen)
  Mit diesem Befehl kann eine Verwaltungsklasse als Standardverwaltungsklasse für eine Maßnahmengruppe angegeben werden. Es muß eine Standardverwaltungsklasse für eine Maßnahmengruppe zugeordnet werden, damit diese Maßnahmengruppe aktiviert werden kann.
- AUDIT-Befehle
  Mit den AUDIT-Befehlen kann die Qualität der Datenbankinformationen und der Speicherpooldatenträger überprüft oder untersucht werden. Mit dem Befehl AUDIT LDAPDIRECTORY werden Knoten oder Administrator-IDs auf einem LDAP-Verzeichnisserver gelöscht, die ihre Kennwörter nicht mit dem LDAP-Verzeichnisserver authentifizieren.

- BACKUP-Befehle
  Mit den BACKUP-Befehlen können Sicherungskopien der IBM Spectrum Protect-Informationen oder -Objekte erstellt werden.
- BEGIN EVENTLOGGING (Ereignisprotokollierung beginnen)
  Mit diesem Befehl kann das Protokollieren von Ereignissen für einen oder mehrere Empfänger begonnen werden. Ein Empfänger, für den die Ereignisprotokollierung begonnen hat, ist ein *aktiver Empfänger*.
- CANCEL-Befehle
  Mit den CANCEL-Befehlen kann eine Task oder ein Prozess vor der Beendigung abgebrochen werden.
- CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)
  Mit diesem Befehl kann ein Speicherdatenträger mit sequenziellem Zugriff oder ein Reinigungsband dem Serverdatenträgerbestand für ein automatisiertes Speicherarchiv hinzugefügt werden. Der Server kann einen Datenträger, der sich physisch in einem automatisierten Speicherarchiv befindet, erst verwenden, wenn dieser Datenträger zurückgestellt wurde.
- CHECKOUT LIBVOLUME (Speicherdatenträger aus Kassettenarchiv entnehmen)
  Mit diesem Befehl kann ein Speicherdatenträger mit sequenziellem Zugriff aus dem Serverdatenträgerbestand für ein automatisiertes Kassettenarchiv entfernt werden. Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.
- CLEAN DRIVE (Laufwerk reinigen)
  Verwenden Sie diesen Befehl, wenn IBM Spectrum Protect unabhängig von der Reinigungshäufigkeit sofort eine Reinigungskassette in ein Laufwerk laden soll.
- COMMIT (Festschreiben von Befehlen in einem Makro steuern)
  Mit diesem Befehl kann das Festschreiben eines Befehls in einem Makro gesteuert und die Datenbank nach der Verarbeitung von Befehlen aktualisiert werden. Wird dieser Befehl im Konsolenmodus des Verwaltungsclients ausgegeben, wird keine Nachricht generiert.
- CONVERT STGPOOL (Speicherpool in einen Containerspeicherpool konvertieren)
  Mit diesem Befehl können Sie einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Verzeichniscontainerspeicherpool oder einen Cloud-Containerspeicherpool konvertieren. Sie können Containerspeicherpools sowohl für die Inline-Datendeduplizierung als auch für die clientseitige Datendeduplizierung verwenden.
- COPY-Befehle
  Mit den COPY-Befehlen kann eine Kopie von IBM Spectrum Protect-Objekten oder -Daten erstellt werden.
- DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)
  Mit diesem Befehl können Sie angeben, dass aktive Daten, die für einen Anwendungsclientknoten vor einem angegebenen Datum gesichert wurden, nicht mehr benötigt werden. Der Befehl markiert die Daten als inaktiv, sodass sie gemäß Ihren Datenaufbewahrungsmaßnahmen gelöscht werden können.
- DECOMMISSION-Befehle
  Verwenden Sie die DECOMMISSION-Befehle, um Clientknoten aus der Produktionsumgebung zu entfernen. Clientknoten umfassen Anwendungen, Systeme und virtuelle Maschinen.
- DEFINE-Befehle
  Mit den DEFINE-Befehlen können IBM Spectrum Protect-Objekte erstellt werden.
- DELETE-Befehle
  Mit den DELETE-Befehlen kann ein IBM Spectrum Protect-Objekt gelöscht oder entfernt werden.
- DISABLE-Befehle
  Mit den DISABLE-Befehlen können Sie einige durch den Server ausgeführte Operationstypen verhindern.
- DISMOUNT-Befehl
  Mit dem Befehl DISMOUNT kann ein Datenträger nach der Adresse der realen Einheit oder nach dem Datenträgernamen entladen werden.
- DISPLAY OBJNAME (Vollständigen Objektnamen anzeigen)
  Mit diesem Befehl kann IBM Spectrum Protect einen vollständigen Objektnamen anzeigen, wenn der in einer Nachricht oder in einer Abfrageausgabe angezeigte Name aufgrund der Länge abgekürzt wurde. Objektnamen, die sehr lang sind, sind über normale Betriebssystemfunktionen schwer anzuzeigen und zu verwenden. Der IBM Spectrum Protect-Server kürzt lange Namen ab und ordnet ihnen eine Token-ID zu, die verwendet werden kann, wenn der Objektpfadname 1024 Byte überschreitet. Die Token-ID wird in einer Zeichenfolge angezeigt, die IDs für den Knoten, den Dateibereich und den Objektnamen einschließt. Das Format ist: [TSMOBJ:*nID.fsID.objID*]. Bei Angabe mit dem Befehl DISPLAY OBJNAME kann die Token-ID verwendet werden, um den vollständigen Objektnamen anzuzeigen.
- ENABLE-Befehle
  Mit den ENABLE-Befehlen können Sie einige durch den Server ausgeführte Operationstypen zulassen.
- ENCRYPT STGPOOL (Daten in einem Speicherpool verschlüsseln)
  Mit diesem Befehl können Daten in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool verschlüsselt werden.
- END EVENTLOGGING (Ereignisprotokollierung stoppen)
  Mit diesem Befehl kann das Protokollieren von Ereignissen für einen aktiven Empfänger gestoppt werden.
- EXPIRE INVENTORY (Datenträgerbestandsverfall manuell starten)
  Mit diesem Befehl kann die Verarbeitung des Datenträgerbestandsverfalls manuell gestartet werden. Beim Bestandsverfallsprozess werden Kopien von Clientsicherungs- und Archivierungsdateien aus dem Serverspeicher entfernt. Das Entfernen basiert auf Maßnahmenspezifikationen in den Sicherungs- und Archivierungskopiengruppen der Verwaltungsklassen, an die die Dateien gebunden sind.
- EXPORT-Befehle
  Mit den EXPORT-Befehlen können Informationen von einem IBM Spectrum Protect-Server auf sequenzielle austauschbare Datenträger kopiert werden.
- EXTEND DBSPACE (Speicherbereich für die Datenbank erhöhen)
  Verwenden Sie diesen Befehl, um den Speicherbereich für die Datenbank zu vergrößern, indem Verzeichnisse für die Datenbank hinzugefügt werden.

- GENERATE-Befehle
  Verwenden Sie die GENERATE-Befehle für Sicherungsgruppen für einen ausgewählten Dateibereich oder Clientknoten.
- GRANT-Befehle
  Verwenden Sie den Befehl GRANT, um entsprechende Berechtigungen oder entsprechenden Zugriff zu erteilen.
- HALT (Server abschalten)
  Mit diesem Befehl kann der Server abgeschaltet werden. Der Befehl HALT erzwingt ein sofortiges Abschalten, wobei alle Verwaltungs- und Clientknotensitzungen abgebrochen werden, auch wenn sie noch nicht beendet sind.
- HELP (Hilfe für Befehle und Fehlernachrichten anfordern)
  Mit diesem Befehl können Verwaltungsbefehle und Fehlernachrichten angezeigt werden. Der Befehl kann von einem Verwaltungsbefehlszeilenclient ausgegeben werden.
- IDENTIFY DUPLICATES (Doppelte Daten in einem Speicherpool identifizieren)
  Verwenden Sie diesen Befehl, um Prozesse zu starten oder zu stoppen, die doppelte Daten in einem Speicherpool identifizieren. Sie können die Anzahl der Prozesse zum Identifizieren doppelter Daten und ihre Dauer angeben.
- Befehle IMPORT
  Mit den IMPORT-Befehlen können Informationen von Exportdatenträgern auf einen IBM Spectrum Protect-Server importiert werden.
- INSERT MACHINE (Maschinenkenndaten oder Wiederh.-Anweisungen einfügen)
  Mit diesem Befehl können vorhandenen Maschineninformationen in der Datenbank Client-Maschinenkenndaten oder Wiederherstellungsanweisungen hinzugefügt werden.
- ISSUE MESSAGE (Nachricht aus einem Server-Script ausgeben)
  Diesen Befehl mit Rückkehrcodeverarbeitung in einem Script verwenden, um eine Nachricht aus einem Server-Script auszugeben, mit der die Fehlerquelle bei einem Befehl in dem Script bestimmt wird.
- LABEL LIBVOLUME (Datenträger im Kassettenarchiv Kennsatz zuordnen)
  Mit diesem Befehl kann Banddatenträgern ein Kennsatz zugeordnet werden; in einem automatisierten Kassettenarchiv wird den Datenträgern automatisch beim Zurückstellen ein Kennsatz zugeordnet. Mit diesem Befehl verwendet der Server den Kennsatz mit vollständiger Länge, mit dem die Datenträger häufig vorgekennzeichnet sind.
- LOAD DEFALERTTRIGGERS (Standardgruppe von Alertauslösern laden)
  Verwenden Sie diesen Befehl, um die Standardgruppe von Alertauslösern auf den IBM Spectrum Protect-Server zu laden.
- LOCK-Befehle
  Mit den LOCK-Befehlen kann der Benutzerzugriff auf den Server verhindert werden.
- MACRO (Makro aufrufen)
  Mit diesem Befehl kann eine Datei über die Verwaltungsbefehlszeile aufgerufen werden, die auszuführende IBM Spectrum Protect-Verwaltungsbefehle enthält.
- MIGRATE STGPOOL (Speicherpool in nächsten Speicherpool umlagern)
  Mit diesem Befehl können Dateien aus einem Speicherpool in den nächsten Speicherpool in der Speicherhierarchie umgelagert werden.
- MOVE-Befehle
  Mit den MOVE-Befehlen können Sicherungs- oder Archivierungsdaten zwischen Speicherpools oder Datenträger zur Wiederherstellung nach einem Katastrophenfall vor Ort und an einen ausgelagerten Standort versetzt werden.
- NOTIFY SUBSCRIBERS (Verwaltete Server auf Profilaktualisierung hinweisen)
  Mit diesem Befehl können auf einem Konfigurationsmanager ein oder mehrere verwaltete Server benachrichtigt werden, dass ihre Konfigurationsdaten sofort aktualisiert werden müssen.
- PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Kassettenarchiv definieren oder löschen)
  Verwenden Sie diesen Befehl, um alle Laufwerke und ihre Pfade für ein einzelnes Kassettenarchiv in einem Schritt zu definieren oder zu löschen.
- PING SERVER (Verbindung zwischen Servern testen)
  Mit diesem Befehl kann die Verbindung zwischen dem lokalen Server und einem fernen Server getestet werden.
- PREPARE (Wiederherstellungsplandatei erstellen)
  Mit diesem Befehl kann eine Wiederherstellungsplandatei erstellt werden, die die für die Wiederherstellung eines IBM Spectrum Protect-Servers erforderlichen Daten enthält. Eine Wiederherstellungsplandatei kann in einem Dateisystem gespeichert werden, auf das vom Quellenserver oder einem Zielserver zugegriffen werden kann.
- PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)
  Verwenden Sie diesen Befehl, um Daten in einem Verzeichniscontainerspeicherpool zu schützen, indem eine Kopie der Daten in einem anderen Speicherpool auf einem Zielreplikationsserver oder auf demselben Server gespeichert wird und die Daten auf Band geschützt werden. Wenn Sie den Verzeichniscontainerspeicherpool schützen, können Sie später mithilfe des Befehls REPAIR STGPOOL versuchen, beschädigte Daten in dem Speicherpool zu reparieren.
- QUERY-Befehle
  Mit den QUERY-Befehlen können Informationen zu IBM Spectrum Protect-Objekten angefordert oder angezeigt werden.
- QUIT (Interaktiven Modus des Verwaltungsclient verlassen)
  Mit diesem Befehl kann eine Verwaltungs-Client-Sitzung im interaktiven Modus beendet werden.
- RECLAIM STGPOOL (Datenträger im Speicherpool mit sequenziellem Zugriff wiederherstellen)
  Verwenden Sie diesen Befehl, um Datenträger in einem Speicherpool mit sequenziellem Zugriff wiederherzustellen. Bei der Wiederherstellung werden keine inaktiven Versionen von Sicherungsdaten von Datenträgern in Pools für aktive Daten versetzt.
- RECONCILE VOLUMES (Unterschiede abstimmen)
  Diesen Befehl vom Quellen-Server ausgeben, um Unterschiede zwischen den Definitionen der virtuellen Datenträger auf dem Quellen-Server und den Archivierungsdateien auf dem Ziel-Server abzustimmen. IBM Spectrum Protect sucht alle Datenträger mit der angegebenen Einheitenklasse auf dem Quellen-Server und alle entsprechenden Archivierungsdateien auf dem Ziel-Server. Der Datenträgerbestand auf dem Ziel-Server wird auch mit der lokalen Definition für virtuelle Datenträger verglichen, um festzustellen, ob Inkonsistenzen vorhanden sind.

- REGISTER-Befehle
  Mit den REGISTER-Befehlen können Objekte in IBM Spectrum Protect definiert oder hinzugefügt werden.
- REMOVE-Befehle
  Mit den REMOVE-Befehlen kann ein Objekt aus IBM Spectrum Protect entfernt werden.
- RENAME-Befehle
  Mit den RENAME-Befehlen kann der Name eines vorhandenen Objekts geändert werden.
- REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)
  Mit diesem Befehl können deduplizierte Speicherbereiche in einem Verzeichniscontainerspeicherpool repariert werden. Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die auf dem Zielreplikationsserver oder in Containerkopienspeicherpools auf demselben Server gesichert werden.
- REPLICATE NODE (Daten in Dateibereichen replizieren, die zu einem Clientknoten gehören)
  Verwenden Sie diesen Befehl, um Daten in Dateibereichen zu replizieren, die zu einem oder mehreren Clientknoten oder zu definierten Gruppen von Clientknoten gehören.
- REPLY (Verarbeitung einer Anforderung fortsetzen)
  Mit Hilfe dieses Befehls und einer Identifikationsnummer kann der Server darüber informiert werden, dass eine angeforderte Operation beendet wurde. Nicht alle Serveranforderungen erfordern eine Antwort. Dieser Befehl ist nur erforderlich, wenn die Anforderungsnachricht ausdrücklich angibt, dass eine Antwort benötigt wird.
- RESET PASSEXP (Kennwortablaufdauer zurücksetzen)
  Verwenden Sie den Befehl RESET PASSEXP, um die Kennwortablaufdauer für Kennwörter von Administratoren und Clientknoten auf die allgemeine Kennwortablaufdauer zurückzusetzen. Der Befehl RESET PASSEXP gilt nicht für Kennwörter, die auf einem LDAP-Verzeichnisserver gespeichert werden.
- RESTART EXPORT (Ausgesetzte Exportoperation erneut starten)
  Mit diesem Befehl kann eine ausgesetzte Exportoperation erneut gestartet werden.
- RESTORE-Befehle
  Mit den RESTORE-Befehlen können IBM Spectrum Protect-Speicherpools oder -Datenträger zurückgeschrieben werden.
- REVOKE-Befehle
  Mit den REVOKE-Befehlen können Sie Berechtigungen oder den Zugriff widerrufen.
- ROLLBACK (Nicht festgeschriebene Änderungen in einem Makro rückgängig machen)
  Mit diesem Befehl können innerhalb eines Makros Änderungen rückgängig gemacht werden, die von Befehlen, die vom Server ausgeführt wurden, vorgenommen, jedoch noch nicht in der Datenbank festgeschrieben wurden. Eine festgeschriebene Änderung ist permanent und kann nicht rückgängig gemacht werden. Der Befehl ROLLBACK ist für das Testen von Makros nützlich.
- RUN (IBM Spectrum Protect-Prozedur ausführen)
  Mit diesem Befehl kann eine IBM Spectrum Protect-Prozedur ausgeführt werden. Soll dieser Befehl auf einem anderen Server ausgegeben werden, muß die Prozedur, die ausgeführt wird, auf diesem Server definiert sein.
- SELECT (SQL-Abfrage für die IBM Spectrum Protect-Datenbank ausführen)
  Verwenden Sie den Befehl SELECT, um eine angepasste Abfrage der IBM Spectrum Protect-Datenbank zu erstellen und zu formatieren.
- SET-Befehle
  Mit den SET-Befehlen können Sie Werte angeben, die viele verschiedene IBM Spectrum Protect-Operationen betreffen.
- SETOPT (Serveroption für dynamisches Aktualisieren definieren)
  Mit dem Befehl SETOPT können Sie die meisten Serveroptionen dynamisch aktualisieren, ohne den Server zu stoppen und erneut zu starten. Für die Option DBDIAGLOGSIZE müssen Sie den Server stoppen und erneut starten. Ein Befehl SETOPT, der in einem Makro oder in einer Prozedur enthalten ist, kann nicht rückgängig gemacht werden.
- SHRED DATA (Daten schreddern)
  Verwenden Sie diesen Befehl, um den Prozess zum Schreddern gelöschter sensibler Daten manuell zu starten. Das manuelle Schreddern ist nur möglich, wenn das automatische Schreddern inaktiviert ist.
- SUSPEND EXPORT (Momentan aktive Exportoperation aussetzen)
  Mit diesem Befehl können Sie eine momentan aktive Exportoperation zwischen Servern aussetzen, die einen anderen FILEDATA-Wert als NONE hat. Die Exportoperation, die ausgesetzt werden soll, muss nach der Initialisierungsphase liegen, um für die Aussetzung ausgewählt werden zu können. Der Status der Exportoperation wird gespeichert. Die Operation kann mit dem Befehl RESTART EXPORT erneut gestartet werden.
- UNLOCK-Befehle
  Verwenden Sie die UNLOCK-Befehle, um den Zugriff erneut einzurichten, nachdem ein Objekt gesperrt wurde.
- UPDATE-Befehle
  Mit den UPDATE-Befehlen können ein oder mehrere Attribute eines vorhandenen IBM Spectrum Protect-Objekts geändert werden.
- VALIDATE-Befehle
  Mit dem Befehl VALIDATE kann überprüft werden, ob ein Objekt für IBM Spectrum Protect vollständig oder gültig ist.
- VARY (Datenträger mit wahlfreiem Zugriff an-/abhängen)
  Mit diesem Befehl kann ein Speicherpooldatenträger mit wahlfreiem Zugriff für den Server angehängt oder abgehängt werden.

ACCEPT DATE (Aktuelles Systemdatum akzeptieren)

Mit diesem Befehl können Sie den Server mit der normalen Verarbeitung beginnen lassen, wenn der Server aufgrund einer Abweichung zwischen dem Serverdatum und dem aktuellen Systemdatum die normale Verarbeitung nicht startet.

Wenn der Server aufgrund einer Abweichung zwischen dem Serverdatum und dem aktuellen Datum die normale Verarbeitung nicht startet, wird mit diesem Befehl der Server gezwungen, das aktuelle Datum und die aktuelle Uhrzeit als gültig zu akzeptieren. Ist die Systemzeit gültig und wurde der Server längere Zeit nicht ausgeführt, sollte dieser Befehl ausgeführt werden, um es dem Server zu ermöglichen, mit der normalen Verarbeitung zu beginnen.

Achtung: Ist das Systemdatum ungültig oder wurde der Server zuvor mit einem ungültigen Systemdatum erstellt oder ausgeführt und wird dieser Befehl ausgegeben, kann jede Serververarbeitung oder jeder Befehl, die bzw. der Datumsangaben verwendet, zu unerwarteten Ergebnissen führen. Beispielsweise kann die Dateiverfallsverarbeitung betroffen sein. Wird der Server mit dem korrekten Datum gestartet, werden Dateien, die mit zukünftigen Datumsangaben gesichert wurden, erst dann für die Verfallsverarbeitung berücksichtigt, wenn dieses zukünftige Datum erreicht wird. Dateien, die mit zurückliegenden Datumsangaben gesichert wurden, verfallen schneller. Wenn die Serververarbeitung ein zukünftiges Datum erkennt, wird eine Fehlernachricht ausgegeben.

Wenn der Server ein ungültiges Datum oder eine ungültige Uhrzeit erkennt, werden Serversitzungen inaktiviert (wie bei der Ausgabe des Befehls DISABLE SESSIONS). Die Verarbeitung von Verfalls-, Umlagerungs- und Wiederherstellungsoperationen sowie von Operationen zum Löschen der Datenträgerhistory kann nicht fortgesetzt werden.

Verwenden Sie den Befehl ENABLE SESSIONS ALL nach der Ausgabe des Befehls ACCEPT DATE, um Sitzungen für den Start erneut zu aktivieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-ACCept Date-----------------------------------------------><
```

Parameter

Keine.

Beispiel: Das aktuelle Systemdatum akzeptieren

Dem Server das Akzeptieren des aktuellen Datums als gültiges Datum erlauben.

```
accept date
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für ACCEPT DATE

Befehl	Beschreibung
ENABLE SESSIONS	Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.

ACTIVATE POLICYSET (Neue Maßnahmengruppe aktivieren)

Mit diesem Befehl kann der Inhalt einer Maßnahmengruppe in die AKTIVE Maßnahmengruppe für die Domäne kopiert werden. Der Server verwendet die Regeln in der AKTIVEN Maßnahmengruppe, um Clientoperationen in der Domäne zu verwalten. Für eine Maßnahmendomäne können mehrere Maßnahmengruppen definiert werden, aber es kann nur eine Maßnahmengruppe aktiv sein. Die aktuelle AKTIVE Maßnahmengruppe wird durch die Maßnahmengruppe ersetzt, die bei Ausgabe dieses Befehls angegeben wird. Die AKTIVE Maßnahmengruppe kann nur geändert werden, indem eine andere Maßnahmengruppe aktiviert wird.

Bevor eine Maßnahmengruppe aktiviert wird, muss mit dem Befehl VALIDATE POLICYSET geprüft werden, ob die Maßnahmengruppe vollständig und gültig ist.

Der Befehl ACTIVATE POLICYSET schlägt fehl, wenn eine der folgenden Bedingungen vorhanden ist:

- Eine Kopiengruppe gibt einen Kopienspeicherpool als Zielort an.
- Eine Verwaltungsklasse gibt einen Kopienspeicherpool als Zielort für Dateien an, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.
- Die Maßnahmengruppe hat keine Standardverwaltungsklasse.
- Ein Parameter TOCDESTINATION ist angegeben, und der Speicherpool ist entweder ein Kopienpool oder der Speicherpool hat ein anderes Format als NATIVE oder NONBLOCK.

Die AKTIVE Maßnahmengruppe und die letzte aktivierte Maßnahmengruppe müssen nicht notwendigerweise identisch sein. Die ursprüngliche Maßnahmengruppe, die aktiviert wurde, kann ohne Auswirkungen auf die AKTIVE Maßnahmengruppe geändert werden.

Ist für den Server der Aufbewahrungsschutz für Daten aktiviert, müssen die folgenden Bedingungen zutreffen:

- Alle Verwaltungsklassen in der Maßnahmengruppe, die aktiviert werden soll, müssen eine Archivierungskopiengruppe enthalten.
- Ist eine Verwaltungsklasse in der aktiven Maßnahmengruppe vorhanden, muss eine Verwaltungsklasse mit demselben Namen in der Maßnahmengruppe vorhanden sein, die aktiviert werden soll.

- Ist eine Archivierungskopiengruppe in der aktiven Maßnahmengruppe vorhanden, muss die entsprechende Kopiengruppe in der zu aktivierenden Maßnahmengruppe über einen Wert für RETVER verfügen, der mindestens so groß wie die entsprechenden Werte in der aktiven Kopiengruppe ist.

Achtung: Der Aufbewahrungsschutz gilt nur für Archivierungsobjekte.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

Syntax

```
>>-ACTivate POlicyset--Domänenname--Name_der_Maßnahmengruppe--->< 
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, für die eine Maßnahmengruppe aktiviert werden soll.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, die aktiviert werden soll.

Beispiel: Eine Maßnahmengruppe für eine bestimmte Maßnahmendomäne aktivieren

Die Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE_RECORDS aktivieren.

```
activate policyset employee_records vacation
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ACTIVATE POLICYSET

Befehl	Beschreibung
COPY POLICYSET	Erstellt eine Kopie einer Maßnahmengruppe.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
DELETE POLICYSET	Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
UPDATE POLICYSET	Ändert die Beschreibung einer Maßnahmengruppe.
VALIDATE POLICYSET	Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert.

ASSIGN DEFMGMTCLASS (Standardverwaltungsklasse zuordnen)

Mit diesem Befehl kann eine Verwaltungsklasse als Standardverwaltungsklasse für eine Maßnahmengruppe angegeben werden. Es muß eine Standardverwaltungsklasse für eine Maßnahmengruppe zugeordnet werden, damit diese Maßnahmengruppe aktiviert werden kann.

Um sicherzustellen, dass Clients immer Dateien sichern und archivieren können, wählen Sie eine Standardverwaltungsklasse aus, die sowohl eine Archivierungskopiengruppe als auch eine Sicherungskopiengruppe enthält.

Der Server verwendet die Standardverwaltungsklasse, um Clientdateien zu verwalten, wenn keine Verwaltungsklasse zugeordnet oder geeignet ist. Beispielsweise verwendet der Server die Standardverwaltungsklasse, wenn ein Benutzer keine Verwaltungsklasse in der Einschluss-/Ausschlussliste angibt.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

Syntax

```
>>-ASsign DEFMGmtclass--Domänenname--Name_der_Maßnahmengruppe--Klassenname-><
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Verwaltungsklasse gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, für die die Standardverwaltungsklasse zugeordnet werden soll. Für die aktive Maßnahmengruppe (ACTIVE) kann keine Standardverwaltungsklasse zugeordnet werden.

Klassenname (Erforderlich)
: Gibt die Verwaltungsklasse an, die als Standardverwaltungsklasse für die Maßnahmengruppe verwendet werden soll.

Beispiel: Eine Standardverwaltungsklasse zuordnen

DEFAULT1 als Standardverwaltungsklasse für Maßnahmengruppe SUMMER in der Maßnahmendomäne PROG1 zuordnen.

```
assign defmgmtclass prog1 summer default1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ASSIGN DEFMGMTCLASS

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
DELETE MGMTCLASS	Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.
UPDATE MGMTCLASS	Ändert die Attribute einer Verwaltungsklasse.
VALIDATE POLICYSET	Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert.

AUDIT-Befehle

Mit den AUDIT-Befehlen kann die Qualität der Datenbankinformationen und der Speicherpooldatenträger überprüft oder untersucht werden. Mit dem Befehl AUDIT LDAPDIRECTORY werden Knoten oder Administrator-IDs auf einem LDAP-Verzeichnisserver gelöscht, die ihre Kennwörter nicht mit dem LDAP-Verzeichnisserver authentifizieren.

- AUDIT CONTAINER
  - AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Cloud-Container prüfen)
  - AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)
- AUDIT LDAPDIRECTORY (LDAP-Verzeichnisserver prüfen)
- AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Kassettenarchiv prüfen)
- AUDIT LIBVOLUME (Datenbankinformationen für einen Banddatenträger prüfen)
- AUDIT LICENSES (Serverspeicherbelegung prüfen)
- AUDIT VOLUME (Datenbankinformationen für Speicherpooldatenträger prüfen)

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

AUDIT CONTAINER-Befehle

Mit dem Befehl AUDIT CONTAINER können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Cloud- oder Verzeichnisspeicherpool suchen.

- AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Cloud-Container prüfen)
  Mit diesem Befehl können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Cloud-Containerspeicherpool suchen. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.
- AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)
  Mit diesem Befehl können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Verzeichniscontainerspeicherpool suchen.

AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Cloud-Container prüfen)

Mit diesem Befehl können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Cloud-Containerspeicherpool suchen. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.

Mit diesem Befehl können Sie die folgenden Aktionen für einen Container in einem Cloud-Containerspeicherpool ausführen:

- Den Inhalt eines Containers durchsuchen, um die Integrität der Datenbereiche zu überprüfen
- Daten aus einem Container entfernen, der als *beschädigt* markiert ist, wenn beispielsweise eine Datei Verweise in der Serverdatenbank hat, aber fehlende oder beschädigte Daten in der Cloud hat
- Einen vollständigen Container als beschädigt markieren
- Daten entfernen, die als *verwaist* markiert sind, wenn beispielsweise ein in der Cloud gespeichertes Objekt keinen Verweis in der Serverdatenbank hat

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

Parameter

Containername
: Gibt den Namen des Containers an, der geprüft werden soll. Wird dieser Parameter nicht angegeben, müssen Sie einen Cloud-Containerspeicherpool angeben.

STGpool

Gibt den Namen des Cloud-Containerspeicherpools an, der geprüft werden soll. Dieser Parameter ist wahlfrei. Wird nur dieser Parameter angegeben, werden alle Container geprüft, die für den Speicherpool definiert sind. Wird dieser Parameter nicht angegeben, müssen Sie einen Container angeben.

STGPOOLDIRectory

Gibt den Namen des Cloud-Containerspeicherpoolverzeichnisses an, das geprüft werden soll. Dieser Parameter ist wahlfrei.
Einschränkung: Sie müssen einen Speicherpool angeben, der lokalen Speicher verwendet.

Aktion

Gibt an, welche Aktion der Server ausführt, wenn ein Container in einem Cloud-Containerspeicherpool geprüft wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

SCANAll

Gibt an, dass der Server Datenbanksätze identifiziert, die sich auf Datenbereiche mit Inkonsistenzen beziehen. Es erfolgt eine Überprüfung auf Daten im Cloud-Containerspeicherpool, die nicht mit den Daten in der Serverdatenbank übereinstimmen. Dieser Wert ist der Standardwert. Der Server markiert den Datenbereich in der Datenbank als beschädigt.
Tipp: Wenn Sie den Parameter ACTION=SCANALL für einen IBM® Cloud Object Storage-Speicherpool angeben, der eine Vault mit inaktivierter Namensindexierung verwendet, wird bei der Prüfoperation die gesamte Vault durchsucht, um verwaiste Bereiche in jedem Container zu identifizieren. Geben Sie in dieser Situation WAIT=YES an, wenn die Prüfoperation auf die Beendigung der Suche nach verwaisten Bereichen warten soll, bevor die Prüfung als abgeschlossen zurückgemeldet wird. Diese Suche nach verwaisten Bereichen erfolgt nur, wenn Sie keinen Containernamen angeben. Wenn Sie einen Container angeben, der sich in einer Vault mit inaktivierter Namensindexierung befindet, sucht die Prüfoperation nicht nach verwaisten Bereichen.

REMOVEDamaged

Gibt an, dass der Server alle Referenzen auf beschädigte Bereiche aus der Serverdatenbank entfernt. Falls gefunden, werden die beschädigten Bereiche auch aus dem Cloud-Containerspeicherpool entfernt. Der Server entfernt auch alle verwaisten Bereiche aus dem Cloud-Containerspeicherpool und entfernt die Referenzen auf diese verwaisten Bereiche aus der Datenbank, wie mit dem Parameter FORCEORPHANDBDEL angegeben ist.

MARKDamaged

Gibt an, dass der Server explizit alle Datenbereiche in dem Container als beschädigt markiert.

SCANDamaged

Gibt an, dass der Server nur die vorhandenen beschädigten Bereiche in dem Container überprüft.

Wichtig: Wenn keine Verbindung zur Cloud vorhanden ist, werden die Parameter ACTION=SCANALL und ACTION=SCANDAMAGED nicht ausgeführt. Der Parameter ACTION=MARKDAMAGED wird jedoch ohne eine Cloudverbindung wie erwartet ausgeführt, und der Parameter ACTION=REMOVEDAMAGED markiert alle beschädigten Daten als verwaist. Sobald die Verbindung zur Cloud wieder hergestellt wurde, löscht der Server die verwaisten Bereiche.
Statusrücksetzbedingung: Wenn bei der Prüfung kein Fehler bei einem Datenbereich erkannt wird, der als beschädigt markiert ist, wird der Status des Datenbereichs zurückgesetzt. Der Datenbereich kann dann verwendet werden. Diese Bedingung bietet eine Möglichkeit, den Status von beschädigten Datenbereichen zurückzusetzen, wenn Fehler durch ein korrigierbares Problem verursacht werden. Die Optionen SCANALL und SCANDAMAGED sind die einzigen Optionen, die einen beschädigten Bereich zurücksetzen, wenn festgestellt wird, dass der Bereich nicht beschädigt ist.

FORCEOrphandbdel

Gibt an, dass der Server das Löschen von verwaisten Bereichen aus der Serverdatenbank erzwingt, auch wenn sie nicht aus dem Cloud-Containerspeicherpool gelöscht werden. Dieser Parameter ist wahlfrei. Wenn Sie diesen Parameter angeben, müssen Sie auch den Parameter ACTION=REMOVEDAMAGED angeben. Folgende Optionen sind verfügbar:

Yes

Gibt an, dass der Server alle verwaisten Bereiche aus der Serverdatenbank löscht, auch wenn sie nicht aus dem Cloud-Containerspeicherpool gelöscht werden.

No

Gibt an, dass der Server die verwaisten Bereiche in der Serverdatenbank behält, wenn sie nicht aus dem Cloud-Containerspeicherpool gelöscht werden können. Dieser Wert ist der Standardwert.

MAXProcess

Gibt die maximale Anzahl paralleler Prozesse für die Überprüfung eines Containers in einem Cloud-Containerspeicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 99 ein. Der Standardwert ist 4.
Einschränkung: Der Server ignoriert diesen Parameter, wenn Sie MAXPROCESS mit dem Parameter ACTION=REMOVEDAMAGED verwenden.

Wait

Gibt an, ob die Prüfoperation im Vordergrund oder im Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Folgende Optionen sind verfügbar:

No

Gibt an, dass die Operation im Hintergrund ausgeführt wird. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Dieser Wert ist der Standardwert.

Yes

Gibt an, dass die Operation im Vordergrund ausgeführt wird. Die Ausführung der Operation nimmt unter Umständen viel Zeit in Anspruch. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.
Einschränkung: Sie können den Parameter WAIT=YES nicht an der Serverkonsole angeben.

BEGINDate

Gibt den Datumsbereichswert an, bei dem die Prüfung gestartet werden soll. Container, die zuletzt innerhalb des angegebenen Datumsbereichs geprüft wurden, werden geprüft. Wenn Sie eine Uhrzeit, aber kein Anfangsdatum angeben, wird das aktuelle Datum verwendet. Wenn Sie kein Anfangs- und Enddatum angeben, werden alle Container geprüft. Der Standardwert ist das Datum vor der Ausführung der ersten Prüfung für den Container. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit, zu der die Prüfung beginnen soll, wie folgt angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum.	09/15/2016
TODAY	Das aktuelle Datum.	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–7 *oder* –7. Um alle Container zu prüfen, die in der letzten Woche geprüft wurden, geben Sie BEGINDATE=TODAY-7 oder BEGINDATE= -7 an.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Container einzuschließen, die am Tag vor dem letzten Tag des Vormonats geprüft wurden.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Container einzuschließen, die am zehnten Tag des aktuellen Monats geprüft wurden.

BEGINTime

Gibt den Zeitbereichswert an, bei dem die Prüfung gestartet werden soll. Container, die zuletzt innerhalb des angegebenen Zeitbereichs geprüft wurden, werden geprüft. Wenn Sie keine Anfangs- und Endzeit angeben, wird der Zeitbereich auf 00:00:00 bis 23:59:59 gesetzt. Der Standardwert ist 00:00:00. Wenn Sie keinen Datumsbereich angegeben haben, ist der Standardwert das heutige Datum. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit, zu der die Prüfung beginnen soll, wie folgt angeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Anfangsdatum.	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Anfangsdatum.	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum.	NOW+03:00 *oder* +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW+3 oder BEGINTIME=+3 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 12:00 Uhr oder später am Anfangsdatum geprüft.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum.	NOW-04:00 *oder* -04:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTime=NOW-3:30 oder BEGINTime= -3:30 ausgegeben, prüft IBM Spectrum Protect Container mit der Uhrzeit der letzten Prüfung 5:30 Uhr oder später am Anfangsdatum.

ENDDate

Gibt den Datumsbereichswert an, bei dem die Prüfung gestoppt werden soll. Container, die zuletzt innerhalb des angegebenen Datumsbereichs geprüft wurden, werden geprüft. Wenn Sie eine Uhrzeit, aber keinen Datumswert angeben, wird das aktuelle Datum verwendet. Wenn Sie kein Anfangs- und Enddatum angeben, werden alle Container geprüft. Der Standardwert ist das Datum nach der Ausführung der letzten Prüfung für den Container. Dieser Parameter ist wahlfrei.

Sie können das Datum mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum.	09/15/2016
TODAY	Das aktuelle Datum.	TODAY

Wert	Beschreibung	Beispiel
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–1 *oder* –1. Um Container einzuschließen, die bis gestern geprüft wurden, können Sie ENDDATE=TODAY-1 oder ENDDATE= -1 angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Container einzuschließen, die am Tag vor dem letzten Tag des Vormonats geprüft wurden.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Container einzuschließen, die am zehnten Tag des aktuellen Monats geprüft wurden.

ENDTime

Gibt den Zeitbereichswert an, bei dem die Prüfung gestoppt werden soll. Container, die zuletzt innerhalb des angegebenen Zeitbereichs geprüft wurden, werden geprüft. Wenn Sie keine Anfangs- und Endzeit angeben, wird der Zeitbereich auf 00:00:00 bis 23:59:59 gesetzt. Der Standardwert ist 23:59:59. Dieser Parameter ist wahlfrei.
Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Enddatum.	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Enddatum.	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Enddatum.	NOW+03:00 *oder* +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+3:00 oder ENDTIME= +3:00 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 12:00 Uhr oder früher am angegebenen Enddatum geprüft.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Enddatum.	NOW-03:30 *oder* -03:30. Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME= -3:30 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 5:30 Uhr oder früher am angegebenen Enddatum geprüft.

Beispiel: Einen bestimmten Container in einem Cloud-Containerspeicherpool prüfen

Den Container 42-00000my000example000container000 in einem Cloud-Containerspeicherpool prüfen.

```
audit container 42-00000my000example000container000 action=scanall
```

Beispiel: Einen Cloud-Containerspeicherpool innerhalb eines bestimmten Zeitrahmens prüfen

Einen Cloud-Containerspeicherpool mit dem Namen POOL3 prüfen und nur Container einschließen, die gestern zwischen 9:30 und 12:30 Uhr geprüft wurden.

```
audit container stgpool=pool3 begindate=today-1
begintime=09:30:00 endtime=12:30:00
```

Tabelle 1. Zugehörige Befehle für AUDIT CONTAINER

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY CONTAINER	Zeigt Informationen zu einem Container an.
QUERY DAMAGED	Zeigt Informationen zu beschädigten Dateien an.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

AUDIT CONTAINER (Konsistenz der Datenbankinformationen für einen Verzeichniscontainer prüfen)

Mit diesem Befehl können Sie nach Inkonsistenzen zwischen Datenbankinformationen und einem Container in einem Verzeichniscontainerspeicherpool suchen.

Mit diesem Befehl können Sie die folgenden Aktionen für einen Container in einem Verzeichniscontainerspeicherpool ausführen:

- Den Inhalt eines Containers durchsuchen, um die Integrität der Datenbereiche zu überprüfen
- Beschädigte Daten aus einem Container entfernen
- Einen vollständigen Container als beschädigt markieren

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-AUDit CONTainer--+-Containername-----------------------------------------------+-->
                    +-STGpool--=--Poolname-----------------------------------------+
                    '-STGpool--=--Poolname--STGPOOLDIRectory--=--Verzeichnisname-'

   .-Action--=--SCANAll-----------.
>--+------------------------------+----------------------------->
   '-Action--=--+-SCANAll-------+-'
                +-REMOVEDamaged-+
                +-MARKDamaged---+
                '-SCANDamaged---'

   .-MAXProcess--=--4------.  .-Wait--=--No------.
>--+----------------------+--+------------------+-------------->
   '-MAXProcess--=--Anzahl-'  '-Wait--=--+-No--+-'
                                         '-Yes-'

   .-BEGINDate--=--vor der ersten Prüfung-.
>--+--------------------------------------+---------------------->
   '-BEGINDate--=--Anfangsdatum-----------'

   .-BEGINTime--=--00:00:00----.
>--+---------------------------+------------------------------->
   '-BEGINTime--=--Anfangszeit-'

   .-ENDDate--=--nach der letzten Prüfung-.
>--+--------------------------------------+---------------------->
   '-ENDDate--=--Enddatum-----------------'

   .-ENDTime--=--23:59:59-.
>--+----------------------+----------------------------------><
   '-ENDTime--=--Endzeit--'
```

Parameter

Containername
: Gibt den Namen des Containers an, der geprüft werden soll. Wird dieser Parameter nicht angegeben, müssen Sie einen Verzeichniscontainerspeicherpool angeben.

STGpool
: Gibt den Namen des Verzeichniscontainerspeicherpools an, der geprüft werden soll. Dieser Parameter ist wahlfrei. Wird nur dieser Parameter angegeben, werden alle Container geprüft, die für den Speicherpool definiert sind. Wird dieser Parameter nicht angegeben, müssen Sie einen Container angeben.

STGPOOLDIRectory
: Gibt den Namen des Containerspeicherpoolverzeichnisses an, das geprüft werden soll. Dieser Parameter ist wahlfrei. Wird dieser Parameter angegeben, werden alle Container geprüft, die für das Containerspeicherpoolverzeichnis definiert sind. Um diesen Parameter anzugeben, müssen Sie auch einen Speicherpool angeben.

Aktion
: Gibt an, welche Aktion der Server ausführt, wenn ein Container in einem Verzeichniscontainerspeicherpool geprüft wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  SCANAll
  : Gibt an, dass der Server Datenbanksätze identifiziert, die sich auf Datenbereiche mit Inkonsistenzen beziehen. Dieser Wert ist der Standardwert. Der Server markiert den Datenbereich in der Datenbank als beschädigt.

Tipp: Wenn Sie den Befehl PROTECT STGPOOL für einen Verzeichniscontainerspeicherpool auf dem Zielserver verwendet haben, können Sie den beschädigten Datenbereich mithilfe des Befehls REPAIR STGPOOL reparieren.

REMOVEDamaged
Gibt an, dass der Server alle Dateien aus der Datenbank entfernt, die den beschädigten Datenbereich referenzieren.

MARKDamaged
Gibt an, dass der Server explizit alle Datenbereiche in dem Container als beschädigt markiert.

SCANDamaged
Gibt an, dass der Server nur die vorhandenen beschädigten Bereiche in dem Container überprüft.

Statusrücksetzbedingung: Wenn bei der Prüfung kein Fehler bei einem Datenbereich erkannt wird, der als beschädigt markiert ist, wird der Status des Datenbereichs zurückgesetzt. Der Datenbereich kann dann verwendet werden. Diese Bedingung bietet eine Möglichkeit, den Status von beschädigten Datenbereichen zurückzusetzen, wenn Fehler durch ein korrigierbares Problem verursacht werden. Die Optionen SCANALL und SCANDAMAGED sind die einzigen Optionen, die einen beschädigten Bereich zurücksetzen, wenn festgestellt wird, dass der Bereich nicht beschädigt ist.

MAXProcess
Gibt die maximale Anzahl paralleler Prozesse für die Überprüfung eines Containers in einem Verzeichniscontainerspeicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 99 ein. Der Standardwert ist 4.

Wait
Gibt an, ob die Prüfoperation im Vordergrund oder im Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Folgende Optionen sind verfügbar:

No
Gibt an, dass die Operation im Hintergrund ausgeführt wird. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Dies ist der Standardwert.

Yes
Gibt an, dass die Operation im Vordergrund ausgeführt wird. Die Ausführung der Operation nimmt unter Umständen viel Zeit in Anspruch. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Einschränkung: Sie können den Parameter WAIT=YES nicht an der Serverkonsole angeben.

BEGINDate
Gibt den Datumsbereichswert an, bei dem die Prüfung gestartet werden soll. Container, die zuletzt innerhalb des angegebenen Datumsbereichs geprüft wurden, werden geprüft. Wenn Sie eine Uhrzeit, aber kein Anfangsdatum angeben, wird das aktuelle Datum verwendet. Wenn Sie kein Anfangs- und Enddatum angeben, werden alle Container geprüft. Der Standardwert ist das Datum vor der Ausführung der ersten Prüfung für den Container. Dieser Parameter ist wahlfrei.
Sie können die Uhrzeit, zu der die Prüfung beginnen soll, wie folgt angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum.	09/15/2016
TODAY	Das aktuelle Datum.	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–7 *oder* –7. Um alle Container zu prüfen, die in der letzten Woche geprüft wurden, geben Sie BEGINDATE=TODAY-7 oder BEGINDATE= -7 an.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Container einzuschließen, die am Tag vor dem letzten Tag des Vormonats geprüft wurden.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Container einzuschließen, die am zehnten Tag des aktuellen Monats geprüft wurden.

BEGINTime
Gibt den Zeitbereichswert an, bei dem die Prüfung gestartet werden soll. Container, die zuletzt innerhalb des angegebenen Zeitbereichs geprüft wurden, werden geprüft. Wenn Sie keine Anfangs- und Endzeit angeben, wird der Zeitbereich auf 00:00:00 bis 23:59:59 gesetzt. Der Standardwert ist 00:00:00. Wenn Sie keinen Datumsbereich angegeben haben, ist der Standardwert das heutige Datum. Dieser Parameter ist wahlfrei.
Sie können die Uhrzeit, zu der die Prüfung beginnen soll, wie folgt angeben:

Wert	**Beschreibung**	**Beispiel**

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Anfangsdatum.	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Anfangsdatum.	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum.	NOW+03:00 *oder* +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW+3 oder BEGINTIME=+3 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 12:00 Uhr oder später am Anfangsdatum geprüft.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum.	NOW-04:00 *oder* -04:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTime=NOW-3:30 oder BEGINTime= -3:30 ausgegeben, prüft IBM Spectrum Protect Container mit der Uhrzeit der letzten Prüfung 5:30 Uhr oder später am Anfangsdatum.

ENDDate

Gibt den Datumsbereichswert an, bei dem die Prüfung gestoppt werden soll. Container, die zuletzt innerhalb des angegebenen Datumsbereichs geprüft wurden, werden geprüft. Wenn Sie eine Uhrzeit, aber keinen Datumswert angeben, wird das aktuelle Datum verwendet. Wenn Sie kein Anfangs- und Enddatum angeben, werden alle Container geprüft. Der Standardwert ist das Datum nach der Ausführung der letzten Prüfung für den Container. Dieser Parameter ist wahlfrei.
Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum.	09/15/2016
TODAY	Das aktuelle Datum.	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–1 *oder* –1. Um Container einzuschließen, die bis gestern geprüft wurden, können Sie ENDDATE=TODAY-1 oder ENDDATE= -1 angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Container einzuschließen, die am Tag vor dem letzten Tag des Vormonats geprüft wurden.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Container einzuschließen, die am zehnten Tag des aktuellen Monats geprüft wurden.

ENDTime

Gibt den Zeitbereichswert an, bei dem die Prüfung gestoppt werden soll. Container, die zuletzt innerhalb des angegebenen Zeitbereichs geprüft wurden, werden geprüft. Wenn Sie keine Anfangs- und Endzeit angeben, wird der Zeitbereich auf 00:00:00 bis 23:59:59 gesetzt. Der Standardwert ist 23:59:59. Dieser Parameter ist wahlfrei.
Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Enddatum.	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Enddatum.	NOW

Wert	Beschreibung	Beispiel
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Enddatum.	NOW+03:00 *oder* +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+3:00 oder ENDTIME= +3:00 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 12:00 Uhr oder früher am angegebenen Enddatum geprüft.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Enddatum.	NOW-03:30 *oder* -03:30. Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME= -3:30 ausgegeben, werden Container mit der Uhrzeit der letzten Prüfung 5:30 Uhr oder früher am angegebenen Enddatum geprüft.

Beispiel: Einen bestimmten Speicherpoolcontainer prüfen

Den Speicherpoolcontainer 0000000000000721.dcf prüfen.

```
audit container n:\ddcont2\07\0000000000000721.dcf action=scanall
```

Beispiel: Beschädigte Daten aus einem Verzeichniscontainerspeicherpool entfernen

Einen Verzeichniscontainerspeicherpool mit dem Namen NEWDEDUP prüfen und beschädigte Dateien entfernen.

```
audit container stgpool=newdedup action=removedamaged
```

Beispiel: Alle Daten in einem Verzeichniscontainerspeicherpool als beschädigt markieren

Einen Verzeichniscontainerspeicherpool mit dem Namen NEWDEDUP prüfen und alle Dateien als beschädigt markieren.

```
audit container stgpool=newdedup maxprocess=2 action=markdamaged
```

Beispiel: Einen Verzeichniscontainerspeicherpool innerhalb eines bestimmten Zeitrahmens prüfen

Einen Verzeichniscontainerspeicherpool mit dem Namen POOL2 prüfen und nur Container einschließen, die gestern zwischen 9:30 und 12:30 Uhr geprüft wurden.

```
audit container stgpool=pool2 begindate=today-1
begintime=09:30:00 endtime=12:30:00
```

Tabelle 1. Zugehörige Befehle für AUDIT CONTAINER

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
MOVE CONTAINER	Versetzt den Inhalt eines Speicherpoolcontainers in einen anderen Container.
QUERY DAMAGED	Zeigt Informationen zu beschädigten Dateien an.

AUDIT LDAPDIRECTORY (LDAP-Verzeichnisserver prüfen)

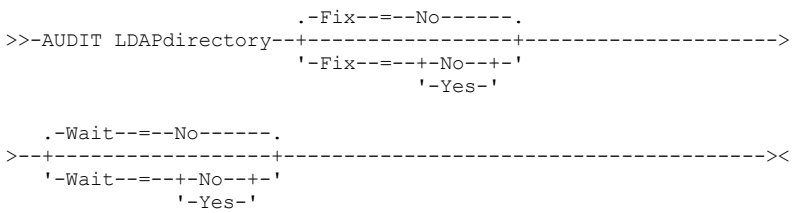
Verwenden Sie diesen Befehl, um einen durch IBM Spectrum Protect gesteuerten Namensbereich auf einem Lightweight Directory Access Protocol-Server (LDAP-Server) zu prüfen. Der LDAP-Server und der Namensbereich werden mithilfe einer oder mehrerer Optionen LDAPURL angegeben.

Einschränkung: Verwenden Sie diesen Befehl nur, wenn Sie die Kennwortauthentifizierung wie in Benutzer mithilfe eines LDAP-Servers authentifizieren beschrieben konfiguriert haben. Die zum Befehl AUDIT LDAPDIRECTORY bereitgestellten Informationen gelten nur für Umgebungen, in denen die Kennwortauthentifizierung wie in Benutzer mithilfe eines LDAP-Servers authentifizieren beschrieben konfiguriert ist. Knoten und Administrator-IDs, die ihre Kennwörter nicht mit dem LDAP-Verzeichnisserver authentifizieren, werden mit dem Befehl AUDIT LDAPDIRECTORY FIX=YES gelöscht. Knoten oder Administrator-IDs, die in der IBM Spectrum Protect-Datenbank nicht mehr vorhanden sind, werden ebenfalls gelöscht.
Stellen Sie vor der Ausgabe dieses Befehls sicher, dass die Option LDAPURL in der Datei dsmserv.opt angegeben ist. Weitere Informationen befinden sich unter Option LDAPURL. Wenn Sie mehrere Optionen LDAPURL in der Datei dsmserv.opt angegeben haben, werden die Optionen in der Reihenfolge ihrer Anordnung geprüft. Wird die Option LDAPURL nicht angegeben, schlägt der Befehl fehl.

Berechtigungsklasse

Für diesen Befehl sind Systemberechtigungen erforderlich.

Syntax



Parameter

Fix
: Dieser optionale Parameter gibt an, wie der IBM Spectrum Protect-Server Inkonsistenzen zwischen der Datenbank und dem externen Verzeichnis beseitigt. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

  No
  : Der Server meldet alle Inkonsistenzen zurück, aber ändert nicht das externe Verzeichnis.

  Yes
  : Der Server beseitigt alle Inkonsistenzen, die er beseitigen kann, und schlägt bei Bedarf weitere Aktionen vor.
  Wichtig: Sind LDAP-Einträge vorhanden, die mit anderen IBM Spectrum Protect-Servern gemeinsam genutzt werden, kann die Auswahl von YES zur Folge haben, dass diese Server nicht mehr synchron sind.

Wait
: Dieser optionale Parameter gibt an, ob darauf gewartet werden soll, dass der IBM Spectrum Protect-Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

  No
  : Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden.

  Yes
  : Der Server verarbeitet diesen Befehl im Vordergrund. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.
  Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

Beispiel: Ein LDAP-Verzeichnis prüfen und Inkonsistenzen beseitigen

Das LDAP-Verzeichnis prüfen, das in der Option LDAPURL angegeben wurde. Der IBM Spectrum Protect-Server beseitigt einige Inkonsistenzen.

```
audit ldapdirectory fix=yes


ANR2749W Administrator ADMIN1 wurde auf dem LDAP-Verzeichnisserver, aber nicht in
der Datenbank lokalisiert.
ANR2749W Administrator ADMIN2 wurde auf dem LDAP-Verzeichnisserver, aber nicht in
der Datenbank lokalisiert.
ANR2749W Administrator NODE1 wurde auf dem LDAP-Verzeichnisserver, aber nicht in
der Datenbank lokalisiert.
ANR2749W Administrator NODE2 wurde auf dem LDAP-Verzeichnisserver, aber nicht in
der Datenbank lokalisiert.
ANR2748W Knoten NODE1 wurde auf dem LDAP-Verzeichnisserver, aber nicht in der Datenbank
lokalisiert.
ANR2748W Knoten NODE2 wurde auf dem LDAP-Verzeichnisserver, aber nicht in der Datenbank
lokalisiert.
ANR2745I Befehl AUDIT LDAPDIRECTORY wurde beendet:
4 Administratoreinträge sind nur auf dem LDAP-Verzeichnisserver (nicht auf dem
IBM Spectrum Protect-Server),
0 Administratoreinträge sind nur auf dem IBM Spectrum Protect-Server (nicht auf dem
LDAP-Verzeichnisserver),
2 Knoteneinträge sind nur auf dem LDAP-Verzeichnisserver (nicht auf dem
IBM Spectrum Protect-Server),
0 Knoteneinträgesind nur auf dem IBM Spectrum Protect-Server (nicht auf dem
LDAP-Verzeichnisserver),
6 Einträge wurden insgesamt auf dem LDAP-Server gelöscht.
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für AUDIT LDAPDIRECTORY

Befehl	Beschreibung
SET DEFAULTAUTHENTICATION	Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an.
SET LDAPPASSWORD	Legt das Kennwort für den LDAPUSER fest.
SET LDAPUSER	Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht.

AUDIT LIBRARY (Datenträgerbestände in einem automatisierten Kassettenarchiv prüfen)

Mit diesem Befehl können Sie Datenträgerbestände in einem automatisierten Kassettenarchiv prüfen und synchronisieren.

Wird der Befehl AUDIT LIBRARY auf einem Kassettenarchivclient ausgegeben, synchronisiert der Client seinen Bestand mit dem Bestand auf dem Kassettenarchivmanager. Stellt der Kassettenarchivclient Inkonsistenzen fest, korrigiert er die Inkonsistenzen, indem er das Eigentumsrecht für den Datenträger auf dem Kassettenarchivmanager ändert.

Wird der Befehl AUDIT LIBRARY auf einem Server ausgegeben, auf dem das Kassettenarchiv ein SCSI-, 349X- oder ACSLS-Kassettenarchiv ist (LIBTYPE=SCSI, LIBTYPE=349X oder LIBTYPE=ACSLS), synchronisiert der Server seinen Bestand mit dem Bestand der Kassettenarchiveinheit. Stellt der Server Inkonsistenzen fest, löscht er fehlende Datenträger aus seinem Bestand.

- In SCSI-Kassettenarchiven aktualisiert der Server auch die Positionen der Datenträger in seinem Bestand, die seit der letzten Prüfung versetzt wurden.
- In 349X-Kassettenarchiven stellt der Server auch sicher, dass sich Arbeitsdatenträger in der Arbeitsdatenträgerkategorie und private Datenträger in der privaten Kategorie befinden.

Wird der Befehl AUDIT LIBRARY auf einem Server ausgegeben, der ein Kassettenarchivmanager für das Kassettenarchiv ist (SHARED=YES), aktualisiert der Server das Eigentumsrecht seiner Datenträger, wenn Inkonsistenzen festgestellt werden.

Unabhängig vom Servertyp oder Kassettenarchivtyp werden durch die Ausgabe des Befehls AUDIT LIBRARY nicht automatisch neue Datenträger zu einem Kassettenarchiv hinzugefügt. Um neue Datenträger hinzuzufügen, müssen Sie den Befehl CHECKIN LIBVOLUME verwenden.

Achtung: Die folgenden Vorsichtsmaßnahmen gelten nur für SCSI-, 349X- und ACSLS-Kassettenarchive (LIBTYPE=SCSI, LIBTYPE=349X und LIBTYPE=ACSLS):

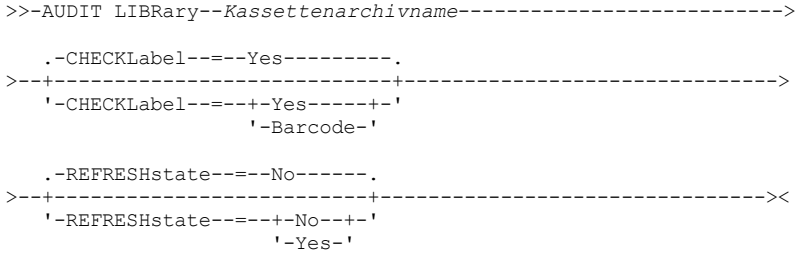
- Die Ausführung des Befehls AUDIT LIBRARY verhindert jede andere Kassettenarchivaktivität, bis die Prüfung abgeschlossen ist. Der Server verarbeitet beispielsweise keine Zurückschreibungs- oder Abrufanforderungen, die das Kassettenarchiv betreffen, wenn der Befehl AUDIT LIBRARY ausgeführt wird.
- Finden andere Aktivitäten in dem Kassettenarchiv statt, geben Sie den Befehl AUDIT LIBRARY nicht aus. Wird der Befehl AUDIT LIBRARY ausgegeben, wenn ein Kassettenarchiv aktiv ist, können unvorhersehbare Ergebnisse auftreten (beispielsweise eine Blockierung), wenn ein Prozess, der gegenwärtig auf das Kassettenarchiv zugreift, das Laden eines neuen Bands anfordert.

Dieser Befehl erstellt einen Hintergrundprozess, den Sie mit dem Befehl CANCEL PROCESS abbrechen können. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax



Parameter

Speicherarchivname (Erforderlich)
Gibt den Namen des Kassettenarchivs an, das geprüft werden soll.

CHECKLabel
Gibt an, wie der Kennsatz des Speicherdatenträgers während des Prüfvorgangs überprüft wird. Dieser Parameter gilt nur für SCSI-Kassettenarchive. Der Parameter wird für andere Kassettenarchivtypen ignoriert. Der Standardwert ist YES. Gültige Werte:

Yes
Gibt an, dass der Server jeden Datenträgerkennsatz überprüft, um die Identität des Datenträgers zu prüfen.

Barcode
Gibt an, dass der Server den Balkencodeleser zum Lesen des Speicherkennsatzes verwendet. Mit Hilfe des Balkencodes kann die Zeit für die Prüfverarbeitung reduziert werden. Dieser Parameter gilt nur für SCSI-Kassettenarchive.
Achtung: Kann der Scanner den Balkencodekennsatz nicht lesen oder fehlt der Balkencodekennsatz, lädt der Server dieses Band in ein Laufwerk, um den Kennsatz zu lesen.

REFRESHstate
Gibt an, ob die Informationen des Servers zu einem Kassettenarchiv, die normalerweise während der Initialisierung angefordert werden, aktualisiert werden, damit alle Änderungen an der Konfiguration widergespiegelt werden. Wird der Parameter REFRESHSTATE auf YES gesetzt, wird diese Aktion ausgeführt, ohne dass der Server erneut gestartet oder das Kassettenarchiv erneut definiert werden muss. Der Standardwert ist 'No'. Gültige Werte sind:

No
Gibt an, dass der Server den Status des Kassettenarchivs nicht aktualisiert, wenn das Kassettenarchiv geprüft wird.

Yes
Gibt an, dass der Server den Status des Kassettenarchivs aktualisiert, wenn der Befehl AUDIT LIBRARY ausgegeben wird.

Beispiel: Ein automatisiertes Kassettenarchiv prüfen

Das automatisierte Kassettenarchiv EZLIFE prüfen.

```
audit library ezlife
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für AUDIT LIBRARY

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DELETE LIBRARY	Löscht ein Kassettenarchiv.
DISMOUNT VOLUME	Entlädt einen sequenziellen entfernbaren Datenträger anhand des Datenträgernamens.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY LIBVOLUME	Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
UPDATE LIBRARY	Ändert die Attribute eines Kassettenarchivs.

AUDIT LIBVOLUME (Datenbankinformationen für einen Banddatenträger prüfen)

Verwenden Sie diesen Befehl, um zu bestimmen, ob ein Banddatenträger unbeschädigt ist, und um Daten auf einem Banddatenträger zu prüfen.

Sie können den Befehl AUDIT LIBVOLUME für jeden Banddatenträger ausgeben, der in ein Speicherarchiv zurückgestellt wurde. Der Befehl wird standardmäßig im Hintergrund ausgeführt. Sie können den Befehl für die folgenden Speicherarchivtypen ausgeben, die über ein Bandlaufwerk IBM® TS1140, IBM LTO 5 oder ein Bandlaufwerk einer späteren Generation verfügen:

- SCSI-Bandarchiv
- Virtuelles Bandarchiv (VTL = Virtual Tape Library)

Die folgende Tabelle enthält die Bandlaufwerke, die Banddatenträger mit den Datenträgertypen für IBM TS1140- und IBM LTO 5-Bandlaufwerke und LTO-Bandlaufwerke einer höheren Generation prüfen können:

Tabelle 1. Bandlaufwerke und Datenträgertypen

Laufwerk	Datenträgertyp
TS1140	JB, JX, JA, JW, JJ, JR, JC, JY und JK
IBM LTO 5	LTO 3, LTO 4 und LTO 5
IBM LTO 6	LTO 4, LTO 5 und LTO 6

Laufwerk	Datenträgertyp
IBM LTO 7	LTO 5, LTO 6 und LTO 7

Die folgende Tabelle zeigt die Mindestversion des Einheitentreibers, die für die Ausführung des Befehls erforderlich ist:

Tabelle 2. Mindestversion des IBM Einheitentreibers

Treibername	Einheitentreiberversion
Atape-Treiber unter AIX	12.3.5.00
lin_tape-Treiber unter Linux	1.6.7.00
IBM Bandtreiber unter Windows	6.2.2.00

Einschränkung: Sie können den Befehl CANCEL PROCESS nicht ausgeben, während der Befehl AUDIT LIBVOLUME ausgeführt wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung oder die uneingeschränkte Speicherberechtigung für das Speicherarchiv erforderlich, für das der Banddatenträger definiert ist.

Syntax

```
>>-AUDit LIBVolume--Speicherarchivname--Datenträgername--------->

   .-Wait--=--No------.
>--+------------------+---------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Speicherarchivs an, in dem sich der Banddatenträger befindet, der geprüft werden soll.

Datenträgername (Erforderlich)
: Gibt den Namen des physischen Banddatenträgers an, der geprüft werden soll.

Wait (Optional)
: Gibt an, ob die Prüfoperation im Vordergrund oder im Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Folgende Optionen sind verfügbar:

  No
  : Gibt an, dass die Operation im Hintergrund ausgeführt wird. Der Wert NO ist der Standardwert.

  Yes
  : Gibt an, dass die Operation im Vordergrund ausgeführt wird. Die Ausführung der Operation nimmt unter Umständen viel Zeit in Anspruch.

Beispiel: Einen Banddatenträger prüfen

Das Speicherarchiv EZLIFE prüfen, das einen Banddatenträger mit dem Namen KM0347L5 enthält.

```
audit libvolume ezlife KM0347L5
```

AUDIT LICENSES (Serverspeicherbelegung prüfen)

Mit diesem Befehl können der Serverspeicher, der von den Clientknoten verwendet wird, und die Serverlizenzen geprüft werden. Der Prüfvorgang bestimmt, ob die aktuelle Konfiguration die Lizenzbedingungen erfüllt.

Ein Prüfvorgang erstellt einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wird der Server angehalten und erneut gestartet, wird ein Prüfvorgang automatisch wie durch den Befehl SET LICENSEAUDITPERIOD angegeben ausgeführt. Zum Anzeigen der Prüfergebnisse den Befehl QUERY LICENSE verwenden.

Achtung: Die Prüfung des Server-Speichers kann viel CPU-Zeit in Anspruch nehmen. Mit der Server-Option AUDITSTORAGE kann angegeben werden, daß der Speicher nicht geprüft werden soll.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-AUDit LICenses-----------------------------------------><
```

Parameter

Keine.

Beispiel: Serverlizenzen prüfen

Den Befehl AUDIT LICENSES ausgeben.

```
audit licenses
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für AUDIT LICENSES

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY AUDITOCCUPANCY	Zeigt die Serverspeicherauslastung für einen Clientknoten an.
QUERY LICENSE	Zeigt Informationen über Lizenzen und Prüfvorgänge an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER LICENSE	Registriert eine Lizenz für den IBM Spectrum Protect-Server.
SET LICENSEAUDITPERIOD	Gibt die Anzahl Tage zwischen den automatischen Lizenzprüfungen an.

AUDIT VOLUME (Datenbankinformationen für Speicherpooldatenträger prüfen)

Mit diesem Befehl können Inkonsistenzen zwischen Datenbankinformationen und einem Datenträger aus dem Speicherpool festgestellt werden. Verarbeitungsinformationen, die während einer Prüfung generiert werden, werden an das Aktivitätenprotokoll und die Serverkonsole gesendet.

Einschränkung: Sie können diesen Befehl nicht für Datenträger verwenden, die Containerkopienspeicherpools zugeordnet sind.
Sie können nur Datenträger prüfen, die zu Speicherpools mit DATAFORMAT=NATIVE und DATAFORMAT=NONBLOCK gehören.

Ein Datenträger kann nicht geprüft werden, wenn er gerade aus einem primären Pool oder einem Kopienspeicherpool gelöscht wird.

Wenn eine Prüfverarbeitung aktiv ist, können Clients keine Daten von dem angegebenen Datenträger zurückschreiben oder neue Daten auf dem Datenträger speichern.

Wird von dem Server eine Datei mit Fehlern erkannt, hängt die Bearbeitung der Datei von dem Typ des Speicherpools ab, zu dem der Datenträger gehört, ob die Option FIX in diesem Befehl angegeben wurde und ob die Datei auch auf einem Datenträger gespeichert ist, der anderen Pools zugeordnet ist.

Wenn IBM Spectrum Protect keine Fehler für eine Datei feststellt, die als beschädigt markiert war, wird der Status der Datei zurückgesetzt, so dass die Datei verwendet werden kann.

Der Server löscht keine Archivierungsdateien, für die das Löschen unzulässig ist. Ist der Aufbewahrungsschutz für Archivierung aktiviert, löscht der Server keine Archivierungsdateien, deren Aufbewahrungszeitraum nicht abgelaufen ist.

Um Informationen über den Inhalt eines Datenträgers aus dem Speicherpool anzuzeigen, den Befehl QUERY CONTENT verwenden.

Sollen mehrere Datenträger geprüft werden, können Sie die Parameter FROMDATE und TODATE verwenden. Sollen alle Datenträger in einem Speicherpool geprüft werden, verwenden Sie den Parameter STGPOOL. Wenn Sie die Parameter FROMDATE und/oder TODATE verwenden, beschränkt der Server die Prüfung auf die Datenträger mit sequenziellem Zugriff, die die Datumskriterien erfüllen, und schließt automatisch alle angehängten Plattendatenträger im Speicher ein. Um die Anzahl der Datenträger, die Plattendatenträger einschließen können, zu begrenzen, verwenden Sie die Parameter FROMDATE, TODATE und STGPOOL.

Wird ein Server mit aktiviertem Aufbewahrungsschutz für Archivierung ausgeführt und sind Daten in Speicherpools gespeichert, die mit dem Parameter RECLAMATIONTYPE=SNAPLOCK definiert sind, sollte das Datum des letzten Zugriffs auf dem NetApp SnapLock-Dateiserver für einen Datenträger mit dem Enddatum der Wiederherstellungsperiode übereinstimmen, das angezeigt wird, wenn Sie einen Befehl QUERY VOLUME F=D für diesen Datenträger ausgeben. Bei der AUDIT VOLUME-Verarbeitung werden diese Daten verglichen. Stimmen sie nicht überein und wird der Befehl AUDIT VOLUME mit dem Parameter FIX=NO ausgeführt, wird eine Nachricht ausgegeben, in der angegeben ist, dass der Befehl mit dem Parameter FIX=YES ausgeführt werden muss, um die Inkonsistenz zu beseitigen. Stimmen die Daten nicht überein und wird der Befehl AUDIT VOLUME mit dem Parameter FIX=YES ausgeführt, werden die Inkonsistenzen beseitigt.

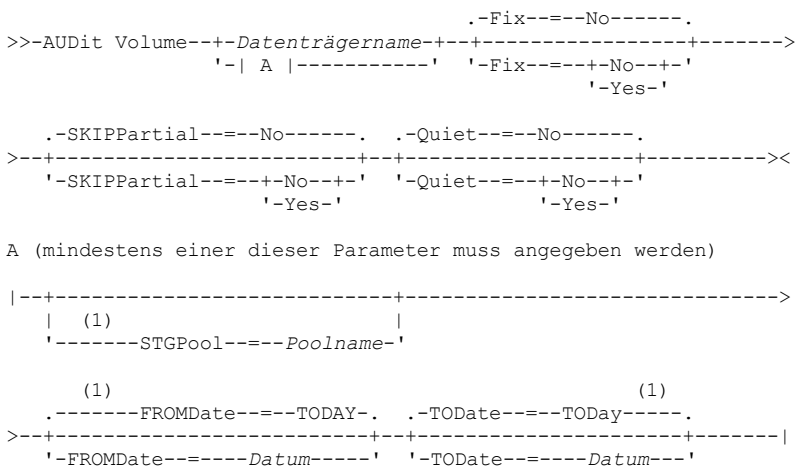
Achtung: Verwenden Sie den Parameter FIX=Yes nur, wenn die Infrastruktur für Ihr Bandlaufwerk und Speicherbereichsnetz (SAN) stabil ist. Stellen Sie sicher, dass die Bandköpfe sauber sind und die Bandeinheitentreiber stabil und zuverlässig sind. Andernfalls besteht die Möglichkeit, dass fehlerfreie Daten gelöscht werden, wenn dieser Parameter verwendet wird. Der Server kann nicht feststellen, ob ein Band physisch beschädigt oder eine Bandspeicherinfrastruktur instabil ist.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich, in dem der Datenträger definiert ist.

Syntax



Anmerkungen:

1. Sie können keinen Datenträgernamen angeben, wenn Sie einen Speicherpoolnamen, FROMDATE oder TODATE angeben.

Parameter

Datenträgername
: Gibt den Namen des Datenträgers aus dem Speicherpool an, der geprüft werden soll. Dieser Parameter ist erforderlich, wenn Sie keinen Speicherpool angeben. Sie können einen Datenträgernamen nicht zusammen mit den Parametern FROMDATE und TODATE angeben.

Fix
: Gibt an, wie der Server Inkonsistenzen zwischen dem Datenträgerbestand und dem angegebenen Datenträger aus dem Speicherpool beseitigt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

  Die Aktionen, die der Server ausführt, sind davon abhängig, ob der Datenträger einem primären Pool oder einem Kopienspeicherpool zugeordnet ist.

  Primärer Speicherpool:

  Anmerkung: Wenn der Befehl AUDIT VOLUME keinen Fehler in einer Datei feststellt, die zuvor als beschädigt markiert war, setzt IBM Spectrum Protect den Status der Datei zurück, so dass sie verwendet werden kann. Auf diese Weise kann der Status beschädigter Dateien zurückgesetzt werden, wenn festgestellt wird, dass die Fehler durch einen korrigierbaren Hardwarefehler, wie z. B. einen verschmutzten Bandkopf, verursacht wurden.

  Fix=No
  : IBM Spectrum Protect listet Datenbanksätze auf, die sich auf Dateien mit Inkonsistenzen beziehen; die Sätze werden jedoch nicht gelöscht.

    - IBM Spectrum Protect markiert die Datei in der Datenbank als beschädigt. Wenn eine Sicherungskopie in einem Kopienspeicherpool gespeichert ist, kann die Datei mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL zurückgeschrieben werden.
    - Handelt es sich bei der Datei um eine Cache-Kopie, müssen Verweise auf die Datei auf diesem Datenträger mit Hilfe des Befehls AUDIT VOLUME und durch die Angabe von FIX=YES gelöscht werden. Wenn die physische Datei keine Cachekopie ist und eine Kopie in einem Kopienspeicherpool gespeichert ist, kann die Datei mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL zurückgeschrieben werden.

  Fix=Yes

Der Server beseitigt alle festgestellten Inkonsistenzen:

- Wenn die physische Datei eine Cache-Kopie ist, löscht der Server die Datenbanksätze, die auf die Cache-Datei verweisen. Die Primärdatei wird auf einem anderen Datenträger gespeichert.
- Wenn die physische Datei keine Cache-Kopie ist und die Datei außerdem in mindestens einem Kopienspeicherpool gespeichert ist, wird der Fehler gemeldet und die physische Datei in der Datenbank als beschädigt markiert. Die physische Datei kann mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL zurückgeschrieben werden.
- Wenn die physische Datei keine Cache-Kopie und nicht in einem Kopienspeicherpool gespeichert ist, werden alle logischen Dateien, bei denen Inkonsistenzen festgestellt werden, aus der Datenbank gelöscht.
- Wird der Aufbewahrungsschutz für Archivierung mit dem Befehl SET ARCHIVERETENTIONPROTECTION aktiviert, kann bei Bedarf eine zwischengespeicherte Kopie von Daten gelöscht werden. Daten in primären Speicherpools und Kopienspeicherpools können nur als beschädigt gekennzeichnet und nie gelöscht werden.

Der Befehl AUDIT VOLUME darf nicht mit FIX=YES verwendet werden, wenn ein Zurückschreibungsprozess (RESTORE STGPOOL oder RESTORE VOLUME) aktiv ist. Durch den Befehl AUDIT VOLUME könnte die Zurückschreibung unvollständig sein.

Kopienspeicherpool:

Fix=No
: Der Server meldet den Fehler und markiert die Kopie der physischen Datei in der Datenbank als beschädigt.

Fix=Yes
: Der Server löscht alle Verweise auf die physische Datei und alle Datenbanksätze, die auf eine nicht vorhandene physische Datei zeigen.

SKIPPartial
: Gibt an, ob IBM Spectrum Protect partielle Dateien ignoriert; hierbei handelt es sich um Dateien, die sich über mehrere Speicherpooldatenträger erstrecken. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Bei der Ausführung einer Prüfoperation für einen Datenträger mit sequenziellem Zugriff verhindert dieser Parameter zusätzliche Ladevorgänge für Datenträger mit sequenziellem Zugriff, die für die Prüfung partieller Dateien eventuell erforderlich sind. Gültige Werte:

  No
  : IBM Spectrum Protect prüft Dateien, die sich über mehrere Datenträger erstrecken.
  Wenn Sie nicht SKIPPARTIAL=YES angeben, versucht IBM Spectrum Protect, alle auf dem Datenträger gespeicherten Dateien, einschließlich der Dateien, die sich über andere Datenträger erstrecken, zu verarbeiten. Um Dateien zu prüfen, die sich über mehrere Datenträger erstrecken, müssen die folgenden Bedingungen erfüllt sein:

  - Bei Datenträgern mit sequentiellem Zugriff müssen die zusätzlichen Datenträger mit sequentiellem Zugriff über den Zugriffsmodus Lesen/Schreiben oder Lesezugriff verfügen.
  - Bei Datenträgern mit wahlfreiem Zugriff müssen die zusätzlichen Datenträger online sein.

  Yes
  : IBM Spectrum Protect prüft nur Dateien, die auf dem Datenträger gespeichert sind, der geprüft werden soll. Der Status aller partiellen Dateien ist unbekannt.

Quiet
: Gibt an, ob IBM Spectrum Protect detaillierte Informationsnachrichten für nicht abrufbare Dateien auf dem Datenträger an das Aktivitätenprotokoll und die Server-Konsole sendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, daß IBM Spectrum Protect detaillierte Informationsnachrichten und einen Ergebnisbericht sendet. Jede Nachricht enthält den Knotennamen, den Dateibereichsnamen und den Client-Namen für die Datei.

  Yes
  : Gibt an, daß IBM Spectrum Protect nur einen Ergebnisbericht sendet.

FROMDate
: Gibt das Anfangsdatum des Bereichs an, für den Datenträger geprüft werden sollen. Standardwert ist das aktuelle Datum. Alle Datenträger mit sequenziellem Zugriff, die die Zeitbereichskriterien erfüllen und nach diesem Datum beschrieben wurden, werden geprüft. Der Server schließt alle angehängten Plattendatenträger im Speicher ein. Der Server startet einen Prüfprozess für jeden Datenträger und führt die Prozesse fortlaufend aus. Sie können diesen Parameter nicht verwenden, wenn Sie einen Datenträger angegeben haben. Dieser Parameter ist wahlfrei. Um die Anzahl der Datenträger, die Plattendatenträger einschließen können, zu begrenzen, verwenden Sie die Parameter FROMDATE, TODATE und STGPOOL.
  Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	10/15/2001 Wird ein Datum eingegeben, werden alle in Frage kommenden Datenträger, die an diesem Tag beschrieben wurden (ab 00:00:01), ausgewertet.
TODAY	Das aktuelle Datum	TODAY

Wert	Beschreibung	Beispiel
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–7 *oder* –7. Sollen Informationen beginnend mit den Datenträgern angezeigt werden, die vor einer Woche beschrieben wurden, können Sie FROMDATE=TODAY-7 oder FROMDATE= -7 angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

TODate

Gibt das Enddatum des Bereichs an, für den Datenträger geprüft werden sollen. Alle Datenträger mit sequenziellem Zugriff, die die Zeitbereichskriterien erfüllen und vor diesem Datum beschrieben wurden, werden geprüft. Der Server schließt alle angehängten Plattendatenträger im Speicher ein. Wird kein Wert angegeben, verwendet der Server standardmäßig das aktuelle Datum. Sie können diesen Parameter nicht verwenden, wenn Sie einen Datenträger angegeben haben. Dieser Parameter ist wahlfrei. Um die Anzahl der Datenträger, die Plattendatenträger einschließen können, zu begrenzen, verwenden Sie die Parameter FROMDATE, TODATE und STGPOOL. Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	10/15/2001 Wird ein Datum eingegeben, werden alle in Frage kommenden Datenträger, die an diesem Tag beschrieben wurden (bis 23:59:59), ausgewertet.
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–1 **oder** –1. Sollen Informationen angezeigt werden, die bis gestern erstellt wurden, können Sie TODATE=TODAY-1 oder einfach TODATE= -1 angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

STGPool

Dieser Parameter gibt an, dass der Server nur die Datenträger aus dem angegebenen Speicherpool prüft. Dieser Parameter ist wahlfrei. Sie können diesen Parameter nicht verwenden, wenn Sie einen Datenträger angegeben haben.

Beispiel: Datenbankinformationen für einen bestimmten Speicherpooldatenträger prüfen

Überprüfen, ob die Datenbankinformationen für den Datenträger aus dem Speicherpool PROG2 konsistent mit den auf dem Datenträger gespeicherten Daten sind. IBM Spectrum Protect berichtigt alle Inkonsistenzen.

```
audit volume prog2 fix=yes
```

Beispiel: Datenbankinformationen für alle Datenträger prüfen, die während eines bestimmten Datumsbereichs beschrieben wurden

Überprüfen, ob die Datenbankinformationen für alle auswählbaren Datenträger, die vom 3/20/2002 bis zum 3/22/2002 beschrieben wurden, mit den auf dem Datenträger gespeicherten Daten konsistent sind.

```
audit volume fromdate=03/20/2002 todate=03/22/2002
```

Beispiel: Datenbankinformationen für alle Datenträger in einem bestimmten Speicherpool prüfen

Überprüfen, ob die Datenbankinformationen für alle Datenträger in Speicherpool STPOOL3 mit den auf dem Datenträger gespeicherten Daten für den aktuellen Tag konsistent sind.

```
audit volume stgpool=STPOOL3
```

Beispiel: Datenbankinformationen für alle Datenträger in einem bestimmten Speicherpool prüfen, die in den letzten beiden Tagen beschrieben wurden

Überprüfen, ob die Datenbankinformationen für alle Datenträger in Speicherpool STPOOL3 mit den auf dem Datenträger gespeicherten Daten für die letzten beiden Tage konsistent sind.

```
audit volume stgpool=STPOOL3 fromdate=-1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für AUDIT VOLUME

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY CONTENT	Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY VOLUME	Zeigt Informationen über Speicherpooldatenträger an.
SET ARCHIVERETENTIONPROTECTION	Gibt an, ob der Aufbewahrungsschutz für Daten aktiviert ist.

BACKUP-Befehle

Mit den BACKUP-Befehlen können Sicherungskopien der IBM Spectrum Protect-Informationen oder -Objekte erstellt werden.

- BACKUP DB (Datenbank sichern)
- BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)
- BACKUP NODE (NAS-Knoten sichern)
- BACKUP STGPOOL (Daten eines primären Speicherpools in einem Kopienspeicherpool sichern)
- BACKUP VOLHISTORY (Protokolldaten sequenzieller Datenträger speichern)

BACKUP DB (Datenbank sichern)

Mit diesem Befehl kann eine IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff gesichert werden.

Achtung: Um eine Datenbank zurückzuschreiben, muss der Server Informationen aus der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei verwenden. Sie müssen Kopien der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei erstellen und speichern. Diese Dateien können nicht erneut erstellt werden.

Um zu bestimmen, wieviel zusätzlichen Speicherbereich eine Sicherung erfordert, geben Sie den Befehl QUERY DB aus.

Einschränkungen: Sie können eine Serverdatenbank nicht zurückschreiben, wenn der Release-Level der Serverdatenbanksicherung von dem Release-Level des Servers abweicht, der zurückgeschrieben wird. Beispielsweise tritt ein Fehler auf, wenn Sie eine Datenbank der Version 6.3 zurückschreiben und Sie einen Server der Version 7.1 verwenden.
Nach der Beendigung der Datenbanksicherung sichert der IBM Spectrum Protect-Server Informationen auf der Basis der Optionen, die in der Serveroptionsdatei angegeben sind. Die folgenden Informationen werden gesichert:

- Protokolldaten sequenzieller Datenträger für alle Dateien, die mit der Option VOLUMEHISTORY angegeben sind
- Informationen zur Einheitenkonfiguration für alle Dateien, die mit der Option DEVCONFIG angegeben sind
- Masterverschlüsselungsschlüssel des Servers

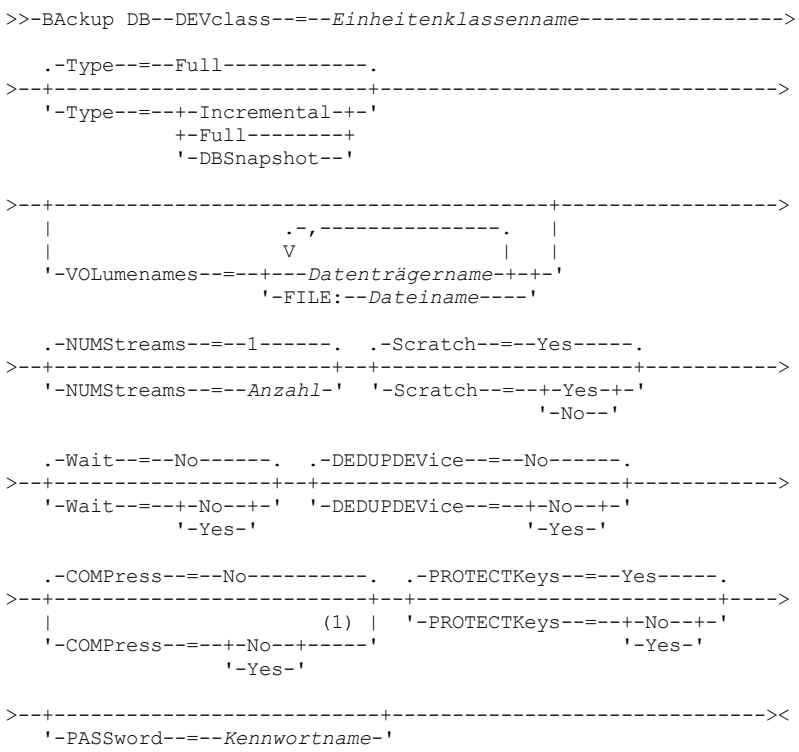
Wenn auf dem Datenträger oder in dem Dateibereich mit dem definierten Verzeichnis für aktive Protokolldateien nicht genügend Speicherbereich verfügbar ist, können Sie die DB2-Option *overflowlogpath* definieren, um ein Verzeichnis mit dem erforderlichen verfügbaren Speicherbereich zu verwenden. Geben Sie beispielsweise den folgenden Befehl aus, um das Verzeichnis /home/tsminst2/overflow_dir zu verwenden:

```
db2 update db cfg for TSMDB1 using overflowlogpath /home/tsminst2/overflow_dir
```

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax



Anmerkungen:

1. Der Standardwert des Parameters COMPRESS ist situationsabhängig. Wird der Parameter COMPRESS im Befehl BACKUP DB angegeben, überschreibt er den Wert des Parameters COMPRESS, der im Befehl SET DBRECOVERY definiert ist. Andernfalls ist der im Befehl SET DBRECOVERY definierte Wert der Standardwert.

Parameter

DEVclass (Erforderlich)
: Gibt den Namen der Einheitenklasse für den sequenziellen Zugriff an, der für die Sicherung verwendet werden soll. Geben Sie den Befehl BACKUP DB aus und handelt es sich bei der Einheitenklasse nicht um die in dem Befehl SET DBRECOVERY angegebene Einheitenklasse, wird eine Warnung ausgegeben. Die Sicherungsoperation wird jedoch fortgesetzt und ist nicht betroffen.

  Wird der Befehl SET DBRECOVERY nicht ausgegeben, um eine Einheitenklasse zu definieren, schlägt der Befehl BACKUP DB fehl.

  Einschränkung:

  - Sie können keine Einheitenklasse mit dem Einheitentyp NAS oder CENTERA verwenden.
  - Eine Operation zum Zurückschreiben einer Datenbank schlägt fehl, wenn die Quelle der Zurückschreibung ein Kassettenarchiv des Typs FILE ist. Ein Kassettenarchiv des Typs FILE wird erstellt, wenn in der Einheitenklasse FILE "SHARED=YES" angegeben ist.

  Sind alle Laufwerke für diese Einheitenklasse während der Ausführung der Sicherung aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, wie beispielsweise Wiederherstellungsoperationen, um ein Laufwerk für die Sicherung verfügbar zu machen.

Type
: Gibt die gewünschte Art der Sicherung an. Dieser Parameter ist wahlfrei. Der Standardwert ist FULL. Die folgenden Werte sind gültig:

  Full
  : Gibt an, dass eine Gesamtsicherung der IBM Spectrum Protect-Datenbank ausgeführt werden soll.

Incremental
: Gibt an, dass eine Teilsicherung der IBM Spectrum Protect-Datenbank ausgeführt werden soll. Ein Teilsicherungsimage (oder kumulatives Sicherungsimage) enthält eine Kopie aller Datenbankdaten, die sich seit der letzten erfolgreichen Gesamtsicherungsoperation geändert haben.

DBSnapshot
: Gibt an, dass eine vollständige Datenbankmomentaufnahmesicherung ausgeführt werden soll. Der gesamte Inhalt einer Datenbank wird kopiert und eine neue Datenbankmomentaufnahmesicherung wird erstellt, ohne dass die vorhandene Gesamtsicherungsserie und Teilsicherungsserie der Datenbank unterbrochen wird.

VOLumenames

Gibt die Datenträger an, die zur Sicherung der Datenbank verwendet werden. Dieser Parameter ist wahlfrei. Wird jedoch SCRATCH=NO angegeben, muß eine Datenträgerliste angegeben werden.

Datenträgername
: Gibt die Datenträger an, die zur Sicherung der Datenbank verwendet werden. Mehrere Datenträger angeben, indem die Namen durch Kommas und ohne Leerzeichen voneinander getrennt werden.

FILE:Dateiname
: Gibt den Namen einer Datei an, die eine Liste der Datenträger enthält, die zur Sicherung der Datenbank verwendet werden. Jeder Datenträgername muss sich auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.
Um beispielsweise die Datenträger DB0001, DB0002 und DB0003 zu verwenden, erstellen Sie eine Datei, die diese Zeilen enthält:

```
DB0001
DB0002
DB0003
```

Geben Sie der Datei den entsprechenden Namen. Beispiel:

- AIX-BetriebssystemeLinux-BetriebssystemeTAPEVOL
- Windows-BetriebssystemeTAPEVOL.DATA

Dann können die Datenträger für den Befehl wie folgt angegeben werden:

AIX-BetriebssystemeLinux-Betriebssysteme

```
VOLUMENAMES=FILE:TAPEVOL
```

Windows-Betriebssysteme

```
VOLUMENAMES=FILE:TAPEVOL.DATA
```

NUMStreams
: Gibt die Anzahl der parallelen Datenversetzungsdatenströme an, die beim Sichern der Datenbank verwendet werden sollen. Der Mindestwert ist 1 und der Maximalwert ist 32. Die Erhöhung des Werts hat eine entsprechende Erhöhung der Anzahl der zu verwendenden Datenbanksicherungssitzungen und der Anzahl von Laufwerken zur Folge, die für die Einheitenklasse verwendet werden müssen. Wird ein Wert für NUMSTREAMS im Befehl BACKUP DB angegeben, überschreibt er den Wert, der in dem Befehl SET DBRECOVERY definiert ist. Andernfalls wird der im Befehl SET DBRECOVERY definierte Wert verwendet. Der Wert für NUMSTREAMS wird für alle Typen der Datenbanksicherung verwendet.
Wird ein Wert angegeben, der größer als die Anzahl der für die Einheitenklasse verfügbaren Laufwerke ist, wird nur die Anzahl der verfügbaren Laufwerke verwendet. Die verfügbaren Laufwerke sind die Laufwerke, die für die Einheitenklasse durch den Parameter MOUNTLIMIT oder durch die Anzahl der Onlinelaufwerke für die angegebene Einheitenklasse definiert sind. Die Sitzung wird in der Ausgabe von QUERY SESSION angezeigt.
Wenn Sie die Anzahl der Datenströme erhöhen, werden mehr Datenträger aus der entsprechenden Einheitenklasse für diese Operation verwendet. Mit einer größeren Anzahl von Datenträgern kann die Geschwindigkeit von Datenbanksicherungen erhöht werden, jedoch auf Kosten einer größeren Anzahl von Datenträgern, die nicht vollständig belegt sind.

Scratch
: Gibt an, ob Arbeitsdatenträger für die Sicherung verwendet werden können. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Die folgenden Werte sind gültig:

  Yes
  : Gibt an, dass Arbeitsdatenträger verwendet werden können.

    Werden SCRATCH=YES und der Parameter VOLUMENAMES angegeben, werden Arbeitsdatenträger von IBM Spectrum Protect nur verwendet, wenn auf den angegebenen Datenträgern kein Speicherbereich verfügbar ist.

    Wird keine Datenträgerliste durch Verwendung des Parameters VOLUMENAMES angegeben, muss entweder SCRATCH=YES angegeben oder der Standardwert verwendet werden.

  No
  : Gibt an, dass Arbeitsdatenträger nicht verwendet werden können.

    Werden Datenträger durch Verwendung des Parameters VOLUMENAMES und SCRATCH=NO angegeben, schlägt die Sicherung fehl, wenn für die Speicherung der Sicherungsdaten auf den angegebenen Datenträgern nicht genügend Speicherbereich zur Verfügung

steht.

Wait
Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist NO. Die folgenden Werte sind gültig:

No
Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wenn ein BACKUP DB-Hintergrundprozess abgebrochen wird, wurde ein Teil der Datenbank vor dem Abbruch eventuell bereits gesichert.

Yes
Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Erst nachdem der Befehl vollständig ausgeführt wurde, kann mit anderen Aufgaben fortgefahren werden. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist.
Einschränkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

DEDUPDEVice
Gibt an, dass eine Zielspeichereinheit die Datendeduplizierung unterstützt. Bei Angabe von YES wird das Format von Sicherungsimages für Datendeduplizierungseinheiten optimiert. Dadurch werden Sicherungsoperationen effizienter ausgeführt. Die folgenden Werte sind gültig:

No
Gibt an, dass eine Zielspeichereinheit die Datendeduplizierung nicht unterstützt. NO ist der Standardwert.
Stellen Sie sicher, dass dieser Parameter für die folgenden Einheiten auf NO gesetzt wird:

- SCSI-Kassettenarchive
- Alle Einheiten, die mit der Einheitenklasse FILE definiert werden
- Virtuelle Bandarchive (VTL, Virtual Tape Library), die die Funktion der Datendeduplizierung nicht unterstützen

Yes

Gibt an, dass eine Zieleinheit die Datendeduplizierung unterstützt und Sicherungen für diese Funktion optimiert werden sollen. Sie können diesen Parameter auf YES setzen, wenn Sie virtuelle Bandarchive (VTL, Virtual Tape Library) verwenden, die die Datendeduplizierung unterstützen.

COMPress
Gibt an, ob Datenträger, die mit dem Befehl BACKUP DB erstellt werden, komprimiert werden. Der Wert für COMPRESS wird für alle Typen der Datenbanksicherungen verwendet. Dieser Parameter ist wahlfrei. Der Standardwert ist situationsabhängig. Wird der Parameter COMPRESS im Befehl BACKUP DB angegeben, überschreibt er den Wert, der im Befehl SET DBRECOVERY definiert ist. Andernfalls ist der im Befehl SET DBRECOVERY definierte Wert der Standardwert. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass die Datenträger, die mit dem Befehl BACKUP DB erstellt werden, nicht komprimiert werden.
Yes

Gibt an, dass die Datenträger, die mit dem Befehl BACKUP DB erstellt werden, komprimiert werden.

Einschränkungen:

- Gehen Sie mit Vorsicht vor, wenn Sie den Parameter COMPRESS angeben. Bei Verwendung der Komprimierung während Datenbanksicherungen kann die Größe der Sicherungsdateien verringert werden. Die Komprimierung kann jedoch die Zeit verlängern, die für die Ausführung der Datenbanksicherungsverarbeitung erforderlich ist.
- Sichern Sie keine komprimierten Daten auf Band. Wenn in Ihrer Systemumgebung Datenbanksicherungen auf Band gespeichert werden, setzen Sie den Parameter COMPRESS in den Befehlen SET DBRECOVERY und BACKUP DB auf No.




PROTECTKeys



Gibt an, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels des Servers enthalten, der zum Verschlüsseln von Speicherpooldaten verwendet wird. Dieser Parameter ist optional. Der Standardwert ist der für den Parameter PROTECTKEYS im Befehl SET DBRECOVERY angegebene Wert. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass Datenbanksicherungen keine Kopie des Masterverschlüsselungsschlüssels des Servers enthalten.
Achtung: Wenn Sie PROTECTKEYS=NO angeben, müssen Sie den Masterverschlüsselungsschlüssel für den Server manuell sichern und den Schlüssel verfügbar machen, wenn Sie die Wiederherstellung nach einem Katastrophenfall (Disaster Recovery) implementieren.
Yes
Gibt an, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels des Servers enthalten.

Achtung: Wenn Sie PROTECTKEYS=YES angeben, müssen Sie auch den Parameter PASSWORD angeben.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemePASSword
AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeGibt das Kennwort an, das zum Schützen der Datenbanksicherung verwendet wird. Der Standardwert ist der für den Parameter PASSWORD im Befehl SET DBRECOVERY angegebene Wert.
Wichtig: Sie müssen sich dieses Kennwort merken. Wenn Sie ein Kennwort für Datenbanksicherungen angeben, müssen Sie dasselbe Kennwort im Befehl RESTORE DB zum Zurückschreiben der Datenbank angeben.

Beispiel: Eine Teilsicherung unter Verwendung eines Arbeitsdatenträgers ausführen

Eine Teilsicherung der Datenbank unter Verwendung eines Arbeitsdatenträgers ausführen. Eine Einheitenklasse FILE für die Sicherung verwenden.

```
backup db devclass=file type=incremental
```

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Beispiel: Speicherpooldaten in Datenbanksicherungen verschlüsseln

Speicherpooldaten verschlüsseln, indem angegeben wird, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels des Servers enthalten. Den folgenden Befehl ausgeben:

```
backup db protectkeys=yes password=Kennwortname
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für BACKUP DB

Befehl	Beschreibung
BACKUP DEVCONFIG	Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.
BACKUP VOLHISTORY	Zeichnet Datenträger-History-Daten in externen Dateien auf.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
DELETE VOLHISTORY	Löscht History-Daten sequenzieller Datenträger aus der Datenträger-History-Datei.
EXPIRE INVENTORY	Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DB	Zeigt Zuordnungsinformationen zu der Datenbank an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.
SET DBRECOVERY	Gibt die Einheitenklasse an, die für automatische Sicherungen verwendet werden soll.
SET DRMDBBACKUPEXPIREDAYS	Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.

BACKUP DEVCONFIG (Sicherungskopien von Einheitenkonfigurationsdaten erstellen)

Mit diesem Befehl können Sie Informationen zur Einheitenkonfiguration für den Server sichern.

Achtung: Um eine Datenbank zurückzuschreiben, muss der Server Informationen aus der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei verwenden. Sie müssen Kopien der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei erstellen und speichern. Diese Dateien können nicht erneut erstellt werden.
Mit diesem Befehl werden die folgenden Informationen in mindestens einer Datei gesichert:

- Einheitenklassendefinitionen
- Kassettenarchivdefinitionen
- Laufwerkdefinitionen
- Pfaddefinitionen bei SRCTYPE=SERVER
- Serverdefinitionen
- Servername

- Serverkennwort
- Informationen zur Datenträgerposition für Kassettenarchive mit LIBTYPE=SCSI

 AIX-Betriebssysteme  Linux-BetriebssystemeMit der Serveroption DEVCONFIG können eine oder mehrere Dateien angegeben werden, in denen Einheitenkonfigurationsinformationen gespeichert werden sollen. IBM Spectrum Protect aktualisiert die Dateien, wenn eine Einheitenklasse, ein Kassettenarchiv oder ein Laufwerk definiert, aktualisiert oder gelöscht wird.

 Windows-BetriebssystemeBei der Installation enthält die Serveroptionsdatei eine Option DEVCONFIG, die eine Einheitenkonfigurationsdatei mit dem Namen devcnfg.out angibt. IBM Spectrum Protect aktualisiert diese Datei, wenn eine Einheitenklasse, ein Kassettenarchiv oder ein Laufwerk definiert, aktualisiert oder gelöscht wird.

Um sicherzustellen, dass die Aktualisierungen abgeschlossen sind, bevor der Server angehalten wird, ist Folgendes zu beachten:

- Halten Sie den Server nicht einige Minuten an, nachdem der Befehl BACKUP DEVCONFIG ausgegeben wurde.
- Geben Sie mehrere DEVCONFIG-Optionen in der Serveroptionsdatei an.
- Überprüfen Sie die Einheitenkonfigurationsdatei und stellen Sie fest, ob die Datei aktualisiert wurde.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben, es sei denn, der Befehl enthält den Parameter FILENAMES. Wird der Parameter FILENAMES angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf YES gesetzt, muss der Administrator die Systemberechtigung haben. Wird der Parameter FILENAMES angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator die Bedienerberechtigung, die Maßnahmenberechtigung, die Speicherberechtigung oder die Systemberechtigung haben.

Syntax

```
>>-BAckup DEVCONFig--+-----------------------------------+------->< 
                     |               .-,-------------.   |
                     |               V               | |
                     '-Filenames--=------Dateiname---+-'
```

Parameter

Filenames
: Gibt die Dateien an, in denen Einheitenkonfigurationsinformationen gespeichert werden sollen. Es können mehrere Dateien angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Dieser Parameter ist wahlfrei.

  Wird kein Dateiname angegeben, speichert IBM Spectrum Protect die Informationen in allen Dateien, die mit der Option DEVCONFIG in der Serveroptionsdatei angegeben wurden.

Beispiel: Einheitenkonfigurationsdaten in einer Datei sichern

Einheitenkonfigurationsdaten in einer Datei mit dem Namen DEVICE sichern.

```
backup devconfig filenames=device
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für BACKUP DEVCONFIG

Befehl	Beschreibung
CHECKIN LIBVOLUME	Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
 AIX-Betriebssysteme  Linux-BetriebssystemeDEFINE DEVCLASS (z/OS Media-Server)	AIX-BetriebssystemeLinux-BetriebssystemeDefiniert eine Einheitenklasse für die Verwendung von Speicher, der von einem z/OS Media-Server verwaltet wird.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
LABEL LIBVOLUME	Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.

Befehl	Beschreibung
QUERY LIBVOLUME	Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.
SET SERVERNAME	Gibt den Namen an, unter dem der Server registriert ist.
SET SERVERPASSWORD	Gibt das Serverkennwort an.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.
AIX-BetriebssystemeLinux-BetriebssystemeUPDATE DEVCLASS (z/OS Media-Server)	AIX-BetriebssystemeLinux-BetriebssystemeÄndert die Attribute einer Einheitenklasse für Speicher, der von einem z/OS Media-Server verwaltet wird.
UPDATE DRIVE	Ändert die Attribute eines Laufwerks.
UPDATE LIBRARY	Ändert die Attribute eines Kassettenarchivs.
UPDATE LIBVOLUME	Ändert den Status eines Speicherdatenträgers.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.
UPDATE SERVER	Aktualisiert Informationen über einen Server.

BACKUP NODE (NAS-Knoten sichern)

Verwenden Sie diesen Befehl, um eine Sicherungsoperation für einen NAS-Knoten (NAS = Network Attached Storage) zu starten.

Sicherungen, die für NAS-Knoten mit diesem Befehl BACKUP NODE erstellt werden, sind funktional äquivalent zu Sicherungen, die mit dem Befehl BACKUP NAS auf einem IBM Spectrum Protect-Client erstellt werden. Sie können diese Sicherungen entweder mit dem Serverbefehl RESTORE NODE oder dem Clientbefehl RESTORE NAS zurückschreiben.

Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie die Systemberechtigung, die Maßnahmenberechtigung für die Domäne, der der Knoten zugeordnet ist, oder die Clienteignerberechtigung für den Knoten haben.

Syntax

```
>>-BAckup Node--Knotenname--+-------------------------+--------->
                            | .-,-------------------. |
                            | V                     | |
                            '-----Dateisystemname---+-'

>--+---------------------------------+-------------------------->
   '-MGmtclass--=--Verwaltungsklasse-'

   .-TOC--=--Preferred-----.  .-Wait--=--No------.
>--+----------------------+--+------------------+--------------->
   '-TOC--=--+-No--------+-'  '-Wait--=--+-No--+-'
             +-Preferred-+               '-Yes-'
             '-Yes-------'

   .-MODE--=--DIFFerential-----.
>--+---------------------------+-------------------------------->
   '-MODE--=--+-FULL---------+-'
              '-DIFFerential-'

   .-TYPE--=--BACKUPImage-----.
>--+--------------------------+--------------------------------><
   '-TYPE--=--+-BACKUPImage-+-'
              '-SNAPMirror--'
```

Parameter

Knotenname (Erforderlich)
: Gibt den Knoten an, für den die Sicherung ausgeführt wird. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

Dateisystemname
: Gibt den Namen eines oder mehrerer Dateisysteme an, die gesichert werden sollen. Sie können auch Namen von virtuellen Dateibereichen angeben, die für den NAS-Knoten definiert wurden. Der angegebene Dateisystemname darf keine Platzhalterzeichen enthalten. Sie können mehrere Dateisysteme angeben, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

Wird kein Dateisystem angegeben, werden alle Dateisysteme gesichert. Alle virtuellen Dateibereiche, die für den NAS-Knoten definiert wurden, werden als Teil des Dateisystemimages und nicht separat gesichert.

Ist auf der NAS-Einheit ein Dateisystem mit demselben Namen wie der angegebene virtuelle Dateibereich vorhanden, wird der vorhandene virtuelle Dateibereich automatisch von IBM Spectrum Protect in der Serverdatenbank umbenannt, und das NAS-Dateisystem, das mit dem angegebenen Namen übereinstimmt, wird gesichert. Verfügt der virtuelle Dateibereich über Sicherungsdaten, wird die Dateibereichsdefinition, die dem virtuellen Dateibereich zugeordnet ist, ebenfalls umbenannt.

Tipp: Weitere Überlegungen zur Benennung finden Sie unter dem Parameter für den Namen des virtuellen Dateibereichs im Befehl DEFINE VIRTUALFSMAPPING.

Bei der Bestimmung der zu verarbeitenden Dateisysteme verwendet der Server keine Anweisungen DOMAIN.NAS, INCLUDE.FS.NAS oder EXCLUDE.FS.NAS in der Clientoptionsdatei oder der Clientoptionsgruppe. Werden mehrere Dateisysteme gesichert, ist die Sicherung jedes Dateisystems ein separater Serverprozess.

MGmtclass
Gibt den Namen der Verwaltungsklasse an, an die diese Sicherungsdaten gebunden werden. Wird keine Verwaltungsklasse angegeben, werden die Sicherungsdaten an die Standardverwaltungsklasse der Maßnahmendomäne gebunden, der der Knoten zugeordnet ist. Bei der Bestimmung der Verwaltungsklasse verwendet der Server *keine* Anweisungen INCLUDE.FS.NAS in der Clientoptionsdatei oder der Clientoptionsgruppe. Die Zielverwaltungsklasse kann auf einen nativen IBM Spectrum Protect-Pool verweisen. In diesem Fall werden NDMP-Daten (NDMP = Network Data Management Protocol) an die native IBM Spectrum Protect-Hierarchie gesendet. Danach verbleiben die Daten in der IBM Spectrum Protect-Hierarchie. Daten, die in native IBM Spectrum Protect-Pools fließen, werden über das LAN gesendet, und Daten, die in NAS-Pools fließen, können direkt angehängt werden oder über ein SAN gesendet werden.

Wenn Sie eine Verwaltungsklasse mit dem Befehl BACKUP NODE angeben, werden alle Versionen der Sicherungsdaten, die zu dem NAS-Knoten gehören, erneut an die neue Verwaltungsklasse gebunden.

TOC
Gibt an, ob für jede Dateisystemsicherung ein Inhaltsverzeichnis gesichert wird. Sie sollten bei der Festlegung, ob ein Inhaltsverzeichnis gesichert werden soll, Folgendes berücksichtigen:

- Wird ein Inhaltsverzeichnis gesichert, können Sie den Befehl QUERY TOC zur Bestimmung des Inhalts einer Dateisystemsicherung zusammen mit dem Befehl RESTORE NODE zur Zurückschreibung von einzelnen Dateien oder Verzeichnisstrukturen verwenden. Sie können auch den IBM Spectrum Protect-Webclient für Sichern/Archivieren verwenden, um die gesamte Dateisystemstruktur zu untersuchen und Dateien und Verzeichnisse zum Zurückschreiben auszuwählen. Für die Erstellung eines Inhaltsverzeichnisses müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsimage gebunden ist. Die Erstellung eines Inhaltsverzeichnisses erfordert zusätzliche Verarbeitung, zusätzliche Netzressourcen, zusätzlichen Speicherpoolplatz und möglicherweise einen Mountpunkt während der Sicherungsoperation.
- Ein Inhaltsverzeichnis für ein NAS-Dateisystem darf keinen Verzeichnispfad haben, der größer als 1024 Zeichen ist.
- Wird ein Inhaltsverzeichnis für eine Dateisystemsicherung nicht gesichert, können Sie dennoch einzelne Dateien oder Verzeichnisstrukturen mit dem Befehl RESTORE NODE zurückschreiben, vorausgesetzt, dass Sie den vollständig qualifizierten Namen jeder Datei oder jedes Verzeichnisses kennen, die bzw. das zurückgeschrieben werden soll, und das Image, in dem dieses Objekt gesichert wurde.

  Dieser Parameter ist wahlfrei. Der Standardwert ist Preferred. Gültige Werte:

  No
  Gibt an, dass keine Inhaltsverzeichnisinformationen für Dateisystemsicherungen gesichert werden.
  Preferred
  Gibt an, dass Inhaltsverzeichnisinformationen für Dateisystemsicherungen gesichert werden sollen. Eine Sicherung schlägt jedoch nicht fehl, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt. Dies ist der Standardwert.
  Yes
  Gibt an, dass Inhaltsverzeichnisinformationen für jede Dateisystemsicherung gesichert werden müssen. Eine Sicherung schlägt fehl, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

Achtung: Wird MODE=DIFFERENTIAL angegeben und ein Inhaltsverzeichnis angefordert (TOC=PREFERRED oder TOC=YES), aber verfügt das letzte vollständige Image über kein Inhaltsverzeichnis, wird eine Gesamtsicherung ausgeführt und ein Inhaltsverzeichnis für diese Gesamtsicherung erstellt.

Wait
Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist NO. Gültige Werte:

No
Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Mit dem Befehl QUERY PROCESS kann die Hintergrundverarbeitung dieses Befehls überwacht werden.
Yes
Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist. Werden mehrere Dateisysteme gesichert, müssen alle Sicherungsprozesse vor Beendigung des Befehls abgeschlossen sein. Achtung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

MODE

Gibt an, ob es sich bei den Dateisystemsicherungen um Gesamt- oder Teilsicherungen handelt. Der Standardwert ist DIFFERENTIAL.

FULL
: Gibt an, dass das vollständige Dateisystem gesichert wird.

DIFFerential
: Gibt an, dass nur die Dateien gesichert werden sollen, die sich seit der letzten Gesamtsicherung geändert haben. Wird eine Sicherung der geänderten Teile ausgewählt und wird keine Gesamtsicherung gefunden, wird eine Gesamtsicherung ausgeführt. Sie können nicht TYPE=SNAPMIRROR angeben, wenn der Parameter MODE auf DIFFERENTIAL gesetzt ist.

TYPE

Gibt die Sicherungsmethode an, die zur Ausführung der NDMP-Sicherungsoperation verwendet wird. Der Standardwert für diesen Parameter ist BACKUPIMAGE, und er sollte verwendet werden, um eine standardmäßige NDMP-Basis- oder -Differenzsicherung auszuführen. Andere Imagetypen stellen Sicherungsmethoden dar, die für einen bestimmten Dateiserver spezifisch sein können. Gültige Werte:

BACKUPImage
: Gibt an, dass das Dateisystem unter Verwendung einer NDMP-Speicherauszugsoperation gesichert werden soll. Dies ist die Standardmethode für die Ausführung einer NDMP-Sicherung. Die Operation des Typs BACKUPIMAGE unterstützt Gesamt- und Differenzsicherungen, Zurückschreibungen auf Dateiebene und Sicherungen auf Verzeichnisebene.

SNAPMirror
: Gibt an, dass das Dateisystem unter Verwendung der NetApp-Funktion 'SnapMirror-auf-Band' in einen IBM Spectrum Protect-Speicherpool kopiert werden soll. SnapMirror-Images sind Gesamtsicherungsimages auf Blockebene eines Dateisystems. Normalerweise wird für die Ausführung einer SnapMirror-Sicherung erheblich weniger Zeit als für die Ausführung einer traditionellen NDMP-Gesamtsicherung des Dateisystems benötigt. Es gibt jedoch Einschränkungen bezüglich der Verwendungsmöglichkeit von SnapMirror-Images. Die Funktion 'SnapMirror-auf-Band' sollte als Option für die Wiederherstellung nach einem Katastrophenfall zum Kopieren sehr großer NetApp-Dateisysteme in den Sekundärspeicher verwendet werden.

  Für die meisten NetApp-Dateisysteme wird die standardmäßige NDMP-Gesamt- oder -Differenzsicherungsmethode verwendet. Weitere Informationen enthält die Dokumentation zu Ihrem NetApp-Dateiserver.

  Die folgenden Einschränkungen gelten, wenn der Parameter TYPE auf SNAPMirror gesetzt wird:

  Einschränkungen:

  - Sie können nicht TOC=YES oder TOC=PREFERRED angeben.
  - Der Dateisystemname kann kein Name eines virtuellen Dateibereichs sein.
  - Die Momentaufnahme, die von dem Dateiserver während der SnapMirror-Kopieroperation automatisch erstellt wird, wird am Ende der Operation gelöscht.
  - Dieser Parameter ist nur für NetApp- und IBM® N-Series-Dateiserver gültig.

Beispiel: Eine Gesamtsicherung ausführen

Eine Gesamtsicherung für das Dateisystem /vol/vol10 des NAS-Knotens NAS1 ausführen.

```
backup node nas1 /vol/vol10 mode=full
```

Beispiel: Eine Sicherung eines Verzeichnisses ausführen und ein Inhaltsverzeichnis erstellen

Das Verzeichnis /vol/vol2/mikes auf dem Knoten NAS1 sichern und ein Inhaltsverzeichnis für das Image erstellen. Für die folgenden beiden Beispiele wird angenommen, dass Tabelle 1 die Definitionen für virtuelle Dateibereiche enthält, die auf dem Server für den Knoten NAS1 vorhanden sind.

```
backup node nas1 /mikesdir
```

Tabelle 1. Definitionen für virtuelle Dateibereiche

Name des virtuellen Dateibereichs	Dateisystem	Pfad
/mikesdir	/vol/vol2	/mikes
/DataDirVol2	/vol/vol2	/project1/data
/TestDirVol1	/vol/vol1	/project1/test

Beispiel: Eine Sicherung für zwei Verzeichnisse ausführen

Die Verzeichnisse /vol/vol2/project1/data und /vol/vol1/project1/test des Knotens NAS1 sichern. In Tabelle 1 befinden sich die Definitionen für virtuelle Dateibereiche, die auf dem Server für den Knoten NAS1 vorhanden sind.

```
backup node nas1 /DataDirVol2,/testdirvol1  mode=full toc=yes
```

Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für BACKUP NODE

Befehl	Beschreibung
BACKUP NAS (Clientbefehl)	Erstellt eine Sicherung der NAS-Knotendaten.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs definieren.
QUERY NASBACKUP	Zeigt Informationen zu NAS-Sicherungsimages an.
QUERY TOC	Zeigt Details zum Inhaltsverzeichnis für ein angegebenes Sicherungsimage an.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
RESTORE NAS (Clientbefehl)	Schreibt eine Sicherung der NAS-Knotendaten zurück.
RESTORE NODE	Schreibt einen NAS-Knoten (NAS = Network Attached Storage) zurück.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.

Zugehörige Konzepte:
Sichern und Zurückschreiben mit der NetApp-Funktion 'SnapMirror to Tape''

BACKUP STGPOOL (Daten eines primären Speicherpools in einem Kopienspeicherpool sichern)

Mit diesem Befehl können Dateien aus dem primären Speicherpool in einem Kopienspeicherpool gesichert werden.

Sie können Daten aus einem primären Speicherpool sichern, der mit dem Format NATIVE, NONBLOCK oder einem der NDMP-Formate (NETAPPDUMP, CELERRADUMP oder NDMPDUMP) definiert ist. Der Kopienspeicherpool, in dem Daten gesichert werden sollen, muss dasselbe Datenformat wie der primäre Speicherpool haben. IBM Spectrum Protect unterstützt die Back-End-Datenversetzung für NDMP-Images.

Ist eine Datei in dem Kopienspeicherpool vorhanden, wird die Datei nicht gesichert, es sei denn, die Kopie der Datei in dem Kopienspeicherpool ist als beschädigt markiert. Es wird jedoch keine neue Kopie erstellt, wenn die Datei in dem primären Speicherpool auch als beschädigt markiert ist. In einem Speicherpool mit wahlfreiem Zugriff werden Cachekopien von umgelagerten Dateien und beschädigte Primärdateien nicht gesichert.

Tipp: Wird dieser Befehl für einen primären Speicherpool ausgegeben, der für die Deduplizierung von Daten definiert ist, werden doppelte Daten entfernt, wenn der Kopienspeicherpool ebenfalls für die Deduplizierung von Daten definiert ist.

Wenn die Umlagerung für einen Speicherpool während der Sicherung dieses Speicherpools startet, werden einige Dateien möglicherweise umgelagert, bevor sie gesichert werden. Speicherpools an einer höheren Position in der Umlagerungshierarchie sollen möglicherweise vor Speicherpools an einer niedrigeren Position gesichert werden.

Einschränkungen:

- Führen Sie die Befehle MOVE DRMEDIA und BACKUP STGPOOL nicht gleichzeitig aus. Stellen Sie sicher, dass die Speicherpoolsicherungsprozesse abgeschlossen wurden, bevor der Befehl MOVE DRMEDIA ausgegeben wird.
- Sie können keine Daten aus oder in Speicherpools sichern, die mit einer Einheitenklasse CENTERA definiert sind.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Kopienspeicherpool erforderlich, in dem Sicherungskopien erstellt werden sollen.

Syntax

```
>>-BAckup STGpool--Name_des_primären_Pools--Name_des_Kopienpools-->

   .-MAXPRocess--=--1------.
>--+-----------------------+----------------------------------->
   '-MAXPRocess--=--Anzahl-'

   .-Preview---=--No-----------------.
>--+-------------------------------+-------------------------->
   '-Preview---=--+-No--------------+-'
                  +-Yes-------------+
                  |             (1) |
                  '-VOLumesonly-----'
```

```
   .-SHREDTONOshred--=--No------.  .-Wait--=--No------.
>--+----------------------------+--+------------------+--------><
   '-SHREDTONOshred--=--+-No--+-'  '-Wait--=--+-No--+-'
                        '-Yes-'               '-Yes-'
```

Anmerkungen:

1. Nur für Speicherpools gültig, die einer Einheitenklasse mit sequenziellem Zugriff zugeordnet sind.

Parameter

Name_des_primären_Pools (Erforderlich)
: Gibt den primären Speicherpool an.

Name_des_Kopienpools (Erforderlich)
: Gibt den Kopienspeicherpool an.

MAXPRocess
: Gibt die maximale Anzahl der Parallelprozesse für die Sicherung von Dateien an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1.

  Die Verwendung mehrerer paralleler Prozesse kann den Durchsatz der Sicherung verbessern. Die Erwartung ist die, dass die für die Ausführung der Speicherpoolsicherung benötigte Zeit verringert wird, indem mehrere Prozesse verwendet werden. Sind mehrere Prozesse aktiv, müssen jedoch in einigen Fällen ein oder mehrere Prozesse auf die Verwendung eines Datenträgers warten, der bereits von einem anderen Sicherungsprozess verwendet wird.

  Bei der Bestimmung dieses Werts ist die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden kann. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Aktivitäten und Systemaktivitäten sowie von den Mountlimits der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Sicherung betroffen sind.

  Jeder Prozess benötigt einen Mountpunkt für Datenträger aus dem Kopienspeicherpool und, falls der Einheitentyp nicht FILE lautet, außerdem ein Laufwerk. Wird ein sequenzieller Speicherpool gesichert, benötigt jeder Prozess einen zusätzlichen Mountpunkt für Datenträger des primären Speicherpools und, falls der Einheitentyp nicht FILE lautet, ein zusätzliches Laufwerk. Beispiel: Angenommen, es werden maximal drei Prozesse für die Zurückschreibung eines primären sequenziellen Speicherpools aus einem Kopienspeicherpool mit derselben Einheitenklasse angegeben. Jeder Prozess benötigt zwei Mountpunkte und zwei Laufwerke. Um alle drei Prozesse ausführen zu können, muss der Grenzwert für Ladeanforderungen für die Einheitenklasse mindestens 6 betragen, und es müssen mindestens sechs Mountpunkte und sechs Laufwerke verfügbar sein.

  Für die Voranzeige einer Zurückschreibung wird nur ein Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

Preview
: Gibt an, ob eine Voranzeige der Sicherung, nicht aber ihre Ausführung gewünscht wird. In der Voranzeige werden die Anzahl der Dateien und die Byte angezeigt, die gesichert werden sollen, sowie eine Liste der Datenträger des primären Speicherpools, die geladen werden müssen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

  No
  : Gibt an, daß die Sicherung ausgeführt wird.

  Yes
  : Gibt an, daß eine Voranzeige der Sicherung, aber nicht die Ausführung der Sicherung gewünscht wird.

  VOLumesonly
  : Gibt an, daß die Voranzeige der Sicherung nur als Liste der Datenträger gewünscht wird, die geladen werden müssen. Diese Auswahl erfordert die geringste Verarbeitungszeit. Die Option VOLUMESONLY ist nur für Speicherpools gültig, die einer Einheitenklasse mit sequenziellem Zugriff zugeordnet sind.
    Die Option VOLUMESONLY kann verwendet werden, um eine Liste der Datenträger abzurufen, die vom Speicherpoolsicherungsprozess benötigt werden. Beispiel:

    ```
    backup stgpool primary_pool copystg preview=volumesonly
    ```

    Die Liste der Datenträger wird im Serveraktivitätenprotokoll mit der Nachricht ANR1228I protokolliert. Fragen Sie das Serveraktivitätenprotokoll ab, um die Liste der erforderlichen Datenträger abzurufen. Beispiel:

    ```
    query actlog msg=1228
    ```

SHREDTONOshred
: Gibt an, ob Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einem Kopienspeicherpool gesichert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

  No
  : Gibt an, dass der Server das Sichern von Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einem Kopienspeicherpool nicht zulässt. Wenn der primäre Speicherpool das Schreddern erzwingt, schlägt die Operation fehl.

  Yes

Gibt an, dass der Server das Sichern von Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einem Kopienspeicherpool zulässt. Die Daten in dem Kopienspeicherpool werden nicht geschreddert, wenn er gelöscht wird.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise einige Dateien bereits vor dem Abbruch gesichert.

Yes

Gibt an, dass der Server diese Operation im Vordergrund verarbeitet. Die Operation muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dem Verwaltungsclient an, wenn die Operation beendet ist. Anmerkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

Beispiel: Den primären Speicherpool sichern

Den primären Speicherpool mit dem Namen PRIMARY_POOL im Kopienspeicherpool mit dem Namen COPYSTG sichern.

```
backup stgpool primary_pool copystg
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für BACKUP STGPOOL

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY SHREDSTATUS	Zeigt Informationen zu Daten an, die auf das Schreddern warten.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
RESTORE STGPOOL	Schreibt Dateien aus Kopienspeicherpools in einen primären Speicherpool zurück.
RESTORE VOLUME	Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopienspeicherpools zurück.
SHRED DATA	Startet manuell den Prozess zum Schreddern gelöschter Daten.

BACKUP VOLHISTORY (Protokolldaten sequenzieller Datenträger speichern)

Mit diesem Befehl können Protokolldaten sequenzieller Datenträger in einer oder in mehreren Dateien gesichert werden.

Tipp: Datenträgerprotokolldaten müssen verwendet werden, wenn die Datenbank erneut geladen wird und betroffene Speicherpooldatenträger geprüft werden. Kann der Server nicht gestartet werden, kann die Protokolldatei für Datenträger verwendet werden, um die Datenbank nach diesen Datenträgern abzufragen.
Das Datenträgerprotokoll umfasst Informationen über die folgenden Datenträgertypen:

- Archivprotokolldatenträger
- Datenbanksicherungsdatenträger
- Exportdatenträger
- Sicherungsgruppendatenträger
- Datenbankmomentaufnahmedatenträger
- Datenträger mit Datenbankwiederherstellungsplandateien
- Datenträger mit Wiederherstellungsplandateien
- Datenträger mit Momentaufnahmen der Wiederherstellungsplandateien
- Die folgenden Speicherpooldatenträger mit sequenziellem Zugriff:
  - Datenträger, die Speicherpools hinzugefügt wurden

- Datenträger, die aufgrund von Wiederherstellungsoperationen oder Operationen MOVE DATA wiederverwendet wurden
- Datenträger, die mit dem Befehl DELETE VOLUME oder während der Wiederherstellung von Arbeitsdatenträgern entfernt wurden

Achtung: Um eine Datenbank zurückzuschreiben, muss der Server Informationen aus der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei verwenden. Sie müssen Kopien der Datenträgerhistorydatei und der Einheitenkonfigurationsdatei erstellen und speichern. Diese Dateien können nicht erneut erstellt werden.

 AIX-Betriebssysteme  Linux-BetriebssystemeSie müssen die Serveroption VOLUMEHISTORY verwenden, um eine oder mehrere Protokolldateien für Datenträger anzugeben. IBM Spectrum Protect aktualisiert Protokolldateien für Datenträger, wenn sich Protokolldaten des Servers zu sequenziellen Datenträgern ändern.

 Windows-BetriebssystemeBei der Installation enthält die Serveroptionsdatei eine Option VOLUMEHISTORY, die eine Standardprotokolldatei für Datenträger mit dem Namen volhist.out angibt. IBM Spectrum Protect aktualisiert Protokolldateien für Datenträger, wenn sich Protokolldaten des Servers zu sequenziellen Datenträgern ändern.

Um sicherzustellen, dass die Aktualisierungen abgeschlossen sind, bevor der Server angehalten wird, führen Sie diese Schritte aus:

- Halten Sie den Server nicht einige Minuten an, nachdem der Befehl BACKUP VOLHISTORY ausgegeben wurde.
- Geben Sie mehrere Optionen VOLUMEHISTORY in der Serveroptionsdatei an.
- Überprüfen Sie die Protokolldatei für Datenträger, um zu bestimmen, ob die Datei aktualisiert wurde.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben, es sei denn, der Befehl enthält den Parameter FILENAMES. Wird der Parameter FILENAMES angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf YES gesetzt, muss der Administrator die Systemberechtigung haben. Wird der Parameter FILENAMES angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator die Bedienerberechtigung, die Maßnahmenberechtigung, die Speicherberechtigung oder die Systemberechtigung haben.

Syntax

```
>>-BAckup VOLHistory--+-----------------------------------+------><
                      |                .-,-------------.  |
                      |                V                 |  |
                      '-Filenames--=-------Dateiname---+-'
```

Parameter

Filenames
: Gibt den Namen einer oder mehrerer Dateien an, in denen eine Sicherungskopie der Datenträgerprotokolldaten gespeichert werden soll. Mehrere Dateinamen müssen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Dieser Parameter ist wahlfrei.

  Wird kein Dateiname angegeben, speichert IBM Spectrum Protect die Informationen in allen Dateien, die mit der Option VOLUMEHISTORY in der Server-Optionsdatei angegeben wurden.

Beispiel: Die Datenträgerprotokolldaten in einer Datei sichern

Sichern Sie die Datenträgerprotokolldaten in der Datei VOLHIST.

```
backup volhistory filenames=volhist
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für BACKUP VOLHISTORY

Befehl	Beschreibung
DELETE VOLHISTORY	Löscht History-Daten sequenzieller Datenträger aus der Datenträger-History-Datei.
DELETE VOLUME	Löscht einen Datenträger aus einem Speicherpool.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.
UPDATE VOLHISTORY	Ändert Standortinformationen für einen Datenträger in der Datenträger-History-Datei oder fügt Informationen hinzu.

BEGIN EVENTLOGGING (Ereignisprotokollierung beginnen)

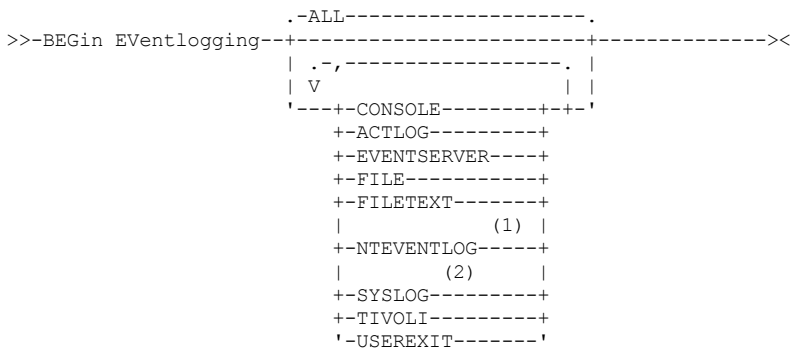
Mit diesem Befehl kann das Protokollieren von Ereignissen für einen oder mehrere Empfänger begonnen werden. Ein Empfänger, für den die Ereignisprotokollierung begonnen hat, ist ein *aktiver Empfänger*.

Wenn der Server gestartet wird, beginnt die Ereignisprotokollierung automatisch für das Konsol- und Aktivitätenprotokoll sowie für alle Empfänger, die auf der Basis von Einträgen in der Server-Optionsdatei automatisch gestartet werden. Mit diesem Befehl kann das Protokollieren von Ereignissen für Empfänger begonnen werden, für die die Ereignisprotokollierung *nicht* automatisch beim Server-Start gestartet wird. Außerdem kann dieser Befehl verwendet werden, nachdem die Ereignisprotokollierung für einen oder mehrere Empfänger inaktiviert wurde.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Anmerkungen:

1. Dieser Parameter ist nur für das Windows-Betriebssystem verfügbar.
2. Dieser Parameter ist nur für das Linux-Betriebssystem verfügbar.

Parameter

Einen oder mehrere Empfänger angeben. Es können mehrere Empfänger angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird ALL angegeben, beginnt das Protokollieren für alle konfigurierten Empfänger. Standardwert ist ALL.

ALL
: Gibt alle Empfänger an, die für die Ereignisprotokollierung konfiguriert sind.

CONSOLE
: Gibt die Server-Konsole als Empfänger an.

ACTLOG
: Gibt das IBM Spectrum Protect-Aktivitätenprotokoll als Empfänger an.

EVENTSERVER
: Gibt den Ereignisserver als Empfänger an.

FILE
: Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist ein Satz in der Datei, und eine Person kann jedes protokollierte Ereignis nicht einfach lesen.

FILETEXT
: Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

Windows-BetriebssystemeNTEVENTLOG
: Windows-BetriebssystemeGibt das Windows-Anwendungsprotokoll als Empfänger an.

Linux-BetriebssystemeSYSLOG
: Linux-BetriebssystemeGibt das Linux-Systemprotokoll als Empfänger an.

TIVOLI
: Gibt Tivoli Management Environment (TME) als Empfänger an.

USEREXIT
: Gibt eine benutzerdefinierte Routine, in die IBM Spectrum Protect Informationen schreibt, als Empfänger an.

Beispiel: Das Protokollieren von Ereignissen beginnen

Das Protokollieren von Ereignissen im IBM Spectrum Protect-Aktivitätenprotokoll beginnen.

```
begin eventlogging actlog
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für BEGIN EVENTLOGGING

Befehl	Beschreibung
DISABLE EVENTS	Inaktiviert bestimmte Ereignisse für Empfänger.
ENABLE EVENTS	Aktiviert bestimmte Ereignisse für Empfänger.
END EVENTLOGGING	Beendet das Ereignisprotokoll für einen bestimmten Empfänger.
QUERY ENABLED	Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an.
QUERY EVENTRULES	Zeigt Informationen über Regeln für Server- und Clientereignisse an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

CANCEL-Befehle

Mit den CANCEL-Befehlen kann eine Task oder ein Prozess vor der Beendigung abgebrochen werden.

- CANCEL EXPIRATION (Verfallsprozess abbrechen)
- CANCEL EXPORT (Ausgesetzte Exportoperation löschen)
- CANCEL PROCESS (Verwaltungsprozess abbrechen)
- CANCEL REPLICATION (Knotenreplikationsprozesse abbrechen)
- CANCEL REQUEST (Ladeanforderungen abbrechen)
- CANCEL RESTORE (Wiederanlauffähige Zurückschreibungssitzung abbrechen)
- CANCEL SESSION (Clientsitzungen abbrechen)

CANCEL EXPIRATION (Verfallsprozess abbrechen)

Verwenden Sie diesen Befehl, um einen Prozess mit einer unbekannten Prozessnummer abzubrechen, der infolge einer Bestandsverfallsoperation ausgeführt wird.

Verwenden Sie den Befehl CANCEL EXPIRATION, wenn die Verfallsprozessnummer nicht bekannt ist; verwenden Sie in allen anderen Fällen den Befehl CANCEL PROCESS und geben Sie die Prozessnummer des Verfallsprozesses an. Mit beiden Befehlen wird derselbe Code zum Beenden des Verfallsprozesses aufgerufen.

Mithilfe des Befehls CANCEL EXPIRATION kann der Abbruch eines Verfallsprozesses automatisiert werden. Wenn Sie beispielsweise den Bestandsverfall um Mitternacht starten und der Prozess aufgrund des Wartungsaufwands auf dem Server um 03:00 Uhr enden muss, können Sie die Ausführung eines Befehls CANCEL EXPIRATION um 03:00 Uhr planen, ohne die Prozessnummer kennen zu müssen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-CANcel EXPIration-------------------------------------------><
```

Beispiel: Einen Bestandsverfallsprozess abbrechen

Den Prozess abbrechen, der durch eine Bestandsverfallsoperation generiert wurde.

```
cancel expiration
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für CANCEL EXPIRATION

Befehl	Beschreibung
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
EXPIRE INVENTORY	Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell.

CANCEL EXPORT (Ausgesetzte Exportoperation löschen)

Mit diesem Befehl kann eine ausgesetzte Exportoperation zwischen Servern gelöscht werden. Nach Ausgabe des Befehls CANCEL EXPORT können Sie die Exportoperation nicht erneut starten. Soll eine momentan aktive Exportoperation gelöscht werden, verwenden Sie den Befehl CANCEL PROCESS.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung erforderlich.

Syntax

```
                  .-*-------------.
>>-CANcel EXPort -+---------------+----------------------------><
                  '---Export-ID---'
```

Parameter

Export-ID
: Die eindeutige ID der ausgesetzten Exportoperation, die Sie löschen wollen. Für die ID können auch Platzhalterzeichen eingegeben werden. Mit dem Befehl QUERY EXPORT können Sie die momentan ausgesetzten Exportoperationen auflisten.

Beispiel: Eine bestimmte ausgesetzte Exportoperation löschen

Die ausgesetzte Exportoperation zwischen Servern EXPORTALLACCTNODES abbrechen.

```
cancel export exportallacctnodes
```

Beispiel: Alle ausgesetzten Exportoperation zwischen Servern löschen

Brechen Sie alle ausgesetzten Exportoperationen zwischen Servern ab.

```
cancel export *
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL EXPORT

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT SERVER	Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server.
QUERY EXPORT	Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.
RESTART EXPORT	Startet eine ausgesetzte Exportoperation erneut.
SUSPEND EXPORT	Setzt eine aktive Exportoperation aus.

CANCEL PROCESS (Verwaltungsprozess abbrechen)

Mit diesem Befehl kann ein Hintergrundprozess abgebrochen werden, der durch einen Verwaltungsbefehl oder durch einen Prozess, wie beispielsweise eine Speicherpoolumlagerung, gestartet wurde.

Folgende Befehle generieren Hintergrundprozesse:

- AUDIT CONTAINER
- AUDIT LIBRARY
- AUDIT LICENSES
- AUDIT VOLUME
- BACKUP DB
- BACKUP NODE
- BACKUP STGPOOL
- CHECKIN LIBVOLUME
- CHECKOUT LIBVOLUME
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeCONVERT STGPOOL
- DELETE FILESPACE
- DELETE VOLUME

- EXPIRE INVENTORY
- EXPORT ADMIN
- EXPORT NODE
- EXPORT POLICY
- EXPORT SERVER
- GENERATE BACKUPSET
- IMPORT ADMIN
- IMPORT NODE
- IMPORT POLICY
- IMPORT SERVER
- MIGRATE STGPOOL
- MOVE DATA
- MOVE DRMEDIA
- MOVE MEDIA
- PREPARE
- PROTECT STGPOOL
- RECLAIM STGPOOL
- REPLICATE NODE
- RESTORE NODE
- RESTORE STGPOOL
- RESTORE VOLUME
- VARY

Folgende interne Serveroperationen generieren Hintergrundprozesse:

- Datenträgerbestandsverfall
- Umlagerung
- Wiederherstellung

Zum Abbrechen eines Prozesses benötigen Sie die Prozessnummer, die Sie durch Ausgabe des Befehls QUERY PROCESS abrufen können.

Einige Prozesse, wie beispielsweise die Wiederherstellung, generieren Ladeanforderungen, um die Verarbeitung abzuschließen. Hat ein Prozess eine anstehende Ladeanforderung, antwortet der Prozess möglicherweise erst dann auf einen Befehl CANCEL PROCESS, wenn unter Verwendung des Befehls REPLY oder CANCEL REQUEST auf die Ladeanforderung geantwortet bzw. die Ladeanforderung abgebrochen wurde, oder wenn eine Zeitlimitüberschreitung aufgetreten ist.

Geben Sie den Befehl QUERY REQUEST aus, um offene Anforderungen aufzulisten, oder fragen Sie das Aktivitätenprotokoll ab, um zu bestimmen, ob ein Prozess eine anstehende Ladeanforderung hat. Eine Ladeanforderung gibt an, dass ein Datenträger für den aktuellen Prozess erforderlich ist, der Datenträger aber in dem Kassettenarchiv nicht verfügbar ist. Der Datenträger ist möglicherweise nicht verfügbar, wenn der Administrator den Befehl MOVE MEDIA oder CHECKOUT LIBVOLUME ausgibt oder den Datenträger manuell aus dem Kassettenarchiv entfernt.

Nachdem Sie einen Befehl CANCEL PROCESS für eine Exportoperation ausgegeben haben, kann der Prozess nicht erneut gestartet werden. Um eine serverübergreifende Exportoperation zu stoppen und die Operation zu einem späteren Zeitpunkt erneut zu starten, geben Sie den Befehl SUSPEND EXPORT aus.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-CANcel PRocess--Prozessnummer------------------------------><
```

Parameter

Prozessnummer (Erforderlich)
Gibt die Nummer des Hintergrundprozesses an, der abgebrochen werden soll.

Beispiel: Einen Hintergrundprozess unter Verwendung seiner Prozessnummer abbrechen

Hintergrundprozess Nummer 3 abbrechen.

```
cancel process 3
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL PROCESS

Befehl	Beschreibung

Befehl	Beschreibung
CANCEL EXPORT	Löscht eine ausgesetzte Exportoperation.
CANCEL REQUEST	Bricht anstehende Datenträgerladeanforderungen ab.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeCONVERT STGPOOL	AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeKonvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemePROTECT STGPOOL	AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeSchützt einen Verzeichniscontainerspeicherpool.
QUERY EXPORT	Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
REPLY	Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.
RESTART EXPORT	Startet eine ausgesetzte Exportoperation erneut.
SUSPEND EXPORT	Setzt eine aktive Exportoperation aus.

CANCEL REPLICATION (Knotenreplikationsprozesse abbrechen)

Verwenden Sie diesen Befehl, um alle Knotenreplikationsprozesse abzubrechen.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-CANcel REPLication-----------------------------------------><
```

Parameter

Keine.

Beispiel: Knotenreplikationsprozesse abbrechen

Alle Knotenreplikationsprozesse abbrechen.

```
cancel replication
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL REPLICATION

Befehl	Beschreibung
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.

CANCEL REQUEST (Ladeanforderungen abbrechen)

Mit diesem Befehl können eine oder mehrere anstehende Anforderungen zum Laden von Datenträgern abgebrochen werden. Um eine Ladeanforderung abzubrechen, muss die Anforderungsnummer bekannt sein, die der Anforderung zugeordnet ist. Diese Nummer ist in der Ladeanforderungsnachricht enthalten und kann auch mit dem Befehl QUERY REQUEST angezeigt werden.

Berechtigungsklasse

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

Syntax

```
>>-CANcel REQuest--+-Anforderungsnummer-+--+-----------+------><
                  '-ALl----------------'  '-PERManent-'
```

Parameter

Anforderungsnummer
: Gibt die Anforderungsnummer der Ladeanforderung an, die abgebrochen werden soll.

ALl
: Gibt an, daß alle anstehenden Ladeanforderungen abgebrochen werden sollen.

PERManent
: Gibt an, daß der Server die Datenträger, für die eine Ladeanforderung abgebrochen wird, als nicht verfügbar markieren soll. Dieser Parameter ist wahlfrei.

Beispiel: Eine Ladeanforderung abbrechen

Anforderungsnummer 2 abbrechen.

```
cancel request 2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL REQUEST

Befehl	Beschreibung
QUERY REQUEST	Zeigt Informationen über alle anstehenden Ladeanforderungen an.
UPDATE VOLUME	Aktualisiert die Attribute der Speicherpooldatenträger.

CANCEL RESTORE (Wiederanlauffähige Zurückschreibungssitzung abbrechen)

Mit diesem Befehl kann eine wiederanlauffähige Zurückschreibungssitzung abgebrochen werden. Zurückschreibungssitzungen können im aktiven oder im wiederanlauffähigen Status abgebrochen werden. Alle ausstehenden Ladeanforderungen, die zu dieser Sitzung gehören, werden automatisch abgebrochen.

Zum Anzeigen wiederanlauffähiger Zurückschreibungssitzungen den Befehl QUERY RESTORE verwenden.

Berechtigungsklasse

Für diesen Befehl ist die System- oder Bedienerberechtigung erforderlich.

Syntax

```
>>-CANcel--RESTore--+-Sitzungsnummer-+------------------------><
                    '-ALl------------'
```

Parameter

Sitzungsnummer
: Gibt die Nummer der wiederanlauffähigen Zurückschreibungssitzung an. Eine aktive Sitzung hat eine positive Nummer und eine wiederanlauffähige Sitzung eine negative Nummer.

ALl
: Gibt an, dass alle wiederanlauffähigen Zurückschreibungssitzungen abgebrochen werden sollen.

Beispiel: Zurückschreibungsoperationen abbrechen

Alle Operationen zum Zurückschreiben abbrechen.

```
cancel restore all
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL RESTORE

Befehl	Beschreibung
QUERY RESTORE	Zeigt Informationen über wiederanlauffähige Zurückschreibungssitzungen an.

CANCEL SESSION (Clientsitzungen abbrechen)

Verwenden Sie diesen Befehl, um vorhandene Verwaltungssitzungen oder Clientknotensitzungen abzubrechen und den Abbruch einer Verwaltungssitzung oder Clientknotensitzung mit dem Server zu erzwingen. Alle ausstehenden Ladeanforderungen, die zu dieser Sitzung gehören, werden automatisch abgebrochen. Der Clientknoten muss eine neue Sitzung starten, um die Aktivitäten wiederaufzunehmen.

Wird eine Sitzung abgebrochen, die sich im inaktiven Status (IdleW) befindet, wird die Client-Sitzung automatisch wieder mit dem Server verbunden, wenn sie mit dem erneuten Senden von Daten beginnt.

Wenn dieser Befehl einen Prozess unterbricht, wie beispielsweise Sicherung oder Archivierung, werden die Ergebnisse der Verarbeitung, die zum Zeitpunkt der Unterbrechung aktiv ist, rückgängig gemacht und nicht in der Datenbank festgeschrieben.

Berechtigungsklasse

Für diesen Befehl ist die System- oder Bedienerberechtigung erforderlich.

Syntax

```
>>-CANcel SEssion--+-Sitzungsnummer-+-------------------------><
                   '-ALl------------'
```

Parameter

Sitzungsnummer
: Gibt die Nummer der Verwaltungs-, Server- oder Clientknotensitzung an, die abgebrochen werden soll.

ALl
: Gibt an, dass alle Clientknotensitzungen abgebrochen werden. Sie können diesen Parameter nicht verwenden, um Verwaltungsclient- oder Serversitzungen abzubrechen.

Beispiel: Eine bestimmte Clientknotensitzung abbrechen

Die Clientknotensitzung mit NODEP (Sitzung 3) abbrechen.

```
cancel session 3
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CANCEL SESSION

Befehl	Beschreibung
DISABLE SESSIONS	Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden.
LOCK ADMIN	Verweigert einem Administrator den Zugriff auf IBM Spectrum Protect.
LOCK NODE	Verhindert, dass ein Client auf den Server zugreift.
QUERY SESSION	Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.

CHECKIN LIBVOLUME (Speicherdatenträger in ein Speicherarchiv zurückstellen)

Mit diesem Befehl kann ein Speicherdatenträger mit sequenziellem Zugriff oder ein Reinigungsband dem Serverdatenträgerbestand für ein automatisiertes Speicherarchiv hinzugefügt werden. Der Server kann einen Datenträger, der sich physisch in einem automatisierten Speicherarchiv befindet, erst verwenden, wenn dieser Datenträger zurückgestellt wurde.

Wichtig:

1. Die Verarbeitung des Befehls CHECKIN LIBVOLUME wartet nicht darauf, dass ein Laufwerk verfügbar wird, auch wenn sich das Laufwerk nur im Status IDLE (Freizustand) befindet. Falls erforderlich, kann ein Speicherarchivlaufwerk verfügbar gemacht werden, indem der Befehl DISMOUNT VOLUME ausgegeben wird, um die Bereitstellung des Datenträgers aufzuheben. Ist ein Speicherarchivlaufwerk verfügbar, geben Sie den Befehl CHECKIN LIBVOLUME erneut aus.
2. In einem externen Speicherarchiv definieren Sie keine Laufwerke, stellen Sie keine Datenträger zurück und kennzeichnen Sie keine Datenträger. Der Server stellt eine Schnittstelle zur Verfügung, die von externen Datenträgerverwaltungssystemen verwendet wird, um mit dem Server zu arbeiten.
3. Werden andere WORM-Bänder als 3592-Bänder zurückgestellt, müssen Sie CHECKLABEL=YES verwenden. Andernfalls werden sie als normale Bänder mit Lese-/Schreibzugriff zurückgestellt.

Dieser Befehl erstellt einen Hintergrundprozess, den Sie mit dem Befehl CANCEL PROCESS abbrechen können. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Ausführliche und aktuelle Informationen zur Laufwerk- und Speicherarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax für SCSI-Speicherarchive

```
>>-CHECKIn LIBVolume--Speicherarchivname------------------------>

                       .-SEARCH--=--No-.
>----+-Datenträgername--+---------------+-+---------------------->
     +-SEARCH-----Yes--+-------+----------+
     |                 '-| A |-'          |
     '-SEARCH---=--Bulk--+-------+---------'
                         '-| A |-'

                            .-OWNer---=--""---------.
>--STATus--=--+-PRIvate-+--+----------------------+-------------->
              +-SCRatch-+  '-OWNer---=--Servername-'
              '-CLEaner-'

   .-CHECKLabel--=--Yes---------.  .-SWAP---=--No------.
>--+----------------------------+--+------------------+--------->
   '-CHECKLabel--=--+-Yes------+-'  '-SWAP---=--+-No--+-'
                    +-No-------+               '-Yes-'
                    '-Barcode-'

   .-WAITTime---=--60---.
>--+--------------------+--+--------------------------+--------><
   '-WAITTime---=--Wert-'  '-CLEanings--=----Anzahl---'

A (SEARCH=Yes, SEARCH=Bulk)

|--+-VOLRange--=-----Datenträgername1,Datenträgername2---+-------|
   |               .-,---------------.                  |
   |               V                 |                  |
   '-VOLList---=--+---Datenträgername-+-+----------------'
                  '-FILE:--Dateiname----'
```

Syntax für 349X-Speicherarchive

```
>>-CHECKIn LIBVolume--Speicherarchivname------------------------>

                       .-SEARCH--=--No-.
>----+-Datenträgername--+---------------+-+---------------------->
     '-SEARCH---=--Yes--+-------+----------'
                        '-| A |-'

                            .-OWNer---=--""---------.
>--STATus--=--+-PRIvate-+--+----------------------+-------------->
              '-SCRatch-'  '-OWNer---=--Servername-'

   .-CHECKLabel--=--Yes-----.
>--+------------------------+--+----------------------+--------->
   '-CHECKLabel--=--+-Yes-+-'  '-DEVType--=--+-3590-+-'
                    '-No--'                  '-3592-'

   .-SWAP--=--No------.  .-WAITTime---=--60---.
>--+------------------+--+------------------+----------------><
   '-SWAP--=--+-No--+-'  '-WAITTime---=--Wert-'
              '-Yes-'

A (SEARCH=Yes)

|--+-VOLRange--=-----Datenträgername1,Datenträgername2---+-------|
   |               .-,---------------.                  |
   |               V                 |                  |
   '-VOLList---=--+---Datenträgername-+-+----------------'
```

```
                '-FILE:--Dateiname----'
```

Syntax für ACSLS-Speicherarchive

```
>>-CHECKIn LIBVolume--Speicherarchivname------------------------>

                        .-SEARCH--=--No-.
>----+-Datenträgername--+---------------+-+--------------------->
     '-SEARCH--=--Yes--+-------+----------'
                       '-| A |-'

                           .-OWNer--=--""---------.
>--STATus--=--+-PRIvate-+--+----------------------+------------->
              '-SCRatch-'  '-OWNer--=--Servername-'

   .-CHECKLabel--=--Yes-----.  .-SWAP--=--No------.
>--+----------------------+--+-----------------+------------->
   '-CHECKLabel--=--+-Yes-+-'  '-SWAP--=--+-No--+-'
                    '-No--'               '-Yes-'

   .-WAITTime--=--60---.
>--+-------------------+--------------------------------------><
   '-WAITTime--=--Wert-'

A (SEARCH=Yes)

|--+-VOLRange--=-----Datenträgername1,Datenträgername2---+-------|
   |               .-,---------------.                  |
   |               V                 |                  |
   '-VOLList--=--+---Datenträgername-+-+----------------'
                 '-FILE:--Dateiname----'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an.

Datenträgername
: Gibt den Datenträgernamen des Speicherdatenträgers an, der zurückgestellt wird. Dieser Parameter ist erforderlich, wenn SEARCH gleich NO ist. Diesen Parameter nicht eingeben, wenn der Parameter SEARCH den Wert YES oder BULK hat. Wird ein Datenträger in ein SCSI-Speicherarchiv mit mehreren Eingangs-/Ausgangsanschlüssen zurückgestellt, wird der Datenträger in dem Schacht mit der niedrigsten Nummer zurückgestellt.

STATus (Erforderlich)
: Gibt den Datenträgerstatus an. Gültige Werte:

  PRIvate
  : Gibt an, dass der Datenträger ein privater Datenträger ist, der nur geladen wird, wenn er mit seinem Namen angefordert wird.

  SCRatch
  : Gibt an, dass der Datenträger ein neuer Arbeitsdatenträger ist. Dieser Datenträger kann geladen werden, um Anforderungen zum Laden eines Arbeitsdatenträgers während Datenspeicheroperationen oder Exportoperationen zu erfüllen.

    Hat ein Datenträger einen Eintrag in der Datenträger-History, können Sie den Datenträger nicht als Arbeitsdatenträger zurückstellen.

  CLEaner
  : Gibt an, dass der Datenträger eine Reinigungskassette und keine Datenkassette ist. Für eine Reinigungskassette ist der Parameter CLEANINGS erforderlich, der auf die Anzahl der Verwendungen der Reinigungskassette gesetzt werden muss.

    Die Angabe CHECKLABEL=YES ist für das Zurückstellen einer Reinigungskassette ungültig. Verwenden Sie STATUS=CLEANER, um eine Reinigungskassette separat von einer Datenkassette zurückzustellen.

OWNer
: Gibt an, welcher Speicherarchivclient der Eigner eines privaten Datenträgers in einem Speicherarchiv ist, das in einem SAN gemeinsam genutzt wird. Der Datenträger, für den das Eigentumsrecht angegeben wird, muss ein privater Datenträger sein. Für einen Arbeitsdatenträger können Sie kein Eigentumsrecht angeben. Außerdem können Sie keinen Eigner angeben, wenn Sie SEARCH=YES oder SEARCH=BULK verwenden.

  Wird der Befehl CHECKIN LIBVOLUME ausgegeben, überprüft der Server den Eigner. Wurde dieser Parameter nicht angegeben, verwendet der Server den Standardwert und übergibt das Datenträgereigentumsrecht an den Speicherarchivclient als Eigner, wie in der Protokolldatei für Datenträger auf dem Speicherarchivmanager aufgezeichnet ist. Hat der Datenträger keinen Speicherarchivclient als Eigner, übergibt der Server das Eigentumsrecht an den Speicherarchivmanager.

SEARCH

Gibt an, ob der Server das Speicherarchiv nach Datenträgern durchsucht, die nicht zurückgestellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Gültige Werte:

No
Gibt an, dass nur der angegebene Datenträger in das Speicherarchiv zurückgestellt wird.

Für SCSI-Speicherarchive: Der Server gibt die Anforderung aus, den Datenträger in einen Kassettenschacht in dem Speicherarchiv oder, falls verfügbar, in einen Eingangsanschluss einzulegen. Der Kassettenschacht oder Eingangsanschluss wird durch die Elementadresse identifiziert. **Für 349X-Speicherarchive:** Der Datenträger befindet sich möglicherweise bereits in dem Speicherarchiv oder Sie können ihn bei Aufforderung in die E/A-Station einlegen.

Yes
Gibt an, dass der Server das Speicherarchiv nach Datenträgern durchsucht, die zurückgestellt werden sollen. Sie können den Parameter VOLRANGE oder VOLLIST verwenden, um die Suche zu begrenzen. Bei Verwendung dieses Parameters sind die folgenden Einschränkungen zu berücksichtigen:

- Wird das Speicherarchiv von Anwendungen gemeinsam genutzt, kann der Server einen Datenträger untersuchen, der von einer anderen Anwendung benötigt wird. Bei 349X-Speicherarchiven fragt der Server den Speicherarchivmanager nach allen Datenträgern ab, die der Kategorie SCRATCH oder PRIVATE und der Kategorie INSERT zugeordnet sind.
- Für SCSI-Speicherarchive dürfen Sie nicht SEARCH=YES und CHECKLABEL=NO in demselben Befehl angeben.

Bulk
Gibt an, dass der Server die Eingangs-/Ausgangsanschlüsse des Speicherarchivs nach Datenträgern durchsucht, die automatisch zurückgestellt werden können. Diese Option gilt nur für SCSI-Speicherarchive.
Wichtig:

1. Sie dürfen CHECKLABEL=NO und SEARCH=BULK nicht gleichzeitig angeben.
2. Sie können den Parameter VOLRANGE oder VOLLIST verwenden, um die Suche zu begrenzen.

VOLRange
Gibt einen Bereich von Datenträgernamen an, die durch Kommas voneinander getrennt sind. Sie können diesen Parameter verwenden, um die Suche nach Datenträgern zu begrenzen, die zurückgestellt werden sollen, wenn SEARCH=YES (349X-, ACSLS- und SCSI-Speicherarchive) oder SEARCH=BULK (nur SCSI-Speicherarchive) angegeben wird. Sind keine Datenträger in dem Speicherarchiv vorhanden, die sich in dem angegebenen Bereich befinden, wird der Befehl ohne Fehler beendet.

Geben Sie nur Datenträgernamen an, die numerisch erhöht werden können. Neben dem Bereich für den Erhöhungswert kann ein Datenträgername ein alphanumerisches Präfix und ein alphanumerisches Suffix enthalten.

Parameter	**Beschreibung**
`volrange=bar110,bar130`	Die 21 Datenträger werden zurückgestellt: bar110, bar111, bar112,...bar129, bar130.
`volrange=bar11a,bar13a`	Die 3 Datenträger werden zurückgestellt: bar11a, bar12a, bar13a.
`volrange=123400,123410`	Die 11 Datenträger werden zurückgestellt: 123400, 123401, ...123409, 123410.

VOLList
Gibt eine Liste mit Datenträgern an. Sie können diesen Parameter verwenden, um die Suche nach Datenträgern zu begrenzen, die zurückgestellt werden sollen, wenn SEARCH=YES (349X-, ACSLS- und SCSI-Speicherarchive) oder SEARCH=BULK (nur SCSI-Speicherarchive) angegeben wird. Sind in dem Speicherarchiv keine Datenträger vorhanden, die sich in der Liste befinden, wird der Befehl ohne Fehler beendet.
Gültige Werte:

Datenträgername
Gibt einen oder mehrere Datenträgernamen an, die durch Kommas und ohne Leerzeichen voneinander getrennt sind. Beispiel: VOLLIST=TAPE01,TAPE02.

FILE:Dateiname
Gibt den Namen einer Datei an, die eine Liste der Datenträger für den Befehl enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert. Um beispielsweise die Datenträger TAPE01, TAPE02 und TAPE03 zu verwenden, erstellen Sie die Datei TAPEVOL, die die folgenden Zeilen enthält:

```
TAPE01
TAPE02
TAPE03
```

Die Datenträger können für den Befehl wie folgt angegeben werden: VOLLIST=FILE:TAPEVOL.

Achtung: Bei dem Dateinamen muss die Groß-/Kleinschreibung beachtet werden.

CHECKLabel
Gibt an, wie oder ob der Server Kennsätze sequenzieller Datenträger lesen soll. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

Yes
Gibt an, dass während des Zurückstellens versucht wird, den Datenträgerkennsatz zu lesen.
Achtung:

1. Für SCSI-Speicherarchive dürfen Sie nicht SEARCH=YES und CHECKLABEL=NO in demselben Befehl angeben.
2. Für andere WORM-Datenträger als 3592 müssen Sie YES angeben.

No
Gibt an, dass der Datenträgerkennsatz während des Zurückstellens nicht gelesen wird. Das Unterdrücken der Kennsatzprüfung kann jedoch später zu Fehlern führen (z. B. kann ein falscher Kennsatz oder ein nicht richtig gekennzeichneter Datenträger Fehler verursachen). Geben Sie für 349X- und ACSLS-Speicherarchive NO an, um das Laden von Kassetten in ein Laufwerk zum Lesen des Datenträgerkennsatzes zu vermeiden. Diese Speicherarchive geben immer die Informationen zu externen Kennsätzen für Kassetten zurück. Diese Informationen werden von IBM Spectrum Protect verwendet.

Barcode
Gibt an, dass der Server das Barcodeetikett liest, wenn das Speicherarchiv über einen Barcodeleser verfügt und die Datenträger externe Barcodeetikett haben. Die Zeit für das Zurückstellen kann durch die Verwendung des Barcodes verkürzt werden. Dieser Parameter gilt nur für SCSI-Speicherarchive.

Kann der Barcodeleser das Barcodeetikett nicht lesen oder verfügt das Band über kein Barcodeetikett, lädt der Server das Band und liest den internen Kennsatz.

DEVType
Gibt den Einheitentyp des Datenträgers an, der zurückgestellt wird. Dieser Parameter ist erforderlich, wenn keines der Laufwerke in diesem Speicherarchiv über definierte Pfade verfügt.

3590
Gibt an, dass der Einheitentyp des Datenträgers, der zurückgestellt wird, 3590 ist.

3592
Gibt an, dass der Einheitentyp des Datenträgers, der zurückgestellt wird, 3592 ist.

SWAP
Gibt an, ob der Server Datenträger auslagert, wenn kein leerer Speicherarchivschacht verfügbar ist. Der für die Auslagerungsoperation ausgewählte Datenträger (Zielauslagerungsdatenträger) wird aus dem Speicherarchiv ausgegeben und durch den zurückgestellten Datenträger ersetzt. Der Server identifiziert einen Zielauslagerungsdatenträger, indem nach einem verfügbaren Arbeitsdatenträger gesucht wird. Ist keiner vorhanden, identifiziert der Server den am wenigsten geladenen Datenträger.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Dieser Parameter ist nur gültig, wenn in dem Befehl ein Datenträgername angegeben ist. Gültige Werte:

No
Gibt an, dass der Server den Datenträger nur zurückstellt, wenn ein leerer Schacht verfügbar ist.

Yes
Gibt an, dass der Server Kassetten auslagert, um den Datenträger zurückzustellen, wenn kein leerer Schacht verfügbar ist.

WAITTime
Gibt die Anzahl Minuten an, die der Server auf Ihre Antwort auf eine Anforderung wartet. Geben Sie einen Wert im Bereich 0-9999 an. Möchten Sie vom Server zur Eingabe aufgefordert werden, geben Sie eine Wartezeit größer als Null an. Der Standardwert ist 60 Minuten. Angenommen, Sie werden vom Server aufgefordert, ein Band in den Eingangs-/Ausgangsanschluss eines Speicherarchivs einzulegen. Haben Sie eine Wartezeit von 60 Minuten angegeben, gibt der Server eine Anforderung aus und wartet 60 Minuten auf Ihre Antwort. Angenommen, Sie haben dagegen eine Wartezeit von 0 angegeben. Wenn Sie bereits ein Band eingelegt haben, hat eine Wartezeit mit dem Wert Null zur Folge, dass die Operation ohne Aufforderung fortgesetzt wird. Haben Sie *kein* Band eingelegt, hat eine Wartezeit mit dem Wert Null zur Folge, dass die Operation fehlschlägt.

CLEanings
Den empfohlenen Wert für die einzelne Reinigungskassette eingeben (ist normalerweise auf der Kassette angegeben). Reinigungen gelten nur für SCSI-Speicherarchive. Dieser Parameter ist bei der Angabe von STATUS=CLEANER erforderlich.

Werden mehrere Reinigungskassetten in das Speicherarchiv zurückgestellt, wird nur eine Reinigungskassette verwendet, bis ihr Wert für den Parameter CLEANINGS den Wert Null erreicht hat. Anschließend wird eine andere Reinigungskassette ausgewählt, und die erste Reinigungskassette kann entnommen und entsorgt werden.

Beispiel: Einen Datenträger in ein SCSI-Speicherarchiv zurückstellen

Stellen Sie den Datenträger `WPDV00` in das SCSI-Speicherarchiv AUTO zurück.

```
checkin libvolume auto wpdv00 status=scratch
```

Beispiel: Einen Barcodeleser verwenden, um ein Speicherarchiv nach einer Reinigungskassette zu durchsuchen

Durchsuchen Sie das SCSI-Speicherarchiv AUTOLIB1 und suchen Sie unter Verwendung des Barcodelesers nach der Reinigungskassette CLNV. SEARCH=YES verwenden, aber die Suche mit dem Parameter VOLLIST eingrenzen.

```
checkin libvolume autolib1 search=yes vollist=cleanv status=cleaner
  cleanings=10 checklabel=barcode
```

Beispiel: Ein Speicherarchiv durchsuchen, um nicht verwendete Datenträger in einem bestimmten Bereich in den Arbeitsdatenträgerstatus (SCRATCH) zu versetzen

Durchsuchen Sie das 349X-Speicherarchiv ABC und begrenzen Sie die Suche auf einen Bereich nicht verwendeter Datenträger BAR110 bis BAR130 und versetzen Sie die Datenträger in den Arbeitsdatenträgerstatus (SCRATCH).

```
checkin libvolume abc search=yes volrange=bar110,bar130
  status=scratch
```

Beispiel: Ein Speicherarchiv durchsuchen, um einen bestimmten Datenträger in den Arbeitsdatenträgerstatus (SCRATCH) zu versetzen

Verwenden Sie den Barcodeleser, um das SCSI-Speicherarchiv MYLIB nach VOL1 zu durchsuchen, und versetzen Sie den Datenträger in den Arbeitsdatenträgerstatus (SCRATCH).

```
checkin libvolume mylib search=yes vollist=vol1 status=scratch
  checklabel=barcode
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CHECKIN LIBVOLUME

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
DISMOUNT VOLUME	Entlädt einen sequenziellen entfernbaren Datenträger anhand des Datenträgernamens.
LABEL LIBVOLUME	Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY LIBVOLUME	Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
REPLY	Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.
UPDATE LIBVOLUME	Ändert den Status eines Speicherdatenträgers.

CHECKOUT LIBVOLUME (Speicherdatenträger aus Kassettenarchiv entnehmen)

Mit diesem Befehl kann ein Speicherdatenträger mit sequenziellem Zugriff aus dem Serverdatenträgerbestand für ein automatisiertes Kassettenarchiv entfernt werden. Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Einschränkungen:

1. Bei der Entnahmeverarbeitung wird nicht darauf gewartet, dass ein Laufwerk verfügbar wird, auch wenn sich das Laufwerk im Status IDLE befindet. Falls erforderlich, können Sie ein Kassettenarchivlaufwerk verfügbar machen, indem der Datenträger mit dem Befehl DISMOUNT VOLUME entladen wird. Sobald ein Laufwerk verfügbar ist, kann der Befehl CHECKOUT LIBVOLUME erneut ausgegeben werden.
2. Bevor Datenträger aus einem 349X-Kassettenarchiv entnommen werden, stellen Sie sicher, dass die 349x-Kassetteneingabe- und -ausgabeeinrichtung über genügend leere Schächte für die Datenträger verfügt, die entnommen werden sollen. Der 3494-Kassettenarchivmanager (Library Manager) teilt einer Anwendung nicht mit, dass die Kassetteneingabe- und -ausgabeeinrichtung voll ist. Er akzeptiert Anforderungen zur Ausgabe einer Kassette und wartet, bis die Kassetteneingabe- und -ausgabeeinrichtung geleert wurde, bevor zum Server zurückgekehrt wird. IBM Spectrum Protect scheint in diesem Fall zu blockieren. Überprüfen Sie das Kassettenarchiv und löschen Sie alle Aufforderungen zum Eingriff.
3. Bevor Datenträger aus einem ACSLS-Kassettenarchiv entnommen werden, stellen Sie sicher, dass die CAP-Priorität in ACSLS größer als Null ist. Ist die CAP-Priorität Null, müssen Sie in dem Befehl CHECKOUT LIBVOLUME einen Wert für den CAP-Parameter angeben.

Ausführliche und aktuelle Informationen zur Laufwerk- und Speicherarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax für SCSI-Speicherarchiv

```
>>-CHECKOut LIBVolume--Speicherarchivname----------------------->

                           .-REMove--=--Bulk-----.
>----+-Datenträgername-+----+---------------------+------------->
     '-| A |-----------'    '-REMove--=--+-Yes--+-'
                                        +-No---+
                                        '-Bulk-'

   .-CHECKLabel--=--Yes-----.  .-FORCE--=--No------.
>--+-------------------------+--+-------------------+----------><
   '-CHECKLabel--=--+-Yes-+-'  '-FORCE--=--+-No--+-'
                    '-No--'                '-Yes-'

A

|--+-VOLRange--=----Datenträgername1,Datenträgername2---+-------|
   |               .-,---------------.                  |
   |               V                 |                  |
   '-VOLList--=--+---Datenträgername-+-+----------------'
                 '-FILE:--Dateiname----'
```

Syntax für 349X-Kassettenarchiv

```
>>-CHECKOut LIBVolume--Speicherarchivname----------------------->

                           .-REMove--=--Bulk-----.
>----+-Datenträgername-+----+---------------------+------------><
     '-| A |-----------'    '-REMove--=--+-Yes--+-'
                                        +-No---+
                                        '-Bulk-'

A

|--+-VOLRange--=----Datenträgername1,Datenträgername2---+-------|
   |               .-,---------------.                  |
   |               V                 |                  |
   '-VOLList--=--+---Datenträgername-+-+----------------'
                 '-FILE:--Dateiname----'
```

Syntax für ACSLS-Kassettenarchiv

```
>>-CHECKOut LIBVolume--Speicherarchivname----------------------->

                            .-REMove--=--Yes------.
>----+-Datenträgername-+----+---------------------+------------->
     '-| A |-----------'    '-REMove--=--+-Yes--+-'
                                        +-No---+
                                        '-Bulk-'

>--+-------------------+---------------------------------------><
   '-CAP--=----x,y,z---'

A

|--+-VOLRange--=-----Datenträgername1,Datenträgername2---+-------|
   |               .-,---------------.                  |
   |               V                 |                  |
   '-VOLList--=---+---Datenträgername-+-+----------------'
                  '-FILE:--Dateiname----'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an.

Datenträgername
: Gibt den Datenträgernamen an.

VOLRange
: Gibt zwei Datenträgernamen an, die durch ein Komma voneinander getrennt sind. Dieser Parameter gibt einen Bereich von Datenträgern an, die entnommen werden sollen. Sind keine Datenträger in dem Kassettenarchiv vorhanden, die sich in dem angegebenen Bereich befinden, wird der Befehl ohne Fehler beendet.

  Geben Sie nur Datenträgernamen an, die numerisch erhöht werden können. Neben dem Bereich für den Erhöhungswert kann ein Datenträgername ein alphanumerisches Präfix und ein alphanumerisches Suffix enthalten.

Parameter	Beschreibung
`volrange=bar110,bar130`	Die 21 Datenträger werden entnommen: bar110, bar111, bar112,...bar129, bar130.
`volrange=bar11a,bar13a`	Die 3 Datenträger werden entnommen: bar11a, bar12a, bar13a.
`volrange=123400,123410`	Die 11 Datenträger werden entnommen: 123400, 123401, ...123409, 123410.

VOLList
: Gibt eine Liste mit Datenträgern an, die entnommen werden sollen. Sind keine Datenträger in dem Kassettenarchiv vorhanden, die sich in der Liste befinden, wird der Befehl ohne Fehler beendet.

  Gültige Werte:

  Datenträgername
  : Gibt die Namen der Datenträger an, die für den Befehl verwendet werden. Beispiel: VOLLIST=TAPE01,TAPE02.

  FILE: Dateiname
  : Gibt den Namen einer Datei an, die eine Liste der Datenträger für den Befehl enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert. Um beispielsweise die Datenträger TAPE01, TAPE02 und TAPE03 zu verwenden, erstellen Sie die Datei TAPEVOL, die die folgenden Zeilen enthält:

    ```
    TAPE01
    TAPE02
    TAPE03
    ```

    Die Datenträger können für den Befehl wie folgt angegeben werden: VOLLIST=FILE:TAPEVOL.

    Achtung: Bei dem Dateinamen muss die Groß-/Kleinschreibung beachtet werden.

REMove
: Gibt an, dass der Server versucht, den Datenträger aus dem Kassettenarchiv in die Serviceein-/-ausgabestation oder die Eingangs-/Ausgangsanschlüsse zu versetzen. Dieser Parameter ist wahlfrei. Abhängig vom Kassettenarchivtyp sind die gültigen Werte YES, BULK und NO. Die Antwort des Servers auf jede dieser Optionen und die Standardwerte werden in den folgenden Abschnitten beschrieben.
  349X-Kassettenarchive: Der Standardwert ist BULK. Die folgende Tabelle zeigt, wie der Server für 349X-Kassettenarchive antwortet.

Tabelle 1. Antwort des Servers für 349X-Kassettenarchive

REMOVE=YES	REMOVE=BULK	REMOVE=NO
Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Serviceein-/-ausgabestation aus.	Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Ausgabeeinrichtung mit hoher Speicherkapazität aus.	Der 3494-Kassettenarchivmanager (Library Manager) gibt den Datenträger nicht aus. Der Server lässt die Kassette für die Verwendung durch andere Anwendungen in dem Kassettenarchiv in der Kategorie INSERT.

SCSI-Kassettenarchive: Der Standardwert ist BULK. Die folgende Tabelle zeigt, wie der Server für ein SCSI-Kassettenarchiv antwortet.

Tabelle 2. Antwort des Servers für SCSI-Kassettenarchive

Wenn ein Kassettenarchiv . . .	Und REMOVE=YES, dann...	Und REMOVE=BULK, dann...	Und REMOVE=NO, dann...
Keine Eingangs-/Ausgangsanschlüsse hat	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.
Eingangs-/Ausgangsanschlüsse *hat* und ein Eingangs-/Ausgangs*anschluss verfügbar ist*	Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an. Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.	Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.
Eingangs-/Ausgangsanschlüsse *hat*, aber *keine Anschlüsse verfügbar sind*	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.	Wartet der Server auf einen verfügbaren Eingangs-/Ausgangsanschluss.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.

ACSLS-Kassettenarchive: Der Standardwert ist YES. Wenn der Parameter auf YES gesetzt wird und der Kassettenzugriffsport (CAP, Cartridge Access Port) den Prioritätswert 0 für die automatische Auswahl hat, müssen Sie eine CAP-ID angeben. Die folgende Tabelle zeigt, wie der Server für ACSLS-Kassettenarchive antwortet.

Tabelle 3. Antwort des Servers für ACSLS-Kassettenarchive

REMOVE=YES oder REMOVE=BULK	REMOVE=NO
Der Server gibt die Kassette an die Serviceein-/-ausgabestation aus und löscht den Datenträgereintrag aus dem Datenträgerbestand im Kassettenarchiv des Servers.	Der Server gibt die Kassette nicht aus. Der Server löscht den Datenträgereintrag aus dem Kassettenarchivbestand des Servers und lässt den Datenträger in dem Kassettenarchiv.

CHECKLabel

Gibt an, wie oder ob der Server Kennsätze sequenzieller Datenträger liest.
Achtung: Dieser Parameter gilt nicht für Kassettenarchive IBM® 349X oder ACSLS.
Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

Yes

Gibt an, daß der Server versucht, den Datenträgerkennsatz zu lesen, um sicherzustellen, daß der korrekte Datenträger entnommen wird.

No
Gibt an, daß der Datenträgerkennsatz während der Entnahme nicht gelesen wird. Da der Lesevorgang entfällt, verbessert sich die Leistung.

FORCE
Gibt an, ob der Server einen Datenträger entnimmt, wenn beim Lesen des Kennsatzes ein Ein-/Ausgabefehler auftritt.
Achtung: Dieser Parameter gilt nicht für Kassettenarchive IBM 349X oder ACSLS.
Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No
Der Server entnimmt keinen Speicherdatenträger, wenn beim Lesen des Kennsatzes ein E/A-Fehler auftritt.
Yes
Der Server entnimmt den Speicherdatenträger, auch wenn ein E/A-Fehler auftritt.

CAP
Gibt an, welcher Cartridge Access Port (CAP) für die Ausgabe von Datenträgern verwendet werden soll, wenn REMOVE=YES angegeben wird. Dieser Parameter gilt nur für Datenträger in ACSLS-Kassettenarchiven. Wenn der CAP-Prioritätswert in dem Kassettenarchiv auf 0 gesetzt wird, ist dieser Parameter erforderlich. Ist ein CAP-Prioritätswert größer als Null in dem Kassettenarchiv definiert, ist dieser Parameter optional. Standardmäßig haben alle CAPs anfänglich den Prioritätswert 0, der bedeutet, dass ACSLS nicht automatisch den Kassettenzugriffsport auswählt.
Zum Anzeigen der gültigen CAP-Kennungen (*x,y,z*) geben Sie den Befehl QUERY CAP mit der Option ALL von der ACSSA-Konsole (ACSSA = Automated Cartridge System System Administrator) auf dem ACSLS-Server-Host aus. Die Kennungen sind:

x
Die ACS-ID (ACS = Automated Cartridge System). Diese Kennung kann eine Zahl im Bereich von 0 bis 126 sein.
y
Die LSM-ID (LSM = Library Storage Module). Diese Kennung kann eine Zahl im Bereich von 0 bis 23 sein.
z
Die CAP-ID. Diese Kennung kann eine Zahl im Bereich von 0 bis 11 sein.

Weitere Informationen enthält die StorageTek-Dokumentation.

Beispiel: Einen Datenträger entnehmen und den Kennsatz prüfen

Den Datenträger mit dem Namen EXB004 aus dem Kassettenarchiv FOREST entnehmen. Den Kennsatz lesen, um den Datenträgernamen zu prüfen, den Datenträger aber nicht aus dem Kassettenarchiv entfernen.

```
checkout libvolume forest exb004 checklabel=yes remove=no
```

Zugehörige Befehle

Tabelle 4. Zugehörige Befehle für CHECKOUT LIBVOLUME

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
CHECKIN LIBVOLUME	Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
LABEL LIBVOLUME	Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY LIBVOLUME	Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
REPLY	Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.
UPDATE LIBVOLUME	Ändert den Status eines Speicherdatenträgers.

CLEAN DRIVE (Laufwerk reinigen)

Verwenden Sie diesen Befehl, wenn IBM Spectrum Protect unabhängig von der Reinigungshäufigkeit sofort eine Reinigungskassette in ein Laufwerk laden soll.

Es gibt einige Besonderheiten, die beachtet werden müssen, wenn dieser Befehl für ein SCSI-Kassettenarchiv verwendet werden soll, das eine automatische Laufwerkreinigung in seiner Einheitenhardware zur Verfügung stellt.

Einschränkung: Sie können den Befehl CLEAN DRIVE nicht für ein Laufwerk ausführen, dessen einzige Pfadquelle ein NAS-Dateiserver ist.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-CLEAN DRIVE--Kassettenarchivname--Laufwerkname-------------><
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, dem das Laufwerk zugeordnet ist.

Laufwerkname (Erforderlich)
: Gibt den Namen des Laufwerks an.

Beispiel: Ein bestimmtes Bandlaufwerk reinigen

Sie haben bereits mit dem Befehl DEFINE LIBRARY ein Kassettenarchiv mit dem Namen AUTOLIB definiert und mit dem Befehl CHECKIN LIBVOL eine Reinigungskassette in das Kassettenarchiv zurückgestellt. Dem Server mitteilen, daß TAPEDRIVE3 in diesem Kassettenarchiv gereinigt werden muß.

```
clean drive autolib tapedrive3
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für CLEAN DRIVE

Befehl	Beschreibung
CHECKIN LIBVOLUME	Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DELETE DRIVE	Löscht ein Laufwerk aus einem Kassettenarchiv.
QUERY DRIVE	Zeigt Informationen zu Laufwerken an.
UPDATE DRIVE	Ändert die Attribute eines Laufwerks.

COMMIT (Festschreiben von Befehlen in einem Makro steuern)

Mit diesem Befehl kann das Festschreiben eines Befehls in einem Makro gesteuert und die Datenbank nach der Verarbeitung von Befehlen aktualisiert werden. Wird dieser Befehl im Konsolenmodus des Verwaltungsclients ausgegeben, wird keine Nachricht generiert.

Tritt während der Verarbeitung der Befehle in einem Makro ein Fehler auf, stoppt der Server die Verarbeitung des Makros und macht alle Änderungen (seit dem letzten COMMIT) rückgängig. Wenn ein Befehl festgeschrieben worden ist, kann er nicht rückgängig gemacht werden.

Wenn die Befehlsverarbeitung gesteuert werden soll, ist sicherzustellen, dass in der Verwaltungsclientsitzung nicht die Option ITEMCOMMIT verwendet wird. Mit der Option ITEMCOMMIT werden Befehle innerhalb eines Scripts oder eines Makros festgeschrieben, während *jeder* Befehl verarbeitet wird.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-COMMIT-----------------------------------------------------><
```

Parameter

Keine.

Beispiel: Festschreiben von Befehlen in einem Makro steuern

Im interaktiven Modus des Verwaltungs-Clients mit dem Makro REG.ADM neue Administratoren registrieren und eine Berechtigung erteilen. Die Änderungen werden festgeschrieben, nachdem die Administratoren registriert worden sind und ihnen eine Berechtigung erteilt worden ist.

Makroinhalt:

```
/* REG.ADM-Maßnahmenadmin. registrieren & Berechtigung erteilen*/
REGister Admin sara hobby
GRant AUTHority sara CLasses=Policy
COMMIT  /* Änderungen festschreiben */REGister Admin ken plane
GRant AUTHority ken CLasses=Policy
COMMIT  /* Änderungen festschreiben */
```

Befehl

```
macro reg.adm
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COMMIT

Befehl	Beschreibung
MACRO	Führt eine angegebene Makrodatei aus.
ROLLBACK	Löscht alle Änderungen, die seit dem letzten COMMIT nicht in der Datenbank festgeschrieben wurden.

Zugehörige Konzepte:
Makros des Verwaltungsclients
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

CONVERT STGPOOL (Speicherpool in einen Containerspeicherpool konvertieren)

Mit diesem Befehl können Sie einen primären Speicherpool, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Verzeichniscontainerspeicherpool oder einen Cloud-Containerspeicherpool konvertieren. Sie können Containerspeicherpools sowohl für die Inline-Datendeduplizierung als auch für die clientseitige Datendeduplizierung verwenden.

Einschränkungen: Die folgenden Einschränkungen gelten für die Speicherpoolkonvertierung:

- Sie können einen Speicherpool nur einmal konvertieren.
- Sie können den Speicherpool während der Konvertierungsverarbeitung nicht aktualisieren. Umlagerungs- und Datenversetzungsprozesse sind nicht verfügbar.
- Sie müssen alle Maßnahmen aktualisieren, um sicherzustellen, dass das Ziel einen Speicherpool angibt, der nicht konvertiert ist oder gerade konvertiert wird.

Während der Konvertierungsverarbeitung werden alle Daten aus dem Quellenspeicherpool in den Zielspeicherpool versetzt. Wenn der Prozess abgeschlossen ist, ist der Quellenspeicherpool nicht mehr verfügbar. Wenn ein Speicherpool nicht verfügbar ist, können Sie keine Daten in den Speicherpool schreiben. Der Quellenspeicherpool kann für das Löschen ausgewählt werden, aber er wird nicht automatisch gelöscht. Bei Bedarf können Sie Daten aus dem Quellenspeicherpool zurückschreiben.
Achtung: Während der Speicherpoolkonvertierung werden Daten aus Kopienspeicherpools und Speicherpools für aktive Daten gelöscht. Diese Aktion wird auch dann ausgeführt, wenn Sie die Anzahl der Tage angegeben haben, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann.

Berechtigungsklasse

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-CONvert STGpool--Quellenspeicherpool--Zielspeicherpool------->

   .-MAXPRocess--=--8----------.
>--+--------------------------+--+---------------------+----->><
   '-MAXPRocess--=----Anzahl---'  '-DUration--=--Minuten-'
```

Parameter

Quellenspeicherpool (Erforderlich)
: Geben Sie einen primären Speicherpool an, der eine Dateieinheitenklasse, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) für die Sicherungs- und Archivierungsverarbeitung verwendet. Dieser Parameter ist erforderlich.

Zielspeicherpool (Erforderlich)
: Geben Sie den Namen eines vorhandenen Verzeichniscontainerspeicherpools oder Cloud-Containerspeicherpools an, in den der Speicherpool konvertiert wird. Dieser Parameter ist erforderlich, wenn Sie zum ersten Mal diesen Befehl ausgeben.
Tipp: Wenn Sie die Speicherpoolkonvertierung erneut starten und der Zielspeicherpool von dem Wert abweicht, der bei der ersten Ausgabe des Befehls CONVERT STGPOOL angegeben wurde, schlägt der Befehl fehl.

MAXPRocess
: Gibt die maximale Anzahl paralleler Prozesse für die Konvertierung von Daten in dem Speicherpool an. Dieser Parameter ist wahlfrei. Sie können eine Zahl im Bereich von 1 bis 99 angeben. Der Standardwert ist 8.
Tipp: Änderungen des Standardwerts werden automatisch gespeichert. Wenn Sie die Speicherpoolkonvertierung erneut starten und der Parameterwert von dem Wert abweicht, der bei der ersten Ausgabe des Befehls CONVERT STGPOOL angegeben wurde, wird der zuletzt angegebene Wert verwendet.

DUration
: Gibt die maximale Anzahl Minuten an, die eine Konvertierung ausgeführt wird, bevor sie abgebrochen wird. Wenn die angegebene Anzahl Minuten verstrichen ist, bricht der Server alle Konvertierungsprozesse für den Speicherpool ab. Sie können eine Zahl im Bereich von 1 bis 9999 angeben. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird die Konvertierung bis zum Abschluss ausgeführt.
Tipp: Die Ausführung der Speicherpoolkonvertierung für große Speicherpools kann Tage dauern. Verwenden Sie diesen Parameter, um die Zeit für die Speicherpoolkonvertierung täglich zu begrenzen. Als Best Practice sollten Sie die Konvertierung für mindestens 2 Stunden für einen Speicherpool, der eine Einheitenklasse FILE verwendet, und für mindestens 4 Stunden für ein VTL planen.

Beispiel: Einen Speicherpool konvertieren und eine maximale Anzahl Prozesse angeben

Konvertieren Sie einen Speicherpool mit dem Namen DEDUPPOOL1, versetzen Sie die Daten in einen Containerspeicherpool mit dem Namen DIRPOOL1 und geben Sie 25 als maximale Anzahl Prozesse an.

```
convert stgpool deduppool1 dirpool1 maxprocess=25
```

Tabelle 1. Zugehörige Befehle für CONVERT STGPOOL

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY CLEANUP	Fragt den Bereinigungsstatus eines Quellenspeicherpools ab.
QUERY CONVERSION	Fragt den Konvertierungsstatus eines Speicherpools ab.
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.
REMOVE DAMAGED	Entfernt beschädigte Daten aus einem Quellenspeicherpool.

COPY-Befehle

Mit den COPY-Befehlen kann eine Kopie von IBM Spectrum Protect-Objekten oder -Daten erstellt werden.

- COPY ACTIVEDATA (Aktive Sicherungsdaten aus einem primären Speicherpool in einen Pool für aktive Daten kopieren)
- COPY CLOPTSET (Clientoptionsgruppe kopieren)
- COPY DOMAIN (Maßnahmendomäne kopieren)
- COPY MGMTCLASS (Verwaltungsklasse kopieren)
- COPY POLICYSET (Maßnahmengruppe kopieren)
- COPY PROFILE (Profil kopieren)
- COPY SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl kopieren)
- COPY SCRIPT (IBM Spectrum Protect-Prozedur kopieren)
- COPY SERVERGROUP (Server-Gruppe kopieren)

COPY ACTIVEDATA (Aktive Sicherungsdaten aus einem primären Speicherpool in einen Pool für aktive Daten kopieren)

Mit diesem Befehl können aktive Versionen von Sicherungsdaten aus einem primären Speicherpool in einen Pool für aktive Daten kopiert werden. Der primäre Vorteil von Pools für aktive Daten sind schnelle Clientzurückschreibungen. Kopieren Sie Ihre aktiven Daten regelmäßig, um sicherzustellen, dass die Daten in einem Katastrophenfall geschützt sind.

Ist eine Datei bereits in dem Pool für aktive Daten vorhanden, wird die Datei nicht kopiert, es sei denn, die Kopie der Datei in dem Pool für aktive Daten ist als beschädigt markiert. Es wird jedoch keine neue Kopie erstellt, wenn die Datei in dem primären Speicherpool auch als beschädigt

markiert ist. In einem Speicherpool mit wahlfreiem Zugriff werden weder Cache-Kopien von umgelagerten Dateien noch beschädigte Primärdateien kopiert.

Wenn die Umlagerung für einen Speicherpool beginnt, während aktive Daten kopiert werden, werden einige Dateien möglicherweise umgelagert, bevor sie kopiert werden. Aus diesem Grund sollten Sie aktive Daten aus Speicherpools, die sich an einer höheren Position in der Umlagerungshierarchie befinden, vor den aktiven Daten aus Speicherpools kopieren, die sich an einer niedrigeren Position befinden. Stellen Sie sicher, dass ein Kopierprozess beendet ist, bevor ein anderer Kopierprozess beginnt.

Hinweis:

- Sie können nur aktive Daten aus Speicherpools kopieren, die das Datenformat NATIVE oder NONBLOCK haben.
- Wird dieser Befehl für einen primären Speicherpool ausgegeben, der für die Deduplizierung von Daten definiert ist, werden doppelte Daten entfernt, wenn der Pool für aktive Daten ebenfalls für die Deduplizierung von Daten definiert ist.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Pool für aktive Daten erforderlich, aus dem aktive Versionen von Sicherungsdaten kopiert werden.

Syntax

```
>>-COPY ACTIVEdata--Name_des_primären_Pools--Name_des_Pools_für_aktive_Daten-->

   .-MAXProcess--=--1----------.
>--+---------------------------+-------------------------------->
   '-MAXProcess--=----Anzahl---'

   .-Preview--=--No-----------------.  .-Wait--=--No------.
>--+---------------------------------+--+-----------------+---->
   '-Preview--=--+-No--------------+-'  '-Wait--=--+-No--+-'
                 +-Yes-------------+               '-Yes-'
                 |             (1) |
                 '-VOLumesonly-----'

   .-SHREDTONOshred--=--No------.
>--+---------------------------+------------------------------><
   '-SHREDTONOshred--=--+-No--+-'
                        '-Yes-'
```

Anmerkungen:

1. Der Parameter VOLUMESONLY gilt nur für Speicherpools mit sequenziellem Zugriff.

Parameter

Name_des_primären_Pools (Erforderlich)
: Gibt den primären Speicherpool an.

Name_des_Pools_für_aktive_Daten (Erforderlich)
: Gibt den Pool für aktive Daten an.

MAXProcess
: Gibt die maximale Anzahl paralleler Prozesse an, die für das Kopieren von Dateien verwendet werden. Dieser Parameter ist wahlfrei. Einen Wert zwischen 1 und 999 eingeben. Der Standardwert ist 1.

  Die Verwendung mehrerer paralleler Prozesse kann den Durchsatz für den Befehl COPY ACTIVEDATA verbessern. Die Erwartung ist die, dass die für das Kopieren der aktiven Daten benötigte Zeit verringert wird, indem mehrere Prozesse verwendet werden. Sind mehrere Prozesse aktiv, müssen jedoch in einigen Fällen ein oder mehrere Prozesse auf die Verwendung eines Datenträgers warten, der bereits von einem anderen COPY ACTIVEDATA-Prozess verwendet wird.

  Bei der Bestimmung dieses Werts ist die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden kann. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet der Server einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von anderen Server- und Systemaktivitäten sowie von den Mountlimits der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die vom Kopieren aktiver Daten betroffen sind.

  Jeder Prozess benötigt einen Mountpunkt für Datenträger des Pools für aktive Daten und, falls der Einheitentyp nicht FILE lautet, außerdem ein Laufwerk. Werden aktive Daten aus einem Speicherpool mit sequenziellem Zugriff kopiert, benötigt jeder Prozess einen zusätzlichen Mountpunkt für Datenträger des primären Speicherpools und, falls der Einheitentyp nicht FILE lautet, ein zusätzliches Laufwerk. Beispiel: Angenommen, es werden maximal 3 Prozesse für das Kopieren eines primären sequenziellen Speicherpools in einen Pool für aktive Daten mit derselben Einheitenklasse angegeben. Jeder Prozess benötigt zwei Mountpunkte und zwei Laufwerke. Um alle drei Prozesse ausführen zu können, muss der Grenzwert für Ladeanforderungen für die Einheitenklasse mindestens sechs betragen, und es müssen mindestens sechs Mountpunkte und sechs Laufwerke verfügbar sein.

Für die Verwendung des Parameters PREVIEW wird nur ein Prozess verwendet, und es werden keine Mountpunkte oder Laufwerke benötigt.

Preview
Gibt an, ob das Kopieren aktiver Daten vorangezeigt, aber nicht tatsächlich ausgeführt werden soll. In der Voranzeige werden die Anzahl der Dateien und die Byte angezeigt, die kopiert werden sollen, sowie eine Liste der Datenträger des primären Speicherpools, die geladen werden müssen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No
Gibt an, dass aktive Daten kopiert werden.
Yes
Gibt an, dass der Prozess vorangezeigt wird, aber keine Daten kopiert werden.
VOLumesonly
Gibt an, dass die Voranzeige des Prozesses nur als Liste der Datenträger gewünscht wird, die geladen werden müssen. Diese Auswahl erfordert die geringste Verarbeitungszeit.

Wait
Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No
Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Bei dem Hintergrundprozess erstellte Nachrichten werden im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise bereits einige Dateien vor dem Abbruch kopiert.

Yes
Gibt an, dass der Server diese Operation im Vordergrund ausführt. Die Operation muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dem Verwaltungsclient an, wenn die Operation beendet ist.

Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

SHREDTONOshred
Gibt an, ob Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einen Pool für aktive Daten, der das Schreddern nicht erzwingt, kopiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No
Gibt an, dass der Server das Kopieren von Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einen Pool für aktive Daten, der das Schreddern nicht erzwingt, nicht zulässt. Wenn der primäre Speicherpool das Schreddern erzwingt und der Pool für aktive Daten das Schreddern nicht erzwingt, schlägt die Operation fehl.
Yes
Gibt an, dass der Server das Kopieren von Daten aus einem primären Speicherpool, der das Schreddern erzwingt, in einen Pool für aktive Daten, der das Schreddern nicht erzwingt, zulässt. Die Daten in dem Pool für aktive Daten werden nicht geschreddert, wenn er gelöscht wird.

Beispiel: Daten aus einem primären Speicherpool in einen Pool für aktive Daten kopieren

Die aktiven Daten aus dem primären Speicherpool PRIMARY_POOL in den Pool für aktive Daten mit dem Namen ACTIVEPOOL kopieren. Den folgenden Befehl ausgeben:

```
copy activedata primary_pool activepool
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY ACTIVEDATA

Befehl	Beschreibung
DEFINE DOMAIN	Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT SERVER	Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT NODE	Schreibt Clientknotendaten von externen Datenträgern zurück.

Befehl	Beschreibung
IMPORT SERVER	Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.
MOVE NODEDATA	Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.
QUERY CONTENT	Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
RESTORE STGPOOL	Schreibt Dateien aus Kopienspeicherpools in einen primären Speicherpool zurück.
RESTORE VOLUME	Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopienspeicherpools zurück.
UPDATE DOMAIN	Ändert die Attribute einer Maßnahmendomäne.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

COPY CLOPTSET (Clientoptionsgruppe kopieren)

Mit diesem Befehl kann eine Clientoptionsgruppe kopiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

Syntax

```
>>-COPy CLOptset--aktueller_Optionsgruppenname--neuer_Optionsgruppenname-><
```

Parameter

aktueller_Optionsgruppenname (Erforderlich)
: Gibt den Namen der zu kopierenden Client-Optionsgruppe an.

neuer_Optionsgruppenname (Erforderlich)
: Gibt den Namen der neuen Client-Optionsgruppe an. Die maximale Länge des Namens beträgt 64 Zeichen.

Beispiel: Eine Clientoptionsgruppe kopieren

Die Clientoptionsgruppe ENG in die neue Clientoptionsgruppe ENG2 kopieren.

```
copy cloptset eng eng2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY CLOPTSET

Befehl	Beschreibung
DEFINE CLIENTOPT	Fügt einer Clientoptionsgruppe eine Clientoption hinzu.
DEFINE CLOPTSET	Definiert eine Clientoptionsgruppe.
DELETE CLIENTOPT	Löscht eine Clientoption aus einer Clientoptionsgruppe.
DELETE CLOPTSET	Löscht eine Clientoptionsgruppe.
QUERY CLOPTSET	Zeigt Informationen über eine Clientoptionsgruppe an.

Befehl	Beschreibung
UPDATE CLIENTOPT	Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe.
UPDATE CLOPTSET	Aktualisiert die Beschreibung einer Clientoptionsgruppe.

COPY DOMAIN (Maßnahmendomäne kopieren)

Mit diesem Befehl kann eine Kopie einer Maßnahmendomäne erstellt werden.

Der Server kopiert die folgenden Informationen in die neue Domäne:

- Beschreibung der Maßnahmendomäne
- Maßnahmengruppen in der Maßnahmendomäne (einschließlich der AKTIVEN Maßnahmengruppe, wenn eine Maßnahmengruppe aktiviert ist)
- Verwaltungsklassen in jeder Maßnahmengruppe (einschließlich der Standardverwaltungsklasse, falls zugeordnet)
- Kopiengruppen in jeder Verwaltungsklasse

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-COPy DOmain--aktueller_Domänenname--neuer_Domänenname------><
```

Parameter

aktueller_Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, die kopiert werden soll.

neuer_Domänenname (Erforderlich)
: Gibt den Namen der neuen Maßnahmendomäne an. Die maximale Länge dieses Namens beträgt 30 Zeichen.

Beispiel: Eine Maßnahmendomäne in eine neue Maßnahmendomäne kopieren

Die Maßnahmendomäne STANDARD in die neue Maßnahmendomäne ENGPOLDOM kopieren, indem der folgende Befehl eingegeben wird:

```
copy domain standard engpoldom
```

ENGPOLDOM enthält jetzt die Standardmaßnahmengruppe, die Verwaltungsklasse, die Sicherungskopiengruppe und die Archivierungskopiengruppe.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY DOMAIN

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE DOMAIN	Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
DELETE COPYGROUP	Löscht eine Sicherungs- oder Archivierungskopiengruppe aus einer Maßnahmendomäne und Maßnahmengruppe.
DELETE DOMAIN	Löscht eine Maßnahmendomäne und, falls vorhanden, Maßnahmenobjekte in der Maßnahmendomäne.

Befehl	Beschreibung
DELETE MGMTCLASS	Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.
UPDATE DOMAIN	Ändert die Attribute einer Maßnahmendomäne.
UPDATE MGMTCLASS	Ändert die Attribute einer Verwaltungsklasse.
UPDATE POLICYSET	Ändert die Beschreibung einer Maßnahmengruppe.
VALIDATE POLICYSET	Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert.

COPY MGMTCLASS (Verwaltungsklasse kopieren)

Mit diesem Befehl kann eine Kopie einer Verwaltungsklasse innerhalb derselben Maßnahmengruppe erstellt werden.

Der Server kopiert die folgenden Informationen in die neue Verwaltungsklasse:

- Beschreibung der Verwaltungsklasse
- Für die Verwaltungsklasse definierte Kopiengruppen
- Alle Attribute für die Verwaltung von Dateien für IBM Spectrum Protect for Space Management-Clients

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die neue Verwaltungsklasse gehört.

Syntax

```
>>-COPy MGmtclass--Domänenname--Name_der_Maßnahmengruppe-------->

>--aktueller_Klassenname--neuer_Klassenname------------------><
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Verwaltungsklasse gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, zu der die Verwaltungsklasse gehört.

aktueller_Klassenname (Erforderlich)
: Gibt die Verwaltungsklasse an, die kopiert werden soll.

neuer_Klassenname (Erforderlich)
: Gibt den Namen der neuen Verwaltungsklasse an. Die maximale Länge dieses Namens beträgt 30 Zeichen.

Beispiel: Eine Verwaltungsklasse in eine neue Verwaltungsklasse kopieren

Die Verwaltungsklasse ACTIVEFILES in die neue Verwaltungsklasse FILEHISTORY kopieren. Die Verwaltungsklasse befindet sich in Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE_RECORDS.

```
copy mgmtclass employee_records vacation
activefiles filehistory
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY MGMTCLASS

Befehl	Beschreibung

Befehl	Beschreibung
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DELETE MGMTCLASS	Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.
UPDATE MGMTCLASS	Ändert die Attribute einer Verwaltungsklasse.

COPY POLICYSET (Maßnahmengruppe kopieren)

Mit diesem Befehl kann eine Maßnahmengruppe (einschließlich der AKTIVEN Maßnahmengruppe) innerhalb derselben Maßnahmendomäne kopiert werden.

Der Server kopiert die folgenden Informationen in die neue Maßnahmengruppe:

- Beschreibung der Maßnahmengruppe
- Verwaltungsklassen in der Maßnahmengruppe (einschließlich der Standardverwaltungsklasse, falls zugeordnet)
- Kopiengruppen in jeder Verwaltungsklasse

Die Maßnahmen in der neuen Maßnahmengruppe werden erst wirksam, wenn Sie die neue Gruppe als Maßnahmengruppe ACTIVE definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die neue Maßnahmengruppe gehört.

Syntax

```
>>-COPy POlicyset--Domänenname--aktueller_Gruppenname--neuer_Gruppenname-><
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Maßnahmengruppe gehört.

aktueller_Gruppenname (Erforderlich)
: Gibt die Maßnahmengruppe an, die kopiert werden soll.

neuer_Gruppenname (Erforderlich)
: Gibt den Namen der neuen Maßnahmengruppe an. Die maximale Länge dieses Namens beträgt 30 Zeichen.

Beispiel: Eine Maßnahmengruppe in eine neue Maßnahmengruppe kopieren

Die Maßnahmengruppe `VACATION` in die neue Maßnahmengruppe `HOLIDAY` in der Maßnahmendomäne `EMPLOYEE_RECORDS` kopieren.

```
copy policyset employee_records vacation holiday
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY POLICYSET

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DELETE POLICYSET	Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.

Befehl	Beschreibung
UPDATE POLICYSET	Ändert die Beschreibung einer Maßnahmengruppe.
VALIDATE POLICYSET	Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert.

COPY PROFILE (Profil kopieren)

Mit diesem Befehl können auf einem Konfigurationsmanager ein Profil und alle zugeordneten Objektnamen in ein neues Profil kopiert werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-COPy PROFIle--aktueller_Profilname--neuer_Profilname-------><
```

Parameter

aktueller_Profilname (Erforderlich)
: Gibt das Profil an, das kopiert werden soll.

neuer_Profilname (Erforderlich)
: Gibt den Namen des neuen Profils an. Die maximale Länge des Profilnamens beträgt 30 Zeichen.

Beispiel: Eine Kopie eines Profils erstellen

Das Profil VAL in das neue Profil VAL2 kopieren.

```
copy profile val val2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY PROFILE

Befehl	Beschreibung
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DEFINE SUBSCRIPTION	Subskribiert einen verwalteten Server für ein Profil.
DELETE PROFASSOCIATION	Löscht die Zuordnung zwischen einem Objekt und einem Profil.
DELETE PROFILE	Löscht ein Profil aus einem Konfigurationsmanager.
DELETE SUBSCRIBER	Löscht veraltete Subskriptionen verwalteter Server.
DELETE SUBSCRIPTION	Löscht eine angegebene Profilsubskription.
LOCK PROFILE	Verhindert die Verteilung eines Konfigurationsprofils.
NOTIFY SUBSCRIBERS	Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.
QUERY PROFILE	Zeigt Informationen über Konfigurationsprofile an.
QUERY SUBSCRIBER	Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.
QUERY SUBSCRIPTION	Zeigt Informationen über Profilsubskriptionen an.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UNLOCK PROFILE	Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

COPY SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl kopieren)

Mit diesem Befehl kann eine Kopie eines Zeitplans erstellt werden.

Der Befehl COPY SCHEDULE kann zwei Formen haben, je nachdem, ob der Zeitplan Client-Operationen oder Verwaltungsbefehle betrifft. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für COPY SCHEDULE

Befehl	Beschreibung
DEFINE ASSOCIATION	Ordnet Clients einem Zeitplan zu.
DEFINE SCHEDULE	Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.
DELETE SCHEDULE	Löscht einen Zeitplan aus der Datenbank.
QUERY SCHEDULE	Zeigt Informationen über Zeitpläne an.
UPDATE SCHEDULE	Ändert die Attribute eines Zeitplans.

- COPY SCHEDULE (Kopie eines Zeitplans für Clientoperationen erstellen)
  Mit dem Befehl COPY SCHEDULE kann eine Kopie eines Zeitplans für Clientoperationen erstellt werden. Ein Zeitplan kann innerhalb einer Maßnahmendomäne oder von einer Maßnahmendomäne in eine andere Maßnahmendomäne kopiert werden. Mit dem Befehl DEFINE ASSOCIATION kann der neue Zeitplan den Clientknoten zugeordnet werden.
- COPY SCHEDULE (Kopie eines Zeitplans für Verwaltungsoperationen erstellen)
  Mit dem Befehl COPY SCHEDULE kann eine Kopie eines Zeitplans für Verwaltungsbefehle erstellt werden.

COPY SCHEDULE (Kopie eines Zeitplans für Clientoperationen erstellen)

Mit dem Befehl COPY SCHEDULE kann eine Kopie eines Zeitplans für Clientoperationen erstellt werden. Ein Zeitplan kann innerhalb einer Maßnahmendomäne oder von einer Maßnahmendomäne in eine andere Maßnahmendomäne kopiert werden. Mit dem Befehl DEFINE ASSOCIATION kann der neue Zeitplan den Clientknoten zugeordnet werden.

Berechtigungsklasse

Zum Kopieren eines Clientzeitplans ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, in die der Zeitplan kopiert wird.

Syntax

```
>>-COPy SCHedule--aktueller_Domänenname-------------------------->

>--aktueller_Zeitplanname--neuer_Domänenname-------------------->

   .-aktueller_Zeitplanname-.  .-REPlace--=--No------.
>--+------------------------+--+--------------------+--------><
   '-neuer_Zeitplanname-----'  '-REPlace--=--+-No--+-'
                                             '-Yes-'
```

Parameter

aktueller_Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an, in der sich der Zeitplan befindet, der kopiert werden soll.

aktueller_Zeitplanname (Erforderlich)
: Gibt den Namen des Zeitplans an, der kopiert werden soll.

neuer_Domänenname (Erforderlich)
: Gibt den Namen einer Maßnahmendomäne an, in die der neue Zeitplan kopiert werden soll.

neuer_Zeitplanname
: Gibt den Namen des neuen Zeitplans an. Für den Namen können bis zu 30 Zeichen angegeben werden.

  Wird dieser Name nicht angegeben, wird der Name des ursprünglichen Zeitplans verwendet.

  Wenn der Zeitplanname bereits in der Maßnahmendomäne definiert ist, muß REPLACE=YES angegeben werden, damit der Befehl nicht fehlschlägt.

REPlace
: Gibt an, ob ein Client-Zeitplan ersetzt werden soll. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, daß ein Client-Zeitplan nicht ersetzt wird.

  Yes
  : Gibt an, daß ein Client-Zeitplan ersetzt wird.

Beispiel: Einen Zeitplan aus einer Maßnahmendomäne in eine andere Maßnahmendomäne kopieren

Den Zeitplan WEEKLY_BACKUP, der zur Maßnahmendomäne EMPLOYEE_RECORDS gehört, in die Maßnahmendomäne PROG1 kopieren und den neuen Zeitplan WEEKLY_BACK2 benennen. Ist bereits ein Zeitplan dieses Namens in der Maßnahmendomäne PROG1 definiert, darf er nicht ersetzt werden.

```
copy schedule employee_records weekly_backup
prog1 weekly_back2
```

COPY SCHEDULE (Kopie eines Zeitplans für Verwaltungsoperationen erstellen)

Mit dem Befehl COPY SCHEDULE kann eine Kopie eines Zeitplans für Verwaltungsbefehle erstellt werden.

Berechtigungsklasse

Zum Kopieren eines Zeitplans für Verwaltungsbefehle ist die Systemberechtigung erforderlich.

Syntax

```
>>-COPy SCHedule--aktueller_Zeitplanname--neuer_Zeitplanname---->

                            .-REPlace--=--No------.
>--Type--=--Administrative--+---------------------+------------><
                            '-REPlace--=--+-No--+-'
                                          '-Yes-'
```

Parameter

aktueller_Zeitplanname (Erforderlich)
: Gibt den Namen des Zeitplans an, der kopiert werden soll.

neuer_Zeitplanname (Erforderlich)
: Gibt den Namen des neuen Zeitplans an. Für den Namen können bis zu 30 Zeichen angegeben werden.

  Wenn der Zeitplanname bereits definiert ist, muß REPLACE=YES angegeben werden, damit der Befehl nicht fehlschlägt.

Type=Administrative
: Gibt an, daß ein Zeitplan für Verwaltungsbefehle kopiert werden soll.

REPlace
: Gibt an, ob ein Zeitplan für Verwaltungsbefehle ersetzt werden soll. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, daß ein Zeitplan für Verwaltungsbefehle nicht ersetzt wird.

  Yes
  : Gibt an, daß ein Zeitplan für Verwaltungsbefehle ersetzt wird.

Beispiel: Einen Zeitplan für Verwaltungsbefehle in einen anderen Zeitplan kopieren

Den Zeitplan für Verwaltungsbefehle mit dem Namen DATA_BACKUP kopieren und in DATA_ENG umbenennen. Ist bereits ein Zeitplan mit diesem Namen vorhanden, den Zeitplan ersetzen.

```
copy schedule data_backup data_eng
type=administrative replace=yes
```

COPY SCRIPT (IBM Spectrum Protect-Prozedur kopieren)

Verwenden Sie diesen Befehl, um eine vorhandene IBM Spectrum Protect-Prozedur in eine neue Prozedur mit einem anderen Namen zu kopieren.

Berechtigungsklasse

Für diesen Befehl ist die Bediener-, Maßnahmen-, Speicher- oder Systemberechtigung erforderlich.

Syntax

```
>>-COPy SCRipt--aktueller_Prozedurname--neuer_Prozedurname-----><
```

Parameter

aktueller_Prozedurname (Erforderlich)
Gibt den Namen der Prozedur an, die kopiert werden soll.
neuer_Prozedurname (Erforderlich)
Gibt den Namen der neuen Prozedur an. Für den Namen können bis zu 30 Zeichen angegeben werden.

Beispiel: Eine Kopie eines Scripts erstellen

Prozedur TESTDEV in eine neue Prozedur kopieren und in ENGDEV umbenennen.

```
copy script testdev engdev
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY SCRIPT

Befehl	Beschreibung
DEFINE SCRIPT	Definiert eine Prozedur für den IBM Spectrum Protect-Server.
DELETE SCRIPT	Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur.
QUERY SCRIPT	Zeigt Informationen über Prozeduren an.
RENAME SCRIPT	Vergibt einen neuen Namen für eine Prozedur.
RUN	Führt ein Script aus.
UPDATE SCRIPT	Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.

COPY SERVERGROUP (Server-Gruppe kopieren)

Mit diesem Befehl kann eine Kopie einer Server-Gruppe erstellt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-COPy SERVERGroup--aktueller_Gruppenname--neuer_Gruppenname--><
```

Parameter

aktueller_Gruppenname (Erforderlich)
Gibt die Server-Gruppe an, die kopiert werden soll.
neuer_Gruppenname (Erforderlich)
Gibt den Namen der neuen Server-Gruppe an. Die maximale Länge dieses Namens beträgt 64 Zeichen.

Beispiel: Eine Kopie einer Servergruppe erstellen

Die Server-Gruppe GRP_PAYROLL in die neue Gruppe HQ_PAYROLL kopieren.

```
copy servergroup grp_payroll hq_payroll
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für COPY SERVERGROUP

Befehl	Beschreibung
DEFINE GRPMEMBER	Definiert einen Server als Teil einer Servergruppe.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DEFINE SERVERGROUP	Definiert eine neue Servergruppe.
DELETE GRPMEMBER	Löscht einen Server aus einer Servergruppe.
DELETE SERVER	Löscht die Definition eines Servers.
DELETE SERVERGROUP	Löscht eine Servergruppe.

Befehl	Beschreibung
MOVE GRPMEMBER	Versetzt einen Teil einer Servergruppe.
QUERY SERVER	Zeigt Informationen über Server an.
QUERY SERVERGROUP	Zeigt Informationen über Servergruppen an.
RENAME SERVERGROUP	Benennt eine Servergruppe um.
UPDATE SERVER	Aktualisiert Informationen über einen Server.
UPDATE SERVERGROUP	Aktualisiert eine Servergruppe.

DEACTIVATE DATA (Daten für einen Clientknoten inaktivieren)

Mit diesem Befehl können Sie angeben, dass aktive Daten, die für einen Anwendungsclientknoten vor einem angegebenen Datum gesichert wurden, nicht mehr benötigt werden. Der Befehl markiert die Daten als inaktiv, sodass sie gemäß Ihren Datenaufbewahrungsmaßnahmen gelöscht werden können.

Einschränkung: Der Befehl DEACTIVATE DATA gilt nur für Anwendungsclients, die Oracle-Datenbanken schützen.

Wenn Sie den Befehl DEACTIVATE DATA ausgeben, werden alle aktiven Sicherungsdaten, die vor dem angegebenen Datum gespeichert wurden, inaktiv. Die Daten können nicht mehr abgerufen werden und werden bei ihrem Verfall gelöscht.

Der Befehl DEACTIVATE DATA betrifft nur die Dateien, die vor dem angegebenen Datum und der angegebenen Zeit auf den Server kopiert wurden. Auf die Dateien, die nach dem angegebenen Datum kopiert wurden, kann noch zugegriffen werden, und der Client kann noch auf den Server zugreifen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEACtivate DAta--Knotenname--TODate--=--Datum----------------->

   .-TOTime--=--23:59:59-.  .-Wait--=--No------.
>--+---------------------+--+------------------+---------------><
   '-TOTime--=--Zeit-----'  '-Wait--=--+-No--+-'
                                       '-Yes-'
```

Parameter

Knotenname (Erforderlich)
: Gibt den Namen eines Anwendungsclientknotens an, dessen Daten inaktiviert werden sollen.

TODate (Erforderlich)
: Gibt das Datum an, das für die Auswahl der Sicherungsdateien, die inaktiviert werden sollen, verwendet werden soll. IBM Spectrum Protect inaktiviert nur die Dateien mit einem Datum bis zu dem angegebenen Datum (einschließlich). Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	01/23/2014
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–30 **oder** –30. Um Dateien zu inaktivieren, die mindestens 30 Tage alt sind, können Sie TODAY-30 oder -30 angeben.
EOLM	Ende des letzten Monats. Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien zu inaktivieren, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM	Anfang dieses Monats. Der erste Tag des aktuellen Monats.	BOTM

Wert	Beschreibung	Beispiel
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien zu inaktivieren, die am zehnten Tag des aktuellen Monats aktiv waren.

TOTime

Gibt an, dass Dateien inaktiviert werden sollen, die vor dieser Zeit am angegebenen Datum auf dem Server erstellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist das Ende des Tages (23:59:59). Geben Sie die Uhrzeit mit einem der folgenden Werte an:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Datum	12:30:22
NOW	Die aktuelle Uhrzeit am angegebenen Datum	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Datum	NOW+03:00 **oder** +03:00. Wenn Sie den Befehl DEACTIVATE DATA um 9:00 Uhr mit TOTIME=NOW+03:00 oder TOTIME=+03:00 ausgeben, inaktiviert IBM Spectrum Protect Dateien, die um 12:00 Uhr oder früher am angegebenen Datum auf den Server gestellt wurden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Datum	NOW-03:30 **oder** -03:30. Wenn Sie den Befehl DEACTIVATE DATA um 9:00 Uhr mit TOTIME=NOW-3:30 oder TOTIME=-3:30 ausgeben, inaktiviert IBM Spectrum Protect Dateien, die um 5:30 Uhr oder früher am angegebenen Datum auf den Server gestellt wurden.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie die folgenden Werte an:

No

Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden.

Yes

Der Server verarbeitet diesen Befehl im Vordergrund. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

Beispiel: Daten für einen Data Protection-Clientknoten inaktivieren

Der Clientknoten BANDIT ist ein IBM Spectrum Protect for Databases: Data Protection for Oracle-Anwendungsclient. Alle Sicherungsdaten sind aktiv und somit werden alle Sicherungsdaten aufbewahrt. Mit dem folgenden Befehl werden Daten inaktiviert, die vor dem 3. Januar 2014 gesichert wurden, sodass die Daten bei ihrem Verfall gelöscht werden können.

```
deactivate data bandit todate=01/23/2014
```

Um Daten regelmäßig zu inaktivieren, sodass sie bei ihrem Verfall gelöscht werden können, können Sie den folgenden Befehl in einem Clientzeitplan ausführen.

```
deactivate data bandit todate=today
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEACTIVATE DATA

Befehl	Beschreibung
DECOMMISSION NODE	Legt einen Anwendungs- oder Systemknoten still.
DECOMMISSION VM	Legt eine virtuelle Maschine still.

DECOMMISSION-Befehle

Verwenden Sie die DECOMMISSION-Befehle, um Clientknoten aus der Produktionsumgebung zu entfernen. Clientknoten umfassen Anwendungen, Systeme und virtuelle Maschinen.

- DECOMMISSION NODE (Anwendungs- oder Systemknoten stilllegen)
- DECOMMISSION VM (Virtuelle Maschine stilllegen)

DECOMMISSION NODE (Anwendungs- oder Systemknoten stilllegen)

Verwenden Sie diesen Befehl, um einen Anwendungs- oder Systemclientknoten der Produktionsumgebung stillzulegen. Alle Sicherungsdaten, die für den Clientknoten gespeichert werden, verfallen gemäß den Maßnahmeneinstellungen, sofern Sie die Daten nicht explizit löschen.

Achtung: Diese Aktion kann nicht umgekehrt werden und hat das Löschen von Daten zur Folge. Obwohl dieser Befehl die Clientknotendefinition erst löscht, nachdem die Daten verfallen sind, kann die Stilllegung des Clientknotens nicht rückgängig gemacht werden. Nachdem Sie diesen Befehl ausgegeben haben, kann der Clientknoten nicht auf den Server zugreifen und seine Daten werden nicht gesichert. Der Clientknoten wird gesperrt und kann nur zum Zurückschreiben von Dateien entsperrt werden. Dateibereiche, die zu dem Clientknoten gehören, und der Clientknoten selbst werden schließlich entfernt.
Mit diesem Befehl können die folgenden Typen von Clientknoten stillgelegt werden:

Anwendungsclientknoten
: Anwendungsclientknoten umfassen E-Mail-Server, Datenbanken und andere Anwendungen. Beispielsweise kann jede der folgenden Anwendungen ein Anwendungsclientknoten sein:

  - IBM Spectrum Protect Snapshot
  - IBM Spectrum Protect for Databases
  - IBM Spectrum Protect for Enterprise Resource Planning
  - IBM Spectrum Protect for Mail
  - IBM Spectrum Protect for Virtual Environments

Systemclientknoten
: Systemclientknoten umfassen Workstations, NAS-Dateiserver und API-Clients.

Wenn ein Clientknoten nicht mehr in der Produktionsumgebung benötigt wird, können Sie diesen Befehl ausgeben, um eine schrittweise, gesteuerte Stilllegungsoperation einzuleiten. Der Befehl führt die folgenden Aktionen aus:

- Löscht alle Zeitplanzuordnungen für den Clientknoten. Zeitpläne werden nicht mehr auf dem Clientknoten ausgeführt. Diese Aktion entspricht der Ausgabe des Befehls DELETE ASSOCIATION für jeden Zeitplan, dem der Clientknoten zugeordnet ist.
- Verhindert, dass der Client auf den Server zugreift. Diese Aktion entspricht der Ausgabe des Befehls LOCK NODE.

Nach der Ausführung des Befehls werden Clientknotendaten nicht mehr auf dem Server gesichert. Daten, die vor der Stilllegung des Clientknotens gesichert wurden, werden nicht sofort auf dem Server gelöscht. Alle Sicherungsdateiversionen, einschließlich der neuesten Sicherung, sind jedoch jetzt inaktive Kopien. Die Clientdateien werden auf dem Server gemäß ihren Speicherverwaltungsmaßnahmen aufbewahrt.

Nach dem Ablauf aller Datenaufbewahrungszeiträume und dem Entfernen aller Clientsicherungs- und -archivierungsdateikopien aus dem Serverspeicher löscht IBM Spectrum Protect die Dateibereiche, die zu dem stillgelegten Knoten gehören. Diese Aktion entspricht der Ausgabe des Befehls DELETE FILESPACE.

Nach dem Löschen der Dateibereiche für den stillgelegten Knoten wird die Knotendefinition auf dem Server gelöscht. Diese Aktion entspricht der Ausgabe des Befehls REMOVE NODE.

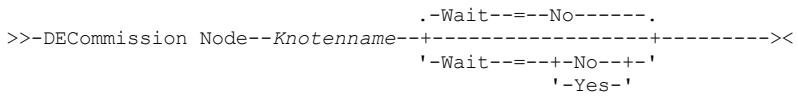
Nach der Stilllegung eines Clientknotens, aber vor dem Entfernen des Knotens auf dem Server können Sie mithilfe des Befehls QUERY NODE überprüfen, ob der Clientknoten stillgelegt ist.

Einschränkung: Sie können keinen Clientknoten stilllegen, der für die Replikation konfiguriert ist. Sie können den Replikationsstatus eines Clientknotens mithilfe des Befehls QUERY NODE bestimmen. Wenn ein Clientknoten für die Replikation konfiguriert ist, können Sie den Clientknoten mit dem Befehl REMOVE REPLNODE aus der Replikation entfernen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, der stillgelegt werden soll.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

  No
  : Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden.

  Yes
  : Der Server verarbeitet diesen Befehl im Vordergrund. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

  Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

Beispiel: Einen Clientknoten stilllegen

Den Clientknoten CODY stilllegen.

```
decommission node cody
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DECOMMISSION NODE

Befehl	Beschreibung
DECOMMISSION VM	Legt eine virtuelle Maschine still.
DEACTIVATE DATA	Inaktiviert Daten für einen Clientknoten.

DECOMMISSION VM (Virtuelle Maschine stilllegen)

Verwenden Sie diesen Befehl, um eine einzelne virtuelle Maschine innerhalb eines Datencenterknotens zu entfernen. Der Dateibereich, der die virtuelle Maschine darstellt, wird erst nach dem Verfall seiner Sicherungsdaten auf dem Server gelöscht.

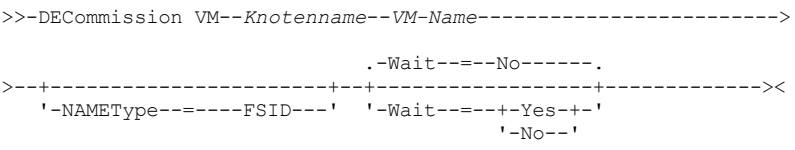
Achtung: Dieser Befehl kann nicht umgekehrt werden und hat das Löschen von Daten zur Folge. Obwohl dieser Befehl den Dateibereich der virtuellen Maschine erst löscht, nachdem die Daten verfallen sind, kann die Stilllegung der virtuellen Maschine nicht rückgängig gemacht werden.

Wenn eine virtuelle Maschine nicht mehr in der Produktionsumgebung benötigt wird, können Sie diesen Befehl ausgeben, um ein schrittweises Entfernen des Dateibereichs der virtuellen Maschine auf dem Server einzuleiten. Der Befehl DECOMMISSION VM markiert alle Daten, die für die virtuelle Maschine gesichert wurden, als inaktiv, sodass sie gemäß Ihren Datenaufbewahrungsmaßnahmen gelöscht werden können. Nachdem alle Daten, die für die virtuelle Maschine gesichert wurden, verfallen sind, wird der Dateibereich, der die virtuelle Maschine darstellt, gelöscht. Der Befehl DECOMMISSION VM betrifft nur die virtuelle Maschine, die Sie angeben. Der Datencenterknoten und die anderen virtuellen Maschinen, die vom Datencenterknoten gehostet werden, sind nicht betroffen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Datencenterknotens an, der die virtuelle Maschine hostet, die stillgelegt werden soll.

VM-Name (Erforderlich)
: Gibt den Dateibereich an, der die virtuelle Maschine darstellt, die stillgelegt werden soll. Jede virtuelle Maschine, die von einem Datencenterknoten gehostet wird, wird als Dateibereich dargestellt.

  Enthält der Name ein oder mehrere Leerzeichen, müssen Sie den Namen in Anführungszeichen einschließen, wenn Sie den Befehl ausgeben.

Standardmäßig interpretiert der Server den von Ihnen eingegebenen Dateibereichsnamen mithilfe der Server-Codepage und versucht außerdem, den Dateibereichsnamen aus der Server-Codepage in die UTF-8-Codepage zu konvertieren. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Server-Codepage nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

Wenn der Name der virtuellen Maschine kein englischer Name ist, muss dieser Parameter die Dateibereichs-ID (FSID) angeben. Durch Angabe des Parameters NAMEType kann der Server angewiesen werden, den Dateibereichsnamen stattdessen anhand der Dateibereichs-ID (FSID) zu interpretieren.

NAMEType
Geben Sie an, wie der Server den Dateibereichsnamen interpretieren soll, den Sie zur Angabe der virtuellen Maschine eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unicode-Unterstützung verfügt. Sie können den folgenden Wert angeben:

FSID
Der Server interpretiert den Dateibereichsnamen anhand der Dateibereichs-ID (FSID).

Wait
Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Sie können die folgenden Werte angeben:

No
Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden.

Yes
Der Server verarbeitet diesen Befehl im Vordergrund. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.

Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

Beispiele: Eine virtuelle Maschine stilllegen

Legen Sie die virtuelle Maschine CODY still.

```
decommission vm dept06node cody
```

Legen Sie die virtuelle Maschine CODY 2 still.

```
decommission vm dept06node "cody 2"
```

Legen Sie eine virtuelle Maschine durch Angabe ihrer Dateibereichs-ID still.

```
decommission vm dept06node 7 nametype=fsid
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DECOMMISSION VM

Befehl	Beschreibung
DECOMMISSION NODE	Legt einen Anwendungs- oder Systemknoten still.
DEACTIVATE DATA	Inaktiviert Daten für einen Clientknoten.

DEFINE-Befehle

Mit den DEFINE-Befehlen können IBM Spectrum Protect-Objekte erstellt werden.

- DEFINE ALERTTRIGGER (Alertauslöser definieren)
- DEFINE ASSOCIATION (Clientknoten einem Zeitplan zuordnen)
- DEFINE BACKUPSET (Sicherungsgruppe definieren)
- DEFINE CLIENTACTION (Einmalige Clientaktion definieren)
- DEFINE CLIENTOPT (Option für eine Optionsgruppe definieren)
- DEFINE CLOPTSET (Clientoptionsgruppennamen definieren)
- DEFINE COLLOCGROUP (Kollokationsgruppe definieren)
- DEFINE COLLOCMEMBER (Kollokationsgruppenmitglied definieren)
- DEFINE COPYGROUP (Kopiengruppe definieren)
- DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren)
- DEFINE DEVCLASS (Einheitenklasse definieren)
- DEFINE DOMAIN (Neue Maßnahmendomäne definieren)
- DEFINE DRIVE (Laufwerk für Kassettenarchiv definieren)

- DEFINE EVENTSERVER (Server als Ereignisserver definieren)
- DEFINE GRPMEMBER (Server zu einer Servergruppe hinzufügen)
- DEFINE LIBRARY (Kassettenarchiv definieren)
- DEFINE MACHINE (Maschineninformationen für die Wiederherstellung nach einem Katastrophenfall definieren)
- DEFINE MACHNODEASSOCIATION (Knoten einer Maschine zuordnen)
- DEFINE MGMTCLASS (Verwaltungsklasse definieren)
- DEFINE NODEGROUP (Knotengruppe definieren)
- DEFINE NODEGROUPMEMBER (Eintrag in der Knotengruppe definieren)
- DEFINE PATH (Pfad definieren)
- DEFINE POLICYSET (Maßnahmengruppe definieren)
- DEFINE PROFASSOCIATION (Profilzuordnung definieren)
- DEFINE PROFILE (Profil definieren)
- DEFINE RECMEDMACHASSOCIATION (Wiederh.-Datenträger Maschine zuordnen)
- DEFINE RECOVERYMEDIA (Wiederherstellungsdatenträger definieren)
- DEFINE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl definieren)
- DEFINE SCRIPT (IBM Spectrum Protect-Prozedur definieren)
- DEFINE SERVER (Server für Übertragung zwischen Servern definieren)
- DEFINE SERVERGROUP (Server-Gruppe definieren)
- DEFINE SPACETRIGGER (Speicherbereichsauslöser definieren)
- DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)
- DEFINE STGPOOL (Speicherpool definieren)
- DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)
- DEFINE SUBSCRIPTION (Profilsubskription definieren)
- DEFINE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs definieren)
- DEFINE VOLUME (Datenträger in einem Speicherpool definieren)

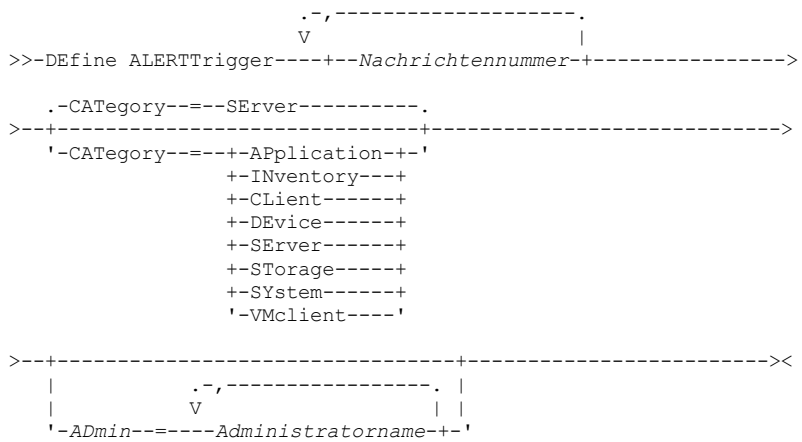
DEFINE ALERTTRIGGER (Alertauslöser definieren)

Verwenden Sie diesen Befehl, um einen Alert auszulösen, wenn ein Server eine bestimmte Fehlernachricht ausgibt. Sie können eine Nachrichtennummer als Alertauslöser definieren, die Nachrichtennummer einer Kategorie zuordnen oder Administratoren angeben, die über den Alert in einer E-Mail benachrichtigt werden können.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Nachrichtennummer (Erforderlich)
: Gibt die Nachrichtennummer an, die dem Alertauslöser zugeordnet werden soll. Geben Sie mehrere Nachrichtennummern durch Kommas getrennt und ohne Leerzeichen an. Nachrichtennummern haben eine maximale Länge von acht Zeichen.

CATegory
: Gibt den Kategorietyp für den Alert an, der durch die Nachrichtentypen bestimmt wird. Der Standardwert ist SERVER.
Anmerkung: Wenn Sie die Kategorie eines Alertauslösers ändern, wird die Kategorie von vorhandenen Alerts auf dem Server nicht geändert. Neue Alerts werden mit der neuen Kategorie kategorisiert.
Geben Sie einen der folgenden Werte an:

APplication
: Der Alert wird als Anwendungskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Anwendungsclients (TDP) zugeordnet sind.

INventory
: Der Alert wird als Bestandskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die der Datenbank, der aktiven Protokolldatei oder der Archivprotokolldatei zugeordnet sind.

CLient
: Der Alert wird als Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Clientaktivitäten zugeordnet sind.

DEvice
: Der Alert wird als Einheitenkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Einheitenklassen, Kassettenarchiven, Laufwerken oder Pfaden zugeordnet sind.

SErver
: Der Alert wird als allgemeine Serverkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Serveraktivitäten oder -ereignissen zugeordnet sind.

STorage
: Der Alert wird als Speicherkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Speicherpools zugeordnet sind.

SYstems
: Der Alert wird als Systemclientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Systemsicherungs- und -archivierungsclients oder HSM-Clients zugeordnet sind.

VMclient
: Der Alert wird als VM-Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die VM-Clients zugeordnet sind.

ADmin
: Dieser optionale Parameter gibt den Namen des Administrators an, der eine E-Mail-Benachrichtigung über diesen Alert empfängt. Der Alertauslöser wird erfolgreich definiert, auch wenn keine Administratornamen angegeben werden.

Einem Alert zwei Nachrichtennummern zuordnen

Mit dem folgenden Befehl angeben, dass zwei Nachrichtennummern einen Alert auslösen sollen:

```
define alerttrigger ANR1067E,ANR1073E
```

Einem Alert eine Nachrichtennummer zuordnen und zwei Administratoren in einer E-Mail benachrichtigen

Den folgenden Befehl ausgeben, um die Nachrichtennummern anzugeben, die einen Alert auslösen sollen und in einer E-Mail an zwei Administratoren gesendet werden sollen:

```
define alerttrigger ANR1067E,ANR1073E ADmin=BILL,DJADMIN
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE ALERTTRIGGER

Befehl	Beschreibung
DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)	Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.
QUERY ALERTSTATUS (Status eines Alert abfragen)	Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.
QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)	Zeigt Nachrichtennummern an, die einen Alert auslösen.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)	Aktualisiert die Attribute eines oder mehrerer Alertauslöser.
UPDATE ALERTSTATUS (Status eines Alert aktualisieren)	Aktualisiert den Status eines zurückgemeldeten Alert.

DEFINE ASSOCIATION (Clientknoten einem Zeitplan zuordnen)

Mit diesem Befehl können ein oder mehrere Clients einem Zeitplan zugeordnet werden. Sie müssen einen Clientknoten der Maßnahmendomäne zuordnen, zu der ein Zeitplan gehört. Client-Knoten verarbeiten Operationen gemäß den Zeitplänen, die den Knoten zugeordnet sind.

Anmerkung:

1. IBM Spectrum Protect kann nicht mehrere Zeitpläne gleichzeitig für denselben Clientknoten ausführen.

2. In einem Makro kann der Server blockieren, wenn einige Befehle (z. B. REGISTER NODE und DEFINE ASSOCIATION) nicht festgeschrieben werden, sobald sie ausgegeben werden. Hinter jedem Befehl in einem Makro könnte ein Befehl COMMIT angegeben werden. Einfacher ist es jedoch, die Option -ITEMCOMMIT im Befehl DSMADMC anzugeben.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Zeitplan gehört

Syntax

```
>>-DEFine ASSOCiation--Domänenname--Zeitplanname---------------->

   .-,----------.
   V            |
>----Knotenname-+---------------------------------------------><
```

Parameter

Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an, zu der der Zeitplan gehört.

Zeitplanname (Erforderlich)
: Gibt den Namen des Zeitplans an, der einem oder mehreren Clients zugeordnet werden soll.

Knotenname (Erforderlich)
: Gibt den Namen eines Clientknotens oder eine Liste mit Clientknoten an, der bzw. die dem angegebenen Zeitplan zugeordnet werden soll(en). Verwenden Sie Kommas, um die Einträge in der Liste voneinander zu trennen. Lassen Sie keine Leerzeichen zwischen den Einträgen und den Kommas. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Der Befehl ordnet einen aufgelisteten Client dem Zeitplan nicht zu, wenn:

  - Der Client bereits dem angegebenen Zeitplan zugeordnet wurde.
  - Der Client nicht der Maßnahmendomäne zugeordnet ist, zu der der Zeitplan gehört.
  - Der Client ein NAS-Knotenname ist. Alle NAS-Knoten werden ignoriert.

Beispiel: Clientknoten einem Zeitplan zuordnen

Die Clientknoten SMITH und JOHN dem Zeitplan WEEKLY_BACKUP zuordnen. Die zugeordneten Clients sind der Maßnahmendomäne EMPLOYEE_RECORDS zugeordnet.

```
define association employee_records
weekly_backup smith*,john*
```

Beispiel: Clientknoten einem Zeitplan zuordnen

Die Clientknoten JOE, TOM und LARRY dem Zeitplan WINTER zuordnen. Die zugeordneten Clients sind der Maßnahmendomäne EMPLOYEE_RECORDS zugeordnet; der Client JOE ist jedoch bereits dem Zeitplan WINTER zugeordnet.

```
define association employee_records
winter joe,tom,larry
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE ASSOCIATION

Befehl	Beschreibung
DEFINE SCHEDULE	Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.
DELETE ASSOCIATION	Löscht die Zuordnung zwischen Clients und einem Zeitplan.
DELETE SCHEDULE	Löscht einen Zeitplan aus der Datenbank.
QUERY ASSOCIATION	Zeigt die Clients an, die einem oder mehreren Zeitplänen zugeordnet sind.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.

DEFINE BACKUPSET (Sicherungsgruppe definieren)

Mit diesem Befehl kann eine Clientsicherungsgruppe definiert werden, die zuvor auf einem Server generiert wurde, und die Sicherungsgruppe für den Server verfügbar gemacht werden, auf dem dieser Befehl ausgeführt wird. Der Clientknoten hat die Option, die Sicherungsgruppe von dem Server zurückzuschreiben, der diesen Befehl ausführt, und nicht von dem Server, auf dem die Sicherungsgruppe generiert wurde.

Jede Sicherungsgruppe, die auf einem Server generiert wurde, kann für einen anderen Server definiert werden, wenn die Server einen Einheitentyp gemeinsam benutzen. Die Stufe des Servers, für die die Sicherungsgruppe definiert wird, muss mindestens so hoch sein wie die Stufe des Servers, der die Sicherungsgruppe generiert hat.

Der Befehl DEFINE BACKUPSET kann auch verwendet werden, um eine Sicherungsgruppe erneut zu definieren, die auf einem Server gelöscht wurde.

Berechtigungsklasse

Wird die Serveroption REQSYSAUTHOUTFILE auf YES (Standardwert) gesetzt, muss der Administrator die Systemberechtigung haben. Ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator über Systemberechtigung oder Maßnahmenberechtigung für die Domäne verfügen, der der Clientknoten zugeordnet ist.

Syntax

Parameter

Knotenname oder Knotengruppenname (Erforderlich)
: Gibt den Namen der Clientknoten oder Knotengruppen an, deren Daten in den angegebenen Sicherungsgruppendatenträgern enthalten sind. Sollen mehrere Knoten- und Knotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Knotennamen können Platzhalterzeichen enthalten, Knotengruppennamen dagegen nicht. Wenn die Sicherungsgruppendatenträger Sicherungsgruppen von mehreren Knoten enthalten, wird jede Sicherungsgruppe, deren Knotenname mit einem der angegebenen Knotennamen übereinstimmt, definiert. Enthalten die Datenträger eine Sicherungsgruppe für einen Knoten, der gegenwärtig nicht registriert ist, wird mit dem Befehl DEFINE BACKUPSET die Sicherungsgruppe für diesen Knoten nicht definiert.

Präfix_des_Sicherungsgruppennamens (Erforderlich)
: Gibt den Namen der Sicherungsgruppe an, die für diesen Server definiert werden soll. Die maximale Länge des Namens beträgt 30 Zeichen.

  Wird ein Name ausgewählt, fügt IBM Spectrum Protect ein Suffix hinzu, um den Sicherungsgruppennamen zu erstellen. Wird die Sicherungsgruppe beispielsweise *mybackupset* genannt, fügt IBM Spectrum Protect eine eindeutige Zahl wie beispielsweise 3099 zum

Namen hinzu. Der Sicherungsgruppenname wird dann als *mybackupset.3099* identifiziert. Sollen später Informationen über diese Sicherungsgruppe angezeigt werden, kann in den Namen ein Platzhalterzeichen wie beispielsweise *mybackupset** eingefügt oder der vollständig qualifizierte Name wie beispielsweise *mybackupset.3099* angegeben werden.

Enthalten die Sicherungsgruppendatenträger Sicherungsgruppen für mehrere Knoten, werden Sicherungsgruppen für jeden der Knoten unter Verwendung desselben Präfix und Suffix des Sicherungsgruppennamens definiert.

DEVclass (Erforderlich)
Gibt den Namen der Einheitenklasse für die Datenträger an, von denen die Sicherungsgruppe gelesen wird.
Anmerkung: Der Einheitentyp, der der angegebenen Einheitenklasse zugeordnet ist, muss mit der Einheitenklasse übereinstimmen, mit der die Sicherungsgruppe ursprünglich generiert wurde.

VOLumes (Erforderlich)
Gibt die Namen der Datenträger an, die zum Speichern der Sicherungsgruppe verwendet werden. Es können mehrere Datenträger angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Die angegebenen Datenträger müssen für den Server verfügbar sein, der die Sicherungsgruppe definiert.
Anmerkung: Die angegebenen Datenträger müssen in der Reihenfolge ihrer Erstellung aufgelistet sein; andernfalls schlägt der Befehl DEFINE BACKUPSET fehl.
Der Server prüft nicht, ob jeder Datenträger, der für eine Sicherungsgruppe mit mehreren Datenträgern angegeben ist, einen Teil der Sicherungsgruppe enthält. Der erste Datenträger wird immer überprüft, und in einigen Fällen werden auch zusätzliche Datenträger überprüft. Sind diese Datenträger korrekt, wird die Sicherungsgruppe definiert, und es werden alle im Befehl aufgelisteten Datenträger vor dem Überschreiben geschützt. Ist ein Datenträger, der einen Teil der Sicherungsgruppe enthält, nicht in dem Befehl aufgelistet, wird der Datenträger nicht geschützt und kann während der normalen Serveroperationen überschrieben werden.
Anmerkung: Standardmäßig versucht der Server, ein Inhaltsverzeichnis zu erstellen, wenn eine Sicherungsgruppe definiert wird. Wird ein falscher Datenträger angegeben oder sind Datenträger nicht in der korrekten Reihenfolge aufgelistet, schlägt die Erstellung des Inhaltsverzeichnisses fehl. Tritt dieser Fehler auf, überprüfen Sie die Datenträgerliste in dem Befehl und ziehen Sie die Verwendung des Befehls QUERY BACKUPSETCONTENTS in Betracht, um den Inhalt der Sicherungsgruppe zu prüfen.

RETention
Gibt die Anzahl Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt wird.Sie können eine ganze Zahl von 0 bis 30000 angeben. Der Standardwert ist 365 Tage. Gültige Werte:

Tage
Gibt die Anzahl der Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt werden soll.

NOLimit
Gibt an, dass die Sicherungsgruppe auf dem Server unbegrenzt aufbewahrt werden muss.

Wird NOLIMIT angegeben, werden die Datenträger mit der Sicherungsgruppe von IBM Spectrum Protect unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datenträger aus dem Serverspeicher.

DESCription
Gibt die Beschreibung an, die der Sicherungsgruppe zugeordnet werden soll, die zu dem Client-Knoten gehört. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

WHEREDATAType
Gibt an, dass die Sicherungsgruppen mit den angegebenen Typen von Daten definiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) definiert werden sollen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Gültige Werte:

ALL
Gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) definiert werden sollen. ALL ist der Standardwert.

FILE
Gibt an, dass eine Sicherungsgruppe auf Dateiebene definiert werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Sicherungsclient gesichert werden.

IMAGE
Gibt an, dass eine Imagesicherungsgruppe definiert werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Clients für Sichern/Archivieren erstellt wurden.

TOC
Gibt an, ob ein Inhaltsverzeichnis (Table of contents - TOC) für die Sicherungsgruppe auf Dateiebene erstellt werden muss, wenn sie definiert wird. Der Parameter TOC wird ignoriert, wenn Image- und Anwendungssicherungsgruppen definiert werden, da für diese Sicherungsgruppen immer ein Inhaltsverzeichnis erstellt wird.
Sie sollten bei der Festlegung, ob ein Inhaltsverzeichnis erstellt werden soll, Folgendes berücksichtigen:

- Wird ein Inhaltsverzeichnis erstellt, können Sie den IBM Spectrum Protect-Webclient für Sichern/Archivieren verwenden, um die gesamte Dateisystemstruktur zu untersuchen und Dateien und Verzeichnisse zum Zurückschreiben auszuwählen. Für die Erstellung eines Inhaltsverzeichnisses müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, die mit dem Parameter TOCMGMTCLASS angegeben wird. Die Erstellung eines Inhaltsverzeichnisses erfordert zusätzliche Verarbeitung, zusätzlichen Speicherpoolbereich und möglicherweise einen Mountpunkt während der Sicherungsgruppenoperation.

- Wird ein Inhaltsverzeichnis für eine Sicherungsgruppe nicht gesichert, können Sie dennoch einzelne Dateien oder Verzeichnisstrukturen mit dem Befehl RESTORE BACKUPSET des Clients für Sichern/Archivieren zurückschreiben, wenn Sie den vollständig qualifizierten Namen jeder Datei oder jedes Verzeichnisses kennen, die bzw. das zurückgeschrieben werden soll.

Dieser Parameter ist wahlfrei. Der Standardwert ist Preferred. Gültige Werte:

No
: Gibt an, dass keine Inhaltsverzeichnisinformationen für Sicherungsgruppen auf Dateiebene gesichert werden.

Preferred
: Gibt an, dass Inhaltsverzeichnisinformationen für Sicherungsgruppen auf Dateiebene gesichert werden müssen. Eine Sicherungsgruppe ist jedoch nicht fehlerhaft, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

Yes
: Gibt an, dass Inhaltsverzeichnisinformationen für jede Sicherungsgruppe auf Dateiebene gesichert werden müssen. Eine Sicherungsgruppe ist fehlerhaft, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

TOCMGmtclass
: Gibt den Namen der Verwaltungsklasse an, an die das Inhaltsverzeichnis gebunden werden muss. Wird keine Verwaltungsklasse angegeben, wird das Inhaltsverzeichnis an die Standardverwaltungsklasse für die Maßnahmendomäne gebunden, der der Knoten zugeordnet ist. In diesem Fall müssen Sie für die Erstellung des Inhaltsverzeichnisses das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die angegebene Verwaltungsklasse definieren.

Beispiel: Eine Sicherungsgruppe definieren

Die Sicherungsgruppe PERS_DATA, die zum Clientknoten JANE gehört, für den Server definieren, der diesen Befehl ausführt. Die Sicherungsgruppe auf dem Server 50 Tage aufbewahren. Angeben, dass die Datenträger VOL001 und VOL002 die Daten für die Sicherungsgruppe enthalten. Die Datenträger sollen von einer Einheit gelesen werden, die der Einheitenklasse AGADM zugeordnet ist. Eine Beschreibung einschließen.

```
define backupset jane pers_data devclass=agadm
volumes=vol1,vol2 retention=50
description="Basisimage Sektor 7"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE BACKUPSET

Befehl	Beschreibung
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DELETE NODEGROUP	Löscht eine Knotengruppe.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
GENERATE BACKUPSETTOC	Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
QUERY BACKUPSETCONTENTS	Zeigt den Inhalt in Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

DEFINE CLIENTACTION (Einmalige Clientaktion definieren)

Mit diesem Befehl können ein oder mehrere Clients für die Verarbeitung eines Befehls für eine einmalige Aktion geplant werden.

Der Server definiert automatisch einen Zeitplan und ordnet dem Zeitplan den Clientknoten zu. Der Server ordnet dem Zeitplan Priorität 1 zu, setzt PERUNITS auf ONETIME und bestimmt die Anzahl der Tage, die der Zeitplan aktiv bleiben soll. Die Anzahl der Tage basiert auf dem Wert, der mit dem Befehl SET CLIENTACTDURATION definiert wird.

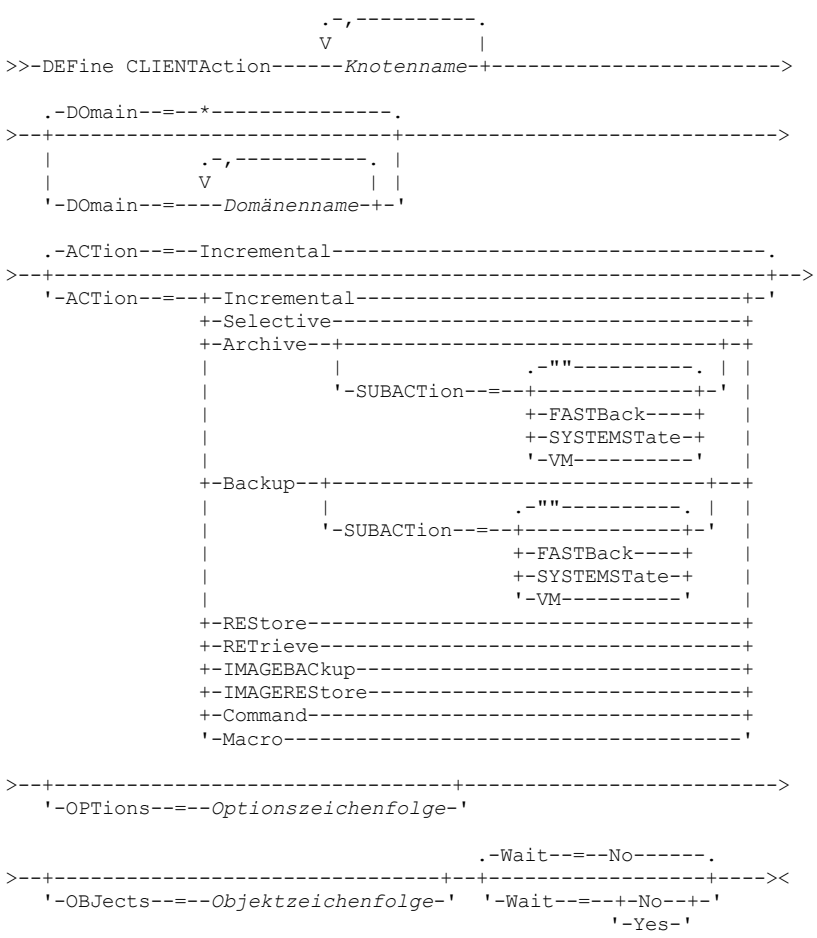
Wie schnell der Client diesen Befehl verarbeitet, ist davon abhängig, ob der Planungsmodus für den Client auf Serversystemanfrage (server-prompted) oder auf Clientsendeaufruf (client-polling) gesetzt ist. Der Client-Scheduler muss auf der Clientdatenstation gestartet werden, damit der Server den Zeitplan verarbeiten kann.

Hinweis: Der Start des IBM Spectrum Protect-Schedulers hängt von der Verarbeitung anderer Threads im Server und anderer Prozesse auf dem IBM Spectrum Protect-Server-Hostsystem ab. Die Zeit, die benötigt wird, um den Scheduler zu starten, hängt außerdem vom Datenaustausch im Netz und davon ab, wie lange es dauert, bis ein Socket geöffnet, die Verbindung zum IBM Spectrum Protect-Client hergestellt und eine Antwort vom Client empfangen wird. Im Allgemeinen gilt: Je größer die Verarbeitungs- und Konnektivitätsanforderungen auf dem IBM Spectrum Protect-Server und -Client sind, desto länger kann es dauern, bis der Scheduler gestartet wird.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Zeitplan gehört.

Syntax



Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, der den Zeitplan verarbeitet, der der Aktion zugeordnet ist. Werden mehrere Knotennamen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können den Stern als Platzhalterzeichen verwenden, um mehrere Namen anzugeben.

DOmain
: Gibt die Liste der Maßnahmendomänen an, mit der die Liste der Client-Knoten begrenzt wird. Nur Client-Knoten, die einer der angegebenen Maßnahmendomänen zugeordnet sind, werden bei der Planung berücksichtigt. Für alle Clients, die einer übereinstimmenden Domäne zugeordnet sind, erfolgt eine Planung. Mehrere Domänennamen sind ohne Leerzeichen durch Kommas voneinander zu trennen. Wird kein Wert angegeben, werden alle Maßnahmendomänen in der Liste berücksichtigt.

ACTion
: Gibt die Aktion an, die bei der Verarbeitung dieses Zeitplans ausgeführt wird.Gültige Werte:

  Incremental
  : Gibt an, daß der Zeitplan alle Dateien sichert, die neu sind oder sich seit der letzten Teilsicherung geändert haben. Mit "Incremental" werden auch alle Dateien gesichert, für die alle vorhandenen Sicherungen möglicherweise verfallen sind.

  Selective
  : Gibt an, daß der Zeitplan nur Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.

Archive
Gibt an, daß der Zeitplan Dateien archiviert, die mit dem Parameter OBJECTS angegeben werden.
Backup
Gibt an, dass der Zeitplan Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.
REStore
Gibt an, daß der Zeitplan Dateien zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

Wenn Sie ACTION=RESTORE für eine geplante Operation angeben, und ist die Option REPLACE auf PROMPT gesetzt, erfolgt keine Aufforderung. Wird die Option auf PROMPT gesetzt, werden die Dateien übersprungen.

Wenn Sie eine zweite Dateispezifikation angeben, agiert diese zweite Dateispezifikation als Zielort für die Zurückschreibung. Müssen mehrere Gruppen von Dateien zurückgeschrieben werden, planen Sie eine für jede Dateispezifikation, die zurückgeschrieben werden muss.

RETrieve
Gibt an, dass der Zeitplan Dateien abruft, die mit dem Parameter OBJECTS angegeben werden.
Hinweis: Eine zweite Datei, die angegeben wird, dient als Abrufzielort. Müssen mehrere Gruppen von Dateien abgerufen werden, erstellen Sie einen separaten Zeitplan für jede Dateigruppe.
IMAGEBACkup
Gibt an, daß der Zeitplan logische Datenträger sichert, die mit dem Parameter OBJECTS angegeben werden.
IMAGEREStore
Gibt an, daß der Zeitplan logische Datenträger zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.
Command
Gibt an, dass der Zeitplan einen Client-Betriebssystembefehl oder ein Script verarbeitet, der bzw. das mit dem Parameter OBJECTS angegeben wird.
Macro
Gibt an, daß ein Client ein Makro verarbeitet, dessen Dateiname im Parameter OBJECTS angegeben ist.
SUBACTion
Sie können einen der folgenden Werte angeben:

""
Wenn eine Nullzeichenfolge (zwei Anführungszeichen) mit ACTION=BACKUP angegeben wird, ist die Sicherung eine Teilsicherung.
FASTBAck
Gibt an, dass eine FastBack-Clientoperation, die durch den Parameter ACTION angegeben wird, für die Verarbeitung geplant werden soll. Der Wert des Parameters ACTION muss ARCHIVE oder BACKUP sein.
SYSTEMSTate
Gibt an, dass eine Clientsystemstatussicherung geplant ist.
VApp
Gibt an, dass eine vApp-Clientsicherung geplant ist. Eine vApp ist eine Sammlung von vorimplementierten virtuellen Maschinen.
VM
Gibt an, dass eine VMware-Clientsicherungsoperation geplant ist.

OPTions
Gibt die Clientoptionen an, die für den geplanten Befehl angegeben werden, wenn der Zeitplan verarbeitet wird. Dieser Parameter ist wahlfrei.
Für diesen Parameter können nur die Optionen angegeben werden, die für den geplanten Befehl gültig sind. Informationen zu den Optionen, die in der Befehlszeile gültig sind, befinden sich im entsprechenden Clienthandbuch. Alle Optionen, für die im Clienthandbuch angegeben ist, dass sie nur in der Anfangsbefehlszeile gültig sind, führen zu einem Fehler oder werden ignoriert, wenn der Zeitplan vom Server ausgeführt wird. Geben Sie beispielsweise die folgenden Optionen nicht an, da sie keinen Einfluss darauf haben, wann der Client den geplanten Befehl verarbeitet:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

Windows-BetriebssystemeWenn Sie einen Scheduler-Service definieren, indem Sie den Befehl DSMCUTIL oder den Assistenten für die GUI des Clients für Sichern/Archivieren verwenden, geben Sie eine Optionsdatei an. Sie können die Optionen in dieser Optionsdatei nicht überschreiben, indem Sie den geplanten Befehl ausgeben. Sie müssen die Optionen in Ihrem Schedulerservice ändern.

Enthält die Optionszeichenfolge mehrere Optionen oder Optionen mit eingebetteten Leerzeichen, schließen Sie die gesamte Optionszeichenfolge in Hochkommas ein. Schließen Sie einzelne Optionen, die Leerzeichen enthalten, in Anführungszeichen ein. Vor der Option muss ein führendes Minuszeichen stehen. Fehler können auftreten, wenn die Optionszeichenfolge Leerzeichen enthält, die nicht korrekt in Anführungszeichen eingeschlossen sind.

Die folgenden Beispiele zeigen, wie einige Clientoptionen angegeben werden:

- Geben Sie Folgendes ein, um `subdir=yes` und `domain all-local -systemobject` anzugeben:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Geben Sie Folgendes ein, um `domain all-local -c: -d:` anzugeben:
  - `options='-domain="all-local -c: -d:"'`

 Windows-BetriebssystemeTipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

OBJects

Gibt die Objekte an, für die die angegebene Aktion ausgeführt wird. Verwenden Sie ein einzelnes Leerzeichen zwischen jedem Objekt. Außer bei ACTION=INCREMENTAL ist dieser Parameter erforderlich. Ist die Aktion eine Sicherungs-, Archivierungs-, Abruf- oder Zurückschreibungsoperation, sind die Objekte Dateibereiche, Verzeichnisse oder logische Datenträger. Dient die Aktion zur Ausführung eines Befehls oder Makros, ist das Objekt der Name des auszuführenden Befehls oder Makros.

Wenn ACTION=INCREMENTAL ohne Angabe eines Werts für diesen Parameter angegeben wird, wird der geplante Befehl ohne angegebene Objekte aufgerufen, und der Befehl versucht, die Objekte wie in der Clientoptionsdatei definiert zu verarbeiten. Um alle Dateibereiche oder Verzeichnisse für eine Aktion auszuwählen, müssen sie explizit in der Objektzeichenfolge aufgeführt werden. Wird nur ein Stern in die Objektzeichenfolge eingegeben, erfolgt die Sicherung nur für das Verzeichnis, bei dem der Scheduler gestartet wurde.

Wichtig:

- Wenn Sie eine zweite Dateispezifikation angeben, und handelt es sich nicht um einen gültigen Zielort, empfangen Sie diesen Fehler:

  ```
  ANS1082E Ungültige
  Zieldateispezifikation <Dateispezifikation> eingegeben.
  ```

- Geben Sie mehr als zwei Dateispezifikationen an, empfangen Sie diesen Fehler:

  ```
  ANS1102E Zu viele Befehlszeilenparameter an das Programm übergeben!
  ```

Wird für diesen Parameter ACTION=ARCHIVE, INCREMENTAL oder SELECTIVE angegeben, können Sie maximal 20 Dateispezifikationen auflisten.

Schließen Sie die Objektzeichenfolge in Anführungszeichen ein, wenn sie Leerzeichen enthält, und schließen Sie dann die Anführungszeichen in Hochkommas ein. Enthält die Objektzeichenfolge mehrere Dateinamen, schließen Sie jeden Dateinamen in Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Fehler können auftreten, wenn Dateinamen ein Leerzeichen enthalten, das nicht korrekt in Anführungszeichen eingeschlossen ist.

 Windows-BetriebssystemeWenn Sie Zeichen verwenden, die für Windows-Benutzer eine besondere Bedeutung haben, wie z. B. Kommas, schließen Sie das gesamte Argument in doppelte Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Die folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

- Geben Sie Folgendes ein, um C:\FILE 2, D:\GIF FILES und E:\MY TEST FILE anzugeben:
  - `OBJECTS='"C:\FILE 2" "D:\GIF FILES" "E:\MY TEST FILE"'`
- Geben Sie Folgendes ein, um D:\TEST FILE anzugeben:
  - `OBJECTS='"D:\TEST FILE"'`
- Geben Sie Folgendes ein, um D:TEST,FILE anzugeben:
  - `OBJECTS='""D:\TEST,FILE""'`

 AIX-Betriebssysteme  Linux-BetriebssystemeDie folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

- Geben Sie Folgendes ein, um /home/file 2, /home/gif files und /home/my test file anzugeben:
  - `OBJECTS='"/home/file 2" "/home/gif files" "/home/my test file"'`
- Geben Sie Folgendes ein, um /home/test file anzugeben:
  - `OBJECTS='"/home/test file"'`

 Windows-BetriebssystemeTipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

Wait

Gibt an, ob auf die Beendigung einer geplanten Clientoperation gewartet werden soll. Dieser Parameter ist nützlich, wenn Clientaktionen aus einer Befehlsprozedur oder einem Makro definiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

No

Gibt an, dass nicht auf die Beendigung der geplanten Clientoperation gewartet wird. Wird dieser Wert angegeben und hat der Parameter ACTION den Wert COMMAND, gibt der Rückkehrcode an, ob die Clientaktion definiert wurde.

Yes

Gibt an, dass auf die Beendigung der geplanten Clientoperation gewartet wird. Wird dieser Wert angegeben und hat der Parameter ACTION den Wert COMMAND, gibt der Rückkehrcode den Status der Clientoperation an.

Der Befehl DEFINE CLIENTACTION mit WAIT=YES kann nicht von der Serverkonsole ausgegeben werden. Der Administrator kann jedoch von der Serverkonsole:

- WAIT=YES mit DEFINE CLIENTACTION als Befehlszeile eines Befehls DEFINE SCRIPT angeben.
- WAIT=YES mit DEFINE CLIENTACTION als Befehlszeile einer Datei angeben, deren Inhalt in die Prozedur eingelesen wird, die durch einen Befehl DEFINE SCRIPT definiert wird.

Einschränkung: Wird der Befehl DEFINE CLIENTACTION mit WAIT=YES in einem Makro angegeben, werden die mit dem Befehl definierten sofortigen Zeitpläne nicht zurückgesetzt, wenn das Makro nicht erfolgreich ausgeführt wird.

Beispiel: Eine einmalige Teilsicherung ausführen

Einen Teilsicherungsbefehl für Clientknoten TOM ausgeben, der der Maßnahmendomäne EMPLOYEE_RECORDS zugeordnet ist. IBM Spectrum Protect definiert einen Zeitplan und ordnet ihn dem Clientknoten TOM zu (vorausgesetzt, der Client-Scheduler ist aktiv).

```
define clientaction tom domain=employee_records
action=incremental
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE CLIENTACTION

Befehl	Beschreibung
DELETE SCHEDULE	Löscht einen Zeitplan aus der Datenbank.
QUERY ASSOCIATION	Zeigt die Clients an, die einem oder mehreren Zeitplänen zugeordnet sind.
QUERY EVENT	Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an.
QUERY SCHEDULE	Zeigt Informationen über Zeitpläne an.
SET CLIENTACTDURATION	Gibt die Dauer eines mit dem Befehl DEFINE CLIENTACTION definierten Zeitplans an.

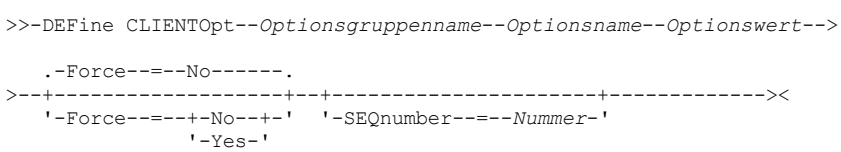
DEFINE CLIENTOPT (Option für eine Optionsgruppe definieren)

Mit diesem Befehl kann eine Clientoption einer Optionsgruppe hinzugefügt werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

Syntax



Parameter

Optionsgruppenname (Erforderlich)
Gibt den Namen der Optionsgruppe an.

Optionsname (Erforderlich)
Gibt eine Client-Option an, die der Optionsgruppe hinzugefügt werden soll.

In Clientoptionen, die vom Server definiert werden können befindet sich eine Liste mit gültigen Optionen.

Anmerkung: Um Einschluss-/Ausschlusswerte zu definieren, geben Sie die Option include oder exclude mit *Optionsname* an, und verwenden Sie *Optionswert*, um alle gültigen Einschluss- oder Ausschlussanweisungen anzugeben, so wie es in der Clientoptionsdatei erfolgen würde. Beispiel:

```
define clientopt Optionsgruppenname inclexcl "include c:\proj\text\devel.*"
```

Optionswert (Erforderlich)
Gibt den Wert für die Option an. Enthält die Option mehr als einen Wert, muss der Wert in Anführungszeichen eingeschlossen werden. Anmerkung:

1. Die Optionen QUIET und VERBOSE haben keinen Optionswert in der Clientoptionsdatei. Um diese Werte in einer Clientoptionsgruppe eines Servers anzugeben, geben Sie den Wert YES oder NO an.
2. Um eine Option INCLUDE oder EXCLUDE für einen Dateinamen hinzuzufügen, der ein oder mehrere Leerzeichen enthält, schließen Sie die Dateispezifikation in Hochkommas und die gesamte Option in Anführungszeichen ein. Weitere Informationen siehe Beispiel: Einer Clientoptionsgruppe eine Option hinzufügen.
3. Der *Optionswert* ist auf 1024 Zeichen begrenzt.

Force
Gibt an, ob der Server den Client zwingt, den Optionsgruppenwert zu verwenden. Der Wert wird für Zusatzoptionen, wie beispielsweise INCLEXCL und DOMAIN, ignoriert. Der Standardwert ist NO. Dieser Parameter ist wahlfrei. Gültige Werte:

Yes
Gibt an, dass der Server den Client zwingt, den Wert zu verwenden. (Der Client kann den Wert nicht überschreiben.)
No
Gibt an, dass der Server den Client nicht zwingt, den Wert zu verwenden. (Der Client kann den Wert überschreiben.)

SEQnumber
Gibt eine Folgenummer an, wenn ein Optionsname mehrmals angegeben wird. Dieser Parameter ist wahlfrei.

Beispiel: Einer Clientoptionsgruppe eine Option hinzufügen

Eine Clientoption (MAXCMDRETRIES 5) der Clientoptionsgruppe ENG hinzufügen.

```
define clientopt eng maxcmdretries 5
```

Beispiel: Eine Option hinzufügen, um eine Datei von der Sicherung auszuschließen

Eine Clientoption zur Optionsgruppe ENGBACKUP hinzufügen, um c:\admin\file.txt von Sicherungsservices auszuschließen.

```
define clientopt engbackup inclexcl "exclude c:\admin\file.txt"
```

Beispiel: Eine Option hinzufügen, um ein Verzeichnis von der Sicherung auszuschließen

Eine Clientoption zur Optionsgruppe WINSPEC hinzufügen, um ein temporäres Internet-Verzeichnis von den Sicherungsservices auszuschließen. Wenn Sie die Option EXCLUDE oder INCLUDE mit Dateinamen verwenden, die Leerzeichen enthalten, schließen Sie die Dateispezifikation in Hochkommas und die gesamte Option in Anführungszeichen ein.

```
define clientopt winspec inclexcl "exclude.dir '*:\...\Temporary
Internet Files'"
```

Beispiel: Eine Option hinzufügen, um Dateien in angegebenen Verzeichnissen zu binden

Clientoptionen zur Optionsgruppe WINSPEC hinzufügen, um alle Dateien in den Verzeichnissen C:\Data und C:\Program Files\My Apps an die Verwaltungsklasse PRODCLASS zu binden.

```
define clientopt winspec inclexcl "include C:\Data\...\* prodclass"
define clientopt winspec inclexcl "include 'C:\Program
      Files\My Apps\...\*' prodclass"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE CLIENTOPT

Befehl	Beschreibung
COPY CLOPTSET	Kopiert eine Clientoptionsgruppe.
DEFINE CLOPTSET	Definiert eine Clientoptionsgruppe.
DELETE CLIENTOPT	Löscht eine Clientoption aus einer Clientoptionsgruppe.
DELETE CLOPTSET	Löscht eine Clientoptionsgruppe.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.

Befehl	Beschreibung
QUERY CLOPTSET	Zeigt Informationen über eine Clientoptionsgruppe an.
UPDATE CLIENTOPT	Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe.
UPDATE CLOPTSET	Aktualisiert die Beschreibung einer Clientoptionsgruppe.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

DEFINE CLOPTSET (Clientoptionsgruppennamen definieren)

Mit diesem Befehl kann ein Name für eine Gruppe von Optionen definiert werden, die den Clients für Archivierungs-, Sicherungs-, Zurückschreibungs- und Abrufoperationen zugeordnet werden können.

Sollen Optionen der neuen Gruppe hinzugefügt werden, den Befehl DEFINE CLIENTOPT ausgeben.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

Syntax

```
>>-DEFine CLOptset--Optionsgruppenname--------------------------->

>--+-------------------------------+---------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Optionsgruppenname (Erforderlich)
: Gibt den Namen der Clientoptionsgruppe an. Die maximale Länge des Namens beträgt 64 Zeichen.

DESCription
: Gibt eine Beschreibung der Clientoptionsgruppe an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Dieser Parameter ist wahlfrei.

Beispiel: Eine Clientoptionsgruppe definieren

Um eine Clientoptionsgruppe mit dem Namen ENG zu definieren, den folgenden Befehl ausgeben:

```
define cloptset eng
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE CLOPTSET

Befehl	Beschreibung
COPY CLOPTSET	Kopiert eine Clientoptionsgruppe.
DEFINE CLIENTOPT	Fügt einer Clientoptionsgruppe eine Clientoption hinzu.
DELETE CLIENTOPT	Löscht eine Clientoption aus einer Clientoptionsgruppe.
DELETE CLOPTSET	Löscht eine Clientoptionsgruppe.
QUERY CLOPTSET	Zeigt Informationen über eine Clientoptionsgruppe an.
UPDATE CLIENTOPT	Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe.
UPDATE CLOPTSET	Aktualisiert die Beschreibung einer Clientoptionsgruppe.

DEFINE COLLOCGROUP (Kollokationsgruppe definieren)

Verwenden Sie diesen Befehl, um eine Kollokationsgruppe zu definieren. Eine *Kollokationsgruppe* ist eine Gruppe von Knoten oder Dateibereichen auf einem Knoten, deren Daten auf eine minimale Anzahl Datenträger mit sequenziellem Zugriff durch Kollokation zusammengefasst werden. Ihre Daten werden nur zusammengefasst, wenn in der Speicherpooldefinition die Kollokation nach Gruppe (COLLOCATE=GROUP) angegeben ist.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine COLLOCGroup--Gruppenname------------------------------>

>--+-----------------------------+--------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Gruppenname
: Gibt den Namen der Kollokationsgruppe an, die erstellt werden soll. Die maximale Länge des Namens beträgt 30 Zeichen.

DESCription
: Gibt eine Beschreibung der Kollokationsgruppe an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

Kollokationsgruppe definieren

Um eine Knoten- oder Dateibereichskollokationsgruppe mit dem Namen GROUP1 zu definieren, geben Sie den folgenden Befehl aus:

```
define collocgroup group1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE COLLOCGROUP

Befehl	Beschreibung
DEFINE COLLOCMEMBER	Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE COLLOCGROUP	Löscht eine Kollokationsgruppe.
DELETE COLLOCMEMBER	Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.
MOVE NODEDATA	Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
UPDATE COLLOCGROUP	Aktualisiert die Beschreibung einer Kollokationsgruppe.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

DEFINE COLLOCMEMBER (Kollokationsgruppenmitglied definieren)

Geben Sie diesen Befehl aus, um einen Clientknoten zu einer Kollokationsgruppe oder einen Dateibereich auf einem Knoten zu einer Kollokationsgruppe hinzuzufügen. Eine Kollokationsgruppe ist eine Gruppe von Knoten oder Dateibereichen auf einem Knoten, deren Daten auf eine minimale Anzahl Datenträger mit sequenziellem Zugriff durch Kollokation zusammengefasst werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
Knoten zu einer Kollokationsgruppe hinzufügen

                                     .-,----------.
                                     V            |
>>-DEFine COLLOCMember--Gruppenname----Knotenname-+------------><
```

Parameter

Gruppenname
: Gibt den Namen der Kollokationsgruppe an, der ein Clientknoten hinzugefügt werden soll.

Knotenname
: Gibt den Namen des Clientknotens an, der zur Kollokationsgruppe hinzugefügt werden soll. Sie können einen oder mehrere Namen angeben. Mehrere Namen sind durch Kommas voneinander zu trennen; verwenden Sie keine Leerzeichen zwischen den Namen. Sie können auch Platzhalterzeichen verwenden, um mehrere Namen anzugeben.

```
Dateibereich auf einem Knoten zu einer Kollokationsgruppe hinzufügen

>>-DEFine COLLOCMember--Gruppenname--Knotenname----------------->

                 .-,-----------------.
                 V                   |
>--FIlespace--=----Dateibereichsname-+-------------------------->

   .-NAMEType--=--SERVER------.
>--+--------------------------+--------------------------------->
   '-NAMEType--=--+-SERVER--+-'
                  +-UNIcode-+
                  '-FSID----'

   .-CODEType--=--BOTH-----------.
>--+-----------------------------+----------------------------><
   '-CODEType--=--+-BOTH-------+-'
                  +-UNIcode----+
                  '-NONUNIcode-'
```

Parameter

Gruppenname
: Gibt den Namen der Kollokationsgruppe an, der ein Dateibereich hinzugefügt werden soll.

Knotenname
: Gibt den Clientknoten an, auf dem sich der Dateibereich befindet.

FIlespace
: Gibt den *Dateibereichsnamen* auf dem Clientknoten an, der der Kollokationsgruppe hinzugefügt werden soll. Sie können einen oder mehrere Dateibereichsnamen angeben, die sich auf einem bestimmten Clientknoten befinden. Wenn Sie mehrere Dateibereichsnamen angeben, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können auch Platzhalterzeichen verwenden, um mehrere Dateibereichsnamen anzugeben. Beispiel:

  ```
  define collocmember manufacturing linux237 filespace=*_linux_fs
  ```

  Mit diesem Befehl werden alle Dateibereiche auf dem Knoten linux237 mit einem Namen, der mit _linux_fs endet, zur Kollokationsgruppe manufacturing hinzugefügt.
  Die folgende Liste enthält Tipps zum Arbeiten mit Kollokationsgruppen:

  - Wenn Sie einer neuen Kollokationsgruppe Mitglieder hinzufügen, bestimmt der Typ des ersten Kollokationsgruppenmitglieds den Typ der Kollokationsgruppe. Die Gruppe kann entweder eine Knotenkollokationsgruppe oder eine Dateibereichskollokationsgruppe sein.
    Einschränkung: Nachdem der Typ der Kollokationsgruppe definiert wurde, kann er nicht geändert werden.
  - Typen von Kollokationsgruppenmitgliedern können nicht gemischt werden, wenn Sie einer Kollokationsgruppe (Knotengruppe oder Dateibereichsgruppe) Mitglieder hinzufügen.
  - Für eine Dateibereichskollokationsgruppe können Sie Dateibereiche zur Gruppe hinzufügen. Die Dateibereiche müssen denselben Wert wie der Parameter *Knotenname* verwenden, der bei der Erstellung der Kollokationsgruppe angegeben wird.
  - Ein Clientknoten kann in mehrere Dateibereichsgruppen eingeschlossen werden. Ist jedoch ein Knoten ein Mitglied einer Knotenkollokationsgruppe, kann er nicht ein Mitglied einer Dateibereichskollokationsgruppe sein.
  - Ein Dateibereich kann nur ein Mitglied einer Dateibereichsgruppe sein.

NAMEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Geben Sie diesen Parameter an, wenn der Server mit Clients kommuniziert, die über Unicode-Unterstützung verfügen. Ein Client für Sichern/Archivieren mit Unicode-Unterstützung ist nur für

Windows-, Macintosh OS 9-, Macintosh OS X- und NetWare-Systeme verfügbar. Der Dateibereichsname kann kein Platzhalterzeichen sein, wenn NAMETYPE für eine Dateibereichskollokationsgruppe angegeben wird. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

SERVER
: Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

UNIcode
: Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Die Zeichen in den Namen und die Server-Codepage bestimmen, ob die Namen konvertiert werden können. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Server-Codepage nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

FSID
: Der Server interpretiert die Dateibereichsnamen nach ihren Dateibereichs-IDs (FSIDs).

CODEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter, wenn Sie ein Platzhalterzeichen für den Dateibereichsnamen verwenden. Beispiel:

```
define collocmember production Win_3419 filespace=* codetype=unicode
```

Mit diesem Beispielbefehl werden alle Dateibereiche auf dem Knoten Win_3419 zur Kollokationsgruppe 'production' hinzugefügt. Der Standardwert lautet BOTH, d. h., die Dateibereiche werden unabhängig vom Codepagetyp eingeschlossen. Sie können einen der folgenden Werte angeben:

BOTH
: Die Dateibereiche unabhängig vom Codepagetyp einschließen.

UNIcode
: Nur Dateibereiche einschließen, die in Unicode sind.

NONUNIcode
: Dateibereiche einschließen, die nicht in Unicode sind.

Zwei Kollokationsgruppenmitglieder definieren

Die beiden Knoten NODE1 und NODE2 für die Kollokationsgruppe GROUP1 definieren.

```
define collocmember group1 node1,node2
```

Ein Dateibereichsgruppenmitglied CNTR90524 auf dem Knoten clifton für die Kollokationsgruppe TSM_alpha_1 definieren

```
define collocmember TSM_alpha_1 clifton filespace=CNTR90524
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE COLLOCMEMBER

Befehl	Beschreibung
DEFINE COLLOCGROUP	Definiert eine Kollokationsgruppe.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE COLLOCGROUP	Löscht eine Kollokationsgruppe.
DELETE COLLOCMEMBER	Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
MOVE NODEDATA	Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.

Befehl	Beschreibung
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
UPDATE COLLOCGROUP	Aktualisiert die Beschreibung einer Kollokationsgruppe.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

DEFINE COPYGROUP (Kopiengruppe definieren)

Mit diesem Befehl kann eine neue Sicherungs- oder Archivierungskopiengruppe in einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden. Der Server verwendet die Sicherungs- und Archivierungskopiengruppen, um zu steuern, wie Clients Dateien sichern und archivieren, und um die gesicherten und archivierten Dateien zu verwalten.

Um Clients die Verwendung der neuen Kopiengruppe zu ermöglichen, muss die Maßnahmengruppe aktiviert werden, die die neue Kopiengruppe enthält.

Für jede Verwaltungsklasse kann eine Sicherungskopiengruppe und eine Archivierungskopiengruppe definiert werden. Um sicherzustellen, dass Clientknoten Dateien sichern können, schließen Sie eine Sicherungskopiengruppe in der Standardverwaltungsklasse für eine Maßnahmengruppe ein.

Achtung: Der Befehl DEFINE COPYGROUP schlägt fehl, wenn ein Kopienspeicherpool als Ziel angegeben wird.

Der Befehl DEFINE COPYGROUP liegt in zwei Formen vor, eine zum Definieren einer Sicherungskopiengruppe und eine zum Definieren einer Archivierungskopiengruppe. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für DEFINE COPYGROUP

Befehl	Beschreibung
ASSIGN DEFMGMTCLASS	Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu.
BACKUP NODE	Sichert einen NAS-Knoten (NAS = Network Attached Storage).
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE COPYGROUP	Löscht eine Sicherungs- oder Archivierungskopiengruppe aus einer Maßnahmendomäne und Maßnahmengruppe.
DELETE MGMTCLASS	Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.
EXPIRE INVENTORY	Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.
SET ARCHIVERETENTIONPROTECTION	Gibt an, ob der Aufbewahrungsschutz für Daten aktiviert ist.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.

- DEFINE COPYGROUP (Sicherungskopiengruppe definieren)
  Mit diesem Befehl kann eine neue Sicherungskopiengruppe innerhalb einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden.
- DEFINE COPYGROUP (Archivierungskopiengruppe definieren)
  Mit diesem Befehl kann eine neue Archivierungskopiengruppe innerhalb einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden.

DEFINE COPYGROUP (Sicherungskopiengruppe definieren)

Mit diesem Befehl kann eine neue Sicherungskopiengruppe innerhalb einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Kopiengruppe gehört.

Syntax

```
>>-DEFine COpygroup--Domänenname--Name_der_Maßnahmengruppe--Klassenname-->

   .-STANDARD-.  .-Type--=--Backup-.
>--+----------+--+-----------------+---------------------------->
   '-STANDARD-'  '-Type--=--Backup-'

                             .-FREQuency--=--0----.
>--DESTination--=--Poolname--+--------------------+------------->
                             '-FREQuency--=--Tage-'

   .-VERExists--=--2-----------.
>--+--------------------------+------------------------------->
   '-VERExists--=--+-Anzahl--+-'
                   '-NOLimit-'

   .-VERDeleted--=--1-----------.
>--+----------------------------+------------------------------>
   '-VERDeleted--=--+-Anzahl--+-'
                    '-NOLimit-'

   .-RETExtra--=--30----------.  .-RETOnly--=--60----------.
>--+-------------------------+--+-------------------------+---->
   '-RETExtra--=--+-Tage----+-'  '-RETOnly--=--+-Tage----+-'
                  '-NOLimit-'                  '-NOLimit-'

   .-MODE--=--MODified-----.
>--+---------------------+------------------------------------->
   '-MODE--=--+-MODified-+-'
              '-ABSolute-'

   .-SERialization--=--SHRSTatic------.
>--+---------------------------------+------------------------->
   '-SERialization--=--+-SHRSTatic--+-'
                       +-STatic-----+
                       +-SHRDYnamic-+
                       '-DYnamic----'

>--+---------------------------------+------------------------><
   '-TOCDestination--=-----Poolname---'
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, für die die Kopiengruppe definiert wird.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, für die die Kopiengruppe definiert wird.

  Für eine Verwaltungsklasse, die zu der aktiven Maßnahmengruppe (ACTIVE) gehört, kann keine Kopiengruppe definiert werden.

Klassenname (Erforderlich)
: Gibt die Verwaltungsklasse an, für die die Kopiengruppe definiert wird.

STANDARD
: Gibt den Namen der Kopiengruppe an, der STANDARD lauten muss. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD.

Type=Backup
: Gibt an, dass eine Sicherungskopiengruppe definiert werden soll. Der Standardparameter ist BACKUP. Dieser Parameter ist wahlfrei.

DESTination (Erforderlich)
: Gibt den primären Speicherpool an, in dem der Server anfänglich Sicherungsdaten speichert. Ein Kopienspeicherpool kann nicht als Zielort angegeben werden.

FREQuency
: Gibt an, wie oft IBM Spectrum Protect eine Datei sichern kann. Dieser Parameter ist wahlfrei. IBM Spectrum Protect sichert eine Datei nur, wenn die angegebene Anzahl Tage seit der letzten Sicherung verstrichen ist. Der Wert für den Parameter FREQUENCY wird nur bei einer vollständigen Teilsicherung verwendet. Dieser Wert wird bei einer selektiven Sicherung oder einer partiellen Teilsicherung ignoriert. Zulässige Werte sind ganze Zahlen von 0 bis 9999. Der Standardwert ist 0. Dieser Standardwert bedeutet, daß IBM Spectrum Protect eine Datei unabhängig vom Datum der letzten Sicherung sichern kann.

VERExists

Gibt die maximale Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die sich momentan im Client-Dateisystem befinden. Dieser Parameter ist wahlfrei. Der Standardwert ist 2.
Wird der Grenzwert durch eine Teilsicherungsoperation überschritten, verfällt die älteste Sicherungsversion, die im Serverspeicher vorhanden ist. Gültige Werte:

Zahl
: Gibt die Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die sich momentan im Client-Dateisystem befinden. Zulässige Werte sind ganze Zahlen von 1 bis 9999.

NOLimit
: Gibt an, daß der Server alle Sicherungsversionen aufbewahren soll.

Die Anzahl der Sicherungsversionen, die aufbewahrt werden sollen, wird so lange durch diesen Parameter gesteuert, bis Versionen den Aufbewahrungszeitraum überschreiten, der durch den Parameter RETEXTRA angegeben ist.

VERDeleted
: Gibt die maximale Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die aus dem Client-Dateisystem gelöscht wurden, nachdem sie mit IBM Spectrum Protect gesichert wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist 1.
Löscht ein Benutzer eine Datei aus dem Clientdateisystem, werden bei der nächsten Teilsicherung die ältesten Versionen der Datei, die diese Anzahl überschreiten, von dem Server als verfallen gekennzeichnet. Das Verfallsdatum der übrigen Versionen wird durch den Aufbewahrungszeitraum bestimmt, der mit dem Parameter RETEXTRA oder RETONLY angegeben wurde. Gültige Werte:

Anzahl
: Gibt die Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die nach der Sicherung aus dem Client-Dateisystem gelöscht werden. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

NOLimit
: Gibt an, dass der Server alle Sicherungsversionen für Dateien, die nach der Sicherung aus dem Clientdateisystem gelöscht werden, aufbewahren soll.

RETExtra
: Gibt die Anzahl Tage an, die eine Sicherungsversion aufbewahrt werden soll, nachdem diese Version inaktiv wurde. Die Version einer Datei wird inaktiv, wenn der Client eine aktuellere Sicherungsversion speichert oder wenn der Client die Datei aus der Datenstation löscht und dann eine vollständige Teilsicherung durchführt. Der Server löscht inaktive Versionen auf der Basis des Aufbewahrungszeitraums, auch wenn die Anzahl der inaktiven Versionen die durch den Parameter VEREXISTS oder VERDELETED erlaubte Anzahl nicht überschreitet. Dieser Parameter ist wahlfrei. Der Standardwert ist 30 Tage. Gültige Werte:

Tage
: Gibt die Anzahl Tage an, die inaktive Sicherungsversionen aufbewahrt werden sollen. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

NOLimit
: Gibt an, dass inaktive Sicherungsversionen unbegrenzt aufbewahrt werden sollen.

  Wird NOLIMIT angegeben, löscht der Server inaktive Sicherungsversionen auf der Basis des Parameters VEREXISTS (wenn die Datei noch im Clientdateisystem vorhanden ist) oder auf der Basis des Parameters VERDELETED (wenn die Datei nicht mehr im Clientdateisystem vorhanden ist).

RETOnly
: Gibt die Anzahl Tage an, die die letzte Sicherungsversion einer Datei aufbewahrt werden soll, die aus dem Client-Dateisystem gelöscht wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Gültige Werte:

Tage
: Gibt die Anzahl Tage an, die die letzte verbleibende inaktive Version einer Datei aufbewahrt werden soll. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

NOLimit
: Gibt an, dass die letzte verbleibende inaktive Version einer Datei unbegrenzt aufbewahrt werden soll.

  Wird NOLIMIT angegeben, wird die letzte verbleibende Sicherungsversion unbegrenzt von dem Server aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datei aus dem Server-Speicher.

MODE
: Gibt an, ob IBM Spectrum Protect eine Datei nur sichert, wenn sich die Datei seit der letzten Sicherung geändert hat oder wenn ein Client eine Sicherung anfordert. Dieser Parameter ist wahlfrei. Der Standardwert ist MODIFIED. Gültige Werte:

MODified
: Gibt an, dass IBM Spectrum Protect die Datei nur sichert, wenn sie sich seit der letzten Sicherung geändert hat. IBM Spectrum Protect betrachtet eine Datei als geändert, wenn folgende Bedingungen zutreffen:

  - Das Datum der letzten Änderung hat sich geändert.
  - Die Dateigröße hat sich geändert.
  - Der Dateieigner hat sich geändert.
  - Die Dateiberechtigungen haben sich geändert.

ABSolute

Gibt an, dass IBM Spectrum Protect die Datei sichert, unabhängig davon, ob sie sich geändert hat.

Der Wert für MODE wird nur für vollständige Teilsicherungen verwendet. Dieser Wert wird bei einer partiellen Teilsicherung oder einer selektiven Sicherung ignoriert.

SERialization
Gibt an, wie IBM Spectrum Protect Dateien oder Verzeichnisse verarbeitet, wenn sie während der Sicherungsverarbeitung geändert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist SHRSTATIC. Gültige Werte:

SHRSTatic
Gibt an, dass IBM Spectrum Protect eine Datei oder ein Verzeichnis nur sichert, wenn die Datei oder das Verzeichnis während der Sicherung nicht geändert wird. IBM Spectrum Protect versucht bis zu viermal, eine Sicherung durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde. Wird die Datei oder das Verzeichnis während jedes Sicherungsversuchs geändert, wird sie bzw. es von IBM Spectrum Protect nicht gesichert.

STatic
Gibt an, dass IBM Spectrum Protect eine Datei oder ein Verzeichnis nur sichert, wenn die Datei oder das Verzeichnis während der Sicherung nicht geändert wird. IBM Spectrum Protect versucht nur einmal, die Sicherung durchzuführen.

Plattformen, die die Option STATIC nicht unterstützen, nehmen den Standardwert SHRSTATIC an.

SHRDYnamic
Gibt an, dass IBM Spectrum Protect die Datei oder das Verzeichnis während des letzten Sicherungsversuchs sichert, auch wenn die Datei oder das Verzeichnis während der Sicherung geändert wird. IBM Spectrum Protect versucht bis zu viermal, eine Sicherung durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde.

DYnamic
Gibt an, dass IBM Spectrum Protect eine Datei oder ein Verzeichnis beim ersten Versuch sichert, auch wenn die Datei oder das Verzeichnis während der Sicherungsverarbeitung geändert wird.
Achtung: Die Werte SHRDYNAMIC und DYNAMIC sind mit Vorsicht zu verwenden. IBM Spectrum Protect bestimmt anhand dieser Werte, ob eine Datei oder ein Verzeichnis gesichert wird, während Änderungen vorgenommen werden. Aus diesem Grund ist die Sicherungsversion möglicherweise nur eine Sicherung mit grober Übereinstimmung. Eine Sicherung mit grober Übereinstimmung gibt den aktuellen Inhalt der Datei oder des Verzeichnisses nicht korrekt wieder, da sie einige, aber nicht alle Änderungen enthält. Wird eine Datei, die eine Sicherung mit grober Übereinstimmung enthält, zurückgeschrieben, ist die Datei möglicherweise nicht brauchbar. Dies ist von der Anwendung abhängig, die die Datei verwendet. Ist eine Sicherung mit grober Übereinstimmung nicht akzeptabel, definieren Sie für SERIALIZATION den Wert SHRSTATIC oder STATIC, damit IBM Spectrum Protect nur dann eine Sicherungsversion erstellt, wenn die Datei oder das Verzeichnis nicht geändert wird.

TOCDestination
Gibt den primären Speicherpool an, in dem ein Inhaltsverzeichnis für jede NDMP-Sicherungs- oder -Sicherungsgruppenoperation anfänglich gespeichert wird, für die ein Inhaltsverzeichnis generiert wird (NDMP - Network Data Management Protocol). Dieser Parameter ist wahlfrei. Ein Kopienspeicherpool kann nicht als Zielort angegeben werden. Der als Zielort angegebene Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben. Um Ladeverzögerungen zu vermeiden, wird empfohlen, dass der Speicherpool die Einheitenklasse DISK oder DEVTYPE=FILE hat. Die Generierung eines Inhaltsverzeichnisses ist eine Option für NDMP-Sicherungsoperationen, wird aber nicht für andere Imagesicherungsoperationen unterstützt.

Wird die Erstellung eines Inhaltsverzeichnisses (TOC) für eine Sicherungsoperation angefordert, die NDMP verwendet, und ist das Image an eine Verwaltungsklasse gebunden, deren Sicherungskopiengruppe keinen Zielort für das Inhaltsverzeichnis angibt, hängt das Ergebnis von dem TOC-Parameter für die Sicherungsoperation ab.

- Bei TOC=PREFERRED (Standardwert) wird die Sicherung ohne Erstellung eines Inhaltsverzeichnisses fortgesetzt.
- Bei TOC=YES schlägt die gesamte Sicherung fehl, da kein Inhaltsverzeichnis erstellt werden kann.

Beispiel: Eine Sicherungskopiengruppe erstellen

Eine Sicherungskopiengruppe STANDARD für Verwaltungsklasse ACTIVEFILES in Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE_RECORDS erstellen. Den Zielort der Sicherung auf BACKUPPOOL setzen. Für das Mindestintervall zwischen Sicherungen drei Tage angeben, unabhängig davon, ob die Dateien geändert wurden. Bis zu fünf Sicherungsversionen einer Datei aufbewahren, während die Datei im Client-Dateisystem vorhanden ist.

```
define copygroup employee_records
vacation activefiles standard type=backup
destination=backuppool frequency=3
verexists=5 mode=absolute
```

DEFINE COPYGROUP (Archivierungskopiengruppe definieren)

Mit diesem Befehl kann eine neue Archivierungskopiengruppe innerhalb einer bestimmten Verwaltungsklasse, Maßnahmengruppe und Maßnahmendomäne definiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Kopiengruppe gehört.

Syntax

```
>>-DEFine COpygroup--Domänenname--Name_der_Maßnahmengruppe--Klassenname-->

   .-STANDARD-.
>--+----------+--Type--=--Archive--DESTination--=--Poolname----->
   '-STANDARD-'

   .-FREQuency--=--Cmd-.  .-RETVer--=--365---------.
>--+-------------------+--+------------------------+------------>
   '-FREQuency--=--Cmd-'  '-RETVer--=--+-Tage----+-'
                                       '-NOLimit-'

   .-RETInit--=--CREATion--.  .-RETMin--=--365------.
>--+---------------------+--+--------------------+----------->
   '-RETInit--=--EVent---'  '-RETMin--=--Tage---'

   .-MODE--=--ABSolute-.
>--+-------------------+---------------------------------------->
   '-MODE--=--ABSolute-'

   .-SERialization--=--SHRSTatic------.
>--+----------------------------------+------------------------><
   '-SERialization--=--+-SHRSTatic--+-'
                       +-STatic-----+
                       +-SHRDYnamic-+
                       '-DYnamic----'
```

Parameter

Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an, für die die Kopiengruppe definiert wird.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt den Namen der Maßnahmengruppe an, für die die Kopiengruppe definiert wird.

  Für eine Verwaltungsklasse, die zu der aktiven Maßnahmengruppe (ACTIVE) gehört, kann keine Kopiengruppe definiert werden.

Klassenname (Erforderlich)
: Gibt den Namen der Verwaltungsklasse an, für die die Kopiengruppe definiert wird.

STANDARD
: Gibt den Namen der Kopiengruppe an, der STANDARD lauten muss. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD.

Type=Archive (Erforderlich)
: Gibt an, dass eine Archivierungskopiengruppe definiert werden soll.

DESTination (Erforderlich)
: Gibt den primären Speicherpool an, in dem der Server anfänglich die Archivierungskopie speichert. Ein Kopienspeicherpool kann nicht als Zielort angegeben werden.

FREQuency=Cmd
: Gibt die Kopienhäufigkeit an, die CMD lauten muss. Dieser Parameter ist wahlfrei. Der Standardwert ist CMD.

RETVer
: Gibt die Anzahl Tage an, die eine Archivierungskopie aufbewahrt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist 365.
  Gültige Werte:

  Tage
  : Gibt den Zeitraum an, den eine Archivierungskopie aufbewahrt werden soll. Sie können eine ganze Zahl im Bereich von 0 bis 30000 angeben.
    Die Serveroption RETENTIONEXTENSION kann sich auf die Datenträgeraufbewahrungsdauer auswirken, wenn die folgenden Bedingungen erfüllt sind:

    - Sie geben Null als Anzahl der Tage an
    - Der Zielspeicherpool für die Archivierungskopiengruppe ist ein SnapLock-Speicherpool (RECLAMATIONTYPE=SNAPLOCK)

    Wenn beide Bedingungen erfüllt sind, wird die Aufbewahrungsdauer der Datenträger durch den Wert der Serveroption RETENTIONEXTENSION definiert. Der Wert der Serveroption RETENTIONEXTENSION wird auch angewendet, wenn Daten durch einen Serverprozess, wie z. B. die Umlagerung, oder mithilfe des Befehls MOVE DATA oder MOVE NODEDATA in den Snaplock-Speicherpool kopiert oder versetzt werden.

  NOLimit
  : Gibt an, dass eine Archivierungskopie unbegrenzt aufbewahrt werden soll.

Wird NOLIMIT angegeben, werden Archivierungskopien von dem Server unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datei aus dem Server-Speicher. Wird NOLIMIT angegeben, können Sie nicht auch EVENT für den Parameter RETINIT angeben.

Der Wert des Parameters RETVER kann Auswirkungen auf die Verwaltungsklasse haben, mit der der Server ein archiviertes Verzeichnis verbindet. Wenn der Client die Option ARCHMC nicht verwendet, verbindet der Server Verzeichnisse, die archiviert werden, mit der Standardverwaltungsklasse. Verfügt die Standardverwaltungsklasse über keine Archivierungskopiengruppe, verbindet der Server Verzeichnisse, die archiviert werden, mit der Verwaltungsklasse mit dem kürzesten Aufbewahrungszeitraum.

Der Parameter RETVER der Archivierungskopiengruppe der Verwaltungsklasse, an die ein Objekt gebunden wird, bestimmt das Aufbewahrungskriterium für jedes Objekt. Eine Beschreibung des Datenschutzes befindet sich unter dem Befehl SET ARCHIVERETENTIONPROTECTION.

Wenn der im Parameter DESTINATION angegebene primäre Speicherpool zu einer Centera-Einheitenklasse gehört und der Datenschutz aktiviert ist, wird der Wert für RETVER zu Zwecken der Aufbewahrungsverwaltung an Centera gesendet. Eine Beschreibung des Datenschutzes befindet sich unter dem Befehl SET ARCHIVERETENTIONPROTECTION.

RETInit
Gibt an, wann der durch das RETVER-Attribut angegebene Aufbewahrungszeitraum beginnt. Dieser Parameter ist wahlfrei. Wenn Sie den Wert für RETINIT während der Erstellung der Kopiengruppe definieren, können Sie ihn später nicht ändern. Der Standardwert ist CREATION. Gültige Werte:

CREATion
Gibt an, dass der durch das RETVER-Attribut angegebene Aufbewahrungszeitraum zu dem Zeitpunkt beginnt, zu dem eine Archivierungskopie auf dem IBM Spectrum Protect-Server gespeichert wird.
EVent
Gibt an, dass der im Parameter RETVER angegebene Aufbewahrungszeitraum zu dem Zeitpunkt beginnt, zu dem eine Clientanwendung den Server über ein Ereignis bezüglich des Aufbewahrungsstarts für die Archivierungskopie informiert. Wird RETINIT=EVENT angegeben, können Sie nicht gleichzeitig RETVER=NOLIMIT angeben.

Tipp: Sie können "Löschen unzulässig" für ein Objekt angeben, das mit RETINIT=EVENT gespeichert wurde und für das noch kein Ereignis gesendet wurde. Wird das Ereignis gesendet, während die Angabe "Löschen unzulässig" wirksam ist, beginnt der Aufbewahrungszeitraum, aber das Objekt wird nicht gelöscht, während "Löschen unzulässig" wirksam ist.

RETMin
Gibt die Mindestanzahl von Tagen an, die eine Archivierungskopie aufbewahrt werden soll, nachdem sie archiviert wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist 365. Wird RETINIT=CREATION angegeben, wird dieser Parameter ignoriert.

MODE=ABSolute
Gibt an, dass eine Datei immer archiviert wird, wenn der Client dies anfordert. Der Parameter MODE muss den Wert ABSOLUTE haben. Dieser Parameter ist wahlfrei. Der Standardwert ist ABSOLUTE.

SERialization
Gibt an, wie IBM Spectrum Protect Dateien verarbeitet, die während der Archivierung geändert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist SHRSTATIC. Gültige Werte:

SHRSTatic
Gibt an, dass IBM Spectrum Protect eine Datei nur archiviert, wenn sie nicht geändert wird. IBM Spectrum Protect versucht bis zu viermal, eine Archivierungsoperation durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wird. Wenn die Datei während des Archivierungsversuchs geändert wird, archiviert IBM Spectrum Protect die Datei nicht.
STatic
Gibt an, dass IBM Spectrum Protect eine Datei nur archiviert, wenn sie nicht geändert wird. IBM Spectrum Protect versucht nur einmal, die Archivierungsoperation durchzuführen.

Plattformen, die die Option STATIC nicht unterstützen, nehmen den Standardwert SHRSTATIC an.

SHRDYnamic
Gibt an, dass IBM Spectrum Protect die Datei während des letzten Archivierungsversuchs archiviert, auch wenn die Datei während der Archivierung geändert wird. IBM Spectrum Protect versucht bis zu viermal, die Datei zu archivieren, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wird.
DYnamic
Gibt an, dass IBM Spectrum Protect eine Datei beim ersten Versuch archiviert, auch wenn sie während der Archivierungsverarbeitung geändert wird.
Achtung: Die Werte SHRDYNAMIC und DYNAMIC sind mit Vorsicht zu verwenden. IBM Spectrum Protect bestimmt anhand dieser Werte, ob eine Datei archiviert wird, während Änderungen vorgenommen werden. Aus diesem Grund ist die Archivierungskopie möglicherweise nur eine Sicherung mit grober Übereinstimmung. Eine Sicherung mit grober Übereinstimmung gibt den Inhalt der Datei nicht korrekt wieder, da sie einige, aber nicht alle Änderungen enthält. Wird eine Datei, die eine Sicherung mit grober Übereinstimmung enthält, abgerufen, ist die Datei möglicherweise nicht brauchbar. Dies ist von der Anwendung abhängig, die die Datei verwendet. Ist eine Sicherung mit grober Übereinstimmung nicht akzeptabel, definieren Sie für SERIALIZATION den Wert SHRSTATIC oder STATIC, damit IBM Spectrum Protect nur dann eine Archivierungskopie erstellt, wenn die Datei nicht geändert wird.

Beispiel: Eine Archivierungskopiengruppe für die ereignisgesteuerte Aufbewahrungsdauer definieren

Eine Archivierungskopiengruppe STANDARD für Verwaltungsklasse EVENTMC in Maßnahmengruppe SUMMER in der Maßnahmendomäne PROG1 erstellen. Den Archivierungszielort auf ARCHIVEPOOL setzen, an dem die Archivierungskopie aufbewahrt wird, bis der Server über ein Ereignis zum Starten des Aufbewahrungszeitraums benachrichtigt wird; danach wird die Archivierungskopie 30 Tage aufbewahrt. Die Archivierungskopie soll mindestens 90 Tage nach dem Speichern auf dem Server aufbewahrt werden, unabhängig davon, wann der Server über ein Ereignis zum Starten des Aufbewahrungszeitraums benachrichtigt wird.

```
define copygroup prog1 summer eventmc standard type=archive
destination=archivepool retinit=event retver=30 retmin=90
```

DEFINE DATAMOVER (Einheit zum Versetzen von Daten definieren)

Verwenden Sie diesen Befehl, um eine Einheit zum Versetzen von Daten zu definieren. Eine Einheit zum Versetzen von Daten ist eine benannte Einheit, die eine Anforderung von IBM Spectrum Protect zum Übertragen von Daten akzeptiert. Eine Einheit zum Versetzen von Daten kann zum Ausführen externer Kopieroperationen verwendet werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DATAMover--Name_der_Einheit_zum_Versetzen_von Daten--->

   .-Type--=--NAS--------------------.
>--+-----------------------------------+--HLAddress--=--Adresse--->
   |                           (1) (2) |
   '-Type--=--+-NASCLUSTER-+----------'
              '-NASVSERVER-'

   .-LLAddress--=--10000---------.
>--+-----------------------------+--USERid--=--Benutzer-ID------>
   '-LLAddress--=--TCP-Anschluss-'

                           .-ONLine--=--Yes-----.
>--PASsword--=--Kennwort--+--------------------+---------------->
                           '-ONLine--=--+-Yes-+-'
                                        '-No--'

>--DATAFormat--=--+-NETAPPDump--+-----------------------------><
                  +-CELERRADump-+
                  '-NDMPDump----'
```

Anmerkungen:

1. Sie können `TYPE=NASCLUSTER` und `TYPE=NASVSERVER` nur auf einem AIX-, Linux- oder Windows-Betriebssystem angeben.
2. Sie können `TYPE=NASCLUSTER` und `TYPE=NASVSERVER` nur bei `DATAFORMAT=NETAPPDUMP` angeben.

Parameter

Name_der_Einheit_zum_Versetzen_von_Daten (Erforderlich)
: Gibt den Namen der Einheit zum Versetzen von Daten an. Dieser Name muss mit einem Knotennamen übereinstimmen, den Sie zuvor mit dem Befehl `REGISTER NODE TYPE=NAS` registriert haben. Die Daten, die von dieser NAS-Einheit zum Versetzen von Daten gesichert werden, werden diesem Knotennamen in der Serverdatenbank zugeordnet. Es können maximal 64 Zeichen zur Angabe des Namens verwendet werden.

Type
: Gibt den Typ der Einheit zum Versetzen von Daten an. Dieser Parameter ist wahlfrei. Der Standardwert ist NAS.

  NAS
  : Gibt an, dass die Einheit zum Versetzen von Daten ein NAS-Dateiserver ist.

  NASCLUSTER
  : Gibt an, dass die Einheit zum Versetzen von Daten ein NAS-Dateiserver in einem Cluster ist.
    Einschränkung: Sie können den Wert NASCLUSTER nur bei `DATAFORMAT=NETAPPDUMP` angeben.

  NASVSERVER
  : Gibt an, dass die Einheit zum Versetzen von Daten eine virtuelle Speichereinheit innerhalb eines Clusters ist.
    Einschränkung: Sie können den Wert NASVSERVER nur bei `DATAFORMAT=NETAPPDUMP` angeben.

HLAddress (Erforderlich)
: Gibt entweder die numerische IP-Adresse oder den Domänennamen an, die bzw. der für den Zugriff auf den NAS-Dateiserver verwendet wird.
  Tipp: Um die numerische IP-Adresse zu bestimmen, greifen Sie auf den NAS-Dateiserver zu. Führen Sie dann die Anweisungen in der Dokumentation für den Dateiserver aus, um die Adresse abzurufen.

LLAddress
Gibt die TCP-Anschlussnummer für den Zugriff auf die NAS-Einheit für NDMP-Sitzungen (NDMP = Network Data Management Protocol) an. Dieser Parameter ist wahlfrei. Der Standardwert ist 10000.

USERid (Erforderlich)
Gibt die Benutzer-ID eines Benutzers an, der berechtigt ist, eine NDMP-Sitzung mit dem NAS-Dateiserver einzuleiten. Geben Sie beispielsweise die Benutzer-ID ein, die auf dem NetApp-Dateiserver für NDMP-Verbindungen konfiguriert ist.
Tipp: Um die Benutzer-ID zu bestimmen, greifen Sie auf den NAS-Dateiserver zu. Führen Sie dann die Anweisungen in der Dokumentation für den Dateiserver aus, um die Benutzer-ID abzurufen.

PASsword (Erforderlich)
Gibt das Kennwort der Benutzer-ID für die Anmeldung beim NAS-Dateiserver an.
Tipp: Um das Kennwort zu bestimmen, greifen Sie auf den NAS-Dateiserver zu. Führen Sie dann die Anweisungen in der Dokumentation für den Dateiserver aus, um das Kennwort abzurufen.

ONLine
Gibt an, ob die Einheit zum Versetzen von Daten für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Yes
Der Standardwert. Gibt an, dass die Einheit zum Versetzen von Daten für die Verwendung verfügbar ist.

No
Gibt an, dass die Einheit zum Versetzen von Daten nicht für die Verwendung verfügbar ist. Wird die Hardware gewartet, können Sie mit dem Befehl UPDATE DATAMOVER die Einheit zum Versetzen von Daten in den Offline-Status setzen.

Wird ein Speicherarchiv durch die Verwendung eines Pfads von einer NAS-Einheit zum Versetzen von Daten zu dem Speicherarchiv gesteuert, und ist die NAS-Einheit zum Versetzen von Daten offline, kann der Server nicht auf das Speicherarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während die NAS-Einheit zum Versetzen von Daten offline ist, wird das Speicherarchiv nicht initialisiert.

DATAFormat (Erforderlich)
Gibt das Datenformat an, das von dieser Einheit zum Versetzen von Daten verwendet wird.

NETAPPDump
Muss für NetApp-NAS-Dateiserver und IBM® System Storage N Series verwendet werden.

CELERRADump
Muss für EMC Celerra NAS-Dateiserver verwendet werden.

NDMPDump
Muss für NAS-Dateiserver verwendet werden, die keine NetApp- oder EMC-Dateiserver sind.

Beispiel: Eine Einheit zum Versetzen von Daten nach Domänenname definieren

Eine Einheit zum Versetzen von Daten für den Knoten NAS1 definieren. Der Domänenname für die Einheit zum Versetzen von Daten lautet NETAPP2.EXAMPLE.COM, die Anschlussnummer ist 10000.

```
define datamover nas1 type=nas hladdress=netapp2.example.com lladdress=10000
    userid=root password=admin dataformat=netappdump
```

Beispiel: Eine Einheit zum Versetzen von Daten nach IP-Adresse definieren

Eine Einheit zum Versetzen von Daten für den Knoten NAS2 definieren. Die numerische IP-Adresse der Einheit zum Versetzen von Daten ist 203.0.113.0, die Anschlussnummer lautet 10000. Der NAS-Dateiserver ist kein NetApp- oder EMC-Dateiserver.

```
define datamover nas2 type=nas hladdress=203.0.113.0 lladdress=10000
    userid=root password=admin dataformat=ndmpdump
```

Beispiel: Eine Einheit zum Versetzen von Daten für einen Clusterdateiserver nach IP-Adresse definieren

Eine Einheit zum Versetzen von Daten für den Clusterdateiserver NAS3 definieren. Der NAS-Dateiserver ist eine NetApp-Einheit. Die numerische IP-Adresse der Einheit zum Versetzen von Daten ist 198.51.100.0, die Anschlussnummer lautet 10000.

```
define datamover nas3 type=nascluster hladdress=198.51.100.0
    lladdress=10000 userid=root password=admin dataformat=netappdump
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE DATAMOVER

Befehl	Beschreibung
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE DATAMOVER	Löscht eine Einheit zum Versetzen von Daten.
QUERY DATAMOVER	Zeigt Definitionen der Einheit zum Versetzen von Daten an.

Befehl	Beschreibung
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
UPDATE DATAMOVER	Ändert die Definition einer Einheit zum Versetzen von Daten.

DEFINE DEVCLASS (Einheitenklasse definieren)

Verwenden Sie diesen Befehl, um eine Einheitenklasse für einen Speichereinheitentyp zu definieren. Für den Server muss eine Einheitenklasse definiert werden, damit eine Einheit verwendet werden kann.

Die neueste Liste der unterstützten Einheiten und gültigen Einheitenklassenformate befindet sich auf der Website für die unterstützten IBM Spectrum Protect-Einheiten: AIX-BetriebssystemeWindows-Betriebssysteme

- Supported devices for AIX and Windows

Linux-Betriebssysteme

- Supported devices for Linux

Anmerkung: Die Einheitenklasse DISK wird von IBM Spectrum Protect definiert und kann mit dem Befehl DEFINE DEVCLASS nicht geändert werden.

AIX-BetriebssystemeLinux-BetriebssystemeWenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server definieren).

Die folgenden IBM Spectrum Protect-Einheitenklassen sind nach Einheitentyp sortiert.

- DEFINE DEVCLASS (Einheitenklasse 3590 definieren)
- DEFINE DEVCLASS (Einheitenklasse 3592 definieren)
- DEFINE DEVCLASS (Einheitenklasse 4MM definieren)
- DEFINE DEVCLASS (Einheitenklasse 8MM definieren)
- DEFINE DEVCLASS (Einheitenklasse CENTERA definieren)
- DEFINE DEVCLASS (Einheitenklasse DLT definieren)
- DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE definieren)
- DEFINE DEVCLASS (Einheitenklasse FILE definieren)
- AIX-BetriebssystemeWindows-BetriebssystemeDEFINE DEVCLASS (Einheitenklasse GENERICTAPE definieren)
- DEFINE DEVCLASS (Einheitenklasse LTO definieren)
- DEFINE DEVCLASS (Einheitenklasse NAS definieren)
- DEFINE DEVCLASS (Einheitenklasse REMOVABLEFILE definieren)
- DEFINE DEVCLASS (Einheitenklasse SERVER definieren)
- DEFINE DEVCLASS (Einheitenklasse VOLSAFE definieren)

Tabelle 1. Zugehörige Befehle für DEFINE DEVCLASS

Befehl	Beschreibung
BACKUP DEVCONFIG	Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DELETE DEVCLASS	Löscht eine Einheitenklasse.
QUERY DEVCLASS	Zeigt Informationen zu Einheitenklassen an.
QUERY DIRSPACE	Zeigt Informationen zu Verzeichnissen FILE an.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.

DEFINE DEVCLASS (Einheitenklasse 3590 definieren)

Verwenden Sie die Einheitenklasse 3590, wenn Sie 3590-Bandeinheiten verwenden.

AIX-BetriebssystemeLinux-BetriebssystemeWenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server definieren).

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>

>--LIBRary--=--Kassettenarchivname--DEVType--=--3590------------>

   .-FORMAT--=--DRIVE-------.
>--+------------------------+--+----------------------+--------->
   '-FORMAT--=--+-DRIVE---+-'  '-ESTCAPacity--=--Größe-'
                +-3590B---+
                +-3590C---+
                +-3590E-B-+
                +-3590E-C-+
                +-3590H-B-+
                '-3590H-C-'

   .-PREFIX--=--ADSM--------------------.
>--+-----------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+---------------------------+--+----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)

: Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

: Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=3590 (Erforderlich)
: Gibt an, dass der Einheitentyp 3590 der Einheitenklasse zugeordnet wird. 3590 gibt an, dass dieser Einheitenklasse Magnetbandkassetteneinheiten IBM® 3590 zugeordnet werden.

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

: Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

: In den folgenden Tabellen sind die Aufzeichnungsformate, die geschätzten Kapazitäten und die Optionen der Aufzeichnungsformate für 3590-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 3590

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
3590B	10,0 GB	Dekomprimiertes (Basis-)Format
3590C	Siehe Anmerkung 20,0 GB	Komprimiertes Format
3590E-B	10,0 GB	Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format

Format	Geschätzte Kapazität	Beschreibung
3590E-C	Siehe Anmerkung 20,0 GB	Komprimiertes Format, ähnlich dem 3590C-Format
3590H-B	30,0 GB (J-Kassette – Standardlänge) 60,0 GB (K-Kassette - erweiterte Länge)	Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format
3590H-C	Siehe Anmerkung 60,0 GB (J-Kassette - Standardlänge) 120,0 GB (K-Kassette - erweiterte Länge)	Komprimiertes Format, ähnlich dem 3590C-Format
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein.		

Tabelle 2. Auswahl des Aufzeichnungsformats für 3590-Einheiten

Einheit	Format					
	3590B	3590C	3590E-B	3590E-C	3590H-B	3590H-C
3590	Lesen/ Schreiben	Lesen/ Schreiben	–	–	–	–
Ultra SCSI	Lesen/ Schreiben	Lesen/ Schreiben	–	–	–	–
3590E	Lesen	Lesen	Lesen/ Schreiben	Lesen/ Schreiben	–	–
3590H	Lesen	Lesen	Lesen	Lesen	Lesen/ Schreiben	Lesen/ Schreiben

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DEFINE DEVCLASS (Einheitenklasse 3592 definieren)

Verwenden Sie die Einheitenklasse 3592, wenn Sie 3592-Bandeinheiten verwenden.

AIX-Betriebssysteme Linux-BetriebssystemeWenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server definieren).

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>

>--LIBRary--=--Kassettenarchivname--DEVType--=--3592------------>

                                                 (1)
   .-LBProtect--=--No------------.  .-WORM--=--No------.
>--+-----------------------------+--+------------------+-------->
   '-LBProtect--=--+-READWrite-+-'  '-WORM--=--+-Yes-+-'
                   +-WRITEOnly-+               '-No--'
                   '-No--------'

   .-SCALECAPacity--=--100-----.  .-FORMAT--=--DRIVE-------.
>--+---------------------------+--+-----------------------+---->
   '-SCALECAPacity--=--+-100-+-'  '-FORMAT--=--+-DRIVE---+-'
                       +-90--+                 +-3592----+
                       '-20--'                 +-3592C---+
                                               +-3592-2--+
                                               +-3592-2C-+
                                               +-3592-3--+
```

```
                                                +-3592-3C-+
                                                +-3592-4--+
                                                '-3592-4C-'

>--+-----------------------+-------------------------------------->
   '-ESTCAPacity--=--Größe-'

   .-PREFIX--=--ADSM---------------------.
>--+-------------------------------------+---------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+---------------------------+--+----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+-------------------------------->
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'

                              (1) (2)
   .-DRIVEEncryption--=--ALLOW---------.
>--+---------------------------------+----------------------><
   '-DRIVEEncryption--=--+-ON-------+--'
                         +-ALLOW----+
                         +-EXTERNAL-+
                         '-OFF------'
```

Anmerkungen:

1. Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
2. Laufwerkverschlüsselung wird nur für 3592-Laufwerke der Generation 2 oder höher unterstützt.

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=3592 (Erforderlich)
Gibt an, dass der Einheitentyp 3592 der Einheitenklasse zugeordnet wird.

LBProtect

Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffschutzinformationen, wenn Daten von dem Band gelesen werden.

Der Standardwert ist NO.

Die folgenden Werte sind gültig:

READWrite
Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

WRITEOnly
Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für

Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

No
: Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur für IBM® 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher unterstützt.

In Technote 1634851, Additional information on the IBM Spectrum Protect LBProtect option, wird erläutert, wann der Parameter LBProtect zu verwenden ist.

WORM
: Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Das Feld kann einen der folgenden Werte enthalten:

Yes
: Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

No
: Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

Hinweis:

1. Um die 3592-WORM-Unterstützung in 3584-Kassettenarchiven zu verwenden, müssen Sie den WORM-Parameter angeben. Der Server unterscheidet zwischen WORM- und Nicht-WORM-Arbeitsdatenträgern. Soll jedoch die 3592-WORM-Unterstützung in 349X-Kassettenarchiven verwendet werden, müssen Sie auch WORMSCRATCHCATEGORY im Befehl DEFINE LIBRARY definieren. Ausführliche Informationen siehe DEFINE LIBRARY (Kassettenarchiv definieren).
2. Bei WORM=Yes ist der einzige gültige Wert für den Parameter SCALECAPACITY der Wert 100.
3. Stellen Sie zusammen mit Ihren Hardwarelieferanten sicher, dass sich Ihre Hardware auf der entsprechenden Unterstützungsstufe befindet.

SCALECAPacity
: Gibt den Prozentsatz der Datenträgerkapazität an, der zum Speichern von Daten verwendet werden kann. Dieser Parameter ist wahlfrei. Der Standardwert ist 100. Gültige Werte sind 20, 90 oder 100.

Wird für SCALECAPacity der Wert 100 angegeben, wird die maximale Speicherkapazität zur Verfügung gestellt. Wird der Wert 20 angegeben, wird die schnellste Zugriffszeit zur Verfügung gestellt.

Anmerkung: Der Wert für SCALECAPacity wird nur wirksam, wenn Daten zum ersten Mal auf einen Datenträger geschrieben werden. Alle Aktualisierungen an der Einheitenklasse für SCALECAPacity haben erst dann Auswirkungen auf Datenträger, auf die bereits Daten geschrieben wurden, wenn die Datenträger wieder in den Arbeitsdatenträgerstatus versetzt werden.

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

In der folgenden Tabelle sind die Aufzeichnungsformate, die geschätzten Kapazitäten und die Optionen der Aufzeichnungsformate für 3592-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 3592

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
3592	300 GB	Dekomprimiertes (Basis-)Format
3592C	Siehe Anmerkung 900 GB	Komprimiertes Format
3592-2	500 GB 700 GB	JA-Bänder mit dekomprimiertem (Basis-)Format JB-Bänder mit dekomprimiertem (Basis-)Format

Format	Geschätzte Kapazität	Beschreibung
3592-2C	1,5 TB	JA-Bänder mit komprimiertem Format
	2,1 TB	JB-Bänder mit komprimiertem Format
3592–3	640 GB	JA-Bänder mit dekomprimiertem (Basis-)Format
	1 TB	JB-Bänder mit dekomprimiertem (Basis-)Format
3592–3C	1,9 TB	JA-Bänder mit komprimiertem Format
	3 TB	JB-Bänder mit komprimiertem Format
3592-4	400 GB	JK-Bänder mit dekomprimiertem (Basis-)Format
	1,5 TB	JB-Bänder mit dekomprimiertem (Basis-)Format
	3,1 TB	JC-Band mit dekomprimiertem (Basis-)Format
3592-4C	1,2 TB	JK-Bänder mit komprimiertem Format
	4,4 TB	JB-Bänder mit komprimiertem Format
	9,4 TB	JC-Bänder mit komprimiertem Format
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann je nach Effektivität der Komprimierung die tatsächliche Kapazität von dem aufgelisteten Wert abweichen.		

Wichtig: Um eine optimale Leistung zu erzielen, sollte das Mischen von Laufwerken verschiedener Generationen in einem einzelnen SCSI-Kassettenarchiv vermieden werden. Müssen Sie Laufwerkgenerationen in einem SCSI-Kassettenarchiv mischen, verwenden Sie eine der speziellen Konfigurationen, die in dem Abschnitt zum Mischen von Generationen von 3592-Datenträgern beschrieben sind.

Spezielle Konfigurationen sind auch erforderlich, wenn verschiedene Generationen von 3592-Laufwerken in 349x- und ACSLS-Kassettenarchiven gemischt werden.

ESTCAPacity
Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

PREFIX
Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DRIVEEncryption

Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei. Der Standardwert ist ALLOW.

ON

Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern, wie beispielsweise Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger, werden nicht verschlüsselt.) Wird ON angegeben und entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

ALLOW

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch erlaubt, wenn entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert ist.

EXTERNAL

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist.
Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert.
Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

OFF

Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

DEFINE DEVCLASS (Einheitenklasse 4MM definieren)

Verwenden Sie die Einheitenklasse 4MM, wenn Sie 4-mm-Bandeinheiten verwenden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>

>--LIBRary--=--Kassettenarchivname--DEVType--=--4MM------------>

   .-FORMAT--=--DRIVE-----.
>--+----------------------+--+----------------------+---------->
   '-FORMAT--=--+-DRIVE-+-'  '-ESTCAPacity--=--Größe-'
                +-DDS1--+
                +-DDS1C-+
                +-DDS2--+
                +-DDS2C-+
                +-DDS3--+
                +-DDS3C-+
                +-DDS4--+
                +-DDS4C-+
                +-DDS5--+
                +-DDS5C-+
                +-DDS6--+
                '-DDS6C-'

   .-PREFIX--=--ADSM--------------------.
>--+-----------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

   .-MOUNTWait--=--60------.  .-MOUNTRetention--=--60------.
>--+--------------------+--+--------------------------+---->
   '-MOUNTWait--=--Minuten-'  '-MOUNTRetention--=--Minuten-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten 4-mm-Bandlaufwerke enthält. Informationen über die Definition eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=4MM (Erforderlich)
: Gibt an, dass der Einheitentyp 4MM der Einheitenklasse zugeordnet wird. 4MM bedeutet, dass dieser Einheitenklasse 4-mm-Bandeinheiten zugeordnet werden.

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

  Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

  In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für 4-mm-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 4-mm-Bänder

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
DDS1	2,6 GB (60 Meter) 4,0 GB (90 Meter)	Dekomprimiertes Format, gilt nur für 60-Meter-Bänder und 90-Meter-Bänder

Format	Geschätzte Kapazität	Beschreibung
DDS1C	Siehe Anmerkung 1,3 GB (60 Meter) 2,0 GB (90 Meter)	Komprimiertes Format, gilt nur für 60-Meter-Bänder und 90-Meter-Bänder
DDS2	4,0 GB	Dekomprimiertes Format, gilt nur für 120-Meter-Bänder
DDS2C	Siehe Anmerkung 8,0 GB	Komprimiertes Format, gilt nur für 120-Meter-Bänder
DDS3	12,0 GB	Dekomprimiertes Format, gilt nur für 125-Meter-Bänder
DDS3C	Siehe Anmerkung 24,0 GB	Komprimiertes Format, gilt nur für 125-Meter-Bänder
DDS4	20,0 GB	Dekomprimiertes Format, gilt nur für 150-Meter-Bänder
DDS4C	Siehe Anmerkung 40,0 GB	Komprimiertes Format, gilt nur für 150-Meter-Bänder
DDS5	36 GB	Dekomprimiertes Format bei Verwendung von DAT 72-Datenträgern
DDS5C	Siehe Anmerkung 72 GB	Komprimiertes Format bei Verwendung von DAT 72-Datenträgern
DDS6	80 GB	Dekomprimiertes Format bei Verwendung von DAT 160-Datenträgern
DDS6C	Siehe Anmerkung 160 GB	Komprimiertes Format bei Verwendung von DAT 160-Datenträgern
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein.		

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zur geschätzten Standardkapazität für 4-mm-Bänder siehe Tabelle 1.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DEFINE DEVCLASS (Einheitenklasse 8MM definieren)

Verwenden Sie die Einheitenklasse 8MM, wenn Sie 8-mm-Bandeinheiten verwenden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>

>--LIBRary--=--Kassettenarchivname--DEVType--=--8MM------------->

   .-WORM--=--No------.  .-FORMAT--=--DRIVE-----.
>--+------------------+--+---------------------+--------------->
   '-WORM--=--+-No--+-'  '-FORMAT--=--+-DRIVE-+-'
              '-Yes-'                 +-8200--+
                                      +-8200C-+
                                      +-8500--+
                                      +-8500C-+
                                      +-8900--+
                                      +-AIT---+
                                      +-AITC--+
                                      +-M2----+
                                      +-M2C---+
                                      +-SAIT--+
                                      +-SAITC-+
```

```
                                    +-VXA2--+
                                    +-VXA2C-+
                                    +-VXA3--+
                                    '-VXA3C-'

>--+----------------------+-------------------------------------->
   '-ESTCAPacity--=--Größe-'

   .-PREFIX--=--ADSM--------------------.
>--+----------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+--------------------------+--+----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

   .-MOUNTLimit--=--DRIVES-----.
>--+-------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten 8-mm-Bandlaufwerke enthält. Informationen über die Definition eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=8MM (Erforderlich)
: Gibt an, dass der Einheitentyp 8MM der Einheitenklasse zugeordnet wird. 8MM bedeutet, dass dieser Einheitenklasse 8-mm-Bandeinheiten zugeordnet werden.

WORM
: Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Das Feld kann einen der folgenden Werte enthalten:

  Yes
  : Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

  No
  : Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

  Anmerkung: Wird Yes ausgewählt, sind nur die folgenden Optionen für den Parameter FORMAT verfügbar:

  - DRIVE
  - AIT
  - AITC

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

  Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

  In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für 8-mm-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformat und geschätzte Standardkapazität für 8-mm-Band

Format **Datenträgertyp**	**Geschätzte Kapazität**	**Beschreibung**
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
8200	2,3 GB	Dekomprimiertes (Standard) Format, verwendet 112-Meter-Standardbandkassetten

Format Datenträgertyp	Geschätzte Kapazität	Beschreibung
8200C	Siehe Anmerkung 3,5 GB 4,6 GB	Komprimiertes Format, verwendet 112-Meter-Standardbandkassetten
8500	Siehe Anmerkung	Laufwerke (Lesen/Schreiben)
15 m	600 MB	Eliant 820 (LS)
15 m	600 MB	Exabyte 8500/8500C (LS)
15 m	600 MB	Exabyte 8505 (LS)
54 m	2,35 GB	Eliant 820 (LS)
54 m	2,35 GB	Exabyte 8500/8500C (LS)
54 m	2,35 GB	Exabyte 8505 (LS)
112 m	5 GB oder 10,0 GB	Eliant 820 (LS)
112 m	5 GB oder 10,0 GB	Exabyte 8500/8500C (LS)
112 m	5 GB oder 10,0 GB	Exabyte 8505 (LS)
160 m XL	7 GB	Eliant 820 (LS)
8500C	Siehe Anmerkung	Laufwerke (Lesen/Schreiben)
15 m	1,2 GB	Eliant 820 (LS)
15 m	1,2 GB	Exabyte 8500/8500C (LS)
15 m	1,2 GB	Exabyte 8505 (LS)
54 m	4,7 GB	Eliant 820 (LS)
54 m	4,7 GB	Exabyte 8500/8500C (LS)
54 m	4,7 GB	Exabyte 8505 (LS)
112 m	5 GB oder 10,0 GB	Eliant 820 (LS)
112 m	5 GB oder 10,0 GB	Exabyte 8500/8500C (LS)
112 m	5 GB oder 10,0 GB	Exabyte 8505 (LS)
160 m XL	7 GB	Eliant 820 (LS)
8900	Siehe Anmerkung	Laufwerk (Lesen/Schreiben)
15 m	–	Mammoth 8900 (L)
54 m	–	Mammoth 8900 (L)
112 m	–	Mammoth 8900 (L)
160 m XL	–	Mammoth 8900 (L)
22 m	2,5 GB	Mammoth 8900 (LS)
125 m	–	Mammoth 8900 (LS mit Upgrade)
170 m	40 GB	Mammoth 8900 (LS)
AIT	Siehe Anmerkung	Laufwerk
SDX1–25C	25 GB	AIT-, AIT2- und AIT3-Laufwerke
SDX1–35C	35 GB	AIT-, AIT2- und AIT3-Laufwerke
SDX2–36C	36 GB	AIT2- und AIT3-Laufwerke
SDX2–50C	50 GB	AIT2- und AIT3-Laufwerke
SDX3–100C	100 GB	AIT3-, AIT4- und AIT5-Laufwerke
SDX3X-150C	150 GB	AIT3-Ex-, AIT4- und AIT5-Laufwerke
SDX4–200C	200 GB	AIT4- und AIT5-Laufwerke
SDX5-400C	400 GB	AIT5-Laufwerk
AITC	Siehe Anmerkung	Laufwerk
SDX1–25C	50 GB	AIT-, AIT2- und AIT3-Laufwerke
SDX1–35C	91 GB	AIT-, AIT2- und AIT3-Laufwerke
SDX2–36C	72 GB	AIT2- und AIT3-Laufwerke
SDX2–50C	130 GB	AIT2- und AIT3-Laufwerke
SDX3–100C	260 GB	AIT3-, AIT4- und AIT5-Laufwerke
SDX3X-150C	390 GB	AIT3-Ex-, AIT4- und AIT5-Laufwerke
SDX4–200C	520 GB	AIT4- und AIT5-Laufwerke
SDX5-400C	1040 GB	AIT5-Laufwerk
M2	Siehe Anmerkung	Laufwerk (Lesen/Schreiben)
75 m	20,0 GB	Mammoth II (LS)
150 m	40,0 GB	Mammoth II (LS)
225 m	60,0 GB	Mammoth II (LS)

Format Datenträgertyp	 Geschätzte Kapazität	Beschreibung
M2C	Siehe Anmerkung	Laufwerk (Lesen/Schreiben)
75 m 150 m 225 m	50,0 GB 100,0 GB 150,0 GB	Mammoth II (LS) Mammoth II (LS) Mammoth II (LS)
SAIT	Siehe Anmerkung 500 GB	Laufwerk (Lesen/Schreiben) Sony SAIT1–500 (LS)
SAITC	Siehe Anmerkung 1300 GB (1,3 TB)	Laufwerk (Lesen/Schreiben) Sony SAIT1–500 (LS)
VXA2 V6 (62 m) V10 (124 m) V17 (170 m)	Siehe Anmerkung 20 GB 40 GB 60 GB	Laufwerk (Lesen/Schreiben) VXA–2
VXA2C V6 (62 m) V10 (124 m) V17 (170 m)	Siehe Anmerkung 40 GB 80 GB 120 GB	Laufwerk (Lesen/Schreiben) VXA–2
VXA3 X6 (62 m) X10 (124 m) X23 (230 m)	Siehe Anmerkung 40 GB 86 GB 160 GB	Laufwerk (Lesen/Schreiben) VXA–3
VXA3C X6 (62 m) X10 (124 m) X23 (230 m)	Siehe Anmerkung 80 GB 172 GB 320 GB	Laufwerk (Lesen/Schreiben) VXA–3
Anmerkung: Die tatsächlichen Kapazitäten können abhängig von den verwendeten Kassetten und Laufwerken variieren. • Für das M2C-Format ist das normale Komprimierungsverhältnis 2,5:1. • Für das AITC- und SAITC-Format ist das normale Komprimierungsverhältnis 2,6:1.		

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zur geschätzten Standardkapazität für 8-mm-Bänder siehe Tabelle 1.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

```
AB.CD2.E
```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

  Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

  Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

Beispiel: Eine 8-mm-Einheitenklasse definieren

Die Einheitenklasse 8MMTAPE für eine 8-mm-Einheit in dem Kassettenarchiv AUTO definieren. Das Format ist DRIVE, Grenzwert für Ladeanforderungen 2, Ladedauer ist 10, Banddatenträgerpräfix lautet ADSMVOL und die geschätzte Kapazität beträgt 6 GB.

```
define devclass 8mmtape devtype=8mm library=auto
format=drive mountlimit=2 mountretention=10
prefix=adsmvol estcapacity=6G
```

DEFINE DEVCLASS (Einheitenklasse CENTERA definieren)

Verwenden Sie die Einheitenklasse CENTERA, wenn Sie EMC Centera-Speichereinheiten verwenden. Der Einheitentyp CENTERA verwendet Dateien als Datenträger zum sequenziellen Speichern von Daten. Er ähnelt der Einheitenklasse FILE.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType--=--CENTERA--->

                     .-,----------.
              (1)    V            |
>--HLAddress------=----ID-Adresse-+-?PEA-Datei------------------>

   .-MINCAPacity--=--100M--.  .-MOUNTLimit--=--1------.
>--+-----------------------+--+----------------------+--------><
   '-MINCAPacity--=--Größe-'  '-MOUNTLimit--=--Anzahl-'
```

Anmerkungen:

1. Für jede Centera-Einheitenklasse müssen Sie mindestens eine IP-Adresse angeben. Ein PEA-Dateiname und -Pfad (PEA = Pool Entry Authorization) sind jedoch optional, und maximal eine PEA-Dateispezifikation kann auf die IP-Adressen folgen. Verwenden Sie das Zeichen "?", um den PEA-Dateinamen und -Pfad von den IP-Adressen zu trennen.

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

DEVType=CENTERA (Erforderlich)
Gibt an, dass der Einheitentyp Centera dieser Einheitenklasse zugeordnet wird. Alle Datenträger, die zu einem Speicherpool gehören, der für diese Einheitenklasse definiert ist, sind logische Datenträger, die eine Art von Datenträger mit sequenziellem Zugriff sind.

HLAddress
Gibt mindestens eine IP-Adresse für die Centera-Speichereinheit und optional den Namen und Pfad einer PEA-Datei (PEA = Pool Entry Authorization) an. Geben Sie die IP-Adressen in Schreibweise mit Trennzeichen an (beispielsweise 9.10.111.222). Eine Centera-Einheit kann mehrere IP-Adressen haben. Werden mehrere IP-Adressen angegeben, wird bei der Speicher- oder Abrufoperation versucht, eine Verbindung mit jeder angegebenen IP-Adresse herzustellen, bis eine gültige Adresse gefunden wird.

AIX-BetriebssystemeBei dem PEA-Dateinamen und -Pfadnamen muss die Groß-/Kleinschreibung beachtet werden.

Werden Name und Pfad einer PEA-Datei angehängt, stellen Sie sicher, dass die Datei in einem Verzeichnis auf dem System gespeichert wird, auf dem der Server ausgeführt wird. Verwenden Sie das Zeichen "?", um den PEA-Dateinamen und -Pfad von der IP-Adresse zu trennen. Beispiel: Windows-Betriebssysteme

```
HLADDRESS=9.10.111.222,9.10.111.223?c:\controlFiles\TSM.PEA
```

AIX-Betriebssysteme

```
HLADDRESS=9.10.111.222,9.10.111.223?/user/ControlFiles/TSM.PEA
```

Geben Sie nur einen PEA-Dateinamen und Pfad für jede Einheitenklassendefinition an. Geben Sie zwei verschiedene Centera-Einheitenklassen an, die auf dieselbe Centera-Speichereinheit zeigen, und enthalten die Einheitenklassendefinitionen verschiedene PEA-Dateinamen und -Pfade, verwendet der Server die PEA-Datei, die im Einheitenklassenparameter HLADDRESS angegeben ist, der zuerst zum Öffnen der Centera-Speichereinheit verwendet wurde.
Tipps:

1. Der Server schließt während der Installation keine PEA-Datei ein. Wenn Sie keine PEA-Datei erstellen, verwendet der Server das Centera-Standardprofil, mit dem es Anwendungen erlaubt werden kann, Daten auf einer Centera-Speichereinheit zu lesen, zu schreiben, zu löschen und abzufragen. Um eine genauere Steuerung zu ermöglichen, erstellen Sie eine PEA-Datei mit der Befehlszeilenschnittstelle, die von EMC Centera zur Verfügung gestellt wird. Ausführliche Informationen zur Centera-Authentifizierung und -Berechtigung befinden sich im EMC Centera *Programmer's Guide*.
2. Sie können den PEA-Dateinamen und -Pfad auch in einer Umgebungsvariablen mit der Syntax CENTERA_PEA_LOCATION=Dateipfad_ Dateiname angeben. Der mit dieser Umgebungsvariablen angegebene PEA-Dateiname und -Pfad gilt für alle Centera-Cluster. Wird diese Variable verwendet, müssen Sie keinen PEA-Dateinamen und -Pfad mit dem Parameter HLADDRESS angeben.

MINCAPacity
Gibt die Mindestgröße für Centera-Datenträger an, die einem Speicherpool in dieser Einheitenklasse zugeordnet sind. Dieser Wert stellt das Mindestdatenvolumen dar, das auf einem Centera-Datenträger gespeichert wird, bevor der Server den Datenträger als voll kennzeichnet. Centera-Datenträger akzeptieren weiterhin Daten, bis das Mindestdatenvolumen gespeichert wurde. Dieser Parameter ist wahlfrei.

Dieser Wert muss als ganze Zahl gefolgt von einem `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte) angegeben werden. Der Standardwert ist 100 MB (MINCAPACITY=100M). Der zulässige Mindestwert ist 1 MB (MINCAPACITY=1M). Der zulässige Maximalwert ist 128 GB (MINCAPACITY=128G).

MOUNTLimit

Gibt die maximale Anzahl von Dateien an, die gleichzeitig für die Ein- und Ausgabe geöffnet sein kann. Der Standardwert ist 1. Dieser Parameter ist optional. Sie können eine beliebige Zahl von 0 aufwärts angeben; die Summe aller Grenzwerte für Ladeanforderungen für alle Einheitenklassen, die derselben Centera-Einheit zugeordnet sind, darf jedoch die maximale Anzahl der von Centera erlaubten Sitzungen nicht überschreiten.

DEFINE DEVCLASS (Einheitenklasse DLT definieren)

Verwenden Sie die Einheitenklasse DLT, wenn Sie DLT-Bandeinheiten verwenden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>

>--LIBRary--=--Kassettenarchivname--DEVType--=--DLT------------->

   .-WORM--=--No------.  .-FORMAT--=--DRIVE--------.
>--+------------------+--+-------------------------+------------>
   '-WORM--=--+-No--+-'  '-FORMAT--=--+-DRIVE----+-'
              '-Yes-'                 +-DLT1-----+
                                      +-DLT1C----+
                                      +-DLT10----+
                                      +-DLT10C---+
                                      +-DLT15----+
                                      +-DLT15C---+
                                      +-DLT20----+
                                      +-DLT20C---+
                                      +-DLT35----+
                                      +-DLT35C---+
                                      +-DLT40----+
                                      +-DLT40C---+
                                      +-DLT2-----+
                                      +-DLT2C----+
                                      +-DLT4-----+
                                      +-DLT4C----+
                                      +-SDLT-----+
                                      +-SDLTC----+
                                      +-SDLT320--+
                                      +-SDLT320C-+
                                      +-SDLT600--+
                                      +-SDLT600C-+
                                      +-DLTS4----+
                                      '-DLTS4C---'

>--+-----------------------+----------------------------------->
   '-ESTCAPacity--=--Größe-'

   .-PREFIX--=--ADSM---------------------.
>--+-----------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+---------------------------+--+----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten DLT-Bandlaufwerke enthält. Informationen über die Definition eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=DLT (Erforderlich)

Gibt an, dass der Einheitentyp DLT der Einheitenklasse zugeordnet wird. DLT bedeutet, dass dieser Einheitenklasse DLT-Bandeinheiten zugeordnet werden.

WORM

Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Das Feld kann einen der folgenden Werte enthalten:

Yes
: Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

No
: Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

Anmerkung: Unterstützung für DLT WORM-Datenträger ist nur für SDLT-600-, Quantum DLT-V4- und Quantum DLT-S4-Laufwerke in manuellen Kassettenarchiven, SCSI- und ACSLS-Kassettenarchiven verfügbar.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für DLT-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformat und geschätzte Standardkapazität für DLT

Format	**Geschätzte Kapazität**	**Beschreibung**
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
DLT1	40,0 GB	Dekomprimiertes Format, verwendet nur CompacTape III-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT1C	Siehe 1. 80,0 GB	Komprimiertes Format, verwendet nur CompacTape III-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT10	10,0 GB	Dekomprimiertes Format, verwendet nur CompacTape III-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT10C	Siehe 1. 20,0 GB	Komprimiertes Format, verwendet nur CompacTape III-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT15	15,0 GB	Dekomprimiertes Format, verwendet nur CompacTape IIIxt-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT15C	Siehe 1. 30,0 GB	Komprimiertes Format, verwendet nur CompacTape IIIxt-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT20	20,0 GB	Dekomprimiertes Format, verwendet nur CompacTape IV-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT20C	Siehe 1. 40,0 GB	Komprimiertes Format, verwendet nur CompacTape IV-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT35	35,0 GB	Dekomprimiertes Format, verwendet nur CompacTape IV-Kassetten Gültig für DLT7000- und DLT8000-Laufwerke
DLT35C	Siehe 1. 70,0 GB	Komprimiertes Format, verwendet nur CompacTape IV-Kassetten Gültig für DLT7000- und DLT8000-Laufwerke
DLT40	40,0 GB	Dekomprimiertes Format, verwendet CompacTape IV-Kassetten Gültig für DLT8000-Laufwerk
DLT40C	Siehe 1. 80,0 GB	Komprimiertes Format, verwendet CompacTape IV-Kassetten Gültig für DLT8000-Laufwerk

Format	Geschätzte Kapazität	Beschreibung
DLT2	80,0 GB	Dekomprimiertes Format, verwendet Quantum DLT VS1-Banddatenträger
DLT2C	Siehe 1. 160,0 GB	Komprimiertes Format, verwendet Quantum DLT VS1-Banddatenträger
DLT4	160,0 GB	Dekomprimiertes Format, verwendet Quantum DLTtape VS1-Kassetten. Gültig für Quantum DLT-V4-Laufwerk
DLT4C	Siehe 1. 320,0 GB	Komprimiertes Format, verwendet Quantum DLTtape VS1-Kassetten. Gültig für Quantum DLT-V4-Laufwerk
SDLT Siehe 2.	100,0 GB	Dekomprimiertes Format, verwendet Super DLT Tape 1-Kassetten Gültig für Super DLT-Laufwerk
SDLTC Siehe 2.	Siehe 1. 200,0 GB	Komprimiertes Format, verwendet Super DLT Tape 1-Kassetten Gültig für Super DLT-Laufwerk
SDLT320 Siehe 2.	160,0 GB	Dekomprimiertes Format, verwendet Quantum SDLT I-Datenträger Gültig für Super DLT-Laufwerk
SDLT320C Siehe 2.	Siehe 1. 320,0 GB	Komprimiertes Format, verwendet Quantum SDLT I-Datenträger Gültig für Super DLT-Laufwerk
SDLT600	300,0 GB	Dekomprimiertes Format, verwendet SuperDLTtape-II-Datenträger Gültig für Super DLT-Laufwerk
SDLT600C	Siehe 1. 600,0 GB	Komprimiertes Format, verwendet SuperDLTtape-II-Datenträger Gültig für Super DLT-Laufwerk
DLTS4	800 GB	Dekomprimiertes Format, verwendet Quantum DLT S4-Datenträger. Gültig für ein DLT-S4-Laufwerk
DLTS4C	Siehe 1. 1,6 TB	Komprimiertes Format, verwendet Quantum DLT S4-Datenträger. Gültig für ein DLT-S4-Laufwerk

Anmerkung:

1. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität größer als der aufgeführte Wert sein.
2. IBM Spectrum Protect unterstützt kein Kassettenarchiv, das sowohl Backward Read Compatible (BRC) SDLT- als auch Non-Backward Read Compatible (NBRC) SDLT-Laufwerke enthält.

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zu geschätzten Kapazitäten siehe Tabelle 1.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

```
AB.CD2.E
```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

  Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

  Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE definieren)

Verwenden Sie die Einheitenklasse ECARTRIDGE, wenn Sie StorageTek-Laufwerke wie beispielsweise StorageTek T9840 oder T10000 verwenden.



Wenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server definieren).

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>
```

```
>--LIBRary--=--Kassettenarchivname--DEVType--=--ECARTridge------>

                                                    (1)
   .-LBProtect--=--No------------.  .-WORM--=--No------.
>--+-----------------------------+--+------------------+-------->
   '-LBProtect--=--+-READWrite-+-'  '-WORM--=--+-No--+-'
                   +-WRITEOnly-+               '-Yes-'
                   '-No--------'

   .-FORMAT--=--DRIVE---------.
>--+--------------------------+--+----------------------+------>
   '-FORMAT--=--+-DRIVE-----+-'  '-ESTCAPacity--=--Größe-'
                +-T9840C----+
                +-T9840C-C--+
                +-T9840D----+
                +-T9840D-C--+
                +-T10000A---+
                +-T10000A-C-+
                +-T10000B---+
                +-T10000B-C-+
                +-T10000C---+
                +-T10000C-C-+
                +-T10000D---+
                '-T10000D-C-'

   .-PREFIX--=--ADSM--------------------.
>--+-----------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+-------------------------+--+-----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+------------------------------->
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'

                              (1) (2)
   .-DRIVEEncryption--=--ALLOW---------.
>--+---------------------------------+----------------------><
   '-DRIVEEncryption--=--+-ON-------+--'
                         +-ALLOW----+
                         +-EXTernal-+
                         '-OFF------'
```

Anmerkungen:

1. Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
2. Sie können die Laufwerkverschlüsselung nur für Oracle StorageTek T10000B-Laufwerke mit dem Formatwert DRIVE, T10000B oder T10000B-C, für Oracle StorageTek T10000C-Laufwerke mit dem Formatwert DRIVE, T10000C oder T10000C-C und für Oracle StorageTek T10000D-Laufwerke mit dem Formatwert DRIVE, T10000D und T10000D-C verwenden.

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die Kassettenbandlaufwerke (ECARTRIDGE) enthält, die von dieser Einheitenklasse verwendet werden können. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=ECARTridge (Erforderlich)
: Gibt an, dass der Einheitentyp ECARTRIDGE der Einheitenklasse zugeordnet wird. ECARTRIDGE gibt an, dass ein bestimmter Typ von Magnetbandkassette (StorageTek) dieser Einheitenklasse zugeordnet ist.

LBProtect

: Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffschutzinformationen, wenn Daten von dem Band gelesen werden.

  Der Standardwert ist NO.

  Die folgenden Werte sind gültig:

READWrite
Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

WRITEOnly
Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

No
Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur auf Oracle StorageTek T10000C- und Oracle StorageTek T10000D-Laufwerken unterstützt.

WORM
Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Das Feld kann einen der folgenden Werte enthalten:

Yes
Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

No
Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

Einschränkung: Wird Yes ausgewählt, sind nur die folgenden Optionen für den Parameter FORMAT verfügbar:

- DRIVE
- T9840C
- T9840C-C
- T9840D
- T9840D-C
- T10000A
- T10000A-C
- T10000B
- T10000B-C
- T10000C
- T10000C-C
- T10000D
- T10000D-C

FORMAT
Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

Wichtig: Wird DRIVE für eine Einheitenklasse angegeben, die über inkompatible Einheiten mit sequenziellem Zugriff verfügt, müssen Datenträger in Einheiten geladen werden, die in dem Format lesen oder schreiben können, das beim ersten Laden des Datenträgers eingerichtet wurde. Dies kann zu Verzögerungen führen, wenn die einzige Einheit mit sequenziellem Zugriff, die auf den Datenträger zugreifen kann, bereits im Gebrauch ist.
In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für ECARTRIDGE-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für ECARTRIDGE-Bänder

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.

Format	Geschätzte Kapazität	Beschreibung
T9840C	40 GB	Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840C-C	80 GB	Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840D	75 GB	Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T9840D-C	150 GB	Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T10000A	500 GB	Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000A-C	1 TB	Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000B	1 TB	Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000B-C	2 TB	Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000C	5 TB	Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000C-C	10 TB	Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D	8 TB	Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D-C	15 TB	Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
Anmerkungen: • Einige Formate verwenden die Datenkomprimierung über Hardware mittels Bandlaufwerk. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität doppelt so groß (oder größer) sein wie der aufgeführte Wert. • T10000A-Laufwerke können nur das T10000A-Format lesen und schreiben. T10000B-Laufwerke können das T10000A-Format lesen, aber nicht schreiben. T10000C-Laufwerke können die T10000A- und T10000B-Formate lesen, aber nicht schreiben. T10000D-Laufwerke können die T10000A-, T10000B- und T10000C-Formate lesen, aber nicht schreiben.		

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES
Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl
Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)
Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DRIVEEncryption
Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei. Der Standardwert ist ALLOW.
Einschränkungen:

1. Sie können die Laufwerkverschlüsselung nur für die folgenden Laufwerke verwenden:
   - Oracle StorageTek T10000B-Laufwerke, die den Formatwert DRIVE, T10000B oder T10000B-C haben
   - Oracle StorageTek T10000C-Laufwerke, die den Formatwert DRIVE, T10000C oder T10000C-C haben
   - Oracle StorageTek T10000D-Laufwerke, die den Formatwert DRIVE, T10000D oder T10000D-C haben
2. Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
3. Ist die Verschlüsselung für eine Einheitenklasse aktiviert und ist die Einheitenklasse einem Speicherpool zugeordnet, sollte der Speicherpool nicht einen Arbeitsdatenträgerpool mit anderen Einheitenklassen gemeinsam nutzen, die nicht verschlüsselt werden können. Ist ein Band verschlüsselt und soll das Band in einem Laufwerk verwendet werden, das nicht verschlüsselt werden kann, müssen Sie das Band manuell mit einem neuen Kennsatz versehen, bevor es in diesem Laufwerk verwendet werden kann.

ON
Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern werden nicht verschlüsselt. Beispielsweise werden Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger nicht verschlüsselt.) Wird ON angegeben und ein anderes Verschlüsselungsverfahren aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

ALLOW
Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

EXTernal
Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist. Geben Sie EXTERNAL an, und stellt

IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert. Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

OFF

Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird ein anderes Verschlüsselungsverfahren aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

DEFINE DEVCLASS (Einheitenklasse FILE definieren)

Verwenden Sie die Einheitenklasse FILE, wenn Dateien im Magnetplattenspeicher als Datenträger verwendet werden, die Daten sequenziell speichern (wie auf Band).

AIX-BetriebssystemeLinux-BetriebssystemeDie Einheitenklasse FILE unterstützt keine Kassettenarchive EXTERNAL.

Windows-BetriebssystemeDie Einheitenklasse FILE unterstützt keine EXTERNAL- oder Remote Storage Manager-Kassettenarchive.

AIX-BetriebssystemeLinux-BetriebssystemeWenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in DEFINE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server definieren).

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType--=--FILE------>

   .-MOUNTLimit--=--20-----.  .-MAXCAPacity--=--10G---.
>--+----------------------+--+---------------------+--------->
   '-MOUNTLimit--=--Anzahl-'  '-MAXCAPacity--=--Größe-'

   .-DIRectory--=--Name_des_aktuellen_Verzeichnisses-.
>--+-------------------------------------------------+---------->
   |               .-,---------------.               |
   |               V                 |               |
   '-DIRectory--=----Verzeichnisname-+---------------'

   .-SHAREd--=--No------.
>--+--------------------+-------------------------------------><
   '-SHAREd--=--+-No--+-'
                '-Yes-'
```

Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

DEVType=FILE (Erforderlich)

Gibt an, dass der Einheitentyp FILE der Einheitenklasse zugeordnet wird. FILE bedeutet, dass dieser Einheitenklasse eine Datei zugeordnet ist. Wenn der Server auf einen Datenträger zugreifen muss, der zu dieser Einheitenklasse gehört, öffnet er eine Datei und liest oder schreibt Dateidaten.

Eine Datei ist eine Form eines Datenträgers mit sequenziellem Zugriff.

MOUNTLimit

Gibt die maximale Anzahl von Dateien an, die gleichzeitig für die Ein- und Ausgabe geöffnet sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist 20. Sie können eine Zahl von 0 bis 4096 angeben.

Windows-BetriebssystemeWird die Einheitenklasse mit einem Speicheragenten gemeinsam genutzt (durch Angabe des Parameters SHARED=YES), werden Laufwerke definiert oder gelöscht, um eine Übereinstimmung mit dem Grenzwert für Ladeanforderung zu erreichen.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

MAXCAPacity

Gibt die maximale Größe einer Datenspeicherdatei an, die für einen Speicherpool in dieser Einheitenklasse definiert ist.

Der Wert des Parameters MAXCAPACITY wird auch als Zuordnungseinheit verwendet, wenn Speicherbereichsauslöser für den Speicherpool Datenträger erstellen. Der Standardwert ist 10 GB (MAXCAPACITY=10G). Der angegebene Wert muss kleiner-gleich der

maximal unterstützten Größe einer Datei im Zieldateisystem sein.

Dieser Wert muss als ganze Zahl gefolgt von einem `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte) angegeben werden. Die Mindestgröße ist 1 MB (MAXCAPACITY=1M). Wenn Sie eine Einheitenklasse FILE für Datenbanksicherungsdatenträger definieren, geben Sie einen Wert für MAXCAPACITY an, der für die Größe der Datenbank angemessen ist und der die Anzahl der Datenbankdatenträger minimiert.

AIX-Betriebssysteme  Linux-BetriebssystemeDefinieren Sie keinen Wert für MAXCAPACITY, der größer als 640 MB ist, wenn diese Datei für die REMOVABLEFILE CD-Unterstützung bestimmt ist. Ein Wert, der kleiner als der verwendbare Speicherbereich (650 MB) einer CD ist, ermöglicht eine Eins-zu-Eins-Übereinstimmung zwischen Dateien aus der Einheitenklasse FILE und Kopien, die sich auf CD befinden.

DIRectory
Gibt die Verzeichnisposition(en) der in dieser Einheitenklasse verwendeten Dateien an. Schließen Sie die gesamte Liste der Verzeichnisse in Anführungszeichen ein und verwenden Sie Kommas, um einzelne Verzeichnisnamen voneinander zu trennen. Sonderzeichen (z. B. Leerzeichen) sind in Verzeichnisnamen zulässig. Die Verzeichnisliste "abc def,xyz" enthält beispielsweise zwei Verzeichnisse: abc def und xyz.

Dieser Parameter ist wahlfrei.

AIX-Betriebssysteme  Linux-BetriebssystemeDer Standardwert ist das aktuelle Arbeitsverzeichnis des Servers zum Zeitpunkt der Befehlsausgabe.

 Windows-BetriebssystemeDer Standardwert ist das aktuelle Arbeitsverzeichnis des Servers zum Zeitpunkt der Befehlsausgabe. Windows-Registry-Informationen werden verwendet, um das Standardverzeichnis zu bestimmen.

Durch die Angabe eines oder mehrerer Verzeichnisnamen wird die Position angegeben, an der der Server die Dateien speichert, die Speicherdatenträger für diese Einheitenklasse darstellen.

Für die NetApp-SnapLock-Unterstützung (Speicherpools mit RECLAMATIONTYPE=SNAPLOCK, die diese Einheitenklasse verwenden) müssen die mit dem Parameter DIRECTORY angegebenen Verzeichnisse auf die Verzeichnisse auf den NetApp-SnapLock-Datenträgern zeigen.

AIX-Betriebssysteme  Linux-BetriebssystemeBei der Verarbeitung des Befehls erweitert der Server den oder die angegebenen Verzeichnisnamen in die vollständig qualifizierte Form (beginnend beim Stammverzeichnis).

Wenn der Server einen Arbeitsdatenträger zuordnen muss, erstellt er eine neue Datei in einem dieser Verzeichnisse. (Der Server kann ein beliebiges der Verzeichnisse auswählen, in dem neue Arbeitsdatenträger erstellt werden sollen.) Bei Arbeitsdatenträgern, die zum Speichern von Clientdaten verwendet werden, hat die durch den Server erstellte Datei die Dateinamenerweiterung .bfs. Bei Arbeitsdatenträgern, auf denen Exportdaten gespeichert werden, wird die Dateinamenerweiterung .exp verwendet.

AIX-Betriebssysteme  Linux-BetriebssystemeWenn Sie beispielsweise eine Einheitenklasse mit dem Verzeichnis tsmstor definieren und der Server einen Arbeitsdatenträger in dieser Einheitenklasse benötigt, um Exportdaten zu speichern, könnte der Name der Datei, die der Server erstellt, /tsmstor/00566497.exp lauten.

 Windows-BetriebssystemeWenn Sie beispielsweise eine Einheitenklasse mit dem Verzeichnis c:\server definieren und der Server einen Arbeitsdatenträger in dieser Einheitenklasse benötigt, um Exportdaten zu speichern, könnte der Name der Datei, die der Server erstellt, c:\server\00566497.exp lauten.

Wichtig: Sie müssen sicherstellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können. Kann der Speicheragent nicht auf einen FILE-Datenträger zugreifen, werden Operationen möglicherweise nur auf einem LAN-Pfad wiederholt, oder die Operationen können fehlschlagen. Weitere Informationen enthält die Beschreibung des Parameters DIRECTORY in DEFINE PATH (Pfad definieren).
Tipp: Geben Sie mehrere Verzeichnisse für eine Einheitenklasse an, stellen Sie sicher, dass die Verzeichnisse separaten Dateisystemen zugeordnet sind. Bei Speicherbereichsauslöserfunktionen und Berechnungen des Speicherbereichs im Speicherpool wird der Speicherbereich berücksichtigt, der in jedem Verzeichnis verbleibt. Wenn Sie mehrere Verzeichnisse für eine Einheitenklasse angeben und sich die Verzeichnisse in demselben Dateisystem befinden, berechnet der Server den Speicherbereich durch Hinzufügen von Werten, die den Speicherbereich darstellen, der in jedem Verzeichnis verbleibt. Diese Speicherbereichsberechnungen sind ungenau. Anstatt einen Speicherpool mit ausreichend Speicherbereich für eine Operation auszuwählen, kann der Server den falschen Speicherpool auswählen und frühzeitig über keinen Speicherbereich mehr verfügen. Bei Speicherbereichsauslösern kann eine ungenaue Berechnung zu einem Fehler bei der Erweiterung des Speicherbereichs führen, der in einem Speicherpool verfügbar ist. Ein Fehler bei der Erweiterung des Speicherbereichs in einem Speicherpool ist eine der Bedingungen, die zur Inaktivierung eines Auslösers führen kann. Wird ein Auslöser inaktiviert, da der Speicherbereich in einem Speicherpool nicht erweitert werden konnte, können Sie den Auslöser erneut aktivieren, indem Sie den folgenden Befehl ausgeben: `update spacetrigger stg`. Es sind keine weiteren Änderungen an dem Speicherbereichsauslöser erforderlich.

SHAREd
Gibt an, dass diese Einheitenklasse FILE von dem Server und von einem oder mehreren Speicheragenten gemeinsam genutzt wird. Zur Vorbereitung der gemeinsamen Nutzung wird automatisch ein Kassettenarchiv zusammen mit einer Anzahl von Laufwerken definiert, die dem Wert des Parameters MOUNTLIMIT entspricht. Die Laufwerknamen bestehen aus dem Namen des Kassettenarchivs plus einer Zahl von 1 bis zum Grenzwert für Ladeanforderung (Mount-Limit). Lautet der Kassettenarchivname beispielsweise FILE und ist der Grenzwert für Ladeanforderung auf 4 gesetzt, haben die Laufwerke die Namen FILE11, FILE12, FILE13, FILE14.

Informationen zu Voraussetzungen, wenn Speicher vom Server und Speicheragenten gemeinsam genutzt wird, befinden sich unter IBM® Support Portal for IBM Spectrum Protect.

Beispiel: Eine Einheitenklasse FILE mit mehreren Verzeichnissen definieren

Eine Einheitenklasse definieren, die mehrere Verzeichnisse angibt.

 AIX-Betriebssysteme

```
define devclass multidir devtype=file
      directory=/usr/xyz,/usr/abc,/usr/uvw
```

 Linux-Betriebssysteme

```
define devclass multidir devtype=file
      directory=/opt/xyz,/opt/abc,/opt/uvw
```

 Windows-Betriebssysteme

```
define devclass multidir devtype=file
      directory=e:\xyz,f:\abc,g:\uvw
```

Beispiel: Eine Einheitenklasse FILE mit einer Kapazität von 50 MB definieren

Die Einheitenklasse PLAINFILES mit dem Einheitentyp FILE und einer maximalen Kapazität von 50 MB definieren.

```
define devclass plainfiles devtype=file
maxcapacity=50m
```

 AIX-Betriebssysteme  Windows-Betriebssysteme

DEFINE DEVCLASS (Einheitenklasse GENERICTAPE definieren)

Verwenden Sie die Einheitenklasse GENERICTAPE für Bandlaufwerke, die von Einheitentreibern des Betriebssystems unterstützt werden.

Bei Verwendung dieses Einheitentyps erkennt der Server weder den Einheitentyp noch das Kassettenaufzeichnungsformat. Wenn ein E/A-Fehler auftritt, sind die Fehlerinformationen weniger ausführlich im Vergleich zu den Fehlerinformationen für einen bestimmten Einheitentyp (z. B. 8MM), da der Server den Einheitentyp nicht erkennt. Bei der Definition von Einheiten für den Server dürfen keine verschiedenen Einheitentypen in demselben Einheitentyp gemischt werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>

>--LIBRary--=--Kassettenarchivname--DEVType--=--GENERICtape----->

                              .-MOUNTRetention--=--60------.
>--+-----------------------+--+---------------------------+---->
   '-ESTCAPacity--=--Größe-'  '-MOUNTRetention--=--Minuten-'

   .-MOUNTWait--=--60------.  .-MOUNTLimit--=--DRIVES-----.
>--+---------------------+--+-------------------------+---><
   '-MOUNTWait--=--Minuten-'  '-MOUNTLimit--=--+-DRIVES-+-'
                                               +-Anzahl-+
                                               '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=GENERICtape (Erforderlich)

Gibt an, dass der Einheitentyp GENERICTAPE der Einheitenklasse zugeordnet wird. GENERICTAPE bedeutet, dass die Datenträger für diese Einheitenklasse in Bandlaufwerken verwendet werden, die vom Bandeinheitentreiber des Betriebssystems unterstützt werden.

Der Server erkennt, dass die Datenträger entfernt und weitere Datenträger eingelegt werden können, innerhalb der mit dem Parameter MOUNTLIMIT für die Einheitenklasse und dem Parameter MAXSCRATCH für den Speicherpool gesetzten Grenzwerte.

Datenträger in einer Einheitenklasse mit dem Einheitentyp GENERICTAPE sind Datenträger mit sequenziellem Zugriff.

ESTCAPacity
Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Geben Sie eine dem verwendeten Bandlaufwerk entsprechende Kapazität an.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

MOUNTRetention
Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES
Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl
Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)
Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DEFINE DEVCLASS (Einheitenklasse LTO definieren)

Verwenden Sie die Einheitenklasse LTO, wenn Sie LTO-Bandeinheiten verwenden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

Anmerkungen:

1. Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
2. Laufwerkverschlüsselung wird nur für Ultrium 4-, Ultrium 5- und Ultrium 6-Laufwerke und -Datenträger unterstützt.

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten LTO-Bandlaufwerke enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=LTO (Erforderlich)
: Gibt an, dass der Einheitentyp LTO (Linear Tape Open) der Einheitenklasse zugeordnet wird.

LBProtect

: Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz

logischer Blöcke und generiert CRC-Zugriffschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffschutzinformationen, wenn Daten von dem Band gelesen werden.

Der Standardwert ist NO.

Die folgenden Werte sind gültig:

READWrite
: Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

  Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

WRITEOnly
: Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

No
: Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur auf IBM® LTO5-Laufwerken und unterstützten LTO6-Laufwerken unterstützt.

WORM
: Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Das Feld kann einen der folgenden Werte enthalten:

  Yes
  : Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

  No
  : Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

  Anmerkung:

  1. Sollen WORM-Datenträger in einem Kassettenarchiv verwendet werden, müssen alle Laufwerke in dem Kassettenarchiv WORM-fähig sein.
  2. Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). (Die Angabe von WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON wird nicht unterstützt.)

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

  Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

  Gehen Sie wie folgt vor, wenn alle Laufwerke von Ultrium-Einheiten auf Ultrium 2-Einheiten migriert werden:

  - Löschen Sie alle vorhandenen Ultrium-Laufwerkdefinitionen und die Pfade, die ihnen zugeordnet sind.
  - Definieren Sie die neuen Ultrium 2-Laufwerke und Pfade.

  Sollen verschiedene Generationen von LTO-Datenträgern und -laufwerken gemischt werden, sind die folgenden Einschränkungen zu beachten.

Tabelle 1. Lese-/Schreibfunktionalität verschiedener Generationen von LTO-Laufwerken

Laufwerke	Datenträger der Generation 1	Datenträger der Generation 2	Datenträger der Generation 3	Datenträger der Generation 4	Datenträger der Generation 5	Datenträger der Generation 6
Generation 1	Lesen und schreiben	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 2	Lesen und schreiben	Lesen und schreiben	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 3 [1]	Nur lesen	Lesen und schreiben	Lesen und schreiben	nicht zutreffend	nicht zutreffend	nicht zutreffend

Laufwerke	Datenträger der Generation 1	Datenträger der Generation 2	Datenträger der Generation 3	Datenträger der Generation 4	Datenträger der Generation 5	Datenträger der Generation 6
Generation 4 [2]	nicht zutreffend	Nur lesen	Lesen und schreiben	Lesen und schreiben	nicht zutreffend	nicht zutreffend
Generation 5 [3]	nicht zutreffend	nicht zutreffend	Nur lesen	Lesen und schreiben	Lesen und schreiben	nicht zutreffend
Generation 6 [4]	nicht zutreffend	nicht zutreffend	nicht zutreffend	Nur lesen	Lesen und schreiben	Lesen und schreiben

[1] In einem Kassettenarchiv mit einem Laufwerk der Generation 3 müssen alle Arbeitsdatenträger der Generation 1 entnommen werden und alle Speicherpooldatenträger der Generation 1 müssen in "schreibgeschützt" aktualisiert werden.

[2] In einem Kassettenarchiv mit einem Laufwerk der Generation 4 müssen alle Arbeitsdatenträger der Generation 2 entnommen werden und alle Speicherpooldatenträger der Generation 2 müssen in "schreibgeschützt" aktualisiert werden.

[3] In einem Kassettenarchiv mit einem Laufwerk der Generation 5 müssen alle Arbeitsdatenträger der Generation 3 entnommen werden und alle Speicherpooldatenträger der Generation 3 müssen in "schreibgeschützt" aktualisiert werden.

[4] In einem Kassettenarchiv mit einem Laufwerk der Generation 6 müssen alle Arbeitsdatenträger der Generation 4 entnommen werden und alle Speicherpooldatenträger der Generation 4 müssen in "schreibgeschützt" aktualisiert werden.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für LTO-Einheiten aufgelistet:

Tabelle 2. Aufzeichnungsformat und geschätzte Standardkapazität für LTO

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
ULTRIUM	100 GB	Dekomprimiertes Format, verwendet Ultrium-Kassetten
ULTRIUMC	Siehe Anmerkung 200 GB	Komprimiertes Format, verwendet Ultrium-Kassetten
ULTRIUM2	200 GB	Dekomprimiertes (Standard) Format, verwendet Ultrium 2-Kassetten
ULTRIUM2C	Siehe Anmerkung 400 GB	Komprimiertes Format, verwendet Ultrium 2-Kassetten
ULTRIUM3	400 GB	Dekomprimiertes (Standard) Format, verwendet Ultrium 3-Kassetten
ULTRIUM3C	Siehe Anmerkung 800 GB	Komprimiertes Format, verwendet Ultrium 3-Kassetten
ULTRIUM4	800 GB	Dekomprimiertes (Standard) Format, verwendet Ultrium 4-Kassetten
ULTRIUM4C	Siehe Anmerkung 1,6 TB	Komprimiertes Format, verwendet Ultrium 4-Kassetten
ULTRIUM5	1,5 TB	Dekomprimiertes (Standard-)Format, verwendet Ultrium 5-Kassetten
ULTRIUM5C	Siehe Anmerkung 3,0 TB	Komprimiertes Format, verwendet Ultrium 5-Kassetten
ULTRIUM6	2,5 TB	Dekomprimiertes (Standard) Format, verwendet Ultrium 6-Kassetten
ULTRIUM6C	Siehe Anmerkung 6,25 TB	Komprimiertes Format, verwendet Ultrium 6-Kassetten
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein.		

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zu geschätzten Kapazitäten siehe Tabelle 2.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES
: Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl
: Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)
: Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DRIVEEncryption
Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei. Der Standardwert ist ALLOW.Laufwerkverschlüsselung wird nur für Ultrium 4-, Ultrium 5- und Ultrium 6-Laufwerke und -Datenträger unterstützt.
Einschränkung: Ist die Verschlüsselung für eine Einheitenklasse aktiviert und ist die Einheitenklasse einem Speicherpool zugeordnet, sollte der Speicherpool nicht einen Arbeitsdatenträgerpool mit anderen Einheitenklassen gemeinsam nutzen, die nicht verschlüsselt werden können. Ist ein Band verschlüsselt und soll das Band in einem Laufwerk verwendet werden, das nicht verschlüsselt werden kann, müssen Sie das Band manuell mit einem neuen Kennsatz versehen, bevor es in diesem Laufwerk verwendet werden kann.

ON
Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern werden nicht verschlüsselt. Beispielsweise werden Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger nicht verschlüsselt.) Wird ON angegeben und ein anderes Verschlüsselungsverfahren aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.
Anmerkung: Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). (Die Angabe von WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON wird nicht unterstützt.)

ALLOW
Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

EXTERNAL
Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist. Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert. Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

OFF
Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird ein anderes Verschlüsselungsverfahren aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

Beispiel: Eine Einheitenklasse LTO definieren

Die Einheitenklasse LTOTAPE für ein LTO-Laufwerk in dem Kassettenarchiv LTOLIB definieren. Das Format ist ULTRIUM, der Grenzwert für Ladeanforderung ist 12, die Ladedauer ist 5, das Banddatenträgerpräfix lautet SMVOL und die geschätzte Kapazität beträgt 100 GB.

```
define devclass ltotape devtype=lto library=ltolib
format=ultrium mountlimit=12 mountretention=5
prefix=smvol estcapacity=100G
```

DEFINE DEVCLASS (Einheitenklasse NAS definieren)

Verwenden Sie die Einheitenklasse NAS (Network Attached Storage), wenn Sie NDMP-Operationen zum Sichern von NAS-Dateiservern verwenden (NDMP - Network Data Management Protocol). Die Einheitenklasse ist für Laufwerke bestimmt, die der NAS-Dateiserver für Sicherungen unterstützt.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType--=--NAS------->

>--LIBRary--=--Kassettenarchivname--MOUNTRetention--=--0-------->

   .-MOUNTWait--=--60------.  .-MOUNTLimit--=--DRIVES-----.
>--+----------------------+--+--------------------------+----->
   '-MOUNTWait--=--Minuten-'  '-MOUNTLimit--=--+-DRIVES-+-'
                                               +-Anzahl-+
                                               '-0------'

>--ESTCAPacity--=--Größe----------------------------------------->

   .-PREFIX--=--ADSM---------------------.
```

```
>--+--------------------------------------+--------------------><
   '-PREFIX--=--+-ADSM------------------+-'
                '-Banddatenträgerpräfix-'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

DEVType=NAS (Erforderlich)
: Gibt an, dass der Einheitentyp NAS (Network-Attached Storage) der Einheitenklasse zugeordnet wird. Der NAS-Einheitentyp ist für Laufwerke bestimmt, die mit einem NAS-Dateiserver verbunden sind und von einem NAS-Dateiserver zum Sichern von NAS-Dateisystemen verwendet werden.

LIBRary (Erforderlich)
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten SCSI-Bandlaufwerke enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

MOUNTRetention=0 (Erforderlich)
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Null (0) ist der einzige unterstützte Wert für Einheitenklassen mit DEVType=NAS.

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

ESTCAPacity (Erforderlich)
: Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind.

  Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

  Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

PREFIX
: Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

  Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

  Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

  - Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

    ```
    AB.CD2.E
    ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

Beispiel: Eine Einheitenklasse NAS definieren

Die Einheitenklasse NASTAPE für ein NAS-Laufwerk in dem Kassettenarchiv NASLIB definieren. Der Grenzwert für Ladeanforderung ist DRIVES, die Ladedauer ist 0, das Banddatenträgerpräfix lautet SMVOL und die geschätzte Kapazität beträgt 200 GB.

```
define devclass nastape devtype=nas library=naslib
mountretention=0 mountlimit=drives
prefix=smvol estcapacity=200G
```

DEFINE DEVCLASS (Einheitenklasse REMOVABLEFILE definieren)

Verwenden Sie die Einheitenklasse REMOVABLEFILE für Einheiten für austauschbare Datenträger, die als lokale, entfernbare Dateisysteme angeschlossen sind.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>

>--LIBRary--=--Kassettenarchivname--DEVType--=--REMOVABLEfile--->

   .-MAXCAPacity--=--verbleibender_Speicherbereich-.
>--+-------------------------------------------------+------------>
   '-MAXCAPacity--=--Größe-------------------------'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+----------------------------+--+----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

   .-MOUNTLimit--=--DRIVES-----.
>--+---------------------------+-------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten Laufwerke für austauschbare Datenträger enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=REMOVABLEfile (Erforderlich)
: Gibt an, dass der Einheitentyp REMOVABLEFILE der Einheitenklasse zugeordnet wird. REMOVABLEFILE bedeutet, dass die Datenträger für diese Einheitenklasse Dateien auf lokalen, austauschbaren Datenträgern sind.

  Datenträger in einer Einheitenklasse mit dem Einheitentyp REMOVABLEFILE sind Datenträger mit sequenziellem Zugriff.

  Verwenden Sie die Dienstprogramme des Einheitenherstellers, um die Datenträger zu formatieren (falls erforderlich) und zu kennzeichnen. Der Kennsatz auf den Datenträgern muss folgende Bedingungen erfüllen:

  - Der Kennsatz darf maximal 11 Zeichen haben.
  - Der Datenträgerkennsatz und der Name der Datei auf dem Datenträger müssen exakt übereinstimmen.
  - AIX-BetriebssystemeWindows-BetriebssystemeDer Parameter MAXCAPACITY muss auf einen Wert gesetzt werden, der niedriger als die Kapazität des Datenträgers ist.

MAXCAPacity
: Gibt die maximale Größe der Datenträger an, die für einen Speicherpool definiert sind, der durch diese Einheitenklasse kategorisiert wird. Dieser Parameter ist wahlfrei.

  Der Parameter MAXCAPACITY muss auf einen Wert gesetzt werden, der niedriger als die Kapazität des Datenträgers ist. Bei CD-Datenträgern kann die maximale Kapazität nicht größer als 650 MB sein.

AIX-BetriebssystemeWindows-BetriebssystemeDa der Server nur eine Datei pro physischen austauschbaren Datenträger öffnet, ist die Kapazität so zu wählen, dass diese eine Datei die Datenträgerkapazität vollständig nutzt.

Verbleibender_Speicherbereich
: Der Standardwert für die maximale Kapazität ist der auf dem Datenträger verbleibende Speicherbereich nach seiner ersten Verwendung.

Größe
: Dieser Wert muss als ganze Zahl gefolgt von einem `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte) angegeben werden.

MAXCAPACITY=5M gibt beispielsweise an, dass die maximale Kapazität eines Datenträgers in dieser Einheitenklasse 5 MB beträgt. Der zulässige Mindestwert ist 1 MB (d. h. MAXCAPACITY=1M).

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES
: Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl
: Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)
: Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DEFINE DEVCLASS (Einheitenklasse SERVER definieren)

Verwenden Sie die Einheitenklasse SERVER, um Speicherdatenträger oder Dateien zu verwenden, die auf einem anderen IBM Spectrum Protect-Server archiviert sind.

Wird der Aufbewahrungsschutz für Daten mit dem Befehl SET ARCHIVERETENTIONPROTECTION aktiviert, können Sie keine Servereinheitenklasse definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType--=--SERVER---->

                              .-MAXCAPacity--=--500M--.
>--SERVERName--=--Servername--+-----------------------+--------->
                              '-MAXCAPacity--=--Größe-'

   .-MOUNTLimit--=--1------.  .-MOUNTRetention--=--60------.
>--+---------------------+--+---------------------------+---->
   '-MOUNTLimit--=--Anzahl-'  '-MOUNTRetention--=--Minuten-'

   .-PREFIX--=--ADSM-----------------.
>--+-----------------------------------+-------------------------->
   '-PREFIX--=--+-ADSM--------------+-'
                '-Datenträgerpräfix-'

   .-RETRYPeriod--=--10-----------------------------.
>--+-------------------------------------------------+---------->
   '-RETRYPeriod--=--Wiederholungszeitraum (Minuten)-'

   .-RETRYInterval--=--30-------------------------------.
>--+-------------------------------------------------+----->
   '-RETRYInterval--=--Wiederholungsintervall (Sekunden)-'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

DEVType=SERVER (Erforderlich)
: Gibt eine Fernverbindung an, die virtuelle Bereiche unterstützt.

SERVERName (Erforderlich)
: Gibt den Namen des Servers an.Der Parameter SERVERNAME muss einem definierten Server entsprechen.

MAXCAPacity
: Gibt die maximale Größe für Objekte an, die auf dem Zielserver erstellt werden; der Standardwert ist 500M. Dieser Parameter ist wahlfrei.

  500M
  : Gibt an, dass die maximale Kapazität 500M (500 MB) beträgt.

  Größe
  : Dieser Wert muss als ganze Zahl gefolgt von einem `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte) angegeben werden. Der zulässige Mindestwert ist 1 MB (MAXCAPACITY=1M).

MOUNTLimit
: Gibt die maximal zulässige Anzahl gleichzeitig stattfindender Sitzungen zwischen dem Quellenserver und dem Zielserver an. Alle Versuche, auf mehr Sitzungen zuzugreifen als mit dem Grenzwert für Ladeanforderung angegeben sind, haben das Warten des Anforderers zur Folge. Dieser Parameter ist wahlfrei. Der Standardwert ist 1. Sie können eine Zahl von 1 bis 4096 angeben.
  Gültige Werte:

  1
  : Gibt an, dass nur eine Sitzung zwischen dem Quellenserver und dem Zielserver zulässig ist.

  Anzahl
  : Gibt die Anzahl der gleichzeitig stattfindenden Sitzungen zwischen dem Quellenserver und dem Zielserver an.

MOUNTRetention
: Gibt die Anzahl Minuten an, die eine inaktive Verbindung mit dem Zielserver aufrechterhalten werden soll, bevor die Verbindung geschlossen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Sie können eine Zahl von 0 bis 9999 angeben.
  Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

PREFIX
: Gibt den Anfangsabschnitt des Archivierungsdateinamens der höheren Ebene auf dem Zielserver an. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

  Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

  Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

  - Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

    ```
    AB.CD2.E
    ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Archivierungsdateinamens der höheren Ebene, der das Standardpräfix verwendet, ist ADSM.volume1.

RETRYPeriod
: Gibt den Wiederholungszeitraum in Minuten an. Der Wiederholungszeitraum ist das Intervall, während dem der Server versucht, eine Verbindung zu einem Zielserver herzustellen, falls ein Übertragungsfehler vermutet wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben. Der Standardwert ist 10 Minuten.

RETRYInterval
: Gibt das Wiederholungsintervall in Sekunden an. Das Wiederholungsintervall gibt an, wie oft Wiederholungen in einer bestimmten Zeitperiode erfolgen. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 1 bis 9999 angeben. Der Standardwert ist 30 Sekunden.

DEFINE DEVCLASS (Einheitenklasse VOLSAFE definieren)

Verwenden Sie den Einheitentyp VOLSAFE, um mit StorageTek VolSafe-Datenträgern und -Laufwerken zu arbeiten. Diese Technologie verwendet Datenträger, die nicht überschrieben werden können. Verwenden Sie diese Datenträger daher nicht für kurzfristige Sicherungen von Clientdateien, der Serverdatenbank oder von Exportbändern.

Einschränkungen:

1. NAS-angeschlossene Kassettenarchive werden nicht unterstützt.
2. VolSafe-Datenträger und Datenträger mit Lese-/Schreibzugriff müssen sich in separaten Speicherpools befinden.
3. Stellen Sie Kassetten mit CHECKLABEL=YES im Befehl CHECKIN LIBVOLUME zurück.
4. Kennzeichnen Sie Kassetten mit OVERWRITE=NO im Befehl LABEL LIBVOLUME. Werden VolSafe-Kassetten mehrmals gekennzeichnet, können keine weiteren Daten auf sie geschrieben werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)

Gibt den Namen des definierten Kassettenarchivobjekts an, das die VolSafe-Laufwerke enthält, die von dieser Einheitenklasse verwendet werden können. Sind Laufwerke in einem Kassettenarchiv VolSafe-aktiviert, müssen alle Laufwerke in dem Kassettenarchiv VolSafe-aktiviert sein. Lesen Sie die Informationen in der Hardwaredokumentation zur Aktivierung von VolSafe auf den 9840- und T10000-Laufwerken.

Informationen über das Definieren eines Kassettenarchivobjekts befinden sich in DEFINE LIBRARY (Kassettenarchiv definieren).

DEVType=VOLSAFE (Erforderlich)

Gibt an, dass der Einheitentyp VOLSAFE der Einheitenklasse zugeordnet wird. Der Kennsatz bei diesem Kassettentyp kann einmal übeschrieben werden. IBM Spectrum Protect führt diese Überschreibung aus, wenn der erste Datenblock geschrieben wird. Daher ist es wichtig, dass die Verwendung des Befehls LABEL LIBVOLUME auf ein Mal pro Datenträger begrenzt wird. Verwenden Sie hierfür den Parameter OVERWRITE=NO.

WORM

Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Der Parameter ist erforderlich. Der Wert muss Yes lauten.

Yes

Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.

Wichtig: Wird DRIVE für eine Einheitenklasse angegeben, die über inkompatible Einheiten mit sequenziellem Zugriff verfügt, müssen Datenträger in Einheiten geladen werden, die in dem Format lesen oder schreiben können, das beim ersten Laden des Datenträgers eingerichtet wurde. Dies kann zu Verzögerungen führen, wenn die einzige Einheit mit sequenziellem Zugriff, die auf den Datenträger zugreifen kann, bereits im Gebrauch ist.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für VolSafe-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für VOLSAFE-Datenträger

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
9840	20 GB	Dekomprimiertes (Standard) Format, verwendet eine 20-GB-Kassette mit 270 Meter Band
9840-C	Siehe Anmerkung 80 GB	Komprimiertes LZ-1 Enhanced-Format (4:1), verwendet eine 80-GB-Kassette mit 270 Meter Band
T9840C	40 GB	Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840C-C	80 GB	Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840D	75 GB	Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T9840D-C	150 GB	Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T10000A	500 GB	Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000A-C	1 TB	Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000B	1 TB	Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000B-C	2 TB	Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000C	5 TB	Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000C-C	10 TB	Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D	8 TB	Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette

Format	Geschätzte Kapazität	Beschreibung
T10000D-C	15 TB	Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette

ESTCAPacity
Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Für weitere Informationen zur geschätzten Standardkapazität von Magnetbandkassetten siehe Tabelle 1.

MOUNTRetention
Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

PREFIX
Gibt den Anfangsabschnitt des Archivierungsdateinamens der höheren Ebene auf dem Zielserver an. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Archivierungsdateinamens der höheren Ebene, der das Standardpräfix verwendet, ist ADSM.volume1.

MOUNTWait
Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Der Standardwert ist 60 Minuten. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVES. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES
Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl
: Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)
: Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

 AIX-Betriebssysteme  Linux-Betriebssysteme

DEFINE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server definieren)

Verwenden Sie den Befehl DEFINE DEVCLASS, um eine Einheitenklasse für einen Speichereinheitentyp zu definieren. Für den Server muss eine Einheitenklasse definiert werden, damit eine Einheit verwendet werden kann. Eine begrenzte Gruppe von Einheitenklassentypen ist für Einheiten verfügbar, auf die über einen z/OS Media-Server zugegriffen wird.

- DEFINE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server definieren)
- DEFINE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server definieren)
- DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server definieren)
- DEFINE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server definieren)

Tabelle 1. Zugehörige Befehle für DEFINE DEVCLASS

Befehl	Beschreibung
BACKUP DEVCONFIG	Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DELETE DEVCLASS	Löscht eine Einheitenklasse.
QUERY DEVCLASS	Zeigt Informationen zu Einheitenklassen an.
UPDATE DEVCLASS (z/OS Media-Server)	Ändert die Attribute einer Einheitenklasse für Speicher, der von einem z/OS Media-Server verwaltet wird.

 AIX-Betriebssysteme  Linux-Betriebssysteme

DEFINE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server definieren)

Um einen z/OS Media-Server für den Zugriff auf 3590-Einheiten zu verwenden, müssen Sie eine Einheitenklasse 3590 definieren. Geben Sie in der Einheitenklassendefinition ein Kassettenarchiv an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>

>--LIBRary--=--ZOSMEDIA-Kassettenarchiv--DEVType--=--3590------->

                              .-ESTCAPacity--=--9G--------.
>--+--------------------------+--+----------------------------+---->
   '-FORMAT--=--+-DRIVE---+-'  '-ESTCAPacity--=----Größe---'
                +-3590B---+
                +-3590C---+
                +-3590E-B-+
                +-3590E-C-+
                +-3590H-B-+
                '-3590H-C-'

   .-PREFIX--=--ADSM----------------------.
>--+--------------------------------------+---------------------->
   '-PREFIX--=--+-ADSM------------------+-'
                '-Banddatenträgerpräfix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+----------------------------+--+----------------------+---->
```

```
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

   .-MOUNTLimit--=--2----------.  .-COMPression--=--Yes-----.
>--+-------------------------+--+-----------------------+--->
   '-MOUNTLimit--=--+-DRIVES-+-'  '-COMPression--=--+-Yes-+-'
                    +-Anzahl-+                    '-No--'
                    '-0------'

>--+-----------------------+----------------------------------->
   +-EXPiration--=--jjjjttt-+
   '-RETention--=--Tage-----'

   .-PROtection--=--No------------.
>--+----------------------------+---------------------------->
   '-PROtection--=--+-No--------+-'
                    +-Yes-------+
                    '-Automatic-'

   .-UNIT--=--3590----------.
>--+-----------------------+---------------------------------><
   '-UNIT--=--Einheitenname-'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)

: Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

: Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

DEVtype=3590 (Erforderlich)
: Gibt an, dass der Einheitentyp 3590 der Einheitenklasse zugeordnet wird. 3590 bedeutet, dass der Einheitenklasse Magnetbandkassetteneinheiten IBM 3590 zugeordnet werden.
Einschränkung: Der z/OS Media-Server unterstützt beim Schreiben auf 3590-Bandlaufwerke 256-KB-Datenblöcke. Überprüfen Sie, ob Ihre Hardware dies unterstützt.

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.
Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für 3590

Format	**Beschreibung**
3590B	Dekomprimiertes (Basis-)Format
3590C	Komprimiertes Format
3590E-B	Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format
3590E-C	Komprimiertes Format, ähnlich dem 3590C-Format
3590H-B	Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format
3590H-C	Komprimiertes Format, ähnlich dem 3590C-Format
Anmerkung: Wenn das Format die Datenkomprimierung über Hardware mittels Bandlaufwerk verwendet, kann die tatsächliche Kapazität je nach Effektivität der Komprimierung zunehmen.	

ESTCAPacity
: Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei. Der Standardwert für die geschätzte Kapazität von 3590-Bändern beträgt 9 GB.

: Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

: Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: `K` (KB), `M` (MB), `G` (GB) oder `T` (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

PREFIX
: Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses

Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Geben Sie eine Zahl von 0 bis 9999 an.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

MOUNTWait
: Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

  Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Geben Sie eine Zahl von 1 bis 9999 an.

  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Standardwert ist 2.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Sie können einen der folgenden Werte angeben:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

COMPression
: Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

  Yes
  : Gibt an, dass die Daten der Banddatenträger komprimiert werden.

  No
  : Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

EXPiration
: Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei. Es gibt keinen Standardwert.

  Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Geben Sie das Verfallsdatum im Format *jjjjttt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als `2014007` angegeben (der siebte Tag des Jahres 2014).

Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

RETention
: Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

  Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

  Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

PROtection
: Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

  No
  : Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

  Yes
  : Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.
    Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

    Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

  Automatic
  : Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

    Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

    Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

    Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

    Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlernachrichten generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

  Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

  Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

UNIT
: Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die 3590-Band unterstützen. Dieser Parameter ist wahlfrei. Der Standardeinheitenname ist 3590. Der Einheitenname kann bis zu 8 Zeichen umfassen.

 AIX-Betriebssysteme  Linux-Betriebssysteme

DEFINE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server definieren)

Um einen z/OS Media-Server für den Zugriff auf 3592-Einheiten zu verwenden, müssen Sie eine Einheitenklasse 3592 definieren. Geben Sie in der Einheitenklassendefinition ein Kassettenarchiv an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=3592 (Erforderlich)
Gibt an, dass der Einheitentyp 3592 der Einheitenklasse zugeordnet wird.

FORMAT
Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.
Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für 3592

Format	Beschreibung

Format	Beschreibung
3592	Dekomprimiertes (Basis-)Format
3592C	Komprimiertes Format
3592-2	Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format
3592-C	Komprimiertes Format, ähnlich dem 3592C-Format
3592-3	Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format
3592-3C	Komprimiertes Format, ähnlich dem 3592C-Format
3592-4	Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format
3592-4C	Komprimiertes Format, ähnlich dem 3592C-Format
DRIVE	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann je nach Effektivität der Komprimierung die tatsächliche Kapazität von dem aufgelisteten Wert abweichen.	

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet. Um optimale Ergebnisse zu erzielen, mischen Sie nicht Generationen von Laufwerken in demselben Kassettenarchiv. Enthält ein Kassettenarchiv gemischte Generationen, können Datenträgerfehler auftreten. Beispielsweise können Laufwerke der Generation 1 und Generation 2 keine Datenträger der Generation 3 lesen. Falls möglich, führen Sie für alle Laufwerke ein Upgrade auf 3592 Generation 3 durch. Kann nicht für alle Laufwerke ein Upgrade auf 3592 Generation 3 durchgeführt werden, müssen Sie eine spezielle Konfiguration verwenden.

WORM
Gibt an, ob die Laufwerke WORM-Datenträger (Write Once, Read Many) verwenden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass die Laufwerke WORM-Datenträger verwenden.

No
Gibt an, dass die Laufwerke keine WORM-Datenträger verwenden.

Tipp: Der IBM Spectrum Protect-Server löscht nicht automatisch Arbeitsdatenträger in WORM-Speicherpools, nachdem die Datenträger durch den Verfallsprozess oder durch andere Prozesse geleert wurden. Um diese Datenträger zu löschen und die Datenträger aus WORM-Speicherpools zu entfernen, müssen Sie den Befehl DELETE VOLUME verwenden. IBM Spectrum Protect kann keine WORM-Datenträger wiederverwenden, die vom Server beschrieben und dann aus einem Speicherpool gelöscht wurden.

ESTCAPacity
Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: `K` (KB), `M` (MB), `G` (GB) oder `T` (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

PREFIX
Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

```
AB.CD2.E
```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Geben Sie eine Zahl von 0 bis 9999 an.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

MOUNTWait
: Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

  Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Geben Sie eine Zahl von 1 bis 9999 an.

  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Standardwert ist 2.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Sie können einen der folgenden Werte angeben:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

COMPression
: Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

  Yes
  : Gibt an, dass die Daten der Banddatenträger komprimiert werden.

  No
  : Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

EXPiration
: Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei. Es gibt keinen Standardwert.

  Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

  Geben Sie das Verfallsdatum im Format *jjjjttt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als `2014007` angegeben (der siebte Tag des Jahres 2014).

  Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

RETention
: Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

  Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

  Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

PROtection
Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

Yes
Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.
Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Automatic
Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlernachrichten generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

UNIT
Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die 3592-Band unterstützen. Dieser Parameter ist wahlfrei. Der Standardwert ist 3592. Der Einheitenname kann bis zu 8 Zeichen umfassen.

 AIX-Betriebssysteme  Linux-Betriebssysteme

DEFINE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server definieren)

Um einen z/OS Media-Server für den Zugriff auf StorageTek-Laufwerke, wie z. B. StorageTek T9840 oder T10000, zu verwenden, müssen Sie eine Einheitenklasse ECARTRIDGE definieren. Geben Sie in der Einheitenklassendefinition ein Kassettenarchiv an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname------------------------>

>--LIBRary--=--ZOSMEDIA-Kassettenarchiv------------------------->
```

```
                          .-FORMAT--=--DRIVE---------.
>--DEVType--=--ECARTridge--+--------------------------+--------->
                          '-FORMAT--=--+-DRIVE-----+-'
                                       +-T9840C----+
                                       +-T9840C-C--+
                                       +-T9840D----+
                                       +-T9840D-C--+
                                       +-T10000A---+
                                       +-T10000A-C-+
                                       +-T10000B---+
                                       +-T10000B-C-+
                                       +-T10000C---+
                                       +-T10000C-C-+
                                       +-T10000D---+
                                       '-T10000D-C-'

   .-ESTCAPacity--=--9G----.
>--+-----------------------+------------------------------------>
   '-ESTCAPacity--=--Größe-'

   .-PREFIX--=--ADSM----------------------.
>--+--------------------------------------+--------------------->
   '-PREFIX--=--+-ADSM------------------+-'
                '-Banddatenträgerpräfix-'

   .-MOUNTRetention--=--60------.  .-MOUNTWait--=--60------.
>--+-----------------------------+--+-------------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

   .-MOUNTLimit--=--2----------.  .-COMPression--=--Yes-----.
>--+---------------------------+--+-------------------------+--->
   '-MOUNTLimit--=--+-DRIVES-+-'  '-COMPression--=--+-Yes-+-'
                    +-Anzahl-+                     '-No--'
                    '-0------'

>--+-----------------------+------------------------------------>
   +-EXPiration--=--jjjjttt-+
   '-RETention--=--Tage-----'

   .-PROtection--=--No------------.
>--+-----------------------------+----------------------------->
   '-PROtection--=--+-No--------+-'
                    +-Yes-------+
                    '-Automatic-'

   .-UNIT--=--9840----------.
>--+-----------------------+------------------------------------><
   '-UNIT--=--Einheitenname-'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary (Erforderlich)

: Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

: Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

DEVType=ECARTridge (Erforderlich)
: Gibt an, dass der Einheitentyp ECARTRIDGE der Einheitenklasse zugeordnet wird. Der Einheitentyp ECARTRIDGE ist für StorageTek-Laufwerke, wie z. B. StorageTek T9840 oder T10000, bestimmt.

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.
: Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für ECARTRIDGE-Bänder

Format	Geschätzte Kapazität	Beschreibung

Format	Geschätzte Kapazität	Beschreibung
DRIVE	-	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. DRIVE ist der Standardwert. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
T9840C	40 GB	Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840C-C	80 GB	Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840D	75 GB	Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T9840D-C	150 GB	Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T10000A	500 GB	Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000A-C	1 TB	Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000B	1 TB	Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000B-C	2 TB	Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000C	5 TB	Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000C-C	10 TB	Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D	8 TB	Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D-C	15 TB	Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette

Anmerkung:

- Einige Formate verwenden eine Komprimierungsfunktion der Bandlaufwerkhardware. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität doppelt so groß (oder größer) sein wie der aufgeführte Wert.
- T10000A-Laufwerke können nur das T10000A-Format lesen und schreiben. T10000B-Laufwerke können das T10000A-Format lesen, aber nicht schreiben. T10000C-Laufwerke können die T10000A- und T10000B-Formate lesen, aber nicht schreiben. T10000D-Laufwerke können die T10000A-, T10000B- und T10000C-Formate lesen, aber nicht schreiben.

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei. Die standardmäßige geschätzte Kapazität ist 9 GB.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: `K` (KB), `M` (MB), `G` (GB) oder `T` (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Der Standardwert ist 60 Minuten. Geben Sie eine Zahl von 0 bis 9999 an.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

MOUNTWait
: Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

  Dieser Parameter ist wahlfrei. Der Standardwert ist 60. Geben Sie eine Zahl von 1 bis 9999 an.

  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Standardwert ist 2.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Sie können einen der folgenden Werte angeben:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

COMPression
: Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

  Yes
  : Gibt an, dass die Daten der Banddatenträger komprimiert werden.

  No
  : Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

EXPiration
: Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei. Es gibt keinen Standardwert.

  Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

  Geben Sie das Verfallsdatum im Format *jjjjttt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als `2014007` angegeben (der siebte Tag des Jahres 2014).

  Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

RETention
: Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

  Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

  Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

PROtection
: Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Der

Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No
: Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

Yes
: Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.
Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

  Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Automatic
: Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

  Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

  Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

  Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

  Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlernachrichten generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

UNIT
: Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die ECARTRIDGE-Bänder unterstützen. Verwenden Sie den Einheitennamen, der die Untergruppe der Laufwerke im Kassettenarchiv darstellt, die mit dem z/OS-System verbunden sind. Dieser Parameter ist wahlfrei. Der Standardwert ist 9840. Der Einheitenname kann bis zu 8 Zeichen umfassen.

Beispiel: Eine Einheitenklasse mit dem Einheitentyp ECARTRIDGE definieren

Die Einheitenklasse E1 mit dem Einheitentyp ECARTRIDGE sowie aktiviertem RACF-Schutz für alle Banddatenträger, die dieser Einheitenklasse zugeordnet sind, definieren. Alle Daten werden für diese Einheitenklasse komprimiert. Die Einheitenklasse gilt für das Kassettenarchiv mit dem Namen ZOSELIB eines z/OS Media-Servers.

```
define devclass e1 devtype=ecartridge library=zoselib compression=yes
   protection=yes
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

DEFINE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server definieren)

Um einen z/OS Media-Server für den Zugriff auf Speicherdatenträger auf Magnetplatteneinheiten zu verwenden, müssen Sie eine Einheitenklasse FILE definieren. Geben Sie in der Einheitenklassendefinition ein Kassettenarchiv an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde.

Ein Datenträger in dieser Einheitenklasse ist eine lineare VSAM-Datei (VSAM - Virtual Storage Access Method), auf die vom z/OS Media-Server zugegriffen wird. Arbeitsdatenträger können mit der Einheitenklasse verwendet werden und der z/OS Media-Server kann die lineare VSAM-Datei dynamisch zuordnen. Es ist nicht erforderlich, Datenträger für den Server zu definieren, um die Einheitenklasse zu verwenden. Wenn Sie Datenträger definieren, definieren Sie das Qualifikationsmerkmal der höheren Ebene so, dass SMS die Zuordnungsanforderung durch den z/OS Media-Server erkennt. Bei Verwendung von definierten Datenträgern wird die Funktion zum Formatieren von Datenträgern für den Server nicht

unterstützt, wenn diese Einheitenklasse verwendet wird. Der z/OS Media-Server verwendet beim Füllen von FILE-Datenträgern ein FormatWrite-Feature des DFSMS Media Manager.

Sie können Datenträger für die Einheitenklasse FILE definieren, indem Sie den Befehl DEFINE VOLUME verwenden. Der z/OS Media-Server ordnet jedoch erst dann Speicherbereich für einen definierten Datenträger zu, wenn der Datenträger für seine erste Verwendung geöffnet wird.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine DEVclass--Einheitenklassenname--DEVType--=--FILE------>

                                    .-MAXCAPacity--=--10G---.
>--LIBRary--=--Kassettenarchivname--+----------------------+--->
                                    '-MAXCAPacity--=--Größe-'

   .-PRIMARYalloc--=--2600M-.  .-SECONDARYalloc--=--2600M-.
>--+---------------------+--+--------------------------+----->
   '-PRIMARYalloc--=--Größe-'  '-SECONDARYalloc--=--Größe-'

   .-PREFIX--=--ADSM-------------------.
>--+---------------------------------+------------------------>
   '-PREFIX--=--Dateidatenträgerpräfix-'

   .-MOUNTLimit--=--20-----.
>--+----------------------+---------------------------------><
   '-MOUNTLimit--=--Anzahl-'
```

Parameter

DEVType=FILE (Erforderlich)
: Gibt an, dass der Einheitentyp FILE der Einheitenklasse zugeordnet wird.

LIBRary (Erforderlich)
: Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Auf den Plattenspeicher, der von dieser Einheitenklasse verwendet wird, wird von dem z/OS Media-Server zugegriffen, und der Plattenspeicher wird von SMS verwaltet.

  Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

MAXCAPacity
: Gibt die maximale Größe der Dateidatenträger an, die für einen Speicherpool in dieser Einheitenklasse definiert sind. Dieser Parameter ist wahlfrei. Der Standardwert ist 10 GB (MAXCAPACITY=10G).

  Dieser Wert muss als ganze Zahl gefolgt von einem `K` (KB), `M` (MB), `G` (GB) oder `T` (TB) angegeben werden. Die Mindestgröße ist 1 MB (MAXCAPACITY=1M). Die maximale Größe ist 16384 GB (MAXCAPACITY=16384G).

PRIMARYalloc
: Gibt den anfänglichen Speicherbereich an, der dynamisch zugeordnet wird, wenn ein neuer Datenträger geöffnet wird. Es muss genügend Speicherbereich verfügbar sein, um den Wert für die primäre Bereichszuordnung zu erfüllen. Die SMS-Richtlinie (SMS = Storage Management Subsystem) bestimmt, ob mehrere physische Datenträger verwendet werden können, um die Anforderung zur primären Bereichszuordnung zu erfüllen.

  Dieser Parameter ist wahlfrei. Dieser Wert muss als ganze Zahl gefolgt von einem `K` (KB), `M` (MB), `G` (GB) oder `T` (TB) angegeben werden. Die Mindestgröße ist 100 KB (PRIMARYALLOC=100K). Die maximale Größe ist 16384 GB (MAXCAPACITY=16384G). Die Standardgröße ist 2600 MB (PRIMARYALLOC=2600M). Alle Werte werden auf das nächsthöhere Vielfache von 256 KB gerundet.

  Um eine ineffiziente Speichernutzung zu vermeiden, verwendet die Operation für die dynamische Zuordnung den kleineren der in den beiden Parametern PRIMARYALLOC und MAXCAPACITY angegebenen Werte.

  SMS-Routinen für die automatische Klassenauswahl können Einfluss darauf haben, ob die Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC verwendet werden.

SECONDARYalloc
: Gibt den Speicherbereich an, um den ein Dateidatenträger erweitert wird, wenn der Speicherbereich, der dem Dateidatenträger bereits zugeordnet ist, verbraucht ist. Die Datei für einen Dateidatenträger wird bis zu der Größe erweitert, die mit dem Parameter MAXCAPACITY definiert ist. Danach wird der Datenträger als voll markiert.

  Da sich die sekundäre Bereichszuordnung einer linearen Datei nicht über physische Datenträger erstrecken kann, muss bei der Auswahl der Größe für die sekundäre Bereichszuordnung die Größe des physischen Datenträgers berücksichtigt werden. Beispielsweise haben physische Datenträger für ein 3390 Modell 3 eine Größe von ungefähr 2,8 GB. Um sicherzustellen, dass mit jeder Erweiterungsanforderung ungefähr der gesamte physische Datenträger belegt wird (aber nicht mehr), verwenden Sie eine Größe für die sekundäre

Bereichszuordnung, die gerade unter 2,8 GB liegt. Mit einer Größe von 2600 MB für die sekundäre Bereichszuordnung wird genügend Speicherbereich für die VSAM-Datenträgerdatei, den Datenträgerkennsatz und das Datenträgerinhaltsverzeichnis zugeordnet.

Dieser Parameter ist wahlfrei. Dieser Wert muss als ganze Zahl gefolgt von einem `K` (KB), `M` (MB), `G` (GB) oder `T` (TB) angegeben werden. Der Mindestwert ist 0 KB (SECONDARYALLOC=0K). Der Standardwert ist 2600 MB. Der Maximalwert ist 16384 GB. Mit Ausnahme von 0 werden alle Werte auf das nächsthöhere Vielfache von 256 KB gerundet.

Geben Sie 0 (SECONDARYALLOC=0) an, kann der Dateidatenträger nicht über den Wert der primären Bereichszuordnung hinaus erweitert werden.

SMS-Routinen für die automatische Klassenauswahl können Einfluss darauf haben, ob die Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC verwendet werden.

Wenn Sie einen Wert für den Parameter SECONDARYALLOCATION angeben, der nicht 0 ist, oder wenn Sie den Standardwert 2600M akzeptieren, muss für die SMS DATACLAS, der die PREFIX-Kennung zugeordnet ist (z. B. Qualifikationsmerkmal der höheren Ebene), das Attribut für die erweiterte Adressierbarkeit (Extended Addressability - EA) angegeben werden. Ohne das EA-Attribut beschränkt die SMS DATACLAS die Zuordnung des linearen VSAM-FILE-Datenträgers auf den primären Bereich. (Siehe die Beschreibung des Parameters PRIMARYALLOCATION). Wenn die Datei auf die primäre Bereichszuordnung beschränkt ist, kann die Datei vom z/OS Media-Server nicht erweitert werden, und der Datenträger wird als FULL markiert, bevor die maximale Kapazität erreicht ist.

Einschränkung: Stellen Sie sicher, dass sich die für die Parameter PRIMARYALLOC und SECONDARYALLOC angegebenen Werte innerhalb praktischer Grenzwerte für die Speichereinheit befinden. Der Server kann nicht überprüfen, ob die Werte praktische Grenzwerte für die Einheit überschreiten, und der Server überprüft nicht, ob die beiden Werte zusammen die aktuelle Einstellung für MAXCAPACITY überschreiten.
Tipp: Um bei der Angabe eines hohen Werts für den Parameter MAXCAPACITY Datenträger zu füllen, geben Sie hohe Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC an. Verwenden Sie höhere MVS-Datenträgergrößen, um die Möglichkeit eines Erweiterungsfehlers zu reduzieren.

PREFIX

Gibt die Kennung der oberen Ebene des Dateinamens an, mit der Dateien von Arbeitsdatenträgern zugeordnet werden. Bei allen in dieser Einheitenklasse erstellten Arbeitsdateidatenträgern verwendet der Server dieses Präfix für die Erstellung des Dateinamens. Dieser Parameter ist wahlfrei. Der Standardwert ist ADSM. Die maximale Länge des Präfix, einschließlich Punkte, beträgt 32 Zeichen.
Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für einen Dateidatenträger unter Verwendung des Standardpräfixes ist `ADSM.B0000021.BFS`.

Wenn Sie eine Namenskonvention für Dateinamen haben, verwenden Sie ein Präfix, das Ihrer Namenskonvention entspricht. Der folgende Wert ist beispielsweise zulässig: `TSM.SERVER2.VSAMFILE`.

Wenn Sie mehrere Serverinstanzen für IBM Spectrum Protect oder Tivoli Storage Manager for z/OS Media ausführen, müssen Sie einen eindeutigen Wert für den Parameter PREFIX für jede definierte Einheitenklasse verwenden.

MOUNTLimit

Gibt die maximale Anzahl FILE-Datenträger an, die gleichzeitig für diese Einheitenklasse geöffnet sein können. Dieser Parameter ist wahlfrei. Der Standardwert ist 20.
Wenn Sie Einheiten IBM® 3995 verwenden, die Einheiten 3390 emulieren, definieren Sie keinen höheren Wert als die Anzahl der parallelen Eingabe- oder Ausgabedatenströme, die auf den physischen Medien möglich sind.

Der in diesem Parameter angegebene Wert ist wichtig, wenn das Umschalten von einem Datenträger zu einem anderen eine große Beeinträchtigung darstellt. Das Umschalten kann beispielsweise erfolgen, wenn Sie Einheiten IBM 3995 verwenden, um Einheiten 3390 zu emulieren. Der angegebene Wert darf nicht höher als die Anzahl der physischen Laufwerke sein, die auf der Einheit verfügbar sind.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

DEFINE DOMAIN (Neue Maßnahmendomäne definieren)

Mit diesem Befehl kann eine neue Maßnahmendomäne definiert werden. Eine Maßnahmendomäne enthält Maßnahmengruppen, Verwaltungsklassen und Kopiengruppen. Ein Client wird einer Maßnahmendomäne zugeordnet. Die AKTIVE Maßnahmengruppe in der Maßnahmendomäne bestimmt die Regeln für Clients, die der Domäne zugeordnet werden. Die Regeln steuern die Archivierungsservices, Sicherungsservices und Speicherverwaltungsservices, die für die Clients zur Verfügung gestellt werden.

Eine Maßnahmengruppe muß in der Domäne aktiviert werden, bevor die der Maßnahmendomäne zugeordneten Clients Dateien sichern, archivieren oder umlagern können.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine DOmain--Domänenname------------------------------------>

>--+-------------------------------+---------------------------->
   '-DESCription--=--Beschreibung-'

   .-BACKRETention--=--30---.  .-ARCHRETention--=--365--.
>--+-----------------------+--+-----------------------+------->
   '-BACKRETention--=--Tage-'  '-ARCHRETention--=--Tage-'

>--+-------------------------------------------------------------+-><
   |                       .-,-----------------------------------. |
   |                       V                                     | |
   '-ACTIVEDESTination--=------Name_des_Pools_für_aktive_Daten---+-'
```

Parameter

Domänenname (Erforderlich)
: Gibt den Namen der zu definierenden Maßnahmendomäne an. Die maximale Länge dieses Namens beträgt 30 Zeichen.

DESCription
: Beschreibung der Maßnahmendomäne. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

BACKRETention
: Gibt die Anzahl Tage an (ab dem Datum, an dem die Sicherungsversionen inaktiv wurden), die Sicherungsversionen von Dateien aufbewahrt werden sollen, die sich nicht mehr im Client-Dateisystem befinden. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 0 bis 9999. Der Standardwert ist 30. Der Server verwendet den Wert für den Aufbewahrungszeitraum für Sicherung, um inaktive Versionen von Dateien zu verwalten, wenn eine der folgenden Bedingungen zutrifft:

  - Eine Datei wird an eine neue Verwaltungsklasse erneut gebunden, aber die neue Verwaltungsklasse und die Standardverwaltungsklasse enthalten keine Sicherungskopiengruppe.
  - Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden. Die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.
  - Die Sicherungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist. Die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.

ARCHRETention
: Gibt die Anzahl Tage an (ab dem Datum der Archivierung), die Archivierungskopien aufbewahrt werden sollen. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 30000 angeben. Der Standardwert ist 365. Der Server verwendet den Wert für den Aufbewahrungszeitraum für Archivierung, um Archivierungskopien von Dateien zu verwalten, wenn eine der folgenden Bedingungen zutrifft:

  - Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden. Die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.
  - Die Archivierungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist. Die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.

ACTIVEDESTination
: Dieser optionale Parameter gibt die Namen der Pools für aktive Daten an, in denen aktive Versionen von Sicherungsdaten für Knoten gespeichert werden, die der Domäne zugeordnet sind. Sie können bis zu 10 Pools für aktive Daten, die durch Kommas getrennt werden müssen, für eine Domäne angeben. Leerzeichen zwischen den Namen sind nicht zulässig.

  Bevor der IBM Spectrum Protect-Server Daten in einen Pool für aktive Daten schreibt, überprüft er, ob der Knoten, der Eigner der Daten ist, einer Domäne zugeordnet ist, für die der Pool für aktive Daten in der ACTIVEDESTINATION-Liste aufgelistet ist. Stellt der Server fest, dass der Knoten diese Kriterien erfüllt, werden die Daten im Pool für aktive Daten gespeichert. Werden die Kriterien vom Knoten nicht erfüllt, werden die Daten nicht im Pool für aktive Daten gespeichert. Werden mit der Funktion für simultanes Schreiben Daten in einen Pool für aktive Daten geschrieben, führt der Server die Prüfung, ob der Knoten die Kriterien erfüllt, während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients unter Verwendung der IBM Spectrum Protect-API aus. Die Prüfung wird auch durchgeführt, wenn aktive Daten mit dem Befehl COPY ACTIVEDATA kopiert werden.

Beispiel: Eine Maßnahmendomäne definieren

Eine Maßnahmendomäne mit dem Namen PROG1 und der Beschreibung "Programming Group Domain" definieren. Angeben, daß Archivierungskopien 90 Tage aufbewahrt werden sollen, wenn Verwaltungsklassen oder Archivierungskopiengruppen gelöscht werden und die Standardverwaltungsklasse keine Archivierungskopiengruppe enthält. Außerdem angeben, dass Sicherungsversionen 60 Tage aufbewahrt werden sollen, wenn Verwaltungsklassen oder Kopiengruppen gelöscht werden und die Standardverwaltungsklasse keine Sicherungskopiengruppe enthält.

```
define domain prog1
description="Programming Group Domain"
backretention=60 archretention=90
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE DOMAIN

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
COPY DOMAIN	Erstellt eine Kopie einer Maßnahmendomäne.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
DELETE DOMAIN	Löscht eine Maßnahmendomäne und, falls vorhanden, Maßnahmenobjekte in der Maßnahmendomäne.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
UPDATE DOMAIN	Ändert die Attribute einer Maßnahmendomäne.

DEFINE DRIVE (Laufwerk für Kassettenarchiv definieren)

Verwenden Sie diesen Befehl, um ein Laufwerk zu definieren. Jedes Laufwerk wird einem Kassettenarchiv zugeordnet, d.h., das Kassettenarchiv muss definiert werden, bevor Sie diesen Befehl ausgeben.

Ein Pfad muss definiert werden, nachdem Sie den Befehl DEFINE DRIVE ausgegeben haben, damit IBM Spectrum Protect das Laufwerk verwenden kann. Weitere Informationen befinden sich in DEFINE PATH (Pfad definieren).Wenn Sie einen Speicherarchivtyp SCSI oder VTL verwenden, lesen Sie die Informationen in PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Kassettenarchiv definieren oder löschen).

Für ein Kassettenarchiv können mehrere Laufwerke definiert werden, indem der Befehl DEFINE DRIVE für jedes Laufwerk ausgegeben wird. Für eigenständige Laufwerke ist immer ein manuelles Kassettenarchiv erforderlich.

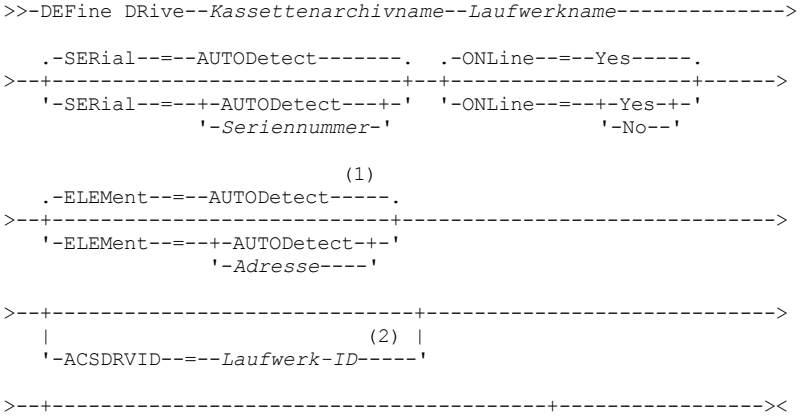
Windows-BetriebssystemeEinschränkung: Bevor Sie den Befehl DEFINE DRIVE für eine Einheit für austauschbare Datenträger, wie beispielsweise ein Jaz-, Zip- oder CD-Laufwerk, ausgeben, müssen Sie das Laufwerk mit ordnungsgemäß formatierten und gekennzeichneten Datenträgern laden.
Ausführliche und aktuelle Informationen zur Laufwerkunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax



```
|                       (3)                 |
'-CLEANFREQuency--=======+-NONE----------+-'
                         |          (4)  |
                         +-ASNEEDED------+
                         '-Gigabyte------'
```

Anmerkungen:

1. Der Parameter ELEMENT ist nur für Laufwerke in SCSI-Kassettenarchiven erforderlich, wenn das Laufwerk an ein Netz angeschlossenes SCSI-Laufwerk (NAS) ist.
2. ACSDRVID ist erforderlich für Laufwerke in ACSLS-Kassettenarchiven. Dieser Parameter ist nicht gültig für Nicht-ACSLS-Kassettenarchive.
3. Der Parameter CLEANFREQUENCY ist nur für Laufwerke in SCSI-Kassettenarchiven gültig.
4. Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht bei allen Bandlaufwerken. Weitere Informationen enthält die Parameterbeschreibung.

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, dem das Laufwerk zugeordnet ist. Dieser Parameter ist erforderlich für alle Laufwerke, einschließlich eigenständiger Laufwerke. Das angegebene Kassettenarchiv muss zuvor mit dem Befehl DEFINE LIBRARY definiert werden.

Laufwerkname (Erforderlich)
: Gibt den Namen an, der dem Laufwerk zugeordnet ist. Die maximale Länge dieses Namens beträgt 30 Zeichen.

SERial
: Gibt die Seriennummer des Laufwerks an, das definiert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist AUTODETECT.

  Bei SERIAL=AUTODETECT wird die vom Laufwerk bei der Definition des Pfads gemeldete Seriennummer als Seriennummer verwendet.

  Bei SERIAL=*Seriennummer* wird die eingegebene Seriennummer verwendet, um zu überprüfen, ob der Pfad zum Laufwerk korrekt ist, wenn der Pfad definiert wird.

  Anmerkung: Je nach Leistungsspektrum der Einheit wird SERIAL=AUTODETECT möglicherweise nicht unterstützt. In diesem Fall wird die Seriennummer als leer gemeldet.

ONLine
: Gibt an, ob das Laufwerk für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

  Yes
  : Gibt an, dass das Laufwerk für die Verwendung verfügbar ist.

  No
  : Gibt an, dass das Laufwerk nicht für die Verwendung verfügbar ist.

ELEMent
: Gibt die Elementadresse eines Laufwerks in einem SCSI- oder VTL-Archiv (VTL - Virtual Tape Library) an. Der Server verwendet die Elementadresse, um die physische Adresse des Laufwerks mit der SCSI- oder VTL-Adresse des Laufwerks zu verbinden. Der Standardwert ist AUTODETECT.

  Bei ELEMENT=AUTODETECT wird die Elementnummer automatisch vom Server erkannt, wenn der Pfad zu dem Laufwerk definiert ist.

  Zum Lokalisieren der Elementadresse für die Archivkonfiguration die Informationen des Herstellers zu Rate ziehen.

  Einschränkung:

  - Der Parameter ELEMENT ist nur für Laufwerke in SCSI-Kassettenarchiven oder virtuellen Bandarchiven (VTLs) gültig, wenn das Laufwerk kein an ein Netz angeschlossenes SCSI-Laufwerk (NAS) ist.
  - Dieser Parameter ist nicht gültig, wenn der Befehl von einem Kassettenarchivclientserver ausgegeben wird (d. h., wenn der Kassettenarchivtyp SHARED ist).
  - Je nach Leistungsspektrum des Kassettenarchivs wird ELEMENT=AUTODETECT möglicherweise nicht unterstützt. In diesem Fall müssen Sie die Elementadresse angeben.

ACSDRVID
: Gibt die ID des Laufwerks an, auf das in einem ACSLS-Kassettenarchiv zugegriffen wird. Die Laufwerk-ID ist eine Zahlengruppe, die die physische Adresse eines Laufwerks in einem ACSLS-Kassettenarchiv angibt. Diese Laufwerk-ID muss als *a,l,p,d,* angegeben werden, wobei *a* die ACSID, *l* das LSM (Library Storage Module), *p* die Anzeigennummer und *d* die Laufwerk-ID ist. Der Server benötigt die Laufwerk-ID, um die physische Adresse des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Die StorageTek-Dokumentation enthält ausführliche Informationen.
  Windows-BetriebssystemeEinschränkung: Um ACSLS-Funktionen verwenden zu können, ist die Installation von StorageTek Library Attach-Software erforderlich.

CLEANFREQuency
: Gibt an, wie oft der Server die Laufwerkreinigung aktiviert. Dieser Parameter ist wahlfrei. Um die Reinigung für ein automatisiertes Kassettenarchiv nahezu vollständig zu automatisieren, müssen Sie eine Reinigungskassette haben, die in den Datenträgerbestand des Kassettenarchivs zurückgestellt wird.

Bei Verwendung der speicherarchivbasierten Reinigung wird NONE empfohlen, wenn Ihr Speicherarchivtyp diese Funktion unterstützt.

Dieser Parameter ist für extern verwaltete Kassettenarchive, wie beispielsweise 3494-Kassettenarchive oder StorageTek-Kassettenarchive, die unter ACSLS verwaltet werden, nicht gültig.

Wichtig: Es gibt einige Besonderheiten, die beachtet werden müssen, wenn die vom Server aktivierte Laufwerkreinigung bei einem SCSI-Kassettenarchiv verwendet werden soll, das eine automatische Laufwerkreinigungsunterstützung in seiner Einheitenhardware zur Verfügung stellt.

NONE
: Gibt an, dass der Server die Reinigung dieses Laufwerks nicht verfolgt. Dieser Wert kann für Kassettenarchive verwendet werden, die über ihre eigene automatische Reinigungsunterstützung verfügen.

ASNEEDED
: Gibt an, dass der Server das Laufwerk mit einer zurückgestellten Reinigungskassette nur lädt, wenn ein Laufwerk dem Einheitentreiber mitteilt, dass eine Reinigung erforderlich ist.

  Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht bei allen Bandlaufwerken. Detaillierte Laufwerkdaten finden Sie auf der Website für unterstützte Einheiten für Ihr Betriebssystem. Wird ASNEEDED nicht unterstützt, können Sie den Gigabyte-Wert für die automatische Reinigung verwenden.

  Für IBM 3592- und LTO-Laufwerke wird die speicherarchivbasierte Reinigung empfohlen. Wird die speicherarchivbasierte Reinigung nicht unterstützt, muss ASNEEDED verwendet werden. Gigabyte wird nicht empfohlen.

  Einschränkung: IBM Spectrum Protect steuert nicht die Laufwerke, die mit dem NAS-Dateiserver verbunden sind. Ist ein Laufwerk nur mit einem NAS-Dateiserver verbunden (keine Verbindung zu einem Speicheragenten oder Server), geben Sie nicht ASNEEDED für die Häufigkeit der Reinigung an.

Gigabyte
: Gibt in Gigabyte an, wieviel Daten auf dem Laufwerk verarbeitet werden, bevor der Server das Laufwerk mit einer Reinigungskassette lädt. Der Server setzt den Zähler für die verarbeiteten Gigabyte zurück, wenn eine Reinigungskassette in das Laufwerk geladen wird.
  Wichtig: Bei CLEANFREQUENCY=Gigabyte kann die Laufwerkreinigung erfolgen, bevor die Einstellung für Gigabyte erreicht ist, wenn das Laufwerk den Einheitentreiber benachrichtigt, dass eine Reinigung erforderlich ist.

  Lesen Sie die Empfehlungen des Laufwerkherstellers bezüglich der Reinigung. Werden Empfehlungen für die Reinigungshäufigkeit in Stunden der Verwendung gegeben, führen Sie wie folgt eine Umrechnung in einen Gigabytewert durch:

  1. Verwenden Sie den Wert für Byte pro Sekunde des Laufwerks, um einen Wert für Gigabyte pro Stunde zu ermitteln.
  2. Multiplizieren Sie den Wert für Gigabyte pro Stunde mit den empfohlenen Stunden der Verwendung zwischen den Reinigungen.
  3. Verwenden Sie das Ergebnis als Wert für die Reinigungshäufigkeit.

  Bei Verwendung der Reinigungshäufigkeit, die von IBM® für IBM Laufwerke empfohlen wird, wird sichergestellt, dass die Reinigung der Laufwerke nicht zu oft durchgeführt wird.

  Geben Sie für IBM 3590-Laufwerke einen Gigabyte-Wert für die Reinigungshäufigkeit an, um eine adäquate Reinigung der Laufwerke sicherzustellen.

Beispiel: Ein Laufwerk für ein Kassettenarchiv definieren

Ein Laufwerk in einem manuellen Kassettenarchiv mit dem Kassettenarchivnamen LIB01 und dem Laufwerknamen DRIVE01 definieren.

```
define drive lib01 drive01
```


AIX-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive
library=lib01 device=/dev/rmt0
```


Linux-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive
library=lib01 device=/dev/tsmscsi/mt0
```


Windows-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive
library=lib01 device=mt3.0.0.0
```

Beispiel: Ein Laufwerk in einem ACSLS-Kassettenarchiv definieren

Ein Laufwerk in einem ACSLS-Kassettenarchiv mit dem Kassettenarchivnamen ACSLIB und dem Laufwerknamen ACSDRV1 definieren.

```
define drive acslib acsdrv1 acsdrvid=1,2,3,4
```

AIX-Betriebssysteme

```
define path server01 acsdrv1 srctype=server desttype=drive
library=acslib device=/dev/rmt0
```

Linux-Betriebssysteme

```
define path server01 acsdrv1 srctype=server desttype=drive
library=acslib device=/dev/tsmscsi/mt0
```

Windows-Betriebssysteme

```
define path server01 acsdrv1 srctype=server desttype=drive
library=acslib device=mt3.0.0.0
```

Beispiel: Ein Laufwerk in einem automatisierten Kassettenarchiv definieren

Ein Laufwerk in einem automatisierten Kassettenarchiv mit dem Kassettenarchivnamen AUTO8MMLIB und dem Laufwerknamen DRIVE01 definieren.

```
define drive auto8mmlib drive01 element=82
```

AIX-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive
library=auto8mmlib device=/dev/rmt0
```

Linux-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive
library=auto8mmlib device=/dev/tsmscsi/mt0
```

Windows-Betriebssysteme

```
define path server01 drive01 srctype=server desttype=drive
library=auto8mmlib device=mt3.0.0.0
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE DRIVE

Befehl	Beschreibung
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE DRIVE	Löscht ein Laufwerk aus einem Kassettenarchiv.
DELETE LIBRARY	Löscht ein Kassettenarchiv.
PERFORM LIBACTION	Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.
QUERY DRIVE	Zeigt Informationen zu Laufwerken an.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE DRIVE	Ändert die Attribute eines Laufwerks.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.

DEFINE EVENTSERVER (Server als Ereignisserver definieren)

Mit diesem Befehl kann ein Server als Ereignisserver definiert werden.

Wird ein Ereignisserver definiert, kann ein IBM Spectrum Protect-Server Ereignisse an einen anderen IBM Spectrum Protect-Server senden, der diese Ereignisse protokolliert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine EVENTSERVer--Servername------------------------------><
```

Parameter

Servername (Erforderlich)
: Gibt den Namen des Ereignis-Servers an. Der angegebene Server muss bereits mit dem Befehl DEFINE SERVER definiert worden sein.

Beispiel: Den Ereignisserver definieren

ASTRO als Ereignisserver definieren.

```
define eventserver astro
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE EVENTSERVER

Befehl	Beschreibung
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DELETE EVENTSERVER	Löscht Verweise auf den Ereignisserver.
DISABLE EVENTS	Inaktiviert bestimmte Ereignisse für Empfänger.
ENABLE EVENTS	Aktiviert bestimmte Ereignisse für Empfänger.
PING SERVER	Testet die Verbindungen zwischen Servern..
QUERY EVENTSERVER	Zeigt den Namen des Ereignisservers an.
QUERY SERVER	Zeigt Informationen über Server an.

Zugehörige Informationen:

Unternehmensweite Ereignisprotokollierung: Ereignisse auf einem anderen Server protokollieren

DEFINE GRPMEMBER (Server zu einer Servergruppe hinzufügen)

Mit diesem Befehl kann ein Server als Teil einer Servergruppe hinzugefügt werden. Es kann auch eine Servergruppe zu einer anderen Servergruppe hinzugefügt werden. Mit Hilfe einer Servergruppe können Befehle an mehrere Server weitergeleitet werden, indem nur der Name der Servergruppe angegeben wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                                .-,--------------.
                               V                 |
>>-DEFine GRPMEMber--Gruppenname----Name_des_Teils-+-----------><
```

Parameter

Gruppenname (Erforderlich)
: Gibt den Namen der Servergruppe an, der das Teil hinzugefügt wird.

Name_des_Teils (Erforderlich)
: Gibt die Namen der Server oder Gruppen an, die der Gruppe hinzugefügt werden sollen. Sollen mehrere Server und Gruppen angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Die Server oder Servergruppen müssen bereits für den Server definiert sein.

Beispiel: Einen Server für eine Servergruppe definieren

Den Server SANJOSE für Server-Gruppe CALIFORNIA definieren.

```
define grpmember california sanjose
```

Beispiel: Einen Server und eine Servergruppe für eine Servergruppe definieren

Den Server TUCSON und die Server-Gruppe CALIFORNIA für Server-Gruppe WEST_COMPLEX definieren.

```
define grpmember west_complex tucson,california
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE GRPMEMBER

Befehl	Beschreibung
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DEFINE SERVERGROUP	Definiert eine neue Servergruppe.
DELETE GRPMEMBER	Löscht einen Server aus einer Servergruppe.
DELETE SERVERGROUP	Löscht eine Servergruppe.
MOVE GRPMEMBER	Versetzt einen Teil einer Servergruppe.
QUERY SERVER	Zeigt Informationen über Server an.
RENAME SERVERGROUP	Benennt eine Servergruppe um.
UPDATE SERVERGROUP	Aktualisiert eine Servergruppe.

DEFINE LIBRARY (Kassettenarchiv definieren)

Mit diesem Befehl kann ein Kassettenarchiv definiert werden. Ein Kassettenarchiv besteht aus einem oder mehreren Laufwerken und unter Umständen auch automatischen Einheiten (je nach Kassettenarchivtyp), über die auf Speicherdatenträger zugegriffen werden kann.

Auf ein Kassettenarchiv kann nur von einer Quelle zugegriffen werden: einem IBM Spectrum Protect-Server oder einer Einheit zum Versetzen von Daten. Auf die Laufwerke in einem Kassettenarchiv können jedoch mehrere Quellen zugreifen.

Die folgenden Kassettenarchivtypen können für den Server definiert werden. Syntax- und Parameterbeschreibungen sind für jeden Typ verfügbar.

- DEFINE LIBRARY (349X-Kassettenarchiv definieren)
- DEFINE LIBRARY (ACSLS-Kassettenarchiv definieren)
- DEFINE LIBRARY (Externes Kassettenarchiv definieren)
- DEFINE LIBRARY (Kassettenarchiv FILE definieren)
- DEFINE LIBRARY (Manuelles Kassettenarchiv definieren)
- DEFINE LIBRARY (SCSI-Kassettenarchiv definieren)
- DEFINE LIBRARY (Gemeinsam genutztes Kassettenarchiv definieren)
- DEFINE LIBRARY (VTL-Speicherarchiv definieren)
- AIX-BetriebssysteLinux-BetriebssystemeDEFINE LIBRARY (Speicherarchivtyp ZOSMEDIA definieren)

Ausführliche und aktuelle Informationen zur Kassettenarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssysteWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Windows-Betriebssysteme

Um Banddatenträger in SCSI-Speicherarchiven automatisch zu kennzeichnen, verwenden Sie den Parameter AUTOLABEL in den Befehlen DEFINE LIBRARY und UPDATE LIBRARY. Wird dieser Parameter verwendet, ist es nicht erforderlich, eine Gruppe von Bändern vorab zu kennzeichnen. Außerdem ist die Verwendung dieses Parameters effizienter als die Verwendung des Befehls LABEL LIBVOLUME, der es erfordert, dass Datenträger separat bereitgestellt werden. Wenn Sie den Parameter AUTOLABEL verwenden, müssen Sie Bänder zurückstellen, indem Sie CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME angeben.

Ein Kennsatz darf keine eingebetteten Leerzeichen oder Punkte enthalten und muss gültig sein, wenn er als Dateiname auf den Datenträgern verwendet wird.

Sie müssen CD-ROM-, Zip- oder Jaz-Datenträger mit den Dienstprogrammen des Einheitenherstellers oder den Windows-Dienstprogrammen kennzeichnen, da IBM Spectrum Protect keine Dienstprogramme zum Formatieren oder Kennzeichnen dieser Datenträgertypen bereitstellt. Die Dienstprogramme des Betriebssystems schließen das Plattenverwaltungsprogramm (Disk Administrator) (eine grafische Benutzerschnittstelle) und den Befehl zum Zuordnen von Kennsätzen ein.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE LIBRARY

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.

Befehl	Beschreibung
CHECKIN LIBVOLUME	Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DELETE DRIVE	Löscht ein Laufwerk aus einem Kassettenarchiv.
DELETE LIBRARY	Löscht ein Kassettenarchiv.
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
LABEL LIBVOLUME	Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.
PERFORM LIBACTION	Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.
QUERY DRIVE	Zeigt Informationen zu Laufwerken an.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY LIBVOLUME	Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE DRIVE	Ändert die Attribute eines Laufwerks.
UPDATE LIBRARY	Ändert die Attribute eines Kassettenarchivs.
UPDATE LIBVOLUME	Ändert den Status eines Speicherdatenträgers.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.

DEFINE LIBRARY (349X-Kassettenarchiv definieren)

Verwenden Sie diese Syntax, um ein 349X-Kassettenarchiv zu definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine LIBRary--Speicherarchivname--LIBType--=--349X--------->

   .-SHAREd--=--No------.  .-RESETDrives--=--No----------.
>--+--------------------+--+---------------------------+------>
   '-SHAREd--=--+-Yes-+-'  |                       (1) |
                '-No--'    '-RESETDrives--=--+-Yes-+-----'
                                             '-No--'

   .-AUTOLabel--=--Yes-----------.
>--+-----------------------------+----------------------------->
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'

   .-SCRATCHCATegory--=--301----.
>--+----------------------------+----------------------------->
   '-SCRATCHCATegory--=--Nummer-'

   .-PRIVATECATegory--=--300----.
>--+----------------------------+----------------------------->
   '-PRIVATECATegory--=--Nummer-'

>--+--------------------------------+-------------------------><
   '-WORMSCRatchcategory--=--Nummer-'
```

Anmerkungen:

1. Der Standardwert des Parameters RESETDRIVES ist situationsabhängig. Wenn der Parameter SHARED auf NO gesetzt ist, ist NO der Wert des Parameters RESETDRIVES. Wenn der Parameter SHARED auf YES gesetzt ist, ist YES der Wert des Parameters RESETDRIVES.

Parameter

Speicherarchivname (Erforderlich)
Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=349X (Erforderlich)



Gibt an, dass das Kassettenarchiv ein IBM 3494 oder 3495 Tape Library Dataserver ist.


Gibt an, dass das Kassettenarchiv ein IBM 3494 Tape Library Dataserver oder ein IBM Tape System Library Manager ist, der einen 3494 Tape Library Dataserver emuliert.

Einschränkung: IBM 3494-Kassettenarchive unterstützen nur jeweils einen eindeutigen Einheitentyp.

SHAREd
Gibt an, ob dieses Kassettenarchiv mit anderen Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam genutzt wird. Dieser Parameter ist erforderlich, wenn Sie ein Kassettenarchiv für den Kassettenarchivmanager definieren.

YES
Gibt an, dass dieses Kassettenarchiv mit anderen Servern gemeinsam genutzt werden kann. Wird YES angegeben, lädt der Kassettenarchivmanagerserver Datenträger, die von anderen Servern angefordert werden, und verfolgt die Laufwerk- und Datenträgerzuordnung zu anderen Servern.

NO
Gibt an, dass dieses Kassettenarchiv nicht mit anderen Servern gemeinsam genutzt werden kann. SHARED=NO ist erforderlich, wenn das Kassettenarchiv durch die Übergabe von Befehlen über einen NAS-Dateiserver gesteuert wird.

AUTOLabel
Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

No
Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes
Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE
Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze nur dann, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

SCRATCHCATegory
Gibt die Kategorienummer für Arbeitsdatenträger im Kassettenarchiv an. Dieser Parameter ist wahlfrei. Der Standardwert ist 301 (wird auf der Einheit IBM 3494 zu X'12D', da sie Hexadezimalwerte verwendet). Es kann eine Zahl von 1 bis 65279 angegeben werden. Diese Zahl muss eindeutig sein. Sie kann nicht mit anderen Anwendungen oder definierten Kassettenarchiven gemeinsam genutzt werden, und sie muss sich von den anderen Kategorienummern in diesem Kassettenarchiv unterscheiden.

PRIVATECATegory
Gibt die Kategorienummer für private Datenträger an, die nach Namen geladen werden müssen. Dieser Parameter ist wahlfrei. Der Standardwert ist 300 (dieser Wert wird auf der Einheit IBM 3494 zu X'12C', da sie Hexadezimalwerte verwendet). Es kann eine Zahl von 1 bis 65279 angegeben werden. Diese Zahl muss eindeutig sein. Sie kann nicht mit anderen Anwendungen oder definierten Kassettenarchiven gemeinsam genutzt werden, und sie muss sich von den anderen Kategorienummern in diesem Kassettenarchiv unterscheiden.

WORMSCRatchcategory
Gibt die Kategorienummer an, die für WORM-Arbeitsdatenträger in dem Kassettenarchiv verwendet werden soll. Dieser Parameter ist erforderlich, wenn WORM-Datenträger verwendet werden. Es kann eine Zahl von 1 bis 65279 angegeben werden. Diese Zahl muss eindeutig sein. Sie kann nicht mit anderen Anwendungen oder definierten Kassettenarchiven gemeinsam genutzt werden, und sie muss sich von den anderen Kategorienummern in diesem Kassettenarchiv unterscheiden. Dieser Parameter ist nur bei Verwendung von WORM-Datenträgern 3592 gültig.
Einschränkung: Ist WORMSCRATCHCATEGORY nicht definiert und ist der Parameter WORM für die Einheitenklasse auf YES gesetzt, schlägt die Ladeoperation mit einer Fehlernachricht fehl.

RESETDrives
Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

AIX-BetriebssystemeWindows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

Konfiguration der Speicherarchiveinheit	Verhalten für persistente Reserve
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt.	Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.	Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben.

AIX-BetriebssystemeWindows-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

Linux-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

Beispiel: Ein Kassettenarchiv 3494 definieren

Ein Kassettenarchiv mit dem Namen `my3494` mit der Arbeitsdatenträgerkategorie 550, der privaten Kategorie 600 und der WORM-Arbeitsdatenträgerkategorie 400 definieren.

```
define library my3494 libtype=349x scratchcategory=550
privatecategory=600 wormscratchcategory=400
```

DEFINE LIBRARY (ACSLS-Kassettenarchiv definieren)

Verwenden Sie diese Syntax, um ein ACSLS-Kassettenarchiv zu definieren.

Berechtigungsklasse

Windows-BetriebssystemeUm ACSLS-Funktionen verwenden zu können, ist die Installation von StorageTek Library Attach-Software erforderlich.

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine LIBRary--Speicherarchivname--LIBType--=--ACSLS-------->

   .-SHAREd--=--No------.  .-RESETDrives--=--No----------.
>--+--------------------+--+----------------------------+------>
   '-SHAREd--=--+-Yes-+-'  |                          (1) |
                '-No--'    '-RESETDrives--=--+-Yes-+-----'
                                             '-No--'

   .-AUTOLabel--=--Yes-----------.
>--+-----------------------------+--ACSID--=--Nummer-----------><
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'
```

Anmerkungen:

1. Der Standardwert des Parameters RESETDRIVES ist situationsabhängig. Wenn der Parameter SHARED auf NO gesetzt ist, ist NO der Wert des Parameters RESETDRIVES. Wenn der Parameter SHARED auf YES gesetzt ist, ist YES der Wert des Parameters RESETDRIVES.

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=ACSLS (Erforderlich)
: Gibt an, dass es sich bei dem Kassettenarchiv um ein StorageTek-Kassettenarchiv handelt, das durch StorageTek Automated Cartridge System Library Software (ACSLS) gesteuert wird.

SHAREd
: Gibt an, ob dieses Kassettenarchiv mit anderen Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam genutzt wird. Dieser Parameter ist erforderlich, wenn Sie ein Kassettenarchiv für den Kassettenarchivmanager definieren.

  YES
  : Gibt an, dass dieses Kassettenarchiv mit anderen Servern gemeinsam genutzt werden kann. Wird YES angegeben, lädt der Kassettenarchivmanagerserver Datenträger, die von anderen Servern angefordert werden, und verfolgt die Laufwerk- und Datenträgerzuordnung zu anderen Servern.

  NO
  : Gibt an, dass dieses Kassettenarchiv nicht mit anderen Servern gemeinsam genutzt werden kann. SHARED=NO ist erforderlich, wenn das Kassettenarchiv durch die Übergabe von Befehlen über einen NAS-Dateiserver gesteuert wird.

RESETDrives
: Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

  AIX-BetriebssystemeWindows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

  Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

  Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

  - Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
  - Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
  - Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

  In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

Konfiguration der Speicherarchiveinheit	Verhalten für persistente Reserve
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt.	Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.

Konfiguration der Speicherarchiveinheit	Verhalten für persistente Reserve
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.	Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben.

 AIX-Betriebssysteme  Windows-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

 Linux-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

AUTOLabel
: Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

No
: Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes
: Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE
: Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

ACSID (Erforderlich)
: Gibt die Nummer dieses StorageTek-Kassettenarchivs an, das von ACSSA (Automatic Cartridge System System Administrator) zugeordnet wird. Hierbei kann es sich um eine Zahl von 0 bis 126 handeln. Geben Sie den Befehl QUERY ACS auf dem System aus, um die Nummer für die Kassettenarchiv-ID abzufragen. Dieser Parameter ist erforderlich.

Weitere Informationen enthält die StorageTek-Dokumentation.

Beispiel: Ein gemeinsam genutztes ACSLS-Kassettenarchiv definieren

Ein Kassettenarchiv mit dem Namen ACSLIB, dem Kassettenarchivtyp ACSLS und der ACSID 1 definieren.

```
define library acslib libtype=acsls acsid=1 shared=yes
```

DEFINE LIBRARY (Externes Kassettenarchiv definieren)

Verwenden Sie diese Syntax, um ein externes Kassettenarchiv zu definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine LIBRary--Kassettenarchivname--LIBType--=--EXTernal---->
```

```
   .-AUTOLabel--=--Yes-----------.
>--+---------------------------+----------------------------><
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=EXTernal (Erforderlich)
: Gibt an, dass das Kassettenarchiv von einem externen Datenträgerverwaltungssystem verwaltet wird. Dieser Kassettenarchivtyp unterstützt keine mit dem Befehl DEFINE DRIVE erstellten Definitionen. Vielmehr bestimmt das externe Datenträgerverwaltungssystem das geeignete Laufwerk für Datenträgerzugriffsoperationen.

   AIX-Betriebssysteme  Windows-BetriebssystemeIn einer IBM Spectrum Protect for Storage Area Networks-Umgebung gibt dieser Parameter an, dass StorageTek Automated Cartridge System Library Software (ACSLS) oder Library Station Software das Kassettenarchiv steuert. Software, wie beispielsweise Gresham EDT-DistribuTAPE, erlaubt es mehreren Servern, das Kassettenarchiv gemeinsam zu benutzen. Die Laufwerke in diesem Kassettenarchiv sind nicht für IBM Spectrum Protect definiert. ACSLS identifiziert das Laufwerk für Datenträgeroperationen.

AUTOLabel
: Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

  Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

  No
  : Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

  Yes
  : Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

  OVERWRITE
  : Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

Beispiel: Ein externes Kassettenarchiv für eine SAN-Konfiguration definieren

Für eine IBM Spectrum Protect for Storage Area Networks-Konfiguration das Kassettenarchiv EXTLIB mit dem Kassettenarchivtyp EXTERNAL definieren. Bei Verwendung von Gresham Enterprise DistribuTAPE befindet sich die ausführbare Datei des externen Kassettenarchivmanagers in dem folgenden Verzeichnis:

-  AIX-Betriebssysteme/usr/lpp/dtelm/bin/elm
-  Linux-Betriebssysteme/opt/OMIdtelm/bin/elm
- Windows-Betriebssystemec:\program files\GES\EDT\bin\elm.exe

Wenn Sie den IBM® Tape System Library Manager verwenden, befindet sich die ausführbare Datei des externen Kassettenarchivmanagers in dem folgenden Verzeichnis:

-  AIX-Betriebssysteme  Linux-Betriebssysteme/opt/IBM/TSLM/client/tsm/elm
-  Windows-Betriebssysteme...\IBM\rmm\client\tsm\elm.exe

Weitere Informationen befinden sich im *IBM Tape System Library Manager User's Guide* unter *http://www.ibm.com/support/docview.wss?uid=ssg1S7004001*.

1. Das Kassettenarchiv definieren:

   ```
   define library extlib libtype=external
   ```

2. Den Pfad definieren:

    AIX-Betriebssysteme

   ```
   define path server1 extlib srctype=server desttype=library
     externalmanager="/usr/lpp/dtelm/bin/elm"
   ```

    Linux-Betriebssysteme

   ```
   define path server1 extlib srctype=server desttype=library
     externalmanager="/opt/OMIdtelm/bin/elm"
   ```

    Windows-Betriebssysteme

```
define path server1 extlib srctype=server desttype=library
  externalmanager="c:\program files\GES\EDT\bin\elm.exe"
```

DEFINE LIBRARY (Kassettenarchiv FILE definieren)

Verwenden Sie diese Syntax, um ein Kassettenarchiv FILE zu definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine LIBRary--Speicherarchivname--LIBType--=--FILE--------->

   .-SHAREd--=--No------.
>--+--------------------+--------------------------------------><
   '-SHAREd--=--+-Yes-+-'
                '-No--'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=FILE (Erforderlich)
: Gibt an, dass ein Pseudokassettenarchiv für sequenzielle Dateidatenträger erstellt wird. Wird der Befehl DEFINE DEVCLASS mit den Parametern DEVTYPE=FILE und SHARED=YES ausgegeben, geschieht dies automatisch. Kassettenarchive des Typs FILE sind nur erforderlich, wenn sequenzielle Dateidatenträger von dem Server und einem oder mehreren Speicheragenten gemeinsam genutzt werden. Die Verwendung von Kassettenarchiven des Typs FILE erfordert die gemeinsame Nutzung von Kassettenarchiven. Gemeinsam genutzte Kassettenarchive des Typs FILE werden nur für die Verwendung in LAN-unabhängigen Sicherungskonfigurationen unterstützt. Sie können ein gemeinsam genutztes Kassettenarchiv des Typs FILE nicht in einer Umgebung verwenden, in der ein Kassettenarchivmanager für die Verwaltung von Kassettenarchivclients verwendet wird.

SHAREd
: Gibt an, ob dieses Kassettenarchiv mit anderen IBM Spectrum Protect-Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam genutzt wird. Dieser Parameter ist erforderlich, wenn Sie ein Kassettenarchiv für den Kassettenarchivmanager definieren.

  YES
  : Gibt an, dass dieses Kassettenarchiv mit anderen Servern gemeinsam genutzt werden kann. Wird YES angegeben, lädt der Kassettenarchivmanagerserver Datenträger, die von anderen Servern angefordert werden, und verfolgt die Laufwerk- und Datenträgerzuordnung zu anderen Servern.

  NO
  : Gibt an, dass dieses Kassettenarchiv nicht mit anderen Servern gemeinsam genutzt werden kann. SHARED=NO ist erforderlich, wenn das Kassettenarchiv durch die Übergabe von Befehlen über einen NAS-Dateiserver gesteuert wird.

Beispiel: Ein gemeinsam genutztes Kassettenarchiv FILE definieren

Ein Kassettenarchiv FILE mit shared=yes definieren.

```
define library file1 libtype=file shared=yes
```

DEFINE LIBRARY (Manuelles Kassettenarchiv definieren)

Verwenden Sie diese Syntax, um ein manuelles Kassettenarchiv zu definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine LIBRary--Kassettenarchivname--LIBType--=--MANUAL------>

   .-RESETDrives--=--Yes-----.
>--+-------------------------+--------------------------------->
   '-RESETDrives--=--+-Yes-+-'
                     '-No--'
```

```
   .-AUTOLabel--=--Yes-----------.
>--+---------------------------+----------------------------><
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'
```

Parameter

Speicherarchivname (Erforderlich)
Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=MANUAL (Erforderlich)
Gibt an, dass das Kassettenarchiv kein automatisiertes Kassettenarchiv ist. Müssen Datenträger in Laufwerke bei diesem Typ von Kassettenarchiv geladen werden, werden Nachrichten an Bediener gesendet. Dieser Kassettenarchivtyp wird bei eigenständigen Laufwerken verwendet.

AUTOLabel
Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No
Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes
Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE
Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

RESETDrives
Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

 AIX-Betriebssysteme  Windows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

 AIX-Betriebssysteme  Windows-Betriebssysteme

Yes
Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

 Linux-Betriebssysteme

Yes
Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

Beispiel: Ein manuelles Kassettenarchiv definieren

Ein Kassettenarchiv mit Namen MANUALMOUNT und Kassettenarchivtyp MANUAL soll definiert werden.

```
define library manualmount libtype=manual
```

DEFINE LIBRARY (SCSI-Kassettenarchiv definieren)

Verwenden Sie diese Syntax, um ein SCSI-Kassettenarchiv zu definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

Anmerkungen:

1. Der Standardwert des Parameters RESETDRIVES ist situationsabhängig. Wenn der Parameter SHARED auf NO gesetzt ist, ist NO der Wert des Parameters RESETDRIVES. Wenn der Parameter SHARED auf YES gesetzt ist, ist YES der Wert des Parameters RESETDRIVES.

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=SCSI (Erforderlich)
: Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet der Server die Datenträgerwechslereinheit.

SHAREd
: Gibt an, ob dieses Kassettenarchiv mit anderen Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam genutzt wird. Dieser Parameter ist erforderlich, wenn Sie ein Kassettenarchiv für den Kassettenarchivmanager definieren.

  YES
  : Gibt an, dass dieses Kassettenarchiv mit anderen Servern gemeinsam genutzt werden kann. Wird YES angegeben, lädt der Kassettenarchivmanagerserver Datenträger, die von anderen Servern angefordert werden, und verfolgt die Laufwerk- und Datenträgerzuordnung zu anderen Servern.

  NO
  : Gibt an, dass dieses Kassettenarchiv nicht mit anderen Servern gemeinsam genutzt werden kann. SHARED=NO ist erforderlich, wenn das Kassettenarchiv durch die Übergabe von Befehlen über einen NAS-Dateiserver gesteuert wird.

AUTOLabel
: Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

  Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

  Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu

kennzeichnen.

No
: Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes
: Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE
: Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

RELABELSCRatch
: Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden. Wird dieser Parameter auf YES gesetzt, wird eine Operation LABEL LIBVOLUME gestartet und der vorhandene Datenträgerkennsatz wird überschrieben. Dieser Parameter ist optional und für die Verwendung mit einem VTL-Speicherarchiv (VTL = Virtual Tape Library) bestimmt.

Haben Sie sowohl virtuelle als auch reale Datenträger in Ihrem VTL, werden beide Typen mit einem neuen Kennsatz versehen, wenn dieser Parameter aktiviert ist. Enthält das VTL reale Datenträger, kann die Angabe dieser Option Auswirkungen auf die Leistung haben.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

No
: Gibt an, dass der Server Datenträger nicht mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

Yes
: Gibt an, dass der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

RESETDrives
: Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

AIX-Betriebssysteme  Windows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

Konfiguration der Speicherarchiveinheit	**Verhalten für persistente Reserve**
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt.	Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.	Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben.
Die Speicherarchiveinheit wird an die NAS-Einheit angeschlossen und der Zugriff erfolgt indirekt durch NDMP (Network Data Management Protocol), und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.	Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben.

AIX-BetriebssystemeWindows-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

Linux-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

SERial
: Gibt die Seriennummer des Speicherarchivs an, das definiert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist AUTODETECT.

Wird SERIAL=AUTODETECT angegeben, wird bei der Definition des Pfads zu dem Speicherarchiv die vom Speicherarchiv gemeldete Seriennummer als Seriennummer verwendet.

Ist SERIAL=*Seriennummer*, wird die eingegebene Nummer mit der Nummer verglichen, die vom Server erkannt wurde.

Achtung: Je nach Leistungsspektrum der Einheit wird SERIAL=AUTODETECT möglicherweise nicht unterstützt. In diesem Fall wird die Seriennummer als leer gemeldet.

Beispiel: Ein SCSI-Kassettenarchiv definieren

Das Kassettenarchiv SCSILIB mit dem Kassettenarchivtyp SCSI definieren.

```
define library scsilib libtype=scsi
```

Das Kassettenarchiv erfordert einen Pfad. Der Einheitenname des Speicherarchivs ist:

- AIX-Betriebssysteme`/dev/lb0`
- Linux-Betriebssysteme`/dev/tsmscsi/lb0`
- Windows-Betriebssysteme`lb3.0.0.0`

Den Pfad definieren:

AIX-Betriebssysteme

```
define path server1 scsilib srctype=server desttype=library
   device=/dev/lb0
```

Linux-Betriebssysteme

```
define path server1 scsilib srctype=server desttype=library
   device=/dev/tsmscsi/lb0
```

Windows-Betriebssysteme

```
define path server1 scsilib srctype=server desttype=library
   device=lb3.0.0.0
```

DEFINE LIBRARY (Gemeinsam genutztes Kassettenarchiv definieren)

Verwenden Sie diese Syntax, um ein gemeinsam genutztes Kassettenarchiv zu definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine LIBRary--Speicherarchivname--LIBType--=--SHAREd------->
```

```
>--PRIMarylibmanager----=Servername----------------------------><
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=SHAREd (Erforderlich)
: Gibt an, dass das Kassettenarchiv mit einem anderen IBM Spectrum Protect-Server über ein Speicherbereichsnetz (Storage Area Network = SAN) oder eine duale SCSI-Verbindung zu Kassettenarchivlaufwerken gemeinsam benutzt wird.
: Wichtig: Geben Sie diesen Kassettenarchivtyp an, wenn das Kassettenarchiv auf einem Kassettenarchivclient definiert wird.

PRIMarylibmanager
: Gibt den Namen des IBM Spectrum Protect-Servers an, der für die Steuerung des Zugriffs auf Kassettenarchivressourcen zuständig ist. Sie müssen diesen Server mit dem Befehl DEFINE SERVER definieren, bevor Sie ihn als Kassettenarchivmanager verwenden können. Dieser Parameter ist nur bei LIBTYPE=SHARED erforderlich und gültig.

Beispiel: Ein gemeinsam genutztes Kassettenarchiv definieren

In einem Speicherbereichsnetz ein Kassettenarchiv mit dem Namen `SHAREDTSM` für einen Kassettenarchivclientserver mit dem Namen LIBMGR1 definieren.

```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

DEFINE LIBRARY (VTL-Speicherarchiv definieren)

Verwenden Sie diese Syntax, um ein Speicherarchiv zu definieren, das über einen SCSI-gesteuerten Datenträgerwechsler verfügt, der durch ein virtuelles Bandarchiv (Virtual Tape Library - VTL) dargestellt wird.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine LIBRary--Speicherarchivname--LIBType--=--VTL---------->

   .-SHAREd--=--No------.  .-RESETDrives--=--No----------.
>--+--------------------+--+---------------------------+------>
   '-SHAREd--=--+-Yes-+-'  |                           (1) |
                '-No--'    '-RESETDrives--=--+-Yes-+-----'
                                             '-No--'

   .-AUTOLabel--=--No------------.
>--+---------------------------+------------------------------>
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'

   .-RELABELSCRatch--=--Yes-----.
>--+--------------------------+-------------------------------->
   '-RELABELSCRatch--=--+-No--+-'
                        '-Yes-'

   .-SERial--=--AUTODetect-------.
>--+--------------------------+------------------------------><
   '-SERial--=--+-AUTODetect---+-'
                '-Seriennummer-'
```

Anmerkungen:

1. Der Standardwert des Parameters RESETDRIVES ist situationsabhängig. Wenn der Parameter SHARED auf NO gesetzt ist, ist NO der Wert des Parameters RESETDRIVES. Wenn der Parameter SHARED auf YES gesetzt ist, ist YES der Wert des Parameters RESETDRIVES.

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType=VTL (Erforderlich)
: Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt, der durch ein virtuelles Bandarchiv (Virtual Tape Library - VTL) dargestellt wird. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet der

Server die Datenträgerwechslereinheit.

Wenn Sie ein VTL-Speicherarchiv definieren, darf Ihre Umgebung keine gemischten Datenträger enthalten und es müssen Pfade zwischen allen Laufwerken in dem Speicherarchiv und allen definierten Servern, einschließlich Speicheragenten, die das Speicherarchiv verwenden, definiert sein. Wenn eine dieser Bedingungen nicht zutrifft, kann die Gesamtleistung in demselben Maße wie beim Kassettenarchivtyp SCSI abnehmen. Dies ist besonders in Zeiten hoher Belastung der Fall.

SHAREd
Gibt an, ob dieses Kassettenarchiv mit anderen Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam genutzt wird. Dieser Parameter ist erforderlich, wenn Sie ein Kassettenarchiv für den Kassettenarchivmanager definieren.

YES
Gibt an, dass dieses Kassettenarchiv mit anderen Servern gemeinsam genutzt werden kann. Wird YES angegeben, lädt der Kassettenarchivmanagerserver Datenträger, die von anderen Servern angefordert werden, und verfolgt die Laufwerk- und Datenträgerzuordnung zu anderen Servern.

NO
Gibt an, dass dieses Kassettenarchiv nicht mit anderen Servern gemeinsam genutzt werden kann. SHARED=NO ist erforderlich, wenn das Kassettenarchiv durch die Übergabe von Befehlen über einen NAS-Dateiserver gesteuert wird.

RESETDrives
Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird. Wenn beispielsweise ein Speicheragent nicht mehr verfügbar ist, aber noch den Pfad zu einem Laufwerk belegt, kann der Server mit der persistenten Reserve die Reservierung des Speicheragenten unterbrechen und auf das Laufwerk zugreifen.

 AIX-Betriebssysteme  Windows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

 AIX-Betriebssysteme  Windows-Betriebssysteme

Yes
Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

 Linux-Betriebssysteme

Yes
Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird. YES ist der Standardwert für ein Kassettenarchiv, das mit SHARED=YES definiert ist.

No
Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird. NO ist der Standardwert für ein Kassettenarchiv, das mit SHARED=NO definiert ist.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

AUTOLabel
Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

No
Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes

Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE
Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

RELABELSCRatch
Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden. Wird dieser Parameter auf YES gesetzt, wird eine Operation LABEL LIBVOLUME gestartet und der vorhandene Datenträgerkennsatz wird überschrieben.

Haben Sie sowohl virtuelle als auch reale Datenträger in Ihrem VTL, werden beide Typen mit einem neuen Kennsatz versehen, wenn dieser Parameter aktiviert ist. Enthält das VTL reale Datenträger, kann die Angabe dieser Option Auswirkungen auf die Leistung haben.

Einschränkung: Wenn Sie ein Kassettenarchiv definieren, das über Laufwerke verfügt, die an eine NAS-Einheit (NAS = Network-attached Storage) angeschlossen sind, müssen Sie den Befehl LABEL LIBVOLUME verwenden, um die Datenträger für dieses Kassettenarchiv zu kennzeichnen.

Yes
Gibt an, dass der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden. YES ist der Standardwert.

No
Gibt an, dass der Server Datenträger nicht mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

SERial
Gibt die Seriennummer des Speicherarchivs an, das definiert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist AUTODETECT.

Wird SERIAL=AUTODETECT angegeben, wird bei der Definition des Pfads zu dem Speicherarchiv die vom Speicherarchiv gemeldete Seriennummer als Seriennummer verwendet.

Ist SERIAL=*Seriennummer*, wird die eingegebene Nummer mit der Nummer verglichen, die vom Server erkannt wurde.

Achtung: Je nach Leistungsspektrum der Einheit wird SERIAL=AUTODETECT möglicherweise nicht unterstützt. In diesem Fall wird die Seriennummer als leer gemeldet.

Beispiel: Ein VTL-Speicherarchiv definieren

Ein Speicherarchiv mit dem Namen VTLLIB mit dem Speicherarchivtyp VTL definieren.

```
define library vtllib libtype=vtl
```

Das Kassettenarchiv erfordert einen Pfad. Der Einheitenname des Speicherarchivs ist:

-  AIX-Betriebssysteme`/dev/lb0`
-  Linux-Betriebssysteme`/dev/tsmscsi/lb0`
- Windows-Betriebssysteme`lb3.0.0.0`

Den Pfad definieren:
 AIX-Betriebssysteme

```
define path server1 vtllib srctype=server desttype=library
   device=/dev/lb0
```

 Linux-Betriebssysteme

```
define path server1 vtllib srctype=server desttype=library
   device=/dev/tsmscsi/lb0
```

 Windows-Betriebssysteme

```
define path server1 vtllib srctype=server desttype=library
   device=lb3.0.0.0
```

AIX-BetriebssystemeLinux-Betriebssysteme

DEFINE LIBRARY (Speicherarchivtyp ZOSMEDIA definieren)

Verwenden Sie diese Syntax, um ein Speicherarchiv zu definieren, das eine TAPE- oder FILE-Speicherressource darstellt, die von Tivoli Storage Manager for z/OS Media verwaltet wird.

Definieren Sie ein Speicherarchiv des Typs ZOSMEDIA, wenn das Speicherarchiv ausschließlich von Tivoli Storage Manager for z/OS Media verwaltet werden soll. Das Speicherarchiv wird dem IBM Spectrum Protect-Server als logische Speichereinheit angezeigt, für die keine

Laufwerkdefinitionen erforderlich sind. Eine Pfaddefinition ist für den Server und alle Speicheragenten erforderlich, die auf die ZOSMEDIA-Speicherarchivressource zugreifen müssen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine LIBRary--Speicherarchivname--LIBType--=--ZOSMEDIA----><
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Speicherarchivs an, das definiert werden soll.

LIBType=ZOSMEDIA (Erforderlich)
: Gibt an, dass der Speicherarchivtyp ZOSMEDIA lautet, der eine TAPE- oder FILE-Speicherressource darstellt, die von Tivoli Storage Manager for z/OS Media verwaltet wird.

Beispiel: ein ZOSMEDIA-Speicherarchiv konfigurieren

Das folgende Beispiel zeigt die Schritte, die zum Definieren und Konfigurieren eines zosmedia-Speicherarchivs erforderlich sind. Die Konfiguration umfasst diese Komponenten:

- Einen Server mit dem Namen sahara
- Ein Speicherarchiv mit dem Namen zebra, das mit dem Typ ZOSMEDIA definiert ist
- Einen z/OS Media-Server mit dem Namen oasis
- Einen Speicheragenten mit dem Namen mirage

Definieren Sie ein Speicherarchiv mit dem Namen ZEBRA mit dem Speicherarchivtyp ZOSMEDIA:

```
define library zebra libtype=zosmedia
```

Den z/OS Media-Server definieren:

```
define server oasis serverpassword=sanddune
hladdress=9.289.19.67 lladdress=1777
```

Der Server erfordert einen Pfad zu der Speicherarchivressource, die von Tivoli Storage Manager for z/OS Media verwaltet wird:

```
define path sahara zebra srctype=server
desttype=library zosmediaserver=oasis
```

Der Speicheragent erfordert einen Pfad zu der Speicherarchivressource, die von Tivoli Storage Manager for z/OS Media verwaltet wird:

```
define path mirage zebra srctype=server
desttype=library zosmediaserver=oasis
```

DEFINE MACHINE (Maschineninformationen für die Wiederherstellung nach einem Katastrophenfall definieren)

Mit diesem Befehl können Fehlerbehebungsinformationen für einen Server oder eine Client-Knoten-Maschine gesichert werden. Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Maschinen zu unterstützen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine MACHine--Maschinenname--------------------------------->

>--+-------------------------------+--+----------------------+--->
   '-DESCription--=--Beschreibung-'  '-BUilding--=--Gebäude-'

>--+---------------------+--+---------------+------------------->
   '-FLoor--=--Stockwerk-'  '-ROom--=--Raum-'
```

```
   .-PRIority--=--50-------.  .-ADSMServer--=--No------.
>--+-----------------------+--+-----------------------+-------><
   '-PRIority--=--Zahl---'  '-ADSMServer--=--+-No--+-'
                                              '-Yes-'
```

Parameter

Maschinenname (Erforderlich)
: Gibt den Maschinennamen an. Der Name kann bis zu 64 Zeichen umfassen.

DESCription
: Gibt eine Maschinenbeschreibung an. Dieser Parameter ist wahlfrei. Der Text kann bis zu 255 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

BUilding
: Gibt das Gebäude an, in dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

FLoor
: Gibt das Stockwerk an, auf dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

ROom
: Gibt den Raum an, in dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

PRIority
: Gibt die Zurückschreibungspriorität für die Maschine als ganze Zahl von 1 bis 99 an. Die höchste Priorität ist 1. Dieser Parameter ist wahlfrei. Der Standardwert ist 50.

ADSMServer
: Gibt an, ob die Maschine ein IBM Spectrum Protect-Server ist. Es kann nur eine Maschine als IBM Spectrum Protect-Server definiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Diese Maschine ist kein IBM Spectrum Protect-Server.

  Yes
  : Diese Maschine ist ein IBM Spectrum Protect-Server.

Beispiel: Informationen zur Wiederherstellung einer Maschine nach einem Katastrophenfall definieren

Die Maschine DISTRICT5 definieren und ein Gebäude, ein Stockwerk und einen Raum angeben. Diese Maschine enthält kritische Daten und hat die höchste Priorität.

```
define machine district5 building=101 floor=27
room=datafacilities priority=1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE MACHINE

Befehl	Beschreibung
DEFINE MACHNODEASSOCIATION	Ordnet einen IBM Spectrum Protect-Knoten einer Maschine zu.
DEFINE RECMEDMACHASSOCIATION	Ordnet Wiederherstellungsdatenträger einer Maschine zu.
DELETE MACHINE	Löscht eine Maschine.
INSERT MACHINE	Fügt Maschinenkenndaten oder Wiederherstellungsanweisungen in die IBM Spectrum Protect-Datenbank ein.
QUERY MACHINE	Zeigt Informationen über Maschinen an.
UPDATE MACHINE	Ändert die Informationen zu einer Maschine.

DEFINE MACHNODEASSOCIATION (Knoten einer Maschine zuordnen)

Mit diesem Befehl können Client-Knoten einer Maschine zugeordnet werden. Während der Fehlerbehebung können anhand dieser Informationen die Client-Knoten identifiziert werden, die sich auf den zerstörten Maschinen befunden haben.

Die Maschine muss in IBM Spectrum Protect definiert sein, und die Knoten müssen für IBM Spectrum Protect registriert sein.

Zum Abrufen der Informationen den Befehl QUERY MACHINE ausgeben. Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Clientmaschinen zu unterstützen.

Ein Knoten bleibt so lange einer Maschine zugeordnet, bis der Knoten, die Maschine oder die Zuordnung selbst gelöscht wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                                          .-,----------.
                                          V            |
>>-DEFine MACHNODEAssociation--Maschinenname----Knotenname-+--->< 
```

Parameter

Maschinenname (Erforderlich)
: Gibt den Maschinennamen an.

Knotenname (Erforderlich)
: Gibt die Knotennamen an. Ein Knoten kann nur einer Maschine zugeordnet sein. Sollen mehrere Knoten angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

Beispiel: Einer Maschine einen Knoten zuordnen

Den Knoten ACCOUNTSPAYABLE der Maschine DISTRICT5 zuordnen.

```
define machnodeassociation district5 accountspayable
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE MACHNODEASSOCIATION

Befehl	Beschreibung
DEFINE MACHINE	Definiert eine Maschine für DRM.
DELETE MACHINE	Löscht eine Maschine.
DELETE MACHNODEASSOCIATION	Löscht die Zuordnung zwischen einer Maschine und einem Knoten.
QUERY MACHINE	Zeigt Informationen über Maschinen an.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.

DEFINE MGMTCLASS (Verwaltungsklasse definieren)

Mit diesem Befehl kann eine neue Verwaltungsklasse in einer Maßnahmengruppe definiert werden. Um Clients die Verwendung der neuen Verwaltungsklasse zu ermöglichen, muß die Maßnahmengruppe aktiviert werden, die die neue Klasse enthält.

Es kann mindestens eine Verwaltungsklasse für jede Maßnahmengruppe in einer Maßnahmendomäne definiert werden. Eine Verwaltungsklasse kann eine Sicherungskopiengruppe und/oder eine Archivierungskopiengruppe enthalten. Der Benutzer eines Client-Knotens kann jede beliebige Verwaltungsklasse in der aktiven Maßnahmengruppe auswählen oder die Standardverwaltungsklasse verwenden.

Achtung: Der Befehl DEFINE MGMTCLASS schlägt fehl, wenn ein Kopienspeicherpool als Zielort für Dateien angegeben wird, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Verwaltungsklasse gehört.

Syntax

```
>>-DEFine MGmtclass--Domänenname--Name_der_Maßnahmengruppe--Klassenname-->

   .-SPACEMGTECHnique--=--NONE----------.
>--+-----------------------------------+---------------------->
   '-SPACEMGTECHnique--=--+-AUTOmatic-+-'
                          +-SELective-+
                          '-NONE------'
```

```
   .-AUTOMIGNOnuse--=--0----.
>--+------------------------+----------------------------------->
   '-AUTOMIGNOnuse--=--Tage-'

   .-MIGREQUIRESBkup--=--Yes-----.
>--+-----------------------------+----------------------------->
   '-MIGREQUIRESBkup--=--+-Yes-+-'
                         '-No--'

   .-MIGDESTination--=--SPACEMGPOOL-.
>--+--------------------------------+--------------------------->
   '-MIGDESTination--=--Poolname----'

>--+-------------------------------+---------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Verwaltungsklasse gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, zu der die Verwaltungsklasse gehört. Für die aktive Maßnahmengruppe (ACTIVE) kann keine Verwaltungsklasse definiert werden.

Klassenname (Erforderlich)
: Gibt den Namen der neuen Verwaltungsklasse an. Die maximale Länge dieses Namens beträgt 30 Zeichen. Als Klassenname kann weder *default* noch *grace_period* verwendet werden.

SPACEMGTECHnique
: Gibt an, ob eine Datei, die diese Verwaltungsklasse verwendet, für die Umlagerung ausgewählt werden kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE. Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungsclients. Gültige Werte:

  AUTOmatic
  : Gibt an, dass die Datei sowohl für die automatische Umlagerung als auch für die selektive Umlagerung auswählbar ist.

  SELective
  : Gibt an, dass die Datei nur für die selektive Umlagerung auswählbar ist.

  NONE
  : Gibt an, dass die Datei nicht für die Umlagerung auswählbar ist.

AUTOMIGNOnuse
: Gibt die Anzahl Tage an, die nach dem letzten Zugriff auf eine Datei verstreichen müssen, bevor die Datei für die automatische Umlagerung ausgewählt werden kann. Dieser Parameter ist wahlfrei. Der Standardwert ist 0. Lautet der Wert für SPACEMGTECHNIQUE nicht AUTOMATIC, ignoriert der Server dieses Attribut. Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben.

  Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungsclients.

MIGREQUIRESBkup
: Gibt an, ob eine Sicherungsversion einer Datei vorhanden sein muß, damit die Datei umgelagert werden kann. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungsclients. Gültige Werte:

  Yes
  : Gibt an, dass eine Sicherungsversion vorhanden sein muss.

  No
  : Gibt an, dass eine Sicherungsversion wahlfrei ist.

MIGDESTination
: Gibt den primären Speicherpool an, in dem der Server anfänglich Dateien speichert, die von IBM Spectrum Protect for Space Management-Clients umgelagert werden. Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig; er ist nicht für Clients für Sichern/Archivieren oder Anwendungsclients gültig. Der Standardwert ist SPACEMGPOOL.
  Ihre Auswahl für das Ziel kann von Faktoren abhängen, wie z. B.:

  - Anzahl Clientknoten, die in den Speicherpool umgelagert werden. Wenn viele Benutzerdateien in demselben Speicherpool gespeichert werden, können Datenträgerkonflikte auftreten, wenn Benutzer versuchen, Dateien in den Speicherpool umzulagern oder Dateien aus dem Speicherpool zurückzurufen.
  - Wie schnell die Dateien zurückgerufen werden müssen. Wenn Sie unmittelbaren Zugriff auf umgelagerte Versionen benötigen, können Sie einen Plattenspeicherpool als Ziel angeben.

  Der Befehl schlägt fehl, wenn Sie einen Kopienspeicherpool oder einen Pool für aktive Daten als Ziel angeben.

DESCription

Beschreibung der Verwaltungsklasse. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

Beispiel: Eine Verwaltungsklasse für eine bestimmte Maßnahmengruppe und Maßnahmendomäne definieren

Eine Verwaltungsklasse mit dem Namen MCLASS1 für Maßnahmengruppe SUMMER in der Maßnahmendomäne PROG1 definieren. Für IBM Spectrum Protect for Space Management-Clients sowohl die automatische Umlagerung als auch die selektive Umlagerung erlauben, und umgelagerte Dateien in dem Speicherpool SMPOOL speichern. Die Beschreibung "Technical Support Mgmt Class" hinzufügen.

```
define mgmtclass prog1 summer mclass1
spacemgtechnique=automatic migdestination=smpool
description="technical support mgmt class"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE MGMTCLASS

Befehl	Beschreibung
ASSIGN DEFMGMTCLASS	Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu.
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
DELETE MGMTCLASS	Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.
UPDATE MGMTCLASS	Ändert die Attribute einer Verwaltungsklasse.

DEFINE NODEGROUP (Knotengruppe definieren)

Verwenden Sie diesen Befehl, um eine Knotengruppe zu definieren. Eine *Knotengruppe* ist eine Gruppe von Clientknoten, die wie eine einzelne Entität bearbeitet werden. Ein Knoten kann ein Mitglied einer oder mehrerer Knotengruppen sein.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

Syntax

```
>>-DEFine NODEGroup--Gruppenname--------------------------------->

>--+-------------------------------+---------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Gruppenname
: Gibt den Namen der Knotengruppe an, die erstellt werden soll. Die maximale Länge des Namens beträgt 64 Zeichen.Der angegebene Name darf nicht mit dem Namen eines vorhandenen Clientknotens übereinstimmen.

DESCription
: Gibt eine Beschreibung der Knotengruppe an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

Beispiel: Eine Knotengruppe definieren

Die Knotengruppe `group1` definieren.

```
define nodegroup group1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE NODEGROUP

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUP	Löscht eine Knotengruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

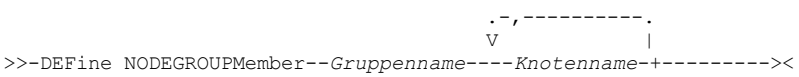
DEFINE NODEGROUPMEMBER (Eintrag in der Knotengruppe definieren)

Verwenden Sie diesen Befehl, um einer Knotengruppe einen Clientknoten hinzuzufügen. Eine *Knotengruppe* ist eine Gruppe von Clientknoten, die wie eine einzelne Entität bearbeitet werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

Syntax



Parameter

Gruppenname
: Gibt den Namen der Knotengruppe an, der ein Clientknoten hinzugefügt werden soll.

Knotenname
: Gibt den Namen des Clientknotens an, der der Knotengruppe hinzugefügt werden soll. Sie können einen oder mehrere Namen angeben. Mehrere Namen sind durch Kommas voneinander zu trennen; verwenden Sie keine Leerzeichen zwischen den Namen. Sie können auch Platzhalterzeichen verwenden, wenn mehrere Namen angegeben werden.

Beispiel: Knoten einer Knotengruppe definieren

Die beiden Knoten `node1` und `node2` für die Knotengruppe `group1` definieren.

```
define nodegroupmember group1 node1,node2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE NODEGROUPMEMBER

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUP	Löscht eine Knotengruppe.

Befehl	Beschreibung
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

DEFINE PATH (Pfad definieren)

Verwenden Sie diesen Befehl, um einen Pfad für eine Quelle für den Zugriff auf ein Ziel zu definieren. Die Quelle und das Ziel müssen definiert werden, bevor Sie einen Pfad definieren können. Ist beispielsweise ein Pfad zwischen einem Server und einem Laufwerk erforderlich, müssen Sie zuerst den Befehl DEFINE DRIVE und dann den Befehl DEFINE PATH ausgeben. Ein Pfad muss definiert werden, nachdem Sie den Befehl DEFINE DRIVE ausgegeben haben, damit der Server das Laufwerk verwenden kann.

Syntax- und Parameterbeschreibungen sind für die folgenden Pfadtypen verfügbar.

- DEFINE PATH (Pfad definieren, wenn das Ziel ein Laufwerk ist)
- DEFINE PATH (Pfad definieren, wenn das Ziel ein Kassettenarchiv ist)
- AIX-BetriebssystemeLinux-BetriebssystemeDEFINE PATH (Pfad definieren, wenn das Ziel ein ZOSMEDIA-Kassettenarchiv ist)

Ausführliche und aktuelle Informationen zur Einheitenunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE PATH

Befehl	Beschreibung
DEFINE DATAMOVER	Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
PERFORM LIBACTION	Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE DATAMOVER	Ändert die Definition einer Einheit zum Versetzen von Daten.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.

DEFINE PATH (Pfad definieren, wenn das Ziel ein Laufwerk ist)

Verwenden Sie diese Syntax, wenn Sie einen Pfad zu einem Laufwerk definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine PATH--Quellenname--Zielname--------------------------->

>--SRCType--=--+-DATAMover-+--+-----------------------+-------->
               '-SERVer----'  '-AUTODetect--=--+-No--+-'
                                               '-Yes-'

>--DESTType--=--DRive--LIBRary--=--Kassettenarchivname---------->
```

```
>----DEVIce--=--+-Einheitenname-+------------------------------>
                '-FILE----------'

   .-GENERICTAPE--=--No------.  .-ONLine--=--Yes-----.
>--+-------------------------+--+--------------------+---------->
   '-GENERICTAPE--=--+-Yes-+-'  '-ONLine--=--+-Yes-+-'
                     '-No--'                 '-No--'

   .-DIRectory--=--Name_des_aktuellen_Verzeichnisses-.
>--+-------------------------------------------------+--------><
   |               .-,---------------.               |
   |               V                 |               |
   '-DIRectory--=----Verzeichnisname-+---------------'
```

Parameter

Quellenname (Erforderlich)
: Gibt den Namen der Quelle des Pfads an. Dieser Parameter ist erforderlich.

Zielname (Erforderlich)
: Gibt den Namen des Ziels an. Dieser Parameter ist erforderlich.

SRCType (Erforderlich)
: Gibt den Typ der Quelle an. Dieser Parameter ist erforderlich. Gültige Werte:

  DATAMover
  : Gibt an, dass eine Einheit zum Versetzen von Daten die Quelle ist.

  SERVer
  : Gibt an, dass ein Speicheragent die Quelle ist.

AUTODetect
: Gibt an, ob die Seriennummer für ein Laufwerk automatisch zu dem Zeitpunkt in der Datenbank aktualisiert wird, zu dem der Pfad definiert wird. Dieser Parameter ist wahlfrei. Dieser Parameter ist nur für Pfade gültig, die von dem lokalen Server zu einem Laufwerk definiert sind. Gültige Werte:

  No
  : Gibt an, dass die Seriennummer nicht automatisch aktualisiert wird. Die Seriennummer wird dennoch mit der Angabe verglichen, die bereits für die Einheit in der Datenbank vorhanden ist. Der Server gibt eine Nachricht aus, wenn keine Übereinstimmung gefunden wird.

  Yes
  : Gibt an, dass die Seriennummer automatisch aktualisiert wird, um dieselbe Seriennummer widerzuspiegeln, die das Laufwerk an den Server meldet.
    Wichtig:

    1. Wurde die Seriennummer bei der Definition des Laufwerks nicht definiert, versucht der Server immer, die Seriennummer zu ermitteln, und AUTODETECT nimmt standardmäßig den Wert YES an. Wurde zuvor eine Seriennummer eingegeben, erhält AUTODETECT den Standardwert NO.
    2. Die Verwendung von AUTODETECT=YES in diesem Befehl bedeutet, dass die in der Laufwerkdefinition angegebene Seriennummer mit der ermittelten Seriennummer aktualisiert wird.
    3. Wenn Sie DESTTYPE=DRIVE und AUTODETECT=YES definieren, wird die Elementnummer des Laufwerks in der Datenbank automatisch geändert, um dieselbe Elementnummer widerzuspiegeln, die der Seriennummer dieses Laufwerks entspricht. Dies gilt für Laufwerke in einem SCSI-Kassettenarchiv. Weitere Informationen zu der Elementnummer befinden sich in der Beschreibung des Befehls DEFINE DRIVE.
    4. Abhängig vom Leistungsspektrum der Einheit wird der Parameter AUTODETECT möglicherweise nicht unterstützt.

DESTType=DRive (Erforderlich)
: Gibt an, dass ein Laufwerk das Ziel ist. Ist das Ziel ein Laufwerk, müssen Sie einen Kassettenarchivnamen angeben.

LIBRary
: Gibt den Namen des Kassettenarchivs an, dem das Laufwerk zugeordnet ist. Das Kassettenarchiv und seine Laufwerke müssen bereits für den Server definiert sein. Verläuft der Pfad von einer NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv, muss das Kassettenarchiv den Typ (LIBTYPE) SCSI, 349X oder ACSLS haben.

DEVIce
: Gibt den Namen der Einheit an, die der Quelle bekannt ist, oder FILE an, wenn die Einheit ein logisches Laufwerk in einem Kassettenarchiv FILE ist.
  AIX-BetriebssystemeWindows-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk. Für Beispiele siehe Tabelle 1.

Tabelle 1. Beispiele für Einheitennamen

Quelle zum Ziel	Beispiel

Quelle zum Ziel	Beispiel

Server zu einem Laufwerk (kein FILE-Laufwerk)	AIX-Betriebssysteme
	`/dev/mt3`
	Windows-Betriebssysteme
	`mt3`

Speicheragent (auf einem Windows-System) zu einem Laufwerk (kein FILE-Laufwerk)	`mt3`
Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist	`FILE`
NAS-Einheit zum Versetzen von Daten zu einem Laufwerk	NetApp NAS-Dateiserver: `rst01` EMC Celerra NAS-Dateiserver: `c436t0l1` IBM® System Storage N Series: `rst01`

Linux-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk. Für Beispiele siehe Tabelle 2.

Tabelle 2. Beispiele für Einheitennamen

Quelle zum Ziel	Beispiel
Server zu einem Laufwerk (kein FILE-Laufwerk)	`/dev/tsmscsi/mt3`
Speicheragent zu einem Laufwerk (kein FILE-Laufwerk)	`/dev/tsmscsi/mt3`
Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist	`FILE`
NAS-Einheit zum Versetzen von Daten zu einem Laufwerk	NetApp NAS-Dateiserver: `rst01` EMC Celerra NAS-Dateiserver: `c436t0l1` IBM System Storage N Series: `rst01`

Wichtig:

- AIX-BetriebssystemeLinux-BetriebssystemeFür 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei /etc/ibmatl.conf angegeben ist. Windows-Betriebssysteme Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei c:\winnt\ibmatl.conf angegeben ist. Weitere Informationen enthält das Handbuch *IBM Tape Device Drivers Installation and User's Guide*, das von der Site der IBM Systemunterstützung unter http://www.ibm.com/support/docview.wss?uid=ssg1S7002972 heruntergeladen werden kann.
- Informationen über Namen für Einheiten, die mit einem NAS-Dateiserver verbunden sind, enthält die Produktinformation für den Dateiserver. Beispiel: Stellen Sie für einen NetApp-Dateiserver unter Verwendung von Telnet eine Verbindung zu dem Dateiserver her und geben Sie den Befehl SYSCONFIG aus. Verwenden Sie diesen Befehl, um Einheitennamen für Laufwerke zu bestimmen:

  ```
  sysconfig -t
  ```

Windows-BetriebssystemeGENERICTAPE

Windows-BetriebssystemeGibt an, ob das Bandlaufwerk, das verwendet werden soll, den Einheitenklassentyp GENERICTAPE hat. Ist die Einheit ein Bandlaufwerk und wird sie nicht von IBM Spectrum Protect, aber für das Windows-Betriebssystem unterstützt, können Sie sie mit dem generischen Bandformat verwenden. Um das Laufwerk zu verwenden, geben Sie GENERICTAPE=Yes an, wenn Sie einen Pfad zu dem Laufwerk definieren. Der Standardwert ist 'No'. Gültige Werte sind:

Yes
: Gibt an, dass das Bandlaufwerk, das verwendet werden soll, den Einheitenklassentyp GENERICTAPE hat.

No
: Gibt an, dass das Bandlaufwerk, das verwendet werden soll, nicht den Einheitenklassentyp GENERICTAPE hat.

ONLine

Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

Yes
: Gibt an, dass der Pfad für die Verwendung verfügbar ist.

No
: Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.

Ist beispielsweise der Pfad von einer Einheit zum Versetzen von Daten zu einem Laufwerk online, aber ist entweder die Einheit zum Versetzen von Daten oder das Laufwerk offline, kann der Pfad nicht verwendet werden.

DIRectory

Gibt die Verzeichnisposition(en) an, an der/denen der Speicheragent die Dateien liest und schreibt, die Speicherdatenträger für die Einheitenklasse FILE darstellen, die dem FILE-Kassettenarchiv zugeordnet ist. Der Parameter DIRECTORY wird auch für Einheiten des Typs REMOVABLEFILE verwendet. Für Einheiten des Typs REMOVABLEFILE stellt der Parameter DIRECTORY in Verbindung mit dem Parameter DRIVE dem Server (kein Speicheragent) Informationen zur Verfügung, die den Zugriff auf die Einheit beschreiben. Dieser Parameter ist wahlfrei.
Für einen Pfad von einem Speicheragenten zu einer FILE-Einheit ist dieser Parameter nur gültig, wenn *alle* folgenden Bedingungen zutreffen:

- Der Quellentyp ist SERVER (d. h., ein Speicheragent, der für diesen Server als Server definiert wurde).
- Der Quellenname ist der Name eines Speicheragenten, *nicht* der Servername.
- Das Ziel ist ein logisches Laufwerk, das Teil eines FILE-Kassettenarchivs ist, das bei der Definition der Einheitenklasse erstellt wurde.

Haben Sie mehrere Verzeichnisse für die Einheitenklasse angegeben, die dem FILE-Kassettenarchiv zugeordnet ist, müssen Sie dieselbe Anzahl Verzeichnisse für jeden Pfad zum FILE-Kassettenarchiv angeben. Sie dürfen keine vorhandenen Verzeichnisse auf dem Server, den der Speicheragent verwendet, ändern oder versetzen, damit die Einheitenklasse und der Pfad synchronisiert bleiben. Das Hinzufügen von Verzeichnissen ist zulässig. Wird eine abweichende Anzahl Verzeichnisse angegeben, kann dies einen Laufzeitfehler verursachen.

Der Standardwert für DIRECTORY ist das Verzeichnis des Servers zum Zeitpunkt der Befehlsausgabe. Die Windows-Registrierungsdatenbank wird zum Lokalisieren des Standardwerts verwendet.

Verwenden Sie eine Namenskonvention, mit der Sie das Verzeichnis einem bestimmten physischen Laufwerk zuordnen können. Damit kann sichergestellt werden, dass Ihre Konfiguration für die gemeinsame Benutzung des FILE-Kassettenarchivs zwischen dem Server und dem Speicheragenten gültig ist. Befindet sich der Speicheragent auf einem Windows-System, verwenden Sie eine allgemeine Namenskonvention. Verfügt der Speicheragent nicht über die Berechtigung für den Zugriff auf fernen Speicher, treten Ladefehler im Speicheragenten auf.

 Windows-BetriebssystemeDas dem Speicheragentendienst zugeordnete Konto muss ein Konto in der Gruppe der lokalen Administratoren oder ein Konto in der Gruppe der Domänenadministratoren sein. Befindet sich das Konto in der Gruppe der lokalen Administratoren, müssen Benutzer-ID und Kennwort den Angaben eines Kontos entsprechen, das über Berechtigungen für den Zugriff auf Speicher verfügt, der von dem System bereitgestellt wird, das den fernen Sharepunkt verwaltet. Wenn beispielsweise ein SAMBA-Server Zugriff auf fernen Speicher bereitstellt, müssen Benutzer-ID und Kennwort in der SAMBA-Konfiguration der Benutzer-ID und dem Kennwort des lokalen Administrators entsprechen, der dem Speicheragentendienst zugeordnet ist.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
define path sta1 file1 srctype=server desttype=drive
library=file1 device=file
directory=\\192.168.1.10\filedir\dir1
```

In dem vorherigen Beispiel erstellt der Befehl DEFINE DEVCLASS das gemeinsam genutzte Dateisystem in dem Verzeichnis, auf das der Server als D:\FILEDIR\DIR1 zugreift. Der Speicheragent verwendet jedoch den UNC-Namen \\192.168.1.10\FILEDIR\DIR1. Das bedeutet, dass das System mit TCP/IP-Adresse 192.168.1.10 dasselbe Verzeichnis gemeinsam nutzt, wobei FILEDIR als gemeinsam genutzter Name verwendet wird. Außerdem verfügt der Speicheragentendienst über ein Konto, das auf diesen Speicher zugreifen kann. Der Zugriff ist möglich, weil das Konto einem lokalen Konto mit derselben Benutzer-ID und demselben Kennwort wie 192.168.1.10 zugeordnet ist oder weil es einem Domänenkonto zugeordnet ist, das sowohl auf dem Speicheragenten als auch auf 192.168.1.10 verfügbar ist. Sie können gegebenenfalls 192.168.1.10 durch einen symbolischen Namen wie folgt ersetzen:

```
Beispiel.IhreFirma.com
```

Achtung:

1. Speicheragenten greifen auf FILE-Datenträger zu, indem ein Verzeichnisname in einem Datenträgernamen durch einen Verzeichnisnamen eines Verzeichnisses in der Liste ersetzt wird, die mit dem Befehl DEFINE PATH zur Verfügung gestellt wird. Mit diesem Parameter angegebene Verzeichnisse werden auf dem Server nicht geprüft.
2. IBM Spectrum Protect erstellt keine Shares oder Berechtigungen und lädt nicht das Zieldateisystem. Sie müssen diese Aktionen ausführen, bevor Sie den Speicheragenten starten.

Beispiel: Einen Pfad von einem Server zu einem Laufwerk definieren

Einen Pfad von einem Server zu einem Laufwerk definieren. In diesem Fall lautet der Servername *NET1*, der Laufwerkname *TAPEDRV6*, der Kassettenarchivname *NETLIB* und der Einheitenname *mt4*. Geben Sie für AUTODETECT NO an.

```
define path net1 tapedrv6 srctype=server autodetect=no desttype=drive
    library=netlib device=mt4
```

Beispiel: Einen Pfad von einer Einheit zum Versetzen von Daten zu einem Laufwerk für die Sicherung und Zurückschreibung definieren

Einen Pfad von der Einheit zum Versetzen von Daten, die ein NAS-Dateiserver ist, zu dem Laufwerk definieren, das von dem NAS-Dateiserver für Sicherungs- und Zurückschreibungsoperationen verwendet wird. In diesem Beispiel hat die NAS-Einheit zum Versetzen von Daten den Namen

NAS1, der Laufwerkname lautet *TAPEDRV3*, das Kassettenarchiv ist NASLIB und der Einheitenname für das Laufwerk lautet *rst0l*.

```
define path nas1 tapedrv3 srctype=datamover desttype=drive library=naslib
    device=rst0l
```

Linux-Betriebssysteme

Beispiel: Einen Pfad von einem Speicheragenten zu einem Laufwerk für die Sicherung und Zurückschreibung definieren

Einen Pfad von dem Speicheragenten *SA1* zu dem Laufwerk definieren, das vom Speicheragenten für Sicherungs- und Zurückschreibungsoperationen verwendet wird. In diesem Beispiel lautet das Kassettenarchiv *TSMLIB*, das Laufwerk ist *TAPEDRV4* und der Einheitenname für das Laufwerk ist /dev/tsmscsi/mt3.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
    device=/dev/tsmscsi/mt3
```

AIX-BetriebssystemeWindows-Betriebssysteme

Beispiel: Einen Pfad von einem Speicheragenten zu einem Laufwerk für die Sicherung und Zurückschreibung definieren

Einen Pfad von dem Speicheragenten *SA1* zu dem Laufwerk definieren, das vom Speicheragenten für Sicherungs- und Zurückschreibungsoperationen verwendet wird. In diesem Beispiel lautet das Kassettenarchiv *TSMLIB*, das Laufwerk ist *TAPEDRV4* und der Einheitenname für das Laufwerk ist /dev/mt3.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
    device=/dev/mt3
```

AIX-BetriebssystemeWindows-Betriebssysteme

Beispiel: Einen Pfad definieren, um einem Speicheragenten den Zugriff auf den gemeinsam genutzten Plattenspeicher zu ermöglichen

Einen Pfad definieren, der es dem Speicheragenten ermöglicht, auf Dateien in einem Plattenspeicher zuzugreifen, der mit dem Server gemeinsam genutzt wird. Laufwerk *FILE9* ist für Kassettenarchiv *FILE1* auf dem Server definiert. Der Speicheragent *SA1* greift auf *FILE9* zu. Auf dem Speicheragenten befinden sich diese Daten im Verzeichnis \\192.168.1.10\filedata.

AIX-BetriebssystemeDie Daten für *FILE9* befinden sich auf dem Server unter /tsmdata/filedata.

Windows-BetriebssystemeDie Daten für *FILE9* befinden sich auf dem Server unter d:\tsmdata\filedata.

```
define path sa1 file9 srctype=server desttype=drive library=file1 device=file
    directory="\\192.168.1.10\filedata"
```

Beispiel: Einen Speicheragenten für die Verwendung eines FILE-Kassettenarchivs konfigurieren

Das folgende Beispiel verdeutlicht die Bedeutung übereinstimmender Einheitenklassen und Pfade, um sicherzustellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können.

Beispiel: Sie möchten folgende drei Verzeichnisse für ein FILE-Kassettenarchiv verwenden: Windows-Betriebssysteme

- c:\server
- d:\server
- e:\server

AIX-BetriebssystemeLinux-Betriebssysteme

- /opt/tivoli1
- /opt/tivoli2
- /opt/tivoli3

1. Verwenden Sie den folgenden Befehl, um ein FILE-Kassettenarchiv mit dem Namen CLASSA mit einem Laufwerk mit dem Namen CLASSA1 auf SERVER1 zu definieren: Windows-Betriebssysteme

   ```
   define devclass classa devtype=file
   directory="c:\server,d:\server,e:\server"
   shared=yes mountlimit=1
   ```

   AIX-BetriebssystemeLinux-Betriebssysteme

   ```
   define devclass classa devtype=file
   directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
   shared=yes mountlimit=1
   ```

2. Sie wollen, dass der Speicheragent STA1 das FILE-Kassettenarchiv verwenden kann. Daher definieren Sie folgenden Pfad für Speicheragent STA1: Windows-Betriebssysteme

   ```
   define path sta1 classa1 srctype=server desttype=drive device=file
   directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
   \\192.168.1.10\e\server" library=classa
   ```

   AIX-BetriebssystemeLinux-Betriebssysteme

   ```
   define path sta1 classa1 srctype=server desttype=drive device=file
   directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
   ```

   Windows-BetriebssystemeIn diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen c:\server durch den Verzeichnisnamen \\192.168.1.10\c\server, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis c:\server auf dem Server befinden.

   AIX-BetriebssystemeLinux-BetriebssystemeIn diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen /opt/tivoli1 durch den Verzeichnisnamen /opt/ibm1/, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis /opt/tivoli1 auf dem Server befinden.

3. Windows-BetriebssystemeFILE-Datenträger c:\server\file1.dsm wird durch SERVER1 erstellt. Wenn Sie das erste Verzeichnis für die Einheitenklassen später mit folgendem Befehl ändern:

   ```
   update devclass classa directory="c:\otherdir,d:\server,e:\server"
   ```

   kann SERVER1 weiterhin auf FILE-Datenträger c:\server\file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.
4. Wird der FILE-Datenträger /opt/tivoli1/file1.dsm auf SERVER1 erstellt und wird der Befehl

   ```
   update devclass classa directory="/opt/otherdir,/opt/tivoli2,
   /opt/tivoli3"
   ```

   ausgegeben, kann SERVER1 weiterhin auf FILE-Datenträger /opt/tivoli1/file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

DEFINE PATH (Pfad definieren, wenn das Ziel ein Kassettenarchiv ist)

Verwenden Sie diese Syntax, wenn Sie einen Pfad zu einem Kassettenarchiv definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine PATH--Quellenname--Zielname---------------------------->

                          (1)
>--SRCType--=--+-DATAMover-----+--+------------------------+---->
               '-SERVer--------'  '-AUTODetect--=--+-No--+-'
                                                   '-Yes-'

>--DESTType--=--LIBRary--+-DEVIce--=--Einheitenname-----+------->
                         '-EXTERNALManager--=--Pfadname-'

   .-ONLine--=--Yes-----.
>--+--------------------+-------------------------------------><
   '-ONLine--=--+-Yes-+-'
                '-No--'
```

Anmerkungen:

1. DATAMOVER gilt nur für NAS-Einheiten.

Parameter

Quellenname (Erforderlich)

Gibt den Namen der Quelle des Pfads an. Dieser Parameter ist erforderlich.

Zielname (Erforderlich)

Gibt den Namen des Ziels an. Dieser Parameter ist erforderlich.

Achtung: Um einen Pfad von einer NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv zu definieren, muss das Kassettenarchiv den Typ (LIBTYPE) SCSI, 349x oder ACSLS haben.

SRCType (Erforderlich)

Gibt den Typ der Quelle an. Dieser Parameter ist erforderlich. Gültige Werte:

DATAMover
: Gibt an, dass eine Einheit zum Versetzen von Daten die Quelle ist.

SERVer
: Gibt an, dass ein Speicheragent die Quelle ist.

AUTODetect

Gibt an, ob die Seriennummer für ein Laufwerk oder Kassettenarchiv automatisch zu dem Zeitpunkt in der Datenbank aktualisiert wird, zu dem der Pfad definiert wird. Dieser Parameter ist wahlfrei. Dieser Parameter ist nur für Pfade gültig, die von dem lokalen Server zu einem Laufwerk oder Kassettenarchiv definiert sind. Gültige Werte:

No
: Gibt an, dass die Seriennummer nicht automatisch aktualisiert wird. Die Seriennummer wird dennoch mit der Angabe verglichen, die bereits für die Einheit in der Datenbank vorhanden ist. Der Server gibt eine Nachricht aus, wenn keine Übereinstimmung gefunden wird.

Yes
: Gibt an, dass die Seriennummer automatisch aktualisiert wird, um dieselbe Seriennummer widerzuspiegeln, die das Laufwerk an IBM Spectrum Protect meldet.
Wichtig:

1. Wurde die Seriennummer bei der Definition des Laufwerks oder des Kassettenarchivs nicht definiert, versucht der Server immer, die Seriennummer zu ermitteln, und AUTODETECT nimmt standardmäßig den Wert YES an. Wurde zuvor eine Seriennummer eingegeben, erhält AUTODETECT den Standardwert NO.
2. Die Verwendung von AUTODETECT=YES in diesem Befehl bedeutet, dass die in der Laufwerk- oder Kassettenarchivdefinition angegebene Seriennummer mit der ermittelten Seriennummer aktualisiert wird.
3. Je nach Leistungsspektrum der Einheit wird der Parameter AUTODETECT möglicherweise nicht unterstützt.

DESTType=LIBRary (Erforderlich)

Gibt an, dass ein Kassettenarchiv das Ziel ist. Dieser Parameter ist erforderlich.

DEVIce

Gibt den Namen der Einheit an, die der Quelle bekannt ist, oder FILE an, wenn die Einheit ein logisches Laufwerk in einem Kassettenarchiv FILE ist.

AIX-BetriebssystemeWindows-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Kassettenarchiv. Für Beispiele siehe Tabelle 1.

Tabelle 1. Beispiele für Einheitennamen

Quelle zum Ziel	**Beispiel**

Server zu einem Kassettenarchiv	AIX-Betriebssysteme
	`/dev/lb4`
	Linux-Betriebssysteme
	`/dev/tsmscsi/lb4`
	Windows-Betriebssysteme
	`lb4.1`

Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist	`FILE`
NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv	`mc0`

Linux-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Kassettenarchiv. Für Beispiele siehe Tabelle 2.

Tabelle 2. Beispiele für Einheitennamen

Quelle zum Ziel	**Beispiel**
Server zu einem Kassettenarchiv	`/dev/tsmscsi/lb4`
NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv	`mc0`

Wichtig:

- AIX-BetriebssystemeLinux-BetriebssystemeFür 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei /etc/ibmatl.conf angegeben ist.Windows-Betriebssysteme Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei c:\winnt\ibmatl.conf angegeben ist. Weitere Informationen enthält das Handbuch *IBM Tape Device Drivers*

Installation and User's Guide, das von der Site der IBM® Systemunterstützung unter http://www.ibm.com/support/docview.wss?uid=ssg1S7002972 heruntergeladen werden kann.

- Informationen über Namen für Einheiten, die mit einem NAS-Dateiserver verbunden sind, enthält die Produktinformation für den Dateiserver. Beispiel: Stellen Sie für einen NetApp-Dateiserver unter Verwendung von Telnet eine Verbindung zu dem Dateiserver her und geben Sie den Befehl SYSCONFIG aus. Verwenden Sie diesen Befehl, um Einheitennamen für Laufwerke zu bestimmen:

  ```
  sysconfig -t
  ```

  Verwenden Sie diesen Befehl, um den Einheitennamen für ein Kassettenarchiv zu bestimmen:

  ```
  sysconfig -m
  ```

EXTERNALManager
: Gibt den Standort des externen Kassettenarchivmanagers an, an den IBM Spectrum Protect Zugriffsanforderungen für Datenträger senden kann. Der Wert dieses Parameters muss zwischen einfachen Anführungszeichen stehen. Geben Sie beispielsweise Folgendes ein:
AIX-Betriebssysteme

  ```
  /usr/lpp/GESedt-acsls/bin/elmdt
  ```

 Linux-Betriebssysteme

  ```
  /opt/GESedt-acsls/bin/elmdt
  ```

 Windows-Betriebssysteme

  ```
  C:\Programme\GES\EDT-ACSLS\bin\elmdt.exe
  ```

  Dieser Parameter ist erforderlich, wenn das Kassettenarchiv ein externes Kassettenarchiv ist.

ONLine
: Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

  Yes
  : Gibt an, dass der Pfad für die Verwendung verfügbar ist.

  No
  : Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

  Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.

  Achtung: Ist der Pfad zu einem Kassettenarchiv offline, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während der Pfad zu dem Kassettenarchiv offline ist, wird das Kassettenarchiv nicht initialisiert.

Beispiel: Einen Pfad von einem Server zu einem Kassettenarchiv definieren

Einen Pfad von dem Server SATURN zu dem SCSI-Kassettenarchiv SCSILIB definieren.  AIX-Betriebssysteme

```
define path saturn scsilib srctype=server
desttype=library device=/dev/lb3
```

 Linux-Betriebssysteme

```
define path saturn scsilib srctype=server
desttype=library device=/dev/tsmscsi/lb3
```

 Windows-Betriebssysteme

```
define path saturn scsilib srctype=server
desttype=library device=lb3.0.0.0
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

DEFINE PATH (Pfad definieren, wenn das Ziel ein ZOSMEDIA-Kassettenarchiv ist)

Verwenden Sie diese Syntax, wenn Sie einen Pfad zu einem ZOSMEDIA-Kassettenarchiv definieren. Sie müssen zuerst den z/OS Media-Server in Ihrer Konfiguration mit dem Befehl DEFINE SERVER definieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DEFine PATH--Quellenname--Zielname--SRCType--=--SERVer------->
```

```
>--DESTType--=--LIBRary--ZOSMEDIASERVER--=--Servername----------><

   .-ONLine--=--Yes-----.
>--+--------------------+-------------------------------------><
   '-ONLine--=--+-Yes-+-'
                '-No--'
```

Parameter

Quellenname (Erforderlich)
: Gibt den Namen der Quelle des Pfads an.

Zielname (Erforderlich)
: Gibt den Namen des ZOSMEDIA-Kassettenarchivs an.

SRCType=SERVer (Erforderlich)
: Gibt an, dass ein Speicheragent oder ein Server die Quelle ist.

DESTType=LIBRary (Erforderlich)
: Gibt an, dass ein Kassettenarchiv das Ziel ist.

ZOSMEDIAServer (Erforderlich)
: Gibt den Namen des Servers an, der einen Tivoli Storage Manager for z/OS Media-Server darstellt.

ONLine
: Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

  Yes
  : Gibt an, dass der Pfad für die Verwendung verfügbar ist.

  No
  : Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

  Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.

  Achtung: Ist der Pfad zu einem Kassettenarchiv offline, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während der Pfad zu dem Kassettenarchiv offline ist, wird das Kassettenarchiv nicht initialisiert.

  Kann während der Initialisierung des IBM Spectrum Protect-Servers nicht auf den z/OS Media-Server zugegriffen werden, wird der Kassettenarchivpfad offline gesetzt. Verwenden Sie den Befehl UPDATE PATH und geben Sie ONLINE=YES an, um das ZOSMEDIA-Kassettenarchiv wieder anzuhängen.

DEFINE POLICYSET (Maßnahmengruppe definieren)

Mit diesem Befehl kann eine Maßnahmengruppe in einer Maßnahmendomäne definiert werden. Eine Maßnahmengruppe enthält Verwaltungsklassen, die Kopiengruppen enthalten. Für jede Maßnahmendomäne können eine oder mehrere Maßnahmengruppen definiert werden.

Um eine Maßnahmengruppe zu aktivieren, muss der Befehl ACTIVATE POLICYSET verwendet werden. In einer Maßnahmendomäne kann nur eine Maßnahmengruppe aktiv sein. Die Kopiengruppen und Verwaltungsklassen innerhalb der aktiven Maßnahmengruppe bestimmen die Regeln, nach denen Client-Knoten Sicherungsoperationen, Archivierungsoperationen und Speicherverwaltungsoperationen ausführen und nach denen die gespeicherten Client-Dateien verwaltet werden.

Bevor eine Maßnahmengruppe mit dem Befehl ACTIVATE POLICYSET aktiviert wird, muss mit dem Befehl VALIDATE POLICYSET überprüft werden, ob sie vollständig und gültig ist.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

Syntax

```
>>-DEFine POlicyset--Domänenname--Name_der_Maßnahmengruppe------>

>--+------------------------------+---------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an, zu der die Maßnahmengruppe gehört.

Name_der_Maßnahmengruppe (Erforderlich)

Gibt den Namen der Maßnahmengruppe an. Die maximale Länge dieses Namens beträgt 30 Zeichen. Eine Maßnahmengruppe mit dem Namen ACTIVE kann nicht definiert werden.

DESCription

Gibt eine Beschreibung für die neue Maßnahmengruppe an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

Beispiel: Eine Maßnahmengruppe definieren

Eine Maßnahmengruppe mit dem Namen `SUMMER` für die Maßnahmendomäne `PROG1` definieren und die Beschreibung "Programming Group Policies" einschließen.

```
define policyset prog1 summer
description="Programming Group Policies"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE POLICYSET

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
COPY POLICYSET	Erstellt eine Kopie einer Maßnahmengruppe.
DEFINE DOMAIN	Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DELETE POLICYSET	Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
UPDATE POLICYSET	Ändert die Beschreibung einer Maßnahmengruppe.
VALIDATE POLICYSET	Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert.

DEFINE PROFASSOCIATION (Profilzuordnung definieren)

Mit diesem Befehl können auf einem Konfigurationsmanager ein oder mehrere Objekte einem Konfigurationsprofil für die Verteilung an subskribierende verwaltete Server zugeordnet werden. Nach der Subskription eines verwalteten Servers für ein Profil sendet der Konfigurationsmanager dem Profil zugeordnete Objektdefinitionen an den verwalteten Server, wo sie in der Datenbank gespeichert werden. Auf diese Weise in der Datenbank eines verwalteten Servers erstellte Objekte werden zu verwalteten Objekten. Ein Objekt kann mehreren Profilen zugeordnet werden.

Mit diesem Befehl können eine anfängliche Gruppe von Profilzuordnungen definiert und vorhandenen Zuordnungen weitere Zuordnungen hinzugefügt werden.

Einem Profil können die folgenden Arten von Objekten zugeordnet werden:

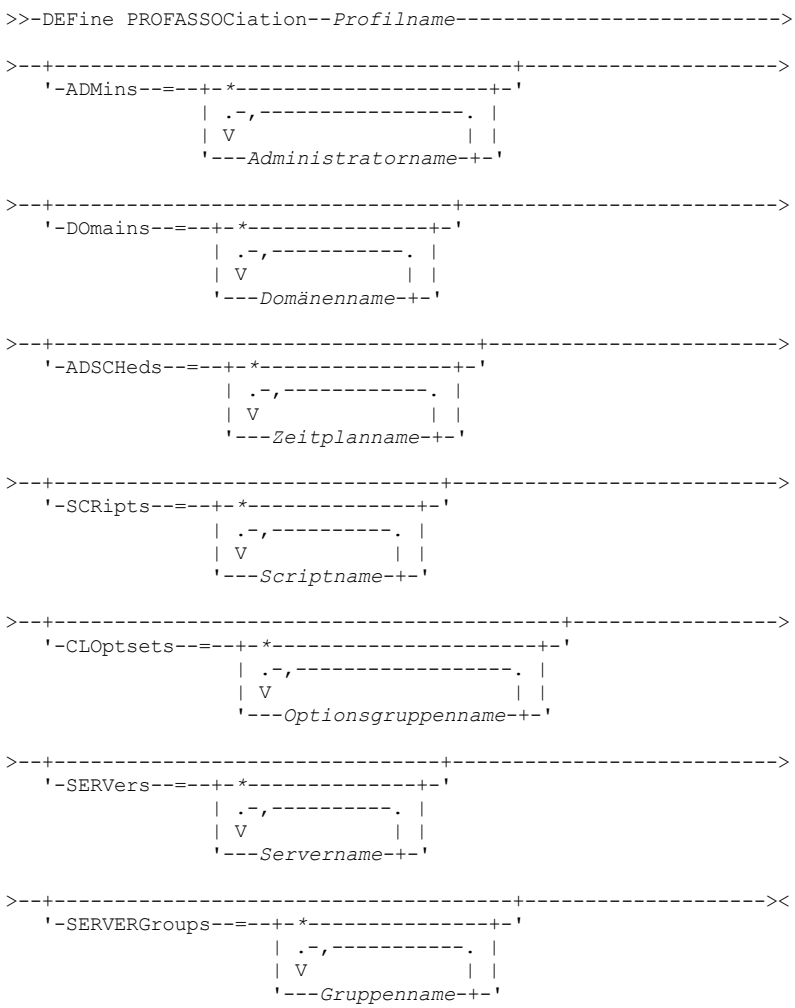
- Administratorregistrierungen und -berechtigungen
- Maßnahmendomänen, die die Maßnahmengruppen der Domänen einschließen, Verwaltungsklassen, Kopiengruppen und Clientzeitpläne
- Verwaltungszeitpläne
- Server-Befehlsprozeduren
- Client-Optionsgruppen
- Serverdefinitionen
- Server-Gruppendefinitionen

Tipp: Der Konfigurationsmanager verteilt keine Statusinformationen für ein Objekt an verwaltete Server. Beispielsweise wird die Anzahl Tage seit dem letzten Zugriff eines Administrators auf den Server nicht an verwaltete Server verteilt. Diese Art der Informationen wird in den Datenbanken der einzelnen verwalteten Server verwaltet.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Profilname (Erforderlich)

Gibt den Namen des Konfigurationsprofils an.

ADMins

Gibt Administratoren an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (*), um alle Administratoren anzugeben, die für den Konfigurationsmanager registriert sind. Wird die globale Definition angegeben und werden später weitere Administratoren hinzugefügt, werden sie automatisch über das Profil verteilt.

Der Konfigurationsmanager verteilt den Administratornamen, das Kennwort, die Kontaktinformationen und die Berechtigungen der Administratoren, die dem Profil zugeordnet sind. Folgendes wird vom Konfigurationsmanager nicht verteilt:

- Der Administrator mit dem Namen SERVER_CONSOLE, auch wenn eine globale Definition verwendet wird
- Der gesperrte oder entsperrte Status eines Administrators

Sind dem Profil bereits Administratoren zugeordnet, gilt folgendes:

- Wird eine Liste mit Administratoren angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition angegeben und ist bereits eine Liste mit Administratoren vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Administratoren angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter ADMINS=* ausgeben.

DOmains

Gibt Maßnahmendomänen an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (*), um alle Domänen anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Domänen hinzugefügt, werden sie automatisch über das Profil verteilt.

Der Konfigurationsmanager verteilt Domäneninformationen, zu denen Definitionen von Maßnahmendomänen, Maßnahmengruppen, Verwaltungsklassen, Kopiengruppen und Clientzeitplänen gehören. Der Konfigurationsmanager verteilt nicht die AKTIVE Maßnahmengruppe. Administratoren auf einem verwalteten Server können eine beliebige Maßnahmengruppe innerhalb einer verwalteten Domäne auf einem verwalteten Server aktivieren.

Sind dem Profil bereits Domänen zugeordnet, gilt folgendes:

- Wird eine Liste mit Domänen angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition verwendet und ist bereits eine Liste mit Domänen vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Domänen angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter DOMAINS=* ausgeben.

Wichtig: Client-Operationen, wie beispielsweise Sichern und Archivieren, schlagen fehl, wenn keine Zielpools vorhanden sind. Daher müssen verwaltete Server, die für dieses Profil subskribieren, über Definitionen für alle Speicherpools verfügen, die als Zielorte in den zugeordneten Domänen angegeben sind. Mit dem Befehl RENAME STGPOOL können vorhandene Speicherpools so umbenannt werden, dass sie den verteilten Zielnamen entsprechen.

ADSCHeds
: Gibt Verwaltungszeitpläne an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (*), um alle Verwaltungszeitpläne anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Verwaltungszeitpläne hinzugefügt, werden sie automatisch über das Profil verteilt.
  Tipp: Verwaltungszeitpläne sind nicht aktiv, wenn sie von einem Konfigurationsmanager verteilt werden. Ein Administrator auf einem verwalteten Server muss jeden Zeitplan aktivieren, damit er auf diesem Server ausgeführt wird.
  Sind dem Profil bereits Verwaltungszeitpläne zugeordnet, gilt folgendes:

  - Wird eine Liste mit Verwaltungszeitplänen angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
  - Wird eine globale Definition verwendet und ist bereits eine Liste mit Verwaltungszeitplänen vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
  - Wird eine Liste mit Verwaltungszeitplänen angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter ADSCHEDS=* ausgeben.

SCRipts
: Gibt Server-Befehlsprozeduren an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (*), um alle Prozeduren anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Prozeduren hinzugefügt, werden sie automatisch über das Profil verteilt.
  Sind dem Profil bereits Prozeduren zugeordnet, gilt folgendes:

  - Wird eine Liste mit Prozeduren angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
  - Wird eine globale Definition verwendet und ist bereits eine Liste mit Prozeduren vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
  - Wird eine Liste mit Prozeduren angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter SCRIPTS=* ausgeben.

CLOptsets
: Gibt Clientoptionsgruppen an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (*), um alle Clientoptionsgruppen anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Client-Optionsgruppen hinzugefügt, werden sie automatisch über das Profil verteilt.
  Sind dem Profil bereits Client-Optionsgruppen zugeordnet, gilt folgendes:

  - Wird eine Liste mit Client-Optionsgruppen angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
  - Wird eine globale Definition verwendet und ist bereits eine Liste mit Client-Optionsgruppen vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
  - Wird eine Liste mit Client-Optionsgruppen angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter CLOPSETS=* ausgeben.

SERVers
: Gibt Server-Definitionen an, die dem Profil zugeordnet werden sollen. Die Definitionen werden an verwaltete Server verteilt, die für dieses Profil subskribieren. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen

Stern (*), um alle Server anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Server hinzugefügt, werden sie automatisch über das Profil verteilt.

Der Konfigurationsmanager verteilt die folgenden Serverattribute: Übertragungsmethode, IP-Adresse, Anschlussadresse, Serverkennwort, URL und die Beschreibung. Für verteilte Serverdefinitionen ist das Attribut ALLOWREPLACE auf dem verwalteten Server immer auf YES gesetzt, unabhängig von dem Wert dieses Parameters auf dem Konfigurationsmanager. Auf dem verwalteten Server kann der Befehl UPDATE SERVER verwendet werden, um alle anderen Attribute zu definieren.

Sind dem Profil bereits Server zugeordnet, gilt folgendes:

- Wird eine Liste mit Servern angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition verwendet und ist bereits eine Liste mit Servern vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Servern angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter SERVERS=* ausgeben.

Wichtig:

1. Eine Serverdefinition auf einem verwalteten Server wird nicht durch eine Definition von dem Konfigurationsmanager ersetzt, es sei denn, es wurde das Ersetzen der Definition auf dem verwalteten Server erlaubt. Um das Ersetzen zu erlauben, die Serverdefinition auf dem verwalteten Server aktualisieren, indem der Befehl UPDATE SERVER mit ALLOWREPLACE=YES verwendet wird.
2. Wenn ein Konfigurationsmanager eine Serverdefinition an einen verwalteten Server verteilt und eine Servergruppe mit demselben Namen auf dem verwalteten Server vorhanden ist, ersetzt die verteilte Serverdefinition die Servergruppendefinition.

SERVERGroups
Gibt Server-Gruppen an, die dem Profil zugeordnet werden sollen. Es können Platzhalterzeichen in den Namen verwendet werden. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Verwenden Sie die globale Definition, einen einzelnen Stern (*), um alle Servergruppen anzugeben, die auf dem Konfigurationsmanager definiert sind. Wird die globale Definition angegeben und werden später weitere Server-Gruppen hinzugefügt, werden sie automatisch über das Profil verteilt.
Tipp: Ein Konfigurationsmanager verteilt eine Servergruppendefinition nicht an einen verwalteten Server, wenn dieser über eine Serverdefinition mit demselben Namen wie die Servergruppe verfügt.
Sind dem Profil bereits Server-Gruppen zugeordnet, gilt folgendes:

- Wird eine Liste mit Server-Gruppen angegeben und ist bereits eine Liste vorhanden, kombiniert IBM Spectrum Protect die neue Liste mit der vorhandenen Liste.
- Wird eine globale Definition verwendet und ist bereits eine Liste mit Server-Gruppen vorhanden, ersetzt IBM Spectrum Protect die Liste durch die globale Definition.
- Wird eine Liste mit Server-Gruppen angegeben und wurde zuvor eine globale Definition angegeben, ignoriert IBM Spectrum Protect die Liste. Zum Entfernen der globalen Definition den Befehl DELETE PROFASSOCIATION mit dem Parameter SERVERGROUPS=* ausgeben.

Beispiel: Eine bestimmte Domäne einem bestimmten Profil zuordnen

Die Domäne MARKETING dem Profil DELTA zuordnen.

```
define profassociation delta domains=marketing
```

Beispiel: Alle Domänen einem bestimmten Profil zuordnen

Es wurde bereits eine Liste mit Domänen dem Profil GAMMA zugeordnet. Jetzt sollen alle Domänen, die auf dem Konfigurationsmanager definiert sind, dem Profil zugeordnet werden.

```
define profassociation gamma domains=*
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE PROFASSOCIATION

Befehl	Beschreibung
COPY PROFILE	Erstellt eine Kopie eines Profils.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DELETE PROFASSOCIATION	Löscht die Zuordnung zwischen einem Objekt und einem Profil.
DELETE PROFILE	Löscht ein Profil aus einem Konfigurationsmanager.
LOCK PROFILE	Verhindert die Verteilung eines Konfigurationsprofils.

Befehl	Beschreibung
NOTIFY SUBSCRIBERS	Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.
QUERY PROFILE	Zeigt Informationen über Konfigurationsprofile an.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UNLOCK PROFILE	Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

DEFINE PROFILE (Profil definieren)

Mit diesem Befehl kann auf einem Konfigurationsmanager ein Profil (eine Gruppe von Konfigurationsdaten) definiert werden, das an verwaltete Server verteilt werden kann.

Nach der Definition eines Profils können mit dem Befehl DEFINE PROFASSOCIATION Objekte angegeben werden, die an subskribierende verwaltete Server für das Profil verteilt werden sollen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine PROFIle--Profilname-------------------------------------->

>--+-------------------------------+---------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Profilname (Erforderlich)
: Gibt den Namen des Profils an. Die maximale Länge des Namens beträgt 30 Zeichen.

DESCription
: Gibt eine Beschreibung des Profils an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Dieser Parameter ist wahlfrei.

Beispiel: Ein neues Profil definieren

Das Profil ALPHA mit der Beschreibung "Programming Center" definieren.

```
define profile alpha
description="Programming Center"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE PROFILE

Befehl	Beschreibung
COPY PROFILE	Erstellt eine Kopie eines Profils.
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DEFINE SUBSCRIPTION	Subskribiert einen verwalteten Server für ein Profil.
DELETE PROFASSOCIATION	Löscht die Zuordnung zwischen einem Objekt und einem Profil.
DELETE PROFILE	Löscht ein Profil aus einem Konfigurationsmanager.
LOCK PROFILE	Verhindert die Verteilung eines Konfigurationsprofils.
QUERY PROFILE	Zeigt Informationen über Konfigurationsprofile an.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UNLOCK PROFILE	Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

DEFINE RECMEDMACHASSOCIATION (Wiederh.-Datenträger Maschine zuordnen)

Mit diesem Befehl können Wiederherstellungsdatenträger einer oder mehreren Maschinen zugeordnet werden. Einer Maschine werden Wiederherstellungsdatenträger zugeordnet, damit der Speicherort der Boot-Datenträger und die Liste der Datenträgernamen zur Verfügung stehen, wenn für die Maschine eine Wiederherstellung erforderlich ist. Zum Abrufen der Informationen den Befehl QUERY MACHINE ausgeben. Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Clientmaschinen zu unterstützen.

Sollen einer Maschine Wiederherstellungsdatenträger zugeordnet werden, müssen die Maschine und die Datenträger in IBM Spectrum Protect definiert sein. Eine Maschine bleibt so lange den Datenträgern zugeordnet, bis die Zuordnung, die Datenträger oder die Maschine gelöscht wird bzw. werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine RECMEDMACHAssociation--Datenträgername---------------->

   .-,-------------.
   V               |
>----Maschinenname-+-------------------------------------------><
```

Parameter

Datenträgername (Erforderlich)
: Gibt den Namen des Wiederherstellungsdatenträgers an, dem Maschinen zugeordnet werden.

Maschinenname (Erforderlich)
: Gibt den Namen der Maschinen an, die dem Wiederherstellungsdatenträger zugeordnet werden sollen. Eine Maschine kann mehreren Wiederherstellungsdatenträgern zugeordnet werden. Soll eine Liste mit Maschinen angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

Beispiel: Wiederherstellungsdatenträgern Maschinen zuordnen

Die Maschinen DISTRICT1 und DISTRICT5 dem Wiederherstellungsdatenträger DIST5RM zuordnen.

```
define recmedmachassociation dist5rm
district1,district5
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE RECMEDMACHASSOCIATION

Befehl	Beschreibung
DEFINE MACHINE	Definiert eine Maschine für DRM.
DEFINE RECOVERYMEDIA	Definiert die Datenträger, die für die Wiederherstellung einer Maschine erforderlich sind.
DELETE MACHINE	Löscht eine Maschine.
DELETE RECMEDMACHASSOCIATION	Löscht die Zuordnung zwischen Wiederherstellungsdatenträgern und einer Maschine.
DELETE RECOVERYMEDIA	Löscht Wiederherstellungsdatenträger.
QUERY MACHINE	Zeigt Informationen über Maschinen an.
QUERY RECOVERYMEDIA	Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an.

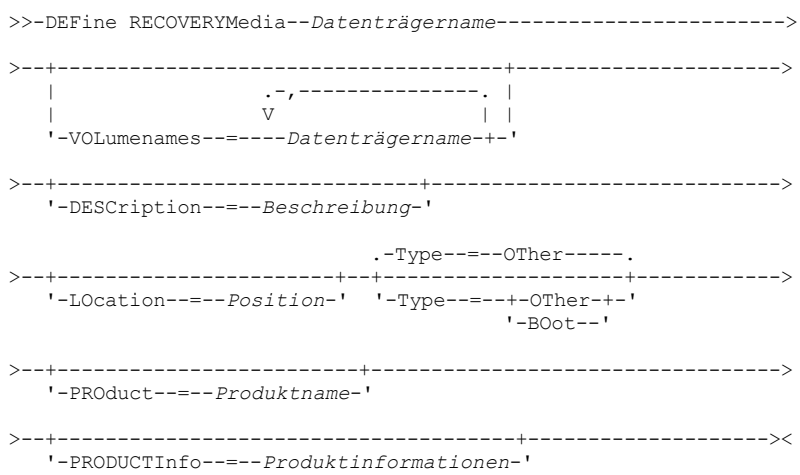
DEFINE RECOVERYMEDIA (Wiederherstellungsdatenträger definieren)

Mit diesem Befehl können die Datenträger definiert werden, die für die Wiederherstellung einer Maschine benötigt werden. Derselbe Datenträger kann mehreren Maschinen zugeordnet werden. Zum Anzeigen der Informationen den Befehl QUERY MACHINE verwenden. Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Client-Maschinen zu unterstützen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Datenträgername (Erforderlich)
: Gibt den Namen des Wiederherstellungsdatenträgers an, der definiert werden soll. Der Name kann bis zu 30 Zeichen umfassen.

VOLumenames
: Gibt die Namen der Datenträger an, die die wiederherstellbaren Daten enthalten (z. B. Abbildkopien des Betriebssystems). Dieser Parameter ist erforderlich, wenn der Datenträgertyp BOOT angegeben wird. Die Namen der Boot-Datenträger in der Reihenfolge angeben, in der sie zur Wiederherstellungszeit in die Maschine eingelegt werden sollen. Die maximale Länge der Datenträgernamensliste beträgt 255 Zeichen. Die Liste in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

DESCription
: Gibt die Beschreibung der Wiederherstellungsdatenträger an. Dieser Parameter ist wahlfrei. Die maximale Länge beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

LOcation
: Gibt den Standort der Wiederherstellungsdatenträger an. Dieser Parameter ist wahlfrei. Die maximale Länge beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Type
: Gibt den Typ von Wiederherstellungsdatenträger an. Dieser Parameter ist wahlfrei. Der Standardwert ist OTHER.

  BOot
  : Gibt an, daß dies ein Boot-Datenträger ist. Der Benutzer muß Datenträgernamen angeben, wenn der Typ BOOT lautet.

  OTher
  : Gibt an, daß dies kein Boot-Datenträger ist. Beispielsweise eine CD, die Handbücher zum Betriebssystem enthält.

PROduct
: Gibt den Namen des Produkts an, das auf diesen Datenträger geschrieben hat. Dieser Parameter ist wahlfrei. Die maximale Länge beträgt 16 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

PRODUCTInfo
: Gibt Informationen zum Produkt an, das auf die Datenträger geschrieben hat. Hierbei handelt es sich um Informationen, die möglicherweise zum Wiederherstellen der Maschine benötigt werden. Dieser Parameter ist wahlfrei. Die maximale Länge beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Beispiel: Die Datenträger definieren, die für die Wiederherstellung einer Maschine benötigt werden

Den Wiederherstellungsdatenträger DIST5RM definieren. Eine Beschreibung und den Standort einschließen.

```
define recoverymedia dist5rm
description="district 5 base system image"
location="district 1 vault"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE RECOVERYMEDIA

Befehl	Beschreibung

Befehl	Beschreibung
DEFINE RECMEDMACHASSOCIATION	Ordnet Wiederherstellungsdatenträger einer Maschine zu.
DELETE RECOVERYMEDIA	Löscht Wiederherstellungsdatenträger.
QUERY RECOVERYMEDIA	Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an.
UPDATE RECOVERYMEDIA	Ändert die Attribute von Wiederherstellungsdatenträgern.

DEFINE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl definieren)

Mit diesem Befehl kann ein Zeitplan für einen Client oder Verwaltungsbefehl erstellt werden.

Der Befehl DEFINE SCHEDULE hat zwei Formen: Eine Form, wenn der Zeitplan Clientoperationen betrifft, und eine Form, wenn der Zeitplan Verwaltungsbefehle betrifft. Innerhalb dieser beiden Formen können Sie entweder Zeitpläne mit klassischer Darstellung oder Zeitpläne mit erweiterter Darstellung auswählen. Syntax und Parameter der jeweiligen Form werden separat definiert.

Für jeden Zeitplan wird ein Startfenster angegeben. Das Startfenster ist der Zeitraum, in dem der Zeitplan eingeleitet werden muß. Die Verarbeitung des Zeitplans wird nicht unbedingt innerhalb dieses Fensters beendet. Wenn der Server beim Start dieses Fensters nicht aktiv ist, aber vor Ende des definierten Fensters gestartet wird, wird der Zeitplan beim Neustart des Servers ausgeführt. Optionen, die jeder Zeitplandarstellung (klassisch und erweitert) zugeordnet sind, bestimmen, wann die Startfenster beginnen sollen.

Tabelle 1. Zugehörige Befehle für DEFINE SCHEDULE

Befehl	Beschreibung
COPY SCHEDULE	Erstellt eine Kopie eines Zeitplans.
DEFINE ASSOCIATION	Ordnet Clients einem Zeitplan zu.
DELETE SCHEDULE	Löscht einen Zeitplan aus der Datenbank.
QUERY EVENT	Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an.
QUERY SCHEDULE	Zeigt Informationen über Zeitpläne an.
SET MAXCMDRETRIES	Gibt die maximale Anzahl Wiederholungen nach der fehlgeschlagenen Ausführung eines geplanten Befehls an.
SET MAXSCHEDSESSIONS	Gibt die maximale Anzahl Client-/Serversitzungen an, die bei der Arbeit mit einem Verarbeitungszeitplan verfügbar sind.
SET RETRYPERIOD	Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.
UPDATE SCHEDULE	Ändert die Attribute eines Zeitplans.

- DEFINE SCHEDULE (Clientzeitplan definieren)
  Verwenden Sie den Befehl DEFINE SCHEDULE, um einen Clientzeitplan zu definieren. IBM Spectrum Protect verwendet diesen Zeitplan, um in angegebenen Intervallen oder an angegebenen Tagen verschiedene Clientoperationen für Ihre Client-Workstations automatisch auszuführen. Nach der Definition eines Zeitplans den Befehl DEFINE ASSOCIATION verwenden, um den Client dem Zeitplan zuzuordnen.
- DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)
  Mit dem Befehl DEFINE SCHEDULE kann ein neuer Zeitplan für die Verarbeitung eines Verwaltungsbefehls erstellt werden.

DEFINE SCHEDULE (Clientzeitplan definieren)

Verwenden Sie den Befehl DEFINE SCHEDULE, um einen Clientzeitplan zu definieren. IBM Spectrum Protect verwendet diesen Zeitplan, um in angegebenen Intervallen oder an angegebenen Tagen verschiedene Clientoperationen für Ihre Client-Workstations automatisch auszuführen. Nach der Definition eines Zeitplans den Befehl DEFINE ASSOCIATION verwenden, um den Client dem Zeitplan zuzuordnen.

Sie müssen den Client-Scheduler auf der Client-Workstation starten, damit IBM Spectrum Protect den Zeitplan verarbeiten kann.

Nicht alle Clients können alle geplanten Operationen ausführen, auch wenn Sie den Zeitplan auf dem Server definieren und ihn dem Client zuordnen können. Ein Macintosh-Client kann beispielsweise keinen Zeitplan ausführen, wenn es sich bei der Aktion um das Zurückschreiben oder Abrufen von Dateien oder um das Ausführen einer ausführbaren Prozedur handelt. Eine ausführbare Prozedur wird auch als Befehlsdatei, Stapeldatei oder Prozedur auf anderen Client-Betriebssystemen bezeichnet.

IBM Spectrum Protect kann nicht mehrere Zeitpläne gleichzeitig für denselben Clientknoten ausführen.

Berechtigungsklasse

Zum Definieren eines Clientzeitplans ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Zeitplan gehört.

Syntax

```
Klassischer Clientzeitplan

>>-DEFine SCHedule--Domänenname--Zeitplanname------------------->

>--+-----------------+--+-----------------------------+-------->
   '-Type--=--Client-'  '-DESCription--=--Beschreibung-'

   .-ACTion--=--Incremental----------------------------------.
>--+-------------------------------------------------------+-->
   '-ACTion--=--+-Incremental----------------------------------+-'
                +-Selective----------------------------------+
                +-Archive--+-----------------------------+---+
                |          |               .-""-------. |   |
                |          '-SUBACTion--=--+----------+-'   |
                |                          '-FASTBack-'     |
                +-Backup--+-------------------------------+-+
                |         |               .-""----------. | |
                |         '-SUBACTion--=--+-------------+-' |
                |                         +-FASTBack----+   |
                |                         +-SYSTEMSTate-+   |
                |                         +-VApp--------+   |
                |                         '-VM----------'   |
                +-REStore------------------------------------+
                +-RETrieve-----------------------------------+
                +-IMAGEBACkup--------------------------------+
                +-IMAGEREStore-------------------------------+
                +-Command------------------------------------+
                +-Macro--------------------------------------+
                '-Deploy-------------------------------------'

>--+---------------------------------+------------------------->
   '-OPTions--=--Optionszeichenfolge-'

>--+-------------------------------------+---------------------->
   |         (1)                         |
   '-OBJects------=--Objektzeichenfolge-'

   .-PRIority--=--5----.  .-STARTDate--=--aktuelles_Datum-.
>--+-------------------+--+-------------------------------+----->
   '-PRIority--=--Zahl-'  '-STARTDate--=--Datum-----------'

   .-STARTTime--=--aktuelle_Zeit-.  .-DURation--=--1----.
>--+-----------------------------+--+------------------+------->
   '-STARTTime--=--Zeit----------'  '-DURation--=--Zahl-'

   .-DURUnits--=--Hours----------.  .-MAXRUNtime--=--0------.
>--+-----------------------------+--+-----------------------+--->
   '-DURUnits--=--+-Minutes----+-'  '-MAXRUNtime--=--Anzahl-'
                  +-Hours------+
                  +-Days-------+
                  '-INDefinite-'

   .-SCHEDStyle--=--Classic-.  .-PERiod--=--1----.
>--+------------------------+--+-----------------+-------------->
   '-SCHEDStyle--=--Classic-'  '-PERiod--=--Zahl-'

   .-PERUnits--=--Days--------.
>--+--------------------------+--------------------------------->
   '-PERUnits--=--+-Hours---+-'
                  +-Days----+
                  +-Weeks---+
                  +-Months--+
                  +-Years---+
                  '-Onetime-'

   .-DAYofweek--=--ANY-----------.
>--+-----------------------------+------------------------------>
   '-DAYofweek--=--+-ANY--------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
```

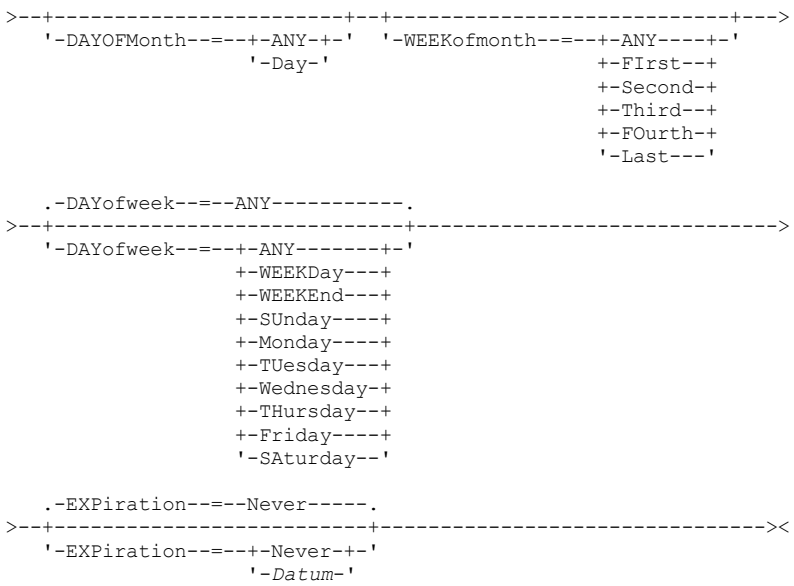
```
                  +-Friday----+
                  '-SAturday--'

   .-EXPiration--=--Never-----.
>--+--------------------------+-------------------------------><
   '-EXPiration--=--+-Never-+-'
                    '-Datum-'
```

Anmerkungen:

1. Der Parameter OBJECTS ist bei `ACTION=INCREMENTAL` optional, für andere Aktionen jedoch erforderlich.

Syntax

```
Erweiterter Clientzeitplan

>>-DEFine SCHedule--Domänenname--Zeitplanname------------------->

>--+-----------------+--+------------------------------+-------->
   '-Type--=--Client-'  '-DESCription--=--Beschreibung-'

   .-ACTion--=--Incremental-----------------------------------.
>--+---------------------------------------------------------+-->
   '-ACTion--=--+-Incremental----------------------------------+-'
                +-Selective--------------------------------+
                +-Archive--+-------------------------+-------+
                |          '-SUBACTion--=--FASTBack-'       |
                +-Backup--+-------------------------------+-+
                |         |               .-""----------. | |
                |         '-SUBACTion--=--+-------------+-' |
                |                         +-FASTBack----+   |
                |                         +-SYSTEMSTate-+   |
                |                         +-VApp--------+   |
                |                         '-VM----------'   |
                +-REStore----------------------------------+
                +-RETrieve---------------------------------+
                +-IMAGEBACkup------------------------------+
                +-IMAGERESTore-----------------------------+
                +-Command----------------------------------+
                '-Macro------------------------------------'

>--+---------------------------------+-------------------------->
   '-OPTions--=--Optionszeichenfolge-'

>--+-----------------------------------+----------------------->
   |         (1)                       |
   '-OBJects------=--Objektzeichenfolge-'

   .-PRIority--=--5----.  .-STARTDate--=--aktuelles_Datum-.
>--+-------------------+--+-------------------------------+----->
   '-PRIority--=--Zahl-'  '-STARTDate--=--Datum-----------'

   .-STARTTime--=--aktuelle_Zeit-.  .-DURation--=--1----.
>--+-----------------------------+--+-------------------+------->
   '-STARTTime--=--Zeit----------'  '-DURation--=--Zahl-'

   .-DURUnits--=--Hours-------.  .-MAXRUNtime--=--0------.
>--+-------------------------+--+----------------------+------>
   '-DURUnits--=--+-Minutes-+-'  '-MAXRUNtime--=--Anzahl-'
                  +-Hours---+
                  '-Days----'

                            .-MONth--=--ANY-----------.
>--SCHEDStyle--=--Enhanced--+------------------------+--------->
                            '-MONth--=--+-ANY--------+-'
                                        +-JAnuary---+
                                        +-February--+
                                        +-MARch-----+
                                        +-APril-----+
                                        +-May-------+
                                        +-JUNe------+
                                        +-JULy------+
                                        +-AUgust----+
                                        +-September-+
                                        +-October---+
                                        +-November--+
                                        '-December--'

   .-DAYOFMonth--=--ANY-----.  .-WEEKofmonth--=--ANY--------.
```



Anmerkungen:

1. Der Parameter OBJECTS ist bei `ACTION=INCREMENTAL` optional, für andere Aktionen jedoch erforderlich.

Parameter

Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an, zu der dieser Zeitplan gehört.

Zeitplanname (Erforderlich)
: Gibt den Namen des Zeitplans an, der definiert werden soll. Für den Namen können bis zu 30 Zeichen angegeben werden.

Type=Client
: Gibt an, daß ein Zeitplan für einen Client definiert wird. Dieser Parameter ist wahlfrei.

DESCription
: Gibt eine Beschreibung des Zeitplans an. Dieser Parameter ist wahlfrei. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

ACTion
: Gibt die Aktion an, die bei der Verarbeitung dieses Zeitplans ausgeführt wird.Gültige Werte:

  Incremental
  : Gibt an, daß der Zeitplan alle Dateien sichert, die neu sind oder sich seit der letzten Teilsicherung geändert haben. Mit "Incremental" werden auch alle Dateien gesichert, für die alle vorhandenen Sicherungen möglicherweise verfallen sind.

  Selective
  : Gibt an, daß der Zeitplan nur Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.

  Archive
  : Gibt an, daß der Zeitplan Dateien archiviert, die mit dem Parameter OBJECTS angegeben werden.

  Backup
  : Gibt an, dass der Zeitplan Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.

  REStore
  : Gibt an, daß der Zeitplan Dateien zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

    Wenn Sie ACTION=RESTORE für eine geplante Operation angeben, und ist die Option REPLACE auf PROMPT gesetzt, erfolgt keine Aufforderung. Wird die Option auf PROMPT gesetzt, werden die Dateien übersprungen.

    Wenn Sie eine zweite Dateispezifikation angeben, agiert diese zweite Dateispezifikation als Zielort für die Zurückschreibung. Müssen mehrere Gruppen von Dateien zurückgeschrieben werden, planen Sie eine für jede Dateispezifikation, die zurückgeschrieben werden muss.

  RETrieve
  : Gibt an, dass der Zeitplan Dateien abruft, die mit dem Parameter OBJECTS angegeben werden.
    Hinweis: Eine zweite Datei, die angegeben wird, dient als Abrufzielort. Müssen mehrere Gruppen von Dateien abgerufen werden, erstellen Sie einen separaten Zeitplan für jede Dateigruppe.

  IMAGEBACkup
  : Gibt an, daß der Zeitplan logische Datenträger sichert, die mit dem Parameter OBJECTS angegeben werden.

  IMAGEREStore
  : Gibt an, daß der Zeitplan logische Datenträger zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

  Command

Gibt an, dass der Zeitplan einen Client-Betriebssystembefehl oder ein Script verarbeitet, der bzw. das mit dem Parameter OBJECTS angegeben wird.

Macro
: Gibt an, daß ein Client ein Makro verarbeitet, dessen Dateiname im Parameter OBJECTS angegeben ist.

SUBACTion
: Sie können einen der folgenden Werte angeben:

  ""
  : Wenn eine Nullzeichenfolge (zwei Anführungszeichen) mit ACTION=BACKUP angegeben wird, ist die Sicherung eine Teilsicherung.

  FASTBAck
  : Gibt an, dass eine FastBack-Clientoperation, die durch den Parameter ACTION angegeben wird, für die Verarbeitung geplant werden soll. Der Wert des Parameters ACTION muss ARCHIVE oder BACKUP sein.

  SYSTEMSTate
  : Gibt an, dass eine Clientsystemstatussicherung geplant ist.

  VApp
  : Gibt an, dass eine vApp-Clientsicherung geplant ist. Eine vApp ist eine Sammlung von vorimplementierten virtuellen Maschinen.

  VM
  : Gibt an, dass eine VMware-Clientsicherungsoperation geplant ist.

Deploy
: Gibt an, ob Client-Workstations mit Implementierungspaketen aktualisiert werden sollen, die mit dem Parameter OBJECTS angegeben werden. Der Parameter OBJECTS muss zwei Spezifikationen enthalten: die Paketdateien, die abgerufen werden sollen, und die Position, an der sie abgerufen werden sollen. Stellen Sie sicher, dass die Objekte die Reihenfolge *`Dateien Position`* haben. Beispiel:

  ```
  define schedule standard deploy_1 action=DEPLOY objects=
  "\\IBM_ANR_WIN\c$\tsm\maintenance\client\v6r2\Windows\X32\v620\v6200\*
  ..\IBM_ANR_WIN\"
  ```

  Die Werte für die folgenden Optionen sind eingeschränkt, wenn Sie ACTION=DEPLOY angeben:

  PERUNITS
  : Geben Sie `PERUNITS=ONETIME` an. Wenn Sie `PERUNITS=PERIOD` angeben, wird der Parameter ignoriert.

  DURUNITS
  : Geben Sie `MINUTES`, `HOURS` oder `DAYS` für den Parameter DURUNITS an. Geben Sie nicht INDEFINITE an.

  SCHEDSTYLE
  : Geben Sie die Standarddarstellung CLASSIC an.

  Der Befehl SCHEDULE schlägt fehl, wenn die Parameter nicht den erforderlichen Parameterwerten wie V.R.M.F entsprechen.

OPTions
: Gibt die Clientoptionen an, die für den geplanten Befehl angegeben werden, wenn der Zeitplan verarbeitet wird. Dieser Parameter ist wahlfrei.
  Für diesen Parameter können nur die Optionen angegeben werden, die für den geplanten Befehl gültig sind. Informationen zu den Optionen, die in der Befehlszeile gültig sind, befinden sich im entsprechenden Clienthandbuch. Alle Optionen, für die im Clienthandbuch angegeben ist, dass sie nur in der Anfangsbefehlszeile gültig sind, führen zu einem Fehler oder werden ignoriert, wenn der Zeitplan vom Server ausgeführt wird. Geben Sie beispielsweise die folgenden Optionen nicht an, da sie keinen Einfluss darauf haben, wann der Client den geplanten Befehl verarbeitet:

  - MAXCMDRETRIES
  - OPTFILE
  - QUERYSCHEDPERIOD
  - RETRYPERIOD
  - SCHEDLOGNAME
  - SCHEDMODE
  - SERVERNAME
  - TCPCLIENTADDRESS
  - TCPCLIENTPORT

  Windows-BetriebssystemeWenn Sie einen Scheduler-Service definieren, indem Sie den Befehl DSMCUTIL oder den Assistenten für die GUI des Clients für Sichern/Archivieren verwenden, geben Sie eine Optionsdatei an. Sie können die Optionen in dieser Optionsdatei nicht überschreiben, indem Sie den geplanten Befehl ausgeben. Sie müssen die Optionen in Ihrem Schedulerservice ändern.

  Enthält die Optionszeichenfolge mehrere Optionen oder Optionen mit eingebetteten Leerzeichen, schließen Sie die gesamte Optionszeichenfolge in Hochkommas ein. Schließen Sie einzelne Optionen, die Leerzeichen enthalten, in Anführungszeichen ein. Vor der Option muss ein führendes Minuszeichen stehen. Fehler können auftreten, wenn die Optionszeichenfolge Leerzeichen enthält, die nicht korrekt in Anführungszeichen eingeschlossen sind.

  Die folgenden Beispiele zeigen, wie einige Clientoptionen angegeben werden:

- Geben Sie Folgendes ein, um `subdir=yes` und `domain all-local -systemobject` anzugeben:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Geben Sie Folgendes ein, um `domain all-local -c: -d:` anzugeben:
  - `options='-domain="all-local -c: -d:"'`

 Windows-BetriebssystemeTipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

OBJects
: Gibt die Objekte an, für die die angegebene Aktion ausgeführt wird. Verwenden Sie ein einzelnes Leerzeichen zwischen jedem Objekt. Außer bei ACTION=INCREMENTAL ist dieser Parameter erforderlich. Ist die Aktion eine Sicherungs-, Archivierungs-, Abruf- oder Zurückschreibungsoperation, sind die Objekte Dateibereiche, Verzeichnisse oder logische Datenträger. Dient die Aktion zur Ausführung eines Befehls oder Makros, ist das Objekt der Name des auszuführenden Befehls oder Makros.

  Wenn ACTION=INCREMENTAL ohne Angabe eines Werts für diesen Parameter angegeben wird, wird der geplante Befehl ohne angegebene Objekte aufgerufen, und der Befehl versucht, die Objekte wie in der Clientoptionsdatei definiert zu verarbeiten. Um alle Dateibereiche oder Verzeichnisse für eine Aktion auszuwählen, müssen sie explizit in der Objektzeichenfolge aufgeführt werden. Wird nur ein Stern in die Objektzeichenfolge eingegeben, erfolgt die Sicherung nur für das Verzeichnis, bei dem der Scheduler gestartet wurde.

  Wichtig:

  - Wenn Sie eine zweite Dateispezifikation angeben, und handelt es sich nicht um einen gültigen Zielort, empfangen Sie diesen Fehler:

    ```
    ANS1082E Ungültige
    Zieldateispezifikation <Dateispezifikation> eingegeben.
    ```

  - Geben Sie mehr als zwei Dateispezifikationen an, empfangen Sie diesen Fehler:

    ```
    ANS1102E Zu viele Befehlszeilenparameter an das Programm übergeben!
    ```

  Wird für diesen Parameter ACTION=ARCHIVE, INCREMENTAL oder SELECTIVE angegeben, können Sie maximal 20 Dateispezifikationen auflisten.

  Schließen Sie die Objektzeichenfolge in Anführungszeichen ein, wenn sie Leerzeichen enthält, und schließen Sie dann die Anführungszeichen in Hochkommas ein. Enthält die Objektzeichenfolge mehrere Dateinamen, schließen Sie jeden Dateinamen in Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Fehler können auftreten, wenn Dateinamen ein Leerzeichen enthalten, das nicht korrekt in Anführungszeichen eingeschlossen ist.

   Windows-BetriebssystemeWenn Sie Zeichen verwenden, die für Windows-Benutzer eine besondere Bedeutung haben, wie z. B. Kommas, schließen Sie das gesamte Argument in doppelte Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Die folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

  - Geben Sie Folgendes ein, um C:\FILE 2, D:\GIF FILES und E:\MY TEST FILE anzugeben:
    - `OBJECTS='"C:\FILE 2" "D:\GIF FILES" "E:\MY TEST FILE"'`
  - Geben Sie Folgendes ein, um D:\TEST FILE anzugeben:
    - `OBJECTS='"D:\TEST FILE"'`
  - Geben Sie Folgendes ein, um D:TEST,FILE anzugeben:
    - `OBJECTS='""D:\TEST,FILE""'`

  AIX-BetriebssystemeLinux-BetriebssystemeDie folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

  - Geben Sie Folgendes ein, um /home/file 2, /home/gif files und /home/my test file anzugeben:
    - `OBJECTS='"/home/file 2" "/home/gif files" "/home/my test file"'`
  - Geben Sie Folgendes ein, um /home/test file anzugeben:
    - `OBJECTS='"/home/test file"'`

   Windows-BetriebssystemeTipp:

  Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

  - Eine Serie von Befehlen des Verwaltungsclients verarbeiten
  - Einzelne Befehle mit dem Verwaltungsclient verarbeiten

PRIority
: Gibt den Prioritätswert für einen Zeitplan an. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 10, wobei 1 die höchste Priorität und 10 die niedrigste Priorität angibt. Der Standardwert ist 5.

Wenn zwei oder mehr Zeitpläne dieselbe Fensterstartzeit haben, legt der angegebene Wert fest, wann IBM Spectrum Protect den Zeitplan verarbeitet. Der Zeitplan mit der höchsten Priorität startet zuerst. Ein Zeitplan mit PRIORITY=3 startet beispielsweise vor einem Zeitplan mit PRIORITY=5.

STARTDate

Gibt das Datum für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Diesen Parameter zusammen mit dem Parameter STARTTIME verwenden, um anzugeben, wann das Anfangsstartfenster des Zeitplans startet.
Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage **oder** +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY +3 **oder** +3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

STARTTime

Gibt die Uhrzeit für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter gibt in Verbindung mit dem Parameter STARTDATE den Beginn des Anfangsstartfensters an.
Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW+02:00 oder STARTTIME=+02:00 ausgegeben, beginnt das Startfenster um 7:00 Uhr.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW-02:00 **oder** -02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW-02:00 oder STARTTIME=-02:00 ausgegeben, beginnt das Startfenster um 3:00 Uhr.

DURation

Gibt die Anzahl Einheiten an, die die Länge des Startfensters der geplanten Operation definiert. Dieser Parameter ist wahlfrei. Dieser Wert muß zwischen 1 und 999 liegen. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter DURUNITS verwenden, um die Länge des Startfensters anzugeben. Werden beispielsweise DURATION=20 und DURUNITS=MINUTES angegeben, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Standardlänge des Startfensters beträgt 1 Stunde. Die Länge des Fensters muß kürzer sein, als der Zeitraum zwischen Fenstern.

Dieser Wert wird ignoriert, wenn DURUNITS=INDEFINITE angegeben wird.

Tipp: Definieren Sie Zeitpläne mit einer Dauer von mehr als 10 Minuten. Damit erhält der IBM Spectrum Protect-Scheduler genügend Zeit, den Zeitplan zu verarbeiten und den Client abzufragen.

DURUnits

Gibt die Zeiteinheiten an, mit denen die Dauer des Fensters bestimmt wird, in dem der Zeitplan starten kann. Dieser Parameter ist wahlfrei. Der Standardwert ist HOURS.

Diesen Parameter zusammen mit dem Parameter DURATION verwenden, um anzugeben, wie lange das Startfenster geöffnet bleibt, um den Zeitplan zu verarbeiten. Gilt beispielsweise DURATION=20 und DURUNITS=MINUTES, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Verarbeitung des Zeitplans muß nicht unbedingt innerhalb dieses Fensters enden.

Wenn der Zeitplan aus irgendeinem Grund wiederholt werden muß, müssen die Wiederholungsversuche vor Ablauf des Startfensters beginnen; andernfalls wird die Operation nicht erneut gestartet.

Der Standardwert für die Länge des Startfensters ist 1 Stunde. Sie können einen der folgenden Werte angeben:

Minutes
: Gibt an, daß die Dauer des Fensters in Minuten definiert wird.

Hours
: Gibt an, daß die Dauer des Fensters in Stunden definiert wird.

Days
: Gibt an, daß die Dauer des Fensters in Tagen definiert wird.

INDefinite
: Gibt an, daß die Dauer des Startfensters der geplanten Operation unbegrenzt ist. Der Zeitplan kann bis zu seinem Verfall zu einem beliebigen Zeitpunkt nach der geplanten Startzeit ausgeführt werden. Sie können DURUNITS=INDEFINITE nur angeben, wenn Sie PERUNITS=ONETIME angeben. Der Wert INDEFINITE ist für erweiterte Zeitpläne nicht zulässig.

MAXRUNtime
: Gibt die maximale Ausführungszeit an. Hierbei handelt es sich um die Anzahl Minuten, in denen alle Clientsitzungen, die von der geplanten Operation gestartet werden, abgeschlossen werden sollten. Sind Sitzungen nach Ablauf der maximalen Ausführungszeit noch aktiv, gibt der Server eine Warnung aus, aber die Ausführung der Sitzungen wird fortgesetzt.
Tipp: Die maximale Ausführungszeit wird ab dem Beginn des Startfensters und nicht ab der Zeit berechnet, zu der Sitzungen innerhalb des Startfensters gestartet werden.
Einschränkungen:

- Der Wert des Parameters wird nicht an Server verteilt, die von einem Manager für unternehmensweite Konfiguration verwaltet werden.
- Der Wert des Parameters wird nicht mit dem Befehl EXPORT exportiert.

Der Parameter ist wahlfrei.Sie können eine Zahl im Bereich von 0 bis 1440 angeben. Der Standardwert ist 0.Der Wert 0 bedeutet, dass die maximale Ausführungszeit unendlich ist und keine Warnung ausgegeben wird. Die maximale Ausführungszeit muss größer als die Dauer des Startfensters sein, die mit den Parametern DURATION und DURUNITS definiert wird.

Ist beispielsweise die Startzeit einer geplanten Operation 21:00 Uhr und beträgt die Dauer des Startfensters 2 Stunden, erstreckt sich das Startfenster von 21:00 Uhr bis 23:00 Uhr. Beträgt die maximale Ausführungszeit 240 Minuten (4 Stunden), sollten alle Clientsitzungen für diese Operation um 1:00 Uhr abgeschlossen sein. Sind eine oder mehrere Sitzungen nach 1:00 Uhr noch aktiv, gibt der Server eine Warnung aus.
Tipp: Alternativ können Sie den Wert 1:00 Uhr für *Ausführungszeitsalert* im IBM Spectrum Protect Operations Center angeben.

SCHEDStyle
: Dieser Parameter ist wahlfrei. SCHEDSTYLE definiert entweder das Intervall zwischen den Zeiten, zu denen ein Zeitplan ausgeführt werden kann, oder die Tage, an denen der Zeitplan ausgeführt wird. Der Standardwert ist die klassische Syntax.
Gültige Werte:

Classic
: Die Parameter für die klassische (classic) Syntax sind: PERIOD, PERUNITS und DAYOFWEEK. Diese Parameter können nicht verwendet werden: MONTH, DAYOFMONTH und WEEKOFMONTH.

Enhanced
: Die Parameter für die erweiterte (enhanced) Syntax sind: MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK. Diese Parameter können nicht verwendet werden: PERIOD und PERUNITS.

PERiod
: Gibt den Zeitraum zwischen Startfenstern für diesen Zeitplan an. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Zulässige Werte sind ganze Zahlen von 1 bis 999. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter PERUNITS verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle fünf Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Zeitraum zwischen den Startfenstern muß länger sein als die Dauer jedes Fensters. Der Standardwert ist 1 Tag.

Dieser Wert wird ignoriert, wenn PERUNITS=ONETIME angegeben wird.

PERUnits
: Gibt die Zeiteinheiten an, mit denen der Zeitraum zwischen Startfenstern für diesen Zeitplan bestimmt wird. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Der Standardwert ist DAYS.
Diesen Parameter zusammen mit dem Parameter PERIOD verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle 5 Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Standardwert ist 1 Tag. Sie können einen der folgenden Werte angeben:

Hours
: Gibt an, daß der Zeitraum zwischen Startfenstern in Stunden angegeben wird.

Days
: Gibt an, daß der Zeitraum zwischen Startfenstern in Tagen angegeben wird.

Weeks

Gibt an, daß der Zeitraum zwischen Startfenstern in Wochen angegeben wird.

Months
: Gibt an, daß der Zeitraum zwischen Startfenstern in Monaten angegeben wird.

  Wird PERUNITS=MONTHS angegeben, wird die geplante Operation jeden Monat an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/04/1998 lautet, wird der Zeitplan danach am 4. jedes Monats verarbeitet. Wenn das Datum jedoch für den nächsten Monat nicht gültig ist, wird die geplante Operation am letzten gültigen Datum in dem Monat verarbeitet. Danach basieren nachfolgende Operationen auf diesem neuen Datum. Wenn das Startdatum beispielsweise 03/31/1998 lautet, wird die Operation des nächsten Monats für den 04/30/1998 geplant. Danach werden alle folgenden Operationen bis Februar am 30. des Monats ausgeführt. Da Februar nur 28 Tage hat, wird die Operation für das Datum 02/28/1999 geplant. Nachfolgende Operationen werden am 28. des Monats verarbeitet.

Years
: Gibt an, daß der Zeitraum zwischen Startfenstern für den Zeitplan in Jahren angegeben wird.

  Wird PERUNITS=YEARS angegeben, wird die geplante Operation jährlich in demselben Monat und an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/29/2004 lautet, wird die geplante Operation des nächsten Jahres am 02/28/2005 ausgeführt, da Februar nur 28 Tage hat. Danach werden folgende Operationen für den 28. Februar geplant.

Onetime
: Gibt an, daß der Zeitplan einmal verarbeitet wird. Dieser Wert überschreibt den für den Parameter PERIOD angegebenen Wert.

DAYofweek
: Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können verschiedene Optionen für den Parameter DAYofweek angeben, abhängig davon, ob die Zeitplandarstellung als 'Klassisch' oder 'Erweitert' definiert wurde:

  Klassischer Zeitplan
  : Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können entweder einen Tag der Woche oder WEEKDAY, WEEKEND oder ANY angeben. Fallen Startdatum und Startzeit auf einen Tag, der nicht einem angegebenen Tag entspricht, werden das Startdatum und die Startzeit in 24-Stunden-Schritten vorverlegt, bis die Angabe im Parameter DAYOFWEEK erfüllt ist.

    Wird für DAYOFWEEK nicht ANY angegeben, werden die Zeitpläne, je nach Angabe für PERIOD und PERUNITS, möglicherweise nicht zum erwarteten Zeitpunkt verarbeitet. Der Standardwert ist ANY.

  Erweiterter Zeitplan
  : Gibt die Tage der Woche an, an denen der Zeitplan ausgeführt werden soll. Sie können entweder mehrere Tage, die durch Kommas und ohne Leerzeichen voneinander getrennt werden, oder WEEKDAY, WEEKEND oder ANY angeben. Werden mehrere Tage angegeben, wird der Zeitplan an jedem angegebenen Tag ausgeführt. Wird WEEKDAY oder WEEKEND angegeben, müssen Sie auch entweder WEEKOFMONTH=FIRST oder WEEKOFMONTH=LAST angeben, und der Zeitplan wird nur einmal pro Monat ausgeführt.

    Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag der Woche oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter DAYOFWEEK muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

  Gültige Werte für den Parameter DAYofweek sind:

  ANY
  : Das Startfenster kann an einem beliebigen Wochentag beginnen.

  WEEKDay
  : Das Startfenster kann am Montag, Dienstag, Mittwoch, Donnerstag oder Freitag beginnen.

  WEEKEnd
  : Das Startfenster kann am Samstag oder Sonntag beginnen.

  SUnday
  : Das Startfenster beginnt am Sonntag.

  Monday
  : Das Startfenster beginnt am Montag.

  TUesday
  : Das Startfenster beginnt am Dienstag.

  Wednesday
  : Das Startfenster beginnt am Mittwoch.

  THursday
  : Das Startfenster beginnt am Donnerstag.

  Friday
  : Das Startfenster beginnt am Freitag.

  SAturday
  : Das Startfenster beginnt am Samstag.

MONth

Gibt die Monate des Jahres an, in denen der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Geben Sie mehrere Werte an, indem Sie Kommas und keine Leerzeichen verwenden. Der Standardwert lautet ANY. Er bedeutet, dass der Zeitplan während aller Monate des Jahres ausgeführt wird.

DAYOFMonth

Gibt den Tag des Monats an, an dem der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Sie können entweder ANY oder eine Zahl von -31 bis 31, ausschließlich Null, angeben. Ein negativer Wert gibt einen Tag an, bei dem vom Ende des Monats zurückgezählt wird. Beispiel: Der letzte Tag des Monats ist -1, der vorletzte Tag des Monats ist -2 usw. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan an jedem angegebenen Tag des Monats ausgeführt. Geben mehrere Werte denselben Tag an, wird der Zeitplan nur einmal an diesem Tag ausgeführt.

Der Standardwert ist ANY. ANY bedeutet, dass der Zeitplan an jedem Tag des Monats oder an den Tagen ausgeführt wird, die durch andere Parameter des erweiterten Zeitplans bestimmt werden. Der Parameter DAYOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFWEEK oder WEEKOFMONTH verwendet wird.

WEEKofmonth

Gibt die Woche des Monats an, in der der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Eine Woche wird als beliebige 7-Tage-Periode betrachtet, die nicht an einem bestimmten Tag der Woche beginnt. Sie können FIRST, SECOND, THIRD, FOURTH, LAST oder ANY angeben. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan während jeder angegebenen Woche des Monats ausgeführt. Geben mehrere Werte dieselbe Woche an, wird der Zeitplan nur einmal während dieser Woche ausgeführt.

Der Standardwert ist ANY. ANY bedeutet, dass der Zeitplan während jeder Woche des Monats oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter WEEKOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

EXPiration

Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NEVER. Sie können einen der folgenden Werte angeben:

Never

Gibt an, dass der Zeitplan nie abläuft.

Ablaufdatum

Gibt das Datum im Format MM/DD/YYYY an, an dem dieser Zeitplan abläuft. Wenn ein Ablaufdatum angegeben wird, läuft der Zeitplan um 23:59:59 Uhr am angegebenen Datum ab.

Beispiel: Einen Zeitplan für eine monatliche Teilsicherung definieren

Den Zeitplan MONTHLY_BACKUP definieren, der eine Teilsicherung aller zugeordneten Knoten einleitet. Als Startdatum Dienstag, den 1. Mai 2001 angeben. Dieses Datum stimmt nicht mit dem angegebenen Wochentag (Sonntag) überein. Daher beginnt das Anfangsstartfenster am ersten Sonntag nach dem 1. Mai 2001 (05/01/2001). Das Startfenster für diesen Zeitplan dauert von 01:00 bis 03:00. Dieser monatliche Zeitplan leitet Sicherungen der Dateibereiche c: und d: für alle zugeordneten Knoten ein.

```
define schedule standard monthly_backup
description="Monthly Backup of c: and d: drives"
objects="c:\* d:\*"
startdate=05/01/2001 starttime=01:00
duration=2 durunits=hours period=1
perunits=months dayofweek=sunday
```

Beispiel: Einen Zeitplan für eine wöchentliche Teilsicherung definieren

Den Zeitplan WEEKLY_BACKUP definieren, der eine Teilsicherung aller zugeordneten Knoten einleitet. Das Anfangsstartfenster für diesen Zeitplan dauert von 23:00 Uhr am Samstag, 7. Juni 1997 (06/07/1997), bis 03:00 Uhr am Sonntag, 8. Juni 1997 (06/08/1997). Nachfolgende Fenster beginnen um 23:00 Uhr an jedem Samstag. Bei der Ausführung dieses Zeitplans werden keine Nachrichten an den Clientknoten zurückgegeben.

```
define schedule employee_records weekly_backup
startdate=06/07/1997 starttime=23:00 duration=4
durunits=hours perunits=weeks
dayofweek=saturday options=-quiet
```

Beispiel: Einen Zeitplan definieren, mit dem ein bestimmtes Verzeichnis vierteljährlich archiviert wird

Einen Zeitplan definieren, der bestimmte Dateien vierteljährlich am letzten Freitag des Monats archiviert.

```
define schedule employee_records quarterly_archive
starttime=20:00 action=archive
object=/home/employee/records/*
duration=1 durunits=hour schedstyle=enhanced
month=mar,jun,sep,dec weekofmonth=last dayofweek=fri
```

DEFINE SCHEDULE (Zeitplan für einen Verwaltungsbefehl definieren)

Mit dem Befehl DEFINE SCHEDULE kann ein neuer Zeitplan für die Verarbeitung eines Verwaltungsbefehls erstellt werden.

In den Zeitplan eines Verwaltungsbefehls können Prozeduren eingeschlossen werden, so dass die Befehle automatisch verarbeitet werden.
Anmerkung:

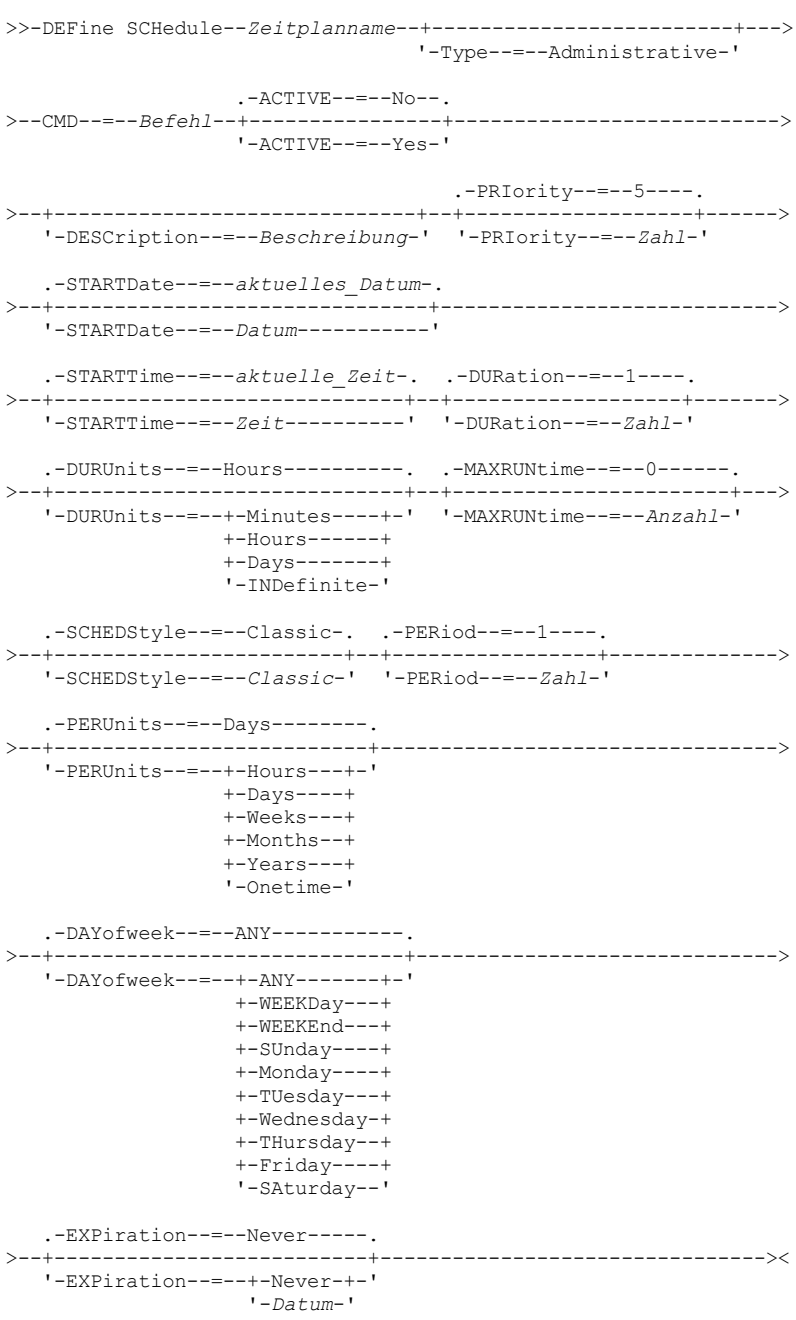
1. Der Befehl MACRO und der Befehl QUERY ACTLOG können nicht geplant werden.
2. Wenn Sie einen Befehl planen, der den Parameter WAIT angibt, muss der Parameter auf YES gesetzt werden, damit der Prozess für die Sitzung, die ihn gestartet hat, einen Rückkehrcode zur Verfügung stellen kann. Weitere Informationen zum Parameter WAIT befinden sich in Serverbefehlsverarbeitung.

Berechtigungsklasse

Zum Definieren eines Zeitplans für Verwaltungsbefehle ist die Systemberechtigung erforderlich.

Syntax

Klassischer Verwaltungszeitplan



Syntax

```
Erweiterter Verwaltungszeitplan

>>-DEFine SCHedule--Zeitplanname--+-------------------------+--->
                                  '-Type--=--Administrative-'

                  .-ACTIVE--=--NO--.
>--CMD--=--Befehl--+----------------+--------------------------->
                   '-ACTIVE--=--YES-'

                                      .-PRIority--=--5----.
>--+-------------------------------+--+-------------------+------>
   '-DESCription--=--Beschreibung-'  '-PRIority--=--Zahl-'

   .-STARTDate--=--aktuelles_Datum-.
>--+-------------------------------+--------------------------->
   '-STARTDate--=--Datum-----------'

   .-STARTTime--=--aktuelle_Zeit-.  .-DURation--=--1----.
>--+-----------------------------+--+-------------------+------->
   '-STARTTime--=--Zeit----------'  '-DURation--=--Zahl-'

   .-DURUnits--=--Hours-------.  .-MAXRUNtime--=--0------.
>--+-------------------------+--+----------------------+------>
   '-DURUnits--=--+-Minutes-+-'  '-MAXRUNtime--=--Anzahl-'
                  +-Hours---+
                  '-Days----'

                            .-MONth--=--ANY-----------.
>--SCHEDStyle--=--Enhanced--+-------------------------+--------->
                            '-MONth--=--+-ANY-------+-'
                                        +-JAnuary---+
                                        +-February--+
                                        +-MARch-----+
                                        +-APril-----+
                                        +-May-------+
                                        +-JUNe------+
                                        +-JULy------+
                                        +-AUgust----+
                                        +-September-+
                                        +-October---+
                                        +-November--+
                                        '-December--'

   .-DAYOFMonth--=--ANY-----.  .-WEEKofmonth--=--ANY--------.
>--+---------------------------+--+-----------------------------+--->
   '-DAYOFMonth--=--+-ANY-+-'  '-WEEKofmonth--=--+-ANY----+-'
                    '-Day-'                      +-FIrst--+
                                                 +-Second-+
                                                 +-Third--+
                                                 +-FOurth-+
                                                 '-Last---'

   .-DAYofweek--=--ANY-----------.
>--+-----------------------------+------------------------------->
   '-DAYofweek--=--+-ANY-------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
                   +-Friday----+
                   '-SAturday--'

   .-EXPiration--=--Never-----.
>--+--------------------------+-------------------------------><
   '-EXPiration--=--+-Never-+-'
                    '-Datum-'
```

Parameter

Zeitplanname (Erforderlich)
: Gibt den Namen des Zeitplans an, der definiert werden soll. Für den Namen können bis zu 30 Zeichen angegeben werden.

Type=Administrative

Gibt an, daß ein Zeitplan für einen Verwaltungsbefehl definiert wird. Dieser Parameter ist wahlfrei. Ein Verwaltungsbefehl wird angenommen, wenn der Parameter CMD angegeben wird.

CMD (Erforderlich)

Gibt den Verwaltungsbefehl an, der für die Verarbeitung geplant werden soll. Die maximale Länge des Befehls beträgt 512 Zeichen. Den Verwaltungsbefehl in Anführungszeichen einschließen, wenn er Leerzeichen enthält.
Einschränkung: Es können keine Umleitungszeichen mit diesem Parameter angegeben werden.

ACTIVE

Gibt an, ob IBM Spectrum Protect einen Zeitplan für einen Verwaltungsbefehl verarbeitet, wenn das Startfenster erscheint. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Der Zeitplan für den Verwaltungsbefehl muß mit dem Befehl UPDATE SCHEDULE in den aktiven Status versetzt werden, damit IBM Spectrum Protect den Zeitplan verarbeiten kann. Gültige Werte:

YES
: Gibt an, daß IBM Spectrum Protect einen Zeitplan für den Verwaltungsbefehl verarbeitet, wenn das Startfenster beginnt.

NO
: Gibt an, daß IBM Spectrum Protect keinen Zeitplan für den Verwaltungsbefehl verarbeitet, wenn das Startfenster beginnt.

DESCription

Gibt eine Beschreibung des Zeitplans an. Dieser Parameter ist wahlfrei. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

PRIority

Gibt den Prioritätswert für einen Zeitplan an. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 10, wobei 1 die höchste Priorität und 10 die niedrigste Priorität angibt. Der Standardwert ist 5.

Wenn zwei oder mehr Zeitpläne dieselbe Fensterstartzeit haben, legt der angegebene Wert fest, wann IBM Spectrum Protect den Zeitplan verarbeitet. Der Zeitplan mit der höchsten Priorität startet zuerst. Ein Zeitplan mit PRIORITY=3 startet beispielsweise vor einem Zeitplan mit PRIORITY=5.

STARTDate

Gibt das Datum für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Diesen Parameter zusammen mit dem Parameter STARTTIME verwenden, um anzugeben, wann das Anfangsstartfenster des Zeitplans startet.
Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage **oder** +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY +3 **oder** +3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

STARTTime

Gibt die Uhrzeit für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter gibt in Verbindung mit dem Parameter STARTDATE den Beginn des Anfangsstartfensters an.
Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW+02:00 oder STARTTIME=+02:00 ausgegeben, beginnt das Startfenster um 7:00 Uhr.

Wert	Beschreibung	Beispiel
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW-02:00 **oder** -02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW-02:00 oder STARTTIME=-02:00 ausgegeben, beginnt das Startfenster um 3:00 Uhr.

DURation
Gibt die Anzahl Einheiten an, die die Länge des Startfensters der geplanten Operation definiert. Dieser Parameter ist wahlfrei. Dieser Wert muß zwischen 1 und 999 liegen. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter DURUNITS verwenden, um die Länge des Startfensters anzugeben. Werden beispielsweise DURATION=20 und DURUNITS=MINUTES angegeben, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Standardlänge des Startfensters beträgt 1 Stunde. Die Länge des Fensters muß kürzer sein, als der Zeitraum zwischen Fenstern.

Dieser Wert wird ignoriert, wenn DURUNITS=INDEFINITE angegeben wird.

DURUnits
Gibt die Zeiteinheiten an, mit denen die Dauer des Fensters bestimmt wird, in dem der Zeitplan starten kann. Dieser Parameter ist wahlfrei. Der Standardwert ist HOURS.

Diesen Parameter zusammen mit dem Parameter DURATION verwenden, um anzugeben, wie lange das Startfenster geöffnet bleibt, um den Zeitplan zu verarbeiten. Gilt beispielsweise DURATION=20 und DURUNITS=MINUTES, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Verarbeitung des Zeitplans muß nicht unbedingt innerhalb dieses Fensters enden. Wenn der Zeitplan aus irgendeinem Grund wiederholt werden muß, müssen die Wiederholungsversuche vor Ablauf des Startfensters beginnen; andernfalls wird die Operation nicht erneut gestartet.

Der Standardwert für die Länge des Startfensters ist 1 Stunde. Sie können einen der folgenden Werte angeben:

Minutes
Gibt an, daß die Dauer des Fensters in Minuten definiert wird.
Hours
Gibt an, daß die Dauer des Fensters in Stunden definiert wird.
Days
Gibt an, daß die Dauer des Fensters in Tagen definiert wird.
INDefinite
Gibt an, daß die Dauer des Startfensters der geplanten Operation unbegrenzt ist. Der Zeitplan kann bis zu seinem Verfall zu einem beliebigen Zeitpunkt nach der geplanten Startzeit ausgeführt werden. Sie können DURUNITS=INDEFINITE nur angeben, wenn Sie PERUNITS=ONETIME angeben. Der Wert INDEFINITE ist für erweiterte Zeitpläne nicht zulässig.

MAXRUNtime
Gibt die maximale Ausführungszeit an. Hierbei handelt es sich um die Anzahl Minuten, in denen Serverprozesse, die von geplanten Befehlen gestartet werden, abgeschlossen werden müssen. Sind Prozesse nach Ablauf der maximalen Ausführungszeit noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.
Tipps:

- Möglicherweise werden die Prozesse nicht sofort beendet, wenn sie von der zentralen Zeitplanung abgebrochen werden. Sie werden beendet, wenn sie die Benachrichtigung über den Abbruch von der zentralen Zeitplanung registrieren.
- Die maximale Ausführungszeit wird ab dem Zeitpunkt berechnet, an dem der Serverprozess startet. Wenn mit dem Befehl für den Zeitplan mehr als ein Prozess gestartet wird, wird die maximale Ausführungszeit für jeden Prozess ab dem Zeitpunkt berechnet, an dem der jeweilige Prozess startet.
- Dieser Parameter gilt nicht für einige Prozesse, wie z. B. Prozesse zum Identifizieren doppelter Daten, deren Ausführung nach Ablauf der maximalen Ausführungszeit fortgesetzt werden kann.
- Dieser Parameter gilt nicht, wenn der geplante Befehl keinen Serverprozess startet.
- Einigen Befehlen kann eine andere Abbruchzeit zugeordnet werden. Beispielsweise kann der Befehl MIGRATE STGPOOL einen Parameter einschließen, der die Länge der Zeit angibt, die die Speicherpoolumlagerung ausgeführt wird, bevor die Umlagerung automatisch abgebrochen wird. Wenn Sie einen Befehl planen, für den eine Abbruchzeit definiert ist, und Sie außerdem eine maximale Ausführungszeit für den Zeitplan definieren, werden die Prozesse zu der Abbruchzeit abgebrochen, die zuerst erreicht wird.

Einschränkungen:

- Der Wert des Parameters wird nicht an Server verteilt, die von einem Manager für unternehmensweite Konfiguration verwaltet werden.
- Der Wert des Parameters wird nicht mit dem Befehl EXPORT exportiert.

Der Parameter ist wahlfrei. Sie können eine Zahl im Bereich von 0 bis 1440 angeben. Der Standardwert ist 0.Der Wert 0 bedeutet, dass die maximale Ausführungszeit unendlich ist und die zentrale Zeitplanung keine Prozesse abbricht. Die maximale Ausführungszeit muss größer als die Dauer des Startfensters sein, die mit den Parametern DURATION und DURUNITS definiert wird.

Ist beispielsweise die Startzeit eines geplanten Befehls 21:00 Uhr und beträgt die Dauer des Startfensters 2 Stunden, erstreckt sich das Startfenster von 21:00 Uhr bis 23:00 Uhr. Beträgt die maximale Ausführungszeit 240 Minuten (4 Stunden), müssen alle zutreffenden Serverprozesse, die von dem Befehl gestartet werden, um 1:00 Uhr abgeschlossen sein. Sind ein oder mehrere zutreffende Prozesse nach 1:00 Uhr noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.
Tipp: Alternativ können Sie eine *Endzeit* von 1:00 Uhr im IBM Spectrum Protect Operations Center angeben.

SCHEDStyle
Dieser Parameter ist wahlfrei. SCHEDSTYLE definiert entweder das Intervall zwischen den Zeiten, zu denen ein Zeitplan ausgeführt werden soll, oder die Tage, an denen der Zeitplan ausgeführt werden soll. Die Darstellung kann entweder classic oder enhanced sein. Der Standardwert ist die klassische Syntax.

Für klassische Zeitpläne sind diese Parameter zulässig: PERIOD, PERUNITS und DAYOFWEEK. Für klassische Zeitpläne nicht zulässig sind: MONTH, DAYOFMONTH und WEEKOFMONTH.

Für erweiterte Zeitpläne sind diese Parameter zulässig: MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK. Diese Parameter sind nicht zulässig: PERIOD und PERUNITS.

PERiod
Gibt den Zeitraum zwischen Startfenstern für diesen Zeitplan an. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Zulässige Werte sind ganze Zahlen von 1 bis 999. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter PERUNITS verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle fünf Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Zeitraum zwischen den Startfenstern muß länger sein als die Dauer jedes Fensters. Der Standardwert ist 1 Tag.

Dieser Wert wird ignoriert, wenn PERUNITS=ONETIME angegeben wird.

PERUnits
Gibt die Zeiteinheiten an, mit denen der Zeitraum zwischen Startfenstern für diesen Zeitplan bestimmt wird. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Der Standardwert ist DAYS.
Diesen Parameter zusammen mit dem Parameter PERIOD verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle 5 Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Standardwert ist 1 Tag. Sie können einen der folgenden Werte angeben:

Hours
Gibt an, daß der Zeitraum zwischen Startfenstern in Stunden angegeben wird.

Days
Gibt an, daß der Zeitraum zwischen Startfenstern in Tagen angegeben wird.

Weeks
Gibt an, daß der Zeitraum zwischen Startfenstern in Wochen angegeben wird.

Months
Gibt an, daß der Zeitraum zwischen Startfenstern in Monaten angegeben wird.

Wird PERUNITS=MONTHS angegeben, wird die geplante Operation jeden Monat an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/04/1998 lautet, wird der Zeitplan danach am 4. jedes Monats verarbeitet. Wenn das Datum jedoch für den nächsten Monat nicht gültig ist, wird die geplante Operation am letzten gültigen Datum in dem Monat verarbeitet. Danach basieren nachfolgende Operationen auf diesem neuen Datum. Wenn das Startdatum beispielsweise 03/31/1998 lautet, wird die Operation des nächsten Monats für den 04/30/1998 geplant. Danach werden alle folgenden Operationen bis Februar am 30. des Monats ausgeführt. Da Februar nur 28 Tage hat, wird die Operation für das Datum 02/28/1999 geplant. Nachfolgende Operationen werden am 28. des Monats verarbeitet.

Years
Gibt an, daß der Zeitraum zwischen Startfenstern für den Zeitplan in Jahren angegeben wird.

Wird PERUNITS=YEARS angegeben, wird die geplante Operation jährlich in demselben Monat und an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/29/2004 lautet, wird die geplante Operation des nächsten Jahres am 02/28/2005 ausgeführt, da Februar nur 28 Tage hat. Danach werden folgende Operationen für den 28. Februar geplant.

Onetime
Gibt an, daß der Zeitplan einmal verarbeitet wird. Dieser Wert überschreibt den für den Parameter PERIOD angegebenen Wert.

DAYofweek
Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können verschiedene Optionen für den Parameter DAYofweek angeben, abhängig davon, ob die Zeitplandarstellung als 'Klassisch' oder 'Erweitert' definiert wurde:

Klassischer Zeitplan
Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können entweder einen Tag der Woche oder WEEKDAY, WEEKEND oder ANY angeben. Fallen Startdatum und Startzeit auf einen Tag, der nicht einem angegebenen Tag entspricht, werden das Startdatum und die Startzeit in 24-Stunden-Schritten vorverlegt, bis die Angabe im Parameter DAYOFWEEK erfüllt ist.

Wird für DAYOFWEEK nicht ANY angegeben, werden die Zeitpläne, je nach Angabe für PERIOD und PERUNITS, möglicherweise nicht zum erwarteten Zeitpunkt verarbeitet. Der Standardwert ist ANY.

Erweiterter Zeitplan
: Gibt die Tage der Woche an, an denen der Zeitplan ausgeführt werden soll. Sie können entweder mehrere Tage, die durch Kommas und ohne Leerzeichen voneinander getrennt werden, oder WEEKDAY, WEEKEND oder ANY angeben. Werden mehrere Tage angegeben, wird der Zeitplan an jedem angegebenen Tag ausgeführt. Wird WEEKDAY oder WEEKEND angegeben, müssen Sie auch entweder WEEKOFMONTH=FIRST oder WEEKOFMONTH=LAST angeben, und der Zeitplan wird nur einmal pro Monat ausgeführt.

  Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag der Woche oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter DAYOFWEEK muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

Gültige Werte für den Parameter DAYofweek sind:

ANY
: Das Startfenster kann an einem beliebigen Wochentag beginnen.

WEEKDay
: Das Startfenster kann am Montag, Dienstag, Mittwoch, Donnerstag oder Freitag beginnen.

WEEKEnd
: Das Startfenster kann am Samstag oder Sonntag beginnen.

SUnday
: Das Startfenster beginnt am Sonntag.

Monday
: Das Startfenster beginnt am Montag.

TUesday
: Das Startfenster beginnt am Dienstag.

Wednesday
: Das Startfenster beginnt am Mittwoch.

THursday
: Das Startfenster beginnt am Donnerstag.

Friday
: Das Startfenster beginnt am Freitag.

SAturday
: Das Startfenster beginnt am Samstag.

MONth
: Gibt die Monate des Jahres an, in denen der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Geben Sie mehrere Werte an, indem Sie Kommas und keine Leerzeichen verwenden. Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan in jedem Monat des Jahres ausgeführt wird.

DAYOFMonth
: Gibt den Tag des Monats an, an dem der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Sie können entweder ANY oder eine Zahl von -31 bis 31, ausschließlich Null, angeben. Ein negativer Wert gibt einen Tag an, bei dem vom Ende des Monats zurückgezählt wird. Beispiel: Der letzte Tag des Monats ist -1, der vorletzte Tag des Monats ist -2 usw. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan an jedem angegebenen Tag des Monats ausgeführt. Geben mehrere Werte denselben Tag an, wird der Zeitplan nur einmal an diesem Tag ausgeführt.

  Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag des Monats oder an den Tagen ausgeführt wird, die durch andere Parameter des erweiterten Zeitplans bestimmt werden. Der Parameter DAYOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFWEEK oder WEEKOFMONTH verwendet wird.

WEEKofmonth
: Gibt die Woche des Monats an, in der der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Eine Woche wird als beliebige 7-Tage-Periode betrachtet, die nicht an einem bestimmten Tag der Woche beginnt. Sie können FIRST, SECOND, THIRD, FOURTH, LAST oder ANY angeben. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan während jeder angegebenen Woche des Monats ausgeführt. Geben mehrere Werte dieselbe Woche an, wird der Zeitplan nur einmal während dieser Woche ausgeführt.

  Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan während jeder Woche des Monats oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter WEEKOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

EXPiration
: Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NEVER. Sie können einen der folgenden Werte angeben:

  Never
  : Gibt an, dass der Zeitplan nie abläuft.

Ablaufdatum
: Gibt das Datum im Format MM/DD/YYYY an, an dem dieser Zeitplan abläuft. Wenn ein Ablaufdatum angegeben wird, läuft der Zeitplan um 23:59:59 Uhr am angegebenen Datum ab.

Beispiel: Einen Zeitplan definieren, um den primären Speicherpool alle zwei Tage zu sichern

Den Zeitplan BACKUP_ARCHIVEPOOL definieren, der den primären Speicherpool ARCHIVEPOOL im Kopienspeicherpool RECOVERYPOOL sichert. Die Sicherung wird um 20:00 Uhr an jedem zweiten Tag ausgeführt.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
active=yes starttime=20:00 period=2
```

Beispiel: Einen Zeitplan definieren, um den primären Speicherpool zweimal im Monat zu sichern

Den Zeitplan BACKUP_ARCHIVEPOOL definieren, der den primären Speicherpool ARCHIVEPOOL im Kopienspeicherpool RECOVERYPOOL sichert. Einen erweiterten Zeitplan auswählen und den Zeitplan am ersten und fünfzehnten Tag des Monats ausführen.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
schedstyle=enhanced dayofmonth=1,15
```

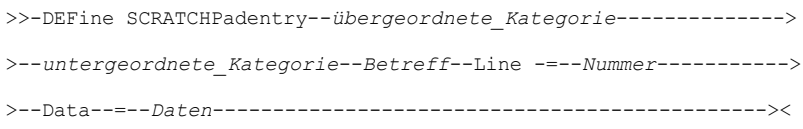
DEFINE SCRATCHPADENTRY (Scratchpadeintrag definieren)

Mit diesem Befehl können Sie Daten in einer neuen Zeile im Scratchpad eingeben. Das Scratchpad ist eine Datenbanktabelle, die sich auf dem Server befindet. Das Scratchpad ermöglicht es Ihnen, verschiedene Informationen in Tabellenformat zu speichern.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

übergeordnete_Kategorie (Erforderlich)
: Gibt die übergeordnete Kategorie an, in der Daten gespeichert werden sollen. Geben Sie eine Textzeichenfolge aus bis zu 100 alphanumerischen Zeichen ein. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

untergeordnete_Kategorie (Erforderlich)
: Gibt die untergeordnete Kategorie an, in der Daten gespeichert werden sollen. Untergeordnete Kategorien sind Abschnitte in übergeordneten Kategorien. Geben Sie eine Textzeichenfolge aus bis zu 100 alphanumerischen Zeichen ein. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Betreff (Erforderlich)
: Gibt den Betreff an, unter dem Daten gespeichert werden sollen. Betreffs sind Abschnitte in untergeordneten Kategorien. Geben Sie eine Textzeichenfolge aus bis zu 100 alphanumerischen Zeichen ein. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Line (Erforderlich)
: Gibt die Nummer der Zeile an, in der Daten gespeichert werden sollen. Zeilen sind Abschnitte in Betreffs. Geben Sie eine ganze Zahl im Bereich von 1 bis 1000 an.

Data (Erforderlich)
: Gibt die Daten an, die in der Zeile gespeichert werden sollen. Sie können bis zu 1000 Zeichen eingeben. Schließen Sie die Daten in Anführungszeichen ein, wenn die Daten ein oder mehrere Leerzeichen enthalten. Bei den Daten muss die Groß-/Kleinschreibung beachtet werden.

Beispiel: Scratchpadeintrag definieren

Geben Sie die Abwesenheitsdaten eines Administrators, Jane, in eine Tabelle ein, in der Informationen zu den Standorten aller Administratoren gespeichert sind.

```
define scratchpadentry admin_info location jane line=2 data=
"Nicht im Büro 1.-15.11."
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SCRATCHPADENTRY

Befehl	Beschreibung
DELETE SCRATCHPADENTRY	Löscht eine Zeile mit Daten aus dem Scratchpad.
QUERY SCRATCHPADENTRY	Zeigt Informationen an, die im Scratchpad enthalten sind.
SET SCRATCHPADRETENTION	Gibt den Zeitraum an, den Scratchpadeinträge aufbewahrt werden.
UPDATE SCRATCHPADENTRY	Aktualisiert Daten in einer Zeile im Scratchpad.

DEFINE SCRIPT (IBM Spectrum Protect-Prozedur definieren)

Mit diesem Befehl kann eine IBM Spectrum Protect-Prozedur definiert oder eine neue IBM Spectrum Protect-Prozedur unter Verwendung des Inhalts aus einer anderen Prozedur erstellt werden.

Mit diesem Befehl kann die erste Zeile für die Prozedur definiert werden. Sollen der Prozedur weitere Zeilen hinzugefügt werden, den Befehl UPDATE SCRIPT verwenden.

Tipps:

- Werden Befehle innerhalb von Prozeduren weitergeleitet, den Server oder die Server-Gruppe in runde Klammern einschließen und den Doppelpunkt übergehen. Enthält die Syntax einen Doppelpunkt, wird der Befehl bei Ausgabe des Befehls RUN nicht weitergeleitet. Stattdessen wird der Befehl nur auf dem Server ausgeführt, von dem aus der Befehl RUN ausgegeben wird.
- Die Ausgabe eines Befehls innerhalb einer IBM Spectrum Protect-Prozedur kann nicht umgeleitet werden. Führen Sie stattdessen die Prozedur aus und geben Sie dann die Befehlsumleitung an. Soll beispielsweise die Ausgabe von script1 in das Verzeichnis c:\temp\test.out übertragen werden, führen Sie wie im folgenden Beispiel die Prozedur aus und geben Sie die Befehlsumleitung an:

  ```
  run script1 > c:\temp\test.out
  ```

Berechtigungsklasse

Für diesen Befehl ist die Bediener-, Maßnahmen-, Speicher- oder Systemberechtigung erforderlich.

Syntax

```
>>-DEFine SCRipt--Prozedurname---------------------------------->

                  .-Line--=--001----.
>--+-Befehlszeile--+-----------------+-+---------------------->
   |               '-Line -=--Nummer-' |
   '-File--=--Dateiname---------------'

>--+-----------------------------+---------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Prozedurname (Erforderlich)
: Gibt den Namen der Prozedur an, die definiert werden soll. Für den Namen können bis zu 30 Zeichen angegeben werden.

Befehlszeile
: Gibt den ersten Befehl an, der in einer Prozedur verarbeitet werden soll. Sie müssen entweder diesen Parameter (und wahlweise den Parameter LINE) oder den Parameter FILE angeben.

  Der angegebene Befehl kann Substitutionsvariablen enthalten und über mehrere Zeilen fortgesetzt werden, wenn als letztes Zeichen in dem Befehl ein Fortsetzungszeichen (-) angegeben wird. Substitutionsvariablen werden mit dem Zeichen '$' gefolgt von einer Zahl angegeben, die den Wert des Parameters angibt, wenn die Prozedur verarbeitet wird. Für die Befehlszeile können bis zu 1200 Zeichen angegeben werden. Den Befehl in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

  Sie können Befehle seriell, parallel oder seriell und parallel auszuführen, indem Sie den Prozedurbefehl SERIAL oder PARALLEL für den Parameter Befehlszeile angeben. Sie können mehrere Befehle parallel ausführen und auf deren Beendigung warten, bevor Sie mit dem nächsten Befehl fortfahren. Befehle werden seriell ausgeführt, bis der parallele Befehl gefunden wird.

  Ablaufanweisungen mit bedingter Logik können verwendet werden. Diese Anweisungen schließen IF, EXIT und GOTO ein.

  Line
  : Gibt die Zeilennummer für die Befehlszeile an. Da Befehle in mehreren Zeilen angegeben werden, wird anhand von Zeilennummern die Reihenfolge der Verarbeitung bestimmt, wenn die Prozedur ausgeführt wird. Die erste Zeile oder Zeile 001 ist der Standardwert. Dieser Parameter ist wahlfrei.

File

Gibt den Namen der Datei an, deren Inhalt in die Prozedur gelesen wird, die definiert werden soll. Die Datei muss sich auf dem Server befinden, auf dem dieser Befehl ausgeführt wird. Wird der Parameter FILE angegeben, kann keine Befehlszeile oder Zeilennummer angegeben werden.

Eine Prozedur kann erstellt werden, indem eine andere Prozedur abgefragt wird und die Parameter FORMAT=RAW und OUTPUTFILE angegeben werden. Die Ausgabe von der Abfrage der Prozedur wird an eine Datei geleitet, die mit dem Parameter OUTPUTFILE angegeben wird. Zum Erstellen der neuen Prozedur wird der Inhalt der zu definierenden Prozedur aus der mit dem Parameter OUTPUTFILE angegebenen Datei eingelesen.

DESCription
Gibt eine Beschreibung für die Prozedur an. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Dieser Parameter ist wahlfrei.

Beispiel: Eine Prozedur schreiben, um AIX-Clients anzuzeigen

Eine Prozedur definieren, die alle AIX-Clients anzeigt.

```
define script qaixc "select node_name from nodes where platform_name='AIX'"
  desc='Display aix clients'
```

Beispiel: Eine Prozedur schreiben und ausführen, um einen Befehl an eine Servergruppe weiterzuleiten

Eine Prozedur definieren und ausführen, die den Befehl QUERY STGPOOL an eine Servergruppe mit dem Namen DEV_GROUP weiterleitet.

```
define script qu_stg "(dev_group) query stgpool"

run qu_stg
```

Beispiel: Eine Prozedur aus einer vorhandenen Prozedur erstellen

Eine Prozedur definieren, deren Befehlszeilen aus einer Datei mit dem Namen MY.SCRIPT gelesen werden, und der neuen Prozedur den Namen AGADM zuordnen. Die Datei muss sich auf dem Server befinden und vom Server gelesen werden.

```
define script agadm file=my.script
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SCRIPT

Befehl	Beschreibung
COPY SCRIPT	Erstellt eine Kopie einer Prozedur.
DELETE SCRIPT	Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur.
QUERY SCRIPT	Zeigt Informationen über Prozeduren an.
RENAME SCRIPT	Vergibt einen neuen Namen für eine Prozedur.
RUN	Führt ein Script aus.
UPDATE SCRIPT	Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.

Zugehörige Konzepte:
Logikablaufanweisungen in einem Script verwenden
Zugehörige Tasks:
Server-Script definieren
Befehle parallel oder seriell ausführen
Tasks gleichzeitig auf mehreren Servern ausführen
Zugehörige Verweise:
Rückkehrcodes für die Verwendung in IBM Spectrum Protect-Scripts

DEFINE SERVER (Server für Übertragung zwischen Servern definieren)

Verwenden Sie diesen Befehl, um einen Server für die Verwendung von Funktionen, wie z. B. virtuelle Datenträger, Knotenreplikation, Befehlsweiterleitung und LAN-unabhängige Datenversetzung, zu definieren.

Mit diesem Befehl kann ein Server für die folgenden Funktionen definiert werden:

- Unternehmensweite Konfiguration
- Unternehmensweite Ereignisprotokollierung
- Befehlsweiterleitung
- Virtuelle Datenträger
- LAN-unabhängige Datenversetzung
- Knotenreplikation

- AIX-BetriebssystemeLinux-BetriebssystemeDatenversetzung mit dem z/OS Media-Server
- Statusüberwachung von fernen Servern
- Alertüberwachung von fernen Servern
- Export zwischen Servern

Wenn Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden, müssen alle Zielserver für LDAP-authentifizierte Kennwörter konfiguriert werden. Auf Daten, die von einem Knoten repliziert werden, der sich mit einem LDAP-Verzeichnisserver authentifiziert, kann nicht zugegriffen werden, wenn der Zielreplikationsserver nicht korrekt konfiguriert ist. Ist Ihr Zielreplikationsserver nicht konfiguriert, können replizierte Daten von einem LDAP-Knoten auf dem Zielserver gespeichert werden. Der Zielreplikationsserver muss jedoch für die Verwendung von LDAP konfiguriert werden, wenn Sie auf die Daten zugreifen möchten.

Die Verwendung von virtuellen Datenträgern wird nicht unterstützt, wenn sich der Quellenserver und der Zielserver auf demselben IBM Spectrum Protect-Server befinden.

Dieser Befehl wird auch verwendet, um einen IBM Spectrum Protect-Speicheragenten zu definieren, als sei er ein Server.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

Für:

- Befehlsweiterleitung
- Statusüberwachung von fernen Servern
- Alertüberwachung von fernen Servern
- Export zwischen Servern

Tipp: Die Befehlsweiterleitung verwendet die ID und das Kennwort des Administrators, der den Befehl ausgibt.

```
>>-DEFine--SERver--Servername--HLAddress--=--IP-Adresse--------->

>--LLAddress--=--TCP-Anschluss--+---------------------+-------->
                                '-COMMmethod--=--TCPIP-'

>--+-------------+--+-----------------------------+------------>
   '-URL--=--URL-'  '-DESCription--=--Beschreibung-'

   .-SSL--=--No------.
>--+-----------------+-------------------------------------------->
   '-SSL--=--+-No--+-'
             '-Yes-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+--------------------------------------+-------------------><
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'
```

Syntax

Für:

- Unternehmensweite Konfiguration
- Unternehmensweite Ereignisprotokollierung
- Speicheragent
- Quellen- und Zielserver für Knotenreplikation
- AIX-BetriebssystemeLinux-Betriebssystemez/OS Media-Server

```
>>-DEFine--SERver--Servername--SERVERPAssword--=--Kennwort------>

>--HLAddress--=--IP-Adresse--LLAddress--=--TCP-Anschluss-------->

>--+----------------------+--+-------------+-------------------->
   '-COMMmethod--=--TCPIP-'  '-URL--=--URL-'

>--+-----------------------------+----------------------------->
   '-DESCription--=--Beschreibung-'

                          (1)
   .-CROSSDEFine--=--No-------. (2)
>--+-------------------------+--------------------------------->
   '-CROSSDEFine--=--+-No--+--'
```

```
                    '-Yes-'

   .-VALIdateprotocol--=--No------.  .-SSL--=--No------.
>--+-------------------------------+--+-----------------+-------->
   '-VALIdateprotocol--=--+-No--+-'  '-SSL--=--+-No--+-'
                          '-All-'              '-Yes-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+-----------------------------------+---------------------->
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'

   .-TRANSFERMethod--=--Tcpip--------.
>--+-------------------------------+------------------------><
   '-TRANSFERMethod--=--+-Tcpip----+-'
                        |      (3) |
                        '-Fasp-----'
```

Anmerkungen:

1. Der Parameter CROSSDEFINE gilt nicht für Speicheragentendefinitionen.
2. Der Parameter VALIDATEPROTOCOL ist veraltet und gilt nur für Speicheragentendefinitionen.
3. Linux-BetriebssystemeDer Parameter TRANSFERMETHOD ist nur auf Betriebssystemen Linux x86_64 verfügbar.

Syntax für virtuelle Datenträger

```
>>-DEFine--SERver--Servername--PAssword--=--Kennwort------------>

>--HLAddress--=--IP-Adresse--LLAddress--=--TCP-Anschluss-------->

>--+----------------------+--+-------------+-------------------->
   '-COMMmethod--=--TCPIP-'  '-URL--=--URL-'

>--+--------------------------+--+--------------------------+----->
   '-DELgraceperiod--=--Tage-'  '-NODEName--=--Knotenname-'

                                    .-SSL--=--No------.
>--+-------------------------------+--+-----------------+-------->
   '-DESCription--=--Beschreibung-'  '-SSL--=--+-No--+-'
                                               '-Yes-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+-----------------------------------+---------------------><
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'
```

Parameter

Servername (Erforderlich)
: Gibt den Namen des Servers an.Dieser Name muss auf dem Server eindeutig sein. Die maximale Länge dieses Namens beträgt 64 Zeichen.

  Für die Ereignisprotokollierung zwischen Servern, die gemeinsame Speicherarchivnutzung,und die Knotenreplikation müssen Sie einen Servernamen angeben, der mit dem Namen übereinstimmt, der mit dem Befehl SET SERVERNAME auf dem Zielserver definiert wurde.

PAssword
: Gibt das Kennwort an, das für die Anmeldung am Zielserver für virtuelle Datenträger verwendet wird. Wenn Sie den Parameter NODENAME angeben, müssen Sie den Parameter PASSWORD angeben. Wird der Parameter PASSWORD, aber nicht der Parameter NODENAME angegeben, wird als Knotenname standardmäßig der Servername verwendet, der mit dem Befehl SET SERVERNAME angegeben wird.

SERVERPAssword
: Gibt das Kennwort des Servers an, der definiert wird. Dieses Kennwort muss mit dem Kennwort übereinstimmen, das mit dem Befehl SET SERVERPASSWORD definiert wird. Dieser Parameter ist für die unternehmensweite Konfiguration und die Ereignisprotokollierung zwischen Servern erforderlich.

HLAddress (Erforderlich)
: Gibt die IP-Adresse des Servers an (in der Schreibweise mit Trennzeichen).

  Verwenden Sie nicht die Loopback-Adresse als Wert dieses Parameters. Virtuelle Datenträger werden nicht unterstützt, wenn der Quellenserver und der Zielserver derselbe IBM Spectrum Protect-Server sind.

LLAddress (Erforderlich)
: Gibt die Adresse der unteren Ebene des Servers an. Diese Adresse stimmt normalerweise mit der Adresse in der Serveroption TCPPORT des Zielservers überein. Bei SSL=YES muss der Anschluss bereits für die SSL-Übertragung auf dem Zielserver definiert sein.

COMMmethod
: Gibt die Übertragungsmethode an, mit der die Verbindung zum Server hergestellt wird. Dieser Parameter ist wahlfrei.

URL
Gibt die URL-Adresse dieses Servers an. Der Parameter ist wahlfrei.

DELgraceperiod
Gibt die Anzahl Tage an, die ein Objekt auf dem Zielserver verbleibt, nachdem es zum Löschen markiert wurde. Sie können einen Wert von 0 bis 9999 angeben. Der Standardwert ist 5. Dieser Parameter ist optional.

NODEName
Gibt einen Knotennamen an, den der Server für die Verbindung zum Zielserver verwenden soll. Dieser Parameter ist wahlfrei. Wenn der Parameter NODENAME angegeben wird, muss auch der Parameter PASSWORD angegeben werden. Wird der Parameter PASSWORD, aber nicht der Parameter NODENAME angegeben, wird als Knotenname standardmäßig der Servername verwendet, der mit dem Befehl SET SERVERNAME angegeben wurde.

DESCription
Gibt eine Beschreibung des Servers an. Der Parameter ist wahlfrei. Die Beschreibung kann bis zu 255 Zeichen umfassen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

CROSSDEFine
Gibt an, ob der Server, der diesen Befehl ausführt, sich selbst für den Server definiert, der durch diesen Befehl angegeben wird. Dieser Parameter ist wahlfrei.
AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeWichtig: Dieser Parameter gilt nicht für Speicheragentdefinitionen.
Wird dieser Parameter angegeben, müssen auch die Befehle SET SERVERNAME, SET SERVERPASSWORD, SET SERVERHLADDRESS, SET CROSSDEFINE und SET SERVERLLADDRESS ausgegeben werden. Der Standardwert ist NO.
Hinweis:

- Für Replikationsoperationen müssen die Namen der Quellen- und Zielreplikationsserver mit den Namen übereinstimmen, die in diesem Befehl angegeben werden.
- CROSSDEFINE kann mit SSL=YES verwendet werden, wenn alle Bedingungen, die für den Parameter SSL=YES angegeben werden, auf dem Quellen- und Zielserver wirksam sind.

Sie können einen der folgenden Werte angeben:

No
Die Querdefinition wird nicht ausgeführt.

Yes
Die Querdefinition wird ausgeführt.

VALIdateprotocol (veraltet)

Gibt an, ob eine zyklische Blockprüfung die Daten validiert, die zwischen dem Speicheragenten und dem IBM Spectrum Protect-Server gesendet werden. Der Parameter ist wahlfrei. Der Standardwert ist NO.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 wird die durch diesen Parameter aktivierte Validierung durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter VALIDATEPROTOCOL wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

SSL
Gibt den Kommunikationsmodus des Servers an. Der Standardwert ist NO.
Wichtig: Ab Version 8.1.2 verwendet der Parameter SSL SSL, um einen Teil der Kommunikation mit dem angegebenen Server zu verschlüsseln, auch wenn SSL=NO definiert ist.
Die folgenden Bedingungen und Hinweise gelten, wenn Sie den Parameter SSL angeben:

- Selbst signierte Zertifikate der Partnerserver müssen sich in der Schlüsseldatenbankdatei (cert.kdb) jedes Servers befinden, bevor die Server gestartet werden.
- Sie können mehrere Servernamen mit verschiedenen Parametern für denselben Zielserver definieren.
- Speicheragenten können den Befehl DSMSTA SETSTORAGESERVER ausgeben und den Parameter SSL einschließen, um die Schlüsseldatenbank zu erstellen.

Sie können einen der folgenden Werte angeben:

No
Gibt eine SSL-Sitzung für die gesamte Kommunikation mit dem angegebenen Server an, außer wenn der Server Objektdaten sendet oder empfängt. Objektdaten werden mithilfe von TCP/IP gesendet und empfangen. Wird ausgewählt, dass die Objektdaten nicht verschlüsselt werden, ähnelt die Serverleistung der Kommunikation über eine TCP/IP-Sitzung und die Sitzung ist sicher.

Yes
Gibt eine SSL-Sitzung für die gesamte Kommunikation mit dem angegebenen Server an, auch wenn der Server Objektdaten sendet und empfängt.

SESSIONSECurity
Gibt an, ob der Server, der definiert wird, die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

STRict

Gibt an, dass die striktesten Sicherheitseinstellungen für den Server, der definiert wird, durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem angegebenen Server und einem IBM Spectrum Protect-Server verwendet.
Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der angegebene Server mit dem IBM Spectrum Protect-Server authentifizieren kann:

- Der Server, der definiert wird, und der IBM Spectrum Protect-Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Server, der definiert wird, muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen sich selbst und dem IBM Spectrum Protect-Server konfiguriert werden.

Server, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem IBM Spectrum Protect-Server authentifizieren.

TRANSitional
: Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Server durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

  Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Server nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Server weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Server jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Server kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Server erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Server nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Server, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Server nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. virtuelle Datenträger, Befehlsweiterleitung oder Export zwischen Servern, wenn sich ein Knoten oder Administrator beim IBM Spectrum Protect-Server als Knoten oder Administrator von einem anderen Server authentifiziert.

Linux-BetriebssystemeTRANSFERMethod
: Linux-BetriebssystemeGibt die Methode an, die für die Datenübertragung zwischen Servern verwendet wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  Tcpip
  : Gibt an, dass TCP/IP für die Übertragung von Daten verwendet wird. Dies ist der Standardwert.

  Fasp
  : Gibt an, dass die Aspera FASP-Technologie (Fast Adaptive Secure Protocol) für die Übertragung von Daten verwendet wird. Mit der Aspera FASP-Technologie kann die Datenübertragung in einem Weitverkehrsnetz (WAN) optimiert werden.
  Einschränkungen:

  - Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie bestimmen, ob die Technologie für Ihre Systemumgebung geeignet ist, und die entsprechenden Lizenzen installieren. Anweisungen finden Sie unter Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann. Wenn die Lizenzen fehlen oder abgelaufen sind, schlagen Datenübertragungsoperationen fehl.
  - Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.
  - Wenn Sie TRANSFERMETHOD=FASP im Befehl PROTECT STGPOOL oder REPLICATE NODE angeben, überschreibt dieser Wert den Parameter TRANSFERMETHOD in den Befehlen DEFINE SERVER und UPDATE SERVER.

Beispiel: Zwei Server definieren, die SSL für die Kommunikation verwenden sollen (manuelle Konfiguration)

Tipp: Wenn beide Server Software der Version 8.1.2 oder höher verwenden, wird SSL automatisch zwischen den Servern konfiguriert und die manuelle Konfiguration ist nicht erforderlich.
Wenn beide Server keine Software der Version 8.1.2 verwenden, müssen Sie die beiden Server manuell für die Verwendung von SSL für die Kommunikation konfigurieren.
Die Serveradressen lauten:

- ServerA befindet sich unter `bfa.tucson.ibm.com`
- ServerB befindet sich unter `bfb.tucson.ibm.com`

Führen Sie die folgenden Schritte aus, um die beiden Server für SSL zu definieren:

1. Geben Sie die Option TCPPORT 1500 für beide Server in der Optionsdatei dsmserv.opt an.
2. Starten Sie beide Server.
3. Fahren Sie beide Server herunter, um das Partnerzertifikat cert256 zu importieren. Für ServerA befindet sich das Zertifikat im Instanzverzeichnis /tsma. Für ServerB befindet sich das Zertifikat im Instanzverzeichnis /tsmb.
4. Starten Sie beide Server. Die Datei /tsma/cert256.arm wird in /tsmb/cert256.bfa.arm unter der Adresse bfb.tucson.ibm.com kopiert. Die Datei /tsmb/cert256.arm wird in /tsmb/cert256.bfb.arm unter der Adresse bfa.tucson.ibm.com kopiert.
5. Geben Sie den folgenden Befehl aus:
   - Auf ServerA:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label "bfb" -file /tsma/cert256.bfb.arm
```

- Auf ServerB:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label "bfa" -file /tsmb/cert256.bfa.arm
```

Sie können auf jedem Server die Zertifikate in der Schlüsseldatenbank anzeigen, indem Sie den folgenden Befehl ausgeben:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

6. Starten Sie die Server erneut.
7. Geben Sie den entsprechenden Befehl DEFINE SERVER aus. Geben Sie für ServerA den folgenden Beispielbefehl aus:

```
DEFINE SERVER BFB hla=bfb.tucson.ibm.com lla=1542
serverpa=Kennwortfürbfb SSL=YES
```

Geben Sie für ServerB den folgenden Beispielbefehl aus:

```
DEFINE SERVER BFA hla=bfa.tucson.ibm.com lla=1542
serverpa=Kennwortfürbfa SSL=YES
```

Wird SSL nicht verwendet, geben Sie den folgenden Beispielbefehl DEFINE SERVER auf ServerA aus:

```
DEFINE SERVER BFBTCP hla=bfb.tucson.ibm.com lla=1500
serverpa=Kennwortfürbfb SSL=NO
```

Wird SSL nicht verwendet, geben Sie den folgenden Beispielbefehl DEFINE SERVER auf ServerB aus:

```
DEFINE SERVER BFATCP hla=bfa.tucson.ibm.com lla=1500
serverpa=Kennwortfürbfa SSL=NO
```

Beispiel: Einen Server für die Kommunikation mit einem anderen Server unter Verwendung der Sitzungssicherheit 'strict' definieren

Einen Server mit dem Namen SERVER1 definieren, um die striktesten Sicherheitseinstellungen für die Authentifizierung mit dem IBM Spectrum Protect-Server zu verwenden.

```
define server server1 sessionsecurity=strict
```

Beispiel: Einen Zielserver definieren

Ein Zielserver hat die Adresse der höheren Ebene 9.116.2.67 und die Adresse der unteren Ebene 1570. Diesen Zielserver für den Quellenserver definieren, den Namen SERVER2 zuordnen und das Kennwort auf SECRET setzen. Angeben, dass Objekte 7 Tage auf dem Zielserver verbleiben, nachdem sie zum Löschen markiert wurden.

```
define server server2 password=secret
  hladdress=9.115.3.45 lladdress=1570 delgraceperiod=7
```

Beispiel: Einen Server definieren, der Befehle von anderen Servern empfängt

Einen Server definieren, der von anderen Servern weitergeleitete Befehle empfangen kann. Dem Server den Namen WEST_COMPLEX zuordnen. Die Adresse der höheren Ebene auf 9.172.12.35, die Adresse der unteren Ebene auf 1500 und die URL-Adresse auf http://west_complex:1580/ setzen.

```
define server west_complex
hladdress=9.172.12.35 lladdress=1500
url=http://west_complex:1580/
```

Beispiel: Zwei Server über Querdefinition definieren

Mit Hilfe der Querdefinition SERVER_A und SERVER_B definieren.

1. Auf SERVER_B den Servernamen, das Kennwort sowie die Adressen der höheren und der unteren Ebene von SERVER_B angeben. Angeben, dass Querdefinitionen zulässig sind.

```
set servername server_b
set serverpassword mylife
set serverhladdress 9.115.20.80
set serverlladdress 1860
set crossdefine on
```

2. Auf SERVER_A den Servernamen, das Kennwort sowie die Adressen der höheren und der unteren Ebene von SERVER_A angeben.

```
set servername server_a
set serverpassword yourlife
```

```
set serverhladdress 9.115.20.97
set serverlladdress 1500
```

3. SERVER_B auf SERVER_A definieren:

```
define server server_b hladdress=9.115.20.80 lladdress=1860
serverpassword=mylife crossdefine=yes
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SERVER

Befehl	Beschreibung
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
AIX-BetriebssystemeLinux-BetriebssystemeDEFINE PATH	AIX-BetriebssystemeLinux-BetriebssystemeDefiniert einen Pfad, wenn das Ziel ein z/OS Media-Server ist.
DELETE DEVCLASS	Löscht eine Einheitenklasse.
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
DELETE SERVER	Löscht die Definition eines Servers.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY SERVER	Zeigt Informationen über Server an.
RECONCILE VOLUMES	Stimmt Definitionen von virtuellen Datenträgern auf dem Quellenserver mit Archivierungsobjekten des Zielservers ab.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
SET CROSSDEFINE	Gibt an, ob Server überkreuz definiert werden sollen.
SET SERVERNAME	Gibt den Namen an, unter dem der Server registriert ist.
SET SERVERHLADDRESS	Gibt die Adresse der höheren Ebene eines Servers an.
SET SERVERLLADDRESS	Gibt die Adresse der unteren Ebene eines Servers an.
SET SERVERPASSWORD	Gibt das Serverkennwort an.
SET REPLSERVER	Gibt einen Zielreplikationsserver an.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.
AIX-BetriebssystemeLinux-BetriebssystemeUPDATE PATH	AIX-BetriebssystemeLinux-BetriebssystemeDefiniert einen Pfad, wenn das Ziel ein z/OS Media-Server ist.
UPDATE SERVER	Aktualisiert Informationen über einen Server.

DEFINE SERVERGROUP (Server-Gruppe definieren)

Mit diesem Befehl kann eine Server-Gruppe definiert werden. Mit einer Servergruppe können Befehle an mehrere Server weitergeleitet werden, indem nur der Gruppenname angegeben wird. Nach der Definition der Servergruppe können mit dem Befehl DEFINE GRPMEMBER Server zur Gruppe hinzugefügt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine SERVERGroup--Gruppenname------------------------------>

>--+------------------------------+--------------------------><
```

```
'-DESCription--=--Beschreibung-'
```

Parameter

Gruppenname (Erforderlich)
: Gibt den Namen der Server-Gruppe an. Die maximale Länge des Namens beträgt 64 Zeichen.

DESCription
: Gibt eine Beschreibung der Server-Gruppe an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

Beispiel: Eine Servergruppe definieren

Die Server-Gruppe WEST_COMPLEX definieren.

```
define servergroup west_complex
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SERVERGROUP

Befehl	Beschreibung
COPY SERVERGROUP	Erstellt eine Kopie einer Servergruppe.
DEFINE GRPMEMBER	Definiert einen Server als Teil einer Servergruppe.
DELETE GRPMEMBER	Löscht einen Server aus einer Servergruppe.
DELETE SERVERGROUP	Löscht eine Servergruppe.
MOVE GRPMEMBER	Versetzt einen Teil einer Servergruppe.
QUERY SERVERGROUP	Zeigt Informationen über Servergruppen an.
RENAME SERVERGROUP	Benennt eine Servergruppe um.
UPDATE SERVERGROUP	Aktualisiert eine Servergruppe.

DEFINE SPACETRIGGER (Speicherbereichsauslöser definieren)

Mit diesem Befehl können Einstellungen für Auslöser definiert werden, die festlegen, wann und wie der Server zusätzlichen Speicherbereich vorbereitet, wenn vordefinierte Schwellen in Speicherpools, die die Einheitenklassen FILE und DISK verwenden, überschritten werden. Speicherbereichsauslöser werden für Speicherpools mit dem Parameter RECLAMATIONTYPE=SNAPLOCK nicht aktiviert.

Der IBM Spectrum Protect-Server ordnet weiteren Speicherbereich zu, wenn die Speicherauslastung einen angegebenen Wert erreicht. Nachdem weiterer Speicherbereich zugeordnet wurde, fügt der Server den Speicherbereich dem angegebenen Pool hinzu (Platte mit wahlfreiem Zugriff oder sequenziellem Zugriff).

Wichtig: Bei Speicherbereichsauslöserfunktionen und Berechnungen des Speicherbereichs im Speicherpool wird der Speicherbereich berücksichtigt, der in jedem Verzeichnis verbleibt. Eine ungenaue Berechnung kann zu einem Fehler bei der Erweiterung des Speicherbereichs führen, der in einem Speicherpool verfügbar ist. Ein Fehler bei der Erweiterung des Speicherbereichs in einem Speicherpool ist eine der Bedingungen, die zur Inaktivierung eines Auslösers führen kann.

Wenn Sie beispielsweise mehrere Verzeichnisse für eine Einheitenklasse angeben und sich die Verzeichnisse in demselben Dateisystem befinden, berechnet der Server den Speicherbereich durch Hinzufügen von Werten, die den Speicherbereich darstellen, der in jedem Verzeichnis verbleibt. Diese Speicherbereichsberechnungen sind ungenau. Anstatt einen Speicherpool mit ausreichend Speicherbereich für eine Operation auszuwählen, kann der Server das Verzeichnis auswählen, das für die Einheitenklasse angegeben ist, und frühzeitig über keinen Speicherbereich mehr verfügen.

Um mögliche Probleme zu vermeiden und eine genaue Berechnung sicherzustellen, sollten Sie jedem Verzeichnis ein separates Dateisystem zuordnen. Wird ein Auslöser inaktiviert, da der Speicherbereich in einem Speicherpool nicht erweitert werden konnte, können Sie den Auslöser erneut aktivieren, indem Sie den folgenden Befehl angeben: `update spacetrigger stg`. Es sind keine weiteren Änderungen an dem Speicherbereichsauslöser erforderlich.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
                                .-Fullpct---=---80------.
>>-DEFine SPACETrigger----STG----+---------------------+-------->
```

```
                                '-Fullpct----Prozent-'

   .-SPACEexpansion----20------.
>--+---------------------------+------------------------------>
   '-SPACEexpansion----Prozent-'

>--+---------------------------+------------------------------>
   '-EXPansionprefix-----Präfix-'

>--+-----------------------------+---------------------------><
   '-STGPOOL-----Speicherpoolname-'
```

Parameter

STG
: Gibt einen Speicherbereichsauslöser für den Speicherpool an.

Fullpct
: Dieser Parameter gibt den Auslastungsprozentsatz des Speicherpools an. Dieser Parameter ist wahlfrei. Geben Sie einen ganzzahligen Wert von 0 bis 99 an. Der Standardwert ist 80. Der Wert 0 inaktiviert den Speicherbereichsauslöser.Wird dieser Wert überschritten, erstellt der Speicherbereichsauslöser neue Datenträger. Bei Überschreiten der Schwelle werden neue Datenträger möglicherweise erst bei der nächsten Anforderung von Speicherbereich erstellt.

  Sie können die Auslastung des Speicherpools bestimmen, indem Sie den Befehl QUERY STGPOOL mit FORMAT=DETAILED ausgeben. Der Prozentsatz der Speicherpoolauslastung wird im Feld "Ausl. für Speicherbereichsauslöser" angezeigt. Die Berechnung dieses Prozentsatzes schließt keine potenziellen Arbeitsdatenträger ein. Die Berechnung der prozentualen Auslastung, die für die Umlagerung und Wiederherstellung verwendet wird, schließt jedoch potenzielle Arbeitsdatenträger ein.

SPACEexpansion
: Für Speicherpools des Typs FILE mit sequenziellem Zugriff wird dieser Parameter bei der Bestimmung der Anzahl zusätzlicher Datenträger verwendet, die in dem Speicherpool erstellt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist 20. Datenträger werden unter Verwendung des Werts für MAXCAPACITY aus der Einheitenklasse des Speicherpools erstellt. Für DISK-Speicherpools mit wahlfreiem Zugriff erstellt der Speicherbereichsauslöser einen einzelnen Datenträger unter Verwendung von EXPANSIONPREFIX.

EXPansionprefix
: Für DISK-Speicherpools mit wahlfreiem Zugriff gibt dieser Parameter das Präfix an, das der Server zum Erstellen neuer Speicherpooldateien verwendet. Dieser Parameter ist wahlfrei und gilt nur für Einheitenklassen DISK mit wahlfreiem Zugriff. Das Standardpräfix ist der Serverinstallationspfad.
  Das Präfix kann ein oder mehrere Verzeichnistrennzeichen enthalten. Beispiel:  AIX-Betriebssysteme  Linux-Betriebssysteme

  ```
  /opt/tivoli/tsm/server/bin/
  ```

   Windows-Betriebssysteme

  ```
  c:\Programme\tivoli\tsm\
  ```

   AIX-Betriebssysteme  Linux-BetriebssystemeEs können bis zu 250 Zeichen angegeben werden. Wird ein ungültiges Präfix angegeben, kann die automatische Erweiterung fehlschlagen.

   Windows-BetriebssystemeSie können bis zu 200 Zeichen angeben. Wird ein ungültiges Präfix angegeben, kann die automatische Erweiterung fehlschlagen.Wird der Server als Windows-Dienst ausgeführt, ist das Standardpräfix das Verzeichnis c:\wnnt\system32.

  Dieser Parameter ist für Speicherbereichsauslöser für FILE-Speicherpools mit sequenziellem Zugriff nicht gültig. Es werden Präfixe der Verzeichnisse verwendet, die mit der zugeordneten Einheitenklasse angegeben werden.

STGPOOL
: Gibt den Speicherpool an, der diesem Speicherbereichsauslöser zugeordnet ist. Dieser Parameter ist für Speicherbereichsauslöser für den Speicherpool wahlfrei. Wird der Parameter STG angegeben, aber der Parameter STGPOOL nicht angegeben, wird ein Speicherbereichsauslöser erstellt, der für alle DISK-Speicherpools mit wahlfreiem Zugriff und alle FILE-Speicherpools mit sequenziellem Zugriff gilt, die keinen spezifischen Speicherbereichsauslöser haben.

  Dieser Parameter gilt nicht für Speicherpools mit dem Parameter RECLAMATIONTYPE=SNAPLOCK.

Beispiel: Einen Speicherbereichsauslöser definieren, um den Speicherbereich im Speicherpool um 25 Prozent zu erhöhen

Einen Speicherbereichsauslöser für den Speicherpool definieren, um den Speicherbereich in einem Speicherpool um 25 Prozent zu vergrößern, wenn der Speicherpool zu 80 Prozent mit vorhandenen Datenträgern belegt ist. Speicherbereich wird in den Verzeichnissen erstellt, die der Einheitenklasse zugeordnet sind.

```
define spacetrigger stg spaceexpansion=25 stgpool=file
```

Beispiel: Einen Speicherbereichsauslöser definieren, um den Speicherbereich im Speicherpool um 40 Prozent zu erhöhen

Einen Speicherbereichsauslöser für den Speicherpool WINPOOL1 definieren, um den Speicherbereich in dem Speicherpool um 40 Prozent zu vergrößern, wenn der Speicherpool zu 80 Prozent mit vorhandenen Datenträgern belegt ist.

```
define spacetrigger stg spaceexpansion=40 stgpool=winpool1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SPACETRIGGER

Befehl	Beschreibung
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
DELETE SPACETRIGGER	Löscht den Speicherbereichsauslöser für den Speicherpool.
QUERY SPACETRIGGER	Zeigt Informationen zu einem Speicherbereichsauslöser für den Speicherpool an.
UPDATE SPACETRIGGER	Ändert Attribute des Speicherbereichsauslösers für den Speicherpool.

DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)

Mit diesem Befehl können Sie einen neuen Schwellenwert für die Statusüberwachung definieren.

Mit Statusüberwachungsschwellenwerten werden die definierten Bedingungen mit den Serverabfragen für die Statusüberwachung verglichen und die Ergebnisse in die Statusüberwachungstabelle eingefügt.

Es können mehrere Schwellenwerte für eine Aktivität definiert werden. Sie können beispielsweise einen Schwellenwert erstellen, der einen Warnstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 80 % ist. Sie können dann einen anderen Schwellenwert erstellen, der einen Fehlerstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 90 % ist.

Anmerkung: Wenn bereits ein Schwellenwert für eine Bedingung EXISTS definiert ist, können Sie keinen anderen Schwellenwert mit einem der anderen Bedingungstypen definieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine STAtusthreshold--Schwellenwertname--Aktivität--------->

   .-Condition--=--EXists-----.
>--+--------------------------+--+----------------+------------->
   '-Condition--=--+-EXists-+-'  '-Value--=--Wert-'
                   +-GT-----+
                   +-GE-----+
                   +-LT-----+
                   +-LE-----+
                   '-EQual--'

   .-STatus--=--Normal------.
>--+----------------------+---------------------------------><
   '-STatus--=--+-Normal--+-'
                +-Warning-+
                '-Error---'
```

Parameter

Schwellenwertname (Erforderlich)
: Gibt den Schwellenwertnamen an. Der Name darf 48 Zeichen nicht überschreiten.

Aktivität (Erforderlich)
: Gibt die Aktivität an, für die Statusanzeiger erstellt werden sollen. Geben Sie einen der folgenden Werte an:

  PROCESSSUMMARY
  : Gibt die Anzahl Prozesse an, die gegenwärtig aktiv sind.

  SESSIONSUMMARY

Gibt die Anzahl Sitzungen an, die gegenwärtig aktiv sind.

CLIENTSESSIONSUMMARY
: Gibt die Anzahl Clientsitzungen an, die gegenwärtig aktiv sind.

SCHEDCLIENTSESSIONSUMMARY
: Gibt die Anzahl geplanter Clientsitzungen an.

DBUTIL
: Gibt die prozentuale Datenbankauslastung an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

DBFREESPACE
: Gibt den freien Speicherbereich in Gigabyte an, der in der Datenbank verfügbar ist.

DBUSEDSPACE
: Gibt den verwendeten Datenbankbereich in Gigabyte an.

ARCHIVELOGFREESPACE
: Gibt den freien Speicherbereich in Gigabyte an, der im Archivprotokoll verfügbar ist.

STGPOOLUTIL
: Gibt die prozentuale Auslastung des Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

STGPOOLCAPACITY
: Gibt die Speicherpoolkapazität in Gigabyte an.

AVGSTGPOOLUTIL
: Gibt die durchschnittliche prozentuale Speicherpoolauslastung für alle Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

TOTSTGPOOLCAPACITY
: Gibt die Gesamtspeicherpoolkapazität in Gigabyte für alle verfügbaren Speicherpools an.

TOTSTGPOOLS
: Gibt die Anzahl der definierten Speicherpools an.

TOTRWSTGPOOLS
: Gibt die Anzahl der definierten Speicherpools an, die lesbar oder änderbar sind.

TOTNOTRWSTGPOOLS
: Gibt die Anzahl der definierten Speicherpools an, die nicht lesbar oder änderbar sind.

STGPOOLINUSEANDDEFINED
: Gibt die Gesamtzahl der definierten Datenträger an, die im Gebrauch sind.

ACTIVELOGUTIL
: Gibt die aktuelle prozentuale Auslastung der aktiven Protokolldatei an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

ARCHLOGUTIL
: Gibt die aktuelle Auslastung des Archivprotokolls an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

CPYSTGPOOLUTIL
: Gibt die prozentuale Auslastung eines Kopienspeicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

PMRYSTGPOOLUTIL
: Gibt die prozentuale Auslastung eines primären Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

DEVCLASSPCTDRVOFFLINE
: Gibt die prozentuale Auslastung von Laufwerken an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTDRVPOLLING
: Gibt den Sendeaufruf für Laufwerke nach Einheitenklasse an. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTLIBPATHSOFFLINE
: Gibt die Kassettenarchivpfade an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTPATHSOFFLINE
: Gibt den Prozentsatz der Einheitenklassenpfade an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTDISKSNOTRW
: Gibt den Prozentsatz der Platten an, die für die Einheitenklasse DISK nicht beschreibbar sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTDISKSUNAVAILABLE
: Gibt den Prozentsatz der Plattendatenträger an (nach Einheitenklasse), die nicht verfügbar sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

FILEDEVCLASSPCTSCRUNALLOCATABLE
: Gibt den Prozentsatz der Arbeitsdatenträger an, die der Server für eine bestimmte Einheitenklasse FILE, die nicht gemeinsam genutzt wird, nicht zuordnen kann. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

Condition

Gibt die Bedingung an, die verwendet wird, um die Aktivitätsausgabe mit dem angegebenen Wert zu vergleichen. Der Standardwert ist EXISTS. Geben Sie einen der folgenden Werte an:

EXists
: Erstellt einen Statusüberwachungsanzeiger, wenn die Aktivität vorhanden ist.

GT
: Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis größer als der angegebene Wert ist.

GE
: Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis größer-gleich dem angegebenen Wert ist.

LT
: Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis kleiner als der angegebene Wert ist.

LE
: Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis kleiner-gleich dem angegebenen Wert ist.

EQual
: Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis gleich dem angegebenen Wert ist.

Value (Erforderlich)
: Gibt den Wert an, der mit der Aktivitätsausgabe für die angegebene Bedingung verglichen wird. Sie müssen diesen Parameter angeben, wenn CONDITION nicht auf EXISTS gesetzt ist. Sie können eine ganze Zahl im Bereich von 0 bis 999999999999999 angeben.

STatus
: Gibt den Status des Anzeigers an, der bei der Statusüberwachung erstellt wird, wenn die Bedingung, die ausgewertet wird, erfüllt ist. Dieser optionale Parameter hat den Standardwert NORMAL. Geben Sie einen der folgenden Werte an:

Normal
: Gibt an, dass der Statusanzeiger einen normalen Statuswert hat.

Warnung
: Gibt an, dass der Statusanzeiger einen Warnstatuswert hat.

Fehler
: Gibt an, dass der Statusanzeiger einen Fehlerstatuswert hat.

Statusschwellenwert definieren

Mit dem folgenden Befehl einen Statusschwellenwert für die durchschnittliche prozentuale Speicherpoolauslastung definieren:

```
define statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=85 condition=gt status=warning
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE STATUSTHRESHOLD

Befehl	Beschreibung
DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)	Löscht einen Schwellenwert für die Statusüberwachung.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)	Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.
UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)	Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.

DEFINE STGPOOL (Speicherpool definieren)

Mit diesem Befehl kann ein primärer Speicherpool, ein Kopienspeicherpool, ein Pool für aktive Daten, ein Verzeichniscontainerspeicherpool, ein Containerkopienspeicherpool oder ein Containerspeicherpool in einer Cloudumgebung definiert werden.

Ein primärer Speicherpool stellt einen Zielort für Sicherungsdateien, Archivierungsdateien oder Dateien zur Verfügung, die von Clientknoten umgelagert werden. Ein Kopienspeicherpool stellt einen Zielort für Kopien von Dateien zur Verfügung, die sich in primären Speicherpools befinden. Ein Pool für aktive Daten stellt einen Zielort für aktive Versionen von Sicherungsdaten zur Verfügung, die sich in primären Speicherpools befinden. Ein Containerspeicherpool stellt ein Ziel für deduplizierte Dateien bereit. Ein Cloudspeicherpool stellt Speicher in einer Cloudumgebung bereit. Ein Containerkopienspeicherpool stellt eine Bandkopie eines Verzeichniscontainerspeicherpools bereit. Die maximale Anzahl der Speicherpools, die für einen Server definiert werden kann, beträgt 999.

Alle Datenträger in einem Speicherpool gehören zu derselben Einheitenklasse. Speicherpools mit wahlfreiem Zugriff verwenden den Einheitentyp DISK. Nach der Definition eines Speicherpools mit wahlfreiem Zugriff müssen Datenträger für den Pool definiert werden, um Speicherbereich zu erstellen.

Speicherpools mit sequenziellem Zugriff verwenden Einheitenklassen, die Sie für Bandeinheiten, Dateien auf Platte (Einheitentyp FILE) und Speicher auf einem anderen Server (Einheitentyp SERVER) definieren. Zum Erstellen von Speicherbereich in einem Speicherpool mit sequenziellem Zugriff müssen Arbeitsdatenträger für den Pool zugelassen werden, wenn dieser definiert oder aktualisiert wird, oder es müssen Datenträger für den Pool definiert werden, nachdem der Pool definiert wurde. Es können auch beide Vorgehensweisen verwendet werden.

Einschränkung: Wenn ein Client die Funktion für gleichzeitiges Schreiben und die Datendeduplizierung verwendet, wird das Feature für die Datendeduplizierung während der Ausführung von Sicherungen in einem Speicherpool inaktiviert.

Der Befehl DEFINE STGPOOL verwendet sieben Formen. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für DEFINE STGPOOL

Befehl	**Beschreibung**
BACKUP DB	Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff.
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
DEFINE COLLOCGROUP	Definiert eine Kollokationsgruppe.
DEFINE COLLOCMEMBER	Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
DEFINE STGPOOLDIRECTORY	Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
DELETE COLLOCGROUP	Löscht eine Kollokationsgruppe.
DELETE COLLOCMEMBER	Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.
DELETE STGPOOL	Löscht einen Speicherpool aus dem Serverspeicher.
MOVE DATA	Versetzt Daten aus einem angegebenen Speicherpooldatenträger in einen anderen Speicherpooldatenträger.
MOVE MEDIA	Versetzt Speicherpooldatenträger, die von einem automatisierten Kassettenarchive verwaltet werden.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
QUERY DEVCLASS	Zeigt Informationen zu Einheitenklassen an.
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY SHREDSTATUS	Zeigt Informationen zu Daten an, die auf das Schreddern warten.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
RENAME STGPOOL	Benennt einen Speicherpool um.
REPAIR STGPOOL	Repariert einen Verzeichniscontainerspeicherpool.
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.
RESTORE STGPOOL	Schreibt Dateien aus Kopienspeicherpools in einen primären Speicherpool zurück.

Befehl	Beschreibung
RESTORE VOLUME	Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopienspeicherpools zurück.
SET DRMPRIMSTGPOOL	Gibt an, dass primäre Speicherpools von DRM verwaltet werden.
SHRED DATA	Startet manuell den Prozess zum Schreddern gelöschter Daten.
UPDATE COLLOCGROUP	Aktualisiert die Beschreibung einer Kollokationsgruppe.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

- DEFINE STGPOOL (Cloud-Containerspeicherpool definieren)
  Mit diesem Befehl können Sie einen Containerspeicherpool in einer Cloudumgebung definieren. Dieser Typ des Speicherpools wird für die Datendeduplizierung verwendet. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.
- DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren)
  Mit diesem Befehl kann ein Verzeichniscontainerspeicherpool definiert werden, der für die Datendeduplizierung verwendet wird.
- DEFINE STGPOOL (Containerkopienspeicherpool definieren)
  Mit diesem Befehl kann ein Containerkopienspeicherpool definiert werden, in dem eine Kopie der Daten aus einem Verzeichniscontainerspeicherpool gespeichert wird.
- DEFINE STGPOOL (Primären Speicherpool definieren, der Einheiten mit wahlfreiem Zugriff zugeordnet wird)
  Mit diesem Befehl kann ein primärer Speicherpool definiert werden, der Einheiten mit wahlfreiem Zugriff zugeordnet wird.
- DEFINE STGPOOL (Primären Speicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)
  Mit diesem Befehl kann ein primärer Speicherpool definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.
- DEFINE STGPOOL (Kopienspeicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)
  Mit diesem Befehl kann ein Kopienspeicherpool definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.
- DEFINE STGPOOL (Pool für aktive Daten definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)
  Mit diesem Befehl kann ein Pool für aktive Daten definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.

DEFINE STGPOOL (Cloud-Containerspeicherpool definieren)

Mit diesem Befehl können Sie einen Containerspeicherpool in einer Cloudumgebung definieren. Dieser Typ des Speicherpools wird für die Datendeduplizierung verwendet. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.

Tipp: Um die Sicherungs- und Archivierungsleistung zu optimieren, definieren Sie eines oder mehrere lokale Speicherverzeichnisse zum temporären Speichern von Daten, die von IBM Spectrum Protect in die Cloud übertragen werden. Nachdem Sie mit dem Befehl DEFINE STGPOOL einen Cloud-Containerspeicherpool definiert haben, verwenden Sie den Befehl DEFINE STGPOOLDIRECTORY, um dem Cloud-Containerspeicherpool lokale Speicherverzeichnisse zuzuordnen. Weitere Informationen finden Sie in Leistung für Cloudobjektspeicher optimieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine STGpool--Poolname--STGType--=--CLoud------------------>

   .-POoltype--=--PRimary-.
>--+----------------------+--+-------------------------------+--->
   '-POoltype--=--PRimary-'  '-DESCription--=--Beschreibung-'

   .-CLOUDType--=--SWift---------.
>--+-----------------------------+--CLOUDUrl--=--Cloud-URL------>
   '-CLOUDType--=--+-AZure-----+-'
                   +-S3--------+
                   +-SOftlayer-+
                   +-SWift-----+
                   '-V1Swift---'

                        (1)
>--IDentity--=--Cloud-ID------PAssword--=--Kennwort------------->

   .-CLOUDLocation--=--OFfpremise-----.
>--+---------------------------------+------------------------->
   '-CLOUDLocation--=--+-OFfpremise-+-'
                       '-ONpremise--'

>--+-------------------------------+--------------------------->
   |                           (2) |
   '-BUCKETName--=--Bucketname-----'
```

```
   .-ACCess--=--READWrite-------.
>--+----------------------------+------------------------------->
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                '-UNAVailable-'

   .-MAXWriters--=--NOLimit--------------------.
>--+----------------------------------------+---------------->
   '-MAXWriters--=--+-NOLimit----------------+-'
                    '-maximale_Anzahl_Writer-'

   .-REUsedelay--=--1----.  .-ENCRypt--=--Yes---------.
>--+--------------------+--+-------------------------+--------->
   '-REUsedelay--=--Tage-'  |                     (3) |
                            '-ENCRypt--=--+-Yes-+-----'
                                          '-No--'

   .-COMPRession--=--Yes-----.
>--+-------------------------+-------------------------------><
   '-COMPRession--=--+-Yes-+-'
                     '-No--'
```

Anmerkungen:

1. Wenn Sie CLOUDTYPE=AZURE angegeben haben, geben Sie nicht den Parameter IDENTITY an.
2. Dieser Parameter ist nur gültig, wenn Sie CLOUDTYPE=S3 angeben.
3. Der Standardwert des Parameters ENCRYPT ist bedingt. Der Server verschlüsselt Daten standardmäßig, wenn der Parameter CLOUDLOCATION auf OFFPREMISE gesetzt ist. Wenn der Parameter CLOUDLOCATION auf ONPREMISE gesetzt ist, ist der Standardwert No.

Parameter

Poolname (Erforderlich)
: Gibt den Cloudspeicherpool an, der definiert werden soll. Dieser Parameter ist erforderlich. Die maximale Länge des Namens beträgt 30 Zeichen.

STGType=CLoud (Erforderlich)
: Gibt den Typ des Speichers an, der für einen Cloudspeicherpool definiert werden soll. Um sicherzustellen, dass der Speicherpool in einer Cloudumgebung verwendet werden kann, müssen Sie STGTYPE=CLOUD angeben.
Tipp: Um die Leistung zu optimieren, definieren Sie ein oder mehrere lokale Speicherverzeichnisse zum temporären Speichern von Daten, die in die Cloud versetzt werden. Verwenden Sie nach der Definition eines Cloud-Containerspeicherpools den Befehl DEFINE STGPOOLDIRECTORY, um dem Cloud-Containerspeicherpool lokale Verzeichnisse zuzuordnen.

POoltype=PRimary
: Gibt an, dass ein primärer Speicherpool definiert werden soll. Dieser Parameter ist wahlfrei.

DESCription
: Gibt eine Beschreibung des Cloudspeicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

CLOUDType
: Gibt den Typ der Cloudumgebung an, in der der Speicherpool konfiguriert wird.
Sie können einen der folgenden Werte angeben:

  AZure
  : Gibt an, dass der Speicherpool ein Cloud-Computing-System 'Microsoft Azure' verwendet.

  S3
  : Gibt an, dass der Speicherpool ein Cloud-Computing-System mit dem Protokoll 'Simple Storage Service' (S3) verwendet, wie z. B. IBM® Cloud Object Storage oder Amazon Web Services (AWS) S3. Wenn Sie einen Speicherpool für die Verwendung von S3 mit diesem Parameter definieren, können Sie später den Speicherpooltyp mithilfe des Befehls UPDATE STGPOOL nicht ändern.

  SOftlayer
  : Gibt an, dass der Speicherpool ein Cloud-Computing-System 'IBM SoftLayer' mit Swift verwendet.

  SWift
  : Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 2 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

  V1Swift
  : Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 1 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

  Dieser Parameter ist wahlfrei. Wird der Parameter nicht angegeben, wird der Standardwert SWIFT verwendet.

CLOUDUrl

Gibt die URL der Cloudumgebung an, in der der Speicherpool konfiguriert wird. Auf der Basis Ihres Cloud-Providers können Sie einen BLOB-Dienstendpunkt, eine Regionsendpunkt-URL, eine Accesser-IP-Adresse, einen Endpunkt für öffentliche Authentifizierung (Public Authentication Endpoint) oder einen ähnlichen Wert für diesen Parameter verwenden. Stellen Sie sicher, dass das Protokoll wie z. B. `https://` oder `http://` am Anfang der URL eingefügt wird. Die maximale Länge der Webadresse beträgt 870 Zeichen. Der Parameter CLOUDURL wird erst geprüft, wenn die erste Sicherung beginnt.
Weitere Informationen zum Ermitteln dieser Werte erhalten Sie, wenn Sie Ihren Cloud-Service-Provider in der Liste auf der Seite Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren auswählen.
Tipp: Um mehrere IBM Cloud Object Storage-Accesser zu verwenden, listen Sie die Accesser-IP-Adressen getrennt durch einen vertikalen Balken (|) ohne Leerzeichen auf. Beispiel: *CLOUDURL=<Accesser-URL1>|<Accesser-URL2>|<Accesser-URL3>*. Falls Sie das Operations Center verwenden, geben Sie im Feld URL des Assistenten 'Speicherpool hinzufügen' eine Accesser-IP-Adresse ein und drücken Sie dann die Eingabetaste, um weitere IP-Adressen hinzuzufügen. Die Verwendung mehrerer Accesser verbessert die Leistung.
Dieser Parameter ist erforderlich, wenn Sie den Parameter CLOUDTYPE angeben.

- AZure
- S3 (Simple Storage Service)
- SOftlayer
- SWift
- V1Swift

IDentity
: Gibt die Benutzer-ID für die Cloud an, die im Parameter STGTYPE=CLOUD angegeben ist. Dieser Parameter ist für alle unterstützten Cloud-Computing-Systeme außer Azure erforderlich. Wenn Sie CLOUDTYPE=AZURE angegeben haben, geben Sie nicht den Parameter IDENTITY an. Auf der Basis Ihres Cloud-Providers können Sie eine Zugriffsschlüssel-ID, einen Benutzernamen, einen Tenantnamen und Benutzernamen oder einen ähnlichen Wert für diesen Parameter verwenden. Die maximale Länge der Benutzer-ID beträgt 255 Zeichen.

PAssword (Erforderlich)
: Gibt das Kennwort für die Cloud an, die im Parameter STGTYPE=CLOUD angegeben ist. Auf der Basis Ihres Cloud-Providers können Sie ein SAS-Token (SAS = Shared Access Signature), einen geheimen Zugriffsschlüssel, einen API-Schlüssel, ein Kennwort oder einen ähnlichen Wert für diesen Parameter verwenden. Dieser Parameter ist erforderlich. Die maximale Länge des Kennworts beträgt 255 Zeichen. Die Parameter IDENTITY und PASSWORD werden erst geprüft, wenn die erste Sicherung beginnt.

CLOUDLocation
: Gibt die physische Position der Cloud an, die im Parameter CLOUD angegeben ist. Dieser Parameter ist wahlfrei. Der Standardwert ist OFFPREMISE. Sie können einen der folgenden Werte angeben:

- OFfpremise
- ONpremise

BUCKETName
: Gibt den Namen für ein AWS S3-Bucket oder eine IBM Cloud Object Storage-Vault an, das bzw. die anstelle des Standardbuckets oder der Standardvault mit diesem Speicherpool verwendet werden soll. Dieser Parameter ist optional und ist nur gültig, wenn Sie CLOUDTYPE=S3 angeben. Wenn der von Ihnen angegebene Name nicht vorhanden ist, erstellt der Server ein Bucket oder eine Vault mit dem angegebenen Namen, bevor das Bucket bzw. die Vault verwendet wird. Beachten Sie die Einschränkungen Ihres Cloud-Providers bei der Benennung, wenn Sie diesen Parameter angeben. Überprüfen Sie die Berechtigungen für das Bucket oder die Vault und stellen Sie sicher, dass die Berechtigungsnachweise für diesen Speicherpool über die Berechtigung zum Lesen, Schreiben, Auflisten und Löschen von Objekten in diesem Bucket oder dieser Vault haben. Wenn Sie die Berechtigungen nicht ändern oder anzeigen können und nicht bereits Daten in diesen Speicherpool geschrieben wurden, verwenden Sie den Befehl UPDATE STGPOOL mit dem Parameter BUCKETNAME, um ein anderes Bucket oder eine andere Vault zu verwenden.

ACCess
: Gibt an, wie Clientknoten und Serverprozesse auf den Cloudspeicherpool zugreifen. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Sie können einen der folgenden Werte angeben:

  READWrite
  : Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff für den Cloudspeicherpool haben. Dieser Wert ist der Standardwert.

  READOnly
  : Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff für den Cloudspeicherpool haben.

  UNAVailable
  : Gibt an, dass Clientknoten und Serverprozesse nicht auf den Cloudspeicherpool zugreifen können.

MAXWriters
: Gibt die maximale Anzahl der Schreibsitzungen an, die gleichzeitig für den Cloudspeicherpool ausgeführt werden können. Geben Sie eine maximale Anzahl von Schreibsitzungen an, um zu steuern, dass die Leistung des Cloudspeicherpools keine negativen Auswirkungen auf andere Systemressourcen hat. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können einen der folgenden Werte angeben:

  NOLimit
  : Gibt an, dass für die Anzahl der Writer, die Sie verwenden können, kein Grenzwert für die maximale Größe vorhanden ist. Dieser Wert ist der Standardwert.

  maximale_Anzahl_Writer
  : Begrenzt die maximale Anzahl der Writer, die Sie verwenden können. Geben Sie eine ganze Zahl im Bereich von 1 bis 99999 an.

REUsedelay

Gibt die Anzahl Tage an, die verstreichen müssen, nachdem alle deduplizierten Speicherbereiche aus einem Cloudspeicherpool entfernt wurden. Dieser Parameter steuert die Dauer, die deduplizierte Speicherbereiche einem Cloudspeicherpool zugeordnet sind. Wenn der für den Parameter angegebene Wert abläuft, werden die deduplizierten Speicherbereiche aus dem Cloudspeicherpool gelöscht. Der Standardwert ist 1. Sie können einen der folgenden Werte angeben:

1
: Gibt an, dass deduplizierte Speicherbereiche nach 1 Tag aus einem Cloudspeicherpool gelöscht werden. Dieser Wert ist der Standardwert.

Tage
: Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben.

Tipp: Setzen Sie diesen Parameter auf einen Wert, der größer als die für den Befehl SET DRMDBBACKUPEXPIREDAYS angegebene Anzahl ist. Wird dieser Parameter auf einen höheren Wert gesetzt, können Sie sicherstellen, dass Verweise auf Dateien im Cloudspeicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird.

ENCRypt
: Gibt an, ob der Server Clientdaten verschlüsselt, bevor er sie in den Speicherpool schreibt. Sie können die folgenden Werte angeben:

Yes
: Gibt an, dass Clientdaten vom Server verschlüsselt werden.

No
: Gibt an, dass Clientdaten nicht vom Server verschlüsselt werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist von der physischen Position der Cloud abhängig, die durch den Parameter CLOUDLOCATION angegeben wird. Wenn sich die Cloud außerhalb des Unternehmens (off premise) befindet, werden Daten standardmäßig vom Server verschlüsselt. Wenn sich die Cloud vor Ort (on premises) befindet, werden Daten standardmäßig nicht vom Server verschlüsselt.

COMPRession
: Gibt an, ob Daten in dem Speicherpool komprimiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No
: Gibt an, dass Daten in dem Speicherpool nicht komprimiert werden.

Yes
: Gibt an, dass Daten in dem Speicherpool komprimiert werden. Dies ist der Standardwert.

Beispiel 1: Einen OpenStack Swift-Cloudspeicherpool definieren

Einen OpenStack Swift-Cloudspeicherpool mit dem Namen STGPOOL1 definieren.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password description="OpenStack Swift cloud"
```

Beispiel 2: Einen primären Cloudspeicherpool definieren

Einen primären Cloudspeicherpool mit dem Namen STGPOOL1 definieren.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password pooltype=primary
```

Beispiel 3: Einen Cloudspeicherpool mit Lesezugriff definieren

Einen Cloudspeicherpool mit dem Namen STGPOOL1 mit Lesezugriff definieren.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password access=readonly
```

Beispiel 4: Einen Cloudspeicherpool mit 99 Schreibsitzungen definieren

Einen Cloudspeicherpool mit dem Namen STGPOOL1 mit 99 Schreibsitzungen definieren.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password maxwr=99
```

Beispiel 5: Einen Cloudspeicherpool definieren, in dem deduplizierte Speicherbereiche nach zwei Tagen gelöscht werden

Einen Cloudspeicherpool mit dem Namen STGPOOL1 definieren, in dem deduplizierte Speicherbereiche nach zwei Tagen gelöscht werden.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password reusedelay=2
```

Zugehörige Tasks:
Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren
Zugehörige Informationen:
Leistung für Cloudobjektspeicher optimieren
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren)

Mit diesem Befehl kann ein Verzeichniscontainerspeicherpool definiert werden, der für die Datendeduplizierung verwendet wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

Parameter

Poolname (Erforderlich)
Gibt den Speicherpool an, der definiert werden soll. Dieser Parameter ist erforderlich. Die maximale Länge des Namens beträgt 30 Zeichen.

STGType=DIrectory (Erforderlich)
Gibt den Typ des Speichers an, der für einen Speicherpool definiert werden soll. Dieser Parameter gibt an, dass dem Speicherpool ein Speicherpool des Typs Verzeichniscontainer zugeordnet wird. Sie müssen mit dem Befehl DEFINE STGPOOLDIRECTORY ein Speicherpoolverzeichnis für diesen Typ von Speicherpool definieren.
Voraussetzungen:

- Stellen Sie sicher, dass für den Verzeichniscontainerspeicherpool genügend Speicherbereich im Dateisystem verfügbar ist.
- Sie müssen den Verzeichniscontainerspeicherpool und die DB2-Datenbank auf separaten Mountpunkten im Dateisystem speichern. Der Verzeichniscontainerspeicherpool kann anwachsen und den gesamten Speicherbereich in dem Verzeichnis belegen, in dem er gespeichert ist.
- Sie müssen ein anderes Dateisystem als das Dateisystem verwenden, in dem sich der IBM Spectrum Protect-Server befindet.

POoltype=PRimary
Gibt an, dass der Speicherpool als primärer Speicherpool verwendet werden soll. Dieser Parameter ist wahlfrei.

DESCription
Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

ACCess
Gibt an, wie Clientknoten und Serverprozesse auf den Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

READWrite
Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff für den Speicherpool haben.

READOnly
Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff für den Speicherpool haben.

UNAVailable
Gibt an, dass Clientknoten und Serverprozesse nicht auf den Speicherpool zugreifen können.

MAXSIze
Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können einen der folgenden Werte angeben:

NOLimit
Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

maximale_Dateigröße
Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl im Bereich von 1 bis 999999 gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 GB ist. Sie können einen der folgenden Maßstabsfaktoren verwenden:

Tabelle 1. Maßstabsfaktor für die maximale Dateigröße

Maßstabsfaktor	Bedeutung
K	Kilobyte
M	Megabyte
G	Gigabyte
T	Terabyte

Tipp: Wenn Sie keine Maßeinheit für die maximale Dateigröße angeben, wird der Wert in Byte angegeben.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

Tabelle 2. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool

Angegebener Pool	Ergebnis
Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben.	Die Datei wird vom Server nicht gespeichert.
Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben.	Der Server speichert die Datei in dem Speicherpool, den Sie angegeben haben.

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSIze=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Werden während der Datendeduplizierungsverarbeitung mehrere Dateien gesendet, betrachtet der Server die Größe des Datendeduplizierungsprozesses als Dateigröße. Wenn die Gesamtgröße aller Dateien in dem Prozess die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

MAXWriters
Gibt die maximale Anzahl E/A-Threads für die folgenden Prozesse an:

- Die Anzahl E/A-Threads, die gleichzeitig für den Verzeichniscontainerspeicherpool ausgeführt werden können.
- Die Anzahl E/A-Threads, die gleichzeitig in den Verzeichniscontainerspeicherpool geschrieben werden.

Dieser Parameter ist wahlfrei. Verwenden Sie als Best Practice den Standardwert NOLIMIT. Sie können die folgenden Werte angeben:

NOLimit

Gibt an, dass keine maximale Anzahl E/A-Threads in den Speicherpool geschrieben wird.

maximale_Anzahl_Writer
Begrenzt die maximale Anzahl der E/A-Threads, die Sie verwenden können. Geben Sie eine ganze Zahl im Bereich von 1 bis 99999 an.

Tipp: Der IBM Spectrum Protect-Server steuert die Anzahl der E/A-Threads automatisch auf der Basis der verfügbaren Ressourcen und der Serverauslastung.

NEXTstgpool
Gibt den Namen eines Speicherpools mit wahlfreiem Zugriff oder eines primären sequenziellen Speicherpools an, in dem Dateien gespeichert werden, wenn der Verzeichniscontainerspeicherpool voll ist. Dieser Parameter ist wahlfrei.
Einschränkungen:

- Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
- Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
- Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
- Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.

PROTECTstgpool
Gibt den Namen des Verzeichniscontainerspeicherpools auf dem Zielreplikationsserver an, in dem die Daten gesichert werden, wenn Sie den Befehl PROTECT STGPOOL für diesen Speicherpool verwenden. Dieser Parameter ist wahlfrei.

PROTECTLOCalstgpools
Gibt den Namen des Containerkopienspeicherpools auf einer lokalen Einheit an, in dem die Daten gesichert werden. Dieser Containerkopienspeicherpool ist ein lokaler Zielspeicherpool, wenn Sie den Befehl PROTECT STGPOOL verwenden. Sie können maximal zwei Containerkopienspeicherpoolnamen angeben. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Die maximale Länge jedes Namens beträgt 30 Zeichen. Dieser Parameter ist wahlfrei.

REUsedelay
Gibt die Anzahl Tage an, die verstreichen müssen, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool entfernt werden. Dieser Parameter steuert die Dauer, die deduplizierte Speicherbereiche einem Verzeichniscontainerspeicherpool zugeordnet sind, nachdem sie nicht mehr referenziert werden. Wenn der für den Parameter angegebene Wert abläuft, werden die deduplizierten Speicherbereiche aus dem Verzeichniscontainerspeicherpool gelöscht. Geben Sie eine ganze Zahl im Bereich von 0 bis 9999 an. Der Standardwert für Verzeichniscontainerspeicherpools ist 1. Dies bedeutet, dass deduplizierte Speicherbereiche, die nicht mehr referenziert werden, nach 1 Tag aus einem Verzeichniscontainerspeicherpool gelöscht werden.

Setzen Sie diesen Parameter auf einen Wert, der größer als der Wert ist, der als Datenbanksicherungsperiode angegeben ist, um sicherzustellen, dass Datenbereiche noch gültig sind, wenn die Datenbank auf eine andere Stufe zurückgeschrieben wird.

ENCRypt
Gibt an, ob der Server Clientdaten verschlüsselt, bevor der Server die Daten in den Speicherpool schreibt. Sie können die folgenden Werte angeben:

Yes
Gibt an, dass Clientdaten vom Server verschlüsselt werden.

No
Gibt an, dass Clientdaten nicht vom Server verschlüsselt werden.

COMPRession
Gibt an, ob Daten in dem Speicherpool komprimiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass Daten in dem Speicherpool nicht komprimiert werden.

Yes
Gibt an, dass Daten in dem Speicherpool komprimiert werden. Dies ist der Standardwert.

Beispiel: Einen Verzeichniscontainerspeicherpool definieren, der für Überlaufspeicher konfiguriert wird, wenn der Speicherpool voll ist

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1. Der Speicherpool wird für Überlaufspeicher in einem Bandspeicherpool konfiguriert, wenn der Speicherpool voll ist.

```
define stgpool stgpool1 stgtype=directory nextstgpool=overflow_tape_pool
```

Beispiel: Einen Verzeichniscontainerspeicherpool definieren, der die maximale Dateigröße angibt

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL2. Der Speicherpool gibt als maximale Dateigröße 100 Megabyte an, die der Server im Speicherpool speichern kann.

```
define stgpool stgpool2 stgtype=directory maxsize=100M
```

Beispiel: Einen Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver mit einem Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver zum Sichern von Daten definieren

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL3. Die Daten für Speicherpool STGPOOL3 werden in dem Verzeichniscontainerspeicherpool TARGET_STGPOOL3 auf dem Zielreplikationsserver gesichert.

```
define stgpool stgpool3 stgtype=directory protectstgpool=target_stgpool3
```

Beispiel: Einen Verzeichniscontainerspeicherpool auf dem Quellenreplikationsserver mit einem Containerkopienspeicherpool definieren, um Daten lokal zu sichern

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL3. Die Daten für Speicherpool STGPOOL3 werden in dem lokalen Containerkopienspeicherpool TARGET_LOCALSTGPOOL gesichert.

```
define stgpool stgpool3 stgtype=directory protectlocalstgpools=target_localstgpool
```

Beispiel: Einen Verzeichniscontainerspeicherpool definieren und die Komprimierung inaktivieren

Definieren Sie einen Verzeichniscontainerspeicherpool mit dem Namen STGPOOL1 und inaktivieren Sie die Komprimierung.

```
define stgpool stgpool1 stgtype=directory compression=no
```

Tabelle 3. Zugehörige Befehle für DEFINE STGPOOL (Verzeichniscontainerspeicherpool definieren)

Befehl	Beschreibung
DEFINE STGPOOLDIRECTORY	Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.
QUERY CONTAINER	Zeigt Informationen zu einem Container an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REPAIR STGPOOL	Repariert einen Verzeichniscontainerspeicherpool.
UPDATE STGPOOL (Verzeichniscontainer)	Aktualisiert einen Verzeichniscontainerspeicherpool.

DEFINE STGPOOL (Containerkopienspeicherpool definieren)

Mit diesem Befehl kann ein Containerkopienspeicherpool definiert werden, in dem eine Kopie der Daten aus einem Verzeichniscontainerspeicherpool gespeichert wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine STGpool--Poolname--Einheitenklassenname--------------->

>--POoltype--=--COPYCONtainer--MAXSCRatch-----Anzahl------------>

>--+------------------------------+----------------------------->
   '-DESCription--=--Beschreibung-'

   .-ACCess--=--READWrite-------.
>--+--------------------------------+-------------------------------->
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                '-UNAVailable-'

   .-PROTECTPRocess--=--2------.  .-RECLaim--=--100-----.
>--+--------------------------+--+---------------------+------->
   '-PROTECTPRocess--=--Anzahl-'  '-RECLaim--=--Prozent-'

   .-RECLAIMLIMit--=--NOLimit------------------.
>--+-----------------------------------------+---------------->
   '-RECLAIMLIMit--=--+-NOLimit--------------+-'
                      '-Datenträgergrenzwert-'

   .-REUsedelay--=--0----.
>--+--------------------+------------------------------------><
```

```
'-REUsedelay--=--Tage-'
```

Parameter

Poolname (Erforderlich)
: Gibt den Namen des Containerkopienspeicherpools an. Der Name muss eindeutig sein, und die maximale Länge beträgt 30 Zeichen.

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse für den sequenziellen Zugriff an, der dieser Speicherpool zugeordnet ist.
Einschränkung: Die folgenden Einheitenklassentypen können nicht angegeben werden:

- DISK
- FILE
- CENTERA
- NAS
- REMOVABLEFILE
- SERVER

Einschränkung: Virtuelle Bandarchive werden nicht unterstützt, unabhängig davon, welcher Speicherarchivtyp definiert wird. Es wird nur physisches Band unterstützt.

POoltype=COPYCONtainer (Erforderlich)
: Gibt an, dass ein Containerkopienspeicherpool definiert werden soll. Ein Containerkopienspeicherpool wird nur verwendet, um eine Kopie der Daten aus einem Verzeichniscontainerspeicherpool zu speichern.

MAXSCRatch (Erforderlich)
: Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Sie können eine ganze Zahl im Bereich von 0 bis 100000000 angeben. Wenn der Server Arbeitsdatenträger nach Bedarf anfordern kann, müssen Sie nicht jeden zu verwendenden Datenträger definieren.

Mit dem Wert dieses Parameters wird die Gesamtzahl der im Speicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Speicherpools geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Lautet jedoch der Zugriffsmodus für einen Arbeitsdatenträger OFFSITE, wird der Datenträger erst dann aus dem Speicherpool gelöscht, wenn der Zugriffsmodus geändert wird. Ein Administrator kann dann den Server nach leeren ausgelagerten Arbeitsdatenträgern abfragen und diese an den Standort vor Ort zurückgeben.

DESCription
: Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

ACCess
: Gibt an, wie Serverprozesse, wie z. B. Speicherpoolschutz und Reparatur, auf Daten in dem Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Sie können einen der folgenden Werte angeben:

  READWrite
  : Gibt an, dass der Server Lese- und Schreibzugriff auf Datenträger in dem Speicherpool hat.

  READOnly
  : Gibt an, dass der Server nur Lesezugriff auf Datenträger in dem Speicherpool hat. Der Server kann Daten in dem Speicherpool verwenden, um Bereiche in Verzeichniscontainerspeicherpools zurückzuschreiben. Operationen, mit denen Daten in den Containerkopienspeicherpool geschrieben werden, sind nicht zulässig.

  UNAVailable
  : Gibt an, dass der Server nicht auf Daten zugreifen kann, die auf Datenträgern im Speicherpool gespeichert sind.

PROTECTPRocess
: Gibt die maximale Anzahl paralleler Prozesse an, die verwendet werden, wenn Sie den Befehl PROTECT STGPOOL ausgeben, um Daten aus einem Verzeichniscontainerspeicherpool in diesen Pool zu kopieren. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 20 ein. Der Standardwert ist 2.

Die Zeit, die für die Ausführung der Kopieroperation erforderlich ist, kann durch die Verwendung mehrerer Prozesse verringert werden. Sind mehrere Prozesse aktiv, müssen jedoch in einigen Fällen ein oder mehrere Prozesse auf die Verwendung eines Datenträgers warten, der bereits von einem anderen Prozess verwendet wird.

Berücksichtigen Sie bei der Angabe dieses Werts die Anzahl der logischen und physischen Laufwerke, die der Kopieroperation zugeordnet werden können. Für den Zugriff auf einen Banddatenträger verwendet der Server einen Mountpunkt und ein Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von dem Mountlimit der Einheitenklasse für den Speicherpool und von anderen Server- und Systemaktivitäten abhängig.

Dieser Parameter wird ignoriert, wenn Sie die Option PREVIEW=YES im Befehl PROTECT STGPOOL verwenden. In diesem Fall wird nur ein Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

RECLaim
: Gibt an, wann ein Datenträger für die Konsolidierung und Wiederverwendung auswählbar ist. Geben Sie die Auswählbarkeit als Prozentsatz des Speicherbereichs eines Datenträgers an, der von Bereichen belegt ist, die nicht mehr im zugeordneten

Verzeichniscontainerspeicherpool gespeichert werden. Bei der Konsolidierung werden alle Bereiche, die noch im zugeordneten Verzeichniscontainerspeicherpool gespeichert werden, von auswählbaren Datenträgern auf andere Datenträger versetzt. Die Konsolidierung erfolgt nur, wenn mit einem Befehl PROTECT STGPOOL Daten in diesem Speicherpool gespeichert werden.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 1 bis 100 angeben. Der Standardwert 100 bedeutet, dass keine Datenträger in diesem Speicherpool konsolidiert werden.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Wird der Wert für 'Reclaim' auf 50 Prozent oder höher gesetzt, belegen Daten, die von zwei konsolidierten Datenträgern versetzt werden, maximal das Äquivalent eines neuen Datenträgers.

Gehen Sie mit Vorsicht vor, wenn Sie die Konsolidierung mit Containerkopienspeicherpools verwenden, die über ausgelagerte Datenträger verfügen. Wenn ein ausgelagerter Datenträger für die Konsolidierung auswählbar wird, werden die Bereiche auf dem Datenträger vom Server an den Standort vor Ort zurückversetzt. Wenn vor Ort ein Katastrophenfall eintritt, kann der Server Bereiche vom ausgelagerten Datenträger anfordern, wenn die zurückgeschriebene Datenbank auf Bereiche auf dem ausgelagerten Datenträger verweist. Stellen Sie daher zu Zwecken der Wiederherstellung nach einem Katastrophenfall sicher, dass Sie die Ausführung von Datenbanksicherungen planen, nachdem Speicherpoolschutzzeitpläne und DRM-Versetzungszeitpläne ausgeführt wurden, und stellen Sie sicher, dass alle Datenbanksicherungsdatenträger zusammen mit den DRM-Datenträgern ausgelagert werden.

Tipp: Definieren Sie verschiedene Konsolidierungswerte für Containerkopienspeicherpools an einem anderen Standort und Containerkopienspeicherpools vor Ort. Da Containerkopienspeicherpools deduplizierte Daten speichern, sind die Datenbereiche auf mehrere Banddatenträger verteilt. Wenn Sie einen Schwellenwert für die Konsolidierung für eine Kopie an einem anderen Standort auswählen, beachten Sie sorgfältig die Anzahl verfügbarer Mountpunkte und die Anzahl Banddatenträger, die abgerufen werden müssen, wenn ein Katastrophenfall eintritt. Wird ein höherer Schwellenwert definiert, bedeutet dies, dass Sie mehr Datenträger abrufen müssen als bei einem niedrigeren Konsolidierungswert. Bei Verwendung eines niedrigeren Schwellenwerts wird die Anzahl der Mountpunkte reduziert, die in einem Katastrophenfall erforderlich sind. Die bevorzugte Methode ist die Angabe des Konsolidierungswerts 60 für Kopien an einem anderen Standort. Für Kopien vor Ort liegt er im Bereich von 90 bis 100.

RECLAIMLIMit
: Gibt die maximale Anzahl von Datenträgern an, die der Server konsolidiert, wenn Sie den Befehl PROTECT STGPOOL ausgeben und die Option RECLAIM=YESLIMITED oder RECLAIM=ONLYLIMITED angeben. Dieser Parameter ist nur für Containerkopienspeicherpools gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können einen der folgenden Werte angeben:

  NOLimit
  : Gibt an, dass alle Datenträger im Containerkopienspeicherpool für die Konsolidierung verarbeitet werden.

  Datenträgergrenzwert
  : Gibt die maximale Anzahl der Datenträger im Containerkopienspeicherpool an, die konsolidiert werden. Der von Ihnen angegebene Wert bestimmt, wie viele neue Arbeitsbänder nach Abschluss der Konsolidierungsverarbeitung verfügbar sind. Sie können eine Zahl im Bereich von 1 bis 100000 angeben.

REUsedelay
: Gibt die Anzahl Tage an, die nach dem Löschen aller Bereiche von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerstatus versetzt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben. Der Standardwert ist 0, was bedeutet, dass ein Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerstatus versetzt werden kann, sobald alle Bereiche auf dem Datenträger gelöscht wurden.
  Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Bereiche im Speicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Wenn Sie Disaster Recovery Manager verwenden, muss die für diesen Parameter angegebene Anzahl Tage mit der für den Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl übereinstimmen.

Beispiel: Einen Containerkopienspeicherpool mit einer Einheitenklasse LTO7A definieren

Den Containerkopienspeicherpool CONTAINER1_COPY2 für die Einheitenklasse LTO7A definieren. Maximal 50 Arbeitsdatenträger für diesen Pool zulassen. Die Wiederverwendung der Datenträger um 45 Tage verzögern.

```
define stgpool container1_copy2 lto7a pooltype=copycontainer
 maxscratch=50 reusedelay=45
```

Tabelle 1. Zugehörige Befehle für DEFINE STGPOOL (Containerkopienspeicherpool definieren)

Befehl	Beschreibung
DEFINE STGPOOL (Verzeichniscontainer)	Definiert einen Verzeichniscontainerspeicherpool.
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REPAIR STGPOOL	Repariert einen Verzeichniscontainerspeicherpool.

Befehl	Beschreibung
UPDATE STGPOOL (Containerkopie)	Aktualisiert einen Containerkopienspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden.
UPDATE STGPOOL (Verzeichniscontainer)	Aktualisiert einen Verzeichniscontainerspeicherpool.

DEFINE STGPOOL (Primären Speicherpool definieren, der Einheiten mit wahlfreiem Zugriff zugeordnet wird)

Mit diesem Befehl kann ein primärer Speicherpool definiert werden, der Einheiten mit wahlfreiem Zugriff zugeordnet wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>--+-----------------------------------------+---------------><
   |                                  (1) (2) |
   '-SHRED--=--Anzahl_Überschreibungen---------'
```

Anmerkungen:

1. Dieser Parameter ist für CENTERA- oder SnapLock-Speicherpools nicht verfügbar.
2. Linux-BetriebssystemeDieser Parameter ist für SnapLock-Speicherpools nicht verfügbar.

Parameter

Poolname (Erforderlich)
: Gibt den Namen des Speicherpools an, der definiert werden soll. Der Name muss eindeutig sein, und die maximale Länge beträgt 30 Zeichen.

DISK (Erforderlich)
: Gibt an, dass ein Speicherpool für die Einheitenklasse DISK definiert werden soll (die Einheitenklasse DISK wird während der Installation vordefiniert).

POoltype=PRimary
: Gibt an, dass ein primärer Speicherpool definiert werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist PRIMARY.

STGType
: Gibt den Typ des Speichers an, der für einen Speicherpool definiert werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DEVCLASS.

  Devclass
  : Gibt an, dass dem Speicherpool ein Speicherpool des Typs Einheitenklasse zugeordnet wird.

DESCription
: Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

ACCess
: Gibt an, wie Clientknoten und Serverprozesse (wie Umlagerung und Wiederherstellung) auf Dateien im Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Sie können die folgenden Werte angeben:

  READWrite
  : Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien haben, die auf Datenträgern in dem Speicherpool gespeichert sind.

  READOnly
  : Gibt an, dass Clientknoten Dateien auf den Datenträgern im Speicherpool nur lesen können.

    Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

    Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *readonly (schreibgeschützt)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

  UNAVailable
  : Gibt an, dass Clientknoten nicht auf Dateien, die auf Datenträgern im Speicherpool gespeichert sind, zugreifen können.

    Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Außerdem können sie Dateien aus diesem Speicherpool in einen anderen Speicherpool versetzen oder kopieren. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

    Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *unavailable (nicht verfügbar)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

MAXSIze
: Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können die folgenden Werte angeben:

  NOLimit
  : Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

  maximale_Dateigröße
  : Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl zwischen 1 und 999999 Terabyte gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 GB ist. Sie können einen der folgenden Maßstabsfaktoren verwenden:

Maßstabsfaktor	Bedeutung
K	Kilobyte
M	Megabyte

Maßstabsfaktor	Bedeutung
G	Gigabyte
T	Terabyte

Der Client schätzt die Größe der Dateien, die an den Server gesendet werden. Die Schätzung des Clients wird verwendet und nicht das tatsächliche Datenvolumen, das an den Server gesendet wird. Clientoptionen, wie z. B. Deduplizierung, Komprimierung und Verschlüsselung, können zur Folge haben, dass das tatsächliche Datenvolumen, das an den Server gesendet wird, größer oder kleiner als die Größenschätzung ist. Beispielsweise kann eine komprimierte Datei kleiner als die Schätzung sein, sodass weniger Daten als der Schätzwert gesendet werden. Des Weiteren kann eine Binärdatei nach der Komprimierungsverarbeitung größer sein, sodass mehr Daten als der Schätzwert gesendet werden.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

Tabelle 1. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool

Dateigröße	Angegebener Pool	Ergebnis
Überschreitet die maximale Größe	Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben	Die Datei wird vom Server nicht gespeichert
	Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben	Der Server speichert die Datei im nächsten Speicherpool, der die Dateigröße akzeptiert

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSIze=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Bei mehreren Dateien, die in einer einzelnen Transaktion gesendet werden, betrachtet der Server die Größe der Transaktion als Dateigröße. Wenn die Gesamtgröße aller Dateien in der Transaktion die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

CRCData
: Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

  Yes
  : Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da mehr Aufwand erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

  No
  : Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

NEXTstgpool
: Gibt einen primären Speicherpool an, in den Dateien umgelagert werden. Dieser Parameter ist wahlfrei.
Wird kein nächster Speicherpool angegeben, gilt Folgendes:

  - Der Server kann keine Dateien aus diesem Speicherpool umlagern
  - Der Server kann keine Dateien, die die maximale Größe für diesen Speicherpool überschreiten, in einem anderen Speicherpool speichern

  Einschränkungen:

  - Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
  - Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
  - Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
  - Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.

HIghmig
: Gibt an, dass der Server die Umlagerung für diesen Speicherpool startet, wenn der Datenumfang in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100 angeben. Der Standardwert ist 90.

  Wenn der Speicherpool die obere Umlagerungsschwelle überschreitet, kann der Server die Umlagerung von Dateien in den nächsten Speicherpool nach Knoten starten. Der Parameter NEXTSTGPOOL definiert diese Einstellung. Sie können HIGHMIG=100 angeben, um die Umlagerung für diesen Speicherpool zu verhindern.

LOwmig

Gibt an, dass der Server die Umlagerung für diesen Speicherpool stoppt, wenn der Datenumfang in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 99 angeben. Der Standardwert ist 70.

Wenn die Umlagerung nach Knoten oder Dateibereich erfolgt (abhängig von der Kollokation), kann der Wert für den Speicherpool unter den für diesen Parameter angegebenen Wert fallen. Um den Speicherpool zu leeren, definieren Sie LOWMIG=0.

CAChe
Gibt an, ob der Umlagerungsprozess eine Cachekopie einer Datei in diesem Speicherpool zurücklässt, nachdem die Datei in den nächsten Speicherpool umgelagert wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

Yes
Caching ist aktiviert.

No
Caching ist inaktiviert.

Die Verwendung von Cache kann die Abrufbarkeit von Dateien verbessern, kann jedoch die Leistung anderer Prozesse negativ beeinflussen.

MIGPRocess
Gibt die Anzahl der Prozesse an, die der Server zum Umlagern von Dateien aus diesem Speicherpool verwendet. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 999 angeben. Der Standardwert ist 1.

Während der Umlagerung werden diese Prozesse parallel ausgeführt, um die Umlagerungsgeschwindigkeit zu verbessern.

Tipps:

- Die Anzahl der Umlagerungsprozesse ist von den folgenden Einstellungen abhängig:
  - Einstellung des Parameters MIGPROCESS
  - Kollokationseinstellung des nächsten Pools
  - Anzahl der Knoten oder Anzahl der Kollokationsgruppen mit Daten in dem Speicherpool, der umgelagert wird

  Beispiel: Angenommen, dass `MIGPROCESS =6` angegeben und der Parameter COLLOCATE für den nächsten Pool auf NODE gesetzt ist, aber nur zwei Knoten mit Daten in dem Speicherpool vorhanden sind. Die Umlagerungsverarbeitung besteht nur aus zwei, nicht sechs Prozessen. Wird der Parameter COLLOCATE auf GROUP gesetzt und befinden sich beide Knoten in derselben Gruppe, besteht die Umlagerungsverarbeitung nur aus einem Prozess. Wird der Parameter COLLOCATE auf NO oder FILESPACE gesetzt und hat jeder Knoten zwei Dateibereiche mit Sicherungsdaten, besteht die Umlagerungsverarbeitung aus vier Prozessen.
- Beachten Sie bei der Angabe dieses Parameters, ob die Funktion für simultanes Schreiben für die Serverdatenumlagerung aktiviert ist. Jeder Umlagerungsprozess erfordert einen Mountpunkt und ein Laufwerk für jeden Kopienspeicherpool und Pool für aktive Daten, der für den Zielspeicherpool definiert ist.

MIGDelay
Gibt die Mindestanzahl Tage an, die eine Datei in einem Speicherpool verbleiben muss, bevor sie für die Umlagerung ausgewählt werden kann. Um einen Wert zu berechnen, der mit dem angegebenen Wert für MIGDELAY verglichen wird, zählt der Server:

- Die Anzahl der Tage, die die Datei im Speicherpool war
- Die Anzahl der Tage (falls zutreffend), seit die Datei von einem Client abgerufen wurde

Der kleinere der beiden Werte wird mit dem angegebenen Wert für MIGDELAY verglichen. Beispiel: Sind alle folgenden Bedingungen wahr, wird eine Datei nicht umgelagert:

- Eine Datei war fünf Tage in einem Speicherpool.
- Auf die Datei wurde innerhalb der letzten drei Tage von einem Client zugegriffen.
- Der für den Parameter MIGDELAY angegebene Wert beträgt vier Tage.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert 0 gibt an, dass die Umlagerung nicht verzögert werden soll.

Soll der Server die Anzahl der Tage ab dem Tag zählen, an dem eine Datei gespeichert wurde, und nicht ab dem Tag, an dem sie abgerufen wurde, die Serveroption NORETRIEVEDATE verwenden.

MIGContinue
Gibt an, ob der Server Dateien umlagern darf, die der Verzögerungszeit für die Umlagerung nicht entsprechen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Da angegeben werden kann, dass Dateien eine Mindestanzahl Tage in dem Speicherpool verbleiben müssen, kann der Server alle auswählbaren Dateien in den nächsten Speicherpool umlagern, obwohl sie dem Wert für die untere Umlagerungsschwelle nicht entsprechen. Mit diesem Parameter kann angegeben werden, ob der Server den Umlagerungsprozess fortsetzen darf, indem Dateien umgelagert werden, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sie können einen der folgenden Werte angeben:

Yes

Muss die untere Umlagerungsschwelle eingehalten werden, gibt dieser Wert an, dass der Server mit der Umlagerung von Dateien fortfährt, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sind mehrere Umlagerungsprozesse für den Speicherpool zulässig, werden einige Dateien, die der Verzögerungszeit für die Umlagerung nicht entsprechen, unter Umständen unnötigerweise umgelagert. Während ein Prozess Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte ein zweiter Prozess mit der Umlagerung von Dateien beginnen, die der Verzögerungszeit für die Umlagerung nicht entsprechen, um die untere Umlagerungsschwelle einzuhalten. Der erste Prozess, der noch Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte selbst die Einhaltung der unteren Umlagerungsschwelle bewirkt haben.

No
: Gibt an, dass der Server die Umlagerung stoppt, wenn keine auswählbaren Dateien mehr für die Umlagerung verfügbar sind; dies gilt auch vor Erreichen der unteren Umlagerungsschwelle. Der Server lagert nur Dateien um, die der Verzögerungszeit für die Umlagerung entsprechen.

AUTOCopy
: Gibt an, wann IBM Spectrum Protect Operationen mit simultanem Schreiben ausführt. Der Standardwert ist CLIENT. Dieser Parameter ist wahlfrei und betrifft die folgenden Operationen:

- Clientspeichersitzungen
- Serverimportprozesse
- Serverdatenumlagerungsprozesse

Tritt ein Fehler auf, wenn Daten während eines Umlagerungsprozesses gleichzeitig in einen Kopienspeicherpool oder einen Pool für aktive Daten geschrieben werden, stoppt der Server das Schreiben in die fehlerhaften Speicherpools für den Rest des Prozesses. Der Server speichert jedoch weiterhin Dateien in dem primären Speicherpool und in allen verbleibenden Kopienspeicherpools oder Pools für aktive Daten. Diese Pools bleiben für die Dauer des Umlagerungsprozesses aktiv. Kopienspeicherpools werden mit dem Parameter COPYSTGPOOLS angegeben. Pools für aktive Daten werden mit dem Parameter ACTIVEDATAPOOLS angegeben.

Sie können einen der folgenden Werte angeben:

None
: Gibt an, dass die Funktion für simultanes Schreiben inaktiviert ist.

CLient
: Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen oder Serverimportprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverimportprozessen werden Daten nur gleichzeitig in Kopienspeicherpools geschrieben. Daten werden während der Ausführung von Serverimportprozessen nicht in Pools für aktive Daten geschrieben.

MIGRation
: Gibt an, dass Daten nur während der Umlagerung in diesen Speicherpool gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverdatenumlagerungsprozessen werden Daten in Kopienspeicherpools und Pools für aktive Daten nur dann gleichzeitig geschrieben, wenn die Daten in diesen Pools nicht vorhanden sind. Knoten, deren Daten umgelagert werden, müssen sich in einer Domäne befinden, die einem Pool für aktive Daten zugeordnet ist. Befinden sich die Knoten nicht in einer Domäne, die einem Pool für aktive Daten zugeordnet ist, können die Daten nicht in den Pool geschrieben werden.

All
: Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen oder Serverdatenumlagerungsprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Mit diesem Wert wird sichergestellt, dass Daten immer dann gleichzeitig geschrieben werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

COPYSTGpools
: Gibt die Namen von Kopienspeicherpools an, in die der Server gleichzeitig Daten schreibt. Der Parameter COPYSTGPOOLS ist optional. Sie können maximal drei Kopienpoolnamen angeben, die durch Kommas voneinander getrennt werden müssen. Leerzeichen zwischen den Namen der Kopienpools sind nicht zulässig. Wenn Sie einen Wert für den Parameter COPYSTGPOOLS angeben, können Sie auch einen Wert für den Parameter COPYCONTINUE angeben.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Kopienspeicherpools und den Wert für COPYCONTINUE aus dem primären Speicherpool. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann während der Ausführung der folgenden Operationen Daten gleichzeitig in Kopienspeicherpools schreiben:

- Sicherungs- und Archivierungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder Anwendungsclients, die die IBM Spectrum Protect-API verwenden
- Umlagerungsoperationen durch IBM Spectrum Protect for Space Management-Clients
- Importoperationen, die das Kopieren von exportierten Dateidaten von externen Datenträgern in einen primären Speicherpool einbeziehen, der einer Kopienspeicherpoolliste zugeordnet ist

Einschränkung: Die Funktion für simultanes Schreiben wird für die folgenden Speicheroperationen nicht unterstützt:

- Wenn die Operation die LAN-unabhängige Datenversetzung verwendet. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch berücksichtigt.
- NAS-Sicherungsoperationen. Sind für den primären Speicherpool, der in DESTINATION oder TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Kopienspeicherpools definiert, werden
  - die Kopienspeicherpools ignoriert.
  - die Daten nur im primären Speicherpool gespeichert.

Achtung: Die mit dem Parameter COPYSTGPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl BACKUP STGPOOL ersetzen. Wird der Parameter COPYSTGPOOLS verwendet, verwenden Sie weiterhin den Befehl BACKUP STGPOOL, um sicherzustellen, dass die Kopienspeicherpools vollständige Kopien des primären Speicherpools sind. Es gibt Fälle, in denen eine Kopie möglicherweise nicht erstellt wird. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

COPYContinue
Gibt an, wie der Server normalerweise auf einen Fehler beim Schreiben in einen der Kopienspeicherpools reagiert, die im Parameter COPYSTGPOOLS aufgelistet sind. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Wenn Sie den Parameter COPYCONTINUE angeben, müssen Sie auch den Parameter COPYSTGPOOLS angeben.
Sie können die folgenden Werte angeben:

Yes
Ist der Parameter COPYCONTINUE auf YES gesetzt, stoppt der Server das Schreiben in die fehlerhaften Kopienpools für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Kopienpools fort. Die Liste der Kopienspeicherpools ist nur für die Dauer der Clientsitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.

No
Ist der Parameter COPYCONTINUE auf NO gesetzt, wird die aktuelle Transaktion vom Server nicht ausgeführt und die Speicheroperation nicht fortgesetzt.

Einschränkungen:

- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf Pools für aktive Daten. Tritt für einen der Pools für aktive Daten ein Schreibfehler auf, stoppt der Server das Schreiben in den fehlerhaften Pool für aktive Daten für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Pools für aktive Daten und Kopienspeicherpools fort. Die Liste der Pools für aktive Daten ist nur für die Dauer der Sitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Ausführung eines Serverimportprozesses. Werden Daten gleichzeitig geschrieben und tritt für den primären Speicherpool oder einen Kopienspeicherpool ein Schreibfehler auf, schlägt der Serverimportprozess fehl.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Serverdatenumlagerung. Werden Daten gleichzeitig geschrieben und tritt für einen Kopienspeicherpool oder Pool für aktive Daten ein Schreibfehler auf, wird der fehlerhafte Speicherpool entfernt und der Datenumlagerungsprozess wird fortgesetzt. Bei Schreibfehlern für den primären Speicherpool schlägt der Umlagerungsprozess fehl.

ACTIVEDATApools
Gibt die Namen der Pools für aktive Daten an, in die der Server während einer Clientsicherungsoperation gleichzeitig Daten schreibt. Der Parameter ACTIVEDATAPOOLS ist optional. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Pools für aktive Daten aus dem Zielspeicherpool, der in der Kopiengruppe angegeben ist. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann nur während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients, die die IBM Spectrum Protect-API verwenden, Daten gleichzeitig in Pools für aktive Daten schreiben.
Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat "NATIVE" oder "NONBLOCK" verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
   - NETAPPDUMP
   - CELERRADUMP
   - NDMPDUMP
2. Das simultane Schreiben in Pools für aktive Daten wird nicht unterstützt, wenn die LAN-unabhängige Datenversetzung verwendet wird. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch berücksichtigt.
3. Die Funktion für simultanes Schreiben wird nicht unterstützt, wenn eine NAS-Sicherungsoperation eine Inhaltsverzeichnisdatei schreibt. Sind für den primären Speicherpool, der in TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Pools für aktive Daten definiert, werden
   - die Pools für aktive Daten ignoriert.

- die Daten nur im primären Speicherpool gespeichert.

4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.
5. Daten, die importiert werden, werden nicht in Pools für aktive Daten gespeichert. Verwenden Sie nach einer Importoperation den Befehl COPY ACTIVEDATA, um die importierten Daten in einem Pool für aktive Daten zu speichern.

Achtung: Die mit dem Parameter ACTIVEDATAPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl COPY ACTIVEDATA ersetzen. Wird der Parameter ACTIVEDATAPOOLS verwendet, verwenden Sie den Befehl COPY ACTIVEDATA, um sicherzustellen, dass die Pools für aktive Daten alle aktiven Daten des primären Speicherpools enthalten.

SHRED

Gibt an, ob Daten beim Löschen physisch überschrieben werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 10 angeben. Der Standardwert ist 0.

Wird der Wert Null angegeben, löscht der Server die Daten aus der Datenbank. Der Speicher, in dem die Daten gespeichert waren, wird jedoch nicht überschrieben, und die Daten sind weiterhin im Speicher vorhanden, bis dieser Speicher für andere Daten wiederverwendet wird. Möglicherweise können die Daten nach dem Löschen erkannt und wiederhergestellt werden.

Wenn Sie einen Wert größer als Null angeben, löscht der Server die Daten sowohl logisch als auch physisch. Der Server überschreibt den Speicher, in dem die Daten gespeichert waren, so oft wie angegeben wurde. Durch das Überschreiben wird es schwieriger, die Daten zu erkennen und wiederherzustellen, nachdem sie gelöscht wurden.

Um sicherzustellen, dass alle Kopien der Daten geschreddert werden, geben Sie einen SHRED-Wert größer als Null für den im Parameter NEXTSTGPOOL angegebenen Speicherpool an. Geben Sie nicht COPYSTGPOOLS oder ACTIVEDATAPOOLS an. Durch die Angabe relativ hoher Werte für die Anzahl Überschreibungen wird im Allgemeinen die Sicherheitsstufe erhöht, aber sie kann umgekehrt die Leistung beeinflussen.

Das Überschreiben gelöschter Daten wird asynchron ausgeführt, nachdem die Löschoperation abgeschlossen ist. Daher bleibt der durch die gelöschten Daten belegte Speicherbereich für einige Zeit belegt. Der Speicherbereich ist nicht als freier Speicherbereich für neue Daten verfügbar.

Ein SHRED-Wert größer als null kann nicht verwendet werden, wenn der Parameter CACHE den Wert YES hat.

Wichtig: Nachdem eine Exportoperation die Identifizierung von Dateien für den Export beendet hat, werden alle Änderungen des Werts SHRED für den Speicherpool ignoriert. Eine Exportoperation, die ausgesetzt ist, behält während der gesamten Operation den ursprünglichen SHRED-Wert. Möglicherweise möchten Sie Ihre Exportoperation abbrechen, wenn Änderungen des Werts SHRED für den Speicherpool die Operation gefährden. Sie können den Exportbefehl nach einer erforderlichen Bereinigung erneut ausgeben.

Beispiel: Einen primären Speicherpool für eine Einheitenklasse DISK definieren

Den primären Speicherpool POOL1 für die Verwendung der Einheitenklasse DISK mit aktiviertem Caching definieren. Die maximale Dateigröße auf 5 MB begrenzen. Alle Dateien, die größer sind als 5 MB, in untergeordneten Speicherpools speichern (beginnend bei Speicherpool PROG2). Die obere Umlagerungsschwelle auf 70 Prozent und die untere Umlagerungsschwelle auf 30 Prozent setzen.

```
define stgpool pool1 disk
 description="main disk storage pool" maxsize=5m
 highmig=70 lowmig=30 cache=yes
 nextstgpool=prog2
```

DEFINE STGPOOL (Primären Speicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)

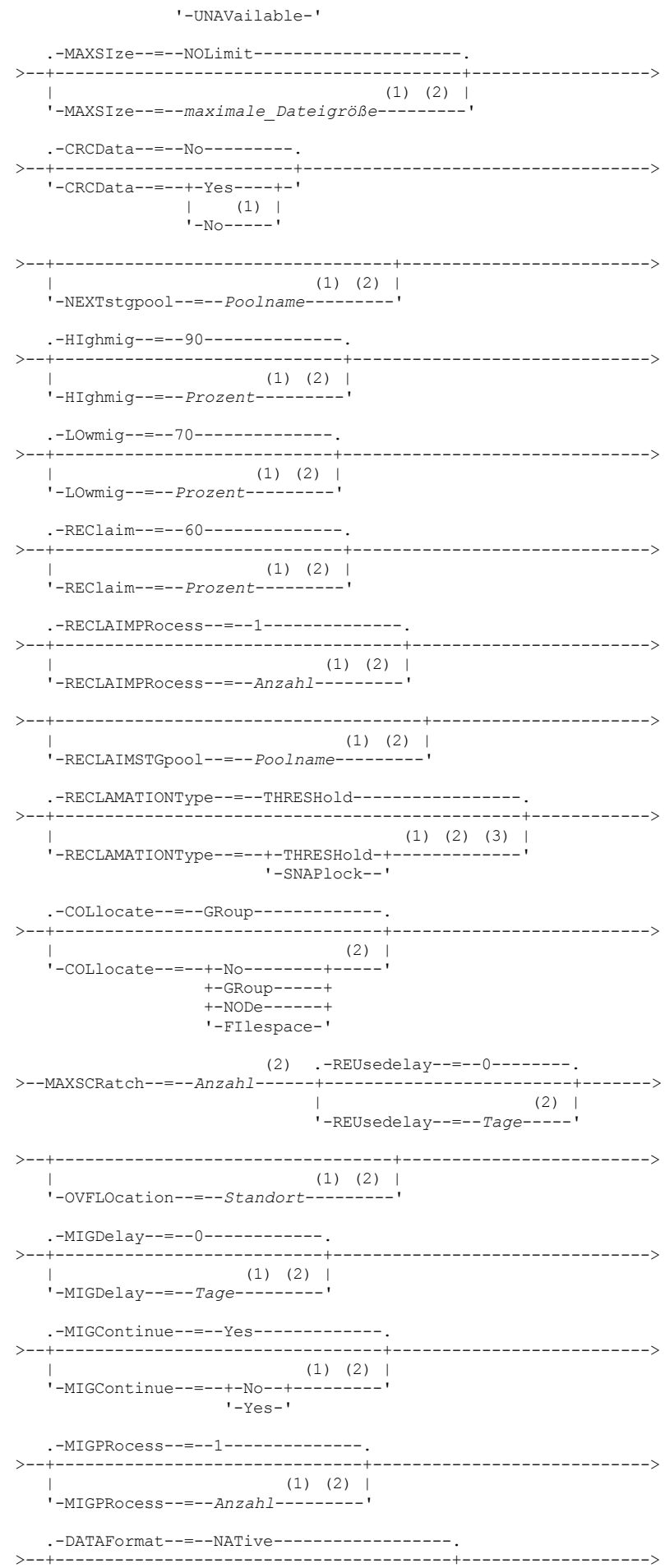
Mit diesem Befehl kann ein primärer Speicherpool definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine STGpool--Poolname--Einheitenklassenname--------------->

   .-POoltype--=--PRimary-.  .-STGType--=--Devclass-.
>--+---------------------+--+---------------------+----------->
   '-POoltype--=--PRimary-'  '-STGType--=--Devclass-'

>--+-----------------------------+---------------------------->
   '-DESCription--=--Beschreibung-'

   .-ACCess--=--READWrite-------.
>--+---------------------------+------------------------------>
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
```


'-UNAVailable-'
.-MAXSIze--=--NOLimit---------.
>--+-----------------------------------+----------->
| (1) (2) |
'-MAXSIze--=--maximale_Dateigröße---------'
.-CRCData--=--No---------.
>--+-------------------------+-------------------->
'-CRCData--=--+-Yes----+-'
| (1) |
'-No-----'
>--+---------------------------------+------------->
| (1) (2) |
'-NEXTstgpool--=--Poolname---------'
.-HIghmig--=--90--------------.
>--+-----------------------------+----------------->
| (1) (2) |
'-HIghmig--=--Prozent---------'
.-LOwmig--=--70--------------.
>--+----------------------------+------------------>
| (1) (2) |
'-LOwmig--=--Prozent---------'
.-RECLaim--=--60--------------.
>--+-----------------------------+----------------->
| (1) (2) |
'-RECLaim--=--Prozent---------'
.-RECLAIMPRocess--=--1--------------.
>--+-----------------------------------+------------->
| (1) (2) |
'-RECLAIMPRocess--=--Anzahl---------'
>--+-------------------------------------+----------->
| (1) (2) |
'-RECLAIMSTGpool--=--Poolname---------'
.-RECLAMATIONType--=--THRESHold-----------------.
>--+---+------------>
| (1) (2) (3) |
'-RECLAMATIONType--=--+-THRESHold-+-------------'
'-SNAPlock--'
.-COLlocate--=--GRoup-------------.
>--+---------------------------------+------------->
| (2) |
'-COLlocate--=--+-No--------+-----'
+-GRoup-----+
+-NODe------+
'-FIlespace-'
(2) .-REUsedelay--=--0--------.
>--MAXSCRatch--=--Anzahl------+-------------------------+------->
| (2) |
'-REUsedelay--=--Tage-----'
>--+---------------------------------+------------->
| (1) (2) |
'-OVFLOcation--=--Standort---------'
.-MIGDelay--=--0------------.
>--+----------------------------+------------------>
| (1) (2) |
'-MIGDelay--=--Tage---------'
.-MIGContinue--=--Yes-------------.
>--+---------------------------------+------------->
| (1) (2) |
'-MIGContinue--=--+-No--+----------'
'-Yes-'
.-MIGPRocess--=--1--------------.
>--+------------------------------+---------------->
| (1) (2) |
'-MIGPRocess--=--Anzahl---------'
.-DATAFormat--=--NATive------------------.
>--+--------------------------------------+------------>

Anmerkungen:

1. Dieser Parameter ist für Speicherpools, die das Datenformat NETAPPDUMP, CELERRADUMP oder NDMPDUMP verwenden, nicht verfügbar.
2. Dieser Parameter ist für CENTERA-Speicherpools nicht verfügbar oder wird ignoriert.
3. Die Einstellung RECLAMATIONTYPE=SNAPLOCK ist nur für Speicherpools gültig, die für Server definiert sind, die für IBM Spectrum Protect for Data Retention aktiviert sind. Der Speicherpool muss einer Einheitenklasse FILE zugeordnet sein, und die in der Einheitenklasse angegebenen Verzeichnisse müssen NetApp SnapLock-Datenträger sein.
4. Die Werte NETAPPDUMP, CELERRADUMP und NDMPDUMP sind nicht für Speicherpools gültig, die mit einer Einheitenklasse des Typs FILE definiert sind.
5. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
6. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

Parameter

Poolname (Erforderlich)
: Gibt den Namen des Speicherpools an, der definiert werden soll. Der Name muss eindeutig sein, und die maximale Länge beträgt 30 Zeichen.

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse an, der dieser Speicherpool zugeordnet ist. Mit Ausnahme der Einheitenklasse DISK kann jede Einheitenklasse angegeben werden.

POoltype=PRimary
: Gibt an, dass ein primärer Speicherpool definiert werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist PRIMARY.

STGType
: Gibt den Typ des Speichers an, der für einen Speicherpool definiert werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DEVCLASS.

  Devclass
  : Gibt an, dass dem Speicherpool ein Speicherpool des Typs Einheitenklasse zugeordnet wird.

DESCription
: Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

ACCess

Gibt an, wie Clientknoten und Serverprozesse (wie Umlagerung und Wiederherstellung) auf Dateien im Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Sie können die folgenden Werte angeben:

READWrite
: Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien haben, die auf Datenträgern in dem Speicherpool gespeichert sind.

READOnly
: Gibt an, dass Clientknoten Dateien auf den Datenträgern im Speicherpool nur lesen können.

  Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

  Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *readonly (schreibgeschützt)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

UNAVailable
: Gibt an, dass Clientknoten nicht auf Dateien, die auf Datenträgern im Speicherpool gespeichert sind, zugreifen können.

  Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Außerdem können sie Dateien aus diesem Speicherpool in einen anderen Speicherpool versetzen oder kopieren. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

  Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *unavailable (nicht verfügbar)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

MAXSIze
: Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können einen der folgenden Werte angeben:

  NOLimit
  : Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

  maximale_Dateigröße
  : Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl zwischen 1 und 999999 Terabyte gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 Gigabyte ist. Maßstabsfaktoren sind:

Maßstabsfaktor	**Bedeutung**
K	Kilobyte
M	Megabyte
G	Gigabyte
T	Terabyte

Der Client schätzt die Größe der Dateien, die an den Server gesendet werden. Die Schätzung des Clients wird verwendet und nicht das tatsächliche Datenvolumen, das an den Server gesendet wird. Clientoptionen, wie z. B. Deduplizierung, Komprimierung und Verschlüsselung, können zur Folge haben, dass das tatsächliche Datenvolumen, das an den Server gesendet wird, größer oder kleiner als die Größenschätzung ist. Beispielsweise kann eine komprimierte Datei kleiner als die Schätzung sein, sodass weniger Daten als der Schätzwert gesendet werden. Des Weiteren kann eine Binärdatei nach der Komprimierungsverarbeitung größer sein, sodass mehr Daten als der Schätzwert gesendet werden.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

Tabelle 1. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool

Dateigröße	**Angegebener Pool**	**Ergebnis**
Überschreitet die maximale Größe	Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben	Die Datei wird vom Server nicht gespeichert
	Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben	Der Server speichert die Datei im nächsten Speicherpool, der die Dateigröße akzeptiert

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSIze=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Bei mehreren Dateien, die in einer einzelnen Transaktion gesendet werden, betrachtet der Server die Größe der Transaktion als Dateigröße. Wenn die Gesamtgröße aller Dateien in der Transaktion die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

Einschränkung:

Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

CRCData
: Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

  Yes
  : Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

  No
  : Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

  Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

  Tipp:

  Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

  Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

  - IBM® LTO5 und höher
  - IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
  - Oracle StorageTek T10000C- und T10000D-Laufwerke

NEXTstgpool
: Gibt einen primären Speicherpool an, in den Dateien umgelagert werden. Sie können keine Daten aus einem Speicherpool mit sequenziellem Zugriff in einen Speicherpool mit wahlfreiem Zugriff umlagern. Dieser Parameter ist wahlfrei.

  Verfügt dieser Speicherpool nicht über einen nächsten Speicherpool, kann der Server nicht Dateien aus diesem Speicherpool umlagern und Dateien, die die maximale Größe für diesen Speicherpool überschreiten, nicht in einem anderen Speicherpool speichern.

  Ist in dem aktuellen Speicherpool nicht genügend Speicherbereich verfügbar, erlaubt der Parameter NEXTSTGPOOL für Speicherpools mit sequenziellem Zugriff nicht das Speichern von Daten im nächsten Pool. In diesem Fall gibt der Server eine Nachricht aus, und die Transaktion schlägt fehl.

  Für nächste Speicherpools mit dem Einheitentyp FILE führt der Server eine vorläufige Überprüfung durch, um zu bestimmen, ob genügend Speicherbereich verfügbar ist. Ist kein Speicherbereich verfügbar, springt der Server zum nächsten Speicherpool in der Hierarchie. Ist Speicherbereich verfügbar, versucht der Server, Daten in diesem Pool zu speichern. Die Speicheroperation kann jedoch fehlschlagen, wenn zum Zeitpunkt der tatsächlichen Speicheroperation der Speicherbereich nicht mehr verfügbar ist.

  Einschränkungen:

  - Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
  - Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
  - Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
  - Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.
  - Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
    - NETAPPDUMP
    - CELERRADUMP
    - NDMPDUMP

HIghmig
: Gibt an, dass der Server die Umlagerung startet, wenn die Speicherpoolauslastung diesen Prozentsatz erreicht. Für Plattenspeicherpools mit sequenziellem Zugriff (FILE) ist die Auslastung das Verhältnis der Daten in einem Speicherpool zur Summe der geschätzten

Datenkapazität des Pools, einschließlich der Kapazität aller für den Pool angegebenen Arbeitsdatenträger. Für Speicherpools, die Banddatenträger verwenden, ist die Auslastung das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100 angeben. Der Standardwert ist 90.

Wenn der Speicherpool die obere Umlagerungsschwelle überschreitet, kann der Server die Umlagerung von Dateien in den nächsten definierten Speicherpool nach Datenträger starten. Die obere Umlagerungsschwelle kann auf 100 gesetzt werden, um die Umlagerung für den Speicherpool zu verhindern.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

LOwmig
Gibt an, dass der Server die Umlagerung stoppt, wenn die Speicherpoolauslastung diesen Prozentsatz erreicht oder unter diesem Prozentsatz liegt. Für Plattenspeicherpools mit sequenziellem Zugriff (FILE) ist die Auslastung das Verhältnis der Daten in einem Speicherpool zur Summe der geschätzten Datenkapazität des Pools, einschließlich der Kapazität aller für den Pool angegebenen Arbeitsdatenträger. Für Speicherpools, die Banddatenträger verwenden, ist die Auslastung das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 99 angeben. Der Standardwert ist 70.

Wenn der Speicherpool die untere Umlagerungsschwelle erreicht, wird die Umlagerung von Dateien von einem anderen Datenträger von dem Server nicht gestartet. Die Angabe von 0 für die untere Umlagerungsschwelle erlaubt eine Umlagerung, um den Speicherpool zu leeren.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLaim
Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der Datenbank gelöscht wurden.

Bei der Wiederherstellung wird der zerstückelte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien von einem Datenträger auf einen anderen wieder verwendbar, wodurch der ursprüngliche Datenträger wiederverwendet werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Standardwert ist 60, außer für Speicherpools, die WORM-Einheiten verwenden.

 AIX-Betriebssysteme  Windows-BetriebssystemeFür Speicherpools, die eine Einheitenklasse WORM verwenden, kann der Standardwert 100 verringert werden. Damit wird es dem Server ermöglicht, Daten bei Bedarf auf weniger Datenträger zusammenzulegen. Datenträger, die durch die Wiederherstellung geleert werden, können aus dem Kassettenarchiv entnommen werden, wodurch Schächte für neue Datenträger freigegeben werden. Da die Datenträger nur einmal beschrieben werden können, ist eine Wiederverwendung der Datenträger nicht möglich.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Einen Wert von 50 Prozent oder höher für diesen Parameter angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMPRocess
Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1. Sie können einen oder mehrere Wiederherstellungsprozesse für jeden primären Speicherpool mit sequenziellem Zugriff angeben.
Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Wenn der Parameter RECLAIMSTGPOOL nicht angegeben ist oder der Wiederherstellungsspeicherpool dieselbe Einheitenklasse wie der Speicherpool hat, der wiederhergestellt wird, benötigt jeder Prozess zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 16 haben.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMSTGpool
Gibt einen anderen primären Speicherpool als Ziel für wiederhergestellte Daten aus diesem Speicherpool an. Dieser Parameter ist wahlfrei. Wenn der Server Datenträger für den Speicherpool zurückfordert, versetzt der Server nicht verfallene Daten von den Datenträgern, die zurückgefordert werden, in den Speicherpool, der in diesem Parameter angegeben ist.

Ein Wiederherstellungsspeicherpool ist besonders nützlich für einen Speicherpool, der nur ein Laufwerk in seinem Kassettenarchiv hat. Wird dieser Parameter angegeben, versetzt der Server alle Daten von den zurückgeforderten Datenträgern in den Wiederherstellungsspeicherpool, unabhängig von der Anzahl der Laufwerke in dem Kassettenarchiv.

Um die Daten aus dem Wiederherstellungsspeicherpool wieder in den ursprünglichen Speicherpool zu versetzen, ist die Speicherpoolhierarchie zu verwenden. Den ursprünglichen Speicherpool als nächsten Speicherpool für den Wiederherstellungsspeicherpool angeben.

Einschränkung:

- Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAMATIONType
Gibt die Methode an, mit der Datenträger wiederhergestellt und verwaltet werden. Dieser Parameter ist wahlfrei. Der Standardwert ist THRESHOLD. Gültige Werte:

THRESHold
Gibt an, dass Datenträger, die zu diesem Speicherpool gehören, gemäß dem Schwellenwert im Attribut RECLAIM für diesen Speicherpool wiederhergestellt werden.

SNAPlock
Gibt an, dass FILE-Datenträger, die zu diesem Speicherpool gehören, mit NetApp Data ONTAP-Software und NetApp SnapLock-Datenträgern für die Aufbewahrung verwaltet werden. Dieser Parameter ist nur für Speicherpools gültig, die für einen Server definiert sind, auf dem der Aufbewahrungsschutz für Daten aktiviert ist und der einer Einheitenklasse FILE zugeordnet ist. Datenträger in diesem Speicherpool werden nicht anhand des Schwellenwerts wiederhergestellt. Der RECLAIM-Wert für den Speicherpool wird ignoriert.

Alle Datenträger in diesem Speicherpool werden als FILE-Datenträger erstellt. Ein Aufbewahrungsdatum, das von den Aufbewahrungsattributen in der Archivierungskopiengruppe für den Speicherpool abgeleitet wird, wird in den Metadaten für den FILE-Datenträger mit der SnapLock-Funktion des Betriebssystems NetApp Data ONTAP definiert. Bis zum Ablauf des Aufbewahrungsdatums können der FILE-Datenträger und alle darauf befindlichen Daten nicht von dem physischen SnapLock-Datenträger gelöscht werden, auf dem sie gespeichert sind.

Der Parameter RECLAMATIONTYPE muss für alle Speicherpools, die definiert werden, identisch sein, wenn er für denselben Einheitenklassennamen definiert wird. Der Befehl DEFINE kann fehlschlagen, wenn der angegebene Parameter RECLAMATIONTYPE von der Angabe abweicht, die für Speicherpools definiert ist, die bereits für den Einheitenklassennamen definiert wurden.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

COLlocate
Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei. Der Standardwert ist GROUP.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger. Die Kollokation kann sich auch auf die Anzahl Prozesse zum Umlagern von Platten in den sequenziellen Pool auswirken.

Sie können eine der folgenden Optionen angeben:

No
: Gibt an, dass die Kollokation inaktiviert ist. Während der Umlagerung von Platte werden Prozesse auf einer Dateibereichsebene erstellt.

GRoup
: Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

  Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

  Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

  - Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
  - Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.
  - Während der Umlagerung von Platte erstellt der Server Umlagerungsprozesse auf der Kollokationsgruppenebene für gruppierte Knoten und auf der Knotenebene für nicht gruppierte Knoten.

  Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

  - Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
  - Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.
  - Während der Umlagerung von Platte erstellt der Server Umlagerungsprozesse auf der Kollokationsgruppenebene für gruppierte Dateibereiche.

  Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

NODe
: Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

  Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

  Bei COLLOCATE=NODE erstellt der Server Prozesse auf der Knotenebene, wenn Daten von Platte umgelagert werden.

FIlespace
: Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

  Bei COLLOCATE=FILESPACE erstellt der Server Prozesse auf der Dateibereichsebene, wenn Daten von Platte umgelagert werden.

MAXSCRatch (Erforderlich)
: Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

  Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Speicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Speicherpools geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Wenn Arbeitsdatenträger mit dem Einheitentyp FILE gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

REUsedelay
Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert ist 0, was bedeutet, dass ein Datenträger neu beschrieben oder in den Arbeitsdatenträgerpool zurückgestellt werden kann, sobald alle Dateien von dem Datenträger gelöscht wurden.
Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Speicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl entsprechen.

OVFLOcation
Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.
Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGDelay
Gibt die Mindestanzahl Tage an, die eine Datei in einem Speicherpool verbleiben muss, bevor sie für die Umlagerung ausgewählt werden kann. Alle Dateien auf einem Datenträger müssen für die Umlagerung auswählbar sein, bevor der Server den Datenträger für die Umlagerung auswählt. Um einen Wert zu berechnen, der mit dem angegebenen Wert für MIGDELAY verglichen wird, zählt der Server die Anzahl der Tage, die die Datei im Speicherpool war.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert 0 gibt an, dass die Umlagerung nicht verzögert werden soll. Soll der Server die Anzahl der Tage nur ab dem Tag zählen, an dem eine Datei gespeichert wurde, und nicht ab dem Tag, an dem sie abgerufen wurde, die Serveroption NORETRIEVEDATE verwenden.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGContinue
Gibt an, ob der Server Dateien umlagern darf, die der Verzögerungszeit für die Umlagerung nicht entsprechen. Dieser Parameter ist wahlfrei. Der Standardwert ist YES.

Da angegeben werden kann, dass Dateien eine Mindestanzahl Tage in dem Speicherpool verbleiben müssen, kann der Server alle auswählbaren Dateien in den nächsten Speicherpool umlagern, obwohl sie dem Wert für die untere Umlagerungsschwelle nicht entsprechen. Mit diesem Parameter kann angegeben werden, ob der Server den Umlagerungsprozess fortsetzen darf, indem Dateien umgelagert werden, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sie können einen der folgenden Werte angeben:

Yes
Muss die untere Umlagerungsschwelle eingehalten werden, gibt dieser Wert an, dass der Server mit der Umlagerung von Dateien fortfährt, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sind mehrere Umlagerungsprozesse für den Speicherpool zulässig, werden einige Dateien, die der Verzögerungszeit für die Umlagerung nicht entsprechen, unter Umständen unnötigerweise umgelagert. Während ein Prozess Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte ein zweiter Prozess mit der Umlagerung von Dateien beginnen, die der Verzögerungszeit für die Umlagerung nicht entsprechen, um die untere Umlagerungsschwelle einzuhalten. Der erste Prozess, der noch Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte selbst die Einhaltung der unteren Umlagerungsschwelle bewirkt haben.

No
Gibt an, dass der Server die Umlagerung stoppt, wenn keine auswählbaren Dateien mehr für die Umlagerung verfügbar sind; dies gilt auch vor Erreichen der unteren Umlagerungsschwelle. Der Server lagert nur Dateien um, die der Verzögerungszeit für die Umlagerung entsprechen.

MIGPRocess
Gibt die Anzahl paralleler Prozesse für das Umlagern der Dateien von den Datenträgern in diesen Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1.

Bei der Berechnung des Werts für diesen Parameter ist die Anzahl der sequenziellen Speicherpools, die von der Umlagerung betroffen sind, und die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die der Operation zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect- und Systemaktivitäten sowie von den Grenzwerten für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Umlagerung betroffen sind.

Beispiel: Angenommen, Sie möchten gleichzeitig die Dateien von Datenträgern in zwei primären sequenziellen Speicherpools umlagern und Sie möchten drei Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Hat der Speicherpool, in den Dateien umgelagert werden, dieselbe Einheitenklasse wie der Speicherpool, aus dem Dateien umgelagert werden, benötigt jeder Prozess zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um sechs Umlagerungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 12 Mountpunkte und 12 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 12 haben.

Überschreitet die angegebene Anzahl der Umlagerungsprozesse die Anzahl der verfügbaren Mountpunkte oder Laufwerke, warten die Prozesse, die keine Mountpunkte oder Laufwerke anfordern können, bis Mountpunkte oder Laufwerke verfügbar werden. Werden Mountpunkte oder Laufwerke innerhalb der MOUNTWAIT-Zeit nicht verfügbar, werden die Umlagerungsprozesse beendet. Informationen zur Angabe der MOUNTWAIT-Zeit befinden sich in DEFINE DEVCLASS (Einheitenklasse definieren).

Der IBM Spectrum Protect-Server startet die angegebene Anzahl der Umlagerungsprozesse, unabhängig von der Anzahl der Datenträger, die für die Umlagerung ausgewählt werden können. Geben Sie beispielsweise zehn Umlagerungsprozesse an und können nur sechs Datenträger für die Umlagerung ausgewählt werden, startet der Server zehn Prozesse, von denen vier beendet werden, ohne dass ein Datenträger verarbeitet wird.

Tipp: Beachten Sie bei der Angabe dieses Parameters, ob die Funktion für simultanes Schreiben für die Serverdatenumlagerung aktiviert ist. Jeder Umlagerungsprozess erfordert einen Mountpunkt und ein Laufwerk für jeden Kopienspeicherpool und Pool für aktive Daten, der für den Zielspeicherpool definiert ist.
Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

DATAFormat
Gibt das Datenformat an, das zum Sichern von Dateien in diesem Speicherpool und zum Zurückschreiben von Dateien aus diesem Speicherpool verwendet werden soll. Das Standardformat ist das NATIVE-Serverformat. Sie können die folgenden Werte angeben:

NATive
Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und Block-Header einschließt.
NONblock
Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und keine Block-Header einschließt.
Die standardmäßige Mindestblockgröße auf einem Datenträger, der der Einheitenklasse FILE zugeordnet ist, beträgt 256 KB, unabhängig davon, wie viele Daten auf den Datenträger geschrieben werden. Für bestimmte Tasks können Sie die ineffiziente Speichernutzung auf Speicherdatenträgern minimieren, indem Sie das Datenformat NONBLOCK angeben. Sie können beispielsweise das Datenformat NONBLOCK für die folgenden Tasks angeben:

- Verwendung von Content-Management-Produkten
- Verwendung der Clientoption DIRMC zum Speichern von Verzeichnisinformationen
- Umlagerung sehr kleiner Dateien mit IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows

In den meisten Situationen wird jedoch das native Format bevorzugt.
NETAPPDump
Gibt an, dass die Daten das NetApp-Speicherauszugsformat haben. Dieses Datenformat muss für Dateisystemimages angegeben werden, die ein Speicherauszugsformat haben und die von einem NetApp-Dateiserver oder einem IBM System Storage N Series-Dateiserver unter Verwendung von NDMP gesichert wurden. Der Server führt keine Umlagerung, Wiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=NETAPPDUMP aus. Mit dem Befehl MOVE DATA können Sie Daten aus einem primären Speicherpool in einen anderen primären Speicherpool oder von einem Datenträger versetzen, wenn der Datenträger wiederverwendet werden muss.
CELERRADump
Gibt an, dass die Daten das EMC Celerra-Speicherauszugsformat haben. Dieses Datenformat muss für Dateisystemimages angegeben werden, die ein Speicherauszugsformat haben und die von einem EMC Celerra-Dateiserver unter Verwendung von NDMP gesichert wurden. Der Server führt keine Umlagerung, Wiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=CELERRADUMP aus. Mit dem Befehl MOVE DATA können Sie Daten aus einem primären Speicherpool in einen anderen primären Speicherpool oder von einem Datenträger versetzen, wenn der Datenträger wiederverwendet werden muss.
NDMPDump

Gibt an, dass die Daten ein lieferantenspezifisches NAS-Sicherungsformat haben. Verwenden Sie dieses Datenformat für Dateisystemimages, die von einem NAS-Dateiserver gesichert wurden, der kein NetApp-Dateiserver oder EMC Celerra-Dateiserver ist. Der Server führt keine Umlagerung, Wiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=NDMPDUMP aus. Mit dem Befehl MOVE DATA können Sie Daten aus einem primären Speicherpool in einen anderen primären Speicherpool oder von einem Datenträger versetzen, wenn der Datenträger wiederverwendet werden muss.

AUTOCopy
Gibt an, wann IBM Spectrum Protect Operationen mit simultanem Schreiben ausführt. Der Standardwert ist CLIENT. Dieser Parameter ist wahlfrei und betrifft die folgenden Operationen:

- Clientspeichersitzungen
- Serverimportprozesse
- Serverdatenumlagerungsprozesse

Wenn die Option AUTOCOPY auf `ALL` oder `CLIENT` gesetzt wird und mindestens ein Speicherpool vorhanden ist, der in der Option COPYSTGPOOLS oder ACTIVEDATAPOOLS aufgelistet ist, wird die clientseitige Deduplizierung inaktiviert.

Tritt ein Fehler auf, wenn Daten während eines Umlagerungsprozesses gleichzeitig in einen Kopienspeicherpool oder einen Pool für aktive Daten geschrieben werden, stoppt der Server das Schreiben in die fehlerhaften Speicherpools für den Rest des Prozesses. Der Server speichert jedoch weiterhin Dateien in dem primären Speicherpool und in allen verbleibenden Kopienspeicherpools oder Pools für aktive Daten. Diese Pools bleiben für die Dauer des Umlagerungsprozesses aktiv. Kopienspeicherpools werden mit dem Parameter COPYSTGPOOLS angegeben. Pools für aktive Daten werden mit dem Parameter ACTIVEDATAPOOLS angegeben.

Sie können einen der folgenden Werte angeben:

None
Gibt an, dass die Funktion für simultanes Schreiben inaktiviert ist.
CLient
Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen oder Serverimportprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverimportprozessen werden Daten nur gleichzeitig in Kopienspeicherpools geschrieben. Daten werden während der Ausführung von Serverimportprozessen nicht in Pools für aktive Daten geschrieben.
MIGRation
Gibt an, dass Daten nur während der Umlagerung in diesen Speicherpool gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverdatenumlagerungsprozessen werden Daten in Kopienspeicherpools und Pools für aktive Daten nur dann gleichzeitig geschrieben, wenn die Daten in diesen Pools nicht vorhanden sind. Knoten, deren Daten umgelagert werden, müssen sich in einer Domäne befinden, die einem Pool für aktive Daten zugeordnet ist. Befinden sich die Knoten nicht in einer Domäne, die einem Pool für aktive Daten zugeordnet ist, können die Daten nicht in den Pool geschrieben werden.
All
Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen oder Serverdatenumlagerungsprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Mit diesem Wert wird sichergestellt, dass Daten immer dann gleichzeitig geschrieben werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

COPYSTGpools
Gibt die Namen von Kopienspeicherpools an, in die der Server gleichzeitig Daten schreibt. Der Parameter COPYSTGPOOLS ist optional. Sie können maximal drei Kopienpoolnamen angeben, die durch Kommas voneinander getrennt werden müssen. Leerzeichen zwischen den Namen der Kopienpools sind nicht zulässig. Wenn Sie einen Wert für den Parameter COPYSTGPOOLS angeben, können Sie auch einen Wert für den Parameter COPYCONTINUE angeben.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSTGPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Kopienspeicherpools und den Wert für COPYCONTINUE aus dem primären Speicherpool. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann während der Ausführung der folgenden Operationen Daten gleichzeitig in Kopienspeicherpools schreiben:

- Sicherungs- und Archivierungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder Anwendungsclients, die die IBM Spectrum Protect-API verwenden
- Umlagerungsoperationen durch IBM Spectrum Protect for Space Management-Clients
- Importoperationen, die das Kopieren von exportierten Dateidaten von externen Datenträgern in einen Speicherpool einbeziehen, der mit einer Kopienspeicherpoolliste definiert ist

Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat NATIVE oder NONBLOCK verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
    - NETAPPDUMP
    - CELERRADUMP

- NDMPDUMP

2. Das simultane Schreiben in Kopienspeicherpools wird nicht unterstützt, wenn die LAN-unabhängige Datenversetzung verwendet wird. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
3. Die Funktion für simultanes Schreiben wird für NAS-Sicherungsoperationen nicht unterstützt. Sind für den primären Speicherpool, der in DESTINATION oder TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Kopienspeicherpools definiert, werden die Kopienspeicherpools ignoriert und die Daten werden nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.

Achtung: Die mit dem Parameter COPYSTGPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl BACKUP STGPOOL ersetzen. Wird der Parameter COPYSTGPOOLS verwendet, verwenden Sie weiterhin den Befehl BACKUP STGPOOL, um sicherzustellen, dass die Kopienspeicherpools vollständige Kopien des primären Speicherpools sind. Es gibt Fälle, in denen eine Kopie möglicherweise nicht erstellt wird. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

COPYContinue

Gibt an, wie der Server auf einen Fehler beim Schreiben in einen der Kopienspeicherpools reagiert, die im Parameter COPYSTGPOOLS aufgelistet sind. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Wenn Sie den Parameter COPYCONTINUE angeben, müssen Sie auch den Parameter COPYSTGPOOLS angeben.

Der Parameter COPYCONTINUE hat keine Auswirkung auf die Funktion für simultanes Schreiben während der Umlagerung.

Sie können die folgenden Werte angeben:

Yes
: Ist der Parameter COPYCONTINUE auf YES gesetzt, stoppt der Server das Schreiben in die fehlerhaften Kopienpools für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Kopienpools fort. Die Liste der Kopienspeicherpools ist nur für die Dauer der Clientsitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.

No
: Ist der Parameter COPYCONTINUE auf NO gesetzt, wird die aktuelle Transaktion vom Server nicht ausgeführt und die Speicheroperation nicht fortgesetzt.

Einschränkungen:

- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf Pools für aktive Daten. Tritt für einen der Pools für aktive Daten ein Schreibfehler auf, stoppt der Server das Schreiben in den fehlerhaften Pool für aktive Daten für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Pools für aktive Daten und Kopienspeicherpools fort. Die Liste der Pools für aktive Daten ist nur für die Dauer der Sitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Ausführung eines Serverimportprozesses. Werden Daten gleichzeitig geschrieben und tritt für den primären Speicherpool oder einen Kopienspeicherpool ein Schreibfehler auf, schlägt der Serverimportprozess fehl.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Serverdatenumlagerung. Werden Daten gleichzeitig geschrieben und tritt für einen Kopienspeicherpool oder Pool für aktive Daten ein Schreibfehler auf, wird der fehlerhafte Speicherpool entfernt und der Datenumlagerungsprozess wird fortgesetzt. Bei Schreibfehlern für den primären Speicherpool schlägt der Umlagerungsprozess fehl.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

ACTIVEDATApools

Gibt die Namen der Pools für aktive Daten an, in die der Server während einer Clientsicherungsoperation gleichzeitig Daten schreibt. Der Parameter ACTIVEDATAPOOLS ist optional. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Pools für aktive Daten aus dem Zielspeicherpool, der in der Kopiengruppe angegeben ist. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann nur während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients, die die IBM Spectrum Protect-API verwenden, Daten gleichzeitig in Pools für aktive Daten schreiben.
Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat NATIVE oder NONBLOCK verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
   - NETAPPDUMP
   - CELERRADUMP
   - NDMPDUMP

2. Das simultane Schreiben in Pools für aktive Daten wird nicht unterstützt, wenn die LAN-unabhängige Datenversetzung verwendet wird. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
3. Die Funktion für simultanes Schreiben wird nicht unterstützt, wenn eine NAS-Sicherungsoperation eine Inhaltsverzeichnisdatei schreibt. Sind für den primären Speicherpool, der in TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Pools für aktive Daten definiert, werden die Pools für aktive Daten ignoriert und die Daten werden nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.
5. Daten, die importiert werden, werden nicht in Pools für aktive Daten gespeichert. Verwenden Sie nach einer Importoperation den Befehl COPY ACTIVEDATA, um die importierten Daten in einem Pool für aktive Daten zu speichern.

Achtung: Die mit dem Parameter ACTIVEDATAPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl COPY ACTIVEDATA ersetzen. Wird der Parameter ACTIVEDATAPOOLS verwendet, verwenden Sie den Befehl COPY ACTIVEDATA, um sicherzustellen, dass die Pools für aktive Daten alle aktiven Daten des primären Speicherpools enthalten.

DEDUPlicate
Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Der Standardwert ist NO.

IDENTIFYPRocess
Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Datendeduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 0 bis 50 ein. Der Standardwert ist 1. Hat der Parameter DEDUPLICATE den Wert NO, hat die Standardeinstellung für IDENTIFYPROCESS keine Auswirkung. Hinweis: Datendeduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Datendeduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Datendeduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Datendeduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

Beispiel: Einen primären Speicherpool mit einer Einheitenklasse 8MMTAPE definieren

Den primären Speicherpool 8MMPOOL für die Einheitenklasse 8MMTAPE (mit Einheitentyp 8MM) mit einer maximalen Dateigröße von 5 MB definieren. Alle Dateien, die größer sind als 5 MB, in untergeordneten Pools speichern (beginnend bei Pool POOL1). Die Kollokation von Dateien für Clientknoten aktivieren. Maximal 5 Arbeitsdatenträger für diesen Speicherpool zulassen.

```
define stgpool 8mmpool 8mmtape maxsize=5m
 nextstgpool=pool1 collocate=node
 maxscratch=5
```

Zugehörige Verweise:
SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsserie angeben)

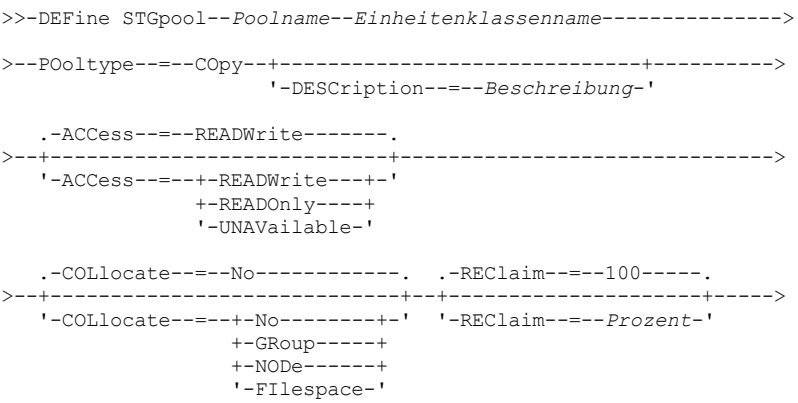
DEFINE STGPOOL (Kopienspeicherpool definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)

Mit diesem Befehl kann ein Kopienspeicherpool definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Anmerkungen:

1. Die Einstellung RECLAMATIONTYPE=SNAPLOCK ist nur für Speicherpools gültig, die für Server definiert sind, die für IBM Spectrum Protect for Data Retention aktiviert sind. Der Speicherpool muss einer Einheitenklasse FILE zugeordnet sein, und die in der Einheitenklasse angegebenen Verzeichnisse müssen NetApp SnapLock-Datenträger sein.
2. Die Werte NETAPPDUMP, CELERRADUMP und NDMPDUMP sind nicht für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
3. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
4. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

Parameter

Poolname (Erforderlich)
Gibt den Namen des Speicherpools an, der definiert werden soll. Der Name muss eindeutig sein, und die maximale Länge beträgt 30 Zeichen.

Einheitenklassenname (Erforderlich)
Gibt den Namen der Einheitenklasse für den sequenziellen Zugriff an, der dieser Kopienspeicherpool zugeordnet ist. Mit Ausnahme von DISK kann jede Einheitenklasse angegeben werden.

POoltype=COpy (Erforderlich)
Gibt an, dass ein Kopienspeicherpool definiert werden soll.

DESCription
Gibt eine Beschreibung des Kopienspeicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

ACCess
Gibt an, wie Clientknoten und Serverprozesse (wie Wiederherstellung) auf Dateien im Kopienspeicherpool zugreifen können. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Sie können die folgenden Werte angeben:

READWrite
Gibt an, dass Dateien auf die Datenträger im Kopienspeicherpool geschrieben und daraus gelesen werden können.

READOnly
Gibt an, dass Clientknoten Dateien, die auf den Datenträgern im Kopienspeicherpool gespeichert sind, nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Kopienspeicherpool verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Kopienspeicherpool sind jedoch keine neuen Schreiboperationen durch Datenträger außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht im Kopienspeicherpool gesichert werden.

UNAVailable
Gibt an, dass Clientknoten nicht auf Dateien zugreifen können, die auf Datenträgern im Kopienspeicherpool gespeichert sind.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Kopienspeicherpool verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Kopienspeicherpool sind jedoch keine neuen Schreiboperationen durch Datenträger außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht im Kopienspeicherpool gesichert werden.

COLlocate
Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger.

Sie können eine der folgenden Optionen angeben:

No
Gibt an, dass die Kollokation inaktiviert ist.
GRoup
Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.

Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

NODe
Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

FIlespace
Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

RECLaim
Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

Bei der Wiederherstellung wird der zerstückelte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien von einem Datenträger auf einen anderen wieder verwendbar, wodurch der ursprüngliche Datenträger wiederverwendet werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Standardwert 100 bedeutet, dass keine Wiederherstellung erfolgt.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Wird der Standardwert geändert, einen Wert von 50 Prozent oder höher angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

Wenn ein ausgelagerter Kopienspeicherpooldatenträger für die Wiederherstellung ausgewählt werden kann, versucht der Wiederherstellungsprozess, die nicht verfallenen Dateien auf einem zurückforderbaren Datenträger aus einem primären Speicherpool oder einem Kopienspeicherpool vor Ort abzurufen. Der Prozess schreibt dann diese Dateien auf einen verfügbaren Datenträger in dem ursprünglichen Kopienspeicherpool. Tatsächlich werden diese Dateien wieder an den Standort vor Ort versetzt. Die Dateien können jedoch nach einem Katastrophenfall auch vom ausgelagerten Datenträger abgerufen werden, wenn eine Datenbanksicherung verwendet wird, die auf die Dateien auf dem ausgelagerten Datenträger verweist. Wegen der Art, mit der ausgelagerte Datenträger bei der Wiederherstellung bearbeitet werden, sollte die Wiederherstellung bei Kopienspeicherpools mit Vorsicht verwendet werden.

RECLAIMPRocess
Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1.
Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Jeder Prozess benötigt zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 16 haben.

Sie können einen oder mehrere Wiederherstellungsprozesse für jeden Kopienspeicherpool angeben. Sie können mehrere gleichzeitig ablaufende Wiederherstellungsprozesse für einen einzelnen Kopienspeicherpool angeben. Damit wird eine bessere Nutzung Ihrer verfügbaren Bandlaufwerke oder FILE-Datenträger erreicht. Wenn die gleichzeitig ablaufende Verarbeitung mehrerer Prozesse nicht erforderlich ist, geben Sie den Wert 1 für den Parameter RECLAIMPROCESS an.

RECLAMATIONType
Gibt die Methode an, mit der Datenträger wiederhergestellt und verwaltet werden. Dieser Parameter ist wahlfrei. Der Standardwert ist THRESHOLD. Gültige Werte:

THRESHold
Gibt an, dass Datenträger, die zu diesem Speicherpool gehören, gemäß dem Schwellenwert im Attribut RECLAIM für diesen Speicherpool wiederhergestellt werden.

SNAPlock
Gibt an, dass FILE-Datenträger, die zu diesem Speicherpool gehören, mit NetApp Data ONTAP-Software und NetApp SnapLock-Datenträgern für die Aufbewahrung verwaltet werden. Dieser Parameter ist nur für Speicherpools gültig, die für einen Server definiert sind, auf dem der Aufbewahrungsschutz für Daten aktiviert ist und der einer Einheitenklasse FILE zugeordnet ist. Datenträger in diesem Speicherpool werden nicht anhand des Schwellenwerts wiederhergestellt. Der RECLAIM-Wert für den Speicherpool wird ignoriert.

Alle Datenträger in diesem Speicherpool werden als FILE-Datenträger erstellt. Ein Aufbewahrungsdatum, das von den Aufbewahrungsattributen in der Archivierungskopiengruppe für den Speicherpool abgeleitet wird, wird in den Metadaten für den FILE-Datenträger mit der SnapLock-Funktion des Betriebssystems NetApp Data ONTAP definiert. Bis zum Ablauf des Aufbewahrungsdatums können der FILE-Datenträger und alle darauf befindlichen Daten nicht von dem physischen SnapLock-Datenträger gelöscht werden, auf dem sie gespeichert sind.

Der Parameter RECLAMATIONTYPE muss für alle Speicherpools, die definiert werden, identisch sein, wenn er für denselben Einheitenklassennamen definiert wird. Der Befehl DEFINE schlägt fehl, wenn der angegebene Parameter RECLAMATIONTYPE von der Angabe abweicht, die für Speicherpools definiert ist, die bereits für den Einheitenklassennamen definiert wurden.

OFFSITERECLAIMLimit
Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool zurückgefordert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können die folgenden Werte angeben:

NOLimit
Gibt an, dass der Speicherbereich auf allen ausgelagerten Datenträgern wiederhergestellt werden soll.

Anzahl
Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich wiederhergestellt werden soll. Sie können eine ganze Zahl von 0 bis 99999 angeben. Der Wert 0 bedeutet, dass für keine ausgelagerten Datenträger der Speicherbereich wiederhergestellt wird.
Tipp:

Um den Wert für OFFSITERECLAIMLIMIT zu bestimmen, verwenden Sie die statistischen Informationen in der Nachricht, die am Ende der Wiederherstellungsoperation für den ausgelagerten Datenträger ausgegeben wird. Die statistischen Informationen umfassen die folgenden Elemente:

- Die Anzahl der ausgelagerten Datenträger, die verarbeitet wurden
- Die Anzahl der parallelen Prozesse, die verwendet wurden
- Die Gesamtzeit, die für die Verarbeitung benötigt wurde

Die Reihenfolge, in der ausgelagerte Datenträger wiederhergestellt werden, basiert auf dem Umfang des freien Speicherplatzes auf einem Datenträger. (Freier Speicherplatz umfasst den Speicherbereich, der auf dem Datenträger nie verwendet wurde, und den Speicherbereich, der aufgrund des Löschens von Dateien frei geworden ist.) Datenträger mit dem größten freien Speicherplatz werden zuerst wiederhergestellt.

Beispiel: Angenommen, ein Kopienspeicherpool enthält drei Datenträger: VOL1, VOL2 und VOL3. VOL1 hat den größten freien Speicherplatz, und VOL3 hat den kleinsten freien Speicherplatz. Weiter wird angenommen, dass der Prozentsatz des freien Speicherplatzes auf jedem der drei Datenträger größer als der Wert des Parameters RECLAIM ist. Wird kein Wert für den Parameter OFFSITERECLAIMLIMIT angegeben, werden alle drei Datenträger wiederhergestellt, wenn die Wiederherstellung ausgeführt wird. Wird der Wert 2 angegeben, werden nur VOL1 und VOL2 bei der Wiederherstellung wiederhergestellt. Wird der Wert 1 angegeben, wird nur VOL1 wiederhergestellt.

MAXSCRatch (Erforderlich)
Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern nach Bedarf erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Kopienspeicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Kopienspeicherpools geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Lautet jedoch der Zugriffsmodus für einen Arbeitsdatenträger OFFSITE, wird der Datenträger erst dann aus dem Kopienspeicherpool gelöscht, wenn der Zugriffsmodus geändert wird. Ein Administrator kann dann den Server nach leeren ausgelagerten Arbeitsdatenträgern abfragen und diese an den Standort vor Ort zurückgeben.

Wenn Arbeitsdatenträger mit dem Einheitentyp FILE leer werden und gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

REUsedelay
Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert ist 0, was bedeutet, dass ein Datenträger neu beschrieben oder in den Arbeitsdatenträgerpool zurückgestellt werden kann, sobald alle Dateien von dem Datenträger gelöscht wurden.
Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Kopienspeicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl entsprechen.

OVFLOcation
Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

DATAFormat
Gibt das Datenformat an, das zum Sichern von Dateien in diesem Speicherpool und zum Zurückschreiben von Dateien aus diesem Speicherpool verwendet werden soll. Das Standardformat ist das NATIVE-Serverformat. Sie können die folgenden Werte angeben:

NATive

Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und Block-Header einschließt.

NONblock
: Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und keine Block-Header einschließt.
Die standardmäßige Mindestblockgröße auf einem Datenträger, der der Einheitenklasse FILE zugeordnet ist, beträgt 256 KB, unabhängig davon, wie viele Daten auf den Datenträger geschrieben werden. Für bestimmte Tasks können Sie die ineffiziente Speichernutzung auf Speicherdatenträgern minimieren, indem Sie das Datenformat NONBLOCK angeben. Sie können beispielsweise das Datenformat NONBLOCK für die folgenden Tasks angeben:

- Verwendung von Content-Management-Produkten
- Verwendung der Clientoption DIRMC zum Speichern von Verzeichnisinformationen
- Umlagerung sehr kleiner Dateien mit IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows

In den meisten Situationen wird jedoch das native Format bevorzugt.

NETAPPDump
: Gibt an, dass die Daten das NetApp-Speicherauszugsformat haben. Geben Sie dieses Datenformat nicht für Dateisystemimages an, die ein Speicherauszugsformat haben und die von einem NetApp-Dateiserver unter Verwendung von NDMP gesichert wurden. Der Server führt keine Speicherpoolwiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=NETAPPDUMP aus. Sie können den Befehl MOVE DATA verwenden, um NDMP-generierte Daten von einem Datenträger zu versetzen, wenn der Datenträger wiederverwendet werden muss.

CELERRADump
: Gibt an, dass die Daten das EMC Celerra-Speicherauszugsformat haben. Geben Sie dieses Datenformat nicht für Dateisystemimages an, die ein Speicherauszugsformat haben und die von einem EMC Celerra-Dateiserver unter Verwendung von NDMP gesichert wurden. Der Server führt keine Speicherpoolwiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=CELERRADUMP aus. Sie können den Befehl MOVE DATA verwenden, um NDMP-generierte Daten von einem Datenträger zu versetzen, wenn der Datenträger wiederverwendet werden muss.

NDMPDump
: Gibt an, dass die Daten ein lieferantenspezifisches NAS-Sicherungsformat haben. Geben Sie dieses Datenformat nicht für Dateisystemimages an, die ein Sicherungsformat haben und die von einem anderen NAS-Dateiserver als von einem NetApp- oder EMC Celerra-Dateiserver gesichert wurden. Der Server führt keine Speicherpoolwiederherstellung oder AUDIT VOLUME für einen Speicherpool mit DATAFORMAT=NDMPDUMP aus. Sie können den Befehl MOVE DATA verwenden, um NDMP-generierte Daten von einem Datenträger zu versetzen, wenn der Datenträger wiederverwendet werden muss.

CRCData
: Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

  Yes
  : Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

  No
  : Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

  Tipp:

  Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

  Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

  - IBM® LTO5 und höher
  - IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
  - Oracle StorageTek T10000C- und T10000D-Laufwerke

DEDUPlicate
: Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Der Standardwert ist NO.

IDENTIFYPRocess
: Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Datendeduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 0 bis 50 ein.

  Der Standardwert für diesen Parameter ist 0. Datendeduplizierungsprozesse für einen Kopienspeicherpool sind nicht erforderlich, wenn Sie Datendeduplizierungsprozesse für den primären Speicherpool angeben. Wenn IBM Spectrum Protect eine Datei in einem Speicherpool

analysiert, analysiert IBM Spectrum Protect die Datei auch in allen anderen Speicherpools.

Hinweis: Datendeduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Datendeduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Datendeduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Datendeduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

Beispiel: Einen Kopienspeicherpool mit einer Einheitenklasse DC480 definieren

Den Kopienspeicherpool TAPEPOOL2 für die Einheitenklasse DC480 definieren. Maximal 50 Arbeitsdatenträger für diesen Pool zulassen. Die Wiederverwendung der Datenträger um 45 Tage verzögern.

```
define stgpool tapepool2 dc480 pooltype=copy
 maxscratch=50 reusedelay=45
```

Zugehörige Verweise:
SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsserie angeben)

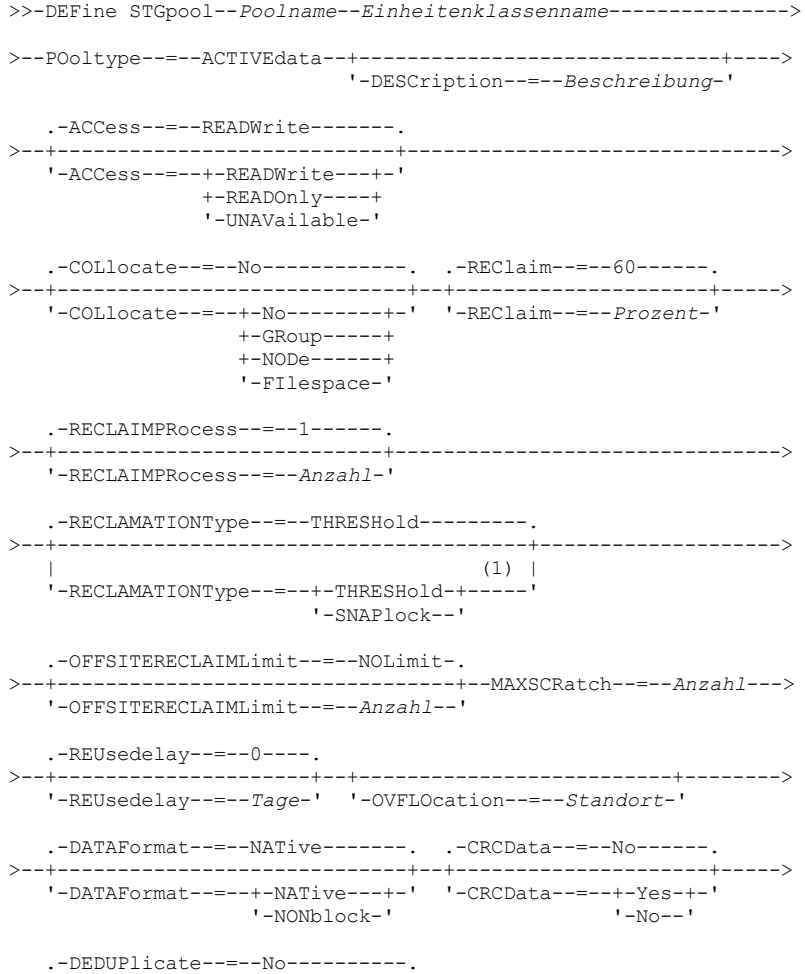
DEFINE STGPOOL (Pool für aktive Daten definieren, der Einheiten mit sequenziellem Zugriff zugeordnet wird)

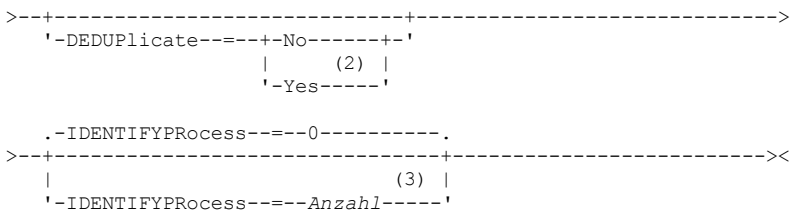
Mit diesem Befehl kann ein Pool für aktive Daten definiert werden, der Einheiten mit sequenziellem Zugriff zugeordnet wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax





Anmerkungen:

1. Die Einstellung RECLAMATIONTYPE=SNAPLOCK ist nur für Speicherpools gültig, die für Server definiert sind, die für IBM Spectrum Protect for Data Retention aktiviert sind. Der Speicherpool muss einer Einheitenklasse FILE zugeordnet sein, und die in der Einheitenklasse angegebenen Verzeichnisse müssen NetApp SnapLock-Datenträger sein.
2. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
3. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

Parameter

Poolname (Erforderlich)
: Gibt den Namen des Speicherpools an, der definiert werden soll. Der Name muss eindeutig sein, und die maximale Länge beträgt 30 Zeichen.

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse für den sequenziellen Zugriff an, der dieser Pool für aktive Daten zugeordnet ist. Mit Ausnahme von DISK kann jede Einheitenklasse angegeben werden.

POoltype=ACTIVEdata (Erforderlich)
: Gibt an, dass ein Pool für aktive Daten definiert werden soll.

DESCription
: Gibt eine Beschreibung des Pools für aktive Daten an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

ACCess
: Gibt an, wie Clientknoten und Serverprozesse (wie Wiederherstellung) auf Dateien im Pool für aktive Daten zugreifen können. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Sie können die folgenden Werte angeben:

  READWrite
  : Gibt an, dass Dateien auf die Datenträger im Pool für aktive Daten geschrieben und daraus gelesen werden können.

  READOnly
  : Gibt an, dass Clientknoten Dateien, die auf den Datenträgern im Pool für aktive Daten gespeichert sind, nur lesen können.

    Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Pool für aktive Daten verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Pool für aktive Daten sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht in den Pool für aktive Daten kopiert werden.

  UNAVailable
  : Gibt an, dass Clientknoten nicht auf Dateien zugreifen können, die auf Datenträgern im Pool für aktive Daten gespeichert sind.

    Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Pool für aktive Daten verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Pool für aktive Daten sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht in den Pool für aktive Daten kopiert werden.

COLlocate
: Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

  - Ein einzelner Clientknoten
  - Eine Gruppe von Dateibereichen
  - Eine Gruppe von Clientknoten
  - Ein Clientdateibereich

  Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

  Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger.

  Sie können eine der folgenden Optionen angeben:

  No
  : Gibt an, dass die Kollokation inaktiviert ist.

  GRoup

Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.

Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

NODe
: Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

  Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

FIlespace
: Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

RECLaim
: Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

  Bei der Wiederherstellung werden der fragmentierte Speicherbereich und der durch inaktive Sicherungsdateien belegte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien und der aktiven Sicherungsdateien von einem Datenträger auf einen anderen Datenträger wieder verwendbar. Mit dieser Aktion kann der ursprüngliche Datenträger wiederverwendet werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Standardwert ist 60.

  Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

  Wird der Standardwert geändert, einen Wert von 50 Prozent oder höher angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

  Wenn ein ausgelagerter Datenträger des Pools für aktive Daten für die Wiederherstellung ausgewählt werden kann, versucht der Wiederherstellungsprozess, die nicht verfallenen Dateien auf einem zurückforderbaren Datenträger aus einem primären Speicherpool oder einem Pool für aktive Daten vor Ort abzurufen. Der Prozess schreibt dann diese Dateien auf einen verfügbaren Datenträger in dem ursprünglichen Pool für aktive Daten. Tatsächlich werden diese Dateien wieder an den Standort vor Ort versetzt. Die Dateien können jedoch nach einem Katastrophenfall auch vom ausgelagerten Datenträger abgerufen werden, wenn eine Datenbanksicherung verwendet wird, die auf die Dateien auf dem ausgelagerten Datenträger verweist. Wegen der Art, mit der ausgelagerte Datenträger bei der Wiederherstellung bearbeitet werden, sollte die Wiederherstellung bei Pools mit aktiven Daten mit Vorsicht verwendet werden.

RECLAIMPRocess

Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Der Standardwert ist 1.
Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Jeder Prozess benötigt zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 16 haben.

Sie können einen oder mehrere Wiederherstellungsprozesse für jeden Pool für aktive Daten angeben. Sie können mehrere gleichzeitig ablaufende Wiederherstellungsprozesse für einen einzelnen Pool für aktive Daten angeben. Damit wird eine bessere Nutzung Ihrer verfügbaren Bandlaufwerke oder FILE-Datenträger erreicht. Wenn die gleichzeitig ablaufende Verarbeitung mehrerer Prozesse nicht erforderlich ist, geben Sie den Wert 1 für den Parameter RECLAIMPROCESS an.

RECLAMATIONType
Gibt die Methode an, mit der Datenträger wiederhergestellt und verwaltet werden. Dieser Parameter ist wahlfrei. Der Standardwert ist THRESHOLD. Gültige Werte:

THRESHold
Gibt an, dass Datenträger, die zu diesem Speicherpool gehören, gemäß dem Schwellenwert im Attribut RECLAIM für diesen Speicherpool wiederhergestellt werden.

SNAPlock
Gibt an, dass FILE-Datenträger, die zu diesem Speicherpool gehören, mit NetApp Data ONTAP-Software und NetApp SnapLock-Datenträgern für die Aufbewahrung verwaltet werden. Dieser Parameter ist nur für Speicherpools gültig, die für einen Server definiert werden, auf dem der Aufbewahrungsschutz für Daten aktiviert ist und der einer Einheitenklasse FILE zugeordnet ist. Datenträger in diesem Speicherpool werden nicht anhand des Schwellenwerts wiederhergestellt. Der RECLAIM-Wert für den Speicherpool wird ignoriert.

Alle Datenträger in diesem Speicherpool werden als FILE-Datenträger erstellt. Ein Aufbewahrungsdatum, das von den Aufbewahrungsattributen in der Archivierungskopiengruppe für den Speicherpool abgeleitet wird, wird in den Metadaten für den FILE-Datenträger mit der SnapLock-Funktion des Betriebssystems NetApp Data ONTAP definiert. Bis zum Ablauf des Aufbewahrungsdatums können der FILE-Datenträger und alle darauf befindlichen Daten nicht von dem physischen SnapLock-Datenträger gelöscht werden, auf dem sie gespeichert sind.

Der Parameter RECLAMATIONTYPE muss für alle Speicherpools, die definiert werden, identisch sein, wenn er für denselben Einheitenklassennamen definiert wird. Der Befehl DEFINE schlägt fehl, wenn der angegebene Parameter RECLAMATIONTYPE von der Angabe abweicht, die für Speicherpools definiert ist, die bereits für den Einheitenklassennamen definiert wurden.

OFFSITERECLAIMLimit
Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool zurückgefordert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Sie können die folgenden Werte angeben:

NOLimit
Gibt an, dass der Speicherbereich auf allen ausgelagerten Datenträgern wiederhergestellt werden soll.

Anzahl
Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich wiederhergestellt werden soll. Sie können eine ganze Zahl von 0 bis 99999 angeben. Der Wert 0 bedeutet, dass für keine ausgelagerten Datenträger der Speicherbereich wiederhergestellt wird.
Tipp:

Um den Wert für OFFSITERECLAIMLIMIT zu bestimmen, verwenden Sie die statistischen Informationen in der Nachricht, die am Ende der Wiederherstellungsoperation für den ausgelagerten Datenträger ausgegeben wird. Die statistischen Informationen umfassen die folgenden Elemente:

- Die Anzahl der ausgelagerten Datenträger, die verarbeitet wurden
- Die Anzahl der parallelen Prozesse, die verwendet wurden
- Die Gesamtzeit, die für die Verarbeitung benötigt wurde

Die Reihenfolge, in der ausgelagerte Datenträger wiederhergestellt werden, basiert auf dem Umfang des freien Speicherplatzes auf einem Datenträger. (Freier Speicherplatz umfasst den Speicherbereich, der auf dem Datenträger nie verwendet wurde, und den Speicherbereich, der aufgrund des Löschens von Dateien frei geworden ist.) Datenträger mit dem größten freien Speicherplatz werden zuerst wiederhergestellt.

Beispiel: Angenommen, ein Pool für aktive Daten enthält drei Datenträger: VOL1, VOL2 und VOL3. VOL1 hat den größten freien Speicherplatz, und VOL3 hat den kleinsten freien Speicherplatz. Weiter wird angenommen, dass der Prozentsatz des freien Speicherplatzes auf jedem der drei Datenträger größer als der Wert des Parameters RECLAIM ist. Wird kein Wert für den Parameter OFFSITERECLAIMLIMIT angegeben, werden alle drei Datenträger wiederhergestellt, wenn die Wiederherstellung ausgeführt wird. Wird der Wert 2 angegeben, werden nur VOL1 und VOL2 bei der Wiederherstellung wiederhergestellt. Wird der Wert 1 angegeben, wird nur VOL1 wiederhergestellt.

MAXSCRatch (Erforderlich)
Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern nach Bedarf erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Pool für aktive Daten verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Pools für aktive Daten geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Lautet jedoch der Zugriffsmodus für einen Arbeitsdatenträger OFFSITE, wird der Datenträger erst dann aus dem Pool für aktive Daten gelöscht, wenn der Zugriffsmodus geändert wird. Ein Administrator kann dann den Server nach leeren ausgelagerten Arbeitsdatenträgern abfragen und diese an den Standort vor Ort zurückgeben.

Wenn Arbeitsdatenträger mit dem Einheitentyp FILE leer werden und gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

REUsedelay
Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert ist 0, was bedeutet, dass ein Datenträger neu beschrieben oder in den Arbeitsdatenträgerpool zurückgestellt werden kann, sobald alle Dateien von dem Datenträger gelöscht wurden.
Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Pool für aktive Daten noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl entsprechen.

OVFLOcation
Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

DATAFormat
Gibt das Datenformat an, das zum Kopieren von Dateien in diesen Speicherpool und zum Zurückschreiben von Dateien aus diesem Speicherpool verwendet werden soll. Das Standardformat ist das NATIVE-Serverformat. Sie können die folgenden Werte angeben:

NATive
Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und Block-Header einschließt.

NONblock
Gibt an, dass das Datenformat das native IBM Spectrum Protect-Serverformat ist und keine Block-Header einschließt.
Die standardmäßige Mindestblockgröße auf einem Datenträger, der der Einheitenklasse FILE zugeordnet ist, beträgt 256 KB, unabhängig davon, wie viele Daten auf den Datenträger geschrieben werden. Für bestimmte Tasks können Sie die ineffiziente Speichernutzung auf Speicherdatenträgern minimieren, indem Sie das Datenformat NONBLOCK angeben. Sie können beispielsweise das Datenformat NONBLOCK für die folgenden Tasks angeben:

- Verwendung von Content-Management-Produkten
- Verwendung der Clientoption DIRMC zum Speichern von Verzeichnisinformationen
- Umlagerung sehr kleiner Dateien mit IBM Spectrum Protect for Space Management oder IBM Spectrum Protect HSM for Windows

In den meisten Situationen wird jedoch das native Format bevorzugt.

CRCData
Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

Yes

Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

No
Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

Tipp:

Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

- IBM® LTO5 und höher
- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke

DEDUPlicate
Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Der Standardwert ist NO.

IDENTIFYPRocess
Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Datendeduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 0 bis 50 ein.

Der Standardwert für diesen Parameter ist 0. Datendeduplizierungsprozesse für einen Kopienspeicherpool sind nicht erforderlich, wenn Sie Datendeduplizierungsprozesse für den primären Speicherpool angeben. Wenn IBM Spectrum Protect eine Datei in einem Speicherpool analysiert, analysiert IBM Spectrum Protect die Datei auch in allen anderen Speicherpools.

Hinweis: Datendeduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Datendeduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Datendeduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Datendeduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

Beispiel: Einen Pool für aktive Daten mit einer Einheitenklasse DC500 definieren.

Den Pool für aktive Daten TAPEPOOL2 für die Einheitenklasse DC500 definieren. Maximal 50 Arbeitsdatenträger für diesen Pool zulassen. Die Wiederverwendung der Datenträger um 45 Tage verzögern.

```
define stgpool tapepool3 dc500 pooltype=activedata
 maxscratch=50 reusedelay=45
```

Zugehörige Verweise:
SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsserie angeben)

DEFINE STGPOOLDIRECTORY (Speicherpoolverzeichnis definieren)

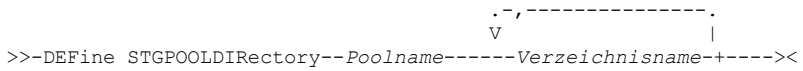
Mit diesem Befehl können Sie ein oder mehrere Verzeichnisse in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool definieren.

Tipp: Erstellen Sie nach der Definition eines Cloud-Containerspeicherpools ein oder mehrere Verzeichnisse, die für lokalen Speicher verwendet werden. Sie können während der Datenaufnahme Daten temporär im lokalen Speicher speichern, bevor die Daten in die Cloud versetzt werden. Auf diese Weise können Sie die Sicherungs- und Archivierungsleistung verbessern. Weitere Informationen finden Sie in Leistung für Cloudobjektspeicher optimieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Poolname (Erforderlich)
: Gibt den Namen eines Verzeichniscontainer- oder Cloud-Containerspeicherpools an. Dieser Parameter ist erforderlich.

Verzeichnisname (Erforderlich)
: Gibt das Verzeichnis an, das in dem Speicherpool definiert werden soll. Dieser Parameter ist erforderlich. Sie können mehrere Verzeichnisnamen angeben, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

  Wenn Sie den Verwaltungsclient verwenden und der Verzeichnisname ein Komma oder einen Backslash ("\") enthält, schließen Sie den Namen in Anführungszeichen ein.

Beispiel: Ein Speicherpoolverzeichnis definieren

Definieren Sie ein Speicherpoolverzeichnis mit dem Namen DIR1 unter Verwendung eines Verzeichniscontainerspeicherpools mit dem Namen POOL1.

AIX-Betriebssysteme Linux-Betriebssysteme

```
define stgpooldirectory pool1 /storage/dir1
```

Windows-Betriebssysteme

```
define stgpooldirectory pool1 c:\storage\dir1
```

Beispiel: Mehrere Speicherpoolverzeichnisse definieren

Definieren Sie Speicherpoolverzeichnisse mit dem Namen DIR1 und DIR2 unter Verwendung eines Verzeichniscontainerspeicherpools mit dem Namen POOL1.

AIX-Betriebssysteme Linux-Betriebssysteme

```
define stgpooldirectory pool1 /storage/dir1,/storage/dir2
```

Windows-Betriebssysteme

```
define stgpooldirectory pool1 e:\storage\dir1,f:\storage\dir2
```

Beispiel: Lokalen Speicher für einen Cloud-Containerspeicherpool definieren

Erstellen Sie ein Speicherpoolverzeichnis mit dem Namen DIR3 in einem Cloud-Containerspeicherpool mit dem Namen CLOUDLOCALDISK1.

AIX-Betriebssysteme Linux-Betriebssysteme

```
define stgpooldirectory cloudlocaldisk1 /storage/dir3
```

Windows-Betriebssysteme

```
define stgpooldirectory cloudlocaldisk1 c:\storage\dir3
```

Tabelle 1. Zugehörige Befehle für DEFINE STGPOOLDIRECTORY

Befehl	Beschreibung
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE STGPOOLDIRECTORY	Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool.
QUERY STGPOOLDIRECTORY	Zeigt Informationen zu Speicherpoolverzeichnissen an.
UPDATE STGPOOLDIRECTORY	Ändert die Attribute eines Speicherpoolverzeichnisses.

DEFINE SUBSCRIPTION (Profilsubskription definieren)

Mit diesem Befehl kann ein verwalteter Server für ein Profil subskribiert werden.

Wenn ein Server für sein erstes Profil subskribiert, wird auch eine Subskription für das Standardprofil (falls vorhanden) des Konfigurationsmanagers erstellt. Der Server fragt dann den Konfigurationsmanager in regelmäßigen Abständen nach Konfigurationsaktualisierungen ab.

Einschränkungen:

1. Ein Server kann nicht für Profile von mehreren Konfigurationsmanagern subskribieren.
2. Wenn ein Server für ein Profil mit einem zugeordneten Objekt subskribiert, das bereits auf dem Server definiert ist, wird die lokale Definition durch die Definition vom Konfigurationsmanager ersetzt. Wenn ein Server beispielsweise über den Verwaltungszeitplan

WEEKLY_BACKUP verfügt, dann für ein Profil subskribiert, das ebenfalls einen Verwaltungszeitplan mit dem Namen WEEKLY_BACKUP hat, wird die lokale Definition ersetzt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DEFine SUBSCRIPtion--Profilname--+-----------------------+--><
                                    '-SERVer--=--Servername-'
```

Parameter

Profilname (Erforderlich)
: Gibt den Namen des Profils an, für das der Server subskribiert.

SERVer
: Gibt den Namen des Konfigurationsmanagers an, von dem die Konfigurationsdaten abgerufen werden. Dieser Parameter ist erforderlich, wenn der verwaltete Server nicht mindestens eine Subskription hat. Hat der verwaltete Server eine Subskription, kann dieser Parameter übergangen werden. Als Standardwert wird dann der Konfigurationsmanager für diese Subskription verwendet.

Beispiel: Eine Profilsubskription definieren

Das Profil BETA subskribieren, das sich auf dem Konfigurationsmanager TOM befindet.

```
define subscription beta server=tom
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE SUBSCRIPTION

Befehl	Beschreibung
COPY PROFILE	Erstellt eine Kopie eines Profils.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DELETE PROFILE	Löscht ein Profil aus einem Konfigurationsmanager.
DELETE SUBSCRIBER	Löscht veraltete Subskriptionen verwalteter Server.
DELETE SUBSCRIPTION	Löscht eine angegebene Profilsubskription.
LOCK PROFILE	Verhindert die Verteilung eines Konfigurationsprofils.
NOTIFY SUBSCRIBERS	Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.
QUERY PROFILE	Zeigt Informationen über Konfigurationsprofile an.
QUERY SUBSCRIBER	Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.
QUERY SUBSCRIPTION	Zeigt Informationen über Profilsubskriptionen an.
SET CONFIGREFRESH	Gibt das Zeitintervall an, in dem verwaltete Server die Konfigurationsmanager ansprechen sollen.
UNLOCK PROFILE	Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

DEFINE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs definieren)

Verwenden Sie diesen Befehl, um eine Zuordnung des virtuellen Dateibereichs zu definieren.

Namen von virtuellen Dateibereichen können in den NAS-Datenoperationen BACKUP NODE und RESTORE NODE ähnlich wie Dateisystemnamen verwendet werden. Die Dokumentation zu Ihrer NAS-Einheit enthält Anleitungen zur Angabe der Parameter für diesen Befehl.
Anmerkung: Dem NAS-Knoten muss eine Definition für eine Einheit zum Versetzen von Daten zugeordnet sein, da bei der Aktualisierung der Zuordnung eines virtuellen Dateibereichs durch den IBM Spectrum Protect-Server der Server versucht, die NAS-Einheit anzusprechen, um das virtuelle Dateisystem und den Dateisystemnamen zu prüfen.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Domäne, der der NAS-Knoten zugeordnet ist

Syntax

```
>>-DEFine VIRTUALFSmapping  -Knotenname------------------------>

>--Name_des_virtuellen_Dateibereichs--Dateisystemname--Pfad----->

   .-NAMEType--=--SERVER----------.
>--+-----------------------------+----------------------------><
   '-NAMEType--=--+-SERVER------+-'
                  '-HEXadecimal-'
```

Parameter

Knotenname (Erforderlich)

Gibt den NAS-Knoten an, auf dem sich das Dateisystem und der Pfad befinden. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

Name_des_virtuellen_Dateibereichs (Erforderlich)

Gibt den Namen an, der auf diese Definition des virtuellen Dateibereichs verweist. Bei dem Namen des virtuellen Dateibereichs muss die Groß-/Kleinschreibung beachtet werden, und das erste Zeichen muss ein Schrägstrich / sein. Die Länge des Namens darf 64 Zeichen, einschließlich des erforderlichen Schrägstrichs, nicht überschreiten. Die Namen der virtuellen Dateibereiche sind auf denselben Zeichensatz wie alle anderen Objekte im Server beschränkt, mit der Ausnahme, dass auch der Schrägstrich / zulässig ist.

Der Name des virtuellen Dateibereichs darf mit keinem Dateisystem auf dem NAS-Knoten übereinstimmen. Beachten Sie bei der Auswahl des Namens für einen virtuellen Dateibereich die folgenden Einschränkungen:

- Wird auf der NAS-Einheit ein Dateisystem mit demselben Namen wie ein virtuelles Dateisystem erstellt, tritt eine Namensunverträglichkeit auf dem Server auf, wenn der neue Dateibereich gesichert wird. Verwenden Sie eine Zeichenfolge für den Namen des virtuellen Dateibereichs, die in der Zukunft wahrscheinlich nicht als Name eines realen Dateisystems auf Ihrer NAS-Einheit verwendet wird.

  Beispiel: Ein Benutzer verwendet die Namenskonvention zum Erstellen von Dateibereichen auf einer NAS-Einheit mit Namen in der Form /vol1, /vol2, /vol3. Der Benutzer definiert einen virtuellen Dateibereich für den Server mit dem Namen /vol9. Wenn der Benutzer weiterhin dieselbe Namenskonvention verwendet, wird der Name des virtuellen Dateibereichs irgendwann in der Zukunft mit dem Namen eines realen Dateibereichs in Konflikt stehen.

- Bei Sicherungs- und Zurückschreibungsoperationen prüft der Server vor dem Starten der Operation, ob eine Namensunverträglichkeit vorliegt.
- Der Name des virtuellen Dateibereichs erscheint in der Ausgabe des Befehls QUERY FILESPACE sowie in den Sicherungs- und Zurückschreibungsanzeigen des IBM Spectrum Protect-Web-Clients als Dateibereich. Wählen Sie daher einen Namen aus, der dieses Objekt eindeutig als Verzeichnispfad auf der NAS-Einheit identifiziert.

Dateisystemname (Erforderlich)

Gibt den Namen des Dateisystems an, in dem sich der Pfad befindet. Der Dateisystemname muss auf dem angegebenen NAS-Knoten vorhanden sein. Der Dateisystemname darf keine Platzhalterzeichen enthalten.

Pfad (Erforderlich)

Gibt den Pfad vom Stamm des Dateisystems zum Verzeichnis an. Der Pfad kann nur auf ein Verzeichnis verweisen. Die maximale Länge des Pfads beträgt 1024 Zeichen. Bei dem Pfadnamen muss die Groß-/Kleinschreibung beachtet werden.

NAMEType

Gibt an, wie der Server den angegebenen Pfadnamen interpretieren soll. Dieser Parameter ist nützlich, wenn ein Pfad Zeichen enthält, die nicht Teil der Codepage sind, in der der Server ausgeführt wird. Der Standardwert lautet SERVER.

Gültige Werte:

SERVER
: Der Server verwendet die Codepage des Servers, um den Pfadnamen zu interpretieren.

HEXadecimal

Der Server interpretiert den eingegebenen Pfad als hexadezimale Darstellung des Pfads. Diese Option sollte verwendet werden, wenn ein Pfad Zeichen enthält, die nicht eingegeben werden können. Diese Situation kann auftreten, wenn für das NAS-Dateisystem eine Sprache definiert ist, die von der Sprache abweicht, in der der Server ausgeführt wird.

Beispiel: Eine Zuordnung des virtuellen Dateibereichs definieren

Den Namen /mikeshomedir für die Zuordnung des virtuellen Dateibereichs für den Pfad /home/mike in dem Dateisystem /vol/vol1 auf dem NAS-Knoten NAS1 definieren.

```
define virtualfsmapping nas1 /mikeshomedir /vol/vol1 /home/mike
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DEFINE VIRTUALFSMAPPING

Befehl	Beschreibung
DELETE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs löschen.
QUERY VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs abfragen.
UPDATE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs aktualisieren.

DEFINE VOLUME (Datenträger in einem Speicherpool definieren)

Mit diesem Befehl kann einem Speicherpool ein Datenträger mit wahlfreiem Zugriff oder mit sequentiellem Zugriff zugeordnet werden.

Wenn Sie einen Speicherpooldatenträger mit wahlfreiem Zugriff (DISK) oder einen Speicherpooldatenträger mit sequenziellem Zugriff definieren, der einer Einheitenklasse FILE zugeordnet ist, kann der Datenträger von dem Server erstellt werden, bevor er zugeordnet wird. Sie können auch Speicherbereichsauslöser verwenden, um im voraus zugeordnete Datenträger zu erstellen, wenn zuvor festgelegte Schwellenwerte für die Speicherauslastung überschritten wurden. Ausführliche Informationen zu Speicherbereichsauslösern befinden sich in DEFINE SPACETRIGGER (Speicherbereichsauslöser definieren). Für Datenträger, die anderen Einheitenklassen als DISK oder anderen Einheitentypen als FILE zugeordnet sind, können Sie den Befehl DEFINE VOLUME verwenden, um einen bereits erstellten Datenträger einem Speicherpool zuzuordnen.

AIX-BetriebssystemeLinux-BetriebssystemeWenn Sie eine Einheitenklasse FILE für Speicher verwenden, der von einem z/OS Media-Server verwaltet wird, ist es nicht erforderlich, Datenträger zu formatieren oder zu definieren. Wenn Sie einen Datenträger für eine solche Einheitenklasse FILE mit dem Befehl DEFINE VOLUME definieren, ordnet der z/OS Media-Server erst dann Speicherbereich für den Datenträger zu, wenn der Datenträger für seine erste Verwendung geöffnet wird.

Achtung: Datenträger für den z/OS Media-Server, die mit dem Befehl DEFINE VOLUME erstellt werden, bleiben physisch voll oder zugeordnet, nachdem der Server den Datenträger leert, wie beispielsweise nach der Verfallsverarbeitung oder der Wiederherstellung. Bei FILE-Datenträgern wird der DASD-Speicherbereich nicht für das System freigegeben, wenn der Datenträger geleert wird. Wenn ein Speicherpool einen leeren Datenträger oder einen Datenträger, der gefüllt wird, erfordert, kann der FILE-Datenträger verwendet werden. Im Gegensatz dazu sind Banddatenträger, die logisch leer sind, auch physisch leer. FILE-Datenträger und Banddatenträger bleiben im Server definiert. Dagegen werden Arbeitsdatenträger, einschließlich des physischen Speichers, der FILE-Arbeitsdatenträgern zugeordnet ist, nach der Leerung an das System zurückgegeben.

Um Speicherbereich in Speicherpools mit sequenziellem Zugriff zu erstellen, können Sie Datenträger definieren, oder Sie können es dem Server erlauben, bei Bedarf Arbeitsdatenträger anzufordern, wie mit dem Parameter MAXSCRATCH für den Speicherpool angegeben ist. Für Speicherpools, die der Einheitenklasse FILE zugeordnet sind, kann der Server bei Bedarf unter Verwendung von Speicherbereichsauslösern für den Speicherpool private Datenträger erstellen. Für DISK-Speicherpools ist der Arbeitsdatenträgermechanismus nicht verfügbar. Sie können jedoch Speicherbereich erstellen, indem Sie Datenträger erstellen und dann die Datenträger für den Server definieren. Alternativ kann der Server Datenträger erstellen, die Speicherbereichsauslöser für den Speicherpool verwenden.

Der Server prüft nicht das Vorhandensein eines Datenträgernamens, wenn ein Datenträger in einem Speicherpool definiert wird, der einem Kassettenarchiv zugeordnet ist. Der definierte Datenträger hat die geschätzte Kapazität "0", bis Daten auf den Datenträger geschrieben werden.

Achtung: Die Größe eines Speicherpooldatenträgers kann nicht mehr geändert werden, nachdem sie für den Server definiert wurde.

AIX-BetriebssystemeWenn Sie die Größe von IBM Spectrum Protect-Datenträgern ändern, indem Sie unformatierte logische Datenträger mit SMIT erweitern oder indem Sie die Dateigrößen der Datenträger mit Betriebssystembefehlen oder Dienstprogrammen ändern, wird der Server möglicherweise nicht korrekt initialisiert und es können Daten verloren gehen.

Windows-BetriebssystemeWenn Sie die Größe von Datenträgern ändern, indem Sie die Dateigrößen der Datenträger mit Betriebssystembefehlen oder Dienstprogrammen ändern, wird der Server möglicherweise nicht korrekt initialisiert und es können Daten verloren gehen.

Einschränkungen:

- Sie können diesen Befehl nicht verwenden, um Datenträger in Speicherpools mit der Parametereinstellung `RECLAMATIONTYPE=SNAPLOCK` zu definieren. Datenträger in diesem Typ des Speicherpools werden mit dem Parameter MAXSCRATCH in der Speicherpooldefinition zugeordnet.

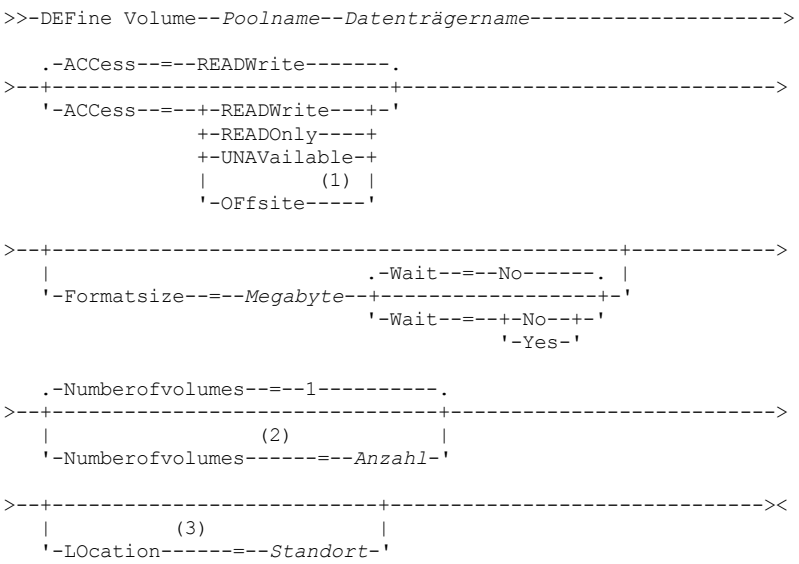
- Sie können keine Datenträger in einem Speicherpool definieren, der mit der Einheitenklasse CENTERA definiert ist.
- Linux-BetriebssystemeSie können keine unformatierten logischen Datenträger für Speicherpooldatenträger verwenden.

Physische Dateien, die mit dem Befehl DEFINE VOLUME zugeordnet werden, werden nicht aus einem Dateibereich entfernt, wenn Sie den Befehl DELETE VOLUME ausgeben.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich, dem der Datenträger zugeordnet ist.

Syntax



Anmerkungen:

1. Dieser Wert ist nur für Datenträger gültig, die Kopienspeicherpools zugeordnet sind.
2. Dieser Parameter ist nur für Datenträger DISK oder FILE gültig.
3. Dieser Parameter ist nur für Datenträger mit sequenziellem Zugriff gültig.

Parameter

Poolname (Erforderlich)
Gibt den Namen des Speicherpools an, dem der Datenträger zugeordnet ist.

Datenträgername (Erforderlich)
Gibt den Namen des Speicherpooldatenträgers an, der definiert werden soll. Wird für den Parameter NUMBEROFVOLUMES eine Zahl größer als 1 angegeben, wird der Datenträgername als Präfix zum Generieren mehrerer Datenträgernamen verwendet. Der Datenträgername, der angegeben wird, hängt von dem Einheitentyp ab, den der Speicherpool verwendet.

Jeder Datenträger, der von einem Server für einen beliebigen Zweck verwendet wird, muss einen eindeutigen Namen haben. Diese Anforderung gilt für alle Datenträger, unabhängig davon, ob die Datenträger für Speicherpools oder für Operationen, wie beispielsweise Datenbanksicherung oder -export, verwendet werden. Die Anforderung gilt auch für Datenträger, die sich in verschiedenen Kassettenarchiven befinden, die aber von demselben Server verwendet werden.

AIX-BetriebssystemeLinux-BetriebssystemeHinweis: Datenträgernamen dürfen keine eingebetteten Leerzeichen oder Gleichheitszeichen enthalten.
Windows-BetriebssystemeHinweis: Datenträgernamen dürfen keine eingebetteten Leerzeichen oder Gleichheitszeichen enthalten. Dies gilt nicht für DISK- oder FILE-Datenträger.
Die folgenden Tabellen enthalten die Anforderungen an Datenträgernamen:

- Tabelle 1: DISK
- Tabelle 2: FILE
- AIX-BetriebssystemeLinux-BetriebssystemeTabelle 3: FILE für den z/OS Media-Server
- Tabelle 4: Band
- AIX-BetriebssystemeLinux-BetriebssystemeTabelle 5: Band für den z/OS Media-Server
- Tabelle 6: REMOVABLEFILE

Tabelle 1. Anforderungen an Datenträgernamen für DISK

Anforderungen für Datenträgername	Beispiel

Der Name der Datei, die die Datenträgerdaten enthalten soll, entweder mit dem vollständig qualifizierten Pfadnamen oder mit einem Pfadnamen, der sich auf das aktuelle Arbeitsverzeichnis bezieht.
 	
Windows-BetriebssystemeEnthält ein Name eingebettete Leerzeichen, Gleichheitszeichen oder andere Sonderzeichen, ist die Liste in Anführungszeichen einzuschließen.
	AIX-BetriebssystemeLinux-Betriebssysteme
	
	`/usr/storage/sbkup01.dsm`
	
	AIX-BetriebssystemeWird ein logischer AIX-Datenträger verwendet, geben Sie den Pfadnamen wie folgt ein:
	
	`/dev/rxxx`
	
	xxx ist der Name des logischen Datenträgers.
	Windows-Betriebssysteme
	
	`"c:\program files\tivoli\tsm\server\data3.dsm"`

Tabelle 2. Anforderungen an Datenträgernamen für FILE

Anforderungen für Datenträgername	Beispiel

Der Name der Datei, die die Datenträgerdaten enthalten soll, entweder mit dem vollständig qualifizierten Pfadnamen oder mit dem Pfadnamen, der sich auf ein Verzeichnis bezieht, das im Parameter DIRECTORY für die Einheitenklasse angegeben ist.
 	
Windows-BetriebssystemeEnthält ein Name eingebettete Leerzeichen, Gleichheitszeichen oder andere Sonderzeichen, ist die Liste in Anführungszeichen einzuschließen.
 	
Stellen Sie FILE-Datenträger in eines der Verzeichnisse, die mit dem Parameter DIRECTORY des Befehls DEFINE DEVCLASS angegeben werden. Andernfalls haben Speicheragenten möglicherweise keinen Zugriff auf die Datenträger. Ausführliche Informationen siehe DEFINE PATH (Pfad definieren).
	AIX-BetriebssystemeLinux-Betriebssysteme
	
	`/data/fpool01.dsm`
	
	Windows-Betriebssysteme
	
	`"f:\data storage\fpool01.dsm"`

AIX-BetriebssystemeLinux-Betriebssysteme

Tabelle 3. z/OS Media-Server: Anforderungen an Datenträgernamen für FILE

Anforderungen für Datenträgername	Beispiel

Anforderungen für Datenträgername	Beispiel
Geben Sie für FILE-Datenträger, die mit dem z/OS Media-Server verwendet werden, einen Dateinamen an. Der Dateiname kann aus einem oder aus mehreren Qualifikationsmerkmalen bestehen, die durch einen Punkt begrenzt werden. Die Qualifikationsmerkmale können maximal 8 Zeichen enthalten. Die maximale Länge des Dateinamens beträgt 44 Zeichen. Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@#$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen. Um die zugehörige lineare VSAM-Datei zuzuordnen, wenn der Datenträger auf dem z/OS-System bereitgestellt wird, wird das Qualifikationsmerkmal der höheren Ebene (High Level Qualifier - HLQ) normalerweise von bestimmten ACS-Routinen innerhalb der SMS-Maßnahmenvorgaben auf dem System gefiltert, auf dem der z/OS Media-Server ausgeführt wird. Das Verhalten des Qualifikationsmerkmals der höheren Ebene ähnelt dem Verhalten des PREFIX-Namens bei der Anforderung eines Arbeitsdatenträgers. Das Qualifikationsmerkmal der höheren Ebene wird normalerweise von DFSMS für Zuordnungsattribute verwendet, wie z. B. für die erweiterte Adressierbarkeit für Dateien, von denen eine Erweiterung erwartet wird, wenn der Speicherbereich, der dem Dateidatenträger bereits zugeordnet ist, belegt ist. Wenn die Datei nicht vorhanden ist, wird sie vom Server erstellt, wenn der Datenträger für eine bestimmte IBM Spectrum Protect-Speicheroperation verwendet wird. Die Datei wird nicht erstellt, wenn der Datenträger definiert ist. Ein Datenverlust kann auftreten, wenn Datenträger definiert werden, da der Datenträger oder die lineare VSAM-Datei vom z/OS Media-Server wiederverwendet wird, wenn er bzw. sie zum Zeitpunkt der Zuordnung vorhanden ist. Wichtig: Um dem Server die Erstellung von Datenträgernamen zu ermöglichen, ziehen Sie die Verwendung von Arbeitsdatenträgern in Betracht.	 AIX-Betriebssysteme  Linux-Betriebssysteme `SERVER1.BFS.POOL3.VOLA`

Tabelle 4. Anforderungen an Datenträgernamen für Band

Anforderungen für Datenträgername	Beispiel
Verwenden Sie 1 - 32 alphanumerische Zeichen. Der Datenträgername darf keine eingebetteten Leerzeichen oder Gleichheitszeichen enthalten.	`DSMT01`

AIX-Betriebssysteme  Linux-Betriebssysteme

Tabelle 5. z/OS Media-Server: Anforderungen an Datenträgernamen für Band

Anforderungen für Datenträgername	Beispiel
Geben Sie für Bandkassetten einen Banddatenträgernamen mit 1 - 6 alphanumerischen Zeichen an. Der Server setzt Banddatenträgernamen in Großbuchstaben um. Der Datenträgername darf keine eingebetteten Leerzeichen oder Gleichheitszeichen enthalten. Jeder Datenträger, der von einem Server für einen beliebigen Zweck verwendet wird, muss einen eindeutigen Namen haben. Diese Anforderung gilt für alle Datenträger, unabhängig davon, ob die Datenträger für Speicherpools oder für Operationen, wie beispielsweise Datenbanksicherung oder -export, verwendet werden. Die Anforderung gilt auch für Datenträger, die sich in verschiedenen z/OS-Kassettenarchiven befinden, die aber von demselben Server verwendet werden.	`DSMT01`

Tabelle 6. Anforderungen an Datenträgernamen für REMOVABLEFILE

Anforderungen für Datenträgername	Beispiel
1–6 alphanumerische Zeichen Der Server setzt Datenträgernamen in Großbuchstaben um.	`DSM01`

ACCess
: Gibt an, wie Clientknoten und Serverprozesse (wie Umlagerung) auf Dateien auf dem Speicherpooldatenträger zugreifen können. Dieser Parameter ist wahlfrei. Der Standardwert ist READWRITE. Gültige Werte:

  READWrite
  : Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien des Datenträgers haben.

  READOnly
  : Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff auf Dateien des Datenträgers haben.

  UNAVailable
  : Gibt an, dass Clientknoten oder Serverprozesse nicht auf Dateien zugreifen können, die auf dem Datenträger gespeichert sind.

    Wird ein Datenträger mit wahlfreiem Zugriff als UNAVAILABLE definiert, kann der Datenträger nicht angehängt werden.

    Wird ein Datenträger mit sequenziellem Zugriff als UNAVAILABLE definiert, versucht der Server nicht, auf den Datenträger zuzugreifen.

  OFfsite
  : Gibt an, dass sich der Datenträger an einem ausgelagerten Standort befindet, von dem er nicht geladen werden kann. Sie können diesen Wert nur für Datenträger in Kopienspeicherpools oder Speicherpools für aktive Daten angeben.
    Mit diesem Wert können Datenträger an ausgelagerten Standorten verfolgt werden. Der Server behandelt ausgelagerte Datenträger anders:

    - Der Server generiert keine Ladeanforderungen für ausgelagerte Datenträger.
    - Der Server fordert Daten von ausgelagerten Datenträgern zurück oder versetzt Daten von ausgelagerten Datenträgern, indem Dateien aus anderen Speicherpools abgerufen werden.
    - Der Server löscht nicht automatisch leere ausgelagerte Arbeitsdatenträger aus einem Kopienspeicherpool oder Speicherpool für aktive Daten.

LOcation
: Gibt den Standort des Datenträgers an. Dieser Parameter ist wahlfrei. Er kann nur für Datenträger in Speicherpools mit sequenziellem Zugriff angegeben werden. Die Standortinformationen dürfen eine maximale Länge von 255 Zeichen haben. Wenn die Beschreibung des Standorts Leerzeichen enthält, muß sie in Anführungszeichen stehen.

Formatsize
: Gibt die Größe des Datenträgers mit wahlfreiem Zugriff oder des FILE-Datenträgers an, der in einem Schritt erstellt und formatiert wird. Der Wert wird in Megabyte angegeben. Die maximale Größe beträgt 8 000 000 MB (8 Terabyte).Dieser Parameter ist erforderlich, wenn eine der folgenden Bedingungen zutrifft:

  - Ein einzelner FILE- oder DISK-Datenträger wird angegeben, der in einem Schritt erstellt und formatiert werden soll.
  - Der Wert für den Parameter NUMBEROFVOLUMES ist größer als 1, und DISK-Datenträger werden erstellt.
  - Der Wert des Parameters NUMBEROFVOLUMES ist größer als 1 und der Wert des Parameters FORMATSIZE ist kleiner-gleich dem Parameter MAXCAPACITY des Befehls DEFINE DEVCLASS.

  Wenn Sie Datenträger auf einem z/OS Media-Server zuordnen, ist dieser Parameter nicht gültig.

  Für einen FILE-Datenträger müssen Sie einen Wert kleiner-gleich dem Wert des Parameters MAXCAPACITY der Einheitenklasse angeben, die dem Speicherpool zugeordnet ist.

  Sie können diesen Parameter nicht für mehrere vordefinierte Datenträger verwenden. Die Operation wird als Hintergrundprozess ausgeführt, wenn nicht `WAIT=YES` angegeben wird.

Numberofvolumes
: Gibt die Anzahl der Datenträger an, die in einem Schritt erstellt und formatiert werden. Dieser Parameter gilt nur für Speicherpools mit Einheitenklassen DISK oder FILE. Dieser Parameter ist wahlfrei. Der Standardwert ist 1. Wird ein Wert größer als 1 angegeben, müssen Sie auch einen Wert für den Parameter FORMATSIZE angeben. Geben Sie eine Zahl von 1 bis 256 an.

  Wenn Sie Datenträger auf einem z/OS Media-Server zuordnen, ist der einzige von diesem Parameter unterstützte Wert der Standardwert 1.

  Ist der Wert für den Parameter NUMBEROFVOLUMES größer als 1, wird dem angegebenen Datenträgernamen ein numerisches Suffix angehängt, um jeden Namen zu erstellen, z. B. tivolivol001 und tivolivol002. Stellen Sie sicher, dass ein Datenträgername ausgewählt wird, mit dem ein gültiger Dateiname für das Zieldateisystem erstellt wird, wenn das Suffix angehängt wird.

  Wichtig: Sie müssen sicherstellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können. Weitere Informationen siehe DEFINE PATH (Pfad definieren).

Wait
: Gibt an, ob eine Erstellungs- und Formatierungsoperation für einen Datenträger im Vordergrund oder im Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Er wird ignoriert, es sei denn, Sie geben auch den Parameter FORMATSIZE an.

No

Gibt an, dass eine Erstellungs- und Formatierungsoperation für einen Datenträger im Hintergrund ausgeführt wird. Der Wert NO ist der Standardwert, wenn auch eine Formatgröße angegeben wird.

Yes

Gibt an, dass eine Erstellungs- und Formatierungsoperation für einen Datenträger im Vordergrund ausgeführt wird. Hinweis: Sie können nicht `WAIT=YES` an der Serverkonsole angeben.

Beispiel: Einen Hintergrundprozess verwenden, um einen neuen Datenträger mit 100 MB für einen Plattenspeicherpool zu definieren

Einen Datenträger mit 100 MB in dem Plattenspeicherpool BACKUPPOOL erstellen. AIX-BetriebssystemeLinux-BetriebssystemeDer Datenträgername lautet /var/storage/bf.dsm. Windows-BetriebssystemeDer Datenträgername lautet j:\storage\bf.dsm. Der Datenträger soll als Hintergrundprozess erstellt werden. AIX-BetriebssystemeLinux-Betriebssysteme

```
define volume backuppool
/var/storage/bf.dsm formatsize=100
```

Windows-Betriebssysteme

```
define volume backuppool j:\storage\bf.dsm formatsize=100
```

Beispiel: Einen Datenträger für einen Plattenspeicherpool mit Lese- und Schreibzugriff definieren

Der Speicherpool POOL1 ist einer Bandeinheitenklasse zugeordnet. Den Datenträger TAPE01 für diesen Speicherpool mit READWRITE-Zugriff definieren.

```
define volume pool1 tape01 access=readwrite
```

Beispiel: Einen Datenträger für einen Dateispeicherpool definieren

Der Speicherpool FILEPOOL ist einer Einheitenklasse mit dem Einheitentyp FILE zugeordnet. AIX-BetriebssystemeLinux-Betriebssysteme Für diesen Speicherpool einen Datenträger mit dem Namen filepool_vol01 definieren.Windows-BetriebssystemeFür diesen Speicherpool einen Datenträger mit dem Namen fp_vol01.dsm definieren. AIX-BetriebssystemeLinux-Betriebssysteme

```
define volume filepool /usr/storage/filepool_vol01
```

Windows-Betriebssysteme

```
define volume filepool j:\storage\fp_vol01.dsm
```

Beispiel: Einen Hintergrundprozess verwenden, um 10 Datenträger für einen Dateispeicherpool mit einer maximalen Kapazität von 5 GB zu definieren

10 Datenträger in einem sequenziellen Speicherpool definieren, der eine Einheitenklasse FILE verwendet. Der Speicherpool hat den Namen FILEPOOL. Der Wert des Parameters MAXCAPACITY für die Einheitenklasse, die diesem Speicherpool zugeordnet ist, lautet 5 GB. Die Erstellung muss im Hintergrund erfolgen.

```
define volume filepool filevol numberofvolumes=10 formatsize=5000
```

Der Server erstellt die Datenträgernamen filevol001 bis filevol010.

Datenträger werden in dem Verzeichnis oder in den Verzeichnissen erstellt, das bzw. die mit dem Parameter DIRECTORY der Einheitenklasse angegeben ist bzw. sind, die dem Speicherpool "filepool" zugeordnet ist. Wenn Sie mehrere Verzeichnisse für die Einheitenklasse angegeben haben, können einzelne Datenträger in den Verzeichnissen in der Liste erstellt werden.

Zugehörige Befehle

Tabelle 7. Zugehörige Befehle für DEFINE VOLUME

Befehl	Beschreibung
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
QUERY VOLUME	Zeigt Informationen über Speicherpooldatenträger an.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.
UPDATE LIBVOLUME	Ändert den Status eines Speicherdatenträgers.
UPDATE VOLUME	Aktualisiert die Attribute der Speicherpooldatenträger.

DELETE-Befehle

Mit den DELETE-Befehlen kann ein IBM Spectrum Protect-Objekt gelöscht oder entfernt werden.

- DELETE ASSOCIATION (Knotenzuordnung zu einem Zeitplan löschen)
- DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)
- DELETE BACKUPSET (Sicherungsgruppe löschen)
- DELETE CLIENTOPT (Option in einer Optionsgruppe löschen)
- DELETE CLOPTSET (Clientoptionsgruppe löschen)
- DELETE COLLOCGROUP (Kollokationsgruppe löschen)
- DELETE COLLOCMEMBER (Kollokationsgruppenmitglied löschen)
- DELETE COPYGROUP (Sicherungs- oder Archivierungskopiengruppe löschen)
- DELETE DATAMOVER (Einheit zum Versetzen von Daten löschen)
- DELETE DEDUPSTATS (Datendeduplizierungsstatistikdaten löschen)
- DELETE DEVCLASS (Einheitenklasse löschen)
- DELETE DOMAIN (Maßnahmendomäne löschen)
- DELETE DRIVE (Laufwerk aus einem Kassettenarchiv löschen)
- DELETE EVENT (Ereignissätze löschen)
- DELETE EVENTSERVER (Definition des Ereignisservers löschen)
- DELETE FILESPACE (Clientknotendaten aus dem Server löschen)
- DELETE GRPMEMBER (Server aus einer Servergruppe löschen)
- DELETE LIBRARY (Kassettenarchiv löschen)
- DELETE MACHINE (Maschineninformationen löschen)
- DELETE MACHNODEASSOCIATION (Zuordnung zwischen Maschine und Knoten löschen)
- DELETE MGMTCLASS (Verwaltungsklasse löschen)
- DELETE NODEGROUP (Knotengruppe löschen)
- DELETE NODEGROUPMEMBER (Eintrag aus der Knotengruppe löschen)
- DELETE PATH (Pfad löschen)
- DELETE POLICYSET (Maßnahmengruppe löschen)
- DELETE PROFASSOCIATION (Profilzuordnung löschen)
- DELETE PROFILE (Profil löschen)
- DELETE RECMEDMACHASSOCIATION (Zuordnung Datenträger/Maschine löschen)
- DELETE RECOVERYMEDIA (Wiederherstellungsdatenträger löschen)
- DELETE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl löschen)
- DELETE SCRIPT (Befehlszeilen aus Prozedur oder gesamte Prozedur löschen)
- DELETE SERVER (Server-Definition löschen)
- DELETE SERVERGROUP (Servergruppe löschen)
- DELETE SPACETRIGGER (Speicherbereichsauslöser für Speicherpool löschen)
- DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)
- DELETE STGPOOL (Speicherpool löschen)
- DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)
- DELETE SUBSCRIBER (Subskriptionen aus Konfigurationsmanagerdatenbank löschen)
- DELETE SUBSCRIPTION (Profilsubskription löschen)
- DELETE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs löschen)
- DELETE VOLHISTORY (Protokolldaten sequenzieller Datenträger löschen)
- DELETE VOLUME (Speicherpooldatenträger löschen)

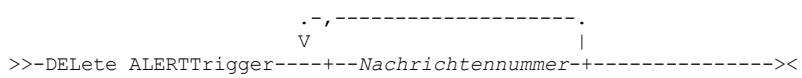
DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)

Verwenden Sie diesen Befehl, um eine Nachricht aus der Liste der Alertauslöser zu entfernen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Nachrichtennummer (Erforderlich)
: Gibt die Nachrichtennummer an, die aus der Liste der Alertauslöser entfernt werden soll. Geben Sie mehrere Nachrichtennummern durch Kommas getrennt und ohne Leerzeichen an. Nachrichtennummern haben eine maximale Länge von acht Zeichen. Platzhalterzeichen können verwendet werden, um Nachrichtennummern anzugeben.

Alertauslöser löschen

Mit dem folgenden Befehl zwei Nachrichtennummern löschen, die als Alerts angegeben sind:

```
delete alerttrigger ANR1067E,ANR1073E
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE ALERTTRIGGER

Befehl	Beschreibung
DEFINE ALERTTRIGGER (Alertauslöser definieren)	Ordnet angegebene Nachrichten einem Alertauslöser zu.
QUERY ALERTSTATUS (Status eines Alert abfragen)	Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.
QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)	Zeigt Nachrichtennummern an, die einen Alert auslösen.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)	Aktualisiert die Attribute eines oder mehrerer Alertauslöser.
UPDATE ALERTSTATUS (Status eines Alert aktualisieren)	Aktualisiert den Status eines zurückgemeldeten Alert.

DELETE ASSOCIATION (Knotenzuordnung zu einem Zeitplan löschen)

Mit diesem Befehl kann die Zuordnung eines Clientknotens zu einem Clientzeitplan gelöscht werden. IBM Spectrum Protect führt den Zeitplan nicht mehr auf dem Clientknoten aus.

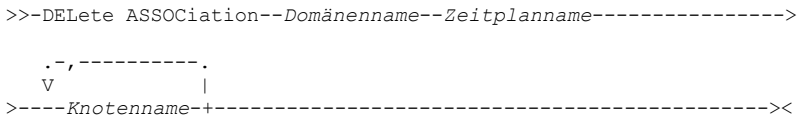
Wird versucht, eine Zuordnung zwischen einem Client und einem Zeitplan aufzuheben, zwischen denen keine Zuordnung besteht, bleibt dieser Befehl für diesen Client ohne Wirkung.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Domäne, zu der der Zeitplan gehört

Syntax



Parameter

Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an, zu der der Zeitplan gehört.

Zeitplanname (Erforderlich)
: Gibt den Namen des Zeitplans an, dessen Zuordnung zu Clients aufgehoben werden soll.

Knotenname (Erforderlich)
: Gibt den Namen des Client-Knotens an, der nicht mehr dem Client-Zeitplan zugeordnet ist. Es kann eine Liste der Clients angegeben werden, deren Zuordnung zu dem angegebenen Zeitplan aufgehoben werden soll. Trennen Sie die Einträge in der Liste durch Kommas ohne Leerzeichen voneinander. Es kann auch ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Die Zuordnung aller übereinstimmenden Clients zu dem angegebenen Zeitplan wird aufgehoben.

Beispiel: Zuordnung eines Knotens zu einem Zeitplan löschen

Den folgenden Befehl ausgeben, um die Zuordnung des Knotens JEFF, der der Maßnahmendomäne DOMAIN1 zugeordnet ist, zu dem Zeitplan WEEKLY_BACKUP zu löschen:

```
delete association domain1 weekly_backup jeff
```

Beispiel: Zuordnung eines Knotens zu einem Zeitplan unter Verwendung eines Platzhalterzeichens für die Knotenauswahl löschen

Die Zuordnung ausgewählter Clients, die der Maßnahmendomäne DOMAIN1 zugeordnet sind, zu dem Zeitplan WEEKLY_BACKUP löschen, so dass dieser Zeitplan nicht mehr von diesen Clients ausgeführt wird. Die Namen der Knoten, deren Zuordnung zu dem Zeitplan aufgehoben werden soll, enthalten die Buchstaben ABC oder XYZ. Den folgenden Befehl ausgeben:

```
delete association domain1 weekly_backup *abc*,*xyz*
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE ASSOCIATION

Befehl	Beschreibung
DEFINE ASSOCIATION	Ordnet Clients einem Zeitplan zu.
QUERY ASSOCIATION	Zeigt die Clients an, die einem oder mehreren Zeitplänen zugeordnet sind.

DELETE BACKUPSET (Sicherungsgruppe löschen)

Mit diesem Befehl können Sie eine Sicherungsgruppe manuell löschen, bevor ihr Aufbewahrungszeitraum abläuft.

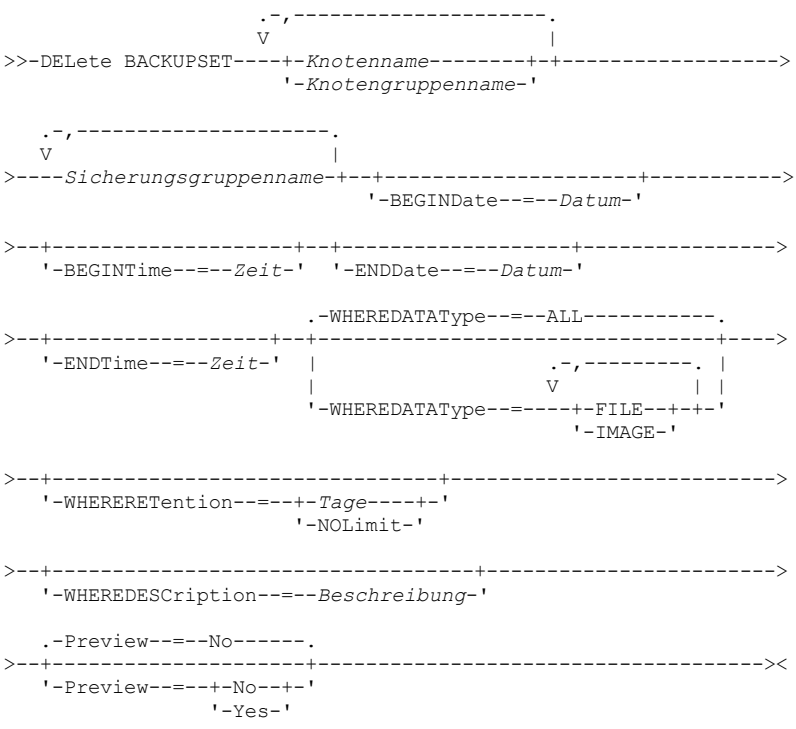
Wenn der Server eine Sicherungsgruppe erstellt, bestimmt der der Sicherungsgruppe zugeordnete Aufbewahrungszeitraum, wie lange die Sicherungsgruppe in der Datenbank verbleibt. Wird dieses Datum erreicht, löscht der Server automatisch die Sicherungsgruppe, wenn die Verfallsverarbeitung ausgeführt wird. Der Benutzer kann jedoch die Sicherungsgruppe des Clients auch manuell vom Server löschen, bevor die Sicherungsgruppe verfällt, indem der Befehl DELETE BACKUPSET verwendet wird.

Achtung: Enthalten die Datenträger mehrere Sicherungsgruppen, kehren Sie erst dann in den Status 'Scratch' zurück, wenn alle Sicherungsgruppen verfallen oder gelöscht sind.

Berechtigungsklasse

Wird die Serveroption REQSYSAUTHOUTFILE auf YES (Standardwert) gesetzt, muss der Administrator die Systemberechtigung haben. Ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator über Systemberechtigung oder Maßnahmenberechtigung für die Domäne verfügen, der der Clientknoten zugeordnet ist.

Syntax



Parameter

Knotenname oder Knotengruppenname (Erforderlich)

Gibt den Namen der Clientknoten oder Knotengruppen an, deren Daten in den angegebenen Sicherungsgruppendatenträgern enthalten sind. Sollen mehrere Knoten- und Knotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Alle angegebenen Knotennamen können Platzhalterzeichen enthalten, aber Knotengruppennamen dürfen keine Platzhalterzeichen enthalten. Wenn Sicherungsgruppendatenträger Sicherungsgruppen von mehreren Knoten enthalten, wird jede Sicherungsgruppe, deren Knotenname mit einem der angegebenen Knotennamen übereinstimmt, gelöscht.

Sicherungsgruppenname (Erforderlich)

Gibt den Namen der Sicherungsgruppe an, die gelöscht werden soll. Der angegebene Sicherungsgruppenname kann Platzhalterzeichen enthalten. Es können mehrere Sicherungsgruppennamen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

BEGINDate

Gibt das Anfangsdatum an, an dem die zu löschende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Anfangsdatum ohne eine Anfangszeit angegeben, lautet die Zeit 24:00 (Mitternacht) an dem angegebenen Datum.

Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1999
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage *oder* +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage.	TODAY +3 *oder* +3.
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage.	TODAY -3 *oder* -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt die Anfangszeit an, zu der die zu löschende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann zusammen mit dem Parameter BEGINDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Anfangszeit ohne ein Anfangsdatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Uhrzeit.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten	NOW+02:00 *oder* +02:00.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW-02:00 *oder* –02:00.

ENDDate

Gibt das Enddatum an, an dem die zu löschende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann zusammen mit dem Parameter ENDTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Enddatum ohne eine Endzeit angegeben, lautet die Zeit 23:59:59 am angegebenen Enddatum.

Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1999
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage *oder* +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage.	TODAY +3 *oder* +3.

Wert	Beschreibung	Beispiel
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage.	TODAY -3 *oder* -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDTime
Gibt die Endzeit des Bereichs an, in dem die zu löschende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann zusammen mit dem Parameter ENDDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Endzeit ohne ein Enddatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Zeit.
Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum	NOW+02:00 *oder* +02:00.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum	NOW-02:00 *oder* -02:00.

WHEREDATAType
Gibt an, dass die Sicherungsgruppen mit den angegebenen Typen von Daten gelöscht werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) gelöscht werden sollen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Gültige Werte:

ALL
Gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) gelöscht werden sollen. Dies ist der Standardwert.
FILE
Gibt an, dass eine Sicherungsgruppe auf Dateiebene gelöscht werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Client für Sichern/Archivieren gesichert wurden.
IMAGE
Gibt an, dass eine Imagesicherungsgruppe gelöscht werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Clients für Sichern/Archivieren erstellt wurden.

WHERERETention
Gibt den Aufbewahrungszeitraum in Tagen an, der der zu löschenden Sicherungsgruppe zugeordnet ist. Sie können eine ganze Zahl von 0 bis 30000 angeben. Gültige Werte:

Tage
Gibt an, dass Sicherungsgruppen, die diese Anzahl Tage aufbewahrt werden, gelöscht werden.
NOLimit
Gibt an, dass die Sicherungsgruppen, die unbegrenzt aufbewahrt werden, gelöscht werden.

WHEREDESCription
Gibt die Beschreibung an, die der zu löschenden Sicherungsgruppe zugeordnet ist. Die angegebene Beschreibung kann ein Platzhalterzeichen enthalten. Dieser Parameter ist wahlfrei. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.
Preview
Gibt an, ob die Liste der zu löschenden Sicherungsgruppen vorab angezeigt werden soll, ohne die Sicherungsgruppen tatsächlich zu löschen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No
Gibt an, dass die Sicherungsgruppen gelöscht werden.
Yes
Gibt an, dass der Server die Liste der zu löschenden Sicherungsgruppen anzeigt, ohne die Sicherungsgruppen tatsächlich zu löschen.

Beispiel: Eine Sicherungsgruppe löschen

Die Sicherungsgruppe PERS_DATA.3099 löschen, die zum Clientknoten JANE gehört. Die Sicherungsgruppe wurde am 11/19/1998 um 10:30:05 generiert und die Beschreibung lautet "Documentation Shop".

```
delete backupset pers_data.3099
 begindate=11/19/1998 begintime=10:30:05wheredescription="documentation shop"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE BACKUPSET

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DELETE NODEGROUP	Löscht eine Knotengruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
GENERATE BACKUPSETTOC	Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
QUERY BACKUPSETCONTENTS	Zeigt den Inhalt in Sicherungsgruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

DELETE CLIENTOPT (Option in einer Optionsgruppe löschen)

Mit diesem Befehl kann eine Clientoption in einer Optionsgruppe gelöscht werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung erforderlich.

Syntax

```
>>-DELete CLIENTOpt--Optionsgruppenname--Optionsname------------>

>--+--------------------------+-------------------------------><
   '-SEQnumber--=--+-Nummer-+-'
                   '-ALL----'
```

Parameter

Optionsgruppenname (Erforderlich)
: Gibt den Namen der Client-Optionsgruppe an.

Optionsname (Erforderlich)
: Gibt eine gültige Client-Option an.

SEQnumber
: Gibt eine Folgenummer an, wenn ein Optionsname mehrmals angegeben wird. Dieser Parameter ist wahlfrei. Gültige Werte sind:

  n
  : Gibt eine ganze Zahl größer oder gleich 0 an.

  ALL
  : Gibt alle Folgenummern an.

Beispiel: Die Option für das Datumsformat löschen

Die Option für das Datumsformat in der Optionsgruppe *ENG* löschen.

```
delete clientopt eng dateformat
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE CLIENTOPT

Befehl	Beschreibung
COPY CLOPTSET	Kopiert eine Clientoptionsgruppe.
DEFINE CLIENTOPT	Fügt einer Clientoptionsgruppe eine Clientoption hinzu.
DEFINE CLOPTSET	Definiert eine Clientoptionsgruppe.
DELETE CLOPTSET	Löscht eine Clientoptionsgruppe.
QUERY CLOPTSET	Zeigt Informationen über eine Clientoptionsgruppe an.
UPDATE CLIENTOPT	Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe.
UPDATE CLOPTSET	Aktualisiert die Beschreibung einer Clientoptionsgruppe.

DELETE CLOPTSET (Clientoptionsgruppe löschen)

Mit diesem Befehl kann eine Clientoptionsgruppe gelöscht werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung erforderlich.

Syntax

```
>>-DELete CLOptset--Optionsgruppenname------------------------><
```

Parameter

Optionsgruppenname (Erforderlich)
Gibt den Namen der zu löschenden Clientoptionsgruppe an.

Beispiel: Eine Clientoptionsgruppe löschen

Löschen Sie die Clientoptionsgruppe mit dem Namen ENG.

```
delete cloptset eng
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE CLOPTSET

Befehl	Beschreibung
COPY CLOPTSET	Kopiert eine Clientoptionsgruppe.
DEFINE CLIENTOPT	Fügt einer Clientoptionsgruppe eine Clientoption hinzu.
DEFINE CLOPTSET	Definiert eine Clientoptionsgruppe.
DELETE CLIENTOPT	Löscht eine Clientoption aus einer Clientoptionsgruppe.
QUERY CLOPTSET	Zeigt Informationen über eine Clientoptionsgruppe an.
UPDATE CLIENTOPT	Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe.
UPDATE CLOPTSET	Aktualisiert die Beschreibung einer Clientoptionsgruppe.

DELETE COLLOCGROUP (Kollokationsgruppe löschen)

Verwenden Sie diesen Befehl, um eine Kollokationsgruppe zu löschen. Eine Kollokationsgruppe kann nicht gelöscht werden, wenn sie Mitglieder enthält.

Sie können alle Mitglieder in der Kollokationsgruppe entfernen, indem Sie den Befehl DELETE COLLOCMEMBER mit einem Platzhalterzeichen im Parameter Knotenname ausgeben.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DELete COLLOCGroup--Gruppenname-----------------------------><
```

Parameter

Gruppenname
: Gibt den Namen der Kollokationsgruppe an, die gelöscht werden soll.

Beispiel: Eine Kollokationsgruppe löschen

Die Kollokationsgruppe group1 löschen.

```
delete collocgroup group1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE COLLOCGROUP

Befehl	Beschreibung
DEFINE COLLOCGROUP	Definiert eine Kollokationsgruppe.
DEFINE COLLOCMEMBER	Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE COLLOCMEMBER	Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.
MOVE NODEDATA	Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
UPDATE COLLOCGROUP	Aktualisiert die Beschreibung einer Kollokationsgruppe.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

DELETE COLLOCMEMBER (Kollokationsgruppenmitglied löschen)

Verwenden Sie diesen Befehl, um einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe zu löschen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
Knoten aus einer Kollokationsgruppe löschen

                                  .-,----------.
```

```
                                      V            |
>>-DELete COLLOCMember--Gruppenname----Knotenname-+------------><
```

Parameter

Gruppenname
: Gibt den Namen der Kollokationsgruppe an, aus der ein Clientknoten gelöscht werden soll.

Knotenname
: Gibt den Namen des Clientknotens an, der aus der Kollokationsgruppe gelöscht werden soll. Sie können einen oder mehrere Namen angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können auch Platzhalterzeichen verwenden, um mehrere Knoten anzugeben.

Dateibereich aus einer Dateibereichskollokationsgruppe löschen

```
>>-DELete COLLOCMember--Gruppenname--Knotenname----------------->

                 .-,-----------------.
                 V                   |
>--FIlespace--=----Dateibereichsname-+-------------------------->

   .-NAMEType--=--SERVER------.
>--+------------------------+--------------------------------->
   '-NAMEType--=--+-SERVER--+-'
                  +-UNIcode-+
                  '-FSID----'

   .-CODEType--=--BOTH-----------.
>--+---------------------------+----------------------------><
   '-CODEType--=--+-BOTH--------+-'
                  +-UNIcode----+
                  '-NONUNIcode-'
```

Parameter

Gruppenname
: Gibt den Namen der Kollokationsgruppe an, aus der ein Dateibereich gelöscht werden soll.

Knotenname
: Gibt den Clientknoten an, auf dem sich der Dateibereich befindet.

FIlespace
: Gibt den *Dateibereichsnamen* auf dem Clientknoten an, der aus der Kollokationsgruppe gelöscht werden soll. Sie können einen oder mehrere Dateibereichsnamen angeben, die sich auf einem bestimmten Clientknoten befinden. Werden mehrere Dateibereichsnamen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können auch Platzhalterzeichen verwenden, wenn mehrere Dateibereichsnamen angegeben werden.

NAMEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unicode-Unterstützung verfügt. Ein Client für Sichern/Archivieren mit Unicode-Unterstützung ist nur für Windows, Macintosh OS 9, Macintosh OS X und NetWare verfügbar. Verwenden Sie diesen Parameter, wenn Sie einen Dateibereichsnamen angeben, der kein einzelnes Platzhalterzeichen ist. Sie können einen vollständig qualifizierten Dateibereichsnamen angeben, der kein Platzhalterzeichen enthält. Sie können auch einen teilweise qualifizierten Dateibereichsnamen angeben, der ein Platzhalterzeichen enthalten kann, aber andere Zeichen enthalten muss. Der Standardwert lautet SERVER. Gültige Werte:

  SERVER
  : Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

  UNIcode
  : Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in den Namen und der Server-Codepage ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Server-Codepage nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

  FSID
  : Der Server interpretiert die Dateibereichsnamen nach ihren Dateibereichs-IDs (FSIDs).

CODEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen verwenden. Der Standardwert lautet BOTH, d. h., die Dateibereiche werden unabhängig vom Codepagetyp eingeschlossen. Die folgenden Werte sind verfügbar:

  BOTH
  : Die Dateibereiche unabhängig vom Codepagetyp einschließen.

UNIcode
Nur Dateibereiche einschließen, die in Unicode sind.

NONUNIcode
Dateibereiche einschließen, die nicht in Unicode sind.

Kollokationsgruppenmitglieder löschen

Die beiden Knoten NODE1 und NODE2 aus der Kollokationsgruppe GROUP1 löschen.

```
delete collocmember group1 node1,node2
```

Dateibereich aus einer Dateibereichskollokationsgruppe löschen

Den folgenden Befehl ausgeben, um den Dateibereich *cap_27400* aus der Kollokationsgruppe *collgrp_2* auf dem Knoten *hp_4483* zu löschen:

```
delete collocmember collgrp_2 hp_4483 filespace=cap_27400
```

Ein Mitglied einer Dateibereichskollokationsgruppe auf einem Knoten löschen, der Unicode verwendet

Befindet sich der Dateibereich auf einem Knoten, der Unicode verwendet, können Sie dies im Befehl angeben. Geben Sie den folgenden Befehl aus, um den Dateibereich *cap_257* aus der Kollokationsgruppe *collgrp_3* auf dem Knoten *win_4687* zu löschen:

```
delete collocmember collgrp_3 win_4687 filespace=cap_257 codetype=unicode
```

Dateibereich mit einem Namensteil löschen

Wenn der Dateibereich einen Namensteil hat, können Sie ein Platzhalterzeichen verwenden, um den Dateibereich zu löschen. Geben Sie den folgenden Befehl aus, um den Dateibereich *cap_* aus der Kollokationsgruppe *collgrp_4* auf dem Knoten *win_4687* zu löschen:

```
delete collocmember collgrp_4 win_4687 filespace=cap_* codetype=unicode
```

Sind mehrere Dateibereiche vorhanden, deren Namen mit cap_ beginnen, werden diese Dateibereiche ebenfalls gelöscht.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE COLLOCMEMBER

Befehl	Beschreibung
DEFINE COLLOCGROUP	Definiert eine Kollokationsgruppe.
DEFINE COLLOCMEMBER	Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE COLLOCGROUP	Löscht eine Kollokationsgruppe.
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
MOVE NODEDATA	Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
UPDATE COLLOCGROUP	Aktualisiert die Beschreibung einer Kollokationsgruppe.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

DELETE COPYGROUP (Sicherungs- oder Archivierungskopiengruppe löschen)

Mit diesem Befehl kann eine Sicherungs- oder Archivierungskopiengruppe aus einer Verwaltungsklasse gelöscht werden. Eine Kopiengruppe in der AKTIVEN Maßnahmengruppe kann nicht gelöscht werden.

Wird die geänderte Maßnahmengruppe aktiviert, werden alle Dateien, die an eine gelöschte Kopiengruppe gebunden sind, durch die Standardverwaltungsklasse verwaltet.

Die vordefinierte Kopiengruppe STANDARD in der Maßnahmendomäne STANDARD (Maßnahmengruppe STANDARD, Verwaltungsklasse STANDARD) kann gelöscht werden. Wird der IBM Spectrum Protect-Server jedoch später erneut installiert, schreibt der Prozess alle Maßnahmenobjekte STANDARD zurück.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Kopiengruppe gehört.

Syntax

```
>>-DELete COpygroup--Domänenname--Name_der_Maßnahmengruppe--Klassenname-->

   .-STANDARD-.  .-Type--=--Backup------.
>--+----------+--+----------------------+----------------------><
   '-STANDARD-'  '-Type--=--+-Backup--+-'
                            '-Archive-'
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Kopiengruppe gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, zu der die Kopiengruppe gehört.

Klassenname (Erforderlich)
: Gibt die Verwaltungsklasse an, zu der die Kopiengruppe gehört.

STANDARD
: Gibt die Kopiengruppe an, die immer STANDARD lautet. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD.

Type
: Gibt die Art der Kopiengruppe an, die gelöscht werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist BACKUP. Gültige Werte:

  Backup
  : Gibt an, daß die Sicherungskopiengruppe gelöscht wird.

  Archive
  : Gibt an, daß die Archivierungskopiengruppe gelöscht wird.

Beispiel: Eine Sicherungskopiengruppe löschen

Die Sicherungskopiengruppe aus der Verwaltungsklasse ACTIVEFILES löschen, die sich in der Maßnahmengruppe VACATION der Maßnahmendomäne EMPLOYEE_RECORDS befindet.

```
delete copygroup employee_records
vacation activefiles
```

Beispiel: Eine Archivierungskopiengruppe löschen

Die Archivierungskopiengruppe aus der Verwaltungsklasse MCLASS1 löschen, die sich in der Maßnahmengruppe SUMMER der Maßnahmendomäne PROG1 befindet.

```
delete copygroup prog1 summer mclass1 type=archive
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE COPYGROUP

Befehl	Beschreibung
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.

DELETE DATAMOVER (Einheit zum Versetzen von Daten löschen)

Verwenden Sie diesen Befehl, um eine Einheit zum Versetzen von Daten zu löschen. Sie können die Einheit zum Versetzen von Daten nicht löschen, wenn für diese Einheit zum Versetzen von Daten Pfade definiert sind.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DELete DATAMover--Name_der_Einheit_zum_Versetzen_von Daten--><
```

Parameter

Name_der_Einheit_zum_Versetzen_von_Daten (Erforderlich)
Gibt den Namen der Einheit zum Versetzen von Daten an.
Anmerkung: Mit diesem Befehl wird die Einheit zum Versetzen von Daten auch dann gelöscht, wenn für den entsprechenden NAS-Knoten Daten vorhanden sind.

Beispiel: Eine Einheit zum Versetzen von Daten löschen

Die Einheit zum Versetzen von Daten für den Knoten NAS1 löschen.

```
delete datamover nas1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DATAMOVER

Befehl	Beschreibung
DEFINE DATAMOVER	Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
QUERY DATAMOVER	Zeigt Definitionen der Einheit zum Versetzen von Daten an.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE DATAMOVER	Ändert die Definition einer Einheit zum Versetzen von Daten.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

DELETE DEDUPSTATS (Datendeduplizierungsstatistikdaten löschen)

Verwenden Sie diesen Befehl, um Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool oder einen Cloudspeicherpool zu löschen. Die neuesten Datendeduplizierungsstatistikdaten für einen Clientknoten und einen Dateibereich können nicht gelöscht werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich.

Syntax

```
>>-DELete DEDUPSTats--Poolname--+------------+------------------>
                               '-Knotenname-'

   .-*---------------------.  .-CODEType--=--BOTH-----------.
>--+-----------------------+--+-----------------------------+--->
   | .-,-----------------. |  '-CODEType--=--+-UNIcode----+-'
   | V                   | |                 +-NONUNIcode-+
   +---Dateibereichsname-+-+                  '-BOTH-------'
   | .-,---------.         |
   | V           |         |
   '-----FSID----+---------'
```

```
   .-NAMEType--=--SERVER------.
>--+--------------------------+--+------------------+----------->
   '-NAMEType--=--+-SERVER--+-'  '-TODate--=--Datum-'
                  +-UNIcode-+
                  '-FSID----'

>--+-----------------+-------------------------------------------><
   '-TOTime--=--Zeit-'
```

Parameter

Poolname (Erforderlich)
: Gibt den Namen des Verzeichniscontainerspeicherpools an, der in den Datendeduplizierungsstatistikdaten aufgelistet wird. Für den Speicherpoolnamen können bis zu 30 Zeichen angegeben werden. Wenn Sie mehr als 30 Zeichen angeben, schlägt der Befehl fehl.
Einschränkung: Sie können nur Verzeichniscontainerspeicherpools oder Cloudspeicherpools angeben.

Knotenname
: Gibt den Namen des Clientknotens an, der in den Datendeduplizierungsstatistikdaten aufgelistet wird. Dieser Parameter ist wahlfrei. Wird für diesen Parameter kein Wert angegeben, werden alle Knoten angezeigt. Für den Knotennamen können bis zu 64 Zeichen angegeben werden. Wenn Sie mehr als 64 Zeichen angeben, schlägt der Befehl fehl.

Dateibereichsname oder FSID
: Gibt den Namen oder die Dateibereichs-ID (FSID) eines oder mehrerer Dateibereiche an, die in den Datendeduplizierungsstatistikdaten aufgelistet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Der Standardwert ist ein Stern. Geben Sie einen der folgenden Werte an:

  *
  : Geben Sie einen Stern (*) an, um alle Dateibereiche oder IDs anzuzeigen.

  Dateibereichsname
  : Gibt den Namen des Dateibereichs an. Geben Sie mehrere Dateibereiche an, indem Sie die Namen durch Kommas ohne Zwischenleerschritte voneinander trennen. FSID gibt die Dateibereichs-ID an. Dieser Parameter ist für Clients mit Dateibereichen in Unicode-Format gültig. Geben Sie mehrere Dateibereiche an, indem Sie die Namen durch Kommas ohne Zwischenleerschritte voneinander trennen.

  Für Clients mit Dateibereichen in Unicode-Format können Sie entweder einen Dateibereichsnamen oder eine Dateibereichs-ID (FSID) eingeben. Wenn Sie einen Dateibereichsnamen eingeben, muss der Server möglicherweise den eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Codepage des Servers in Unicode konvertieren.
  Einschränkungen: Die folgenden Einschränkungen gelten für Dateibereichsnamen und Dateibereichs-IDs (FSID):

  - Ein Knotenname muss angegeben werden, wenn ein Dateibereichsname angegeben wird.
  - In demselben Befehl dürfen nicht gleichzeitig Dateibereichsnamen und Dateibereichs-IDs (FSIDs) angegeben werden.

CODEType
: Gibt an, welcher Typ von Dateibereichen in den Bericht eingeschlossen werden soll. Der Standardwert lautet BOTH. Dieser Standardwert gibt an, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie einen Stern zum Anzeigen von Informationen zu allen Dateibereichen eingeben. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

  UNIcode
  : Dateibereiche einschließen, die ein Unicode-Format haben.

  NONUNIcode
  : Dateibereiche einschließen, die kein Unicode-Format haben.

  BOTH
  : Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen. Dies ist der Standardwert.

NAMEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter, wenn IBM Spectrum Protect-Clients über Dateibereiche in Unicode-Format verfügen und die Clients unter dem Betriebssystem Windows, NetWare oder Macintosh OS X ausgeführt werden. Dieser Parameter ist wahlfrei.
Dieser Parameter ist erforderlich, wenn Sie einen Knotennamen und einen Dateibereichsnamen bzw. eine Dateibereichs-ID (FSID) angeben.
Einschränkung: Wenn Sie diesen Parameter angeben, darf der Dateibereichsname keinen Stern enthalten.

  Geben Sie einen der folgenden Werte an:

  SERVER
  : Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren. Dies ist der Standardwert.

  UNIcode
  : Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers

ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

FSID

Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

TODate

Gibt das späteste Datum für die zu löschenden Statistikdaten an. IBM Spectrum Protect löscht nur die Statistikdaten mit einem Datum bis zu dem angegebenen Datum (einschließlich). Dieser Parameter ist wahlfrei.

Geben Sie einen der folgenden Werte an:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum.	10/15/2015 Wenn Sie ein Datum angeben, werden alle Kandidatensätze, die an diesem Tag (bis 23:59:59 Uhr) geschrieben wurden, ausgewertet.
TODAY	Das aktuelle Datum.	TODAY
TODAY-Tage oder -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–1 oder –1. Sollen Informationen angezeigt werden, die bis gestern erstellt wurden, können Sie TODATE=TODAY-1 oder TODATE= -1 angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Sätze einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Sätze einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

TOTime

Gibt an, dass Datendeduplizierungsstatistikdaten gelöscht werden sollen, die zu oder vor dieser Zeit am angegebenen Datum erstellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist das Ende des Tages (23:59:59). Geben Sie einen der folgenden Werte an:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Datum.	12:30:22
NOW	Die aktuelle Uhrzeit am angegebenen Datum.	NOW
NOW+HH:MM oder +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Datum.	NOW+03:00 oder +03:00. Wenn Sie den Befehl DELETE DEDUPSTATS um 9:00 Uhr mit TOTIME=NOW+03:00 oder TOTIME=+03:00 ausgeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 Uhr oder früher an dem angegebenen Datum.
NOW-HH:MM oder -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Datum.	NOW-03:30 oder -03:30. Wenn Sie den Befehl DELETE DEDUPSTATS um 9:00 Uhr mit TOTIME=NOW-3:30 oder TOTIME=-3:30 ausgeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 5:30 Uhr oder früher an dem angegebenen Datum.

Beispiel: Datendeduplizierungsstatistikdaten für einen Dateibereich löschen

Datendeduplizierungsstatistikdaten eines Dateibereichs mit dem Namen /srvr löschen, der zum Verzeichniscontainerspeicherpool POOL1 gehört, der auf dem Clientknoten NODE1 gespeichert ist.

```
delete dedupstats pool1 node1 /srvr
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DEDUPSTATS

Befehl	Beschreibung
GENERATE DEDUPSTATS	Generiert Datendeduplizierungsstatistikdaten.
   QUERY DEDUPSTATS	Zeigt Datendeduplizierungsstatistikdaten an.

DELETE DEVCLASS (Einheitenklasse löschen)

Mit diesem Befehl kann eine Einheitenklasse gelöscht werden.

Um diesen Befehl verwenden zu können, müssen zunächst alle Speicherpools gelöscht werden, die der Einheitenklasse zugeordnet sind, und, falls erforderlich, alle Datenbankexport- oder -importprozesse abgebrochen werden, die die Einheitenklasse verwenden.

Die bei der Installation vordefinierte Einheitenklasse DISK kann nicht gelöscht werden; es können jedoch alle Einheitenklassen gelöscht werden, die von dem IBM Spectrum Protect-Administrator definiert wurden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DELete DEVclass--Einheitenklassenname----------------------><
```

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der Einheitenklasse an, die gelöscht werden soll.

Beispiel: Eine Einheitenklasse löschen

Die Einheitenklasse mit dem Namen MYTAPE löschen. Der Einheitenklasse sind keine Speicherpools zugeordnet.

```
delete devclass mytape
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DEVCLASS

Befehl	Beschreibung
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
  DEFINE DEVCLASS (z/OS Media-Server)	  Definiert eine Einheitenklasse für die Verwendung von Speicher, der von einem z/OS Media-Server verwaltet wird.
QUERY DEVCLASS	Zeigt Informationen zu Einheitenklassen an.
QUERY DIRSPACE	Zeigt Informationen zu Verzeichnissen FILE an.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.
  UPDATE DEVCLASS (z/OS Media-Server)	  Ändert die Attribute einer Einheitenklasse für Speicher, der von einem z/OS Media-Server verwaltet wird.

DELETE DOMAIN (Maßnahmendomäne löschen)

Mit diesem Befehl kann eine Maßnahmendomäne gelöscht werden. Alle zugeordneten Maßnahmengruppen, einschließlich der Maßnahmengruppe ACTIVE, Verwaltungsklassen und Kopiengruppen werden mit der Maßnahmendomäne gelöscht.

Eine Maßnahmendomäne, für die Client-Knoten registriert sind, kann nicht gelöscht werden. Um zu bestimmen, ob Clientknoten für eine Maßnahmendomäne registriert sind, geben Sie den Befehl QUERY DOMAIN oder den Befehl QUERY NODE aus. Versetzen Sie alle Clientknoten in eine andere Maßnahmendomäne oder löschen Sie die Knoten.

Die vordefinierte Maßnahmendomäne STANDARD kann gelöscht werden. Wird der IBM Spectrum Protect-Server jedoch später erneut installiert, schreibt der Prozess alle Maßnahmenobjekte STANDARD zurück.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete DOmain--Domänenname----------------------------------><
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, die gelöscht werden soll.

Beispiel: Eine Maßnahmendomäne löschen

Die Maßnahmendomäne EMPLOYEE_RECORDS löschen.

```
delete domain employee_records
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DOMAIN

Befehl	Beschreibung
COPY DOMAIN	Erstellt eine Kopie einer Maßnahmendomäne.
DEFINE DOMAIN	Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
UPDATE DOMAIN	Ändert die Attribute einer Maßnahmendomäne.

DELETE DRIVE (Laufwerk aus einem Kassettenarchiv löschen)

Mit diesem Befehl kann ein Laufwerk aus einem Kassettenarchiv gelöscht werden. Ein Laufwerk, das gerade verwendet wird, kann nicht gelöscht werden.

Alle Pfade zu einem Laufwerk müssen gelöscht werden, bevor das Laufwerk selbst gelöscht werden kann.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DELete DRive--Kassettenarchivname--Laufwerkname-------------><
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, in dem sich das Laufwerk befindet.

Laufwerkname (Erforderlich)
: Gibt den Namen des Laufwerks an, das gelöscht werden soll.

Beispiel: Ein Laufwerk aus einem Kassettenarchiv löschen

Laufwerk DRIVE3 aus dem Kassettenarchiv AUTO löschen.

```
delete drive auto drive3
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE DRIVE

Befehl	Beschreibung

Befehl	Beschreibung
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DELETE LIBRARY	Löscht ein Kassettenarchiv.
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
PERFORM LIBACTION	Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.
QUERY DRIVE	Zeigt Informationen zu Laufwerken an.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
UPDATE DRIVE	Ändert die Attribute eines Laufwerks.

DELETE EVENT (Ereignissätze löschen)

Mit diesem Befehl können Ereignissätze aus der Datenbank gelöscht werden. Ein Ereignissatz wird erstellt, wenn die Verarbeitung eines geplanten Befehls gestartet wird oder fehlschlägt.

Dieser Befehl löscht nur die Ereignissätze, die zum Zeitpunkt der Befehlsverarbeitung vorhanden sind. Ein Ereignissatz wird nicht gefunden, wenn:

- Der Ereignissatz nie erstellt wurde (das Ereignis ist für die Zukunft geplant)
- Das Ereignis bereits stattgefunden hat und der Ereignissatz bereits gelöscht wurde.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

Syntax

```
                        .-00:00-.
>>-DELete EVent--Datum--+-------+-------------------------------->
                        '-Zeit--'

   .-TYPE--=--Client-------------.
>--+----------------------------+----------------------------><
   '-TYPE--=--+-Client---------+-'
              +-ADministrative-+
              '-ALl------------'
```

Parameter

Datum (Erforderlich)
: Gibt das Datum an, mit dem bestimmt wird, welche Ereignissätze gelöscht werden sollen. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.

  Diesen Parameter in Verbindung mit dem Parameter TIME verwenden, um ein Datum und eine Uhrzeit zum Löschen von Ereignissätzen anzugeben. Alle Sätze, deren geplanter Start vor dem angegebenen Datum und der angegebenen Zeit liegt, werden gelöscht. Sätze von Ereignissen, deren Startfenster noch nicht abgelaufen ist, werden jedoch nicht gelöscht.

  Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage	TODAY-3 *oder* -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.

Wert	Beschreibung	Beispiel
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

Zeit

Gibt die Zeit an, mit der bestimmt wird, welche Ereignissätze gelöscht werden sollen. Diesen Parameter in Verbindung mit dem Parameter DATE verwenden, um ein Datum und eine Uhrzeit zum Löschen von Ereignissätzen anzugeben. Alle Sätze, deren geplanter Start vor dem angegebenen Datum und der angegebenen Zeit liegt, werden gelöscht. Sätze von Ereignissen, deren Startfenster noch nicht abgelaufen ist, werden jedoch nicht gelöscht. Der Standardwert ist 00:00.
Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten	NOW+03:00 oder +03:00 Achtung: Wird dieser Befehl um 9:00 Uhr unter Verwendung von NOW+03:00 *oder* +03:00 ausgegeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 oder einer späteren Uhrzeit an dem Datum, das angegeben wird.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW-03:00 *oder* –03:00

TYPE

Gibt die Art der zu löschenden Ereignisse an. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT. Gültige Werte:

Client
: Gibt an, dass Ereignissätze für Clientzeitpläne gelöscht werden sollen.

ADministrative
: Gibt an, dass Ereignissätze für Verwaltungsbefehlszeitpläne gelöscht werden sollen.

ALl
: Gibt an, dass Ereignissätze für Client- und Verwaltungsbefehlszeitpläne gelöscht werden sollen.

Beispiel: Ereignissätze löschen

Sätze für Ereignisse löschen, deren geplante Startzeit vor 08:00 am 26. Mai 1998 (05/26/1998) liegt und deren Startfenster abgelaufen sind. Die Sätze für diese Ereignisse werden unabhängig davon gelöscht, ob der durch den Befehl SET EVENTRETENTION angegebene Aufbewahrungszeitraum für Ereignissätze bereits verstrichen ist.

```
delete event 05/26/1998 08:00
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE EVENT

Befehl	Beschreibung
QUERY EVENT	Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an.
SET EVENTRETENTION	Gibt die Anzahl Tage für die Aufbewahrung von Sätzen geplanter Operationen an.

DELETE EVENTSERVER (Definition des Ereignisservers löschen)

Mit diesem Befehl kann die Definition des Ereignisservers gelöscht werden. Dieser Befehl muss ausgegeben werden, bevor der Befehl DELETE SERVER ausgegeben wird. Wenn der als Ereignisserver definierte Server im Befehl DELETE SERVER angegeben wird, wird eine Fehlernachricht angezeigt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete EVENTSERVer-----------------------------------------><
```

Beispiel: Eine Ereignisserverdefinition löschen

Die Definition des Ereignisservers ASTRO löschen.

```
delete eventserver
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE EVENTSERVER

Befehl	Beschreibung
DEFINE EVENTSERVER	Definiert einen Server als Ereignisserver.
QUERY EVENTSERVER	Zeigt den Namen des Ereignisservers an.

DELETE FILESPACE (Clientknotendaten aus dem Server löschen)

Mit diesem Befehl können Dateibereiche aus dem Server gelöscht werden. Dateien, die zu dem Dateibereich gehören, werden aus primären Speicherpools, Speicherpools für aktive Daten und Kopienspeicherpools sowie aus allen Dateibereichskollokationsgruppen gelöscht.

IBM Spectrum Protect löscht einen oder mehrere Dateibereiche als eine Serie von Stapeldatenbanktransaktionen, wodurch eine ROLLBACK- oder COMMIT-Operation für einen vollständigen Dateibereich als eine einzelne Aktion verhindert wird. Wird der Prozess abgebrochen oder tritt ein Systemfehler auf, kann ein partielles Löschen erfolgen. Mit einem nachfolgenden Befehl DELETE FILESPACE für denselben Knoten oder Eigner können die übrigen Daten gelöscht werden.

Wird dieser Befehl auf einen WORM-Datenträger (WORM = Write Once, Read Many) angewendet, kehrt der Datenträger in den Arbeitsdatenträgerstatus zurück, wenn er über Speicherbereich verfügt, in den Daten geschrieben werden können. (Daten auf WORM-Datenträgern, einschließlich gelöschter und verfallener Daten, können nicht überschrieben werden. Daher können Daten nur in Speicherbereich geschrieben werden, der keine aktuellen, gelöschten oder verfallenen Daten enthält.) Verfügt ein WORM-Datenträger über keinen Speicherbereich mehr, in den Daten geschrieben werden können, verbleibt der Datenträger im privaten Status. Soll der Datenträger aus dem Kassettenarchiv entfernt werden, müssen Sie den Befehl CHECKOUT LIBVOLUME verwenden.

Tipps:

- Ist der Aufbewahrungsschutz für Archivierung aktiviert, löscht der Server Archivierungsdateien mit abgelaufenen Aufbewahrungszeiträumen. Weitere Informationen finden Sie in der Beschreibung des Befehls SET ARCHIVERETENTIONPROTECTION.
- Archivierungsdateien, für die "Löschen unzulässig" angegeben wurde, können vom Server erst gelöscht werden, wenn die Löschsperre aufgehoben wird.
- Die Wiederherstellung wird nicht gestartet, solange der Befehl DELETE FILESPACE ausgeführt wird.
- Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
- Wenn Sie einen Dateibereich in einem deduplizierten Speicherpool löschen, wird der Dateibereichsname DELETED in der Ausgabe des Befehls QUERY OCCUPANCY angezeigt, bis alle Deduplizierungsabhängigkeiten entfernt wurden.
- Wenn die Replikation für einen Dateibereich konfiguriert ist, löscht der Befehl DELETE FILESPACE nur den Dateibereich auf dem Server, auf dem der Befehl ausgegeben wurde. Wird der Befehl REPLICATE NODE ausgegeben, wird der Dateibereich nicht auf dem anderen Replikationsserver gelöscht.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

Syntax

```
>>-DELete FIlespace--Knotenname--Dateibereichsname-------------->

   .-Type--=--ANY--------------.  .-DAta--=--ANY------------.
>--+---------------------------+--+-------------------------+--->
   '-Type--=--+-ANY-----------+-'  '-DAta--=--+-ANY--------+-'
              +-Backup-------+               +-FIles------+
              +-ARchive------+               |        (1) |
              +-SPacemanaged-+               '-IMages-----'
              '-SERver-------'

   .-Wait--=--No------.
>--+------------------+--+----------------------+--------------->
   '-Wait--=--+-No--+-'  '-OWNer--=--Eignername-'
```

```
              '-Yes-'

   .-NAMEType--=--SERVER------.
>--+--------------------------+--------------------------------->
   '-NAMEType--=--+-SERVER--+-'
                  +-UNIcode-+
                  '-FSID----'

   .-CODEType--=--BOTH-----------.
>--+---------------------------+----------------------------><
   '-CODEType--=--+-UNIcode----+-'
                  +-NONUNIcode-+
                  '-BOTH-------'
```

Anmerkungen:

1. Dieser Parameter kann nur verwendet werden, wenn `TYPE=ANY` oder `TYPE=BACKUP` angegeben wird.

Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, zu dem der Dateibereich gehört.

Dateibereichsname (Erforderlich)
: Gibt den Namen des Dateibereichs an, der gelöscht werden soll. Bei diesem Namen muss die Groß-/Kleinschreibung berücksichtigt werden, und der Name muss genau so eingegeben werden, wie er dem Server bekannt ist. Um zu bestimmen, wie der Name eingegeben wird, den Befehl QUERY FILESPACE verwenden. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden.

  Ein Server, der über Clients mit Unterstützung für Unicode verfügt, muss möglicherweise den Dateibereichsnamen, den Sie eingeben, konvertieren. Beispielsweise muss der Server gegebenenfalls den eingegebenen Namen aus der Codepage des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich unter dem Parameter NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

Type
: Gibt den zu löschenden Datentyp an. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Sie können die folgenden Werte verwenden:

  ANY
  : Nur gesicherte Versionen von Dateien und archivierte Kopien von Dateien löschen.

    Wenn Sie `delete filespace` *`Knotenname`* `* type=any` angeben, werden alle gesicherten Daten und archivierten Daten in allen Dateibereichen für diesen Knoten gelöscht. Dateibereiche werden nur gelöscht, wenn sie keine Dateien enthalten, die von einem IBM Spectrum Protect for Space Management-Client versetzt werden.

  Backup
  : Sicherungsdaten für den Dateibereich löschen.

  ARchive
  : Alle archivierten Daten auf dem Server für den Dateibereich löschen.

  SPacemanaged
  : Dateien löschen, die aus dem lokalen Dateisystem eines Benutzers von einem IBM Spectrum Protect for Space Management-Client umgelagert werden. Der Parameter OWNER wird ignoriert, wenn TYPE=SPACEMANAGED angegeben wird.

  SERver
  : Alle archivierten Dateien in allen Dateibereichen für einen Knoten löschen, der als TYPE=SERVER registriert ist.

DAta
: Gibt zu löschende Objekte an. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Sie können einen der folgenden Werte angeben:

  ANY
  : Dateien, Verzeichnisse und Abbilder löschen.

  FIles
  : Dateien und Verzeichnisse löschen.

  IMages
  : Abbildobjekte löschen. Sie können diesen Parameter nur verwenden, wenn Sie TYPE=ANY oder TYPE=BACKUP angegeben haben.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Sie können einen der folgenden Werte angeben:

  No
  : Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

    Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Yes
: Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Erst nachdem der Befehl vollständig ausgeführt wurde, kann mit anderen Aufgaben fortgefahren werden. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungs-Client an, wenn der Befehl beendet ist.
Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

OWNer
: Beschränkt die zu löschenden Daten auf Dateien, die zu dem Eigner gehören. Dieser Parameter ist wahlfrei; er wird bei TYPE=SPACEMANAGED ignoriert. Dieser Parameter gilt nur für Clientmehrbenutzersysteme, wie z. B. AIX, Linux und Solaris OS.

NAMEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode verfügt. Ein Client für Sichern/Archivieren mit Unterstützung für Unicode ist nur für die folgenden Betriebssysteme verfügbar: Windows, Macintosh OS X und NetWare.

  Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

  SERVER
  : Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

  UNIcode
  : Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

  FSID
  : Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

CODEType
: Angeben, welche Art von Dateibereichen in der Operation berücksichtigt werden soll. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Sie können einen der folgenden Werte angeben:

  UNIcode
  : Dateibereiche einschließen, die in Unicode sind.

  NONUNIcode
  : Dateibereiche einschließen, die nicht in Unicode sind.

  BOTH
  : Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

Dateibereich löschen

Den Dateibereich C_Drive löschen, der zum Clientknoten HTANG gehört.

```
delete filespace htang C_Drive
```

Alle speicherverwalteten Dateien für einen Clientknoten löschen

Alle Dateien löschen, die vom Clientknoten APOLLO umgelagert werden (d. h., alle speicherverwalteten Dateien).

```
delete filespace apollo * type=spacemanaged
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE FILESPACE

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY OCCUPANCY	Zeigt Dateibereichsdaten anhand des Speicherpools an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
RENAME FILESPACE	Vergibt einen neuen Namen für einen Clientdateibereich auf dem Server.

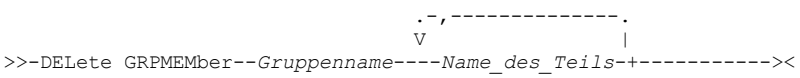
DELETE GRPMEMBER (Server aus einer Servergruppe löschen)

Mit diesem Befehl kann ein Server oder eine Servergruppe aus einer Servergruppe gelöscht werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Gruppenname (Erforderlich)
: Gibt die Gruppe an.

Name_des_Teils (Erforderlich)
: Gibt den Server oder die Gruppe an, der bzw. die aus der Gruppe gelöscht werden soll. Sollen mehrere Namen angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

Beispiel: Einen Server aus einer Servergruppe löschen

Teil PHOENIX aus Gruppe WEST_COMPLEX löschen.

```
delete grpmember west_complex phoenix
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE GRPMEMBER

Befehl	Beschreibung
DEFINE GRPMEMBER	Definiert einen Server als Teil einer Servergruppe.
DEFINE SERVERGROUP	Definiert eine neue Servergruppe.
DELETE SERVER	Löscht die Definition eines Servers.
DELETE SERVERGROUP	Löscht eine Servergruppe.
MOVE GRPMEMBER	Versetzt einen Teil einer Servergruppe.
QUERY SERVER	Zeigt Informationen über Server an.
QUERY SERVERGROUP	Zeigt Informationen über Servergruppen an.
RENAME SERVERGROUP	Benennt eine Servergruppe um.
UPDATE SERVERGROUP	Aktualisiert eine Servergruppe.

DELETE LIBRARY (Kassettenarchiv löschen)

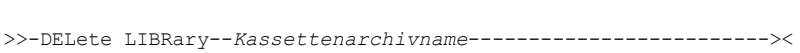
Mit diesem Befehl kann ein Kassettenarchiv gelöscht werden. Bevor Sie ein Kassettenarchiv löschen, müssen Sie andere zugeordnete Objekte, wie beispielsweise den Pfad, löschen.

Mit diesem Befehl kann ein Kassettenarchiv gelöscht werden. Bevor Sie ein Kassettenarchiv löschen, löschen Sie den Pfad und alle zugeordneten Laufwerke.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax



Parameter

Speicherarchivname (Erforderlich)
Gibt den Namen des Kassettenarchivs an, das gelöscht werden soll.

Beispiel: Ein manuelles Kassettenarchiv löschen

Das manuelle Kassettenarchiv LIBR1 löschen.

```
delete library libr1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE LIBRARY

Befehl	Beschreibung
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE DRIVE	Löscht ein Laufwerk aus einem Kassettenarchiv.
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
PERFORM LIBACTION	Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.
QUERY DRIVE	Zeigt Informationen zu Laufwerken an.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE DRIVE	Ändert die Attribute eines Laufwerks.
UPDATE LIBRARY	Ändert die Attribute eines Kassettenarchivs.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.

DELETE MACHINE (Maschineninformationen löschen)

Mit diesem Befehl können Maschineninformationen gelöscht werden. Sollen vorhandene Informationen ersetzt werden, diesen Befehl ausgeben und dann einen Befehl INSERT MACHINE verwenden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete MACHine--Maschinenname--------------------------------->

   .-Type--=--All----------------------.
>--+-----------------------------------+----------------------><
   '-Type--=--+-All------------------+-'
              +-RECOVERYInstructions-+
              '-CHaracteristics------'
```

Parameter

Maschinenname (Erforderlich)
Gibt den Namen der Maschine an, deren Informationen gelöscht werden sollen.

Type
Gibt die Art der Maschineninformationen an. Dieser Parameter ist wahlfrei. Standardwert ist ALL. Gültige Werte:

All
Gibt alle Informationen an.

RECOVERYInstructions
Gibt die Anweisungen zur Fehlerbehebung an.

CHaracteristics
Gibt die Maschinenkenndaten an.

Beispiel: Informationen zu einer bestimmten Maschine löschen

Die Maschinenkenndaten löschen, die der Maschine DISTRICT5 zugeordnet sind.

```
delete machine district5 type=characteristics
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE MACHINE

Befehl	Beschreibung
DEFINE MACHINE	Definiert eine Maschine für DRM.
INSERT MACHINE	Fügt Maschinenkenndaten oder Wiederherstellungsanweisungen in die IBM Spectrum Protect-Datenbank ein.
QUERY MACHINE	Zeigt Informationen über Maschinen an.
QUERY RECOVERYMEDIA	Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an.
UPDATE MACHINE	Ändert die Informationen zu einer Maschine.

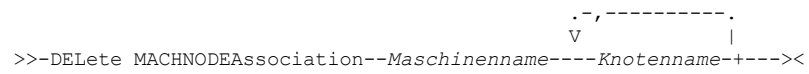
DELETE MACHNODEASSOCIATION (Zuordnung zwischen Maschine und Knoten löschen)

Mit diesem Befehl kann die Zuordnung zwischen einer Maschine und einem oder mehreren Knoten gelöscht werden. Dieser Befehl löscht nicht den Knoten aus IBM Spectrum Protect.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Maschinenname (Erforderlich)
: Gibt den Namen einer Maschine an, die einem oder mehreren Knoten zugeordnet ist.

Knotenname (Erforderlich)
: Gibt den Namen eines Knotens an, der einer Maschine zugeordnet ist. Wird eine Liste mit Knotennamen angegeben, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.Ist ein Knoten nicht der Maschine zugeordnet, wird dieser Knoten ignoriert.

Beispiel: Eine Zuordnung zwischen einem Knoten und einer Maschine löschen

Die Zuordnung zwischen Maschine DISTRICT5 und Knoten ACCOUNTSPAYABLE löschen.

```
delete machnodeassociation district5 accountspayable
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE MACHNODEASSOCIATION

Befehl	Beschreibung
DEFINE MACHNODEASSOCIATION	Ordnet einen IBM Spectrum Protect-Knoten einer Maschine zu.
QUERY MACHINE	Zeigt Informationen über Maschinen an.

DELETE MGMTCLASS (Verwaltungsklasse löschen)

Mit diesem Befehl kann eine Verwaltungsklasse gelöscht werden. Eine Verwaltungsklasse in der aktiven Maßnahmengruppe (ACTIVE) kann nicht gelöscht werden. Alle Kopiengruppen in der Verwaltungsklasse werden mit der Verwaltungsklasse gelöscht.

Der Benutzer kann die Verwaltungsklasse löschen, die als Standardwert für eine Maßnahmengruppe zugeordnet ist, eine Maßnahmengruppe kann jedoch nur aktiviert werden, wenn sie über eine Standardverwaltungsklasse verfügt.

Die vordefinierte Verwaltungsklasse STANDARD in der Maßnahmendomäne STANDARD kann gelöscht werden. Wird der IBM Spectrum Protect-Server jedoch später erneut installiert, schreibt der Prozess alle Maßnahmenobjekte STANDARD zurück.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Verwaltungsklasse gehört.

Syntax

```
>>-DELete MGmtclass--Domänenname--Name_der_Maßnahmengruppe--Klassenname-><
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Verwaltungsklasse gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, zu der die Verwaltungsklasse gehört.

Klassenname (Erforderlich)
: Gibt die Verwaltungsklasse an, die gelöscht werden soll.

Beispiel: Eine Verwaltungsklasse löschen

Die Verwaltungsklasse ACTIVEFILES aus der Maßnahmengruppe VACATION der Maßnahmendomäne EMPLOYEE_RECORDS löschen.

```
delete mgmtclass employee_records
vacation activefiles
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE MGMTCLASS

Befehl	Beschreibung
ASSIGN DEFMGMTCLASS	Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu.
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.
UPDATE MGMTCLASS	Ändert die Attribute einer Verwaltungsklasse.

DELETE NODEGROUP (Knotengruppe löschen)

Verwenden Sie diesen Befehl, um eine Knotengruppe zu löschen. Eine Knotengruppe kann nicht gelöscht werden, wenn sie Einträge enthält.

Achtung: Sie können alle Einträge in der Knotengruppe entfernen, indem Sie den Befehl DELETE NODEGROUPMEMBER mit einem Platzhalterzeichen im Parameter Knotenname ausgeben.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

Syntax

```
>>-DELete NODEGroup--Gruppenname------------------------------><
```

Parameter

Gruppenname
: Gibt den Namen der Knotengruppe an, die gelöscht werden soll.

Beispiel: Eine Knotengruppe löschen

Die Knotengruppe `group1` löschen.

```
delete nodegroup group1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE NODEGROUP

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

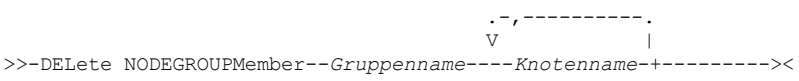
DELETE NODEGROUPMEMBER (Eintrag aus der Knotengruppe löschen)

Verwenden Sie diesen Befehl, um einen Clientknoten aus einer Knotengruppe zu löschen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

Syntax



Parameter

Gruppenname
: Gibt den Namen der Knotengruppe an, aus der ein Clientknoten gelöscht werden soll.

Knotenname
: Gibt den Namen des Clientknotens an, der aus der Knotengruppe gelöscht werden soll. Sie können einen oder mehrere Namen angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können auch Platzhalterzeichen verwenden, um mehrere Knoten anzugeben.

Beispiel: Knoten aus einer Knotengruppe löschen

Die beiden Knoten `node1` und `node2` aus der Knotengruppe `group1` löschen.

```
delete nodegroupmember group1 node1,node2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE NODEGROUPMEMBER

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUP	Löscht eine Knotengruppe.

Befehl	Beschreibung
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

DELETE PATH (Pfad löschen)

Verwenden Sie diesen Befehl, um eine Pfaddefinition zu löschen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DELete PATH--Quellenname--Zielname--------------------------->

                           (1)
>--SRCType--=--+-DATAMover-----+-------------------------------->
               '-SERVer--------'

                        (2)
>--DESTType--=--+-DRive------LIBRary--=--Kassettenarchivname-+-><
                '-LIBRary-----------------------------------'
```

Anmerkungen:

1. Dieser Parameter ist nur für die Betriebssysteme AIX, HP-UX, Linux, Solaris und Windows verfügbar.
2. Dieser Parameter ist nur für die Betriebssysteme AIX, HP-UX, Linux, Solaris und Windows verfügbar.

Parameter

Quellenname (Erforderlich)
: Gibt den Namen der Quelle des Pfads an, der gelöscht werden soll. Dieser Parameter ist erforderlich.

  Bei dem angegebenen Namen muss es sich um den Namen eines Servers oder einer Einheit zum Versetzen von Daten handeln, der bereits für den Server definiert ist.

Zielname (Erforderlich)
: Gibt den Namen des Ziels des Pfads an, der gelöscht werden soll. Dieser Parameter ist erforderlich.

SRCType (Erforderlich)
: Gibt den Typ der Quelle des Pfads an, der gelöscht werden soll. Dieser Parameter ist erforderlich. Gültige Werte:

  DATAMover
  : Gibt an, dass eine Einheit zum Versetzen von Daten die Quelle ist.

  SERVer
  : Gibt an, dass ein Speicheragent die Quelle ist.

DESTType (Erforderlich)
: Gibt den Typ des Ziels an. Gültige Werte:

  DRive LIBRary=Kassettenarchivname
  : Gibt an, dass ein Laufwerk das Ziel ist. Die Parameter DRIVE und LIBRARY sind erforderlich, wenn der Zieltyp DRIVE ist.

  LIBRary
  : Gibt an, dass ein Kassettenarchiv das Ziel ist.
    Achtung: Wird der Pfad von einer Einheit zum Versetzen von Daten zu einem Kassettenarchiv oder der Pfad vom Server zu einem Kassettenarchiv gelöscht, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird bei diesem Status der Server angehalten und erneut gestartet, wird das Kassettenarchiv nicht initialisiert.

Beispiel: Einen Pfad von einer NAS-Einheit zum Versetzen von Daten löschen

Einen Pfad von der NAS-Einheit zum Versetzen von Daten NAS1 zu dem Kassettenarchiv NASLIB löschen.

```
delete path nas1 naslib srctype=datamover desttype=library
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE PATH

Befehl	Beschreibung
DEFINE DATAMOVER	Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
PERFORM LIBACTION	Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.

DELETE POLICYSET (Maßnahmengruppe löschen)

Mit diesem Befehl kann eine Maßnahmengruppe gelöscht werden. Wenn eine Maßnahmengruppe gelöscht wird, werden alle Verwaltungsklassen und Kopiengruppen, die zu der Maßnahmengruppe gehören, ebenfalls gelöscht.

Die Maßnahmengruppe ACTIVE in einer Maßnahmendomäne kann nicht gelöscht werden. Sie können den Inhalt der Maßnahmengruppe ACTIVE ersetzen, indem Sie eine andere Maßnahmengruppe aktivieren. Andernfalls können Sie die Maßnahmengruppe ACTIVE nur entfernen, indem Sie die Maßnahmendomäne löschen, die die Maßnahmengruppe enthält.

Die vordefinierte Maßnahmengruppe STANDARD kann gelöscht werden. Wird der IBM Spectrum Protect-Server jedoch später erneut installiert, schreibt der Prozess alle Maßnahmenobjekte STANDARD zurück.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

Syntax

```
>>-DELete POlicyset--Domänenname--Name_der_Maßnahmengruppe-----><
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Maßnahmengruppe gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, die gelöscht werden soll.

Beispiel: Eine Maßnahmengruppe löschen

Die Maßnahmengruppe `VACATION` aus der Maßnahmendomäne `EMPLOYEE_RECORDS` löschen, indem der folgende Befehl ausgegeben wird:

```
delete policyset employee_records vacation
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE POLICYSET

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
COPY POLICYSET	Erstellt eine Kopie einer Maßnahmengruppe.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
UPDATE POLICYSET	Ändert die Beschreibung einer Maßnahmengruppe.
VALIDATE POLICYSET	Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert.

DELETE PROFASSOCIATION (Profilzuordnung löschen)

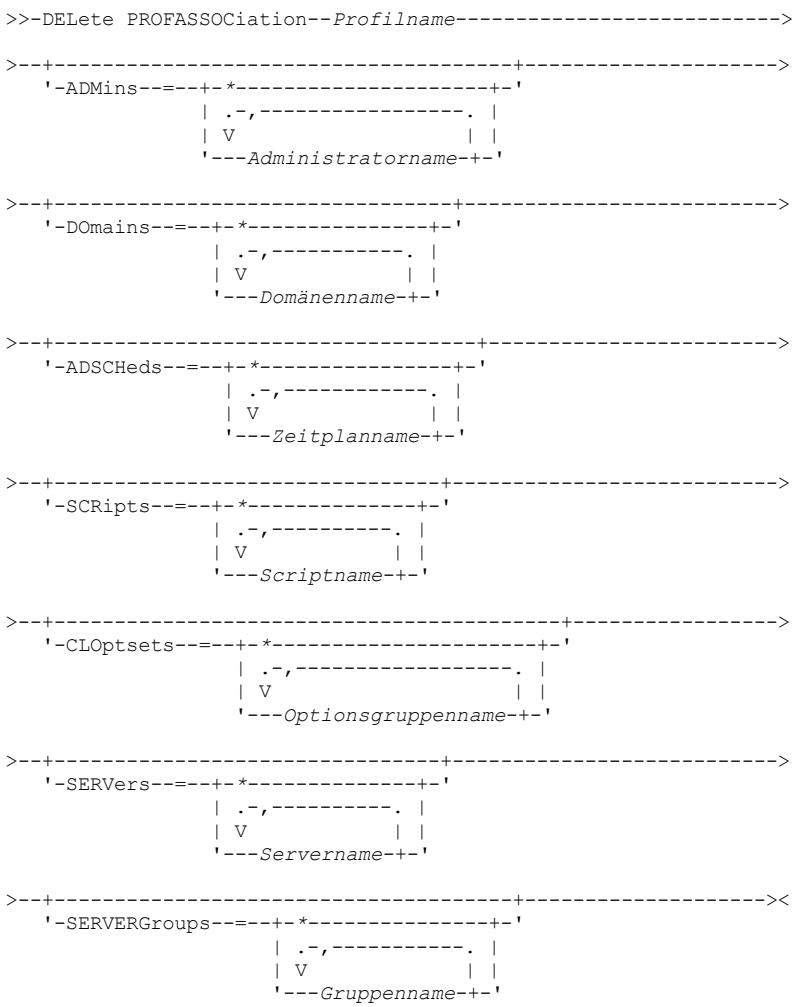
Mit diesem Befehl kann auf einem Konfigurationsmanager die Zuordnung von einem oder mehreren Objekten aus einem Profil gelöscht werden. Werden Zuordnungen gelöscht, werden die Objekte nicht mehr an subskribierende verwaltete Server verteilt. Wenn verwaltete Server aktualisierte Konfigurationsdaten anfordern, informiert sie der Konfigurationsmanager über die gelöschten Objekte.

Ein verwalteter Server löscht die Objekte, die aus dem Profil gelöscht wurden, es sei denn, die Objekte sind einem anderen Profil zugeordnet, für das dieser Server subskribiert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Profilname (Erforderlich)
: Gibt das Profil an, aus dem Zuordnungen gelöscht werden sollen.

ADMins
: Gibt die Administratoren an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen * verwenden, um alle Administratoren aus dem Profil zu löschen. Wird eine Administratorliste angegeben und ist für das Profil eine globale Definition vorhanden, schlägt der Befehl fehl. Administratordefinitionen werden auf dem Konfigurationsmanager nicht geändert. Sie werden jedoch bei der nächsten Konfigurationsaktualisierung automatisch aus allen subskribierenden verwalteten Servern gelöscht. Dabei gelten folgende Ausnahmen:

  - Ein Administrator wird nicht gelöscht, wenn dieser Administrator eine offene Sitzung auf dem Server hat.
  - Ein Administrator wird nicht gelöscht, wenn der verwaltete Server als Folge des Löschens über keine Administratoren mit Systemberechtigung verfügen würde.

DOmains
Gibt die Domänen an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen * verwenden, um alle Domänen aus dem Profil zu löschen. Wird eine Domänenliste angegeben und ist für das Profil eine globale Domänendefinition vorhanden, schlägt der Befehl fehl.

Die Domäneninformationen werden automatisch aus allen subskribierenden verwalteten Servern gelöscht. Eine Maßnahmendomäne, der Client-Knoten zugeordnet sind, wird jedoch nicht gelöscht. Um die Domäne auf dem verwalteten Server zu löschen, müssen diese Clientknoten einer anderen Maßnahmendomäne zugeordnet werden.

ADSCHeds
Gibt eine Liste der Verwaltungszeitpläne an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird eine Verwaltungszeitplanliste angegeben und ist für das Profil eine globale Verwaltungszeitplandefinition vorhanden, schlägt der Befehl fehl. Das Zeichen * verwenden, um alle Verwaltungszeitpläne aus dem Profil zu löschen.

Die Verwaltungszeitpläne werden automatisch aus allen subskribierenden verwalteten Servern gelöscht. Ein Verwaltungszeitplan wird jedoch nicht gelöscht, wenn der Zeitplan auf dem verwalteten Server aktiv ist. Um einen aktiven Zeitplan zu löschen, muß der Zeitplan inaktiviert werden.

SCRipts
Gibt die Server-Befehlsprozeduren an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen * verwenden, um alle Prozeduren aus dem Profil zu löschen. Wird eine Prozedurliste angegeben und ist für das Profil eine globale Prozedurdefinition vorhanden, schlägt der Befehl fehl. Die Server-Befehlsprozeduren werden automatisch aus allen subskribierenden verwalteten Servern gelöscht.

CLOptsets
Gibt die Client-Optionsgruppen an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen * verwenden, um alle Client-Optionsgruppen aus dem Profil zu löschen. Wird eine Client-Optionsgruppenliste angegeben und ist für das Profil eine globale Client-Optionsgruppendefinition vorhanden, schlägt der Befehl fehl. Die Clientoptionsgruppen werden automatisch aus allen subskribierenden verwalteten Servern gelöscht.

SERVers
Gibt die Server an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen * verwenden, um alle Server aus dem Profil zu löschen. Wird eine Server-Liste angegeben und ist für das Profil eine globale Server-Definition vorhanden, schlägt der Befehl fehl. Die Serverdefinitionen werden automatisch aus allen subskribierenden verwalteten Servern gelöscht. Dabei gelten folgende Ausnahmen:

- Eine Serverdefinition wird nicht gelöscht, wenn der verwaltete Server über eine geöffnete Verbindung zu einem anderen Server verfügt.
- Eine Serverdefinition wird nicht gelöscht, wenn der verwaltete Server über eine Einheitenklasse des Einheitentyps SERVER verfügt, die auf den anderen Server verweist.
- Eine Serverdefinition wird nicht gelöscht, wenn es sich um den Ereignisserver für den verwalteten Server handelt.

SERVERGroups
Gibt die Server-Gruppen an, deren Zuordnung zu dem Profil gelöscht wird. Es können mehrere Namen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Das Zeichen * verwenden, um alle Server-Gruppen aus dem Profil zu löschen. Wird eine Server-Gruppenliste angegeben und ist für das Profil eine globale Gruppendefinition vorhanden, schlägt der Befehl fehl. Die Servergruppendefinitionen werden automatisch aus allen subskribierenden verwalteten Servern gelöscht.

Beispiel: Die Domänenzuordnungen für ein bestimmtes Profil löschen

Alle Domänenzuordnungen aus dem Profil MIKE löschen.

```
delete profassociation mike domains=*
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE PROFASSOCIATION

Befehl	Beschreibung
COPY PROFILE	Erstellt eine Kopie eines Profils.
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DELETE PROFILE	Löscht ein Profil aus einem Konfigurationsmanager.
LOCK PROFILE	Verhindert die Verteilung eines Konfigurationsprofils.
NOTIFY SUBSCRIBERS	Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.

Befehl	Beschreibung
QUERY PROFILE	Zeigt Informationen über Konfigurationsprofile an.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UNLOCK PROFILE	Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

DELETE PROFILE (Profil löschen)

Mit diesem Befehl kann auf einem Konfigurationsmanager ein Profil gelöscht und seine Verteilung an verwaltete Server gestoppt werden.

Ein gesperrtes Profil kann nicht gelöscht werden. Das Profil muss zuerst mit dem Befehl UNLOCK PROFILE entsperrt werden.

Durch das Löschen eines Profils aus einem Konfigurationsmanager werden die diesem Profil zugeordneten Objekte nicht aus den verwalteten Servern gelöscht. Mit dem Befehl DELETE SUBSCRIPTION und dem Parameter DISCARDOBJECTS=YES können auf jedem subskribierenden verwalteten Server Subskriptionen für das Profil und die zugeordneten Objekte gelöscht werden. Auf diese Weise wird auch verhindert, dass die verwalteten Server weitere Aktualisierungen des Profils anfordern.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                                .-Force--=--No------.
>>-DELete PROFIle--Profilname--+-------------------+-----------><
                                '-Force--=--+-No--+-'
                                            '-Yes-'
```

Parameter

Profilname (Erforderlich)
: Gibt das Profil an, das gelöscht werden soll.

Force
: Gibt an, ob das Profil gelöscht wird, wenn ein oder mehrere verwaltete Server über Subskriptionen für das Profil verfügen. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, dass das Profil nicht gelöscht wird, wenn ein oder mehrere verwaltete Server über Subskriptionen für das Profil verfügen. Die Subskriptionen auf jedem verwalteten Server können mit dem Befehl DELETE SUBSCRIPTION gelöscht werden.

  Yes
  : Gibt an, dass das Profil gelöscht wird, auch wenn ein oder mehrere verwaltete Server über Subskriptionen für das Profil verfügen. Alle subskribierenden Server fordern weiterhin Aktualisierungen für das gelöschte Profil an, bis die Subskription gelöscht wird.

Beispiele: Ein Profil löschen

Das Profil BETA löschen, auch wenn Subskriptionen von verwalteten Servern vorhanden sind.

```
delete profile beta force=yes
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE PROFILE

Befehl	Beschreibung
COPY PROFILE	Erstellt eine Kopie eines Profils.
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DEFINE SUBSCRIPTION	Subskribiert einen verwalteten Server für ein Profil.
DELETE PROFASSOCIATION	Löscht die Zuordnung zwischen einem Objekt und einem Profil.
DELETE SUBSCRIPTION	Löscht eine angegebene Profilsubskription.
LOCK PROFILE	Verhindert die Verteilung eines Konfigurationsprofils.

Befehl	Beschreibung
QUERY PROFILE	Zeigt Informationen über Konfigurationsprofile an.
QUERY SUBSCRIPTION	Zeigt Informationen über Profilsubskriptionen an.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UNLOCK PROFILE	Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

DELETE RECMEDMACHASSOCIATION (Zuordnung Datenträger/Maschine löschen)

Mit diesem Befehl kann die Zuordnung von Maschinen zu einem Wiederherstellungsdatenträger aufgehoben werden. Dieser Befehl löscht nicht die Maschine aus IBM Spectrum Protect.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete RECMEDMACHAssociation--Datenträgername---------------->

   .-,-------------.
   V               |
>----Maschinenname-+-------------------------------------------><
```

Parameter

Datenträgername (Erforderlich)
: Gibt den Namen des Wiederherstellungsdatenträgers an, der einer oder mehreren Maschinen zugeordnet ist.

Maschinenname (Erforderlich)
: Gibt den Namen der Maschine an, die dem Wiederherstellungsdatenträger zugeordnet ist. Soll eine Liste mit Maschinennamen angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.Ist eine Maschine nicht dem Wiederherstellungsdatenträger zugeordnet, wird die Maschine ignoriert.

Beispiel: Die Zuordnung einer Maschine zu Wiederherstellungsdatenträgern löschen

Die Zuordnung zwischen dem Wiederherstellungsdatenträger DIST5RM und den Maschinen DISTRICT1 und DISTRICT5 löschen.

```
delete recmedmachassociation
dist5rm district1,district5
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE RECMEDMACHASSOCIATION

Befehl	Beschreibung
DEFINE RECMEDMACHASSOCIATION	Ordnet Wiederherstellungsdatenträger einer Maschine zu.
QUERY MACHINE	Zeigt Informationen über Maschinen an.
QUERY RECOVERYMEDIA	Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an.

DELETE RECOVERYMEDIA (Wiederherstellungsdatenträger löschen)

Mit diesem Befehl kann die Definition eines Wiederherstellungsdatenträgers aus IBM Spectrum Protect gelöscht werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete RECOVERYMedia--Datenträgername----------------------><
```

Parameter

Datenträgername (Erforderlich)
Gibt den Namen des Wiederherstellungsdatenträgers an.

Beispiel: Die Definition eines Wiederherstellungsdatenträgers löschen

Den Wiederherstellungsdatenträger DIST5RM löschen.

```
delete recoverymedia dist5rm
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE RECOVERYMEDIA

Befehl	Beschreibung
DEFINE RECOVERYMEDIA	Definiert die Datenträger, die für die Wiederherstellung einer Maschine erforderlich sind.
QUERY RECOVERYMEDIA	Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an.
UPDATE RECOVERYMEDIA	Ändert die Attribute von Wiederherstellungsdatenträgern.

DELETE SCHEDULE (Zeitplan für Client oder Verwaltungsbefehl löschen)

Mit diesem Befehl können Zeitpläne aus der Datenbank gelöscht werden.

Der Befehl DELETE SCHEDULE hat zwei Formen: eine Form, wenn der Zeitplan Clientoperationen betrifft, und eine Form, wenn der Zeitplan Verwaltungsbefehle betrifft. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für DELETE SCHEDULE

Befehl	Beschreibung
COPY SCHEDULE	Erstellt eine Kopie eines Zeitplans.
DEFINE SCHEDULE	Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.
QUERY SCHEDULE	Zeigt Informationen über Zeitpläne an.
UPDATE SCHEDULE	Ändert die Attribute eines Zeitplans.

- DELETE SCHEDULE (Clientzeitplan löschen)
  Mit dem Befehl DELETE SCHEDULE können ein oder mehrere Clientzeitpläne aus der Datenbank gelöscht werden. Alle Clientzuordnungen zu einem Zeitplan werden beim Löschen des Zeitplans entfernt.
- DELETE SCHEDULE (Verwaltungszeitplan löschen)
  Mit diesem Befehl können ein oder mehrere Zeitpläne für Verwaltungsbefehle aus der Datenbank gelöscht werden.

DELETE SCHEDULE (Clientzeitplan löschen)

Mit dem Befehl DELETE SCHEDULE können ein oder mehrere Clientzeitpläne aus der Datenbank gelöscht werden. Alle Clientzuordnungen zu einem Zeitplan werden beim Löschen des Zeitplans entfernt.

Berechtigungsklasse

Zum Löschen eines Clientzeitplans ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die angegebene Maßnahmendomäne erforderlich.

Syntax

```
>>-DELete SCHedule--Domänenname--Zeitplanname------------------>

   .-Type--=--Client-.
>--+-----------------+-----------------------------------------><
```

Parameter

Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an, zu der der Zeitplan gehört.

Zeitplanname (Erforderlich)
: Gibt den Namen des zu löschenden Zeitplans an. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

Type=Client
: Gibt an, dass ein Clientzeitplan gelöscht werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT.

Beispiel: Einen bestimmten Zeitplan aus einer bestimmten Maßnahmendomäne löschen

Den Zeitplan WEEKLY_BACKUP löschen, der zu der Maßnahmendomäne EMPLOYEE_RECORDS gehört.

```
delete schedule employee_records weekly_backup
```

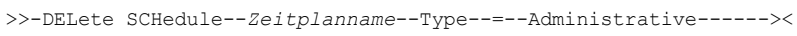
DELETE SCHEDULE (Verwaltungszeitplan löschen)

Mit diesem Befehl können ein oder mehrere Zeitpläne für Verwaltungsbefehle aus der Datenbank gelöscht werden.

Berechtigungsklasse

Zum Löschen eines Zeitplans für Verwaltungsbefehle ist die Systemberechtigung erforderlich.

Syntax



Parameter

Zeitplanname (Erforderlich)
: Gibt den Namen des zu löschenden Zeitplans an. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

Type=Administrative (Erforderlich)
: Gibt an, dass ein Zeitplan für Verwaltungsbefehle gelöscht werden soll.

Beispiel: Einen Zeitplan für Verwaltungsbefehle löschen

Den Zeitplan für Verwaltungsbefehle mit dem Namen DATA_ENG löschen.

```
delete schedule data_eng type=administrative
```

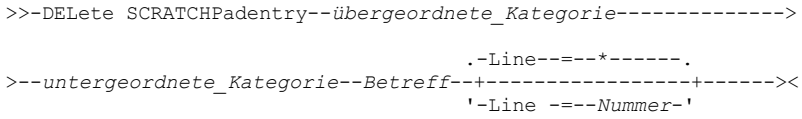
DELETE SCRATCHPADENTRY (Scratchpadeintrag löschen)

Mit diesem Befehl können Sie ein oder mehrere Zeilen mit Daten aus einem Scratchpad löschen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

übergeordnete_Kategorie (Erforderlich)
: Gibt die übergeordnete Kategorie an, aus der eine oder mehrere Zeilen mit Daten gelöscht werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

untergeordnete_Kategorie (Erforderlich)
: Gibt die untergeordnete Kategorie an, aus der eine oder mehrere Zeilen mit Daten gelöscht werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Betreff (Erforderlich)
: Gibt den Betreff an, aus dem eine oder mehrere Zeilen mit Daten gelöscht werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Line
: Gibt eine Zeile mit Daten an, die gelöscht werden soll. Geben Sie für Nummer die Nummer der Zeile ein, die gelöscht werden soll. Es werden alle Daten in der Zeile gelöscht. Die Nummerierung der anderen Zeilen im Betreffabschnitt ist davon nicht betroffen. Sie können alle Zeilen mit Daten aus einem Betreffabschnitt löschen, indem Sie den Parameter Line in diesem Befehl übergehen.

Beispiel: Alle Zeilen mit Daten aus einem Betreff in einem Scratchpad löschen

Löschen Sie alle Zeilen mit Daten zum Standort eines Administrators, Jane, aus einer Datenbank, in der Informationen zu Administratoren gespeichert sind:

```
delete scratchpadentry admin_info location jane
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SCRATCHPADENTRY

Befehl	Beschreibung
DEFINE SCRATCHPADENTRY	Erstellt eine Zeile mit Daten im Scratchpad.
QUERY SCRATCHPADENTRY	Zeigt Informationen an, die im Scratchpad enthalten sind.
SET SCRATCHPADRETENTION	Gibt den Zeitraum an, den Scratchpadeinträge aufbewahrt werden.
UPDATE SCRATCHPADENTRY	Aktualisiert Daten in einer Zeile im Scratchpad.

DELETE SCRIPT (Befehlszeilen aus Prozedur oder gesamte Prozedur löschen)

Mit diesem Befehl kann eine einzelne Zeile aus einer IBM Spectrum Protect-Prozedur oder die vollständige IBM Spectrum Protect-Prozedur gelöscht werden.

Berechtigungsklasse

Um diesen Befehl ausgeben zu können, muß der Administrator die Prozedur zuvor definiert oder die Systemberechtigung haben.

Syntax

```
>>-DELete SCRipt--Prozedurname--+-----------------+------------><
                                '-Line -=--Nummer-'
```

Parameter

Prozedurname (Erforderlich)
: Gibt den Namen der Prozedur an, die gelöscht werden soll. Die Prozedur wird gelöscht, es sei denn, es wird eine Zeilennummer angegeben.

Line
: Gibt die Nummer der Zeile an, die aus der Prozedur gelöscht werden soll. Wird keine Zeilennummer angegeben, wird die vollständige Prozedur gelöscht.

Beispiel: Eine bestimmte Zeile aus einem Script löschen

Das folgende Script mit dem Namen QSAMPLE wird verwendet und ein Befehl ausgegeben, um Zeile 005 aus dem Script zu löschen.

```
001  /* Dies ist eine Beispielprozedur */
005  QUERY STATUS
010  QUERY PROCESS
```

```
delete script qsample line=5
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SCRIPT

Befehl	Beschreibung
COPY SCRIPT	Erstellt eine Kopie einer Prozedur.
DEFINE SCRIPT	Definiert eine Prozedur für den IBM Spectrum Protect-Server.

Befehl	Beschreibung
QUERY SCRIPT	Zeigt Informationen über Prozeduren an.
RENAME SCRIPT	Vergibt einen neuen Namen für eine Prozedur.
RUN	Führt ein Script aus.
UPDATE SCRIPT	Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.

DELETE SERVER (Server-Definition löschen)

Mit diesem Befehl kann eine Server-Definition gelöscht werden.

Dieser Befehl schlägt fehl, wenn der Server

- als Ereignisserver definiert ist.
- in einer Einheitenklassendefinition mit dem Einheitentyp SERVER angegeben ist.
- eine offene Verbindung zu oder von einem anderen Server hat.
- ein Zielserver für virtuelle Datenträger ist.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete--SERver--Servername---------------------------------><
```

Parameter

Servername (Erforderlich)
Gibt einen Server-Namen an.

Beispiel: Die Definition eines Servers löschen

Die Definition für den Server SERVER2 löschen.

```
delete server server2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SERVER

Befehl	Beschreibung
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
QUERY EVENTSERVER	Zeigt den Namen des Ereignisservers an.
QUERY SERVER	Zeigt Informationen über Server an.
RECONCILE VOLUMES	Stimmt Definitionen von virtuellen Datenträgern auf dem Quellenserver mit Archivierungsobjekten des Zielservers ab.
UPDATE SERVER	Aktualisiert Informationen über einen Server.

DELETE SERVERGROUP (Servergruppe löschen)

Mit diesem Befehl kann eine Server-Gruppe gelöscht werden. Ist die Gruppe, die gelöscht wird, ein Teil anderer Server-Gruppen, entfernt IBM Spectrum Protect die Gruppe auch aus den anderen Server-Gruppen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete SERVERGroup--Gruppenname----------------------------><
```

Parameter

Gruppenname (Erforderlich)
: Gibt die Server-Gruppe an, die gelöscht werden soll.

Beispiel: Eine Servergruppe löschen

Die Server-Gruppe WEST_COMPLEX löschen.

```
delete servergroup west_complex
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SERVERGROUP

Befehl	Beschreibung
COPY SERVERGROUP	Erstellt eine Kopie einer Servergruppe.
DEFINE GRPMEMBER	Definiert einen Server als Teil einer Servergruppe.
DEFINE SERVERGROUP	Definiert eine neue Servergruppe.
DELETE GRPMEMBER	Löscht einen Server aus einer Servergruppe.
MOVE GRPMEMBER	Versetzt einen Teil einer Servergruppe.
QUERY SERVERGROUP	Zeigt Informationen über Servergruppen an.
RENAME SERVERGROUP	Benennt eine Servergruppe um.
UPDATE SERVERGROUP	Aktualisiert eine Servergruppe.

DELETE SPACETRIGGER (Speicherbereichsauslöser für Speicherpool löschen)

Mit diesem Befehl kann die Definition des Speicherbereichsauslösers für den Speicherpool gelöscht werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-DELete SPACETrigger--STG--+------------------------------+-->&lt;
                            '-STGPOOL--=--Speicherpoolname-'
```

Parameter

STG
: Gibt einen Speicherbereichsauslöser für den Speicherpool an.

STGPOOL
: Gibt den Speicherpoolauslöser an, der gelöscht werden soll. Wird STG ohne STGPOOL angegeben, ist der standardmäßige Speicherbereichsauslöser für den Speicherpool das Löschziel.

Beispiel: Die Definition eines Speicherbereichsauslösers löschen

Die Definition des Speicherbereichsauslösers für den Speicherpool WINPOOL1 löschen.

```
delete spacetrigger stg stgpool=winpool1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SPACETRIGGER

Befehl	Beschreibung
DEFINE SPACETRIGGER	Definiert einen Speicherbereichsauslöser zum Erweitern des Speicherbereichs für einen Speicherpool.

Befehl	Beschreibung
QUERY SPACETRIGGER	Zeigt Informationen zu einem Speicherbereichsauslöser für den Speicherpool an.
UPDATE SPACETRIGGER	Ändert Attribute des Speicherbereichsauslösers für den Speicherpool.

DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)

Mit diesem Befehl können Sie einen vorhandenen Schwellenwert für die Statusüberwachung löschen.

Mit Statusüberwachungsschwellenwerten werden die definierten Bedingungen mit den Serverabfragen für die Statusüberwachung verglichen und die Ergebnisse in die Statusüberwachungstabelle eingefügt.

Es können mehrere Schwellenwerte für eine Aktivität definiert werden. Sie können beispielsweise einen Schwellenwert erstellen, der einen Warnstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 80 % ist. Sie können dann einen anderen Schwellenwert erstellen, der einen Fehlerstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 90 % ist.

Anmerkung: Wenn bereits ein Schwellenwert für eine Bedingung EXISTS definiert ist, können Sie keinen anderen Schwellenwert mit einem der anderen Bedingungstypen definieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete STAtusthreshold--Schwellenwertname-------------------><
```

Parameter

Schwellenwertname (Erforderlich)
Gibt den Schwellenwertnamen an, der gelöscht werden soll.

Einen vorhandenen Statusschwellenwert löschen

Mit dem folgenden Befehl einen vorhandenen Statusschwellenwert löschen:

```
delete statusthreshold avgstgpl
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE STATUSTHRESHOLD

Befehl	Beschreibung
DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)	Definiert einen Schwellenwert für die Statusüberwachung.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)	Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)	Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.

DELETE STGPOOL (Speicherpool löschen)

Mit diesem Befehl kann ein Speicherpool gelöscht werden. Um einen Speicherpool zu löschen, müssen zuerst alle Datenträger gelöscht werden, die dem Speicherpool zugeordnet sind.

Ein Speicherpool, der als nächster Speicherpool für einen anderen Speicherpool angegeben ist, kann nicht gelöscht werden. Weitere Informationen zur Speicherpoolhierarchie befinden sich unter dem Parameter NEXTSTGPOOL im Befehl DEFINE STGPOOL.

Einschränkungen:

- Löschen Sie für Containerspeicherpools alle Speicherpoolverzeichnisse, bevor Sie den Speicherpool löschen.
- Es darf kein Speicherpool gelöscht werden, der als Zielort für eine Verwaltungsklasse oder eine Kopiengruppe in der aktiven Maßnahmengruppe angegeben ist. Client-Operationen könnten fehlschlagen.
- Wird ein Kopienspeicherpool gelöscht, der zuvor in der Definition eines primären Speicherpools enthalten war (speziell in der COPYSTGPOOLS-Liste), müssen Sie den Kopienspeicherpool vor dem Löschen aus der Liste entfernen. Andernfalls schlägt der Befehl DELETE STGPOOL fehl, bis alle Verweise auf diesen Kopienpool entfernt werden. Entfernen Sie für jeden primären Speicherpool mit einem Verweis auf den zu löschenden Kopienspeicherpool den Verweis, indem Sie den Befehl UPDATE STGPOOL mit dem Parameter COPYSTGPOOLS mit allen vorherigen Kopienspeicherpools außer dem zu löschenden Kopienspeicherpool eingeben.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete STGpool--Poolname-------------------------------------><
```

Parameter

Poolname (Erforderlich)
Gibt den Speicherpool an, der gelöscht werden soll.

Beispiel: Einen Speicherpool löschen

Den Speicherpool POOLA löschen.

```
delete stgpool poola
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE STGPOOL

Befehl	Beschreibung
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DEFINE STGPOOLDIRECTORY	Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.
DELETE STGPOOLDIRECTORY	Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
QUERY STGPOOLDIRECTORY	Zeigt Informationen zu Speicherpoolverzeichnissen an.
AIX-BetriebssystemeWindows-BetriebssystemeSET DRMCOPYSTGPOOL	AIX-BetriebssystemeWindows-BetriebssystemeGibt an, dass Kopienspeicherpools von DRM verwaltet werden.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.
UPDATE STGPOOLDIRECTORY	Ändert die Attribute eines Speicherpoolverzeichnisses.

DELETE STGPOOLDIRECTORY (Speicherpoolverzeichnis löschen)

Mit diesem Befehl kann eine Definition für ein Speicherpoolverzeichnis gelöscht werden.

Möglicherweise möchten Sie ein Speicherpoolverzeichnis aus den folgenden Gründen löschen:

- Alter Speicher soll stillgelegt werden.
- Die lokale Platte soll nicht weiterverwendet werden, bevor Daten in die Cloud versetzt werden.

- Es besteht kein Bedarf mehr, die Daten in dem Speicherpoolverzeichnis aufzubewahren.

Einschränkungen:

- Sie können diesen Befehl nur ausgeben, wenn keine Container dem Speicherpoolverzeichnis zugeordnet sind. Geben Sie den Befehl QUERY CONTAINER aus, um zu bestimmen, ob dem Speicherpoolverzeichnis Container zugeordnet sind.
- Sollen Container aus einem Speicherpoolverzeichnis entfernt werden, müssen Sie den Befehl UPDATE STGPOOLDIRECTORY ausgeben und den Parameter ACCESS=DESTROYED angeben. Geben Sie dann den Befehl AUDIT CONTAINER aus und geben Sie den Parameter ACTION=REMOVEDAMAGED an. Überprüfen Sie, ob die Container entfernt wurden. Der Parameter ACTION=REMOVEDAMAGED entfernt die Informationen zum Bestand für die Objekte, die gesichert oder archiviert wurden. Sie sollten die Informationen zum Bestand nur dann entfernen, wenn Sie die Sicherungen nicht benötigen.

Falls ein Hardwarefehler oder ein Verlust des Verzeichnisses auftritt, finden Sie weitere Informationen in den Abschnitten über die Befehle AUDIT und REPAIR. Etwaige Reparaturen an der IBM Spectrum Protect-Umgebung sollten Sie vornehmen, bevor Sie das Speicherpoolverzeichnis löschen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete STGPOOLDIRectory--Poolname--Verzeichnis-------------><
```

Parameter

Poolname (Erforderlich)
: Gibt den Speicherpool an, der das zu löschende Verzeichnis enthält. Dieser Parameter ist erforderlich.

Verzeichnis (Erforderlich)
: Gibt das zu löschende Dateisystemverzeichnis des Speicherpools an. Dieser Parameter ist erforderlich.

Beispiel: Ein Speicherpoolverzeichnis aktualisieren, um es zum Löschen vorzubereiten

Das Speicherpoolverzeichnis mit dem Namen DIR1 im Speicherpool POOLA aktualisieren, um es als dauerhaft beschädigt zu markieren. Wenn ein Speicherpool als dauerhaft beschädigt markiert ist, kann er gelöscht werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
update stgpooldirectory poola /storage/dir1 access=destroyed
```

 Windows-Betriebssysteme

```
update stgpooldirectory poola e:\storage\dir1 access=destroyed
```

Beispiel: Ein Speicherpoolverzeichnis löschen

Das Speicherpoolverzeichnis mit dem Namen DIR1 im Speicherpool POOLA löschen.

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
delete stgpooldirectory poola /storage/dir1
```

 Windows-Betriebssysteme

```
delete stgpooldirectory poola e:\storage\dir1
```

Tabelle 1. Zugehörige Befehle für DELETE STGPOOLDIRECTORY

Befehl	Beschreibung
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DEFINE STGPOOLDIRECTORY	Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.
QUERY STGPOOLDIRECTORY	Zeigt Informationen zu Speicherpoolverzeichnissen an.
UPDATE STGPOOLDIRECTORY	Ändert die Attribute eines Speicherpoolverzeichnisses.
QUERY EXTENTUPDATES	Zeigt Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainerspeicherpools an.

DELETE SUBSCRIBER (Subskriptionen aus Konfigurationsmanagerdatenbank löschen)

Verwenden Sie diesen Befehl auf einem Konfigurationsmanager, um Subskriptionen für einen verwalteten Server aus der Datenbank des Konfigurationsmanagers zu löschen. Verwenden Sie diesen Befehl, wenn ein verwalteter Server nicht mehr vorhanden ist oder den Konfigurationsmanager nach dem Löschen einer Subskription nicht informieren kann.

Achtung: Diesen Befehl nur in seltenen Fällen verwenden, in denen die Datenbank des Konfigurationsmanagers einen Eintrag für eine Subskription enthält, der verwaltete Server aber nicht über eine solche Subskription verfügt. Diesen Befehl beispielsweise verwenden, wenn ein verwalteter Server nicht mehr vorhanden ist oder den Konfigurationsmanager nach dem Löschen einer Subskription nicht informieren kann.

Unter normalen Umständen den Befehl DELETE SUBSCRIPTION verwenden, um eine Subskription auf dem verwalteten Server zu löschen. Der verwaltete Server informiert den Konfigurationsmanager, der dann die Subskription aus seiner Datenbank löscht.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete SUBSCRIBer--Servername------------------------------><
```

Parameter

Servername (Erforderlich)
Gibt den Namen des verwalteten Servers an, dessen Subskriptionseinträge gelöscht werden sollen.

Beispiel: Subskriptionseinträge für einen bestimmten verwalteten Server löschen

Alle Subskriptionseinträge für den verwalteten Server DAN löschen.

```
delete subscriber dan
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SUBSCRIBER

Befehl	Beschreibung
DEFINE SUBSCRIPTION	Subskribiert einen verwalteten Server für ein Profil.
DELETE SUBSCRIPTION	Löscht eine angegebene Profilsubskription.
NOTIFY SUBSCRIBERS	Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.
QUERY SUBSCRIBER	Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.
QUERY SUBSCRIPTION	Zeigt Informationen über Profilsubskriptionen an.

DELETE SUBSCRIPTION (Profilsubskription löschen)

Mit diesem Befehl kann auf einem verwalteten Server eine Profilsubskription gelöscht werden. Außerdem können auf dem verwalteten Server alle Objekte gelöscht werden, die dem Profil zugeordnet sind.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DELete SUBSCRIPtion--Profilname------------------------------>

   .-DISCARDobjects--=--No------.
>--+----------------------------+-----------------------------><
   '-DISCARDobjects--=--+-No--+-'
```

```
'-Yes-'
```

Parameter

Profilname (Erforderlich)
: Gibt den Namen des Profils an, für das die Subskription gelöscht werden soll.

DISCARDobjects
: Gibt an, ob Objekte, die dem Profil zugeordnet sind, auf dem verwalteten Server gelöscht werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

  No
  : Gibt an, daß die Objekte nicht gelöscht werden sollen.

  Yes
  : Gibt an, daß die Objekte gelöscht werden sollen, es sei denn, sie sind einem anderen Profil zugeordnet, für das eine Subskription definiert ist.

Beispiel: Eine Profilsubskription löschen

Eine Subskription für das Profil ALPHA und seine zugeordneten Objekte aus einem verwalteten Server löschen.

```
delete subscription alpha discardobjects=yes
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE SUBSCRIPTION

Befehl	Beschreibung
DEFINE SUBSCRIPTION	Subskribiert einen verwalteten Server für ein Profil.
DELETE SUBSCRIBER	Löscht veraltete Subskriptionen verwalteter Server.
NOTIFY SUBSCRIBERS	Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.
QUERY SUBSCRIBER	Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.
QUERY SUBSCRIPTION	Zeigt Informationen über Profilsubskriptionen an.

DELETE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs löschen)

Verwenden Sie diesen Befehl, um eine Definition für die Zuordnung des virtuellen Dateibereichs zu löschen. Virtuelle Dateibereiche, die Daten enthalten, können nur gelöscht werden, wenn zuerst der Befehl DELETE FILESPACE verwendet wird.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Domäne, der der NAS-Knoten zugeordnet ist

Syntax

```
>>-DELete VIRTUALFSmapping  -Knotenname-------------------------->

>--Name_des_virtuellen_Dateibereichs--------------------------><
```

Parameter

Knotenname (Erforderlich)
: Gibt den NAS-Knoten an, auf dem sich das Dateisystem und der Pfad befinden. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

Name_des_virtuellen_Dateibereichs (Erforderlich)
: Gibt den Namen der zu löschenden Definition für die Zuordnung des virtuellen Dateibereichs an. Platzhalterzeichen sind zulässig.

Beispiel: Eine Zuordnung des virtuellen Dateibereichs löschen

Die Definition /mikeshomedir für die Zuordnung des virtuellen Dateibereichs für den NAS-Knoten NAS1 löschen.

```
delete virtualfsmapping nas1 /mikeshomedir
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE VIRTUALFSMAPPING

Befehl	Beschreibung
DEFINE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs definieren.
QUERY VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs abfragen.
UPDATE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs aktualisieren.

DELETE VOLHISTORY (Protokolldaten sequenzieller Datenträger löschen)

Mit diesem Befehl können Sätze in der Protokolldatei für Datenträger gelöscht werden, die nicht mehr benötigt werden (beispielsweise Sätze für veraltete Datenbanksicherungsdatenträger).

Werden Sätze für Datenträger gelöscht, die sich nicht in Speicherpools befinden (beispielsweise Datenbanksicherungs- oder Exportdatenträger), werden die Datenträger auch dann in den Arbeitsdatenträgerstatus zurückversetzt, wenn IBM Spectrum Protect die Datenträger als private Datenträger angefordert hat. Arbeitsdatenträger mit dem Einheitentyp FILE werden gelöscht. Werden die Sätze für Speicherpooldatenträger gelöscht, verbleiben die Datenträger in der IBM Spectrum Protect-Datenbank. Werden Sätze für Wiederherstellungsplandateiobjekte aus einem Quellenserver gelöscht, werden die Objekte auf dem Zielserver zum Löschen markiert.
Einschränkung: Verwenden Sie nicht den Befehl DELETE VOLHISTORY, um Informationen zu Sicherungsgruppendatenträgern aus der Protokolldatei für Datenträger zu löschen. Verwenden Sie zu diesem Zweck den Befehl DELETE BACKUPSET.

Benutzer von DRM müssen sicherstellen, dass der Verfall von Datenbanksicherungen über den Befehl SET DRMDBBACKUPEXPIREDAYS und nicht über diesen Befehl DELETE VOLHISTORY gesteuert wird. Verwenden Sie den Befehl DELETE VOLHISTORY, um einen Satz des Datenträgers zu entfernen. Dadurch können Datenträger verloren gehen, die über den Befehl MOVE DRMEDIA verwaltet wurden. Verwenden Sie den Befehl SET DRMDBBACKUPEXPIREDAYS, um den automatischen Verfall von DRM-Datenbanksicherungsdatenträgern zu verwalten.

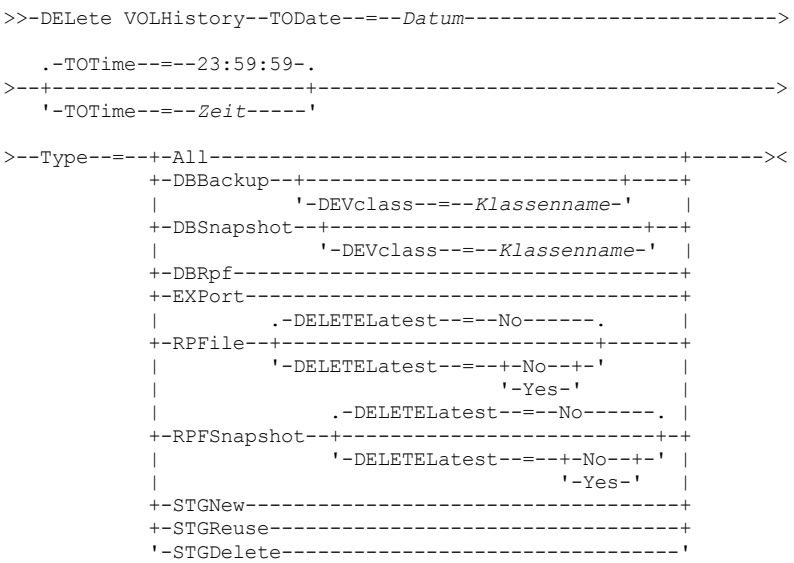
Tipps:

- Datenträger für die neueste Datenbanksicherungsserie werden nicht gelöscht.
- Vorhandene Protokolldateien für Datenträger werden mit diesem Befehl nicht automatisch aktualisiert.
- Mit dem Befehl DEFINE SCHEDULE können Datenträgerprotokollsätze in regelmäßigen Abständen gelöscht werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

TODate (Erforderlich)

Gibt das Datum an, das für die Auswahl der Protokolldaten sequenzieller Datenträger, die gelöscht sollen, verwendet werden soll. Sie können nur die Sätze mit einem Datum bis zu dem angegebenen Datum einschließlich löschen. Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	01/23/1999
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage oder -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–30 oder –30. Um Sätze zu löschen, die mindestens 30 Tage alt sind, kann TODAY-30 oder einfach -30 angegeben werden.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

TOTime

Gibt an, dass Sätze gelöscht werden sollen, die zu oder vor dieser Zeit am angegebenen Datum erstellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist das Ende des Tages (23:59:59). Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Datum	12:30:22
NOW	Die aktuelle Uhrzeit am angegebenen Datum	NOW
NOW+HH:MM oder +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Datum	NOW+03:00 oder +03:00. Wird der Befehl DELETE VOLHISTORY um 9:00 Uhr mit TOTIME=NOW+03:00 oder TOTIME=+03:00 ausgegeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 Uhr oder früher an dem angegebenen Datum.
NOW-HH:MM oder -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Datum	NOW-03:30 oder -03:30. Wird der Befehl DELETE VOLHISTORY um 9:00 Uhr mit TOTIME=NOW-3:30 oder TOTIME=-3:30 ausgegeben, löscht IBM Spectrum Protect Sätze mit der Uhrzeit 5:30 Uhr oder früher an dem angegebenen Datum.

Type (Erforderlich)

Gibt den Typt der Sätze an (die auch den Datums- und Zeitkriterien entsprechen), die aus der Protokolldatei für Datenträger gelöscht werden sollen. Gültige Werte:

All

Gibt an, dass alle Sätze gelöscht werden sollen.

Einschränkung: Mit dem Befehl DELETE VOLHISTORY werden keine Sätze von fernen Datenträgern gelöscht.

DBBackup

Gibt an, dass nur Sätze gelöscht werden, die Informationen zu Datenträgern enthalten, die für Gesamt- und Teilsicherungen der Datenbank verwendet werden, d. h. Datenträger mit den Datenträgertypen BACKUPFULL und BACKUPINCR, und die die angegebenen Datums- und Zeitkriterien erfüllen. Die Sätze aus der letzten Gesamt- und Teilsicherungsserie der Datenbank werden nicht gelöscht.

DEVclass=Klassenname

Gibt den Namen der Einheitenklasse an, die zum Erstellen der Datenbanksicherungen verwendet wurde. Dieser wahlfreie Parameter kann verwendet werden, um Datenbanksicherungen zu löschen, die mithilfe einer Einheitenklasse für virtuelle Datenträger für die Übertragung zwischen Servern erstellt werden. Der Typ der Einheitenklasse muss SERVER lauten. Mit diesem Parameter können nur Datenträgerprotokolleinträge des Typs BACKUPFULL, BACKUPINCR oder DBSNAPSHOT gelöscht werden.

Ein Datenträger für Gesamt- oder Teilsicherungen der Datenbank kann zum Löschen ausgewählt werden, wenn alle folgenden Bedingungen zutreffen:

- Die Einheitenklasse, die zum Erstellen des Datenbanksicherungsdatenträgers verwendet wurde, stimmt mit der angegebenen Einheitenklasse überein.
- Der Datenträger wurde an oder vor dem angegebenen Datum und zu oder vor der angegebenen Uhrzeit erstellt.
- Der Datenträger ist nicht Teil der letzten Gesamt- und Teilsicherungsserie der Datenbank.
- Der Datenträger ist nicht Teil einer Gesamt- und Teilsicherungsserie mit einer Datenbankteilsicherung, die nach dem angegebenen Datum und nach der angegebenen Zeit erstellt wurde.

DBSnapshot
Gibt an, dass nur Sätze gelöscht werden, die Informationen zu Datenträgern enthalten, die für Datenbankmomentaufnahmesicherungen verwendet werden und die die angegebenen Datums- und Zeitkriterien erfüllen. Sätze, die sich auf die letzte Datenbankmomentaufnahmesicherung beziehen, werden nicht gelöscht.

DEVclass=Klassenname
Gibt den Namen der Einheitenklasse an, die zum Erstellen der Datenbanksicherungen verwendet wurde. Dieser wahlfreie Parameter kann verwendet werden, um Datenbanksicherungen zu löschen, die mithilfe einer Einheitenklasse für virtuelle Datenträger für die Übertragung zwischen Servern erstellt werden. Der Typ der Einheitenklasse muss SERVER lauten. Mit diesem Parameter können nur Datenträgerprotokolleinträge des Typs BACKUPFULL, BACKUPINCR oder DBSNAPSHOT gelöscht werden.
Ein Datenträger für Datenbankmomentaufnahmesicherungen kann zum Löschen ausgewählt werden, wenn alle folgenden Bedingungen zutreffen:

- Die Einheitenklasse, die zum Erstellen des Datenbanksicherungsdatenträgers verwendet wird, stimmt mit der angegebenen Einheitenklasse überein
- Der Datenträger wurde an oder vor dem angegebenen Datum und zu oder vor der angegebenen Uhrzeit erstellt
- Der Datenträger ist nicht Teil der letzten Datenbankmomentaufnahmesicherungsserie

DBRpf
Gibt an, dass nur Sätze gelöscht werden, die Informationen über Datenträger mit Gesamt- und Teilsicherungen der Datenbank und über Datenträger mit Wiederherstellungsplandateien enthalten.

EXPort
Gibt an, dass nur Sätze gelöscht werden, die Informationen über Exportdatenträger enthalten.

RPFile
Gibt an, dass nur Sätze gelöscht werden, die Informationen über Wiederherstellungsplandateiobjekte enthalten, die auf einem Zielserver gespeichert sind, und die die angegebenen Datums- und Zeitkriterien erfüllen.

DELETELatest
Gibt an, ob die letzte Wiederherstellungsplandatei zum Löschen ausgewählt werden kann. Dieser wahlfreie Parameter kann verwendet werden, um die letzten Wiederherstellungsplandateien zu löschen, die mithilfe einer Einheitenklasse für virtuelle Datenträger für die Übertragung zwischen Servern erstellt wurden.

Mit diesem Parameter können nur Datenträgerprotokolleinträge des Typs RPFILE gelöscht werden (beispielsweise die Wiederherstellungsplandateien, die mit dem Parameter DEVCLASS im Befehl PREPARE erstellt wurden). Wird dieser Parameter nicht angegeben, werden die letzten RPFILE-Einträge nicht gelöscht.

No
Gibt an, dass die letzte RPFILE-Datei nicht gelöscht wird.

Yes
Gibt an, dass die letzte RPFILE-Datei gelöscht wird, wenn sie den angegebenen Datums- und Zeitkriterien entspricht.

RPFSnapshot
Gibt an, dass nur Sätze gelöscht werden, die Informationen zu Wiederherstellungsplandateiobjekten enthalten, die für Datenbankmomentaufnahmesicherungen erstellt wurden, die auf einem Zielserver gespeichert sind und die die angegebenen Datums- und Zeitkriterien erfüllen. Die letzte RPFSNAPSHOT-Datei wird nicht gelöscht, es sei denn, sie erfüllt die angegebenen Datums- und Zeitkriterien und der Parameter DELETE ist auf Yes gesetzt.

DELETELatest
Gibt an, ob die letzte Wiederherstellungsplandatei zum Löschen ausgewählt werden kann. Dieser wahlfreie Parameter kann verwendet werden, um die letzten Wiederherstellungsplandateien zu löschen, die mithilfe einer Einheitenklasse für virtuelle Datenträger für die Übertragung zwischen Servern erstellt wurden.

Mit diesem Parameter können nur Datenträgerprotokolleinträge des Typs RPFSNAPSHOT gelöscht werden (beispielsweise die Wiederherstellungsplandateien, die mit dem Parameter DEVCLASS im Befehl PREPARE erstellt wurden). Wird dieser Parameter nicht angegeben, werden die letzten RPFSNAPSHOT-Einträge nicht gelöscht.

No
Gibt an, dass die letzte RPFSNAPSHOT-Datei nicht gelöscht wird.

Yes
Gibt an, dass die letzte RPFSNAPSHOT-Datei gelöscht wird, wenn sie den angegebenen Datums- und Zeitkriterien entspricht.

STGNew
: Gibt an, dass nur Sätze gelöscht werden, die Informationen über neue Speicherdatenträger mit sequenziellem Zugriff enthalten.

STGReuse
: Gibt an, dass nur Sätze gelöscht werden, die Informationen über wiederverwendete sequenzielle Datenträger aus dem Speicherpool enthalten.

STGDelete
: Gibt an, dass nur Sätze gelöscht werden, die Informationen über gelöschte sequenzielle Datenträger aus dem Speicherpool enthalten.

Beispiel: Informationen zur Wiederherstellungsplandatei löschen

Alle Informationen zu Wiederherstellungsplandateien löschen, die am oder vor dem 03/28/2016 erstellt wurden.

```
delete volhistory type=rpfile todate=03/28/2016
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE VOLHISTORY

Befehl	Beschreibung
BACKUP VOLHISTORY	Zeichnet Datenträger-History-Daten in externen Dateien auf.
DEFINE SCHEDULE	Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.
DELETE VOLUME	Löscht einen Datenträger aus einem Speicherpool.
EXPIRE INVENTORY	Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY RPFILE	Zeigt Informationen über Wiederherstellungsplandateien an.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.
SET DRMRPFEXPIREDAYS	Definiert Verfallskriterien für Wiederherstellungsplandateien.
SET DRMDBBACKUPEXPIREDAYS	Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.

DELETE VOLUME (Speicherpooldatenträger löschen)

Mit diesem Befehl können ein Datenträger aus dem Speicherpool und wahlweise die Dateien in dem Datenträger gelöscht werden.

Enthält der Datenträger Daten, muß einer der folgenden Schritte ausgeführt werden, um den Datenträger zu löschen:

- Vor dem Löschen des Datenträgers den Befehl MOVE DATA verwenden, um alle Dateien auf einen anderen Datenträger zu versetzen.
- Das Löschen aller Dateien auf dem Datenträger explizit anfordern, wenn der Datenträger gelöscht wird (durch Angabe von DISCARDDATA=YES).

Werden mehrere Datenträger gelöscht, die Datenträger einzeln löschen. Werden mehrere Datenträger gleichzeitig gelöscht, kann dies negative Auswirkungen auf die Server-Leistung haben.

Speicherpooldatenträger können nicht gelöscht werden, wenn sie gerade verwendet werden. Ein Datenträger kann beispielsweise nicht gelöscht werden, wenn ein Benutzer eine Datei zurückschreibt oder abruft, die sich auf dem Datenträger befindet, wenn der Server Informationen auf den Datenträger schreibt oder wenn ein Wiederherstellungsprozess den Datenträger verwendet.

Wenn Sie den Befehl DELETE VOLUME ausgeben, werden Datenträgerinformationen aus der IBM Spectrum Protect-Datenbank gelöscht. Die physischen Dateien, die mit dem Befehl DEFINE VOLUME zugeordnet wurden, werden jedoch nicht aus dem Dateibereich entfernt.

Wird dieser Befehl auf einen WORM-Datenträger (WORM = Write Once, Read Many) angewendet, kehrt der Datenträger in den Arbeitsdatenträgerstatus zurück, wenn er noch über Speicherbereich verfügt, in den Daten geschrieben werden können. Daten auf WORM-Datenträgern, einschließlich gelöschter und verfallener Daten, können nicht überschrieben werden. Daher können Daten nur in Speicherbereich geschrieben werden, der keine aktuellen, gelöschten oder verfallenen Daten enthält. Verfügt ein WORM-Datenträger über keinen Speicherbereich mehr, in den Daten geschrieben werden können, verbleibt der Datenträger im privaten Status. Soll der Datenträger aus dem Kassettenarchiv entfernt werden, müssen Sie den Befehl CHECKOUT LIBVOLUME verwenden.

Mit dem Befehl DELETE VOLUME wird der Datenträgerbestand im Kassettenarchiv des Servers automatisch für sequenzielle Datenträger aktualisiert, wenn der Datenträger in den Status "Arbeitsdatenträger" zurückgesetzt wird, sobald der Datenträger leer wird. Um zu bestimmen, ob ein Datenträger in den Status "Arbeitsdatenträger" zurückgesetzt wird, geben Sie den Befehl QUERY VOLUME aus und überprüfen Sie die

Ausgabe. Wenn der Wert für das Attribut "Arbeitsdatenträger?" "Yes" lautet, wird der Datenträgerbestand im Kassettenarchiv des Servers automatisch aktualisiert.

Lautet der Wert "No", können Sie mit dem Befehl UPDATE LIBVOLUME den Status als Arbeitsdatenträger angeben. Es wird empfohlen, den Befehl UPDATE LIBVOLUME auszugeben, nachdem der Befehl DELETE VOLUME ausgegeben wurde.

Der Versuch, den Befehl DELETE VOLUME zum Löschen von WORM-FILE-Datenträgern in einem Speicherpool mit RECLAMATIONTYPE=SNAPLOCK zu verwenden, schlägt mit einer Fehlernachricht fehl. Das Löschen von leeren WORM-FILE-Datenträgern wird nur durch den Wiederherstellungsprozess ausgeführt.

Wenn Sie den Befehl DELETE VOLUME für einen Datenträger in einem Speicherpool ausgeben, der einen Wert größer als 0 für den Parameter SHRED hat, wird der Datenträger bis zur Ausführung des Schredderns in den Wartestatus versetzt. Das Schreddern ist erforderlich, um das Löschen abzuschließen, auch wenn der Datenträger leer ist.

Wenn Sie den Befehl DELETE VOLUME für einen Datenträger in einem Speicherpool ausgeben, der für die Deduplizierung von Daten definiert ist, löscht der Server alle Objekte, die auf Daten auf diesem Datenträger verweisen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich, in dem der Datenträger definiert ist.

Syntax

```
>>-DELete Volume--Datenträgername------------------------------>

   .-DISCARDdata--=--No------.  .-Wait--=--No------.
>--+-------------------------+--+------------------+-----------><
   '-DISCARDdata--=--+-No--+-'  '-Wait--=--+-No--+-'
                     '-Yes-'               '-Yes-'
```

Parameter

Datenträgername (Erforderlich)
: Gibt den Namen des Datenträgers an, der gelöscht werden soll.

DISCARDdata
: Gibt an, ob die auf dem Datenträger gespeicherten Dateien gelöscht werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.
Gültige Werte:

  No
  : Gibt an, daß die auf dem Datenträger gespeicherten Dateien nicht gelöscht werden. Enthält der Datenträger Dateien, wird der Datenträger nicht gelöscht.

  Yes
  : Gibt an, daß alle auf dem Datenträger gespeicherten Dateien gelöscht werden. Der Server muß den Datenträger für diese Art des Löschens nicht laden.
  Hinweis:

    1. Der Server löscht keine Archivierungsdateien, für die angegeben wurde, dass sie nicht gelöscht werden dürfen.
    2. Ist der Aufbewahrungsschutz für Archivierung aktiviert, löscht der Server nur Archivierungsdateien, deren Aufbewahrungszeitraum abgelaufen ist.

  Ist der Datenträger, der gelöscht wird, ein Datenträger für den primären Speicherpool, überprüft der Server, ob ein Kopienspeicherpool Kopien von Dateien enthält, die gelöscht werden. Werden Dateien gelöscht, die auf einem Datenträger für den primären Speicherpool gespeichert sind, werden alle Kopien dieser Dateien in Kopienspeicherpools ebenfalls gelöscht.

  Wird ein Plattendatenträger in einem primären Speicherpool gelöscht, löscht der Befehl auch alle Dateien, die Cache-Kopien sind (Kopien von Dateien, die in den nächsten Speicherpool umgelagert wurden). Beim Löschen der Cache-Kopien von Dateien werden nicht die Dateien gelöscht, die bereits in Kopienspeicherpools umgelagert oder gesichert wurden. Es sind nur die Cache-Kopien der Dateien betroffen.

  Ist der Datenträger, der gelöscht wird, ein Kopienspeicherpooldatenträger, werden nur Dateien auf dem Kopienpooldatenträger gelöscht. Die Dateien im primären Speicherpool sind nicht betroffen.

  Der Befehl DELETE VOLUME darf nicht mit DISCARDDATA=YES verwendet werden, wenn ein Zurückschreibungsprozess (RESTORE STGPOOL oder RESTORE VOLUME) aktiv ist. Durch den Befehl DELETE VOLUME könnte die Zurückschreibung unvollständig sein.

  Wird der Befehl DELETE VOLUME während der Verarbeitung abgebrochen oder tritt ein Systemfehler auf, verbleiben einige Dateien möglicherweise auf dem Datenträger. Derselbe Datenträger kann erneut gelöscht werden, damit der Server die verbleibenden Dateien und dann den Datenträger löscht.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter hat nur dann Auswirkungen auf die Verarbeitung, wenn auch das Löschen aller Daten auf dem Datenträger angefordert wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

No
: Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

  Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Yes
: Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist. Hinweis: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

Beispiel: Einen Speicherpooldatenträger löschen

Datenträger aus dem Speicherpool stgvol.1 aus dem Speicherpool FILEPOOL löschen.

```
delete volume stgvol.1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DELETE VOLUME

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
MOVE DATA	Versetzt Daten aus einem angegebenen Speicherpooldatenträger in einen anderen Speicherpooldatenträger.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY CONTENT	Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY VOLUME	Zeigt Informationen über Speicherpooldatenträger an.
UPDATE VOLUME	Aktualisiert die Attribute der Speicherpooldatenträger.

DISABLE-Befehle

Mit den DISABLE-Befehlen können Sie einige durch den Server ausgeführte Operationstypen verhindern.

- DISABLE EVENTS (Ereignisse für Ereignisprotokollierung inaktivieren)
- DISABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server verhindern)
- DISABLE SESSIONS (Verhindern, dass neue Sitzungen auf IBM Spectrum Protect zugreifen)

DISABLE EVENTS (Ereignisse für Ereignisprotokollierung inaktivieren)

Mit diesem Befehl kann die Verarbeitung eines oder mehrerer Ereignisse inaktiviert werden. Geben Sie einen Empfänger an, der auf keiner Plattform unterstützt wird, oder geben Sie ein ungültiges Ereignis oder einen ungültigen Namen an, gibt IBM Spectrum Protect eine Fehlernachricht aus. Alle gültigen Empfänger, Ereignisse oder Namen, die angegeben wurden, sind jedoch noch aktiviert.

Tipp: Nachrichten der Kategorie SEVERE und Nachricht ANR9999D können wertvolle Diagnoseinformationen liefern, wenn schwerwiegende Server-Probleme vorliegen. Aus diesem Grund sollten diese Nachrichten nicht inaktiviert werden.
Einschränkung:

- Bestimmte Nachrichten erscheinen an der Konsole, auch wenn sie inaktiviert wurden. Hierzu gehören einige Nachrichten, die während des Systemstarts und des Systemabschlusses des Servers ausgegeben werden, sowie Antworten auf Verwaltungsbefehle.
- Servernachrichten von dem Server, auf dem dieser Befehl ausgegeben wurde, können nicht für das Aktivitätenprotokoll inaktiviert werden.

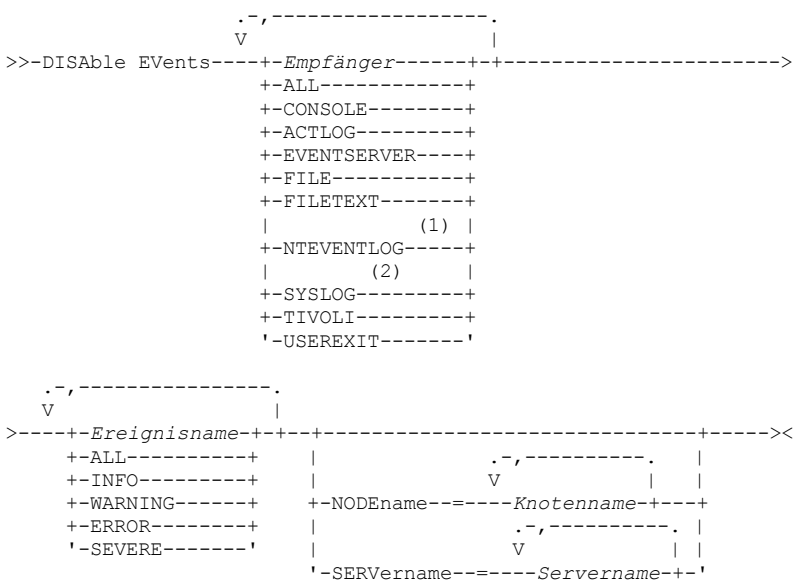
ANR1822I gibt an, daß die Ereignisprotokollierung für den angegebenen Empfänger beendet wird. Wird der Befehl DISABLE EVENTS ausgegeben, wird diese Nachricht auch dann für den Empfänger protokolliert, wenn es sich um ein Ereignis handelt, das inaktiviert wurde. Damit

wird bestätigt, dass die Ereignisprotokollierung für diesen Empfänger beendet wurde. Nachfolgende Nachrichten ANR1822I werden nicht für diesen Empfänger protokolliert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Anmerkungen:

1. NTEVENTLOG ist nur unter Windows verfügbar.
2. SYSLOG ist nur unter Linux verfügbar.

Parameter

Empfänger (Erforderlich)
: Gibt den Namen der Empfänger an, für die Ereignisse inaktiviert werden sollen. Mehrere Empfänger können angegeben werden, indem sie ohne Leerzeichen durch Kommas voneinander getrennt werden. Gültige Werte:

  ALL
  : Alle Empfänger, außer Server-Ereignisse im Aktivitätenprotokollempfänger (ACTLOG). Nur Client-Ereignisse können für den Aktivitätenprotokollempfänger inaktiviert werden.

  CONSOLE
  : Die Standardserverkonsole als Empfänger.

  ACTLOG
  : Das Aktivitätenprotokoll als Empfänger. Es können nur Client-Ereignisse, keine Server-Ereignisse, für das Aktivitätenprotokoll inaktiviert werden.

  EVENTSERVER
  : Der Ereignis-Server als Empfänger.

  FILE
  : Eine Benutzerdatei als Empfänger. Jedes protokollierte Ereignis ist ein Satz in der Datei.Die Sätze können von Personen nicht einfach gelesen werden.

  FILETEXT
  : Eine Benutzerdatei als Empfänger. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

  NTEVENTLOG
  : Das Windows-Anwendungsprotokoll als Empfänger.

  Linux-BetriebssystemeSYSLOG
  : Linux-BetriebssystemeSchreibt Nachrichten direkt in das Systemprotokoll unter Linux.

  TIVOLI
  : Tivoli Enterprise Console (TEC) als Empfänger.

  USEREXIT
  : Ein benutzerdefiniertes Programm als Empfänger. Der Server schreibt Informationen in das Programm.

Ereignisse (Erforderlich)

Gibt die Ereignisse an, die inaktiviert werden sollen. Es können mehrere Ereignisse angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Gültige Werte:

ALL
: Alle Ereignisse.

Ereignisname
: Eine vierstellige Nachrichtennummer, die bei Server-Ereignissen mit den Buchstaben `ANR` beginnt, und bei Client-Ereignissen mit den Buchstaben `ANE`. Gültige Bereiche sind ANR0001 bis ANR9999 und ANE4000 bis ANE4999. Den Parameter NODENAMES angeben, wenn Clientereignisse für übereinstimmende Knoten inaktiviert werden sollen. Den Parameter SERVERNAME angeben, wenn Serverereignisse für übereinstimmende Server inaktiviert werden sollen.
Nur für den TIVOLI-Ereignisempfänger können die folgenden Ereignisnamen für die IBM Spectrum Protect-Anwendungsclients angegeben werden:

IBM Spectrum Protect-Anwendungsclient	Präfix	Bereich
Data Protection for Microsoft Exchange Server	ACN	3500–3649
Data Protection for Lotus Domino	ACD	5200–5299
Data Protection for Oracle	ANS	500–599
Data Protection for Informix	ANS	600–699
Data Protection for Microsoft SQL Server	ACO	3000–3999

Hinweis: Bei Angabe von ALL werden diese Nachrichten inaktiviert. Die Optionen INFO, WARNING, ERROR und SEVERE haben jedoch keine Auswirkungen auf die Nachrichten.

Bewertungskategorien
: Wenn die Ereignisliste eine Bewertungskategorie enthält, werden alle Ereignisse mit dieser Bewertung für die angegebenen Knoten inaktiviert. Die Nachrichtenarten sind:

  INFO
  : Informationsnachrichten (Art I).

  WARNING
  : Warnungen (Art W).

  ERROR
  : Fehlernachrichten (Art E).

  SEVERE
  : Schwerwiegende Fehlernachrichten (Art S).

NODEname
: Gibt die Knotennamen an, für die Ereignisse inaktiviert werden sollen. Es können Platzhalterzeichen (*) verwendet werden, um alle Knoten anzugeben. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, werden die Ereignisse für den Server inaktiviert, auf dem dieser Befehl ausgeführt wird.

SERVername
: Gibt die Server-Namen an, für die Ereignisse inaktiviert werden sollen. Es können Platzhalterzeichen (*) verwendet werden, um alle anderen Server anzugeben, auf denen dieser Befehl nicht ausgeführt wird. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, werden die Ereignisse für den Server inaktiviert, auf dem dieser Befehl ausgeführt wird.

Beispiel: Bestimmte Kategorien von Ereignissen inaktivieren

Alle Clientereignisse in den Kategorien INFO und WARNING für das Aktivitätenprotokoll und die Konsole für alle Knoten inaktivieren.

```
disable events actlog,console
info,warning nodename=*
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DISABLE EVENTS

Befehl	Beschreibung
BEGIN EVENTLOGGING	Startet das Ereignisprotokoll für einen bestimmten Empfänger.
ENABLE EVENTS	Aktiviert bestimmte Ereignisse für Empfänger.
END EVENTLOGGING	Beendet das Ereignisprotokoll für einen bestimmten Empfänger.
QUERY ENABLED	Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an.
QUERY EVENTRULES	Zeigt Informationen über Regeln für Server- und Clientereignisse an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

DISABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server verhindern)

Mit diesem Befehl kann verhindert werden, dass ein Quellenreplikationsserver neue Replikationsprozesse startet.

Mit diesem Befehl werden keine aktiven Replikationsprozesse gestoppt. Aktive Replikationsprozesse werden fortgesetzt, bis sie abgeschlossen sind oder ohne Abschluss beendet werden. Verwenden Sie diesen Befehl und den Befehl ENABLE REPLICATION, um die Replikationsverarbeitung zu steuern.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-DISAble REPLication----------------------------------------><
```

Parameter

Keine.

Beispiel: Replikationsverarbeitung inaktivieren

Die Replikationsverarbeitung auf einem Quellenreplikationsserver inaktivieren.

```
disable replication
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DISABLE REPLICATION

Befehl	Beschreibung
CANCEL REPLICATION	Bricht Knotenreplikationsprozesse ab.
DISABLE SESSIONS	Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden.
ENABLE REPLICATION	Ermöglicht die Verarbeitung abgehender Replikation auf einem Server.
ENABLE SESSIONS	Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.

DISABLE SESSIONS (Verhindern, dass neue Sitzungen auf IBM Spectrum Protect zugreifen)

Verwenden Sie diesen Befehl, um zu verhindern, dass neue Sitzungen auf IBM Spectrum Protect zugreifen. Aktive Sitzungen werden abgeschlossen. Für einen bestimmten Server können Sie angeben, ob eingehende Sitzungen und/oder abgehende Sitzungen inaktiviert werden sollen.

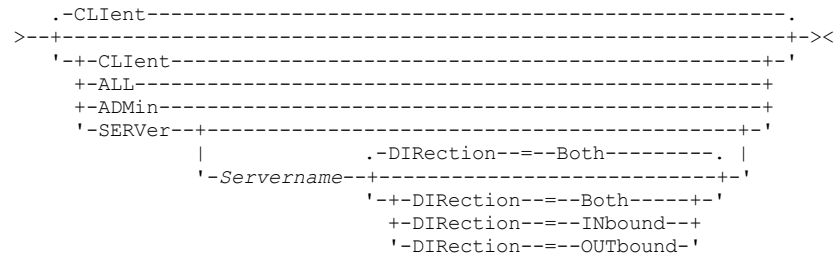
Serverprozesse, wie beispielsweise die Umlagerung und Wiederherstellung, sind nicht betroffen, wenn Sie den Befehl DISABLE SESSIONS ausgeben.

Berechtigungsklasse

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

Syntax

```
>>-DISAble SESSions---------------------------------------------->
```



Parameter

Gibt den Typ der Sitzung an, der inaktiviert werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT. Sie können einen der folgenden Werte angeben:

CLIent
: Inaktiviert nur Sicherungs- und Archivierungsclientsitzungen.

ALL
: Inaktiviert alle Sitzungstypen.

ADMin
: Inaktiviert nur Verwaltungssitzungen.

SERVer
: Inaktiviert nur Sitzungen zwischen Servern. Es werden nur die folgenden Typen von Sitzungen inaktiviert:

  - Ereignisprotokollierung zwischen Servern
  - Unternehmensverwaltung
  - Serverregistrierung
  - LAN-unabhängig: Speicheragent - Server
  - Virtuelle Datenträger
  - Knotenreplikation

  Sie können auch angeben, ob eingehende Sitzungen und/oder abgehende Sitzungen für einen bestimmten Server inaktiviert werden sollen.

  Servername
  : Gibt den Namen eines Servers an, dessen Sitzungen inaktiviert werden sollen. Dieser Parameter ist wahlfrei. Wenn Sie diesen Parameter nicht angeben, werden neue Sitzungen mit anderen Servern nicht gestartet. Aktive Sitzungen werden nicht abgebrochen.

    DIRection
    : Gibt an, ob eingehende Sitzungen und/oder abgehende Sitzungen inaktiviert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist BOTH. Die folgenden Werte sind gültig:

      Both
      : Gibt an, dass eingehende Sitzungen vom angegebenen Server und abgehende Sitzungen zum angegebenen Server inaktiviert werden.

      INbound
      : Gibt an, dass nur eingehende Sitzungen vom angegebenen Server inaktiviert werden.

      OUTbound
      : Gibt an, dass nur abgehende Sitzungen zum angegebenen Server inaktiviert werden.

Beispiel: Neue Clientknotensicherungs- und -archivierungssitzungen auf dem Server verhindern

Den Zugriff neuer Client-Knotensitzungen auf den Server vorübergehend verhindern.

```
disable sessions
```

Beispiel: Alle neuen Sitzungen auf dem Server verhindern

Den Zugriff neuer Sitzungen auf den Server vorübergehend verhindern.

```
disable sessions all
```

Beispiel: Abgehende Sitzungen zu einem Server inaktivieren

Abgehende Sitzungen zu dem Server REPLSRV inaktivieren.

```
disable sessions server replsrv direction=outbound
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DISABLE SESSIONS

Befehl	Beschreibung
CANCEL SESSION	Bricht aktive Sitzungen mit dem Server ab.
DISABLE REPLICATION	Verhindert die Verarbeitung abgehender Replikation auf einem Server.
ENABLE SESSIONS	Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.
QUERY SESSION	Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

DISMOUNT-Befehl

Mit dem Befehl DISMOUNT kann ein Datenträger nach der Adresse der realen Einheit oder nach dem Datenträgernamen entladen werden.

- DISMOUNT VOLUME (Datenträger nach Datenträgernamen entladen)

DISPLAY OBJNAME (Vollständigen Objektnamen anzeigen)

Mit diesem Befehl kann IBM Spectrum Protect einen vollständigen Objektnamen anzeigen, wenn der in einer Nachricht oder in einer Abfrageausgabe angezeigte Name aufgrund der Länge abgekürzt wurde. Objektnamen, die sehr lang sind, sind über normale Betriebssystemfunktionen schwer anzuzeigen und zu verwenden. Der IBM Spectrum Protect-Server kürzt lange Namen ab und ordnet ihnen eine Token-ID zu, die verwendet werden kann, wenn der Objektpfadname 1024 Byte überschreitet. Die Token-ID wird in einer Zeichenfolge angezeigt, die IDs für den Knoten, den Dateibereich und den Objektnamen einschließt. Das Format ist: [TSMOBJ:*nID.fsID.objID*]. Bei Angabe mit dem Befehl DISPLAY OBJNAME kann die Token-ID verwendet werden, um den vollständigen Objektnamen anzuzeigen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-DISplay OBJname--Token-ID----------------------------------><
```

Parameter

Token-ID (Erforderlich)
: Gibt die im Tag [TSMOBJ:] zurückgemeldete ID an, wenn ein Objektname zu lang ist, um angezeigt werden zu können.

Beispiel: Den vollständigen Objektnamen einer Token-ID in einer Nachricht anzeigen

Angenommen, Sie empfangen die folgende Nachricht:

```
ANR9999D file.c(1999) Fehler bei der Bearbeitung von Datei [TSMOBJ:1.1.649498]
aufgrund fehlender Serverressourcen.
```

Den vollständigen Objektnamen für die Datei anzeigen, auf die in der Fehlernachricht verwiesen wird, indem die Token-ID im Befehl DISPLAY OBJNAME angegeben wird.

```
display obj 1.1.649498
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für DISPLAY OBJNAME

Befehl	Beschreibung
QUERY CONTENT	Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.

ENABLE-Befehle

Mit den ENABLE-Befehlen können Sie einige durch den Server ausgeführte Operationstypen zulassen.

- ENABLE EVENTS (Server- oder Clientereignisse zum Protokollieren aktivieren)
- ENABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server ermöglichen)
- ENABLE SESSIONS (Benutzeraktivität auf dem Server wiederaufnehmen)

ENABLE EVENTS (Server- oder Clientereignisse zum Protokollieren aktivieren)

Mit diesem Befehl kann die Verarbeitung eines oder mehrerer Ereignisse aktiviert werden. Geben Sie einen Empfänger an, der auf keiner Plattform unterstützt wird, oder geben Sie ein ungültiges Ereignis oder einen ungültigen Namen an, gibt IBM Spectrum Protect eine Fehlernachricht aus. Alle gültigen Empfänger, Ereignisse oder Namen, die angegeben wurden, sind jedoch noch aktiviert.

Einschränkung: Bestimmte Ereignisse, wie z. B. während des Starts oder des Systemabschlusses des Servers ausgegebene Nachrichten, werden automatisch an die Konsole weitergeleitet. Sie werden nicht an andere Empfänger weitergeleitet, auch wenn sie aktiviert sind.

Verwaltungsbefehle werden an den zurückgegeben, der den Befehl ausgegeben hat, und werden nur als nummerierte Ereignisse protokolliert. Diese nummerierten Ereignisse werden nicht an der Systemkonsole, sondern in anderen Empfängern protokolliert, einschließlich Verwaltungsbefehlszeilensitzungen, die im Konsolenmodus ausgeführt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

Anmerkungen:

1. NTEVENTLOG ist nur unter Windows verfügbar.
2. Dieser Parameter ist nur für das Linux-Betriebssystem verfügbar.

Parameter

Empfänger (Erforderlich)
: Gibt einen oder mehrere Empfänger an, für die aktivierte Ereignisse protokolliert werden sollen. Es können mehrere Empfänger angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Gültige Werte sind:

  ALL
  : Alle Empfänger.

  CONSOLE
  : Die Standardserverkonsole als Empfänger.

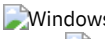
  ACTLOG
  : Das Serveraktivitätenprotokoll als Empfänger.

  EVENTSERVER
  : Der Ereignis-Server als Empfänger.

  FILE
  : Eine Benutzerdatei als Empfänger. Jedes protokollierte Ereignis ist ein Satz in der Datei.Die Sätze können von Personen nicht einfach gelesen werden.

  FILETEXT

Eine Benutzerdatei als Empfänger. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.


NTEVENTLOG


Das Windows-Anwendungsprotokoll als Empfänger.


SYSLOG


Gibt das Linux-Systemprotokoll als Empfänger an.

TIVOLI
: Tivoli Enterprise Console (TEC) als Empfänger.

USEREXIT
: Ein benutzerdefiniertes Programm als Empfänger. Der Server schreibt Informationen in das Programm.

Ereignisse (Erforderlich)
: Gibt die Art der Ereignisse an, die aktiviert werden sollen. Es können mehrere Ereignisse angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Gültige Werte:

  ALL
  : Alle Ereignisse.

  Ereignisname
  : Eine vierstellige Nachrichtennummer, die bei Server-Ereignissen mit den Buchstaben `ANR` beginnt, und bei Client-Ereignissen mit den Buchstaben `ANE`. Gültige Bereiche sind ANR0001 bis ANR9999 und ANE4000 bis ANE4999. Den Parameter NODENAME angeben, wenn Clientereignisse für übereinstimmende Knoten aktiviert werden sollen. Den Parameter SERVERNAME angeben, wenn Serverereignisse für übereinstimmende Server aktiviert werden sollen.
    Für den TIVOLI-Ereignisempfänger können die folgenden zusätzlichen Bereiche für die IBM Spectrum Protect-Anwendungsclients angegeben werden:

IBM Spectrum Protect-Anwendungsclient	Präfix	Bereich
Data Protection for Microsoft Exchange Server	ACN	3500–3649
Data Protection for Lotus Domino	ACD	5200–5299
Data Protection for Oracle	ANS	500–599
Data Protection for Informix	ANS	600–699
Data Protection for Microsoft SQL Server	ACO	3000–3999

    Einschränkung: Für den Anwendungsclient muss die erweiterte Tivoli Event Console-Unterstützung aktiviert sein, damit diese Nachrichten an die Tivoli Event Console weitergeleitet werden.
    Tipp:

    - Bei Angabe der Option ALL werden diese Nachrichten aktiviert. Die Optionen INFO, WARNING, ERROR und SEVERE haben jedoch keine Auswirkungen auf die Nachrichten.
    - Aufgrund der Anzahl der Nachrichten sollten nicht alle Nachrichten eines Knotens zum Protokollieren auf der Tivoli Event Console aktiviert werden.

  Bewertungskategorien
  : Wenn die Ereignisliste eine Bewertungskategorie enthält, werden alle Ereignisse mit dieser Bewertung für die angegebenen Knoten aktiviert. Die Nachrichtenarten sind:

    INFO
    : Informationsnachrichten (Art I) werden aktiviert.

    WARNING
    : Warnungen (Art W) werden aktiviert.

    ERROR
    : Fehlernachrichten (Art E) werden aktiviert.

    SEVERE
    : Schwerwiegende Fehlernachrichten (Art S) werden aktiviert.

NODEname
: Gibt einen oder mehrere Clientknoten an, für die Ereignisse aktiviert werden. Es kann ein Platzhalterzeichen verwendet werden, um alle Clientknoten anzugeben. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, werden Ereignisse für den Server aktiviert, auf dem dieser Befehl ausgeführt wird.

SERVername
: Gibt einen oder mehrere Server an, für die Ereignisse aktiviert werden sollen. Es kann ein Platzhalterzeichen verwendet werden, um alle anderen Server anzugeben, von denen dieser Befehl nicht ausgegeben wird. Der Benutzer kann SERVERNAME oder NODENAME angeben. Wird keiner der Parameter angegeben, werden die Ereignisse für den Server aktiviert, auf dem dieser Befehl ausgeführt wird.

Beispiel: Bestimmte Kategorien von Ereignissen aktivieren

Alle Client-Ereignisse ERROR und SEVERE für den Empfänger USEREXIT und den Knoten BONZO aktivieren.

```
enable events userexit error,severe nodename=bonzo
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ENABLE EVENTS

Befehl	Beschreibung
BEGIN EVENTLOGGING	Startet das Ereignisprotokoll für einen bestimmten Empfänger.
DISABLE EVENTS	Inaktiviert bestimmte Ereignisse für Empfänger.
END EVENTLOGGING	Beendet das Ereignisprotokoll für einen bestimmten Empfänger.
QUERY ENABLED	Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an.
QUERY EVENTRULES	Zeigt Informationen über Regeln für Server- und Clientereignisse an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

ENABLE REPLICATION (Verarbeitung abgehender Replikation auf einem Server ermöglichen)

Verwenden Sie diesen Befehl, um es einem Quellenreplikationsserver zu ermöglichen, die normale Replikationsverarbeitung nach einer Datenbankzurückschreibung zu starten. Sie können diesen Befehl auch verwenden, um die Replikationsverarbeitung wiederaufzunehmen, nachdem der Befehl DISABLE REPLICATION ausgegeben wurde.

Achtung: Bevor die Replikation nach einer Datenbankzurückschreibung aktiviert wird, bestimmen Sie, ob Kopien von Daten, die sich auf dem Zielserver befinden, benötigt werden. Ist dies der Fall, müssen Sie Clientknotendaten synchronisieren, indem die Daten vom Zielreplikationsserver auf den Quellenreplikationsserver repliziert werden. Der Replikationsprozess ersetzt die Daten auf dem Quellenserver, die aufgrund der Datenbankzurückschreibung nicht mehr vorhanden waren.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-ENable REPLication-------------------------------------------><
```

Parameter

Keine.

Beispiel: Replikationsverarbeitung ermöglichen

Die Replikationsverarbeitung auf einem Quellenreplikationsserver ermöglichen.

```
enable replication
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ENABLE REPLICATION

Befehl	Beschreibung
DISABLE REPLICATION	Verhindert die Verarbeitung abgehender Replikation auf einem Server.
DISABLE SESSIONS	Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden.
ENABLE SESSIONS	Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.

ENABLE SESSIONS (Benutzeraktivität auf dem Server wiederaufnehmen)

Verwenden Sie diesen Befehl nach der Ausgabe des Befehls DISABLE SESSIONS, um neue Sitzungen zu starten, die auf einen Server zugreifen können. Für einen bestimmten Server können Sie angeben, ob eingehende Sitzungen und/oder abgehende Sitzungen aktiviert werden sollen.

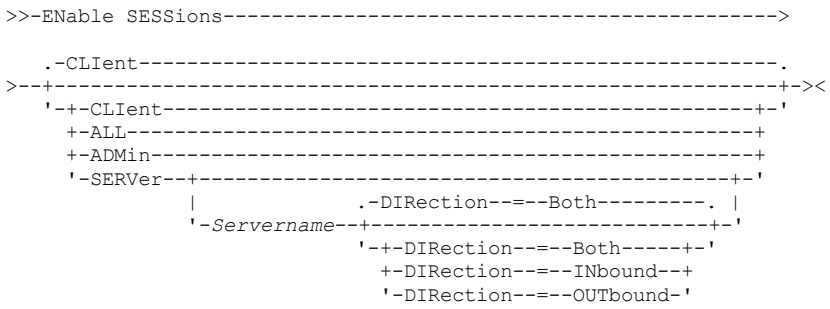
Die Verarbeitung dieses Befehls hat keine Auswirkungen auf Systemprozesse, wie beispielsweise Umlagerung und Wiederherstellung.

Mit dem Befehl QUERY STATUS kann die Verfügbarkeit des Servers angezeigt werden.

Berechtigungsklasse

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

Syntax



Parameter

Gibt den Typ der Sitzung an, der aktiviert werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT. Sie können einen der folgenden Werte angeben:

CLIent
: Aktiviert nur Sicherungs- und Archivierungsclientsitzungen.

ALL
: Aktiviert alle Sitzungstypen.

ADMin
: Aktiviert nur Verwaltungssitzungen.

SERVer
: Aktiviert nur Sitzungen zwischen Servern. Sie können auch angeben, ob eingehende Sitzungen und/oder abgehende Sitzungen für einen bestimmten Server aktiviert werden sollen.

  Servername
  : Gibt den Namen eines bestimmten Servers an, dessen Sitzungen aktiviert werden sollen. Dieser Parameter ist wahlfrei. Wenn Sie diesen Parameter nicht angeben, werden neue Sitzungen mit allen anderen Servern aktiviert.

    DIRection
    : Gibt an, ob eingehende Sitzungen und/oder abgehende Sitzungen aktiviert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist BOTH. Die folgenden Werte sind gültig:

      Both
      : Gibt an, dass eingehende Sitzungen vom angegebenen Server und abgehende Sitzungen zum angegebenen Server aktiviert werden.

      INbound
      : Gibt an, dass nur eingehende Sitzungen zum angegebenen Server aktiviert werden.

      OUTbound
      : Gibt an, dass nur abgehende Sitzungen vom angegebenen Server aktiviert werden.

Beispiel: Clientknotenaktivität auf dem Server wieder aufnehmen

Den Normalbetrieb wiederaufnehmen und den Zugriff der Client-Knoten auf den Server ermöglichen.

```
enable sessions
```

Beispiel: Alle Aktivitäten auf dem Server wieder aufnehmen

Den Normalbetrieb wiederaufnehmen und den Zugriff aller Sitzungen auf den Server ermöglichen.

```
enable sessions all
```

Beispiel: Abgehende Sitzungen zu einem Server aktivieren

Abgehende Sitzungen zu dem Server REPLSRV aktivieren.

```
enable sessions server replsrv direction=outbound
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ENABLE SESSIONS

Befehl	Beschreibung
ACCEPT DATE	Akzeptiert das aktuelle Datum auf dem Server.
CANCEL SESSION	Bricht aktive Sitzungen mit dem Server ab.
ENABLE REPLICATION	Ermöglicht die Verarbeitung abgehender Replikation auf einem Server.
DISABLE SESSIONS	Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden.
QUERY SESSION	Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

ENCRYPT STGPOOL (Daten in einem Speicherpool verschlüsseln)

Mit diesem Befehl können Daten in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool verschlüsselt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                              .-MAXPRocess--==--4------.
>>-ENCrypt STGpool--Poolname--+-----------------------+--------->
                              '-MAXPRocess--==--Anzahl-'

   .-Preview--==--No------.  .-Wait--==--No------.
>--+--------------------+--+-----------------+--------------><
   '-Preview--==--+-Yes-+-'  '-Wait--==--+-No--+-'
                  '-No--'               '-Yes-'
```

Parameter

Poolname (Erforderlich)
: Gibt den Namen des Speicherpools an, der Daten enthält, die verschlüsselt werden müssen.
Einschränkungen:

- Sie können nur Verzeichniscontainerspeicherpools oder Cloud-Containerspeicherpools angeben.
- Für den Speicherpoolnamen können bis zu 30 Zeichen angegeben werden. Wenn Sie mehr als 30 Zeichen angeben, schlägt der Befehl fehl.

MAXPRocess
: Gibt die maximale Anzahl paralleler Prozesse an, die ausgeführt werden können, wenn der Speicherpool Daten verschlüsselt. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 99 ein. Der Standardwert ist 4.

Preview
: Gibt an, ob eine Voranzeige mit allen Befehlen angezeigt wird, die als Teil des Befehls ENCRYPT STGPOOL verarbeitet werden. Dieser Parameter ist wahlfrei. Die folgenden Werte sind gültig:

  No
  : Gibt an, dass keine Voranzeige der Befehle angezeigt wird. Dies ist der Standardwert.

  Yes
  : Gibt an, dass eine Voranzeige der Befehle angezeigt wird.

Wait
: Gibt an, ob die Speicherpoolverschlüsselung im Vordergrund oder Hintergrund ausgeführt wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  No

Gibt an, dass die Operation im Hintergrund ausgeführt wird. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Dies ist der Standardwert.

Yes

Gibt an, dass die Operation im Vordergrund ausgeführt wird. Die Ausführung der Operation nimmt unter Umständen viel Zeit in Anspruch. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Einschränkung: Sie können den Parameter WAIT=YES nicht an der Serverkonsole angeben.

Beispiel: Daten in einem Speicherpool verschlüsseln

Daten in einem Speicherpool mit dem Namen POOL1 verschlüsseln und eine maximale Anzahl von 30 parallelen Prozessen angeben.

```
encrypt stgpool pool1 maxprocess=30
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ENCRYPT STGPOOL

Befehl	Beschreibung
DEFINE STGPOOL (Verzeichniscontainer)	Definiert einen Verzeichniscontainerspeicherpool.

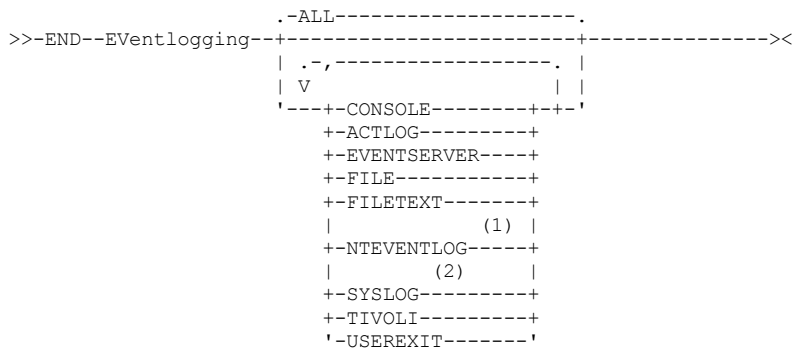
END EVENTLOGGING (Ereignisprotokollierung stoppen)

Mit diesem Befehl kann das Protokollieren von Ereignissen für einen aktiven Empfänger gestoppt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Anmerkungen:

1. Dieser Parameter ist nur für das Windows-Betriebssystem verfügbar.
2. Dieser Parameter ist nur für das Linux-Betriebssystem verfügbar.

Parameter

Eine Empfängerart angeben. Es können mehrere Empfänger angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden. Dieser Parameter ist wahlfrei. Standardwert ist ALL. Wird ALL oder kein Empfänger angegeben, endet das Protokollieren für alle Empfänger.

ALL
: Gibt alle Empfänger an.

CONSOLE
: Gibt die Server-Konsole als Empfänger an.

ACTLOG
: Gibt das IBM Spectrum Protect-Aktivitätenprotokoll als Empfänger an. Das Protokollieren kann nur für Client-Ereignisse gestoppt werden.

EVENTSERVER
: Gibt den Ereignisserver als Empfänger an.

FILE

Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist ein Satz in der Datei, und eine Person kann jedes protokollierte Ereignis nicht einfach lesen.

FILETEXT
Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.


Windows-BetriebssystemeNTEVENTLOG

Windows-BetriebssystemeGibt das Windows-Anwendungsprotokoll als Empfänger an.


Linux-BetriebssystemeSYSLOG

Linux-BetriebssystemeGibt das Linux-Systemprotokoll als Empfänger an.

TIVOLI
Gibt Tivoli Management Environment (TME) als Empfänger an.

USEREXIT
Gibt eine benutzerdefinierte Routine, in die IBM Spectrum Protect Informationen schreibt, als Empfänger an.

Beispiel: Das Protokollieren von Ereignissen stoppen

Das Protokollieren von Ereignissen für den Benutzerausgang beenden.

```
end eventlogging userexit
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für END EVENTLOGGING

Befehl	Beschreibung
BEGIN EVENTLOGGING	Startet das Ereignisprotokoll für einen bestimmten Empfänger.
DISABLE EVENTS	Inaktiviert bestimmte Ereignisse für Empfänger.
ENABLE EVENTS	Aktiviert bestimmte Ereignisse für Empfänger.
QUERY ENABLED	Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an.
QUERY EVENTRULES	Zeigt Informationen über Regeln für Server- und Clientereignisse an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

EXPIRE INVENTORY (Datenträgerbestandsverfall manuell starten)

Mit diesem Befehl kann die Verarbeitung des Datenträgerbestandsverfalls manuell gestartet werden. Beim Bestandsverfallsprozess werden Kopien von Clientsicherungs- und Archivierungsdateien aus dem Serverspeicher entfernt. Das Entfernen basiert auf Maßnahmenspezifikationen in den Sicherungs- und Archivierungskopiengruppen der Verwaltungsklassen, an die die Dateien gebunden sind.

Ist die Disaster Recovery Manager-Funktion für den IBM Spectrum Protect-Server verfügbar, entfernt der Bestandsverfallsprozess auch auswählbare virtuelle Datenträger, die von den folgenden Prozessen verwendet werden:

- Datenbanksicherungen der Art BACKUPFULL, BACKUPINCR und DBSNAPSHOT. Der Befehl SET DRMDBBACKUPEXPIREDAYS steuert, wann diese Datenträger für den Verfall auswählbar sind.
- Wiederherstellungsplandateien der Art RPFILE und RPFSNAPSHOT. Der Befehl SET DRMRPFEXPIREDAYS steuert, wann diese Datenträger für den Verfall auswählbar sind.

Der Datenträgerbestandsverfall, der während der Serverinitialisierung ausgeführt wird, entfernt nicht diese virtuellen Datenträger.

Es kann nur jeweils ein Verfallsprozess ausgeführt werden, aber dieser Prozess kann auf maximal 40 Threads verteilt werden. Wird ein Verfallsprozess ausgeführt, kann kein anderer Prozess gestartet werden.

Mit der Serveroption EXPINTERVAL kann die automatische Verfallsverarbeitung konfiguriert werden. Wird die Option EXPINTERVAL auf 0 gesetzt, wird die Verfallsverarbeitung von dem Server nicht automatisch ausgeführt, und Sie müssen den Befehl EXPIRE INVENTORY ausgeben, um die Verfallsverarbeitung zu starten.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Wird dieser Befehl auf einen WORM-Datenträger angewendet, kehrt der Datenträger in den Arbeitsdatenträgerstatus zurück, wenn er noch über Speicherbereich verfügt, in den Daten geschrieben werden können. Daten auf WORM-Datenträgern, einschließlich gelöschter und verfallener Daten, können nicht überschrieben werden. Daher können Daten nur in Speicherbereich geschrieben werden, der keine aktuellen, gelöschten oder verfallenen Daten enthält. Verfügt ein WORM-Datenträger über keinen Speicherbereich mehr, in den Daten geschrieben werden können, verbleibt der Datenträger im privaten Status. Soll der Datenträger aus dem Kassettenarchiv entfernt werden, müssen Sie den Befehl CHECKOUT LIBVOLUME verwenden.

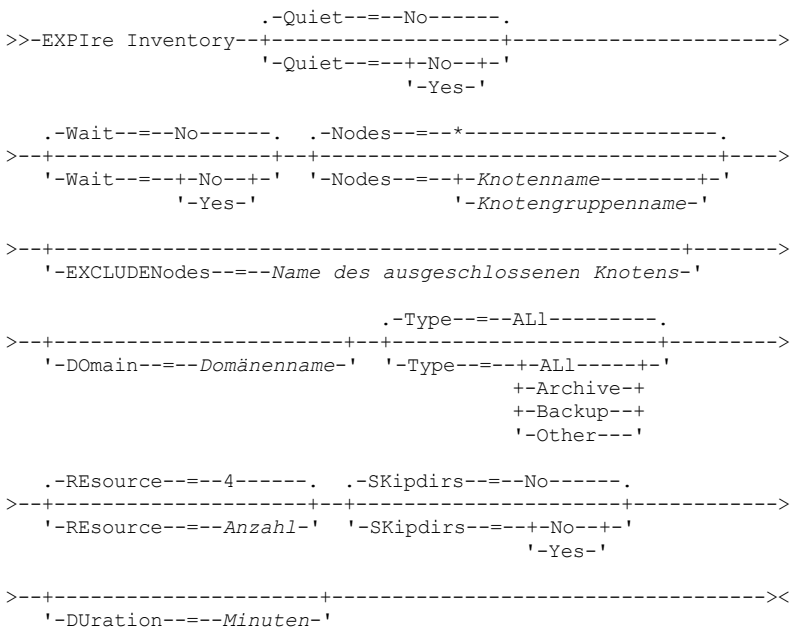
Führen Sie den Befehl EXPIRE INVENTORY aus, um Dateien aus dem Serverspeicher zu löschen, wenn sie bei der Verwendung von Clientlöschoperationen nicht gelöscht wurden.

Weitere Informationen zu Clientlöschoperationen befinden sich in Optionen und Befehle des Clients für Sichern/Archivieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Quiet
: Gibt an, ob der Server während der Verfallsverarbeitung detaillierte Nachrichten zu Maßnahmenänderungen unterdrückt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, dass der Server ausführliche Informationsnachrichten sendet.

  Yes
  : Gibt an, dass der Server nur Übersichtsnachrichten sendet. Der Server gibt Nachrichten zu Maßnahmenänderungen nur aus, wenn Dateien gelöscht werden und entweder die Standardverwaltungsklasse oder der Aufbewahrungszeitraum der Domäne für den Dateiverfall verwendet wurde.

    Außerdem kann mit der Option EXPQUIET in der Serveroptionsdatei automatisch festgestellt werden, ob die Verfallsverarbeitung mit Übersichtsnachrichten ausgeführt wird.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

    Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

  Yes
  : Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Sie warten auf die Beendigung des Befehls, bevor Sie mit anderen Tasks fortfahren. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist. Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

SKipdirs

Gibt an, ob der Server während der Verfallsverarbeitung Objekte mit einem Verzeichnistyp überspringt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No
: Gibt an, dass der Server Dateien und Verzeichnisse auf der Basis der entsprechenden Maßnahmekriterien als verfallen kennzeichnet.

Yes
: Gibt an, dass der Server Sicherungs- und Archivierungsobjekte mit einem Verzeichnistyp während der Verfallsverarbeitung überspringt, auch wenn die Verzeichnisse für die Verfallsverarbeitung ausgewählt werden können. Bei Angabe von YES verhindern Sie das Löschen von Verzeichnissen und die Verfallsverarbeitung kann schneller ausgeführt werden.
Achtung: Diese Option sollte nicht immer verwendet werden. Mit IBM Spectrum Protect Version 6.0 und höher können Sie mehrere Threads (Ressourcen) für einen Verfallsprozess ausführen. Wird YES oft angegeben, wächst außerdem die Datenbank an, da die Verzeichnisobjekte akkumulieren, und es erhöht sich die für die Verfallsverarbeitung benötigte Zeit. Führen Sie SKIPDIRS=NO regelmäßig aus, um die Verzeichnisse als verfallen zu kennzeichnen und die Größe der Datenbank zu reduzieren.

Nodes
: Gibt den Namen der Clientknoten oder Knotengruppen an, deren Daten verarbeitet werden sollen. Sollen mehrere Knoten- und Knotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Knotennamen können Platzhalterzeichen enthalten, Knotengruppennamen dagegen nicht. Dieser Parameter ist wahlfrei.

  Sie können NODES, EXCLUDENODES, DOMAIN oder eine beliebige Kombination angeben. Wenn Sie mehrere dieser Parameter angeben, werden nur die Knoten verarbeitet, die den Kriterien für die Befehlsparameter NODES und DOMAIN entsprechen, und nicht den Kriterien für den Befehlsparameter EXCLUDENODES entsprechen. Wenn Sie keinen Wert für NODES, EXCLUDENODES oder DOMAIN angeben, werden Daten für alle Knoten verarbeitet.

EXCLUDENodes
: Gibt die Namen der Clientknoten oder Knotengruppen an, deren Daten nicht verarbeitet werden sollen. Sollen mehrere Knoten- und Knotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Knotennamen können Platzhalterzeichen enthalten, Knotengruppennamen dagegen nicht. Dieser Parameter ist wahlfrei.

  Sie können NODES, EXCLUDENODES, DOMAIN oder eine beliebige Kombination angeben. Wenn Sie mehrere dieser Parameter angeben, werden nur die Knoten verarbeitet, die den Kriterien für die Befehlsparameter NODES und DOMAIN entsprechen, und nicht den Kriterien für den Befehlsparameter EXCLUDENODES entsprechen. Wenn Sie keinen Wert für NODES, EXCLUDENODES oder DOMAIN angeben, werden Daten für alle Knoten verarbeitet.

Domain
: Gibt an, dass nur Daten für Clientknoten verarbeitet werden sollen, die der angegebenen Domäne zugeordnet sind. Dieser Parameter ist wahlfrei. Sie können NODES, EXCLUDENODES, DOMAIN oder eine beliebige Kombination angeben. Wenn Sie mehrere dieser Parameter angeben, werden nur die Knoten verarbeitet, die den Kriterien für die Befehlsparameter NODES und DOMAIN entsprechen, und nicht den Kriterien für den Befehlsparameter EXCLUDENODES entsprechen. Wenn Sie keinen Wert für NODES, EXCLUDENODES oder DOMAIN angeben, werden Daten für alle Knoten verarbeitet.

Type
: Gibt den Typ der Daten an, die verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ALL. Gültige Werte:

  ALl
  : Alle Typen von Daten verarbeiten, die für die Verfallsverarbeitung auswählbar sind.

  Archive
  : Nur Clientarchivierungsdaten verarbeiten.

  Backup
  : Nur Clientsicherungsdaten verarbeiten.

  Other
  : Nur Elemente für Disaster Recovery Manager-Funktionen verarbeiten, wie beispielsweise Wiederherstellungsplandateien und veraltete Datenbanksicherungen.

REsource
: Gibt die Anzahl der Threads an, die parallel ausgeführt werden können. Geben Sie einen Wert im Bereich von 1 bis 40 an. Dieser Parameter ist wahlfrei. Der Standardwert ist vier.

  Die Verfallsverarbeitung wird als einzelner Prozess ausgeführt, obwohl die Ressourcen parallele Arbeit durch den Server innerhalb des einzelnen Verfallsprozesses darstellen. Der Verfallsprozess für Archivierungsdaten für einen Knoten wird nur auf einer einzelnen Ressource ausgeführt, aber der Verfallsprozess für Sicherungsdaten kann auf Ressourcen auf Dateibereichsebene verteilt werden. Geben Sie beispielsweise `NODE=X,Y,Z` mit jeweils drei Dateibereichen und `RESOURCE=5` an, wird die Verfallsverarbeitung für die drei Clientknoten X, Y und Z parallel ausgeführt. Mindestens eine Ressource verarbeitet jeden Knoten und mindestens ein Knoten verwendet mehrere Ressourcen für die Verarbeitung der Sicherungsdaten in den Dateibereichen.

DUration
: Gibt die maximale Anzahl Minuten für die Ausführung des Verfallsprozesses an. Der Prozess stoppt, wenn die angegebene Anzahl Minuten überschritten wird oder wenn alle auswählbaren verfallenen Objekte gelöscht werden (je nachdem, welches Ereignis zuerst eintritt). Geben Sie einen Wert im Bereich von 1 bis 2880 an. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, ist die Dauer des Verfallsprozesses nicht zeitlich begrenzt.

Beispiel: Die Bestandsverfallsverarbeitung für einen bestimmten Zeitraum ausführen

Den Verfallsprozess zwei Stunden lang ausführen.

```
expire inventory duration=120
```

Beispiel: Die Bestandsverfallsverarbeitung für Sicherungsdaten für zwei Clientknoten ausführen

Die Bestandsverfallsverarbeitung für die Sicherungsdaten der beiden Clientknoten CHARLIE und ROBBIE ausführen. Der Server soll die Verfallsverarbeitung ausführen, bis sie abgeschlossen ist.

```
expire inventory nodes=charlie,robbie resource=2 type=backup
```

Beispiel: Die Bestandsverfallsverarbeitung für alle Clientknoten mit Ausnahme von zwei Knoten ausführen

Die Bestandsverfallsverarbeitung für alle Clientknoten mit Ausnahme der beiden Knoten CHARLIE und ROBBIE ausführen. Der Server soll die Verfallsverarbeitung ausführen, bis sie abgeschlossen ist.

```
expire inventory excludenodes=charlie,robbie
```

Beispiel: Die Bestandsverfallsverarbeitung für alle Clientknoten in einer Domäne mit Ausnahme eines Knotens ausführen

Die Bestandsverfallsverarbeitung für alle Clientknoten in einer Domäne mit Ausnahme des Knotens ROBBIE ausführen. Der Server soll die Verfallsverarbeitung ausführen, bis sie abgeschlossen ist.

```
expire inventory domain=standard excludenodes=robbie
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für EXPIRE INVENTORY

Befehl	Beschreibung
AUDIT LICENSES	Prüft die Einhaltung der definierten Lizenzen.
CANCEL EXPIRATION	Bricht die Bestandsverfallsverarbeitung ab.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.

EXPORT-Befehle

Mit den EXPORT-Befehlen können Informationen von einem IBM Spectrum Protect-Server auf sequenzielle austauschbare Datenträger kopiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten exportiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls EXPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

- EXPORT ADMIN (Administratorinformationen exportieren)
- EXPORT NODE (Clientknoteninformationen exportieren)
- EXPORT POLICY (Maßnahmeninformationen exportieren)
- EXPORT SERVER (Serverinformationen exportieren)

EXPORT ADMIN (Administratorinformationen exportieren)

Mit diesem Befehl können Administrator- und Berechtigungsdefinitionen von einem Server exportiert werden. Sie können die Informationen auf sequenzielle Datenträger exportieren, um sie später auf einen anderen Server zu importieren, oder Sie können die Informationen direkt auf einen anderen Server exportieren.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten exportiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls EXPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

IBM Spectrum Protect exportiert folgende Administratorinformationen:

- Name, Kennwort und Kontaktinformationen des Administrators
- Dem Administrator erteilte Verwaltungsberechtigungsklassen
- Die Angabe, ob die Administrator-ID für den Server-Zugriff gesperrt ist

Mit dem Befehl QUERY ACTLOG kann der Status der Exportoperation angezeigt werden. Diese Informationen können auch über die Serverkonsole angezeigt werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn Sie Informationen auf sequenzielle Datenträger exportieren und der Hintergrundprozess abgebrochen wird, sind die sequenziellen Datenträger, auf denen sich die exportierten Daten befinden, unvollständig und dürfen nicht zum Importieren von Daten verwendet werden. Wird ein Hintergrundprozess abgebrochen, bei dem Daten von einem Server auf einen anderen Server exportiert werden, kann dies zu einem Teilimport von Daten führen. Werten Sie alle importierten Daten auf dem Zielserver aus, um zu bestimmen, ob die importierten Daten behalten oder gelöscht werden sollen. Überprüfen Sie die Importnachrichten auf Details. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Die folgenden Einschränkungen gelten für die Exportfunktion:

- Exportoperationen aus einer höheren Version und einem höheren Release in eine frühere Version und ein früheres Release werden nicht unterstützt.
- Exportoperationen zwischen Servern, die dieselbe Version und dasselbe Release, aber verschiedene Fixpacks aufweisen, können fehlschlagen. Beispielsweise können Sie keinen Export von einem Server der Version 7.1.3 auf einen Server der Version 7.1.1 oder einen früheren Server ausführen.
- Exportierte Daten von einem Server mit aktiviertem Aufbewahrungsschutz sind nicht durch Aufbewahrung geschützt, wenn sie auf einen anderen Server importiert werden.
- Die Exportverarbeitung schließt Knoten des Typs NAS (Network-attached Storage) aus.
- Das Exportieren von Daten in eine Centera-Einheitenklasse oder das Importieren von Daten aus einer Centera-Einheitenklasse wird nicht unterstützt. Dateien, die in Centera-Speicherpools gespeichert werden, können jedoch exportiert werden, und Dateien, die importiert werden müssen, können auf einer Centera-Speichereinheit gespeichert werden.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Der Befehl EXPORT ADMIN hat zwei Formen: Zum Exportieren von Daten direkt auf einen anderen Server in dem Netz oder zum Exportieren von Daten auf sequenzielle Datenträger. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für EXPORT ADMIN

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT POLICY	Kopiert Maßnahmeninformationen auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT SERVER	Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT ADMIN	Schreibt Verwaltungsdaten von externen Datenträgern zurück.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.

- EXPORT ADMIN (Administratordefinitionen auf sequenzielle Datenträger exportieren)
  Sie können Administrator- und Berechtigungsdefinitionen von einem Server auf sequenzielle Datenträger exportieren, um sie später auf einen anderen Server zu importieren.
- EXPORT ADMIN (Administratorinformationen direkt auf einen anderen Server exportieren)
  Mit diesem Befehl können Administrator- und Berechtigungsdefinitionen direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielserver zur Folge.

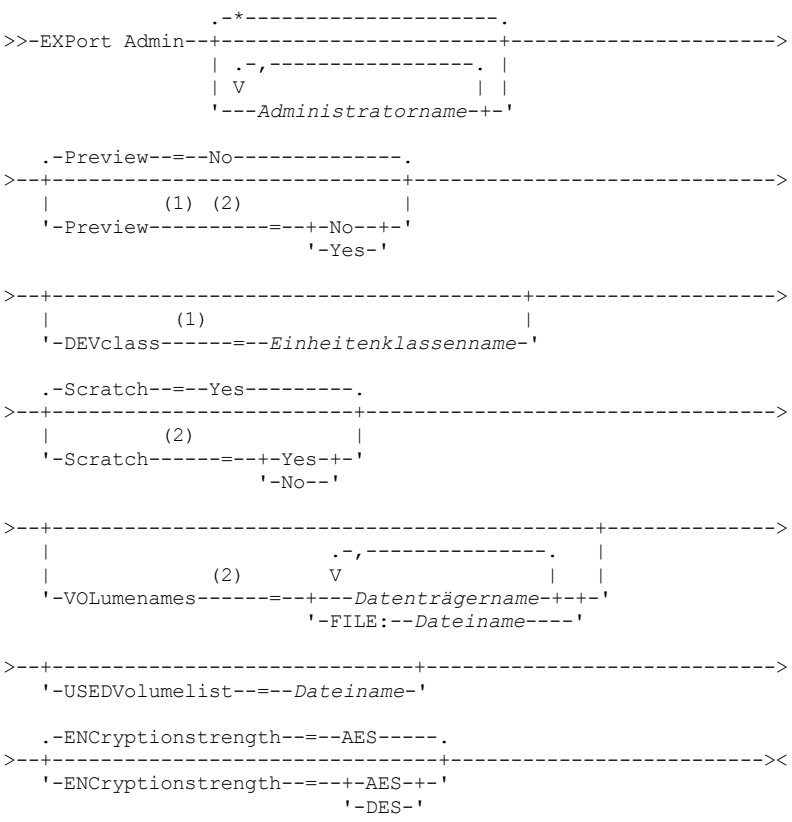
EXPORT ADMIN (Administratordefinitionen auf sequenzielle Datenträger exportieren)

Sie können Administrator- und Berechtigungsdefinitionen von einem Server auf sequenzielle Datenträger exportieren, um sie später auf einen anderen Server zu importieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Anmerkungen:

1. Wenn PREVIEW=NO gilt, muss eine Einheitenklasse angegeben werden.
2. Wenn PREVIEW=NO und SCRATCH=NO gilt, müssen Datenträger angegeben werden.

Parameter

Administratorname
: Gibt die Administratoren an, für die Informationen exportiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Administratoren.

  Die Einträge in der Liste ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

Preview
: Gibt an, ob die Ergebnisse der Exportoperation vorangezeigt werden sollen, ohne die Informationen zu exportieren. Mit diesem Parameter kann der Umfang der zu übertragenden Daten (Byte) vorangezeigt und bestimmt werden, wie viele Datenträger erforderlich sind. Die folgenden Parameterwerte werden unterstützt:

  No
  : Gibt an, dass die Administratorinformationen exportiert werden sollen. Wird dieser Wert angegeben, muss eine Einheitenklasse angegeben werden.

  Yes
  : Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.Wird dieser Wert angegeben, muss keine Einheitenklasse angegeben werden.

  Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

DEVclass

Gibt die Einheitenklasse an, in die die Exportdaten geschrieben werden sollen. Dieser Parameter ist erforderlich, wenn Sie PREVIEW=NO angeben.

Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Exports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, um ein Laufwerk verfügbar zu machen.

Tipp: Daten können in einen Speicherpool auf einem anderen Server exportiert werden, indem eine Einheitenklasse mit dem Einheitentyp SERVER angegeben wird.

Scratch

Gibt an, ob Arbeitsdatenträger verwendet werden können. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

Yes

Gibt an, dass Arbeitsdatenträger zum Exportieren verwendet werden können. Wird auch eine Liste mit Datenträgern angegeben, werden Arbeitsdatenträger nur verwendet, wenn auf den angegebenen Datenträgern nicht genügend Speicherbereich vorhanden ist.

No

Gibt an, dass keine Arbeitsdatenträger zum Exportieren verwendet werden können. Um zu bestimmen, wie viele Datenträger benötigt werden, können Sie den Befehl mit der Angabe PREVIEW=YES ausführen.

VOLumenames

Gibt die Datenträger an, die zum Speichern der exportierten Daten verwendet werden sollen. Dieser Parameter ist wahlfrei, es sei denn, es wird SCRATCH=NO und PREVIEW=NO angegeben. Wird kein Datenträgername angegeben, werden Arbeitsdatenträger verwendet.

Sie können einen der folgenden Werte angeben:

Datenträgername

Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

FILE: Dateiname

Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Folgende Namenskonventionen bei der Angabe von Datenträgern verwenden, die folgenden Einheitentypen zugeordnet sind:

Für Einheit	**Angeben**
Band	1 - 6 alphanumerische Zeichen.
FILE	Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel: AIX-BetriebssystemeLinux-Betriebssysteme/imdata/mt1. Windows-Betriebssystemed:\Programmdateien\tivoli\tsm\data1.dsm.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme REMOVABLEFILE	AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme1 - 6 alphanumerische Zeichen.
SERVER	1 - 250 alphanumerische Zeichen.

USEDVolumelist

Gibt die Datei an, in der eine Liste der Datenträger gespeichert wird, die in der Exportoperation verwendet werden. Dieser Parameter ist wahlfrei.

Diese Datei kann für die Importoperation verwendet werden. Diese Datei enthält Kommentarzeilen mit dem Exportdatum und der Exportuhrzeit sowie dem Befehl, der zum Erstellen des Exports ausgegeben wurde.

Achtung: Wird eine vorhandene Datei angegeben, wird die Datei überschrieben.

ENCryptionstrength

Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES

Gibt den Advanced Encryption Standard an.

DES

Gibt den Data Encryption Standard an.

Beispiel: Administratordefinitionen auf Banddatenträger exportieren

Vom Server die Informationen für alle definierten Administratoren auf die Banddatenträger TAPE01, TAPE02 und TAPE03 exportieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Die Anzahl und die Typen der

exportierten Objekte werden an die Systemkonsole und an das Aktivitätenprotokoll gemeldet. Den folgenden Befehl ausgeben:

```
export admin devclass=menu1
volumenames=tape01,tape02,tape03
```

Beispiel: Administratordefinitionen auf Banddatenträger exportieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Administratoren auf die Banddatenträger exportieren, die in der folgenden Datei aufgelistet sind:

- AIX-BetriebssystemeLinux-BetriebssystemeTAPEVOL
- Windows-BetriebssystemeTAPEVOL.DATA

Diese Datei enthält die folgenden Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass diese Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist. Den folgenden Befehl ausgeben:
AIX-BetriebssystemeLinux-Betriebssysteme

```
export admin devclass=menu1 volumenames=file:tapevol
```

Windows-Betriebssysteme

```
export admin devclass=menu1 volumenames=file:tapevol.data
```

Die Anzahl und die Typen der exportierten Objekte werden an die Systemkonsole und an das Aktivitätenprotokoll gemeldet.

EXPORT ADMIN (Administratorinformationen direkt auf einen anderen Server exportieren)

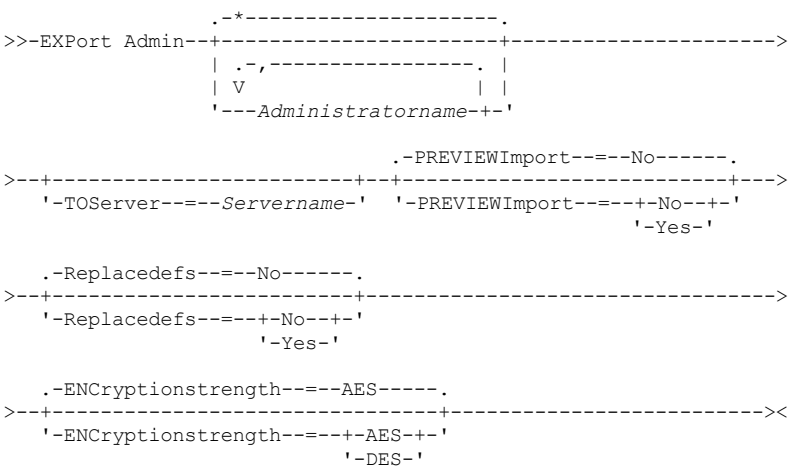
Mit diesem Befehl können Administrator- und Berechtigungsdefinitionen direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielserver zur Folge.

Sie können einen Befehl QUERY PROCESS auf dem Zielserver ausgeben, um den Fortschritt der Importoperation zu überwachen. In EXPORT ADMIN (Administratorinformationen exportieren) finden Sie eine Liste der Einschränkungen, die für die Exportfunktion gelten.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Administratorname
: Gibt die Administratoren an, für die Informationen exportiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Administratoren.

Die Einträge in der Liste ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

TOServer
Gibt den Namen eines Servers an, an den die Exportdaten direkt über das Netz für den sofortigen Import gesendet werden.
Wichtig: Der Zielserver muss mit dem Befehl DEFINE SERVER auf dem Ursprungsserver definiert werden. Der Administrator, der den Exportbefehl ausgibt, muss mit demselben Administratornamen und demselben Kennwort definiert werden und muss auf dem Zielserver über die Systemberechtigung verfügen.

Wenn Sie TOSERVER angeben, können Sie nicht die Parameter DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST und PREVIEW angeben.

PREVIEWImport
Gibt an, ob der Umfang der zu übertragenden Daten angezeigt werden soll, ohne die Daten tatsächlich zu versetzen. Mit diesen Informationen kann bestimmt werden, welcher Speicherpoolbereich auf dem Zielserver benötigt wird. Der Standardwert ist NO.
Gültige Werte sind:

Yes
Gibt an, dass die Ergebnisse der Importoperation auf dem Zielserver vorangezeigt werden sollen, ohne dass die Daten importiert werden. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.
No
Gibt an, dass die Daten in den Zielserver importiert werden sollen, ohne dass die Ergebnisse vorangezeigt werden.

Replacedefs
Gibt an, ob Definitionen (nicht Dateidaten) auf dem Server ersetzt werden sollen. Der Standardwert ist NO.

Gültige Werte sind:

Yes
Gibt an, dass Definitionen auf dem Server ersetzt werden, wenn Definitionen mit demselben Namen wie die zu importierenden Definitionen auf dem Zielserver vorhanden sind.
No
Gibt an, dass importierte Definitionen übersprungen werden, wenn ihre Namen mit Definitionen in Konflikt stehen, die bereits auf dem Zielserver definiert sind.

ENCryptionstrength
Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES
Gibt den Advanced Encryption Standard an.
DES
Gibt den Data Encryption Standard an.

Beispiel: Administratordefinitionen auf einen Zielserver exportieren

Alle Administratordefinitionen auf den Zielserver exportieren, der als OTHERSERVER definiert ist. Die Importoperationen auf dem Zielserver voranzeigen.Den folgenden Befehl ausgeben:

```
export admin * toserver=otherserver previewimport=yes
```

Auf dem Zielserver OTHERSERVER können Sie die Importoperationen anzeigen, indem Sie folgenden Befehl ausgeben:

```
query process
```

EXPORT NODE (Clientknoteninformationen exportieren)

Mit diesem Befehl können Clientknotendefinitionen oder Dateidaten auf sequenzielle Datenträger oder für den sofortigen Import auf einen anderen Server exportiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten exportiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls EXPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.
Die folgenden Informationen sind in jeder Clientknotendefinition enthalten:

- Benutzer-ID, Kennwort und Kontaktinformationen.
- Name der zugeordneten Maßnahmendomäne des Clients.
- Dateikomprimierungsstatus.
- Die Angabe, ob der Benutzer eine Berechtigung zum Löschen von gesicherten oder archivierten Dateien aus dem Serverspeicher hat.

- Die Angabe, ob der Serverzugriff auf die Clientknoten-ID gesperrt ist.

Wahlweise können auch folgende Elemente exportiert werden:

- Dateibereichsdefinitionen.
- Gesicherte Dateien, archivierte Dateien und Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.
- Zugriffsberechtigungsinformationen zu den exportierten Dateibereichen.
- Archivierungsdaten mit dem Status "Löschen unzulässig" (der Status wird beibehalten). Werden die Archivierungsdaten importiert, verbleiben sie im Status "Löschen unzulässig".

Wenn Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden, müssen alle Server, auf die exportiert wird, für LDAP-Kennwörter konfiguriert werden. Auf Knotendaten, die von einem Knoten exportiert werden, der sich mit einem LDAP-Verzeichnisserver authentifiziert, kann nicht zugegriffen werden, wenn der Zielserver nicht korrekt konfiguriert ist. Ist Ihr Zielserver nicht konfiguriert, können Daten von einem LDAP-Knoten dennoch exportiert werden. Der Zielserver muss jedoch für die Verwendung von LDAP konfiguriert werden, damit Sie auf die Daten zugreifen können.

Die folgenden Einschränkungen gelten für die Exportfunktion:

- Exportoperationen aus einer höheren Version und einem höheren Release in eine frühere Version und ein früheres Release werden nicht unterstützt.
- Exportoperationen zwischen Servern, die dieselbe Version und dasselbe Release, aber verschiedene Fixpacks aufweisen, können fehlschlagen. Beispielsweise können Sie keinen Export von einem Server der Version 7.1.3 auf einen Server der Version 7.1.1 oder einen früheren Server ausführen.
- Exportierte Daten von einem Server mit aktiviertem Aufbewahrungsschutz sind nicht durch Aufbewahrung geschützt, wenn sie auf einen anderen Server importiert werden.
- Die Exportverarbeitung schließt Knoten des Typs NAS (Network-attached Storage) aus.
- Das Exportieren von Daten in eine Centera-Einheitenklasse oder das Importieren von Daten aus einer Centera-Einheitenklasse wird nicht unterstützt. Dateien, die in Centera-Speicherpools gespeichert werden, können jedoch exportiert werden, und Dateien, die importiert werden müssen, können auf einer Centera-Speichereinheit gespeichert werden.

- Mit den Befehlen EXPORT NODE und EXPORT SERVER werden keine Daten aus einem Schredderpool exportiert, es sei denn, dies wird explizit zugelassen, indem der Parameter ALLOWSHREDDABLE auf YES gesetzt wird. Wenn dieser Wert angegeben wird und die exportierten Daten Daten aus Schredderpools einschließen, können diese Daten nicht geschreddert werden. Es wird keine Warnung ausgegeben, wenn die Exportoperation Daten aus Schredderpools einschließt.

- Das inkrementelle Exportieren oder Importieren der folgenden Typen von Clientdaten auf einen anderen IBM Spectrum Protect-Server wird nicht unterstützt:
    - VMware-Sicherungen, bei denen Gesamt- und Teilsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
    - Sicherungsgruppen, bei denen Gesamt- und Differenzsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
    - Windows-Systemstatusdaten, die periodisch, inkrementell auf einen anderen Server übertragen werden

  Der vollständige Export oder Import dieser Daten in ein neues Dateisystem auf dem Ziel wird unterstützt, indem der gesamte Dateibereich, der die Daten enthält, exportiert wird. Bei dem Export darf nicht der Parameter FILEDATA=ALLACTIVE, FROMDATE, TODATE oder MERGEFILESPACES verwendet werden.

  Die Verwendung der Knotenreplikation zur inkrementellen Übertragung dieses Typs von Clientdaten zwischen zwei Servern ist optimal.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Der Befehl EXPORT NODE generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn Sie Knoteninformationen auf sequenzielle Datenträger exportieren und der Hintergrundprozess abgebrochen wird, sind die sequenziellen Datenträger, auf denen sich die exportierten Daten befinden, unvollständig und dürfen nicht zum Importieren von Daten verwendet werden. Wird ein Hintergrundprozess abgebrochen, bei dem Daten von einem Server auf einen anderen Server exportiert werden, kann dies zu einem Teilimport von Daten führen. Werten Sie alle importierten Daten auf dem Zielserver aus, um zu bestimmen, ob die importierten Daten behalten oder gelöscht werden sollen. Überprüfen Sie die Importnachrichten auf Details. Um Informationen zu Hintergrundprozessen anzuzeigen, geben Sie den Befehl QUERY PROCESS aus.

Um Informationen zu aktiven und ausgesetzten Exportoperation zwischen Servern anzuzeigen, geben Sie den Befehl QUERY EXPORT aus. Mit dem Befehl QUERY EXPORT werden nur Informationen für Exporte angezeigt, die ausgesetzt sind oder ausgesetzt werden können. Exportoperationen, die ausgesetzt und dann erneut gestartet werden können, sind die Exportoperationen zwischen Servern, die einen anderen Wert für FILEDATA als NONE haben. Mit dem Befehl QUERY ACTLOG kann der Status der Exportoperation angezeigt werden.

Aufgrund unvorhersehbarer Ergebnisse führen Sie keine Verfallsverarbeitung, Umlagerung, Sicherung oder Archivierung aus, wenn Sie den Befehl EXPORT NODE ausgeben.

Bei einem Server, der über Clients mit Unterstützung für Unicode verfügt, kann der Server den Dateibereichsnamen konvertieren oder Sie können einen der folgenden Parameter verwenden:

- FSID
- UNIFILESPACE

Der Befehl EXPORT NODE hat zwei Formen: Zum Exportieren von Daten direkt auf einen anderen Server in dem Netz oder zum Exportieren von Daten auf sequenzielle Datenträger. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für EXPORT NODE

Befehl	Beschreibung
CANCEL EXPORT	Löscht eine ausgesetzte Exportoperation.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
EXPORT ADMIN	Kopiert Verwaltungsdaten auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT POLICY	Kopiert Maßnahmeninformationen auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT SERVER	Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT NODE	Schreibt Clientknotendaten von externen Datenträgern zurück.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY EXPORT	Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
RESTART EXPORT	Startet eine ausgesetzte Exportoperation erneut.
SUSPEND EXPORT	Setzt eine aktive Exportoperation aus.

- EXPORT NODE (Knotendefinitionen auf sequenzielle Datenträger exportieren)
  Sie können Knotendefinitionen oder Dateidaten von einem Server auf sequenzielle Datenträger exportieren, um sie später auf einen anderen Server zu importieren.
- EXPORT NODE (Knotendefinitionen oder Dateidaten direkt auf einen anderen Server exportieren)
  Mit diesem Befehl können Clientknotendefinitionen oder Dateidaten für den sofortigen Import direkt auf einen anderen Server exportiert werden.

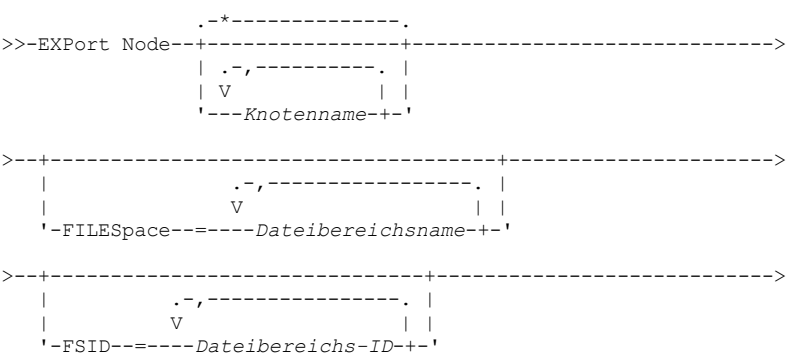
EXPORT NODE (Knotendefinitionen auf sequenzielle Datenträger exportieren)

Sie können Knotendefinitionen oder Dateidaten von einem Server auf sequenzielle Datenträger exportieren, um sie später auf einen anderen Server zu importieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Anmerkungen:

1. Wenn PREVIEW=NO gilt, muss eine Einheitenklasse angegeben werden.
2. Wenn PREVIEW=NO und SCRATCH=NO gilt, müssen Datenträger angegeben werden.

Parameter

Knotenname
: Gibt die Namen der Clientknoten an, für die Informationen exportiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Für jeden eingegebenen Knoten werden alle Dateibereiche in den Dateibereichs-, FSID- und Unicode-aktivierten Listen durchsucht.
Einschränkung: Verwenden Sie Platzhalterzeichen zur Angabe eines Musters für Knotennamen, meldet der Server keine Knotennamen oder Muster, die nicht mit Einträgen in der Datenbank übereinstimmen. Überprüfen Sie die zusammenfassende Statistik im Aktivitätenprotokoll, um sicherzustellen, dass der Server alle gewünschten Knoten exportiert hat.

FILESpace
Gibt die Dateibereiche an, für die Daten exportiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.
Einschränkung: Wenn ein Dateibereich angegeben wird, werden Unicode-fähige Dateibereiche nicht exportiert.

FSID
Gibt die Dateibereiche an, indem ihre Dateibereichs-IDs (File Space IDs = FSIDs) verwendet werden. Der Server verwendet die FSIDs zum Lokalisieren der Dateibereiche, die exportiert werden sollen. Zum Lokalisieren der FSID eines Dateibereichs verwenden Sie den Befehl QUERY FILESPACE. Mehrere Dateibereichs-IDs müssen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Dieser Parameter ist wahlfrei.

UNIFILESpace
Gibt die Dateibereiche an, die dem Server als Unicode-aktiviert bekannt sind. Der Server konvertiert die Namen, die Sie eingeben, aus der Zeichenumsetztabelle des Servers in die Zeichenumsetztabelle UTF-8, um die Dateibereiche zu lokalisieren, die exportiert werden sollen. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Dieser Parameter ist wahlfrei.

DOmains
Gibt die Maßnahmendomänen an, aus denen Knoten exportiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Werden Domänen angegeben, wird ein Knoten nur exportiert, wenn er zu einer der angegebenen Domänen gehört. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

FILEData
Gibt den Typ der Dateien an, die für alle Knoten exportiert werden sollen, die auf den Server exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.
Anmerkung: Wenn Sie einen Knoten exportieren, der über Gruppendaten verfügt, werden möglicherweise Daten exportiert, die nicht Teil der Zielobjekte sind. Beispiele für Gruppendaten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Wird beispielsweise bei FILEDATA=BACKUPACTIVE der Parameter FROMDATE oder TODATE angegeben, ist es möglich, dass inaktive Sicherungsdaten eingeschlossen werden. Die Teilsicherungsverarbeitung für die Daten kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden.

Export auf sequenzielle Datenträger: Die von den Dateidaten verwendete Einheitenklasse wird durch die Einheitenklasse des Speicherpools bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, werden zum Exportieren von Knoteninformationen zwei Laufwerke benötigt. Das Mountlimit für die Einheitenklasse muss mindestens 2 betragen.

Wichtig: Werden Clientknoten exportiert, die als TYPE=SERVER registriert sind, ALL, ARCHIVE oder ALLACTIVE angeben.

In den folgenden Beschreibungen werden *aktive* und *inaktive* Versionen von Sicherungsdateien erwähnt. Eine aktive Version einer Sicherungsdatei ist die aktuellste Sicherungsversion für eine Datei, die noch auf der Client-Workstation vorhanden ist. Alle anderen Versionen der Sicherungsdatei werden als inaktive Kopien bezeichnet. Dieser Parameter unterstützt die folgenden Werte:

ALl
Der Server exportiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

None
Der Server exportiert keine Dateien, nur Knotendefinitionen.

ARchive
Der Server exportiert nur archivierte Dateien.

Backup
Der Server exportiert nur Sicherungsversionen, unabhängig davon, ob sie aktiv oder inaktiv sind.

BACKUPActive
Der Server exportiert nur aktive Sicherungsversionen. Diese aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl EXPORT ausgegeben wird.

ALLActive
Der Server exportiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl EXPORT ausgegeben wird.

SPacemanaged
Der Server exportiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Preview
Gibt an, ob die Ergebnisse der Exportoperation vorangezeigt werden sollen, ohne die Informationen zu exportieren. Mit diesem Parameter kann der Umfang der zu übertragenden Daten (Byte) vorangezeigt werden, um zu bestimmen, wie viele Datenträger benötigt werden. Dieser Parameter unterstützt die folgenden Werte:

No
Gibt an, dass die Knoteninformationen exportiert werden sollen. Wird dieser Wert angegeben, muss auch eine Einheitenklasse angegeben werden.

Yes
Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.Wird dieser Wert angegeben, muss keine Einheitenklasse angegeben werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

DEVclass
Gibt die Einheitenklasse an, in die die Exportdaten geschrieben werden sollen. Dieser Parameter ist erforderlich, wenn Sie PREVIEW=NO angeben.

Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Exports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, um ein Laufwerk verfügbar zu machen.

Tipp: Daten können in einen Speicherpool auf einem anderen Server exportiert werden, indem eine Einheitenklasse mit dem Einheitentyp SERVER angegeben wird.

Scratch
Gibt an, ob Arbeitsdatenträger verwendet werden können. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass Arbeitsdatenträger zum Exportieren verwendet werden können. Wird auch eine Liste mit Datenträgern angegeben, werden Arbeitsdatenträger nur verwendet, wenn auf den angegebenen Datenträgern nicht genügend Speicherbereich vorhanden ist.

No
Gibt an, dass keine Arbeitsdatenträger zum Exportieren verwendet werden können. Um zu bestimmen, wie viele Datenträger benötigt werden, können Sie den Befehl mit der Angabe PREVIEW=YES ausführen.

VOLumenames
Gibt die Datenträger an, die zum Speichern der exportierten Daten verwendet werden sollen. Dieser Parameter ist wahlfrei, es sei denn, es wird SCRATCH=NO und PREVIEW=NO angegeben. Wird kein Datenträgername angegeben, werden Arbeitsdatenträger verwendet.

Sie können einen der folgenden Werte angeben:

Datenträgername
Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

FILE: Dateiname
Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Folgende Namenskonventionen bei der Angabe von Datenträgern verwenden, die folgenden Einheitentypen zugeordnet sind:

Für Einheit	**Angeben**
Band	1 - 6 alphanumerische Zeichen.
FILE	Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel: AIX-BetriebssystemeLinux-Betriebssysteme/imdata/mt1. Windows-Betriebssystemed:\Programmdateien\tivoli\tsm\data1.dsm.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme REMOVABLEFILE	AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme1 - 6 alphanumerische Zeichen.
SERVER	1 - 250 alphanumerische Zeichen.

USEDVolumelist
Gibt die Datei an, in der eine Liste der Datenträger gespeichert wird, die in der Exportoperation verwendet werden. Dieser Parameter ist wahlfrei.

Diese Datei kann für die Importoperation verwendet werden. Diese Datei enthält Kommentarzeilen mit dem Exportdatum und der Exportuhrzeit sowie dem Befehl, der zum Erstellen des Exports ausgegeben wurde.

Achtung: Wird eine vorhandene Datei angegeben, wird die Datei überschrieben.

FROMDate
Gibt das früheste Datum an, für das Dateien, die exportiert werden sollen, auf dem Server gespeichert wurden. Dateien, die vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter FROMDATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
Verzeichnisverarbeitung: Der Parameter FROMDATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.
Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Gruppendaten auf dem Knoten sind beispielsweise Daten virtueller Maschinen oder Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.
Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY -3 **oder** -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

Wird dieser Parameter nicht angegeben, exportiert IBM Spectrum Protect alle Objekte, die vor dem Datum im Parameter TODATE gespeichert wurden und die durch den Parameter FILEDATA qualifiziert sind. Wird kein Parameter TODATE angegeben, werden alle Daten exportiert, die durch den Parameter FILEDATA qualifiziert sind.

Wenn eine Exportoperation zwischen Servern ein relatives FROMDATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird FROMDATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

TODate

Gibt das späteste Datum für Dateien an, die vom Server exportiert werden sollen. Dateien, die auf dem Server an einem späteren Datum als dem für TODATE angegebenen Datum gespeichert werden, werden nicht exportiert. TODATE gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen.

- IBM Spectrum Protect ignoriert den Parameter TODATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
- Wenn ein Parameter TODATE ohne einen Parameter TOTIME angegeben wird, exportiert der Server alle Objekte, die an oder vor dem durch den Parameter TODATE angegebenen Tag eingefügt wurden.
- Wurde der Parameter FROMDATE angegeben, muss der Wert von TODATE größer-gleich dem Wert von FROMDATE sein. Sind TODATE und FROMDATE gleich, muss der Wert für den Parameter TOTIME größer als der Wert für den Parameter FROMTIME sein.
- Der Parameter TODATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die nach dem Datum oder der Zeit im Parameter TODATE oder TOTIME gesichert wurden, exportiert werden. Beispiele für Gruppendaten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	10/15/2006
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY –3 **oder** –3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.

Wert	Beschreibung	Beispiel
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

Wenn eine Exportoperation zwischen Servern ein relatives TODATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird TODATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und 10 Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

FROMTime

Gibt die früheste Uhrzeit an, für die Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Geben Sie FROMTIME an, müssen Sie auch den Parameter FROMDATE verwenden. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. Objekte, die vor der angegebenen Uhrzeit und vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. IBM Spectrum Protect ignoriert den Parameter FROMTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.
Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Beispiele für Gruppendaten auf dem Knoten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Bei Verwendung mit dem Parameter FROMDATE lautet der Standardwert für diesen Parameter Mitternacht (00:00:00).

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.FROMTIME+ kann nur mit einem FROMDATE vor heute verwendet werden.	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW+02:00 oder FROMTIME=+02:00 ausgegeben, enthält die Exportoperation nur Dateien, die nach 7:00 Uhr an dem angegebenen FROMDATE auf den Server gestellt wurden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW -02:00 **oder** -02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW-02:00 oder FROMTIME=-2:00 ausgegeben, enthält der Export Dateien, die nach 3:00 Uhr auf den Server gestellt wurden.

TOTime

Gibt den spätesten Zeitpunkt an, an dem Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Sie müssen den Parameter TODATE angeben, um den Parameter TOTIME verwenden zu können. TOTIME gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter TOTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Bei Verwendung mit dem Parameter TODATE lautet der Standardwert für diesen Parameter Mitternacht minus eine Sekunde (23:59:59).

Wichtig: Die Werte für die Parameter TOTIME und TODATE müssen größer als die Werte für die Parameter FROMDATE und FROMTIME sein.
Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08

Wert	Beschreibung	Beispiel
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW+02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 7 Uhr gespeichert wurden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten.	NOW-02:00 **oder** -02:00. Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW-02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 3 Uhr gespeichert wurden.

ENCryptionstrength
Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES
Gibt den Advanced Encryption Standard an.
DES
Gibt den Data Encryption Standard an.

ALLOWSHREDdable
Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Dieser Parameter unterstützt die folgenden Werte:

No
Gibt an, dass Daten nicht aus einem Speicherpool exportiert werden, der das Schreddern erzwingt.
Yes
Gibt an, dass Daten aus einem Speicherpool exportiert werden können, der das Schreddern erzwingt. Die Daten auf den Exportdatenträgern werden nicht geschreddert.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Beispiel: Clientknoteninformationen auf bestimmte Banddatenträger exportieren

Vom Server Clientknoteninformationen auf die Banddatenträger TAPE01, TAPE02 und TAPE03 exportieren. Angeben, dass diese Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
export node devclass=menu1 volumenames=tape01,tape02,tape03
```

Beispiel: Clientknoteninformationen unter Verwendung der FSID exportieren

Verwenden Sie auf dem Server die FSID, um aktive Sicherungsversionen der Dateidaten für Clientknoten JOE auf den Banddatenträger TAPE01 zu exportieren. Um die FSID zu bestimmen, geben Sie zuerst einen Befehl QUERY FILESPACE aus.

1. Um die FSID zu bestimmen, geben Sie einen Befehl QUERY FILESPACE aus.

   ```
   query filespace joe

   Knotenname Dateibe-  FSID Platt-  Dateibe-    Ist       Kapazi-   %
              reichsname     form    reichstyp   Dateiber. tät (MB) Ausl.
                                                 Unicode?
   ---------- ---------- ---- -------  ---------  --------- -------- ----
   JOE        \\joe\c$    1  WinNT     NTFS         Yes     2.502,3  75,2
   JOE        \\joe\d$    2  WinNT     NTFS         Yes     6.173,4  59,6
   ```

2. Exportieren Sie die aktiven Sicherungsversionen der Dateidaten und geben Sie an, dass der Banddatenträger von einer Einheit verwendet wird, die der Einheitenklasse MENU1 zugeordnet ist.

   ```
   export node joe fsid=1,2 filedata=backupactive devclass=menu1
   volumenames=tape01
   ```

Beispiel: Clientknoteninformationen auf Banddatenträger exportieren, die in einer Datei aufgelistet sind

Vom Server die Clientknoteninformationen auf Banddatenträger exportieren, die in der folgenden Datei aufgelistet sind:

- AIX-BetriebssystemeLinux-BetriebssystemeTAPEVOL
- Windows-BetriebssystemeTAPEVOL.DATA

Die Datei enthält die folgenden Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass die Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist. Geben Sie den folgenden Befehl aus:
 AIX-Betriebssysteme  Linux-Betriebssysteme

```
export node devclass=menu1 volumenames=file:tapevol
```

 Windows-Betriebssysteme

```
export node devclass=menu1 volumenames=file:tapevol.data
```

EXPORT NODE (Knotendefinitionen oder Dateidaten direkt auf einen anderen Server exportieren)

Mit diesem Befehl können Clientknotendefinitionen oder Dateidaten für den sofortigen Import direkt auf einen anderen Server exportiert werden.

Wichtig: Knoten des Typs NAS können nicht exportiert werden. Die Exportverarbeitung schließt diese Knoten aus.

Sie können eine Exportoperation zwischen Servern, die einen anderen Wert als NONE für FILEDATA hat, aussetzen und erneut starten. Der Server sichert den Status der Exportoperation, sodass die Exportoperation an dem Punkt erneut gestartet werden kann, an dem sie fehlgeschlagen ist oder ausgesetzt wurde. Die Exportoperation kann zu einem späteren Zeitpunkt erneut gestartet werden, indem der Befehl RESTART EXPORT ausgegeben wird.

Wichtig: Eine Exportoperation wird ausgesetzt, wenn eine der folgenden Bedingungen festgestellt wird:

- Ein Befehl SUSPEND EXPORT wird für die aktive Exportoperation ausgegeben
- Segmentvorableerung - die Datei, die für den Export gelesen wird, wird von einem anderen Prozess gelöscht
- Übertragungsfehler bei einem Export zwischen Servern
- Keine verfügbaren Mountpunkte
- Erforderliche Datenträger sind nicht verfügbar
- E/A-Fehler wurden festgestellt

Mit dem Befehl QUERY EXPORT können Informationen zu allen aktiven und ausgesetzten Exportoperationen angezeigt werden.

Die Exportoperation kann nicht erneut gestartet werden, wenn die Exportoperation fehlschlägt, bevor die auswählbaren Knoten- und Dateibereichsdefinitionen auf den Zielserver übertragen werden. Sie müssen den Befehl erneut eingeben, um eine neue Exportoperation zu beginnen.

Sie können einen Befehl QUERY PROCESS auf dem Zielserver ausgeben, um den Fortschritt der Importoperation zu überwachen. Geben Sie den Befehl QUERY EXPORT aus, um alle wiederanlauffähigen Exportoperationen zwischen Servern aufzulisten. In EXPORT ADMIN (Administratorinformationen exportieren) finden Sie eine Liste der Einschränkungen, die für die Exportfunktion gelten.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                .-*----------.
>>-EXPort Node--+------------+---------------------------------->
                '-Knotenname-'

>--+---------------------------------+-------------------------->
   '-FILESpace--=--Dateibereichsname-'

>--+-----------------------------+------------------------------->
   '-FSID--=--Dateibereichs-ID-'

>--+-------------------------------------+----------------------->
   '-UNIFILESpace--=--Dateibereichsname-'

>--+-------------------------+---------------------------------->
   '-DOmains--=--Domänenname-'

   .-FILEData--=--None-------------.
>--+-------------------------------+--------------------------->
   '-FILEData--=--+-ALl----------+-'
                  +-None---------+
                  +-ARchive------+
                  +-Backup-------+
```

Parameter

Knotenname
: Gibt die Namen der Clientknoten an, für die Informationen exportiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Für jeden eingegebenen Knoten werden alle Dateibereiche in den Dateibereichs-, FSID- und Unicode-aktivierten Listen durchsucht.
Einschränkung: Wenn Sie eine Liste der Knotennamen oder Knotenmuster angeben, meldet der Server keine Knotennamen oder Knotenmuster zurück, die nicht mit Einträgen in der Datenbank übereinstimmen. Überprüfen Sie die zusammenfassende Statistik im Aktivitätenprotokoll, um sicherzustellen, dass der Server alle gewünschten Knoten exportiert hat.

FILESpace
: Gibt die Dateibereiche an, für die Daten exportiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.
Einschränkung: Wenn ein Dateibereich angegeben wird, werden keine Unicode-fähigen Dateibereiche exportiert.

FSID
: Gibt die Dateibereiche an, indem ihre Dateibereichs-IDs (File Space IDs = FSIDs) verwendet werden. Der Server verwendet die FSIDs zum Lokalisieren der Dateibereiche, die exportiert werden sollen. Zum Lokalisieren der FSID eines Dateibereichs verwenden Sie den Befehl QUERY FILESPACE. Mehrere Dateibereichs-IDs müssen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Dieser Parameter ist wahlfrei.

UNIFILESpace
: Gibt die Dateibereiche an, die dem Server als Unicode-aktiviert bekannt sind. Der Server konvertiert die Namen, die Sie eingeben, aus der Zeichenumsetztabelle des Servers in die Zeichenumsetztabelle UTF-8, um die Dateibereiche zu lokalisieren, die exportiert werden sollen. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Dieser Parameter ist wahlfrei.

DOmains
: Gibt die Maßnahmendomänen an, aus denen Knoten exportiert werden. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Wenn Sie Domänen angeben, exportiert IBM Spectrum Protect einen Knoten nur dann, wenn er zu einer der angegebenen Domänen gehört. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

FILEData

Gibt den Typ der Dateien an, die für alle Knoten exportiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.
Anmerkung: Wenn Sie einen Knoten exportieren, der über Gruppendaten verfügt, werden möglicherweise Daten exportiert, die nicht Teil der Zielobjekte sind. Beispiele für Gruppendaten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Wird beispielsweise bei FILEDATA=BACKUPACTIVE der Parameter FROMDATE oder TODATE angegeben, ist es möglich, dass inaktive Sicherungsdaten eingeschlossen werden. Die Teilsicherungsverarbeitung für die Daten kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden.

Wenn der Export auf sequenzielle Datenträger erfolgt, wird die von den Dateidaten verwendete Einheitenklasse durch die Einheitenklasse des Speicherpools bestimmt. Wenn es sich um dieselbe Einheitenklasse wie in diesem Befehl handelt, benötigt IBM Spectrum Protect zwei Laufwerke zum Exportieren von Knoteninformationen. Das Mountlimit für die Einheitenklasse muss mindestens 2 betragen.

Wichtig: Wenn Sie Clientknoten exportieren, die als TYPE=SERVER registriert sind, geben Sie ALL, ARCHIVE oder ALLACTIVE an.
In den folgenden Beschreibungen werden *aktive* und *inaktive* Versionen von Sicherungsdateien erwähnt. Eine aktive Version einer Sicherungsdatei ist die aktuellste Sicherungsversion für eine Datei, die noch auf der Client-Workstation vorhanden ist. Alle anderen Versionen der Sicherungsdatei werden als inaktive Kopien bezeichnet. Folgende Werte sind verfügbar:

ALl
: Der Server exportiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert werden.

None
: Der Server exportiert keine Dateien, nur Knotendefinitionen.

ARchive
: Der Server exportiert nur archivierte Dateien.

Backup
: Der Server exportiert nur Sicherungsversionen, unabhängig davon, ob sie aktiv oder inaktiv sind.

BACKUPActive
: Der Server exportiert nur aktive Sicherungsversionen. Diese aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl EXPORT ausgegeben wird.

ALLActive
: Der Server exportiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl EXPORT ausgegeben wird.

SPacemanaged
: Der Server exportiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

FROMDate

Gibt das früheste Datum an, für das Dateien, die exportiert werden sollen, auf dem Server gespeichert wurden. Dateien, die vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter FROMDATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
Verzeichnisverarbeitung: Der Parameter FROMDATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.
Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Gruppendaten auf dem Knoten sind beispielsweise Daten virtueller Maschinen oder Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.
Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY -3 **oder** -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM

Wert	Beschreibung	Beispiel
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

Wird dieser Parameter nicht angegeben, exportiert IBM Spectrum Protect alle Objekte, die vor dem Datum im Parameter TODATE gespeichert wurden und die durch den Parameter FILEDATA qualifiziert sind. Wird kein Parameter TODATE angegeben, werden alle Daten exportiert, die durch den Parameter FILEDATA qualifiziert sind.

Wenn eine Exportoperation zwischen Servern ein relatives FROMDATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird FROMDATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

TODate

Gibt das späteste Datum für Dateien an, die vom Server exportiert werden sollen. Dateien, die auf dem Server an einem späteren Datum als dem für TODATE angegebenen Datum gespeichert werden, werden nicht exportiert. TODATE gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen.

- IBM Spectrum Protect ignoriert den Parameter TODATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
- Wenn ein Parameter TODATE ohne einen Parameter TOTIME angegeben wird, exportiert der Server alle Objekte, die an oder vor dem durch den Parameter TODATE angegebenen Tag eingefügt wurden.
- Wurde der Parameter FROMDATE angegeben, muss der Wert von TODATE größer-gleich dem Wert von FROMDATE sein. Sind TODATE und FROMDATE gleich, muss der Wert für den Parameter TOTIME größer als der Wert für den Parameter FROMTIME sein.
- Der Parameter TODATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die nach dem Datum oder der Zeit im Parameter TODATE oder TOTIME gesichert wurden, exportiert werden. Beispiele für Gruppendaten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	10/15/2006
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY –3 **oder** –3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

Wenn eine Exportoperation zwischen Servern ein relatives TODATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird TODATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und 10 Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

FROMTime

Gibt die früheste Uhrzeit an, für die Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Geben Sie FROMTIME an, müssen Sie auch den Parameter FROMDATE verwenden. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. Objekte, die vor der angegebenen Uhrzeit und vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. IBM Spectrum Protect ignoriert den Parameter FROMTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.
Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Beispiele für Gruppendaten auf dem Knoten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Bei Verwendung mit dem Parameter FROMDATE lautet der Standardwert für diesen Parameter Mitternacht (00:00:00).

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.FROMTIME+ kann nur mit einem FROMDATE vor heute verwendet werden.	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW+02:00 oder FROMTIME=+02:00 ausgegeben, enthält die Exportoperation nur Dateien, die nach 7:00 Uhr an dem angegebenen FROMDATE auf den Server gestellt wurden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW -02:00 **oder** -02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW-02:00 oder FROMTIME=-2:00 ausgegeben, enthält der Export Dateien, die nach 3:00 Uhr auf den Server gestellt wurden.

TOTime

Gibt den spätesten Zeitpunkt an, an dem Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Sie müssen den Parameter TODATE angeben, um den Parameter TOTIME verwenden zu können. TOTIME gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter TOTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Bei Verwendung mit dem Parameter TODATE lautet der Standardwert für diesen Parameter Mitternacht minus eine Sekunde (23:59:59).

Wichtig: Die Werte für die Parameter TOTIME und TODATE müssen größer als die Werte für die Parameter FROMDATE und FROMTIME sein.
Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW+02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 7 Uhr gespeichert wurden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten.	NOW-02:00 **oder** -02:00. Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW-02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 3 Uhr gespeichert wurden.

TOServer

Gibt den Namen eines Servers an, an den die Exportdaten direkt über das Netz für den sofortigen Import gesendet werden.
Wichtig: Der Zielserver muss mit dem Befehl DEFINE SERVER auf dem Ursprungsserver definiert werden. Der Administrator, der den Exportbefehl ausgibt, muss mit demselben Administratornamen und demselben Kennwort definiert werden und muss auf dem Zielserver über die Systemberechtigung verfügen.

Wenn Sie TOSERVER angeben, können Sie nicht die Parameter DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST und PREVIEW angeben.

PREVIEWImport

Gibt an, ob der Umfang der zu übertragenden Daten angezeigt werden soll, ohne die Daten tatsächlich zu versetzen. Mit diesen Informationen kann bestimmt werden, welcher Speicherpoolbereich auf dem Zielserver benötigt wird. Der Standardwert ist NO. Gültige Werte sind:

Yes
: Gibt an, dass die Ergebnisse der Importoperation auf dem Zielserver vorangezeigt werden sollen, ohne dass die Daten importiert werden. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.

No
: Gibt an, dass die Daten in den Zielserver importiert werden sollen, ohne dass die Ergebnisse vorangezeigt werden.

MERGEfilespaces
: Gibt an, ob IBM Spectrum Protect Clientdateien in vorhandene Dateibereiche auf dem Zielserver mischt (sofern sie vorhanden sind) oder ob IBM Spectrum Protect neue Dateibereichsnamen generiert. Der Standardwert ist NO.

Gültige Werte sind:

Yes
: Gibt an, dass importierte Daten auf dem Zielserver in den vorhandenen Dateibereich gemischt werden, wenn ein Dateibereich mit demselben Namen auf dem Zielserver vorhanden ist.

No
: Gibt an, dass IBM Spectrum Protect einen neuen Dateibereichsnamen für importierte Daten auf dem Zielserver generiert, wenn Dateibereiche mit demselben Namen vorhanden sind.

Replacedefs
: Gibt an, ob Definitionen (nicht Dateidaten) auf dem Server ersetzt werden sollen. Der Standardwert ist NO.

Gültige Werte sind:

Yes
: Gibt an, dass Definitionen auf dem Server ersetzt werden, wenn Definitionen mit demselben Namen wie die zu importierenden Definitionen auf dem Zielserver vorhanden sind.

No
: Gibt an, dass importierte Definitionen übersprungen werden, wenn ihre Namen mit Definitionen in Konflikt stehen, die bereits auf dem Zielserver definiert sind.

PROXynodeassoc
: Gibt an, ob Proxyknotenzuordnungen exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

ENCryptionstrength
: Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES
: Gibt den Advanced Encryption Standard an.

DES
: Gibt den Data Encryption Standard an.

ALLOWSHREDdable
: Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No
: Gibt an, dass der Server keine Daten aus einem Speicherpool exportiert, der das Schreddern erzwingt.

Yes
: Gibt an, dass der Server Daten aus einem Speicherpool exportiert, der das Schreddern erzwingt. Die Daten auf den Exportdatenträgern werden nicht geschreddert.

Einschränkung: Nachdem eine Exportoperation die Identifizierung von Dateien für den Export beendet hat, werden alle Änderungen des Werts ALLOWSHREDABLE für den Speicherpool ignoriert. Eine Exportoperation, die ausgesetzt ist, behält während der gesamten Operation den ursprünglichen Wert für ALLOWSHREDABLE. Möglicherweise möchten Sie Ihre Exportoperation abbrechen, wenn Änderungen des Werts ALLOWSHREDABLE für den Speicherpool die Operation gefährden. Sie können den Exportbefehl nach einer erforderlichen Bereinigung erneut ausgeben.

EXPORTIDentifier
: Dieser optionale Parameter gibt den Namen an, den Sie zum Identifizieren dieser Exportoperation auswählen. Geben Sie keine ID an, wird vom Server eine ID generiert. Die Export-ID darf 64 Zeichen nicht überschreiten, darf keine Platzhalterzeichen enthalten und ist nicht von der Groß-/Kleinschreibung abhängig. Mit dieser ID können Sie auf Exportoperationen in den Befehlen QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT oder CANCEL EXPORT verweisen.
Einschränkung: Sie müssen den Parameter TOSERVER angeben, wenn Sie den Parameter EXPORTIDENTIFIER angeben. EXPORTIDENTIFIER wird bei FILEDATA=NONE ignoriert.

Beispiel: Clientknoteninformationen und alle Clientdateien exportieren

Um Clientknoteninformationen und alle Clientdateien für NODE1 direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus:

```
export node node1 filedata=all toserver=serverb
```

Beispiel: Clientknoteninformationen und alle Clientdateien für einen bestimmten Datumsbereich exportieren

Um Clientknoteninformationen und alle Clientdateien für NODE1 zwischen dem 1. Februar 2009 und heute direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus.

```
export node node1 filedata=all toserver=serverb
fromdate=02/01/2009 todate=today
```

Beispiel: Clientknoteninformationen und alle Clientdateien für einen bestimmten Datums- und Zeitbereich exportieren

Um Clientknoteninformationen und alle Clientdateien für NODE1 zwischen dem 1. Februar 2009 um 8 Uhr bis heute um 8 Uhr direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus:

```
export node node1 filedata=all toserver=serverb
fromdate=02/01/2009 fromtime=08:00:00
todate=today totime=08:00:00
```

Beispiel: Clientknoteninformationen und alle Clientdateien für die letzten drei Tage exportieren

Um Clientknoteninformationen und alle Clientdateien für NODE1 für die letzten drei Tage direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus:

```
export node node1 filedata=all toserver=serverb
fromdate=today -3
```

EXPORT POLICY (Maßnahmeninformationen exportieren)

Mit diesem Befehl können Maßnahmeninformationen von einem IBM Spectrum Protect-Server auf sequenzielle Datenträger oder für den sofortigen Import direkt auf einen anderen Server exportiert werden. Wenn eine Maßnahme mit dem Befehl EXPORT POLICY exportiert wird, werden die aktiven Datenpoolinformationen in der Domäne nicht exportiert.

Der Server exportiert folgende Maßnahmeninformationen:

- Maßnahmendomänendefinitionen
- Maßnahmengruppendefinitionen, einschließlich der aktiven Maßnahmengruppe
- Verwaltungsklassendefinitionen, einschließlich der Standardverwaltungsklasse
- Sicherungskopiengruppen- und Archivierungskopiengruppendefinitionen
- Zeitplandefinitionen für jede Maßnahmendomäne
- Client-Knotenzuordnungen, wenn der Client-Knoten auf dem Ziel-Server vorhanden ist

Mit dem Befehl QUERY ACTLOG kann der Status der Exportoperation angezeigt werden. Diese Informationen können auch über die Serverkonsole angezeigt werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn Sie Maßnahmeninformationen auf sequenzielle Datenträger exportieren und der Hintergrundprozess abgebrochen wird, sind die sequenziellen Datenträger, auf denen sich die exportierten Daten befinden, unvollständig und dürfen nicht zum Importieren von Daten verwendet werden. Wird ein Hintergrundprozess abgebrochen, bei dem Daten von einem Server auf einen anderen Server exportiert werden, kann dies zu einem Teilimport von Daten führen. Werten Sie alle importierten Daten auf dem Zielserver aus, um zu bestimmen, ob die importierten Daten behalten oder gelöscht werden sollen. Überprüfen Sie die Importnachrichten auf Details. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Die folgenden Einschränkungen gelten für die Exportfunktion:

- Exportoperationen aus einer höheren Version und einem höheren Release in eine frühere Version und ein früheres Release werden nicht unterstützt.
- Exportoperationen zwischen Servern, die dieselbe Version und dasselbe Release, aber verschiedene Fixpacks aufweisen, können fehlschlagen. Beispielsweise können Sie keinen Export von einem Server der Version 7.1.3 auf einen Server der Version 7.1.1 oder einen früheren Server ausführen.
- Exportierte Daten von einem Server mit aktiviertem Aufbewahrungsschutz sind nicht durch Aufbewahrung geschützt, wenn sie auf einen anderen Server importiert werden.
- Die Exportverarbeitung schließt Knoten des Typs NAS (Network-attached Storage) aus.
- Das Exportieren von Daten in eine Centera-Einheitenklasse oder das Importieren von Daten aus einer Centera-Einheitenklasse wird nicht unterstützt. Dateien, die in Centera-Speicherpools gespeichert werden, können jedoch exportiert werden, und Dateien, die importiert werden müssen, können auf einer Centera-Speichereinheit gespeichert werden.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Der Befehl EXPORT POLICY hat zwei Formen: Zum Exportieren von Daten direkt auf einen anderen Server in dem Netz oder zum Exportieren von Daten auf sequenzielle Datenträger. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für EXPORT POLICY

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
EXPORT ADMIN	Kopiert Verwaltungsdaten auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT SERVER	Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT POLICY	Schreibt Maßnahmendaten von externen Datenträgern zurück.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.

- EXPORT POLICY (Maßnahmeninformationen auf sequenzielle Datenträger exportieren)
  Mit diesem Befehl können Maßnahmeninformationen von einem IBM Spectrum Protect-Server auf sequenzielle Datenträger exportiert werden, um sie später auf einen anderen Server zu importieren.
- EXPORT POLICY (Eine Maßnahme direkt auf einen anderen Server exportieren)
  Mit diesem Befehl können Maßnahmeninformationen direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielserver zur Folge.

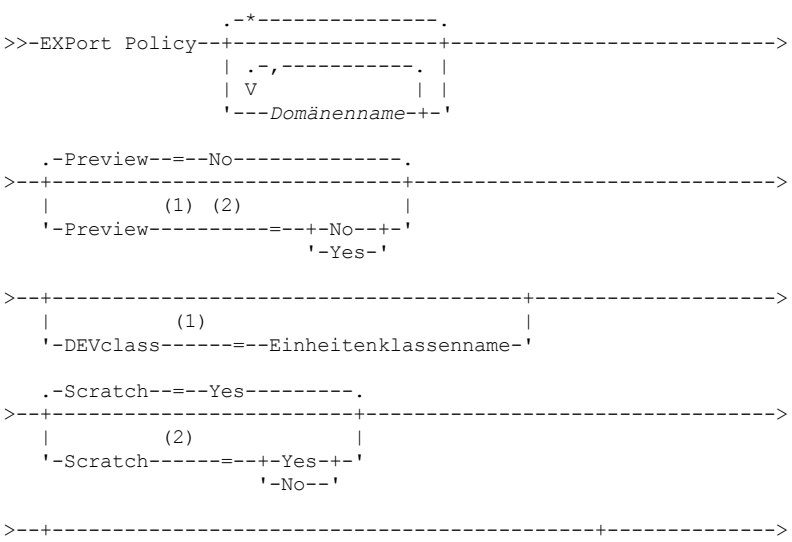
EXPORT POLICY (Maßnahmeninformationen auf sequenzielle Datenträger exportieren)

Mit diesem Befehl können Maßnahmeninformationen von einem IBM Spectrum Protect-Server auf sequenzielle Datenträger exportiert werden, um sie später auf einen anderen Server zu importieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



```
   |                      .-,---------------.    |
   |             (2)      V                 |    |
   '-VOLumenames-------=--+---Datenträgername-+-+-'
                          '-FILE:--Dateiname----'

>--+------------------------------+-----------------------------><
   '-USEDVolumelist-=--Dateiname-'
```

Anmerkungen:

1. Wenn PREVIEW=NO gilt, muss eine Einheitenklasse angegeben werden.
2. Wenn PREVIEW=NO und SCRATCH=NO gilt, müssen Datenträger angegeben werden.

Parameter

Domänenname
: Gibt die Maßnahmendomänen an, für die Informationen exportiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Maßnahmendomänen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

Preview
: Gibt an, ob die Ergebnisse der Exportoperation vorangezeigt werden sollen, ohne die Informationen zu exportieren. Mit diesem Parameter kann der Umfang der zu übertragenden Daten (Byte) vorangezeigt werden, um zu bestimmen, wie viele Datenträger benötigt werden. Dieser Parameter unterstützt die folgenden Werte:

  No
  : Gibt an, dass die Maßnahmeninformationen exportiert werden sollen. Wird dieser Wert angegeben, muss auch eine Einheitenklasse angegeben werden.

  Yes
  : Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.Wird dieser Wert angegeben, muss keine Einheitenklasse angegeben werden.

  Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

DEVclass
: Gibt die Einheitenklasse an, in die die Exportdaten geschrieben werden sollen. Dieser Parameter ist erforderlich, wenn Sie PREVIEW=NO angeben.

  Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

  Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Exports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, um ein Laufwerk verfügbar zu machen.

  Tipp: Daten können in einen Speicherpool auf einem anderen Server exportiert werden, indem eine Einheitenklasse mit dem Einheitentyp SERVER angegeben wird.

Scratch
: Gibt an, ob Arbeitsdatenträger verwendet werden können. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

  Yes
  : Gibt an, dass Arbeitsdatenträger zum Exportieren verwendet werden können. Wird auch eine Liste mit Datenträgern angegeben, werden Arbeitsdatenträger nur verwendet, wenn auf den angegebenen Datenträgern nicht genügend Speicherbereich vorhanden ist.

  No
  : Gibt an, dass keine Arbeitsdatenträger zum Exportieren verwendet werden können. Um zu bestimmen, wie viele Datenträger benötigt werden, können Sie den Befehl mit der Angabe PREVIEW=YES ausführen.

VOLumenames
: Gibt die Datenträger an, die zum Speichern der exportierten Daten verwendet werden sollen. Dieser Parameter ist wahlfrei, es sei denn, es wird SCRATCH=NO und PREVIEW=NO angegeben. Wird kein Datenträgername angegeben, werden Arbeitsdatenträger verwendet.

  Sie können einen der folgenden Werte angeben:

  Datenträgername
  : Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

  FILE: Dateiname
  : Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

  Folgende Namenskonventionen bei der Angabe von Datenträgern verwenden, die folgenden Einheitentypen zugeordnet sind:

Für Einheit	**Angeben**
Band	1 - 6 alphanumerische Zeichen.

Für Einheit	Angeben
FILE	Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel: AIX-BetriebssystemeLinux-Betriebssysteme/imdata/mt1. Windows-Betriebssystemed:\Programmdateien\tivoli\tsm\data1.dsm.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme REMOVABLEFILE	AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme1 - 6 alphanumerische Zeichen.
SERVER	1 - 250 alphanumerische Zeichen.

USEDVolumelist
Gibt die Datei an, in der eine Liste der Datenträger gespeichert wird, die in der Exportoperation verwendet werden. Dieser Parameter ist wahlfrei.

Diese Datei kann für die Importoperation verwendet werden. Diese Datei enthält Kommentarzeilen mit dem Exportdatum und der Exportuhrzeit sowie dem Befehl, der zum Erstellen des Exports ausgegeben wurde.

Achtung: Wird eine vorhandene Datei angegeben, wird die Datei überschrieben.

Beispiel: Maßnahmeninformationen auf bestimmte Banddatenträger exportieren

Vom Server Maßnahmeninformationen auf die Banddatenträger TAPE01, TAPE02 und TAPE03 exportieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
export policy devclass=menu1
volumenames=tape01,tape02,tape03
```

Beispiel: Maßnahmeninformationen auf Banddatenträger exportieren, die in einer Datei aufgelistet sind

Vom Server die Maßnahmeninformationen auf Banddatenträger exportieren, die in der folgenden Datei aufgelistet sind:

- AIX-BetriebssystemeLinux-BetriebssystemeTAPEVOL
- Windows-BetriebssystemeTAPEVOL.DATA

Diese Datei enthält die folgenden Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass diese Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist. Geben Sie den folgenden Befehl aus: AIX-BetriebssystemeLinux-Betriebssysteme

```
export policy devclass=menu1 volumenames=file:tapevol
```

Windows-Betriebssysteme

```
export policy devclass=menu1 volumenames=file:tapevol.data
```

EXPORT POLICY (Eine Maßnahme direkt auf einen anderen Server exportieren)

Mit diesem Befehl können Maßnahmeninformationen direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielserver zur Folge.

Sie können einen Befehl QUERY PROCESS auf dem Zielserver ausgeben, um den Fortschritt der Importoperation zu überwachen. In EXPORT ADMIN (Administratorinformationen exportieren) finden Sie eine Liste der Einschränkungen, die für die Exportfunktion gelten.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                  .-*---------------.
>>-EXPort Policy--+-----------------+--------------------------->
                  | .-,-----------. |
                  | V             | |
```

```
                '---Domänenname-+-'

                                .-PREVIEWImport--=--No------.
>--+-------------------------+--+---------------------------+--->
   '-TOServer--=--Servername-'  '-PREVIEWImport--=--+-No--+-'
                                                   '-Yes-'

   .-Replacedefs--=--No------.
>--+-------------------------+--------------------------------><
   '-Replacedefs--=--+-No--+-'
                     '-Yes-'
```

Parameter

Domänenname
: Gibt die Maßnahmendomänen an, für die Informationen exportiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Maßnahmendomänen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

TOServer
: Gibt den Namen eines Servers an, an den die Exportdaten direkt über das Netz für den sofortigen Import gesendet werden.
Wichtig: Der Zielserver muss mit dem Befehl DEFINE SERVER auf dem Ursprungsserver definiert werden. Der Administrator, der den Exportbefehl ausgibt, muss mit demselben Administratornamen und demselben Kennwort definiert werden und muss auf dem Zielserver über die Systemberechtigung verfügen.

  Wenn Sie TOSERVER angeben, können Sie nicht die Parameter DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST und PREVIEW angeben.

PREVIEWImport
: Gibt an, ob der Umfang der zu übertragenden Daten angezeigt werden soll, ohne die Daten tatsächlich zu versetzen. Mit diesen Informationen kann bestimmt werden, welcher Speicherpoolbereich auf dem Zielserver benötigt wird. Der Standardwert ist NO.
Gültige Werte sind:

  Yes
  : Gibt an, dass die Ergebnisse der Importoperation auf dem Zielserver vorangezeigt werden sollen, ohne dass die Daten importiert werden. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.

  No
  : Gibt an, dass die Daten in den Zielserver importiert werden sollen, ohne dass die Ergebnisse vorangezeigt werden.

Replacedefs
: Gibt an, ob Definitionen (nicht Dateidaten) auf dem Server ersetzt werden sollen. Der Standardwert ist NO.

  Gültige Werte sind:

  Yes
  : Gibt an, dass Definitionen auf dem Server ersetzt werden, wenn Definitionen mit demselben Namen wie die zu importierenden Definitionen auf dem Zielserver vorhanden sind.

  No
  : Gibt an, dass importierte Definitionen übersprungen werden, wenn ihre Namen mit Definitionen in Konflikt stehen, die bereits auf dem Zielserver definiert sind.

Beispiel: Maßnahme auf einen anderen Server exportieren

Um Maßnahmeninformationen direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus:

```
export policy replacedefs=yes toserver=othersrv
```

EXPORT SERVER (Serverinformationen exportieren)

Mit diesem Befehl können die Serversteuerungsinformationen und Clientdateidaten (falls angegeben) vollständig oder teilweise aus dem Server auf sequenzielle Datenträger exportiert werden.

Wenn Sie Serverinformationen auf sequenzielle Datenträger exportieren, können Sie später die Datenträger verwenden, um die Informationen auf einen anderen Server mit einem kompatiblen Einheitentyp zu importieren.
Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

Sie haben auch die Option, eine Exportoperation direkt auf einem anderen Server in dem Netz zu verarbeiten. Dies hat einen sofortigen Importprozess zur Folge, ohne dass kompatible sequenzielle Einheitentypen zwischen den beiden Servern verwendet werden müssen.

Sie können die folgenden Typen von Serverinformationen exportieren, indem Sie den Befehl EXPORT SERVER ausgeben:

- Maßnahmendomänendefinitionen
- Maßnahmengruppendefinitionen
- Verwaltungsklassen- und Kopiengruppendefinitionen
- Zeitpläne, die für jede Maßnahmendomäne definiert sind
- Administratordefinitionen
- Clientknotendefinitionen

Sie können wahlweise die folgenden Typen von Daten exportieren:

- Dateibereichsdefinitionen
- Zugriffsberechtigungsinformationen zu den exportierten Dateibereichen
- Gesicherte Dateien, archivierte Dateien und Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn Sie Serverinformationen auf sequenzielle Datenträger exportieren und der Hintergrundprozess abgebrochen wird, sind die sequenziellen Datenträger, auf denen sich die exportierten Daten befinden, unvollständig und dürfen nicht zum Importieren von Daten verwendet werden. Wird ein Hintergrundprozess abgebrochen, bei dem Daten von einem Server auf einen anderen Server exportiert werden, kann dies zu einem Teilimport von Daten führen. Werten Sie alle importierten Daten auf dem Zielserver aus, um zu bestimmen, ob die importierten Daten behalten oder gelöscht werden sollen. Überprüfen Sie die Importnachrichten auf Details.

Geben Sie den Befehl QUERY PROCESS auf dem Zielserver aus, um den Fortschritt der Importoperation zu überwachen. Geben Sie den Befehl QUERY EXPORT aus, um alle aktiven oder ausgesetzten Exportoperationen zwischen Servern aufzulisten (die einen anderen Wert für FILEDATA als NONE haben).

Mit dem Befehl QUERY ACTLOG können die tatsächlichen Statusinformationen angezeigt werden, die Auskunft über die Größe und den Erfolg oder das Fehlschlagen der Exportoperation geben.

Die folgenden Einschränkungen gelten für die Exportfunktion:

- Exportoperationen aus einer höheren Version und einem höheren Release in eine frühere Version und ein früheres Release werden nicht unterstützt.
- Exportoperationen zwischen Servern, die dieselbe Version und dasselbe Release, aber verschiedene Fixpacks aufweisen, können fehlschlagen. Beispielsweise können Sie keinen Export von einem Server der Version 7.1.3 auf einen Server der Version 7.1.1 oder einen früheren Server ausführen.
- Exportierte Daten von einem Server mit aktiviertem Aufbewahrungsschutz sind nicht durch Aufbewahrung geschützt, wenn sie auf einen anderen Server importiert werden.
- Die Exportverarbeitung schließt Knoten des Typs NAS (Network-attached Storage) aus.
- Das Exportieren von Daten in eine Centera-Einheitenklasse oder das Importieren von Daten aus einer Centera-Einheitenklasse wird nicht unterstützt. Dateien, die in Centera-Speicherpools gespeichert werden, können jedoch exportiert werden, und Dateien, die importiert werden müssen, können auf einer Centera-Speichereinheit gespeichert werden.

- Mit den Befehlen EXPORT NODE und EXPORT SERVER werden keine Daten aus einem Schredderpool exportiert, es sei denn, dies wird explizit zugelassen, indem der Parameter ALLOWSHREDDABLE auf YES gesetzt wird. Wenn dieser Wert angegeben wird und die exportierten Daten Daten aus Schredderpools einschließen, können diese Daten nicht geschreddert werden. Es wird keine Warnung ausgegeben, wenn die Exportoperation Daten aus Schredderpools einschließt.

- Das inkrementelle Exportieren oder Importieren der folgenden Typen von Clientdaten auf einen anderen IBM Spectrum Protect-Server wird nicht unterstützt:
    - VMware-Sicherungen, bei denen Gesamt- und Teilsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
    - Sicherungsgruppen, bei denen Gesamt- und Differenzsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
    - Windows-Systemstatusdaten, die periodisch, inkrementell auf einen anderen Server übertragen werden

  Der vollständige Export oder Import dieser Daten in ein neues Dateisystem auf dem Ziel wird unterstützt, indem der gesamte Dateibereich, der die Daten enthält, exportiert wird. Bei dem Export darf nicht der Parameter FILEDATA=ALLACTIVE, FROMDATE, TODATE oder MERGEFILESPACES verwendet werden.

  Die Verwendung der Knotenreplikation zur inkrementellen Übertragung dieses Typs von Clientdaten zwischen zwei Servern ist optimal.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Der Befehl EXPORT SERVER hat zwei Formen: Zum Exportieren von Daten direkt auf einen anderen Server in dem Netz oder zum Exportieren von Daten auf sequenzielle Datenträger. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für EXPORT SERVER

Befehl	Beschreibung
CANCEL EXPORT	Löscht eine ausgesetzte Exportoperation.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
EXPORT ADMIN	Kopiert Verwaltungsdaten auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT POLICY	Kopiert Maßnahmeninformationen auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT SERVER	Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY EXPORT	Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
RESTART EXPORT	Startet eine ausgesetzte Exportoperation erneut.
SUSPEND EXPORT	Setzt eine aktive Exportoperation aus.

- EXPORT SERVER (Server auf sequenzielle Datenträger exportieren)
  Sie können die Serversteuerungsinformationen und Clientdateidaten vollständig oder teilweise von einem Server auf sequenzielle Datenträger exportieren, sodass diese Informationen auf einen anderen Server importiert werden können.
- EXPORT SERVER (Serversteuerungsinformationen und Clientdateidaten auf einen anderen Server exportieren)
  Mit diesem Befehl können die Serversteuerungsinformationen und Clientdateidaten vollständig oder teilweise direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielserver zur Folge.

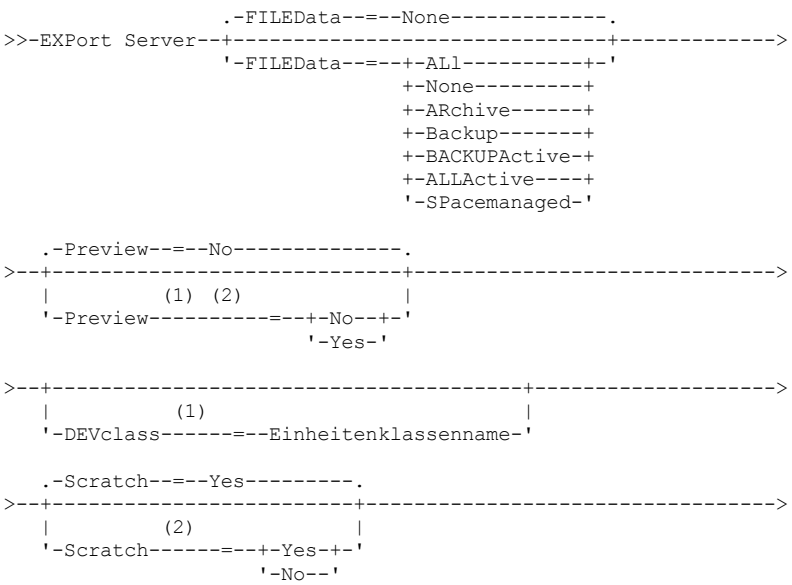
EXPORT SERVER (Server auf sequenzielle Datenträger exportieren)

Sie können die Serversteuerungsinformationen und Clientdateidaten vollständig oder teilweise von einem Server auf sequenzielle Datenträger exportieren, sodass diese Informationen auf einen anderen Server importiert werden können.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



```
>--+-----------------------------------------------+-------------->
   |                        .-,---------------.    |
   |             (2)        V                 |    |
   '-VOLumenames-------=---+---Datenträgername-+-+-'
                           '-FILE:--Dateiname----'

>--+------------------------------+----------------------------->
   '-USEDVolumelist--=--Dateiname-'

>--+-----------------------------------------------+------------>
   |                        .-FROMTime--=--00:00:00-. |
   '-FROMDate--=--Datum--+------------------------+-'
                         '-FROMTime--=--Zeit-----'

>--+-----------------------------------------------+------------->
   |                     .-TOTime--=--23:59:59-. |
   '-TODate--=--Datum--+----------------------+-'
                       '-TOTime--=--Zeit-----'

   .-ENCryptionstrength--=--AES-----.
>--+-------------------------------+--------------------------->
   '-ENCryptionstrength--=--+-AES-+-'
                            '-DES-'

   .-ALLOWSHREDdable--=--No------.
>--+-----------------------------+---------------------------><
   '-ALLOWSHREDdable--=--+-No--+-'
                         '-Yes-'
```

Anmerkungen:

1. Wenn PREVIEW=NO gilt, muss eine Einheitenklasse angegeben werden.
2. Wenn PREVIEW=NO und SCRATCH=NO gilt, müssen Datenträger angegeben werden.

Parameter

FILEData
: Gibt den Typ der Dateien an, die für alle Knoten exportiert werden, die für den Server definiert sind. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

  Beim Export auf sequenzielle Datenträger wird die für den Zugriff auf die Dateidaten verwendete Einheitenklasse durch die Einheitenklasse für den Speicherpool bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, werden zum Exportieren von Serverinformationen zwei Laufwerke benötigt. Der Grenzwert für Ladeanforderungen der Einheitenklasse muss mindestens auf 2 gesetzt werden.

  In den folgenden Beschreibungen werden *aktive* und *inaktive* Versionen von Sicherungsdateien erwähnt. Eine aktive Version einer Sicherungsdatei ist die aktuellste Sicherungsversion für eine Datei, die noch auf der Client-Workstation vorhanden ist. Alle anderen Versionen der Sicherungsdatei werden als inaktive Kopien bezeichnet. Die folgenden Werte sind verfügbar:

  ALl
  : IBM Spectrum Protect exportiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

  None
  : IBM Spectrum Protect exportiert keine Dateien, nur Definitionen.

  ARchive
  : IBM Spectrum Protect exportiert nur archivierte Dateien.

  Backup
  : IBM Spectrum Protect exportiert nur Sicherungsversionen, unabhängig davon, ob die Versionen aktiv oder inaktiv sind.

  BACKUPActive
  : IBM Spectrum Protect exportiert nur aktive Sicherungsversionen.

  ALLActive
  : IBM Spectrum Protect exportiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

  SPacemanaged
  : IBM Spectrum Protect exportiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Preview
: Gibt an, ob die Ergebnisse der Exportoperation vorangezeigt werden sollen, ohne die Informationen zu exportieren. Mit diesem Parameter kann der Umfang der zu übertragenden Daten (Byte) vorangezeigt werden, um zu bestimmen, wie viele Datenträger benötigt werden. Dieser Parameter unterstützt die folgenden Werte:

  No

Gibt an, daß die Server-Informationen exportiert werden sollen. Wird dieser Wert angegeben, muss auch eine Einheitenklasse angegeben werden.

Yes
Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.Wird dieser Wert angegeben, muss keine Einheitenklasse angegeben werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

DEVclass
Gibt die Einheitenklasse an, in die die Exportdaten geschrieben werden sollen. Dieser Parameter ist erforderlich, wenn Sie PREVIEW=NO angeben.

Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Exports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, um ein Laufwerk verfügbar zu machen.

Tipp: Daten können in einen Speicherpool auf einem anderen Server exportiert werden, indem eine Einheitenklasse mit dem Einheitentyp SERVER angegeben wird.

Scratch
Gibt an, ob Arbeitsdatenträger verwendet werden können. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass Arbeitsdatenträger zum Exportieren verwendet werden können. Wird auch eine Liste mit Datenträgern angegeben, werden Arbeitsdatenträger nur verwendet, wenn auf den angegebenen Datenträgern nicht genügend Speicherbereich vorhanden ist.

No
Gibt an, dass keine Arbeitsdatenträger zum Exportieren verwendet werden können. Um zu bestimmen, wie viele Datenträger benötigt werden, können Sie den Befehl mit der Angabe PREVIEW=YES ausführen.

VOLumenames
Gibt die Datenträger an, die zum Speichern der exportierten Daten verwendet werden sollen. Dieser Parameter ist wahlfrei, es sei denn, es wird SCRATCH=NO und PREVIEW=NO angegeben. Wird kein Datenträgername angegeben, werden Arbeitsdatenträger verwendet.

Sie können einen der folgenden Werte angeben:

Datenträgername
Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

FILE: Dateiname
Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Folgende Namenskonventionen bei der Angabe von Datenträgern verwenden, die folgenden Einheitentypen zugeordnet sind:

Für Einheit	**Angeben**
Band	1 - 6 alphanumerische Zeichen.
FILE	Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel: AIX-BetriebssystemeLinux-Betriebssysteme/imdata/mt1. Windows-Betriebssystemed:\Programmdateien\tivoli\tsm\data1.dsm.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme REMOVABLEFILE	AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme1 - 6 alphanumerische Zeichen.
SERVER	1 - 250 alphanumerische Zeichen.

USEDVolumelist
Gibt die Datei an, in der eine Liste der Datenträger gespeichert wird, die in der Exportoperation verwendet werden. Dieser Parameter ist wahlfrei.

Diese Datei kann für die Importoperation verwendet werden. Diese Datei enthält Kommentarzeilen mit dem Exportdatum und der Exportuhrzeit sowie dem Befehl, der zum Erstellen des Exports ausgegeben wurde.

Achtung: Wird eine vorhandene Datei angegeben, wird die Datei überschrieben.

FROMDate
Gibt das früheste Datum an, für das Dateien, die exportiert werden sollen, auf dem Server gespeichert wurden. Dateien, die vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter FROMDATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Verzeichnisverarbeitung: Der Parameter FROMDATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.
Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Gruppendaten auf dem Knoten sind beispielsweise Daten virtueller Maschinen oder Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.
Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY -3 **oder** -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

Wird dieser Parameter nicht angegeben, exportiert IBM Spectrum Protect alle Objekte, die vor dem Datum im Parameter TODATE gespeichert wurden und die durch den Parameter FILEDATA qualifiziert sind. Wird kein Parameter TODATE angegeben, werden alle Daten exportiert, die durch den Parameter FILEDATA qualifiziert sind.

Wenn eine Exportoperation zwischen Servern ein relatives FROMDATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird FROMDATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

TODate

Gibt das späteste Datum für Dateien an, die vom Server exportiert werden sollen. Dateien, die auf dem Server an einem späteren Datum als dem für TODATE angegebenen Datum gespeichert werden, werden nicht exportiert. TODATE gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen.

- IBM Spectrum Protect ignoriert den Parameter TODATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
- Wenn ein Parameter TODATE ohne einen Parameter TOTIME angegeben wird, exportiert der Server alle Objekte, die an oder vor dem durch den Parameter TODATE angegebenen Tag eingefügt wurden.
- Wurde der Parameter FROMDATE angegeben, muss der Wert von TODATE größer-gleich dem Wert von FROMDATE sein. Sind TODATE und FROMDATE gleich, muss der Wert für den Parameter TOTIME größer als der Wert für den Parameter FROMTIME sein.
- Der Parameter TODATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	10/15/2006
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY -3 **oder** -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM

Wert	Beschreibung	Beispiel
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

Wenn eine Exportoperation zwischen Servern ein relatives TODATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird TODATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

FROMTime

Gibt die früheste Uhrzeit an, für die Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Geben Sie FROMTIME an, müssen Sie auch den Parameter FROMDATE verwenden. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. Objekte, die vor der angegebenen Uhrzeit und vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. IBM Spectrum Protect ignoriert den Parameter FROMTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.
Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Beispiele für Gruppendaten auf dem Knoten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Bei Verwendung mit dem Parameter FROMDATE lautet der Standardwert für diesen Parameter Mitternacht (00:00:00).

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.FROMTIME+ kann nur mit einem FROMDATE vor heute verwendet werden.	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW+02:00 oder FROMTIME=+02:00 ausgegeben, enthält die Exportoperation nur Dateien, die nach 7:00 Uhr an dem angegebenen FROMDATE auf den Server gestellt wurden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW -02:00 **oder** -02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW-02:00 oder FROMTIME=-2:00 ausgegeben, enthält der Export Dateien, die nach 3:00 Uhr auf den Server gestellt wurden.

TOTime

Gibt den spätesten Zeitpunkt an, an dem Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Sie müssen den Parameter TODATE angeben, um den Parameter TOTIME verwenden zu können. TOTIME gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter TOTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Bei Verwendung mit dem Parameter TODATE lautet der Standardwert für diesen Parameter Mitternacht minus eine Sekunde (23:59:59).

Wichtig: Die Werte für die Parameter TOTIME und TODATE müssen größer als die Werte für die Parameter FROMDATE und FROMTIME sein.
Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08

Wert	Beschreibung	Beispiel
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW+02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 7 Uhr gespeichert wurden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten.	NOW-02:00 **oder** -02:00. Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW-02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 3 Uhr gespeichert wurden.

ENCryptionstrength
: Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

  AES
  : Gibt den Advanced Encryption Standard an.

  DES
  : Gibt den Data Encryption Standard an.

ALLOWSHREDdable
: Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, dass Daten nicht aus einem Speicherpool exportiert werden, der das Schreddern erzwingt.

  Yes
  : Gibt an, dass Daten aus einem Speicherpool exportiert werden können, der das Schreddern erzwingt. Die Daten auf den Exportdatenträgern werden nicht geschreddert.

Beispiel: Einen Server auf bestimmte Banddatenträger exportieren

Vom Server Server-Informationen auf die Banddatenträger TAPE01, TAPE02 und TAPE03 exportieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
export server devclass=menu1
volumenames=tape01,tape02,tape03
```

Beispiel: Einen Server auf Banddatenträger exportieren, die in einer Datei aufgelistet sind

Vom Server die Serverinformationen auf Banddatenträger exportieren, die in der folgenden Datei aufgelistet sind:

- AIX-BetriebssystemeLinux-BetriebssystemeTAPEVOL
- Windows-BetriebssystemeTAPEVOL.DATA

Die Datei enthält die folgenden Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass die Banddatenträger von einer Einheit verwendet werden, die der Einheitenklasse MENU1 zugeordnet ist. Geben Sie den folgenden Befehl aus:
AIX-BetriebssystemeLinux-Betriebssysteme

```
export server devclass=menu1 volumenames=file:tapevol
```

Windows-Betriebssysteme

```
export server devclass=menu1 volumenames=file:tapevol.data
```

EXPORT SERVER (Serversteuerungsinformationen und Clientdateidaten auf einen anderen Server exportieren)

Mit diesem Befehl können die Serversteuerungsinformationen und Clientdateidaten vollständig oder teilweise direkt auf einen anderen Server in dem Netz exportiert werden. Dies hat einen sofortigen Import auf den Zielserver zur Folge.

Exportoperation zwischen Servern, die einen anderen Wert für FILEDATA als NONE haben, können erneut gestartet werden, nachdem die Operation ausgesetzt wurde. Der Server sichert den Status der Exportoperation, sodass die Exportoperation an dem Punkt erneut gestartet werden kann, an dem sie fehlgeschlagen ist oder an dem sie ausgesetzt wurde. Die Exportoperation kann zu einem späteren Zeitpunkt erneut gestartet werden, indem der Befehl RESTART EXPORT ausgegeben wird. Diese Exportoperationen können manuell ausgesetzt sowie erneut gestartet werden. Schlägt ein Export fehl, wird er daher automatisch ausgesetzt, wenn er die Phase für die Übertragung der Definitionen beendet hat.

Eine Exportoperation wird ausgesetzt, wenn eine der folgenden Bedingungen festgestellt wird:

- Ein Befehl SUSPEND EXPORT wird für die aktive Exportoperation ausgegeben
- Segmentvorableerung - die Datei, die für den Export gelesen wird, wird von einem anderen Prozess gelöscht
- Übertragungsfehler bei einem Export zwischen Servern
- Keine verfügbaren Mountpunkte
- Erforderliche Datenträger sind nicht verfügbar
- E/A-Fehler wurden festgestellt

Die Exportoperation kann nicht erneut gestartet werden, wenn die Exportoperation fehlschlägt, bevor die auswählbaren Knoten- und Dateibereichsdefinitionen auf den Zielserver übertragen werden. Sie müssen den Befehl erneut eingeben, um eine neue Exportoperation zu beginnen.

Geben Sie den Befehl QUERY PROCESS auf dem Zielserver aus, um den Fortschritt der Importoperation zu überwachen. Geben Sie den Befehl QUERY EXPORT aus, um alle aktiven oder ausgesetzten Exportoperationen zwischen Servern aufzulisten (die einen anderen Wert für FILEDATA als NONE haben). In EXPORT ADMIN (Administratorinformationen exportieren) finden Sie eine Liste der Einschränkungen, die für die Exportfunktion gelten.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                  .-FILEData--=--None-------------.
>>-EXPort Server--+-------------------------------+-------------><
                  '-FILEData--=--+-ALl----------+-'
                                 +-None---------+
                                 +-ARchive------+
                                 +-Backup-------+
                                 +-BACKUPActive-+
                                 +-ALLActive----+
                                 '-SPacemanaged-'

>--+-------------------------------------------------+------------><
   |                      .-FROMTime--=--00:00:00-. |
   '-FROMDate--=--Datum--+-----------------------+-'
                         '-FROMTime--=--Zeit-----'

>--+-----------------------------------------+----------------><
   |                   .-TOTime--=--23:59:59-. |
   '-TODate--=--Datum--+---------------------+-'
                       '-TOTime--=--Zeit-----'

>--+---------------------------------+--------------------------><
   '-EXPORTIDentifier--=--Export-ID-'

                                .-PREVIEWImport--=--No------.
>--+-------------------------+--+---------------------------+--><
   '-TOServer--=--Servername-'  '-PREVIEWImport--=--+-No--+-'
                                                   '-Yes-'

   .-MERGEfilespaces--=--No------.
>--+-----------------------------+-----------------------------><
   '-MERGEfilespaces--=--+-No--+-'
                         '-Yes-'

   .-Replacedefs--=--No------.
>--+-------------------------+-------------------------------><
   '-Replacedefs--=--+-No--+-'
                     '-Yes-'

   .-PROXynodeassoc--=--No------.
>--+----------------------------+------------------------------><
   '-PROXynodeassoc--=--+-No--+-'
                        '-Yes-'
```

```
   .-ENCryptionstrength--=--AES-----.
>--+-------------------------------+-------------------------->
   '-ENCryptionstrength--=--+-AES-+-'
                            '-DES-'

   .-ALLOWSHREDdable---=--No------.
>--+-----------------------------+----------------------------><
   '-ALLOWSHREDdable---=--+-No--+-'
                          '-Yes-'
```

Parameter

FILEData

Gibt den Typ der Dateien an, die für alle Knoten exportiert werden sollen, die für den Server definiert sind. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

Export auf sequenzielle Datenträger: Die Einheitenklasse für den Zugriff auf die Dateidaten wird durch die Einheitenklasse des Speicherpools bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, benötigt IBM Spectrum Protect zwei Laufwerke zum Exportieren von Serverinformationen. Sie müssen den Grenzwert für Ladeanforderungen für die Einheitenklasse auf mindestens 2 setzen.

In den folgenden Beschreibungen werden aktive und inaktive Versionen von Sicherungsdateien erwähnt. Eine aktive Version einer Sicherungsdatei ist die aktuellste Sicherungsversion für eine Datei, die noch auf der Client-Workstation vorhanden ist. Alle anderen Versionen der Sicherungsdatei werden als inaktive Kopien bezeichnet. Gültige Werte:

ALl
: IBM Spectrum Protect exportiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

None
: IBM Spectrum Protect exportiert keine Dateien, nur Definitionen.

ARchive
: IBM Spectrum Protect exportiert nur archivierte Dateien.

Backup
: IBM Spectrum Protect exportiert nur Sicherungsversionen, unabhängig davon, ob sie aktiv oder inaktiv sind.

BACKUPActive
: IBM Spectrum Protect exportiert nur aktive Sicherungsversionen.

ALLActive
: IBM Spectrum Protect exportiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

SPacemanaged
: IBM Spectrum Protect exportiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

FROMDate

Gibt das früheste Datum an, für das Dateien, die exportiert werden sollen, auf dem Server gespeichert wurden. Dateien, die vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter FROMDATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
Verzeichnisverarbeitung: Der Parameter FROMDATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.
Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Gruppendaten auf dem Knoten sind beispielsweise Daten virtueller Maschinen oder Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.
Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY -3 **oder** -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM

Wert	Beschreibung	Beispiel
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

Wird dieser Parameter nicht angegeben, exportiert IBM Spectrum Protect alle Objekte, die vor dem Datum im Parameter TODATE gespeichert wurden und die durch den Parameter FILEDATA qualifiziert sind. Wird kein Parameter TODATE angegeben, werden alle Daten exportiert, die durch den Parameter FILEDATA qualifiziert sind.

Wenn eine Exportoperation zwischen Servern ein relatives FROMDATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird FROMDATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

TODate

Gibt das späteste Datum für Dateien an, die vom Server exportiert werden sollen. Dateien, die auf dem Server an einem späteren Datum als dem für TODATE angegebenen Datum gespeichert werden, werden nicht exportiert. TODATE gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen.

- IBM Spectrum Protect ignoriert den Parameter TODATE, wenn der Parameter FILEDATA auf NONE gesetzt ist.
- Wenn ein Parameter TODATE ohne einen Parameter TOTIME angegeben wird, exportiert der Server alle Objekte, die an oder vor dem durch den Parameter TODATE angegebenen Tag eingefügt wurden.
- Wurde der Parameter FROMDATE angegeben, muss der Wert von TODATE größer-gleich dem Wert von FROMDATE sein. Sind TODATE und FROMDATE gleich, muss der Wert für den Parameter TOTIME größer als der Wert für den Parameter FROMTIME sein.
- Der Parameter TODATE gilt nicht für Verzeichnisse. Alle Verzeichnisse in einem Dateibereich werden verarbeitet, auch wenn die Verzeichnisse nicht in dem angegebenen Datumsbereich gesichert wurden.

Verwenden Sie einen der folgenden Werte, um das Datum anzugeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	10/15/2006
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY -3 **oder** -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

Wenn eine Exportoperation zwischen Servern ein relatives TODATE verwendet, wie beispielsweise TODAY-1, und die Operation an einem späteren Datum erneut gestartet wird, verwendet der erneut gestartete Prozess dennoch das Datum, das während der ursprünglichen Operation verwendet wurde. Wird beispielsweise eine Exportoperation zwischen Servern am 04.07.2009 gestartet und wird TODATE als TODAY-1 angegeben, ist das für die Auswahl von Dateien verwendete Datum der 03.07.2009. Wird diese Exportoperation ausgesetzt und zehn Tage später (14.07.2009) erneut gestartet, ist das für die Auswahl von Dateien verwendete Datum dennoch der 03.07.2009. Mit diesem Verhalten wird sichergestellt, dass die gesamte Exportoperation dasselbe Stichdatum für die Auswahl der zu exportierenden Dateien verwendet.

FROMTime

Gibt die früheste Uhrzeit an, für die Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Geben Sie FROMTIME an, müssen Sie auch den Parameter FROMDATE verwenden. Dieser Parameter gilt nur für Clientdateidaten. Dieser Parameter hat keine Auswirkungen auf andere Informationen, die möglicherweise exportiert werden, wie beispielsweise Maßnahmen. Objekte, die vor der angegebenen Uhrzeit und vor dem angegebenen Datum auf dem Server gespeichert wurden, werden nicht exportiert. IBM Spectrum Protect ignoriert den Parameter FROMTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.
Wichtig: Befinden sich Gruppendaten auf dem Knoten, den Sie exportieren, können Daten, die vor dem angegebenen FROMDATE und vor der angegebenen FROMTIME gesichert wurden, ebenfalls exportiert werden. Beispiele für Gruppendaten auf dem Knoten sind Daten virtueller Maschinen und Systemstatussicherungsdaten. Dieser Export ist ein Ergebnis der Teilsicherungsverarbeitung für die Daten. Die Teilsicherungsverarbeitung kann zur Folge haben, dass zusätzliche Dateien, die nicht den Filterkriterien entsprechen, exportiert werden, sodass ein konsistentes Image für die Sicherungsdaten vorhanden ist.

Bei Verwendung mit dem Parameter FROMDATE lautet der Standardwert für diesen Parameter Mitternacht (00:00:00).

Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.FROMTIME+ kann nur mit einem FROMDATE vor heute verwendet werden.	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW+02:00 oder FROMTIME=+02:00 ausgegeben, enthält die Exportoperation nur Dateien, die nach 7:00 Uhr an dem angegebenen FROMDATE auf den Server gestellt wurden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW -02:00 **oder** -02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe FROMTIME=NOW-02:00 oder FROMTIME=-2:00 ausgegeben, enthält der Export Dateien, die nach 3:00 Uhr auf den Server gestellt wurden.

TOTime

Gibt den spätesten Zeitpunkt an, an dem Objekte, die exportiert werden sollen, auf dem Server gespeichert wurden. Sie müssen den Parameter TODATE angeben, um den Parameter TOTIME verwenden zu können. TOTIME gilt nur für Clientdateidaten und hat keinen Einfluss auf andere Informationen, die exportiert werden, wie beispielsweise Maßnahmen. IBM Spectrum Protect ignoriert den Parameter TOTIME, wenn der Parameter FILEDATA auf NONE gesetzt ist.

Bei Verwendung mit dem Parameter TODATE lautet der Standardwert für diesen Parameter Mitternacht minus eine Sekunde (23:59:59).

Wichtig: Die Werte für die Parameter TOTIME und TODATE müssen größer als die Werte für die Parameter FROMDATE und FROMTIME sein.
Verwenden Sie einen der folgenden Werte, um die Zeit anzugeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW+02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 7 Uhr gespeichert wurden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten.	NOW-02:00 **oder** -02:00. Wird dieser Befehl um 5 Uhr mit FROMTIME=01:00 und TOTIME=NOW-02:00 ausgegeben, werden beim Export Dateien eingeschlossen, die von 1 Uhr bis 3 Uhr gespeichert wurden.

TOServer

Gibt den Namen eines Servers an, an den die Exportdaten direkt über das Netz für den sofortigen Import gesendet werden.
Wichtig: Der Zielserver muss mit dem Befehl DEFINE SERVER auf dem Ursprungsserver definiert werden. Der Administrator, der den Exportbefehl ausgibt, muss mit demselben Administratornamen und demselben Kennwort definiert werden und muss auf dem Zielserver über die Systemberechtigung verfügen.

Wenn Sie TOSERVER angeben, können Sie nicht die Parameter DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST und PREVIEW angeben.

PREVIEWImport

Gibt an, ob der Umfang der zu übertragenden Daten angezeigt werden soll, ohne die Daten tatsächlich zu versetzen. Mit diesen Informationen kann bestimmt werden, welcher Speicherpoolbereich auf dem Zielserver benötigt wird. Der Standardwert ist NO. Gültige Werte sind:

Yes
: Gibt an, dass die Ergebnisse der Importoperation auf dem Zielserver vorangezeigt werden sollen, ohne dass die Daten importiert werden. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.

No
: Gibt an, dass die Daten in den Zielserver importiert werden sollen, ohne dass die Ergebnisse vorangezeigt werden.

MERGEfilespaces
: Gibt an, ob IBM Spectrum Protect Clientdateien in vorhandene Dateibereiche auf dem Zielserver mischt (sofern sie vorhanden sind) oder ob IBM Spectrum Protect neue Dateibereichsnamen generiert. Der Standardwert ist NO.

Gültige Werte sind:

Yes
: Gibt an, dass importierte Daten auf dem Zielserver in den vorhandenen Dateibereich gemischt werden, wenn ein Dateibereich mit demselben Namen auf dem Zielserver vorhanden ist.

No
: Gibt an, dass IBM Spectrum Protect einen neuen Dateibereichsnamen für importierte Daten auf dem Zielserver generiert, wenn Dateibereiche mit demselben Namen vorhanden sind.

Replacedefs
: Gibt an, ob Definitionen (nicht Dateidaten) auf dem Server ersetzt werden sollen. Der Standardwert ist NO.

Gültige Werte sind:

Yes
: Gibt an, dass Definitionen auf dem Server ersetzt werden, wenn Definitionen mit demselben Namen wie die zu importierenden Definitionen auf dem Zielserver vorhanden sind.

No
: Gibt an, dass importierte Definitionen übersprungen werden, wenn ihre Namen mit Definitionen in Konflikt stehen, die bereits auf dem Zielserver definiert sind.

PROXynodeassoc
: Gibt an, ob Proxyknotenzuordnungen exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

ENCryptionstrength
: Gibt an, welcher Algorithmus für die Verschlüsselung von Kennwörtern verwendet werden soll, wenn Verwaltungs- und Knotensätze exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist AES. Erfolgt der Export auf einen Server, der AES nicht unterstützt, geben Sie DES an. Sie können einen der folgenden Werte angeben:

AES
: Gibt den Advanced Encryption Standard an.

DES
: Gibt den Data Encryption Standard an.

ALLOWSHREDdable
: Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No
: Gibt an, dass es der Server nicht erlaubt, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden.

Yes
: Gibt an, dass es der Server erlaubt, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, exportiert werden. Die Daten auf den Exportdatenträgern werden nicht geschreddert.

Wichtig: Nachdem eine Exportoperation die Identifizierung von Dateien für den Export beendet hat, werden alle Änderungen des Werts ALLOWSHREDABLE für den Speicherpool ignoriert. Eine Exportoperation, die ausgesetzt ist, behält während der gesamten Operation den ursprünglichen ALLOWSHREDABLE-Wert. Möglicherweise möchten Sie Ihre Exportoperation abbrechen, wenn Änderungen des Werts ALLOWSHREDABLE für den Speicherpool die Operation gefährden. Sie können den Exportbefehl nach einer erforderlichen Bereinigung erneut ausgeben.

EXPORTIDentifier
: Dieser optionale Parameter gibt den Namen an, den Sie zum Identifizieren dieser Exportoperation ausgewählt haben. Geben Sie keinen Befehlsnamen an, wird vom Server ein Name generiert. Die Export-ID darf 64 Zeichen nicht überschreiten, darf keine Platzhalterzeichen enthalten, und ist nicht von der Groß-/Kleinschreibung abhängig. Mit dieser ID können Sie auf Exportoperationen in den Befehlen QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT oder CANCEL EXPORT verweisen. EXPORTIDENTIFIER wird bei FILEDATA=NONE oder PREVIEWIMPORT=YES ignoriert.

Geben Sie den Parameter EXPORTIDENTIFIER an, müssen Sie den Parameter TOSERVER angeben.

Beispiel: Serverinformationen direkt auf einen anderen Server exportieren

Um Serverinformationen direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus.

```
export server filedata=all toserver=serverb
```

Beispiel: Serverinformationen unter Verwendung eines Datumsbereichs direkt auf einen anderen Server exportieren

Um Serverinformationen zwischen dem 1. Februar 2009 und heute direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus.

```
export server filedata=all toserver=serverbfromdate=02/01/2009 todate=today
```

Beispiel: Serverinformationen und Clientdateidaten unter Verwendung eines Datums- und Zeitbereichs direkt auf einen anderen Server exportieren

Um Serverinformationen zwischen dem 1. Februar 2009 um 8 Uhr bis heute um 8 Uhr direkt auf SERVERB zu exportieren, geben Sie den folgenden Befehl aus.

```
export server filedata=all toserver=serverbfromdate=02/01/2009 fromtime=08:00:00
todate=today totime=08:00:00
```

EXTEND DBSPACE (Speicherbereich für die Datenbank erhöhen)

Verwenden Sie diesen Befehl, um den Speicherbereich für die Datenbank zu vergrößern, indem Verzeichnisse für die Datenbank hinzugefügt werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Wenn Sie den Befehl EXTEND DBSPACE ausgeben, werden der Datenbank Verzeichnisse hinzugefügt. Mit den Standardparametereinstellungen werden Daten auf alle Datenbankverzeichnisse verteilt, und Speicherbereich wird zurückgefordert. Mit dieser Aktion wird die Leistung der parallelen E/A verbessert und der neue Verzeichnisbereich für die sofortige Verwendung zur Verfügung gestellt.

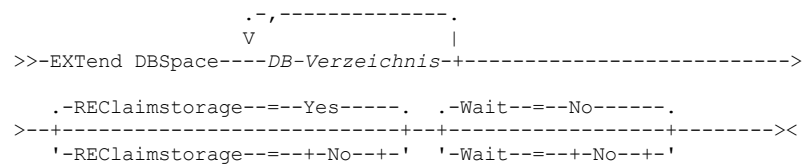
Sollen Daten nicht erneut verteilt werden, wenn Sie neue Verzeichnisse hinzufügen, können Sie `RECLAIMSTORAGE=NO` angeben. Wenn Sie für diesen Parameter `No` angeben, wird der gesamte Speicherbereich in vorhandenen Verzeichnissen gefüllt, bevor neue Verzeichnisse verwendet werden. Sie können später Daten erneut verteilen und Speicherbereich zurückfordern, aber Sie müssen die manuelle Prozedur für diese Task mit DB2-Befehlen ausführen.

Einschränkung: Die Neuverteilung von Daten und die Zurückforderung von Speicherbereich als Teil einer Operation zum Erweitern des Datenbankbereichs funktioniert nur mit DB2-Tabellenbereichen der Version 9.7 oder höher. Die Tabellenbereiche werden erstellt, wenn Sie einen neuen IBM Spectrum Protect-Server der Version 6.2 oder höher formatieren. Wenn Sie für Ihren IBM Spectrum Protect-Server ein Upgrade von Version 6.1 durchgeführt oder Ihren Server aus Version 6.1 zurückgeschrieben haben, können Sie Daten nicht erneut verteilen und Speicherbereich nicht zurückfordern. Sie müssen den Befehl EXTEND DBSPACE mit `RECLAIMSTORAGE=NO` ausgeben.
Wichtig: Bei dem Neuverteilungsprozess werden erhebliche Systemressourcen verwendet. Planen Sie dies ein, wenn der Datenbank Speicherbereich hinzugefügt werden soll. Beachten Sie die folgenden Richtlinien:

- Führen Sie den Prozess aus, wenn der Server keine hohe Arbeitslast verarbeitet.
- Die Zeit, die erforderlich ist, um Daten erneut zu verteilen und Speicherbereich zurückzufordern, kann variieren. Sie wird durch Faktoren beeinflusst, wie z. B. Dateisystemlayout, Verhältnis neuer Pfade zu vorhandenen Speicherpfaden, Server-Hardware und Parallelbetrieb. Um eine grobe Schätzung zu erhalten, können Sie die Operation mit einer kleinen IBM Spectrum Protect-Datenbank auf einem Übungssystem testen. Verwenden Sie Ihre Ergebnisse als Referenz, um die Zeit zu schätzen, die für die Prozedur erforderlich ist.
- Unterbrechen Sie nicht den Neuverteilungsprozess. Wenn Sie versuchen, den Prozess zu stoppen, indem Sie z. B. den Prozess anhalten, der die Arbeit ausführt, müssen Sie den DB2-Server stoppen und erneut starten. Wenn der Server erneut gestartet wird, wechselt er in den Modus für die Wiederherstellung nach einem Systemabsturz. Dies dauert einige Minuten. Danach wird der Neuverteilungsprozess fortgesetzt.

Nachdem eine Operation zum Erweitern des Datenbankbereichs ausgeführt wurde, halten Sie den Server an und starten Sie ihn erneut, um die neuen Verzeichnisse vollständig zu verwenden. Sind die vorhandenen Datenbankverzeichnisse nahezu voll, wenn ein neues Verzeichnis hinzugefügt wird, kann der Server eine Bedingung 'Kein Speicherbereich verfügbar' feststellen (wird in der Datei db2diag.log angegeben). Sie können die Bedingung 'Kein Speicherbereich verfügbar' beseitigen, indem der Server angehalten und erneut gestartet wird.

Syntax



```
                    '-Yes-'              '-Yes-'
```

Parameter

DB-Verzeichnis (Erforderlich)
: Gibt die Verzeichnisse für den Datenbankspeicher an. Die Verzeichnisse müssen leer sein und auf die Verzeichnisse muss durch die Benutzer-ID des Datenbankmanagers zugegriffen werden können. Ein Verzeichnisname muss ein vollständig qualifizierter Name sein und darf 175 Zeichen nicht überschreiten. Schließen Sie den Namen in Anführungszeichen ein, wenn er eingebettete Leerzeichen, ein Gleichheitszeichen oder andere Sonderzeichen enthält. Wenn Sie eine Verzeichnisliste für den Datenbankspeicher angeben, beträgt die maximale Länge der Liste 1400 Zeichen.
 Windows-BetriebssystemeEinschränkung: Sie können keine Pfade mit allgemeiner Namenskonvention angeben.
Tipp: Geben Sie Verzeichnisse an, die dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank.

REClaimstorage
: Gibt an, ob Daten auf neu erstellte Datenbankverzeichnisse erneut verteilt werden und Speicherbereich aus den alten Speicherpfaden zurückgefordert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 'Yes'.

  Die Operation wird als Hintergrundprozess ausgeführt, wenn nicht `WAIT=YES` angegeben wird.

  Yes
  : Gibt an, dass Daten erneut verteilt werden, sodass neue Verzeichnisse für die sofortige Verwendung verfügbar sind.
    Wichtig: Bei dem Neuverteilungsprozess werden erhebliche Systemressourcen verwendet. Planen Sie dies im Voraus ein.

    Nach dem Starten des Prozesses werden Nachrichten ausgegeben, die den Fortschritt angeben. Sie können den Befehl QUERY PROCESS verwenden, um die Operation zu überwachen. Um den Prozess abzubrechen, können Sie den Befehl CANCEL PROCESS verwenden. Ist jedoch eine Operation zur Neuverteilung von Daten aktiv, wird sie beendet, bevor der Prozess gestoppt wird.

  No
  : Gibt an, dass Daten nicht auf Datenbankverzeichnisse erneut verteilt werden und Speicherbereich nicht zurückgefordert wird, wenn Speicherbereich für die Datenbank hinzugefügt wird.

Wait
: Gibt an, ob dieser Befehl im Hintergrund oder Vordergrund verarbeitet wird.

  No
  : Gibt die Hintergrundverarbeitung an. Der Standardwert ist NO.

  Yes
  : Gibt die Vordergrundverarbeitung an.

     AIX-Betriebssysteme  Linux-BetriebssystemeYES kann nicht von der Server-Konsole aus angegeben werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme

Beispiel: Verzeichnisse zum Speicherbereich für die Datenbank hinzufügen, Daten erneut verteilen und Speicher zurückfordern

Zwei Verzeichnisse (/tsm_db/stg1 und tsm_db/stg2) unter dem Verzeichnis /tsm_db zum Speicherbereich für die Datenbank hinzufügen. Den folgenden Befehl ausgeben:

```
extend dbspace /tsm_db/stg1,/tsm_db/stg2
```

 Windows-Betriebssysteme

Beispiel: Laufwerke zum Speicherbereich für die Datenbank hinzufügen, Daten erneut verteilen und Speicher zurückfordern

Die Laufwerke D und E zum Speicherbereich der Datenbank hinzufügen. Den folgenden Befehl ausgeben:

```
extend dbspace D:,E:
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für EXTEND DBSPACE

Befehl	Beschreibung
DSMSERV EXTEND DBSPACE	Fügt Verzeichnisse hinzu, um den Speicherbereich für die Verwendung durch die Datenbank zu vergrößern.
QUERY DB	Zeigt Zuordnungsinformationen zu der Datenbank an.

Befehl	Beschreibung
QUERY DBSPACE	Zeigt Informationen zum Speicherplatz an, der für die Datenbank definiert ist.

Zugehörige Tasks:
Bestandskapazität verwalten

GENERATE-Befehle

Verwenden Sie die GENERATE-Befehle für Sicherungsgruppen für einen ausgewählten Dateibereich oder Clientknoten.

- GENERATE BACKUPSET (Sicherungsgruppe mit Daten des Clients für Sichern/Archivieren generieren)
- GENERATE BACKUPSETTOC (Inhaltsverzeichnis für eine Sicherungsgruppe generieren)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeGENERATE DEDUPSTATS (Datendeduplizierungsstatistikdaten generieren)

GENERATE BACKUPSET (Sicherungsgruppe mit Daten des Clients für Sichern/Archivieren generieren)

Verwenden Sie diesen Befehl, um eine Sicherungsgruppe für einen Knoten des Clients für Sichern/Archivieren zu generieren. Eine *Sicherungsgruppe* ist eine Sammlung der aktiven gesicherten Daten eines Clients für Sichern/Archivieren, die als ein einzelnes Objekt auf bestimmten Datenträgern im Serverspeicher gespeichert und verwaltet wird. Obwohl Sie eine Sicherungsgruppe für jeden Clientknoten erstellen können, kann eine Sicherungsgruppe nur von einem Client für Sichern/Archivieren verwendet werden.

Einschränkung: Eine Sicherungsgruppe im "Deduplizierungsformat" trägt diese Bezeichnung infolge eines Befehls GENERATE BACKUPSET mit mindestens einer der folgenden Spezifikationen:

- Schließt einen Knoten des Clients für Sichern/Archivieren mit Version 6.1.x ein (mindestens Version 6.1.0, aber niedriger als Version 6.2.0).
- Schließt einen Knoten ein, der über einen oder mehrere Knoten verfügt, die berechtigt sind, als Proxy zu agieren. Mindestens einer dieser Proxy-Knoten hat die Version 6.1.x des Clients für Sichern/Archivieren.

Sicherungsgruppen im Deduplizierungsformat können nur von dem Client für Sichern/Archivieren mit Version 6.1.2 oder höher zurückgeschrieben werden. Clients für Sichern/Archivieren vor Version 6.1.2 können keine Zurückschreibung aus einer Sicherungsgruppe ausführen, die das Deduplizierungsformat hat.
Eine Sicherungsgruppe im "verteilten Deduplizierungsformat" trägt diese Bezeichnung infolge eines Befehls GENERATE BACKUPSET mit mindestens einer der folgenden Spezifikationen:

- Schließt einen Knoten des Clients für Sichern/Archivieren mit Version 6.2.0 oder höher ein.
- Schließt einen Knoten ein, der über einen oder mehrere Knoten verfügt, die berechtigt sind, als Proxy zu agieren. Mindestens einer dieser Proxy-Knoten hat die Version 6.2.0 des Clients für Sichern/Archivieren.

Sicherungsgruppen im verteilten Deduplizierungsformat können nur von dem Client für Sichern/Archivieren mit Version 6.2.0 oder höher zurückgeschrieben werden.
Einschränkung: Sie können keine Sicherungsgruppe mit Dateien generieren, die unter Verwendung von NDMP in IBM Spectrum Protect gesichert wurden. Sie können jedoch eine Sicherungsgruppe mit Dateien erstellen, die unter Verwendung der NetApp-Momentaufnahmedifferenz gesichert wurden.

Der Server erstellt Kopien von aktiven Versionen der gesicherten Objekte eines Clients, die sich innerhalb eines oder mehrerer Dateibereiche befinden, die mit diesem Befehl angegeben werden. Der Server fasst diese Kopien dann auf sequenziellen Datenträgern zusammen. Gegenwärtig umfassen die für Sicherungsgruppen unterstützten Sicherungsobjekttypen nur Verzeichnisse und Dateien.

Der Knoten des Clients für Sichern/Archivieren kann die Sicherungsgruppe von dem Server und von den Datenträgern zurückschreiben, auf die die Sicherungsgruppe geschrieben wurde.

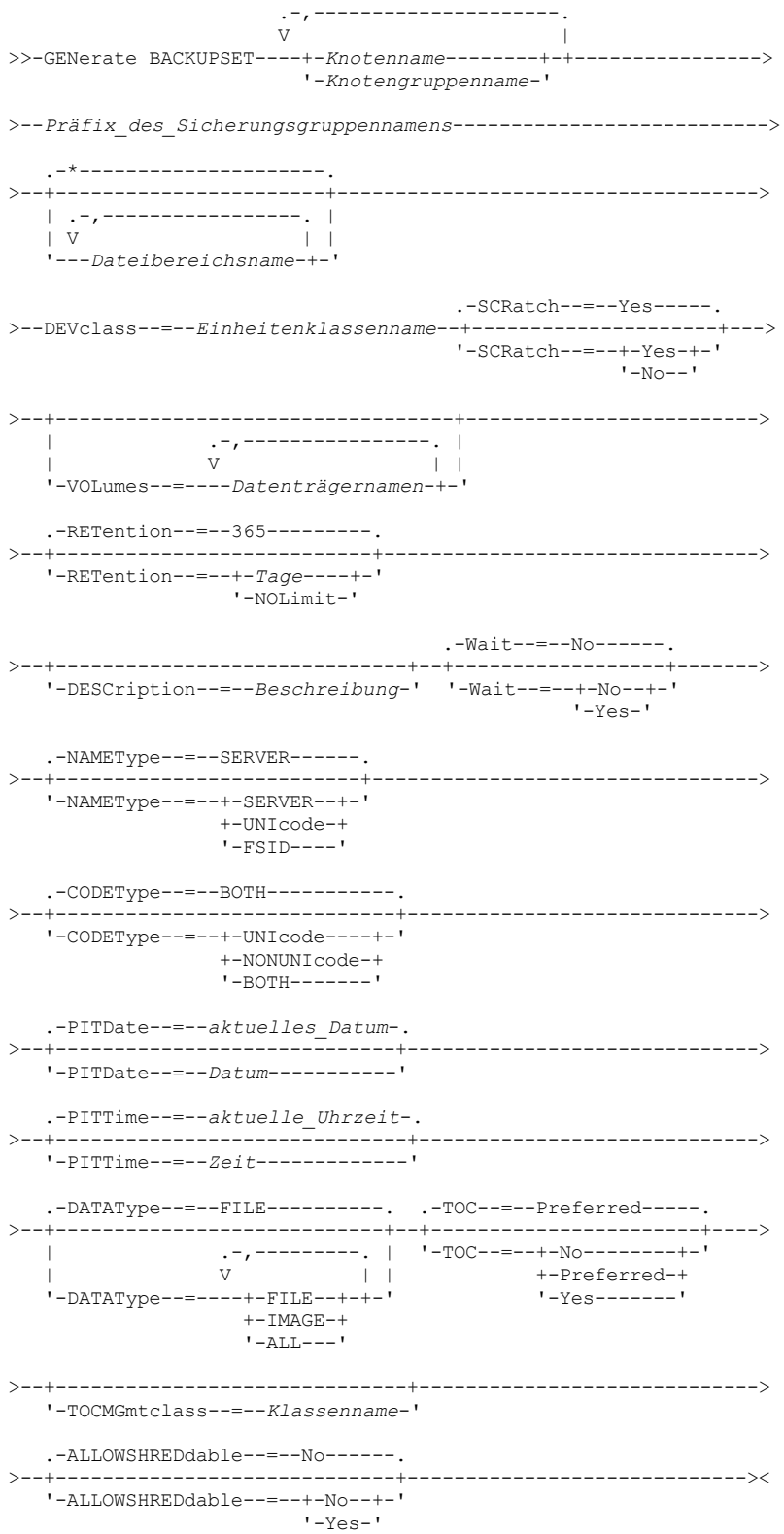
Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wird der durch diesen Befehl erstellte Hintergrundprozess abgebrochen, enthalten die Datenträger möglicherweise keine vollständige Sicherungsgruppe. Mit dem Befehl QUERY PROCESS können Informationen zu dem Hintergrundprozess angezeigt werden, der durch diesen Befehl erstellt wird.

Tipp: Wenn IBM Spectrum Protect eine Sicherungsgruppe generiert, können Sie die Leistung verbessern, wenn die primären Speicherpools, die die Clientdaten enthalten, zusammengefasst werden. Wird ein primärer Speicherpool zusammengefasst, befinden sich die Clientknotendaten wahrscheinlich auf weniger Banddatenträger als dies der Fall wäre, wenn der Speicherpool nicht zusammengefasst würde. Mit der Kollokation wird weniger Zeit für die Suche nach Datenbankeinträgen benötigt, und es sind weniger Ladeoperationen erforderlich.

Berechtigungsklasse

Um diesen Befehl ausgeben zu können, müssen Benutzer die Systemberechtigung oder Maßnahmenberechtigung für die Domäne haben, der der Client-Knoten zugeordnet ist.

Syntax



Parameter

Knotenname oder Knotengruppenname (Erforderlich)

Gibt den Namen des Clientknotens und der Knotengruppe an, dessen bzw. deren Daten in der Sicherungsgruppe enthalten sind. Sollen mehrere Knotennamen und Knotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen für Knotennamen, aber nicht für Knotengruppennamen verwenden. Werden mehrere

Knotennamen angegeben, generiert der Server eine Sicherungsgruppe für jeden Knoten und stellt alle Sicherungsgruppen in eine einzelne Gruppe von Ausgabedatenträgern.

Präfix_des_Sicherungsgruppennamens (Erforderlich)
Gibt den Namen der Sicherungsgruppe für den Client-Knoten an. Die maximale Länge des Namens beträgt 30 Zeichen.

Wird ein Name ausgewählt, fügt IBM Spectrum Protect ein Suffix hinzu, um den Sicherungsgruppennamen zu erstellen. Wird die Sicherungsgruppe beispielsweise *mybackupset* genannt, fügt IBM Spectrum Protect eine eindeutige Zahl wie beispielsweise 3099 zum Namen hinzu. Der Sicherungsgruppenname wird dann für IBM Spectrum Protect als *mybackupset.3099* identifiziert. Sollen später Informationen zu dieser Sicherungsgruppe angezeigt werden, kann in dem Namen ein Platzhalterzeichen wie beispielsweise *mybackupset.** eingefügt oder der vollständig qualifizierte Name wie beispielsweise *mybackupset.3099* angegeben werden.

Werden mehrere Knotennamen oder Knotengruppennamen angegeben, generiert der Server eine Sicherungsgruppe für jeden Knoten oder für jede Knotengruppe und stellt alle Sicherungsgruppen in eine einzelne Gruppe von Ausgabedatenträgern. Jeder Sicherungsgruppe wird derselbe vollständig qualifizierte Name zugeordnet, der aus dem *Präfix_des_Sicherungsgruppennamen*s und einem Suffix besteht, das vom Server bestimmt wird.

Dateibereichsname
Gibt die Namen der Dateibereiche an, die die Daten enthalten, die in der Sicherungsgruppe berücksichtigt werden sollen. Dieser Parameter ist wahlfrei. Der angegebene Dateibereichsname kann Platzhalterzeichen enthalten. Es können mehrere Dateibereiche angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Dateibereich angegeben, werden Daten aus allen gesicherten und aktiven Dateibereichen der Clientknoten in der Sicherungsgruppe berücksichtigt.

Für einen Server, der über Clients mit Unterstützung für Unicode-fähige Dateibereiche verfügt, können Sie entweder einen Dateibereichsnamen oder eine Dateibereichs-ID (FSID) eingeben. Wird ein Dateibereichsname eingegeben, muss der Server möglicherweise den eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich unter dem Parameter NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

DEVclass (Erforderlich)
Gibt den Namen der Einheitenklasse für die Datenträger an, auf die die Sicherungsgruppe geschrieben wird. Die maximale Länge des Namens beträgt 30 Zeichen.
Einschränkung: Sie können keine Einheitenklasse mit dem Einheitentyp NAS oder CENTERA angeben.

SCRatch
Gibt an, ob Arbeitsdatenträger für die Sicherungsgruppe verwendet werden sollen. Wird im Parameter VOLUMES eine Datenträgerliste angegeben, werden Arbeitsdatenträger von dem Server nur verwendet, wenn die Daten nicht auf die angegebenen Datenträger passen. Der Standardwert ist SCRATCH=YES. Gültige Werte:

YES
Gibt an, dass Arbeitsdatenträger für die Sicherungsgruppe verwendet werden sollen.

NO
Gibt an, dass keine Arbeitsdatenträger für die Sicherungsgruppe verwendet werden sollen.

VOLumes
Gibt die Namen der Datenträger an, die die Sicherungsgruppe enthalten sollen. Dieser Parameter ist wahlfrei. Es können mehrere Datenträger angegeben werden, die ohne Leerzeichen durch ein Komma voneinander getrennt werden.

Wird dieser Parameter nicht angegeben, werden Arbeitsdatenträger für die Sicherungsgruppe verwendet.

RETention
Gibt die Anzahl der Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt werden soll. Sie können eine ganze Zahl von 0 bis 30000 angeben. Der Standardwert ist 365 Tage. Gültige Werte:

Tage
Gibt die Anzahl der Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt werden soll.

NOLimit
Gibt an, dass die Sicherungsgruppe auf dem Server unbegrenzt aufbewahrt werden soll.

Wird NOLIMIT angegeben, werden die Datenträger mit der Sicherungsgruppe vom Server unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datenträger aus dem Serverspeicher.

DESCription
Gibt die Beschreibung an, die der Sicherungsgruppe zugeordnet werden soll. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

Wait
Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

Yes
Gibt an, dass der Befehl im Vordergrund verarbeitet wird. Erstellte Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist. Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

No
Gibt an, dass der Befehl im Hintergrund verarbeitet wird. Mit dem Befehl QUERY PROCESS kann die Hintergrundverarbeitung dieses Befehls überwacht werden.

NAMEType
Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode-aktivierte Dateibereiche verfügt. Sie können diesen Parameter für IBM Spectrum Protect-Clients angeben, die die Betriebssysteme Windows, NetWare oder Macintosh OS X verwenden.

Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Gültige Werte:

SERVER
Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.
UNIcode
Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.
FSID
Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).
Wichtig: Gehen Sie bei der Angabe dieses Parameters mit Vorsicht vor, wenn auch mehrere Knotennamen angegeben werden. Verschiedene Knoten können dieselbe Dateibereichs-ID für verschiedene Dateibereiche verwenden oder können verschiedene Dateibereichs-IDs für denselben Dateibereichsnamen verwenden. Wird daher eine Dateibereichs-ID als Dateibereichsname angegeben, kann dies zur Folge haben, dass für einige Knoten die falschen Daten in die Sicherungsgruppe geschrieben werden.

CODEType
Angeben, welche Art von Dateibereichen in der Operation berücksichtigt werden soll. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben oder wenn Sie keine Dateibereichsnamen angeben. Gültige Werte:

UNIcode
Nur Dateibereiche einschließen, die in Unicode sind.
NONUNIcode
Nur Dateibereiche einschließen, die nicht in Unicode sind.
BOTH
Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

PITDate
Gibt an, dass Dateien, die an dem angegebenen Datum aktiv waren und die noch auf dem IBM Spectrum Protect-Server gespeichert sind, in die Sicherungsgruppe eingeschlossen werden sollen, auch wenn sie zum Zeitpunkt der Befehlsausgabe inaktiv sind. Dieser Parameter ist wahlfrei. Der Standardwert ist das Datum, an dem der Befehl GENERATE BACKUPSET ausgeführt wird. Sie können das Datum mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage	TODAY-7 oder -7. Um Dateien einzuschließen, die vor einer Woche aktiv waren, geben Sie PITDATE=TODAY-7 oder PITDATE=-7 an.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

PITTime
Gibt an, dass Dateien, die zu der angegebenen Uhrzeit aktiv waren und die noch auf dem IBM Spectrum Protect-Server gespeichert sind, in die Sicherungsgruppe eingeschlossen werden sollen, auch wenn sie zum Zeitpunkt der Befehlsausgabe inaktiv sind. Dieser Parameter ist wahlfrei. Wurde ein PITDate angegeben, ist der Standardwert Mitternacht (00:00:00); andernfalls ist der Standardwert die Uhrzeit, zu der der Befehl GENERATE BACKUPSET gestartet wird. Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen PIT-Datum	12:33:28
NOW	Die aktuelle Uhrzeit am angegebenen PIT-Datum	NOW
NOW+HH:MM oder +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen PIT-Datum	NOW+03:00 oder +03:00 Wird dieser Befehl um 9:00 Uhr mit der Angabe PITTIME=NOW+03:00 oder PITTIME=+03:00 ausgegeben, schließt IBM Spectrum Protect Dateien ein, die um 12:00 Uhr am angegebenen PIT-Datum aktiv waren.

DATAType
Gibt an, dass Sicherungsgruppen mit den angegebenen Typen von Daten generiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist, dass Sicherungsgruppen auf Dateiebene generiert werden sollen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden.

Der Server generiert eine Sicherungsgruppe für jeden Datentyp und stellt alle Sicherungsgruppen in eine einzelne Gruppe von Ausgabedatenträgern. Jeder Sicherungsgruppe wird derselbe vollständig qualifizierte Name zugeordnet, der aus dem *Präfix_des_Sicherungsgruppennamens* und einem Suffix besteht, das vom Server bestimmt wird. Jede Sicherungsgruppe hat jedoch einen anderen Datentyp, wie vom Befehl QUERY BACKUPSET angezeigt wird. Gültige Werte:

ALL
Gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung), die auf dem Server gesichert wurden, generiert werden sollen.

FILE
Gibt an, dass eine Sicherungsgruppe auf Dateiebene generiert werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Sicherungsclient gesichert werden. Wurden keine Dateien oder Verzeichnisse vom Sicherungsclient gesichert, wird keine Sicherungsgruppe auf Dateiebene generiert. Dies ist der Standardwert.

IMAGE
Gibt an, dass eine Imagesicherungsgruppe generiert werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Sicherungsclients erstellt werden. Imagesicherungsgruppen werden nur generiert, wenn ein Image vom Sicherungsclient gesichert wurde.

TOC
Gibt an, ob für jede Sicherungsgruppe auf Dateiebene ein Inhaltsverzeichnis gesichert wird. Inhaltsverzeichnisse werden immer für Sicherungsgruppen gesichert, die Image- oder Anwendungsdaten enthalten. Der Parameter TOC wird ignoriert, wenn Image- und Anwendungssicherungsgruppen generiert werden. Ein Inhaltsverzeichnis wird immer für Image- und Anwendungssicherungsgruppen generiert.
Sie sollten bei der Festlegung, ob ein Inhaltsverzeichnis gesichert werden soll, Folgendes berücksichtigen:

- Wird ein Inhaltsverzeichnis für eine Sicherungsgruppe gesichert, können Sie den IBM Spectrum Protect-Webclient für Sichern/Archivieren verwenden, um die gesamte Dateisystemstruktur zu untersuchen und Dateien und Verzeichnisse zum Zurückschreiben auszuwählen. Für die Erstellung eines Inhaltsverzeichnisses müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, die mit dem Parameter TOCMGMTCLASS angegeben wird. Die Erstellung eines Inhaltsverzeichnisses erfordert zusätzliche Verarbeitung, zusätzlichen Speicherpoolplatz und möglicherweise einen Mountpunkt während der Sicherungsgruppenoperation.
- Wird ein Inhaltsverzeichnis für eine Sicherungsgruppe nicht gesichert, können Sie dennoch einzelne Dateien oder Verzeichnisstrukturen mit dem Befehl RESTORE BACKUPSET des Clients für Sichern/Archivieren zurückschreiben, wenn Sie den vollständig qualifizierten Namen jeder Datei oder jedes Verzeichnisses kennen, die bzw. das zurückgeschrieben werden soll.

Um den Inhalt von Sicherungsgruppen anzuzeigen, können Sie auch den Befehl QUERY BACKUPSETCONTENTS verwenden.

Dieser Parameter ist wahlfrei. Gültige Werte:

No
Gibt an, dass keine Inhaltsverzeichnisinformationen für Sicherungsgruppen auf Dateiebene gesichert werden.

Preferred
Gibt an, dass Inhaltsverzeichnisinformationen für Sicherungsgruppen auf Dateiebene gesichert werden sollen. Dies ist der Standardwert.Eine Sicherungsgruppe ist jedoch nicht fehlerhaft, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

Yes
Gibt an, dass Inhaltsverzeichnisinformationen für jede Sicherungsgruppe auf Dateiebene gesichert werden müssen. Eine Sicherungsgruppe ist fehlerhaft, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

TOCMGmtclass
Gibt den Namen der Verwaltungsklasse an, an die das Inhaltsverzeichnis gebunden werden soll. Wird keine Verwaltungsklasse angegeben, wird das Inhaltsverzeichnis an die Standardverwaltungsklasse für die Maßnahmendomäne gebunden, der der Knoten zugeordnet ist. In

diesem Fall müssen Sie für die Erstellung des Inhaltsverzeichnisses das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die angegebene Verwaltungsklasse definieren.

ALLOWSHREDdable
Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, in die Sicherungsgruppe eingeschlossen werden sollen. Dieser Parameter ist wahlfrei. Gültige Werte:

No
Gibt an, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, nicht in die Sicherungsgruppe eingeschlossen werden. Dies ist der Standardwert.

Yes
Gibt an, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, in die Sicherungsgruppe eingeschlossen werden können. Die Daten auf dem Sicherungsgruppendatenträger werden nicht geschreddert.

Beispiel: Eine Sicherungsgruppe für einen Dateibereich generieren

Eine Sicherungsgruppe von dem Dateibereich /srvr generieren, der zu dem Clientknoten JANE gehört. Der Sicherungsgruppe den Namen PERS_DATA zuordnen und die Sicherungsgruppe 75 Tage aufbewahren. Angeben, dass die Datenträger VOL1 und VOL2 die Daten der Sicherungsgruppe enthalten. Die Datenträger sollen von einer Einheit gelesen werden, die der Einheitenklasse AGADM zugeordnet ist. Eine Beschreibung einschließen.

```
generate backupset jane pers_data /srvr devclass=agadm
retention=75 volumes=vol1,vol2 description="Basisimage Bereich 51"
```

Beispiel: Eine Sicherungsgruppe von einem Unicode-fähigen Dateibereich generieren

Eine Sicherungsgruppe von dem Unicode-fähigen Dateibereich \\joe\c$ generieren, der zum Clientknoten JOE gehört. Der Sicherungsgruppe den Namen JOES_DATA zuordnen. Angeben, dass der Datenträger VOL1 die Daten der Sicherungsgruppe enthält. Der Datenträger soll von einer Einheit gelesen werden, die der Einheitenklasse AGADM zugeordnet ist. Der Server soll den Dateibereichsnamen \\joe\c$ aus der Server-Codepage in die Codepage UTF-8 konvertieren.

```
generate backupset joe joes_data \\joe\c$ devclass=agadm
volumes=vol1 nametype=unicode
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für GENERATE BACKUPSET

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUP	Löscht eine Knotengruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
GENERATE BACKUPSETTOC	Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
QUERY BACKUPSETCONTENTS	Zeigt den Inhalt in Sicherungsgruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

GENERATE BACKUPSETTOC (Inhaltsverzeichnis für eine Sicherungsgruppe generieren)

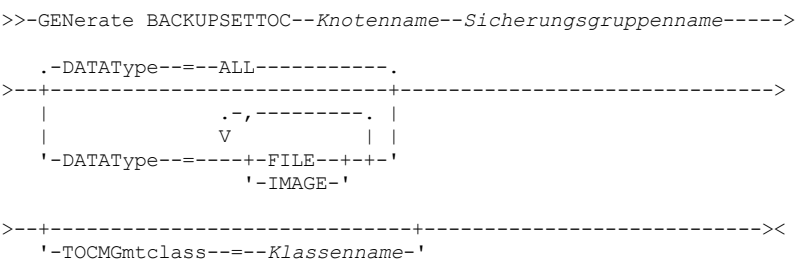
Verwenden Sie diesen Befehl, um ein Inhaltsverzeichnis für eine Sicherungsgruppe zu generieren, die noch nicht über ein Inhaltsverzeichnis verfügt. Der Client für Sichern/Archivieren verwendet das Inhaltsverzeichnis, um die Sicherungsgruppe anzuzeigen. Damit wird es Benutzern ermöglicht, einzelne Dateien zum Zurückschreiben aus der Sicherungsgruppe auszuwählen.

Die Erstellung eines Inhaltsverzeichnisses für eine Sicherungsgruppe erfordert Speicherbereich im Speicherpool und möglicherweise einen oder mehrere Mountpunkte während der Erstellungsoperation.

Berechtigungsklasse

Um diesen Befehl ausgeben zu können, müssen Benutzer die Systemberechtigung oder Maßnahmenberechtigung für die Domäne haben, der der Client-Knoten zugeordnet ist.

Syntax



Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, dessen Daten in der Sicherungsgruppe enthalten sind.Es können keine Platzhalterzeichen verwendet werden, um einen Namen anzugeben, und es kann keine Liste mit Clientknotennamen angegeben werden.

Sicherungsgruppenname (Erforderlich)
: Gibt den Namen der Sicherungsgruppe für den Client-Knoten an. Es können keine Platzhalterzeichen verwendet werden, um einen Namen anzugeben, und es kann keine Liste mit Sicherungsgruppennamen angegeben werden.

DATAType
: Gibt den Datentyp an, der im Inhaltsverzeichnis enthalten sein soll. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Daten eingeschlossen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Gültige Werte:

  ALL
  : Gibt an, dass das Inhaltsverzeichnis alle Typen von Daten (Dateiebene, Image und Anwendung) enthält, die in der Sicherungsgruppe gespeichert sind. Dies ist der Standardwert.

  FILE
  : Gibt an, dass das Inhaltsverzeichnis nur Daten auf Dateiebene enthält. Daten auf Dateiebene bestehen aus Dateien und Verzeichnissen, die vom Client für Sichern/Archivieren gesichert wurden. Enthält die Sicherungsgruppe keine Dateien oder Verzeichnisse, wird das Inhaltsverzeichnis nicht generiert.

  IMAGE
  : Gibt an, dass das Inhaltsverzeichnis nur Imagesicherungen enthält. Imagesicherungen bestehen aus Dateisystemimages, die mit dem Befehl BACKUP IMAGE des Sicherungsclients erstellt wurden. Enthält die Sicherungsgruppe keine Imagesicherungen, wird das Inhaltsverzeichnis nicht generiert.

TOCMGmtclass
: Gibt den Namen der Verwaltungsklasse an, an die das Inhaltsverzeichnis gebunden werden soll. Wird keine Verwaltungsklasse angegeben, wird das Inhaltsverzeichnis an die Standardverwaltungsklasse für die Maßnahmendomäne gebunden, der der Knoten zugeordnet ist. Wird ein Inhaltsverzeichnis erstellt, müssen Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die angegebene Verwaltungsklasse definieren.

Beispiel: Ein Inhaltsverzeichnis generieren

Ein Inhaltsverzeichnis für die Sicherungsgruppe PROJX_DATA generieren, die Daten für den Clientknoten GARY enthält. Das Inhaltsverzeichnis soll an die Standardverwaltungsklasse gebunden werden.

```
generate backupsettoc gary projx_data
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für GENERATE BACKUPSETTOC

Befehl	Beschreibung

Befehl	Beschreibung
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUP	Löscht eine Knotengruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
QUERY BACKUPSETCONTENTS	Zeigt den Inhalt in Sicherungsgruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

GENERATE DEDUPSTATS (Datendeduplizierungsstatistikdaten generieren)

Verwenden Sie diesen Befehl, um Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool oder einen Cloud-Containerspeicherpool zu generieren, um die Datendeduplizierungsleistung zu bestimmen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool erforderlich.

Syntax

```
>>-GENerate DEDUPSTats--Poolname--------------------------------->

   .-,-------------------------.
   V                         |   .-*---------------------.
>------+-Knotenname--------+---+--+-----------------------+----->
       '-Knotengruppenname-'      | .-,-----------------. |
                                  | V                   | |
                                  +---Dateibereichsname-+-+
                                  | .-,--------.          |
                                  | V          |          |
                                  '-----FSID---+----------'

   .-CODEType--=--BOTH-----------.  .-MAXPRocess--=--4------.
>--+-----------------------------+--+----------------------+--->
   '-CODEType--=--+-UNIcode----+-'  '-MAXPRocess--=--Anzahl-'
                  +-NONUNIcode-+
                  '-BOTH-------'

   .-NAMEType--=--SERVER------.  .-Wait--=--No------.
>--+-------------------------+--+------------------+----------><
   '-NAMEType--=--+-SERVER--+-'  '-Wait--=--+-No--+-'
                  +-UNIcode-+               '-Yes-'
                  '-FSID----'
```

Parameter

Poolname (Erforderlich)

Gibt den Namen des Speicherpools an, der in den Datendeduplizierungsstatistikdaten aufgelistet wird. Für den Speicherpoolnamen können bis zu 30 Zeichen angegeben werden. Wenn Sie mehr als 30 Zeichen angeben, schlägt der Befehl fehl.
Einschränkung: Sie können nur Verzeichniscontainerspeicherpools oder Cloudspeicherpools angeben.

Knotenname oder Knotengruppenname (Erforderlich)
Gibt den Namen des Clientknotens oder der definierten Gruppe von Clientknoten an, der bzw. die in den Datendeduplizierungsstatistikdaten aufgelistet wird. Sie können auch eine Kombination von Clientknotennamen und Clientknotengruppennamen angeben. Sollen mehrere Clientknotennamen oder Clientknotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen für Clientknotennamen, aber nicht für Clientknotengruppennamen verwenden.

Dateibereichsname oder FSID
Gibt die Namen der Dateibereiche in den Datendeduplizierungsstatistikdaten an. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Der Standardwert ist ein Stern. Geben Sie einen der folgenden Werte an:

*
Geben Sie einen Stern (*) an, um alle Dateibereiche oder IDs anzuzeigen.

Dateibereichsname
Gibt den Namen des Dateibereichs an. Geben Sie mehrere Dateibereiche an, indem Sie die Namen durch Kommas ohne Zwischenleerschritte voneinander trennen. FSID gibt eine Dateibereichs-ID an. Dieser Parameter ist für Clients mit Dateibereichen in Unicode-Format gültig. Geben Sie mehrere Dateibereiche an, indem Sie die Namen durch Kommas ohne Zwischenleerschritte voneinander trennen.

Für Clients mit Dateibereichen in Unicode-Format können Sie entweder einen Dateibereichsnamen oder eine Dateibereichs-ID (FSID) eingeben. Wenn Sie einen Dateibereichsnamen eingeben, muss der Server möglicherweise den eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Codepage des Servers in Unicode konvertieren.
Einschränkungen: Die folgenden Einschränkungen gelten für Dateibereichsnamen und FSIDs:

- Ein Knotenname muss angegeben werden, wenn ein Dateibereichsname angegeben wird.
- In demselben Befehl dürfen nicht gleichzeitig Dateibereichsnamen und Dateibereichs-IDs (FSIDs) angegeben werden.

CODEType
Gibt an, welcher Typ von Dateibereichen in den Satz eingeschlossen werden soll. Der Standardwert lautet BOTH. Dieser Standardwert gibt an, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie einen Stern zum Anzeigen von Informationen zu allen Dateibereichen eingeben. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

UNIcode
Dateibereiche einschließen, die ein Unicode-Format haben.

NONUNIcode
Dateibereiche einschließen, die kein Unicode-Format haben.

BOTH
Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen. Dies ist der Standardwert.

MAXPRocess
Gibt die maximale Anzahl paralleler Prozesse für die Generierung von Statistikdaten für einen Container in einem Verzeichniscontainer- oder Cloud-Containerspeicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 99 ein. Der Standardwert ist 4.

NAMEType
Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter, wenn IBM Spectrum Protect-Clients über Dateibereiche in Unicode-Format verfügen und die Clients unter dem Betriebssystem Windows, NetWare oder Macintosh OS X ausgeführt werden. Dieser Parameter ist wahlfrei.
Dieser Parameter ist erforderlich, wenn Sie einen Knotennamen und einen Dateibereichsnamen bzw. eine Dateibereichs-ID (FSID) angeben.
Einschränkung: Wenn Sie diesen Parameter angeben, darf der Dateibereichsname keinen Stern enthalten.

Geben Sie einen der folgenden Werte an:

SERVER
Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren. Dies ist der Standardwert.

UNIcode
Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab.
Tipp: Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

FSID
Der Server interpretiert die Dateibereichsnamen als ihre FSIDs.

Wait
Gibt an, ob die Datendeduplizierungsstatistikdaten im Vordergrund oder im Hintergrund generiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No

Gibt an, dass die Operation im Hintergrund ausgeführt wird. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Dies ist der Standardwert.

Yes

Gibt an, dass die Operation im Vordergrund ausgeführt wird. Die Ausführung der Operation nimmt unter Umständen viel Zeit in Anspruch. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden. Einschränkung: Sie können den Parameter WAIT=YES nicht an der Serverkonsole angeben.

Beispiel: Datendeduplizierungsstatistikdaten für einen Dateibereich generieren

Datendeduplizierungsstatistikdaten für einen Dateibereich mit dem Namen /srvr generieren, der zum Verzeichniscontainerspeicherpool POOL1 gehört, der auf dem Clientknoten NODE1 gespeichert ist.

```
generate dedupstats pool1 node1 /srvr
```

Beispiel: Datendeduplizierungsstatistikdaten für einen Unicode-fähigen Dateibereich generieren

Datendeduplizierungsstatistikdaten für einen Unicode-fähigen Dateibereich mit dem Namen \\abc\c$ generieren, der zum Clientknoten NODE2 gehört. Der Dateibereichsname \\abc\c$ wird aus der Server-Codepage in die Codepage UTF-8 konvertiert.

```
generate dedupstats node2 \\abc\c$ nametype=unicode
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für GENERATE DEDUPSTATS

Befehl	Beschreibung
AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeDELETE DEDUPSTATS	Löscht Datendeduplizierungsstatistikdaten.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeQUERY DEDUPSTATS	Zeigt Datendeduplizierungsstatistikdaten an.

GRANT-Befehle

Verwenden Sie den Befehl GRANT, um entsprechende Berechtigungen oder entsprechenden Zugriff zu erteilen.

- GRANT AUTHORITY (Administratorberechtigung hinzufügen)
- GRANT PROXYNODE (Proxyberechtigung einem Clientknoten erteilen)

GRANT AUTHORITY (Administratorberechtigung hinzufügen)

Mit diesem Befehl können einem Administrator Verwaltungsberechtigungsklassen und die Berechtigung für den Zugriff auf Client-Knoten erteilt werden.

Einem uneingeschränkten Maßnahmen- oder Speicheradministrator kann keine eingeschränkte Berechtigung erteilt werden. Hierfür muss dem Administrator die uneingeschränkte Berechtigung mit dem Befehl REVOKE AUTHORITY entzogen und dann mit diesem Befehl die eingeschränkte Berechtigung erteilt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-GRant AUTHority--Administratorname---------------------------->

                    .-,---------------.
           (1)      V                 |
>--CLasses------=----+-SYstem------+-+-------------------------->
                     +-Policy------+
                     +-STorage-----+
                     +-Operator----+
                     '-Node--| A |-'

>--+-----------------------------+------------------------------>
   |             .-,-----------. |
```

```
   |             V             | |
   '-DOmains--=----*Domänenname*-+-'

>--+-----------------------------+-------------------------><
   |                  .-,--------. |
   |          (1)     V          | |
   '-STGpools------=----*Poolname*-+-'

A

   .-AUTHority--=--Access-----.
|--+--------------------------+--+-DOmains--=--*Domänenname*-+----|
   '-AUTHority--=--+-Access-+-'  '-NOde--=--*Knotenname*-----'
                   '-Owner--'
```

Anmerkungen:

1. Mindestens einer dieser Parameter muss angegeben werden.

Parameter

Administratorname (Erforderlich)
: Gibt den Namen des Administrators an, dem eine Verwaltungsberechtigungsklasse erteilt wird.

CLasses
: Gibt eine oder mehrere Berechtigungsklassen an, die einem Administrator erteilt werden sollen. Dieser Parameter ist erforderlich, es sei denn, es wird der Parameter STGPOOLS angegeben. Es können mehrere Berechtigungsklassen angegeben werden, wobei die einzelnen Namen durch Komma voneinander getrennt werden müssen. Gültige Klassen sind:

  SYstem
  : Gibt an, dass einem Administrator die Systemberechtigung erteilt werden soll. Ein Systemadministrator verfügt über die höchste Berechtigungsstufe in IBM Spectrum Protect. Ein Systemadministrator kann alle Verwaltungsbefehle ausgeben und hat die Berechtigung, alle Maßnahmendomänen und alle Speicherpools zu verwalten. Wenn einem Administrator die Systemberechtigung erteilt wird, dürfen keine weiteren Berechtigungsklassen oder die Parameter DOMAINS und STGPOOLS angegeben werden. Nur ein Systemadministrator kann anderen Administratoren Berechtigungen erteilen.

  Policy
  : Gibt an, dass einem Administrator die Maßnahmenberechtigung erteilt werden soll. Wird der Parameter DOMAINS nicht angegeben, wird uneingeschränkte Maßnahmenberechtigung erteilt. Ein Administrator mit uneingeschränkter Maßnahmenberechtigung kann Befehle ausgeben, die alle vorhandenen Maßnahmendomänen sowie alle Maßnahmendomänen betreffen, die in Zukunft definiert werden. Ein Administrator mit uneingeschränkter Maßnahmenberechtigung kann keine Maßnahmendomänen definieren, löschen oder kopieren. Verwenden Sie den Befehl GRANT AUTHORITY mit CLASSES=POLICY und ohne den Parameter DOMAINS, um die eingeschränkte Maßnahmenberechtigung für einen Administrator in die uneingeschränkte Maßnahmenberechtigung zu erweitern.

  STorage
  : Gibt an, dass einem Administrator die Speicherberechtigung erteilt werden soll. Wenn der Parameter STGPOOLS nicht angegeben wird, wird uneingeschränkte Speicherberechtigung Speicherberechtigung erteilt. Ein Administrator mit uneingeschränkter Speicherberechtigung kann alle Befehle ausgeben, die Speicherressourcen für den Server zuordnen und steuern. Ein Administrator mit uneingeschränkter Speicherberechtigung kann Befehle ausgeben, die alle vorhandenen Speicherpools sowie alle Speicherpools betreffen, die in Zukunft definiert werden. Ein Administrator mit uneingeschränkter Speicherberechtigung kann Speicherpools nicht definieren oder löschen. Verwenden Sie den Befehl GRANT AUTHORITY mit CLASSES=STORAGE und ohne den Parameter STGPOOLS, um die eingeschränkte Speicherberechtigung für einen Administrator in die uneingeschränkte Speicherberechtigung zu erweitern.

  Operator
  : Gibt an, dass einem Administrator die Bedienerberechtigung erteilt werden soll. Ein Administrator mit Bedienerberechtigung kann Befehle ausgeben, die den direkten Betrieb des Servers und die Verfügbarkeit von Speicherdatenträgern steuern.

  Node
  : Gibt an, dass einem Benutzer eine Knotenberechtigung erteilt werden soll. Ein Benutzer mit Clientknotenberechtigung kann mit einer Benutzer-ID mit Administratorberechtigung und einem Kennwort von einem fernen System aus auf einen Web-Client für Sichern/Archivieren zugreifen, wenn der Benutzer über die Eignerberechtigung (Owner) oder Zugriffsberechtigung (Access) verfügt. Die Zugriffsberechtigung (Access) ist der Standardwert für eine Knotenberechtigungsklasse.
    Achtung: Wird die Knotenberechtigungsklasse angegeben, muss auch der Parameter DOMAIN oder der Parameter NODE angegeben werden, jedoch nicht beide Parameter.

    AUTHority
    : Gibt die Berechtigungsstufe eines Benutzers mit Knotenberechtigung an. Dieser Parameter ist wahlfrei.

      Hat ein Administrator bereits die System- oder Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Knoten gehört, wird mit diesem Befehl die Berechtigung des Administrators nicht geändert.

      Gültige Berechtigungsstufen sind:

      Access
      : Gibt an, dass einem Benutzer mit der Knotenberechtigungsklasse die Clientzugriffsberechtigung erteilt werden soll. Dies ist der Standardwert, wenn CLASSES=NODE angegeben wird. Ein Benutzer mit Clientzugriffsberechtigung kann

auf einen Web-Client für Sichern/Archivieren zugreifen und Sicherungs- und Zurückschreibungsaktionen auf diesem Client ausführen.
Achtung: Ein Benutzer mit Clientzugriffsberechtigung kann nicht auf diesen Client von einem anderen System aus zugreifen, indem der Parameter -NODENAME oder -VIRTUALNODENAME verwendet wird.

Ein Clientknoten kann die Option REVOKEREMOTEACCESS definieren, um zu verhindern, dass ein Benutzer, der über die Knotenberechtigung mit Clientzugriffsberechtigung verfügt, auf eine Clientdatenstation zugreift, auf der ein Web-Client ausgeführt wird. Diese Option gilt nicht für Administratoren mit Clienteignerberechtigung, Systemberechtigung oder Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Knoten gehört.

Owner
Gibt an, dass einem Benutzer mit der Knotenberechtigungsklasse die Clienteignerberechtigung erteilt werden soll. Ein Benutzer mit Clienteignerberechtigung kann über die Web-Client-Schnittstelle auf einen Web-Client für Sichern/Archivieren und außerdem auf die Daten von einem anderen Client aus zugreifen, indem der Parameter -NODENAME oder -VIRTUALNODENAME verwendet wird.

DOmains
Gibt an, dass dem Administrator Clientzugriffsberechtigung oder Clienteignerberechtigung für alle Clients in der angegebenen Maßnahmendomäne erteilt werden soll. Dieser Parameter kann nicht zusammen mit dem Parameter NODE verwendet werden.

NOde
Gibt an, dass dem Administrator Clientzugriffsberechtigung oder Clienteignerberechtigung für den Knoten erteilt werden soll. Dieser Parameter kann nicht zusammen mit dem Parameter DOMAIN verwendet werden.

DOmains
Gibt bei Verwendung mit CLASSES=POLICY an, dass einem Administrator die eingeschränkte Maßnahmenberechtigung erteilt werden soll.

Mit der eingeschränkten Maßnahmenberechtigung kann ein Administrator einen Teil der Maßnahmenbefehle für die Domänen ausgeben, für die der Administrator eine Berechtigung hat. Mit diesem Parameter kann einem Administrator mit eingeschränkter Maßnahmenberechtigung zusätzliche Maßnahmendomänenberechtigung erteilt werden. Dieser Parameter ist wahlfrei. Es können mehrere Maßnahmendomänen angegeben werden, wobei die einzelnen Namen durch ein Komma getrennt werden müssen.

Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.Es wird die Berechtigung für alle übereinstimmenden Maßnahmendomänen erteilt.

STGpools
Gibt an, dass einem Administrator die eingeschränkte Speicherberechtigung erteilt werden soll. Wenn der Parameter STGPOOLS angegeben wird, ist CLASSES=STORAGE wahlfrei.

Mit der eingeschränkten Speicherberechtigung kann ein Administrator einen Teil der Speicherbefehle für die Speicherpools ausgeben, für die der Administrator eine Berechtigung hat. Mit diesem Parameter kann einem Administrator mit eingeschränkter Speicherberechtigung zusätzliche Speicherpoolberechtigung erteilt werden. Dieser Parameter ist wahlfrei. Es können mehrere Speicherpools angegeben werden, wobei die einzelnen Namen durch ein Komma voneinander getrennt werden müssen.

Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.Für alle übereinstimmenden Speicherpools wird die Berechtigung erteilt.

Beispiel: Einem Administrator die Systemberechtigung erteilen

Administrator Larry die Systemberechtigung erteilen.

```
grant authority larry classes=system
```

Beispiel: Zugriff auf zusätzliche Maßnahmendomänen erteilen

Zusätzliche Maßnahmendomänen angeben, die der Administrator CLAUDIA mit eingeschränkter Maßnahmenberechtigung verwalten kann.

```
grant authority claudia domains=employee_records,prog1
```

Beispiel: Einem Administrator die uneingeschränkte Speicherberechtigung und die eingeschränkte Maßnahmenberechtigung erteilen

Administrator TOM die uneingeschränkte Speicherberechtigung und die eingeschränkte Maßnahmenberechtigung für die Domänen erteilen, deren Namen mit EMP beginnen.

```
grant authority tom classes=storage domains=emp*
```

Beispiel: Einem Administrator Berechtigung erteilen, die auf einen bestimmten Knoten beschränkt ist

Dem Benutzer HELP Knotenberechtigung erteilen, damit die Help-Desk-Mitarbeiter den Clientknoten LABCLIENT beim Sichern oder Zurückschreiben von Daten unterstützen können, ohne über andere IBM Spectrum Protect-Berechtigungen auf höherer Ebene zu verfügen.

```
grant authority help classes=node node=labclient
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für GRANT AUTHORITY

Befehl	Beschreibung
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.
REVOKE AUTHORITY	Widerruft eine oder mehrere Berechtigungsklassen oder schränkt den Zugriff auf Maßnahmendomänen und Speicherpools ein.

GRANT PROXYNODE (Proxyberechtigung einem Clientknoten erteilen)

Verwenden Sie diesen Befehl, um einem Clientknoten auf dem IBM Spectrum Protect-Server Proxyberechtigung zu erteilen.

Zielclientknoten sind Eigner der Daten und Agentenknoten arbeiten für die Zielknoten. Wurde die Proxyberechtigung für einen Zielclientknoten erteilt, kann ein Agentenknoten Sicherungs- und Zurückschreibungsoperationen für den Zielknoten ausführen. Daten, die vom Agentenknoten für den Zielknoten gespeichert werden, werden unter dem Namen des Zielknotens im Serverspeicher gespeichert.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung

Syntax

```
>>-GRant PROXynode TArget--=--Zielknotenname-------------------->

>--AGent--=--Agentenknotenname--------------------------------><
```

Parameter

TArget (Erforderlich)
: Gibt den Namen des Knotens an, der Eigner der Daten ist. Namen mit Platzhalterzeichen können zur Angabe des Zielknotennamens nicht verwendet werden.

AGent (Erforderlich)
: Gibt den Namen des Knotens an, der Operationen für den Zielknoten ausführt. Der Agentenknoten muss sich nicht in derselben Domäne wie der Zielknoten befinden. Platzhalterzeichen und durch Kommas getrennte Listen mit Knotennamen sind zulässig.

Beispiel: Einem Clientknoten Proxy-Berechtigung erteilen

Angenommen, MOE und JOE sind Agentenknoten in einem NAS-Cluster und werden zum Sichern und Zurückschreiben gemeinsam genutzter NAS-Daten verwendet. Um eine Proxy-Berechtigungsbeziehung für den Zielknoten NASCLUSTER zu erstellen, geben Sie den folgenden Befehl aus:

```
grant proxynode target=nascluster agent=moe,joe
```

Geben Sie den folgenden Befehl auf dem Agentenknoten MOE zum Sichern von NAS-Clusterdaten aus, die auf dem Laufwerk E: gespeichert sind. Der Name des Zielknotens ist NASCLUSTER.

```
dsmc -asnode=nascluster incremental e:
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für GRANT PROXYNODE

Befehl	Beschreibung
QUERY PROXYNODE	Zeigt die Knoten an, die die Berechtigung als Proxyknoten haben.
REVOKE PROXYNODE	Entzieht einem Agentenknoten die Proxyberechtigung.

HALT (Server abschalten)

Mit diesem Befehl kann der Server abgeschaltet werden. Der Befehl HALT erzwingt ein sofortiges Abschalten, wobei alle Verwaltungs- und Clientknotensitzungen abgebrochen werden, auch wenn sie noch nicht beendet sind.

Alle laufenden Transaktionen, die durch den Befehl HALT unterbrochen werden, werden beim Neustart des Servers rückgängig gemacht. Der Befehl HALT darf nur verwendet werden, wenn die Verwaltungs- und Clientknotensitzungen abgeschlossen oder abgebrochen wurden. Um den Server abzuschalten, ohne die Verwaltungs- und Client-Knotensitzungen stark zu beeinträchtigen, folgende Schritte ausführen:

1. Mit dem Befehl DISABLE SESSIONS verhindern, dass neue Clientknotensitzungen gestartet werden.
2. Mit dem Befehl QUERY SESSIONS alle vorhandenen Verwaltungs- und Clientknotensitzungen identifizieren.
3. Alle vorhandenen Verwaltungs- und Clientknotensitzungen über das geplante Abschalten des Servers informieren (außerhalb von IBM Spectrum Protect).
4. Mit dem Befehl CANCEL SESSIONS alle vorhandenen Verwaltungs- und Clientknotensitzungen abbrechen.
5. Mit dem Befehl HALT den Server abschalten und alle Verwaltungs- und Clientknotensitzungen stoppen.

Tipp:

Der Befehl HALT kann mit der Serveroption ALIASHALT repliziert werden. Verwenden Sie die Serveroption, um einen anderen Term als HALT zu definieren, mit dem dieselbe Funktion ausgeführt wird. Der Befehl HALT behält jedoch seine normale Funktion, die Serveroption bietet eine zusätzliche Methode zur Ausgabe des Befehls HALT. Für zusätzliche Informationen siehe ALIASHALT.

Berechtigungsklasse

Für diesen Befehl ist die System- oder Bedienerberechtigung erforderlich.

Syntax

```
>>-HALT-------------------------------------------------------><
```

Parameter

Keine.

Beispiel: Den Server abschalten

Den Server über die Serverkonsole oder über einen Verwaltungsclient abschalten. Alle Benutzeraktivitäten werden sofort gestoppt und neue Aktivitäten können nicht gestartet werden.

```
halt
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für HALT

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
CANCEL SESSION	Bricht aktive Sitzungen mit dem Server ab.
DISABLE SESSIONS	Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden.
ENABLE SESSIONS	Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY SESSION	Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.

HELP (Hilfe für Befehle und Fehlernachrichten anfordern)

Mit diesem Befehl können Verwaltungsbefehle und Fehlernachrichten angezeigt werden. Der Befehl kann von einem Verwaltungsbefehlszeilenclient ausgegeben werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Help--+---------------------------------------+-------------><
         +-Nummer_des_Hilfethemas----------------+
         |              .-,--------------------. |
         |              V                      | |
         +-Befehlsname----+------------------+-+-+
         |                 '-Unterbefehlsname-'   |
         +-Nachrichtennummer---------------------+
         +-Serveroptionsname---------------------+
         '-Dienstprogrammname--------------------'
```

Parameter

Nummer_des_Hilfethemas
: Gibt die Nummer Ihrer Auswahl aus den Hilfethemen an. Dieser Parameter ist wahlfrei.
Die Nummern der Hilfethemen werden im Inhaltsverzeichnis angezeigt. Beispiel:

```
3.0 Verwaltungsbefehle
  ...
  3.13.10 DEFINE DEVCLASS (Einheitenklasse definieren)
      3.13.10.1 DEFINE DEVCLASS (Einheitenklasse 3590 definieren)
      3.13.10.2 DEFINE DEVCLASS (Einheitenklasse 3592 definieren)
      ...
```

Die Nummer des Hilfethemas für den Befehl DEFINE DEVCLASS für die Einheitenklasse 3592 ist 3.13.10.2.

Befehlsname
: Gibt den Namen des Verwaltungsbefehls an, der angezeigt werden soll. Dieser Parameter ist wahlfrei.

Unterbefehlsname
: Gibt bis zu zwei der Unterbefehlsnamen an, die dem Namen des Verwaltungsbefehls zugeordnet sind, der angezeigt werden soll. Dieser Parameter ist wahlfrei.

Nachrichtennummer
: Gibt die Nummer der Nachricht an, für die Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei. Es können Hilfeinformationen für Servernachrichten (Präfix ANR) und Clientnachrichten (Präfix ANE oder ANS) angefordert werden. Das Präfix und den Bewertungscode nicht angeben, wenn die Nummer einer Fehlernachricht angegeben wird.

Serveroptionsname
: Gibt den Namen der Serveroption an, für die Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei.

Dienstprogrammname
: Gibt den Namen des Serverdienstprogramms an, für das Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei.

Beispiel: Die Hilfethemen anzeigen

Die Hilfethemen für die Befehlszeilenschnittstelle anzeigen.

```
Hilfe
```

Teilausgabe:

```
1.0 Server von der Befehlszeile aus verwalten
  1.1 Befehle mit dem Verwaltungsclient ausgeben
     1.1.1 Verwaltungsclient starten und stoppen
     1.1.2 Serveraktivitäten vom Verwaltungsclient aus überwachen
```

Beispiel: Ein Hilfethema unter Verwendung der Nummer des Hilfethemas anzeigen

Hilfetext unter Verwendung der Nummer des Hilfethemas aufrufen. Die Nummer des Hilfethemas für den Befehl DEFINE DEVCLASS für die Einheitenklasse 3592 ist 3.13.10.2.

```
help 3.13.10.2
```

Beispiel: Hilfetext für einen Befehl anzeigen

Hilfetext für die REMOVE-Befehle anzeigen.

```
help remove
```

```
3.44 REMOVE-Befehle
Mit den REMOVE-Befehlen kann ein Objekt entfernt werden.
Die folgende Liste enthält die REMOVE-Befehle:
*  3.44.1, "REMOVE ADMIN (Administrator löschen)"
*  3.44.2, "REMOVE NODE (Knoten oder zugehörigen Maschinenknoten
löschen)"
```

Beispiel: Hilfetext für eine bestimmte Fehlernachricht anzeigen

Hilfetext zu der Fehlernachricht ANR2535E aufrufen.

```
help 2535

ANR2535E  Befehl: Der Knotenname kann nicht entfernt oder umbenannt
werden,       da ihm eine Einheit zum Versetzen von Daten zugeordnet ist.
Erläuterung: Sie haben versucht, einen Knoten zu entfernen oder
umzubenennen, dem eine Einheit zum Versetzen von Daten zugeordnet ist.
Systemaktion: Der Knoten wird vom Server nicht entfernt oder umbenannt.
Benutzeraktion: Um den Knoten zu entfernen oder umzubenennen, löschen
Sie die zugeordnete Einheit zum Versetzen von Daten und geben Sie den
Befehl erneut aus.
```

Beispiel: Hilfetext für eine bestimmte Option anzeigen

Die Beschreibung, die Syntax und ein Beispiel für die Serveroption COMMMETHOD anzeigen.

```
help commmethod
```

Beispiel: Hilfetext für ein bestimmtes Dienstprogramm anzeigen

Die Beschreibung, die Syntax und ein Beispiel für das Dienstprogramm DSMSERV anzeigen.

```
help dsmserv
```

IDENTIFY DUPLICATES (Doppelte Daten in einem Speicherpool identifizieren)

Verwenden Sie diesen Befehl, um Prozesse zu starten oder zu stoppen, die doppelte Daten in einem Speicherpool identifizieren. Sie können die Anzahl der Prozesse zum Identifizieren doppelter Daten und ihre Dauer angeben.

Wenn Sie einen neuen Speicherpool für die Datendeduplizierung erstellen, können Sie 0 - 50 Prozesse zum Identifizieren doppelter Daten angeben. IBM Spectrum Protect startet die angegebene Anzahl Prozesse zum Identifizieren doppelter Daten automatisch, wenn der Server gestartet wird. Wenn Sie die Prozesse nicht stoppen, werden sie unbegrenzt ausgeführt.

Dieser Befehl betrifft nur die serverseitige Deduplizierungsverarbeitung. Bei der clientseitigen Datendeduplizierungsverarbeitung werden Duplikate auf dem Client für Sichern/Archivieren identifiziert.

Mit dem Befehl IDENTIFY DUPLICATES können Sie weitere Prozesse starten, einige oder alle Prozesse stoppen und eine Zeit angeben, die die Änderung wirksam bleibt. Wenn Sie die Anzahl der Prozesse zum Identifizieren doppelter Daten erhöht oder verringert haben, können Sie mit dem Befehl IDENTIFY DUPLICATES die Anzahl der Prozesse auf den in der Speicherpooldefinition angegebenen Wert zurücksetzen.

Haben Sie keine Prozesse zum Identifizieren doppelter Daten in der Speicherpooldefinition angegeben, können Sie mit dem Befehl IDENTIFY DUPLICATES alle Prozesse manuell starten und stoppen.

Mit diesem Befehl werden ein oder mehrere Hintergrundprozesse gestartet oder gestoppt, die Sie mit dem Befehl CANCEL PROCESS abbrechen können. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Wichtig:

- Sie können auch die Anzahl der Prozesse zum Identifizieren doppelter Daten ändern, indem Sie mit dem Befehl UPDATE STGPOOL die Speicherpooldefinition aktualisieren. Wenn Sie eine Speicherpooldefinition aktualisieren, können Sie jedoch keine Dauer angeben. Die Prozesse, die Sie in der Speicherpooldefinition angeben, werden unbegrenzt ausgeführt oder bis Sie den Befehl IDENTIFY DUPLICATES ausgeben, die Speicherpooldefinition erneut aktualisieren oder einen Prozess abbrechen.

  Bei der Ausgabe des Befehls IDENTIFY DUPLICATES wird nicht die Einstellung für die Anzahl der Prozesse zum Identifizieren doppelter Daten in der Speicherpooldefinition geändert.

- Prozesse zum Identifizieren doppelter Daten können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig eine Deduplizierung ausführen, sind aktiv. Prozesse, die auf Dateien warten, die dedupliziert werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Prozesse werden nur gestoppt, wenn sie abgebrochen werden oder wenn Sie die Anzahl der Prozesse zum Identifizieren doppelter Daten für den Speicherpool durch einen Wert ersetzen, der kleiner als der angegebene Wert ist. Bevor ein Prozess zum Identifizieren doppelter Daten stoppt, muss er die Datei, für die gegenwärtig eine Deduplizierung ausgeführt wird, fertig stellen.

  Die Ausgabe des Befehls QUERY PROCESS für einen Prozess zum Identifizieren doppelter Daten umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Prozess zum Identifizieren doppelter Daten vier Dateien verarbeitet, dann inaktiv ist und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-IDentify DUPlicates--Speicherpoolname------------------------>

>--+-----------------------+--+---------------------+---------><
   '-NUMPRocess--=--Anzahl-'  '-DURation--=--Minuten-'
```

Parameter

Speicherpoolname (Erforderlich)
: Gibt den Namen des Speicherpools an, in dem doppelte Daten identifiziert werden sollen. Sie können Platzhalterzeichen verwenden.

NUMPRocess
: Gibt die Anzahl der Prozesse zum Identifizieren doppelter Daten an, die nach Beendigung des Befehls ausgeführt werden sollen. Sie können 0 - 50 Prozesse angeben. Der Wert, den Sie für diesen Parameter angeben, überschreibt den in der Speicherpooldefinition angegebenen Wert oder den neuesten Wert, den Sie bei der letzten Ausgabe dieses Befehls angegeben haben. Geben Sie null an, werden alle Prozesse zum Identifizieren doppelter Daten gestoppt.

  Dieser Parameter ist wahlfrei. Wenn Sie keinen Wert angeben, startet oder stoppt der Server Prozesse zum Identifizieren doppelter Daten, so dass die Anzahl der Prozesse mit der in der Speicherpooldefinition angegebenen Anzahl identisch ist.

  Beispiel: Angenommen, Sie definieren einen neuen Speicherpool und geben zwei Prozesse zum Identifizieren doppelter Daten an. Später geben Sie den Befehl IDENTIFY DUPLICATES aus, um die Anzahl der Prozesse auf vier zu erhöhen. Geben Sie den Befehl IDENTIFY DUPLICATES erneut aus, ohne einen Wert für den Parameter NUMPROCESS anzugeben, stoppt der Server zwei Prozesse zum Identifizieren doppelter Daten.

  Haben Sie bei der Definition der Speicherpooldefinition null Prozesse angegeben und geben Sie IDENTIFY DUPLICATES ohne einen Wert für NUMPROCESS aus, werden alle gegenwärtig ausgeführten Prozesse zum Identifizieren doppelter Daten gestoppt, und der Server startet keine neuen Prozesse.

  Hinweis: Wenn Sie IDENTIFY DUPLICATES ohne einen Wert für NUMPROCESS ausgeben, ist der Parameter DURATION nicht verfügbar. Die in der Speicherpooldefinition angegebenen Prozesse zum Identifizieren doppelter Daten werden unbegrenzt ausgeführt oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.

  Wenn der Server einen Prozess zum Identifizieren doppelter Daten stoppt, stellt der Prozess die aktuelle physische Datei fertig, und wird dann gestoppt. Daher kann es einige Minuten dauern, bis die Anzahl der Prozesse zum Identifizieren doppelter Daten erreicht ist, die Sie als Wert für diesen Parameter angegeben haben.

DURation
: Gibt die maximale Anzahl Minuten (1 - 9999) an, die dieser Befehl wirksam bleibt. Nach Ablauf der angegebenen Zeit startet oder stoppt der Server Prozesse zum Identifizieren doppelter Daten, so dass die Anzahl der Prozesse mit der in der Speicherpooldefinition angegebenen Anzahl identisch ist.

  Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden die Prozesse, die nach Ausgabe des Befehls ausgeführt werden, unbegrenzt ausgeführt. Sie werden nur beendet, wenn Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.

  Beispiel: Wenn Sie einen Speicherpool mit zwei Prozessen zum Identifizieren doppelter Daten definieren und den Befehl IDENTIFY DUPLICATES mit `DURATION=60` und `NUMPROCESS=4` ausgeben, startet der Server zwei weitere Prozesse zum Identifizieren doppelter Daten, die 60 Minuten ausgeführt werden. Nach Ablauf dieser Zeit stellen zwei Prozesse die Dateien fertig, die gerade bearbeitet werden, und werden gestoppt. Die beiden Prozesse, die gestoppt werden, sind möglicherweise nicht die beiden Prozesse, die durch Ausgabe dieses Befehls gestartet wurden.

  Der Server stoppt inaktive Prozesse zuerst. Müssen nach dem Stoppen aller inaktiven Prozesse weitere Prozesse gestoppt werden, informiert der Server aktive Prozesse darüber, dass sie gestoppt werden.

  Wenn der Server einen Prozess zum Identifizieren doppelter Daten stoppt, stellt der Prozess die aktuelle physische Datei fertig, und wird dann gestoppt. Daher kann es einige Minuten dauern, bis die Zeit erreicht wird, die Sie als Wert für diesen Parameter angegeben haben.

Beispiel: Die Anzahl und Dauer der Prozesse zum Identifizieren doppelter Daten steuern

In diesem Beispiel haben Sie drei Prozesse zum Identifizieren doppelter Daten in der Speicherpooldefinition angegeben. Sie verwenden den Befehl IDENTIFY DUPLICATES, um die Prozessanzahl zu ändern und um die Zeit anzugeben, die die Änderung wirksam bleiben soll.

Tabelle 1. Prozesse zum Identifizieren doppelter Daten manuell steuern

In der Speicherpooldefinition sind drei Prozesse zum Identifizieren doppelter Daten angegeben. Mit dem Befehl IDENTIFY DUPLICATES geben Sie...	...und eine Dauer von...	Das Ergebnis ist...
2 Prozesse zum Identifizieren doppelter Daten an.	Keine angegeben	Ein Prozess zum Identifizieren doppelter Daten beendet die Datei, die gerade bearbeitet wird (falls vorhanden), und wird dann gestoppt. Zwei Prozesse werden unbegrenzt ausgeführt oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.
	60 Minuten	Ein Prozess zum Identifizieren doppelter Daten beendet die Datei, die gerade bearbeitet wird (falls vorhanden), und wird dann gestoppt. Nach 60 Minuten startet der Server einen Prozess, so dass drei Prozesse ausgeführt werden.
4 Prozesse zum Identifizieren doppelter Daten an.	Keine angegeben	Der Server startet einen Prozess zum Identifizieren doppelter Daten. Vier Prozesse werden unbegrenzt ausgeführt oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.
	60 Minuten	Der Server startet einen Prozess zum Identifizieren doppelter Daten. Nach Ablauf von 60 Minuten beendet ein Prozess die Datei, die gerade bearbeitet wird (falls vorhanden), und wird dann gestoppt. Der zusätzliche Prozess, der durch diesen Befehl gestartet wird, ist möglicherweise nicht der Prozess, der nach Ablauf der Dauer gestoppt wird.
0 Prozesse zum Identifizieren doppelter Daten an.	Keine angegeben	Alle Prozesse zum Identifizieren doppelter Daten beenden die Dateien, die gerade bearbeitet werden (falls vorhanden), und werden dann gestoppt. Diese Änderung bleibt unbegrenzt erhalten oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.
	60 Minuten	Alle Prozesse zum Identifizieren doppelter Daten beenden die Dateien, die gerade bearbeitet werden (falls vorhanden), und werden dann gestoppt. Nach Ablauf von 60 Minuten startet der Server drei Prozesse.
Keine angegeben	Nicht verfügbar	Die Anzahl der Prozesse zum Identifizieren doppelter Daten wird auf die in der Speicherpooldefinition angegebene Prozessanzahl zurückgesetzt. Diese Änderung bleibt unbegrenzt erhalten oder bis Sie den Befehl IDENTIFY DUPLICATES erneut ausgeben, die Speicherpooldefinition aktualisieren oder einen Prozess abbrechen.

Beispiel: Duplikate in einem Speicherpool identifizieren

Duplikate in dem Speicherpool STGPOOLA unter Verwendung von drei Prozessen zum Identifizieren doppelter Daten identifizieren. Angeben, dass diese Änderung 60 Minuten wirksam bleiben soll.

```
identify duplicates stgpoola duration=60 numprocess=3
```

Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für IDENTIFY DUPLICATES

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
QUERY CONTENT	Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

Befehle IMPORT

Mit den IMPORT-Befehlen können Informationen von Exportdatenträgern auf einen IBM Spectrum Protect-Server importiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

- IMPORT ADMIN (Administratorinformationen importieren)
- IMPORT NODE (Clientknoteninformationen importieren)
- IMPORT POLICY (Maßnahmeninformationen importieren)
- IMPORT SERVER (Serverinformationen importieren)

IMPORT ADMIN (Administratorinformationen importieren)

Mit diesem Befehl können Administrator- und Berechtigungsdefinitionen von Administratoren von Exportdatenträgern in den IBM Spectrum Protect-Server importiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

Mit dem Befehl QUERY ACTLOG kann der Status der Importoperation angezeigt werden.

Diese Informationen können auch über die Serverkonsole angezeigt werden.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden. Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn ein Hintergrundprozess des Befehls IMPORT ADMIN abgebrochen wird, wurden einige der Daten bereits importiert. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.
Einschränkung:

- Sind die Versionen des Zielservers und Quellenservers nicht kompatibel, kann die Operation möglicherweise nicht ausgeführt werden.
- Wenn die Administratordefinition, die importiert wird, Analytikerberechtigung enthält, wird die Administratordefinition importiert, aber nicht die Analytikerberechtigung. Die Analytikerberechtigung ist für Server mit V6.1 oder höher nicht gültig.
- Das Importieren von Daten aus einer CENTERA-Einheitenklasse wird nicht unterstützt. Dateien, die importiert werden, können jedoch auf einer CENTERA-Speichereinheit gespeichert werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
'-Yes-'
```

Parameter

Administratorname
: Gibt die Administratoren an, für die Informationen importiert werden sollen. Dieser Parameter ist wahlfrei. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

Preview
: Gibt an, ob die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Administratorinformationen zu importieren. Dieser Parameter ist wahlfrei. Die folgenden Parameterwerte werden unterstützt:

  No
  : Gibt an, dass die Informationen importiert werden sollen.

  Yes
  : Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen über die Anzahl und den Typ der importierten Objekte sowie die Anzahl der übertragenen Byte werden an der Serverkonsole und im Aktivitätenprotokoll aufgelistet.

  Der Standardwert ist NO. Wird für den Wert YES angegeben, müssen Sie die Exportdatenträger laden.

DEVclass (Erforderlich)
: Gibt die Einheitenklasse an, aus der die Importdaten gelesen werden sollen.

  Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

  Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Imports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, wie beispielsweise Wiederherstellungsoperationen, um ein Laufwerk verfügbar zu machen.

VOLumename (Erforderlich)
: Gibt die Datenträger an, die für die Importoperation verwendet werden sollen. Die Datenträger müssen in derselben Reihenfolge importiert werden, in der sie exportiert wurden. Die folgenden Parameterwerte werden unterstützt:

  Datenträgername
  : Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

  FILE: Dateiname
  : Gibt den Namen einer Datei an, die eine Liste der Datenträger enthält, die für die importierten Daten verwendet werden. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

  Verwenden Sie die folgenden Namenskonventionen bei der Angabe von Datenträgern, die den folgenden Einheitentypen zugeordnet sind:

Für Einheit	**Angeben**
Band	1 – 6 alphanumerische Zeichen.
FILE	Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel: AIX-BetriebssysteLinux-Betriebssysteme/imdata/mt1. Windows-Betriebssystemed:\Programmdateien\tivoli\tsm\data1.dsm.
AIX-BetriebssysteLinux-Betriebssysteme Windows-BetriebssystemeREMOVABLEFILE	AIX-BetriebssysteLinux-Betriebssysteme Windows-Betriebssysteme1 – 6 alphanumerische Zeichen.
SERVER	1 – 250 alphanumerische Zeichen.

Replacedefs
: Gibt an, ob Administratordefinitionen auf dem Zielserver ersetzt werden sollen. Die folgenden Parameterwerte werden unterstützt:

  No
  : Gibt an, dass Definitionen nicht ersetzt werden sollen.

  Yes
  : Gibt an, dass Definitionen ersetzt werden sollen.

  Der Standardwert ist NO.

Beispiel: Administratorinformationen von bestimmten Banddatenträgern importieren

Vom Server aus die Informationen für alle definierten Administratoren von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Den folgenden Befehl ausgeben:

```
import admin devclass=menu1
volumenames=tape01,tape02,tape03
```

Beispiel: Administratorinformationen von Banddatenträgern importieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Administratoren von den Banddatenträgern importieren, die in der folgenden Datei aufgelistet sind:

- AIX-BetriebssystemeLinux-BetriebssystemeTAPEVOL
- Windows-BetriebssystemeTAPEVOL.DATA

Diese Datei enthält diese Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Den folgenden Befehl ausgeben:
AIX-BetriebssystemeLinux-Betriebssysteme

```
import admin devclass=menu1 volumenames=file:tapevol
```

Windows-Betriebssysteme

```
import admin devclass=menu1 volumenames=file:tapevol.data
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für IMPORT ADMIN

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
EXPORT ADMIN	Kopiert Verwaltungsdaten auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT NODE	Schreibt Clientknotendaten von externen Datenträgern zurück.
IMPORT POLICY	Schreibt Maßnahmendaten von externen Datenträgern zurück.
IMPORT SERVER	Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.

IMPORT NODE (Clientknoteninformationen importieren)

Mit diesem Befehl können Clientknotendefinitionen von einem Server oder von sequenziellen Datenträgern in einen IBM Spectrum Protect-Zielserver importiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

Wenn Sie eine Domäne auf dem Quellenserver angeben und diese Maßnahmendomäne auch auf dem Zielserver vorhanden ist, werden die importierten Knoten derselben Maßnahmendomäne auf dem Zielserver zugeordnet. Andernfalls werden importierte Knoten der Maßnahmendomäne STANDARD auf dem Zielserver zugeordnet.

IBM Spectrum Protect-Server mit aktiviertem Aufbewahrungsschutz erlauben keine Importoperationen.

Einschränkungen:

1. Sind die Versionen des Zielservers und Quellenservers nicht kompatibel, kann die Operation möglicherweise nicht ausgeführt werden.
2. Das Importieren von Daten aus einer CENTERA-Einheitenklasse wird nicht unterstützt. Dateien, die importiert werden, können jedoch auf einer CENTERA-Speichereinheit gespeichert werden.
3. Wenn Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden, müssen alle Zielserver für LDAP-Kennwörter konfiguriert werden. Auf Daten, die von einem Knoten importiert werden, der sich mit einem LDAP-Verzeichnisserver authentifiziert, kann nicht zugegriffen werden, wenn der Zielserver nicht korrekt konfiguriert ist. Ist Ihr Zielserver nicht konfiguriert, können importierte Daten von einem LDAP-Knoten dennoch auf dem Zielserver gespeichert werden. Der Zielserver muss jedoch für die Verwendung von LDAP konfiguriert werden, damit Sie auf die importierten Daten zugreifen können.
4. Sind die Versionen des Zielservers und Quellenservers nicht kompatibel, kann die Operation möglicherweise nicht ausgeführt werden.

5. Sie können eine Einheitenklasse CENTERA nicht als Zielmedium für einen Exportbefehl oder als Quellenmedium für einen Importbefehl verwenden.
6. Das inkrementelle Exportieren/Importieren der folgenden Typen von Clientdaten auf einen anderen IBM Spectrum Protect-Server wird nicht unterstützt:
   - VMware-Sicherungen, bei denen Gesamt- und Teilsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen.
   - Sicherungsgruppen, bei denen Gesamt- und Differenzsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen.
   - Windows-Betriebssysteme Windows-Systemstatusdaten, die periodisch, inkrementell auf einen anderen Server übertragen werden.

   Der vollständige Export/Import dieser Daten in ein neues Dateisystem auf dem Ziel wird unterstützt, indem der gesamte Dateibereich, der die Daten enthält, exportiert wird. In anderen Worten, bei dem Export darf nicht die Option *FILEDATA=ALLACTIVE*, *FROMDATE*, *TODATE* oder *MERGEFILESPACES* verwendet werden.

   Das bewährte Verfahren für die inkrementelle Übertragung dieses Typs von Daten zwischen zwei Servern ist die Verwendung der Knotenreplikation.

Mit dem Befehl QUERY ACTLOG kann der Status der Importoperation angezeigt werden. Diese Informationen können auch über die Serverkonsole angezeigt werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn ein Hintergrundprozess des Befehls IMPORT NODE abgebrochen wird, wurden möglicherweise einige der Daten bereits importiert. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Bei einem Server, der über Clients mit Unterstützung für Unicode verfügt, kann der Server den eingegebenen Dateibereichsnamen konvertieren oder Sie können die folgenden Parameter verwenden:

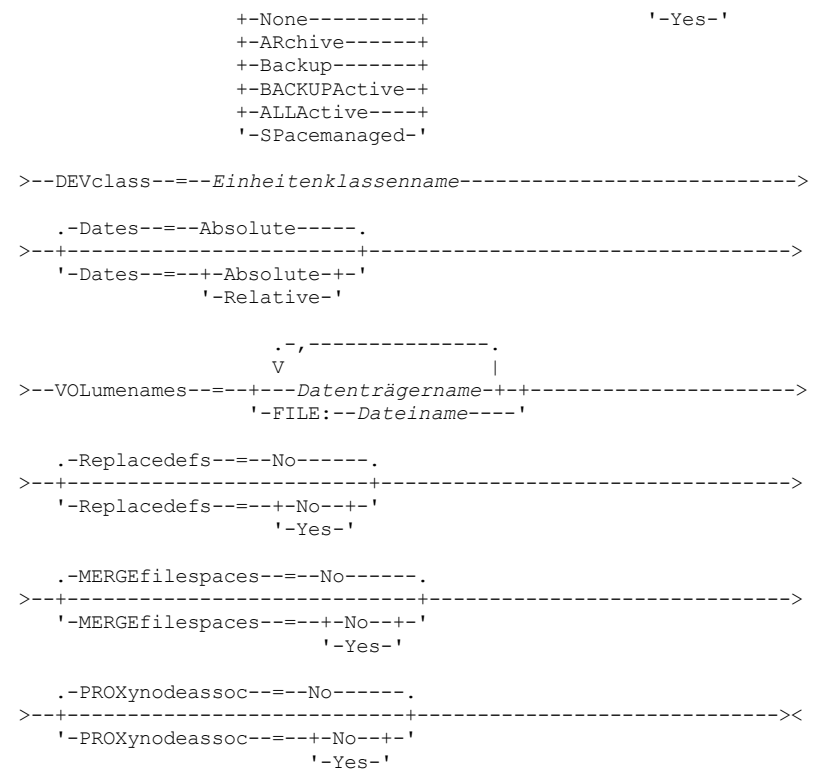
- HEXFILESPACE
- UNIFILESPACE

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Knotenname
: Gibt die Clientknoten an, für die Informationen importiert werden sollen. Dieser Parameter ist wahlfrei.

  Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Knotennamen werden in die Liste aufgenommen.

FILESpace
: Gibt die Namen der Dateibereiche an, für die Informationen importiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist alle Dateibereiche.

  Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

  Wichtig:

  1. Vorhandene Dateibereiche werden nicht ersetzt. Neue Dateibereiche werden erstellt, wenn identische Namen festgestellt werden. Dieser neue Name kann jedoch mit einem vorhandenen Namen auf dem Clientknoten übereinstimmen, der über Dateibereiche verfügt, die noch nicht auf dem Server gesichert wurden.
  2. Dieser Parameter wird nur für Nicht-Unicode-Dateibereiche angegeben. Sollen alle Dateibereiche, sowohl Unicode- als auch Nicht-Unicode-Dateibereiche, importiert werden, verwenden Sie den Parameter FILEDATA=ALL ohne die Parameter FILESPACE und UNIFILESPACE.

DOmains
: Gibt die Maßnahmendomänen an, aus denen Knoteninformationen importiert werden sollen. Diese Domänen müssen in den Daten enthalten sein, die exportiert wurden. Dieser Parameter ist wahlfrei. Der Standardwert gibt alle Domänen an, die exportiert wurden.

  Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.

FILEData
: Gibt den Typ der Dateien an, die für alle angegebenen Knoten importiert werden können und auf dem Exportdatenträger gefunden werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

  Werden Daten von sequenziellen Datenträgern importiert, wird die von den Dateidaten verwendete Einheitenklasse durch die Einheitenklasse des Speicherpools bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, werden zum Importieren der Knoteninformationen zwei Laufwerke benötigt. Der Grenzwert für Ladeanforderungen der Einheitenklasse muss mindestens 2 betragen.

  In den folgenden Beschreibungen werden *aktive* und *inaktive* Sicherungsdateikopien erwähnt. Eine aktive Sicherungsdateikopie ist die aktuellste Sicherungskopie einer Datei, die auf der Clientdatenstation noch vorhanden ist. Alle anderen Sicherungsdateikopien werden als

inaktive Kopien bezeichnet. Der Parameter unterstützt die folgenden Werte:

ALl
: Der Server importiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die eingeschlossenen Dateibereiche sind Unicode- und Nicht-Unicode-Dateibereiche.

None
: Nur Knotendefinitionen werden importiert. Der Server importiert keine Dateien.

ARchive
: Der Server importiert nur archivierte Dateien.

Backup
: Der Server importiert nur Sicherungsversionen, unabhängig davon, ob sie aktiv oder inaktiv sind.

BACKUPActive
: Der Server importiert nur aktive Sicherungsversionen. Diese aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl IMPORT ausgegeben wird.

ALLActive
: Der Server importiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl IMPORT ausgegeben wird.

SPacemanaged
: Der Server importiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Preview
: Gibt an, ob die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Informationen zu importieren. Die Option PREVIEW=YES erfordert das Laden der Exportdatenträger. Die folgenden Werte werden unterstützt:

  No
  : Gibt an, dass die Knoteninformationen importiert werden sollen.

  Yes
  : Gibt an, dass die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Dateien zu importieren. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.

  Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

DEVclass (Erforderlich)
: Gibt die Einheitenklasse an, aus der die Importdaten gelesen werden sollen. Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

  Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Imports aktiv, bricht der Server Operationen mit geringerer Priorität ab, wie beispielsweise die Identifizierung doppelter Daten, um ein Laufwerk verfügbar zu machen.

Dates
: Gibt an, ob die Daten für die Dateikopien auf dasselbe Datum gesetzt werden, an dem die Dateien exportiert wurden, oder ob die Daten an das Importdatum angepasst werden.
  Dieser Parameter unterstützt die folgenden Werte:

  Absolute
  : Die Daten für Dateikopien werden auf die Werte gesetzt, die beim Exportieren der Dateien angegeben wurden.

  Relative
  : Die Daten für Dateikopien werden an das Importdatum angepasst.

  Der Standardwert ist ABSOLUTE.

  Wenn der Exportdatenträger einige Zeit nach dem Export inaktiv ist (z. B. über einen Zeitraum von sechs Monaten), sind die ursprünglichen Sicherungs- oder Archivierungsdaten eventuell alt genug, um die sofortige Verfallsverarbeitung für Dateikopien auszulösen, wenn die Daten auf einen Server importiert werden. Wenn für diesen Wert RELATIVE angegeben wird, wird die seit dem Export verstrichene Zeit angepasst, so dass für die Dateikopien nicht sofort eine Verfallsverarbeitung erfolgt.

  Beispiel: Angenommen, ein Exportband enthält eine Archivierungsdateikopie, die fünf Tage vor der Exportoperation archiviert wurde. Wenn der Datenträger sechs Monate gesichert und dann importiert wird, wird standardmäßig davon ausgegangen, dass die Archivierungsdatei vor sechs Monaten und fünf Tagen eingefügt wurde (DATES=ABSOLUTE). Abhängig vom Aufbewahrungszeitraum, der in der Verwaltungsklasse der Datei angegeben ist, wird für die Datei möglicherweise sofort eine Verfallsverarbeitung durchgeführt. Durch die Angabe von DATES=RELATIVE wird das Archivierungsdatum der Datei während des Imports wieder auf "vor fünf Tagen" zurückgesetzt. Auf diese Weise passt der Parameter DATES=RELATIVE die seit dem Export verstrichene Zeit für Dateisicherungs- und -archivierungsdaten an.

VOLumenames (Erforderlich)
: Gibt die Datenträger an, die für die Importoperation verwendet werden sollen. Die Datenträger müssen in derselben Reihenfolge importiert werden, in der sie exportiert wurden. Der Parameter unterstützt die folgenden Werte:

  Datenträgername
  : Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

FILE:Dateiname
Gibt den Namen einer Datei an, die eine Liste der Datenträger enthält, die für die importierten Daten verwendet werden. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Verwenden Sie die folgenden Namenskonventionen bei der Angabe von Datenträgern, die den folgenden Einheitentypen zugeordnet sind:

Für Einheit	**Angeben**
Band	1 – 6 alphanumerische Zeichen.
FILE	AIX-BetriebssystemeLinux-BetriebssystemeBeliebige, vollständig qualifizierte Dateinamenzeichenfolge. Ein Beispiel ist /imdata/mt1. Windows-BetriebssystemeBeliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel: d:\Programmdateien\tivoli\tsm\data1.dsm.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeREMOVABLEFILE	AIX-BetriebssystemeLinux-Betriebssysteme Windows-Betriebssysteme1 – 6 alphanumerische Zeichen.
SERVER	1 – 250 alphanumerische Zeichen.

Replacedefs
Gibt an, ob Definitionen auf dem Zielserver ersetzt werden sollen. Der Standardwert ist NO. Der Parameter unterstützt die folgenden Werte:

No
Objekte sollen nicht ersetzt werden.
Yes
Objekte sollen ersetzt werden.

HEXFILESpace
Gibt die hexadezimale Darstellung der Dateibereichsnamen im UTF-8-Format an. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

Soll die hexadezimale Darstellung eines Dateibereichsnamens angezeigt werden, können Sie den Befehl QUERY FILESPACE mit FORMAT=DETAILED verwenden.

UNIFILESpace
Gibt an, dass die Dateibereiche, die dem Server bekannt sind, Unicode-fähig sind. Der Server konvertiert die Namen, die Sie eingeben, aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8, um die Dateibereiche zu lokalisieren, die importiert werden sollen. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Dieser Parameter ist wahlfrei.

MERGEfilespaces
Gibt an, ob IBM Spectrum Protect Clientdateien in vorhandene Dateibereiche auf dem Zielserver mischt (sofern sie vorhanden sind) oder ob IBM Spectrum Protect neue Dateibereichsnamen generiert. Der Standardwert ist NO.

Gültige Werte sind:

Yes
Gibt an, dass importierte Daten auf dem Zielserver in den vorhandenen Dateibereich gemischt werden, wenn ein Dateibereich mit demselben Namen auf dem Zielserver vorhanden ist.
No
Gibt an, dass IBM Spectrum Protect einen neuen Dateibereichsnamen für importierte Daten auf dem Zielserver generiert, wenn Dateibereiche mit demselben Namen vorhanden sind.

PROXynodeassoc
Gibt an, ob Proxyknotenzuordnungen importiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Beispiel: Clientknoteninformationen von Bändern importieren

Vom Server aus Clientknoteninformationen von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
import node devclass=menu1 volumenames=tape01,tape02,tape03
```

Beispiel: Clientknoteninformationen von Bändern importieren, die in einer Datei aufgelistet sind

AIX-BetriebssystemeLinux-BetriebssystemeVom Server die Clientknoteninformationen von den Banddatenträgern importieren, die in der Datei TAPEVOL aufgelistet sind.

Windows-BetriebssystemeVom Server die Clientknoteninformationen von den Banddatenträgern importieren, die in der Datei TAPEVOL.DATA aufgelistet sind.

Diese Datei enthält diese Zeilen:

```
TAPE01
TAPE02
TAPE03
```

Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.  AIX-Betriebssysteme  Linux-Betriebssysteme

```
import node devclass=menu1 volumenames=file:tapevol
```

 Windows-Betriebssysteme

```
import node devclass=menu1 volumenames=file:tapevol.data
```

Beispiel: Die aktive Sicherung für einen Clientknoten importieren

Importieren Sie vom Server die aktiven Sicherungsversionen der Dateidaten für Clientknoten JOE vom Banddatenträger TAPE01. Der Dateibereich ist Unicode.

```
import node joe unifilespace=\\joe\c$ filedata=backupactive devclass=menu1
    volumenames=tape01
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für IMPORT NODE

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT ADMIN	Schreibt Verwaltungsdaten von externen Datenträgern zurück.
IMPORT POLICY	Schreibt Maßnahmendaten von externen Datenträgern zurück.
IMPORT SERVER	Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.

IMPORT POLICY (Maßnahmeninformationen importieren)

Mit diesem Befehl können Informationen zu Maßnahmendomänen von sequenziellen Exportdatenträgern in den IBM Spectrum Protect-Server importiert werden. IBM Spectrum Protect-Server mit aktiviertem Aufbewahrungsschutz erlauben keine Importoperationen.

IBM Spectrum Protect-Clientdaten können mit der Export- und Importverarbeitung zwischen Servern versetzt werden, wenn auf beiden Plattformen derselbe austauschbare Datenträgertyp unterstützt wird.

Einschränkung:

1. Sind die Versionen des Zielservers und des Quellenservers nicht kompatibel, kann die Importoperation möglicherweise nicht ausgeführt werden.
2. Das Importieren von Daten aus einer CENTERA-Einheitenklasse wird nicht unterstützt. Dateien, die importiert werden, können jedoch auf einer CENTERA-Speichereinheit gespeichert werden.

Mit dem Befehl QUERY ACTLOG kann der Status der Importoperation angezeigt werden. Diese Informationen können auch über die Serverkonsole angezeigt werden.

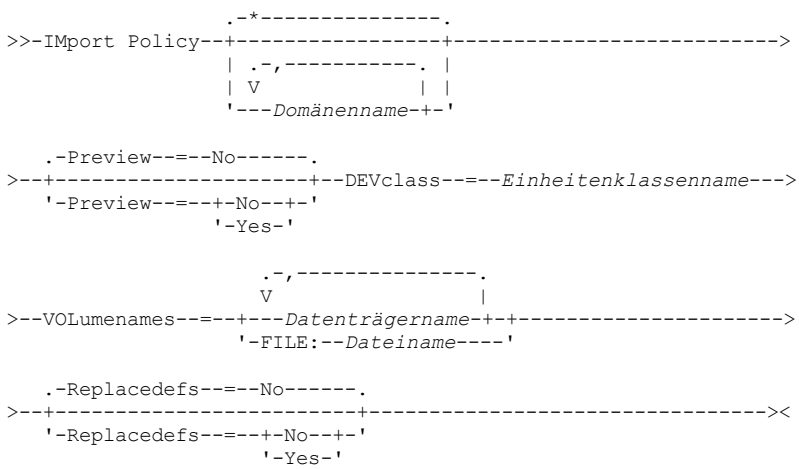
Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn ein Hintergrundprozess des Befehls IMPORT POLICY abgebrochen wird, wurden einige der Daten bereits importiert. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Domänenname
: Gibt die Maßnahmendomänen an, für die Informationen importiert werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Der Standardwert (*) lautet alle Domänen.

Preview
: Gibt an, ob die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Informationen zu importieren. Dieser Parameter unterstützt die folgenden Werte:

  No
  : Gibt an, dass die Informationen importiert werden sollen.

  Yes
  : Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll gemeldet.

  Die Option PREVIEW=YES erfordert das Laden der Exportdatenträger. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

DEVclass (Erforderlich)
: Gibt die Einheitenklasse an, aus der die Importdaten gelesen werden sollen. Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

  Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Imports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, wie beispielsweise Wiederherstellungsoperationen, um ein Laufwerk verfügbar zu machen.

VOLumenames (Erforderlich)
: Gibt die Datenträger an, die für die Importoperation verwendet werden sollen. Die Datenträger müssen in derselben Reihenfolge importiert werden, in der sie exportiert wurden. Dieser Parameter unterstützt die folgenden Werte:

  Datenträgername
  : Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

  FILE:Dateiname
  : Gibt den Namen einer Datei an, die eine Liste mit Datenträgern enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

  Verwenden Sie die folgenden Namenskonventionen bei der Angabe von Datenträgern, die den folgenden Einheitentypen zugeordnet sind:

Für Einheit	Angeben
Band	1 – 6 alphanumerische Zeichen.
FILE	Beliebige, vollständig qualifizierte Dateinamenzeichenfolge. Beispiel: • AIX-Betriebssysteme Linux-Betriebssysteme/imdata/mt1 • Windows-Betriebssystemed:\Programme\tivoli\tsm\data1.dsm.

Für Einheit	Angeben
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeREMOVABLEFILE	AIX-BetriebssystemeLinux-Betriebssysteme Windows-Betriebssysteme1 – 6 alphanumerische Zeichen.
SERVER	1 – 250 alphanumerische Zeichen.

Replacedefs

Gibt an, ob Maßnahmendefinitionen auf dem Zielserver ersetzt werden sollen. Dieser Parameter unterstützt die folgenden Werte:

Yes

Gibt an, dass die Objekte durch importierte Objekte ersetzt werden sollen.

No

Gibt an, dass die Objekte nicht durch importierte Objekte ersetzt werden sollen.

Der Standardwert ist NO.

Beispiel: Maßnahmeninformationen von bestimmten Banddatenträgern importieren

Vom Server aus die Informationen für alle definierten Maßnahmen von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
import policy devclass=menu1
volumenames=tape01,tape02,tape03
```

Beispiel: Maßnahmeninformationen von Banddatenträgern importieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Maßnahmen von den Banddatenträgern importieren, die in der Datei mit folgendem Namen aufgelistet sind:

- AIX-BetriebssystemeLinux-BetriebssystemeTAPEVOL
- TAPEVOL.DATA

Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Die Datei enthält die folgenden Zeilen:

```
TAPE01
TAPE02
TAPE03
```

AIX-BetriebssystemeLinux-Betriebssysteme

```
import policy devclass=menu1 volumenames=file:tapevol
```

Windows-Betriebssysteme

```
import policy devclass=menu1 volumenames=file:tapevol.data
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für IMPORT POLICY

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
EXPORT POLICY	Kopiert Maßnahmeninformationen auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT ADMIN	Schreibt Verwaltungsdaten von externen Datenträgern zurück.
IMPORT NODE	Schreibt Clientknotendaten von externen Datenträgern zurück.
IMPORT SERVER	Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.

IMPORT SERVER (Serverinformationen importieren)

Mit diesem Befehl können die Serversteuerungsinformationen und die angegebenen Clientdateidaten vollständig oder teilweise von Exportdatenträgern auf den IBM Spectrum Protect-Server kopiert werden.

Wichtig: Bei Befehlen, mit denen Administratoren oder Knoten importiert werden, müssen Sie die Methode der Authentifizierung beachten. Der IBM Spectrum Protect-Server kann keine Kennwörter für Knoten oder Administratoren exportieren oder importieren, die sich mit LDAP-Verzeichnisservern authentifizieren. Wenn die aktuelle Authentifizierungsmethode einen LDAP-Verzeichnisserver verwendet und das Kennwort noch nicht durch diesen Server synchronisiert ist, müssen Sie das Kennwort aktualisieren. Definieren Sie nach der Ausgabe des Befehls IMPORT das Kennwort, indem Sie den Befehl UPDATE ADMIN oder UPDATE NODE ausgeben.

IBM Spectrum Protect-Server mit aktiviertem Aufbewahrungsschutz erlauben keine Importoperationen.

Einschränkungen:

- Sind die Versionen des Zielservers und Quellenservers nicht kompatibel, kann die Operation möglicherweise nicht ausgeführt werden.
- Das Importieren von Daten aus einer CENTERA-Einheitenklasse wird nicht unterstützt. Dateien, die importiert werden, können jedoch auf einer CENTERA-Speichereinheit gespeichert werden.
- Wenn Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden, müssen alle Zielserver für LDAP-Kennwörter konfiguriert werden. Auf Serverdaten, die von einem Knoten exportiert werden, der sich mit einem LDAP-Verzeichnisserver authentifiziert, kann nicht zugegriffen werden, wenn der Zielserver nicht korrekt konfiguriert ist. Ist Ihr Zielserver nicht konfiguriert, können exportierte Daten von einem LDAP-Knoten dennoch auf dem Zielserver gespeichert werden. Der Zielserver muss jedoch für die Verwendung von LDAP konfiguriert werden, damit Sie auf die Daten zugreifen können.

- Das inkrementelle Exportieren oder Importieren der folgenden Typen von Clientdaten auf einen anderen IBM Spectrum Protect-Server wird nicht unterstützt:
  - VMware-Sicherungen, bei denen Gesamt- und Teilsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
  - Sicherungsgruppen, bei denen Gesamt- und Differenzsicherungen periodisch, inkrementell auf einen anderen Server übertragen werden müssen
  - Windows-Systemstatusdaten, die periodisch, inkrementell auf einen anderen Server übertragen werden

  Der vollständige Export oder Import dieser Daten in ein neues Dateisystem auf dem Ziel wird unterstützt, indem der gesamte Dateibereich, der die Daten enthält, exportiert wird. Bei dem Export darf nicht der Parameter FILEDATA=ALLACTIVE, FROMDATE, TODATE oder MERGEFILESPACES verwendet werden.

  Die Verwendung der Knotenreplikation zur inkrementellen Übertragung dieses Typs von Clientdaten zwischen zwei Servern ist optimal.

Sie können einen Import von Serverinformationen und Clientdateidaten auch direkt von dem Ursprungsserver einleiten. Weitere Informationen befinden sich unter den Befehlen EXPORT.

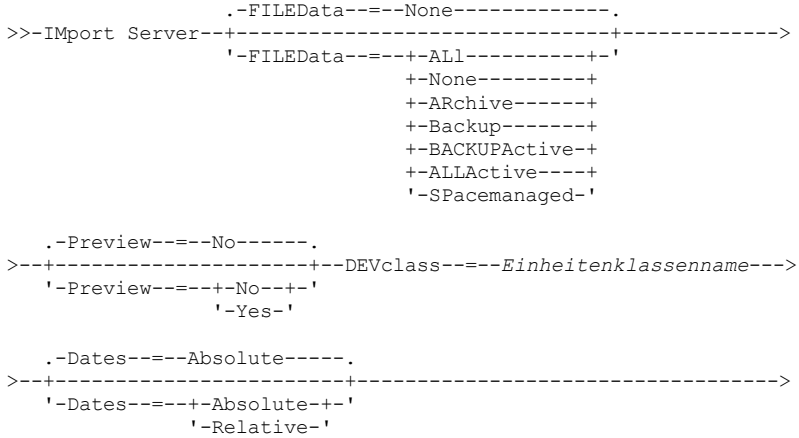
Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Wenn ein Hintergrundprozess des Befehls IMPORT SERVER abgebrochen wird, wurden einige der Daten bereits importiert. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

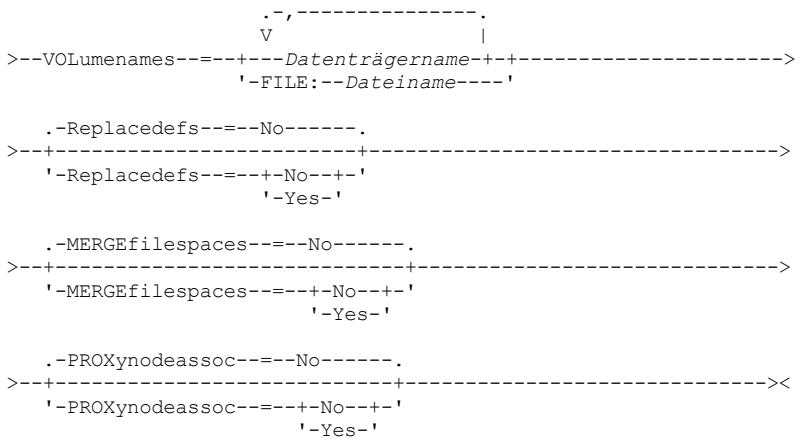
Einschränkung: Der IBM Spectrum Protect-Server führt während Export-, Import- und Knotenreplikationsoperationen keine Codepagekonvertierung aus. Wenn Server in verschiedenen Locales ausgeführt werden, können einige Informationen in Datenbanken oder in der Systemausgabe möglicherweise nicht gelesen werden. Ungültige Zeichen können angezeigt werden, beispielsweise in den Kontaktinformationen für den Administrator und die Clientknoten sowie in Beschreibungen von Maßnahmendomänen. Alle Felder, die im Serverzeichensatz gespeichert werden und erweiterte ASCII-Zeichen enthalten, können betroffen sein. Um das Problem zu beheben, aktualisieren Sie nach der Import- oder Knotenreplikationsoperation die Felder mit den entsprechenden Befehlen UPDATE. Diese Einschränkung für den Server hat keine Auswirkung auf Clientdaten. Alle Clientdaten, die exportiert, importiert oder repliziert wurden, können zurückgeschrieben, abgerufen und zurückgerufen werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax





Parameter

FILEData
: Gibt den Typ der Dateien an, die für alle Knoten importiert werden können, die für den Server definiert sind. Dieser Parameter ist wahlfrei. Der Standardwert ist NONE.

  Die Einheitenklasse für den Zugriff auf die Dateidaten wird durch die Einheitenklasse des Speicherpools bestimmt. Handelt es sich um dieselbe Einheitenklasse wie in diesem Befehl, werden zum Importieren der Informationen zwei Laufwerke benötigt. Der Grenzwert für Ladeanforderungen der Einheitenklasse muss mindestens auf 2 gesetzt werden.

  In den folgenden Beschreibungen werden aktive und inaktive Sicherungsdateikopien erwähnt. Eine aktive Sicherungsdateikopie ist die aktuellste Sicherungskopie einer Datei, die auf der Clientdatenstation noch vorhanden ist. Alle anderen Dateikopien werden als inaktive Kopien bezeichnet. Dieser Parameter unterstützt die folgenden Werte:

  ALl
  : IBM Spectrum Protect importiert alle Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

  None
  : IBM Spectrum Protect importiert keine Dateien, nur Knotendefinitionen.

  ARchive
  : IBM Spectrum Protect importiert nur archivierte Dateien.

  Backup
  : IBM Spectrum Protect importiert nur Sicherungsversionen, unabhängig davon, ob die Versionen aktiv oder inaktiv sind.

  BACKUPActive
  : IBM Spectrum Protect importiert nur aktive Sicherungsversionen. Diese aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl IMPORT ausgegeben wird.

  ALLActive
  : IBM Spectrum Protect importiert alle aktiven Sicherungsversionen von Dateien, alle archivierten Dateien und alle Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden. Die aktiven Sicherungsversionen sind die aktiven Versionen in der IBM Spectrum Protect-Datenbank zu dem Zeitpunkt, zu dem der Befehl IMPORT ausgegeben wird.

  SPacemanaged
  : IBM Spectrum Protect importiert nur Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Preview
: Gibt an, ob die Ergebnisse der Importoperation vorangezeigt werden sollen, ohne die Informationen zu importieren. Dieser Parameter unterstützt die folgenden Werte:

  No
  : Gibt an, dass die Serverinformationen importiert werden sollen.

  Yes
  : Gibt an, dass die Operation vorangezeigt, aber nicht ausgeführt wird. Informationen werden an die Serverkonsole und an das Aktivitätenprotokoll übertragen.

  Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird die Option PREVIEW=YES angegeben, müssen Sie die Exportdatenträger laden.

DEVclass (Erforderlich)
: Gibt die Einheitenklasse an, aus der die Importdaten gelesen werden sollen. Sie können die Einheitenklassen DISK, NAS oder CENTERA nicht angeben.

  Sind alle Laufwerke für die Einheitenklasse während der Ausführung des Imports aktiv, bricht IBM Spectrum Protect Operationen mit geringerer Priorität ab, wie beispielsweise Wiederherstellungsoperationen, um ein Laufwerk verfügbar zu machen.

Dates
Gibt an, ob die Daten für die Dateikopien auf dasselbe Datum gesetzt werden, an dem die Dateien exportiert wurden, oder ob die Daten an das Importdatum angepasst werden.

Wenn der Importdatenträger einige Zeit nach dem Export inaktiv ist (z. B. über einen Zeitraum von sechs Monaten), sind die ursprünglichen Sicherungs- oder Archivierungsdaten eventuell alt genug, um die sofortige Verfallsverarbeitung für Dateikopien auszulösen, wenn die Daten auf einen Server importiert werden. Wenn für diesen Wert RELATIVE angegeben wird, wird die seit dem Export verstrichene Zeit angepasst, so dass für die Dateikopien nicht sofort eine Verfallsverarbeitung erfolgt.

Beispiel: Angenommen, ein Importband enthält eine Archivierungsdateikopie, die fünf Tage vor der Exportoperation archiviert wurde. Wenn der Exportdatenträger sechs Monate gesichert und dann importiert wird, wird standardmäßig davon ausgegangen, dass die Archivierungsdatei vor sechs Monaten und fünf Tagen eingefügt wurde (DATES=ABSOLUTE). Abhängig vom Aufbewahrungszeitraum, der in der Verwaltungsklasse der Datei angegeben ist, wird für die Datei möglicherweise sofort eine Verfallsverarbeitung durchgeführt. Durch die Angabe von DATES=RELATIVE wird das Archivierungsdatum der Datei während des Imports wieder auf "vor fünf Tagen" zurückgesetzt. Auf diese Weise passt der Parameter DATES=RELATIVE die seit dem Export verstrichene Zeit für Dateisicherungs- und -archivierungsdaten an.

Dieser Parameter unterstützt die folgenden Werte:

Absolute
Die Daten für Dateikopien werden auf die Werte gesetzt, die beim Exportieren der Dateien angegeben wurden.
Relative
Die Daten für Dateikopien werden an das Datum des Imports angepasst.

Der Standardwert ist ABSOLUTE.

VOLumenames (Erforderlich)
Gibt die Datenträger an, die für die Importoperation verwendet werden sollen. Die Datenträger müssen in derselben Reihenfolge importiert werden, in der sie exportiert wurden. Dieser Parameter unterstützt die folgenden Werte:

Datenträgername
Gibt den Datenträgernamen an. Sollen mehrere Datenträger angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen.
FILE: Dateiname
Gibt den Namen einer Datei an, die eine Liste der Datenträger enthält, die für die importierten Daten verwendet werden. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert.

Verwenden Sie die folgenden Namenskonventionen bei der Angabe von Datenträgern, die den folgenden Einheitentypen zugeordnet sind:

Für Einheit	**Angeben**
Band	1 – 6 alphanumerische Zeichen.
FILE	 AIX-Betriebssysteme  Linux-BetriebssystemeBeliebige, vollständig qualifizierte Datenträger- oder Dateinamenzeichenfolge. Ein Beispiel ist /imdata/mt1.  Windows-BetriebssystemeBeliebige, vollständig qualifizierte Datenträger- oder Dateinamenzeichenfolge. Beispiel: d:\Programmdateien\tivoli\tsm\data1.dsm.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme REMOVABLEFILE	 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme1 – 6 alphanumerische Zeichen.
SERVER	1 – 250 alphanumerische Zeichen.

Replacedefs
Gibt an, ob Objekte auf dem Server ersetzt werden sollen. Vorhandene Dateibereiche werden nicht ersetzt. Neue Dateibereiche werden erstellt, wenn identische Namen festgestellt werden. Dieser Parameter unterstützt die folgenden Werte:

No
Gibt an, dass die Objekte nicht durch importierte Objekte ersetzt werden sollen.
Yes
Gibt an, dass die Objekte durch importierte Objekte ersetzt werden sollen.

Der Standardwert ist NO.

MERGEfilespaces
Gibt an, ob IBM Spectrum Protect Clientdateien in vorhandene Dateibereiche auf dem Zielserver mischt (sofern sie vorhanden sind) oder ob IBM Spectrum Protect neue Dateibereichsnamen generiert. Nicht-Unicode- und Unicode-Dateibereiche können nicht gemischt werden. Dieser Parameter unterstützt die folgenden Werte:

No
Gibt an, dass IBM Spectrum Protect einen neuen Dateibereichsnamen für importierte Daten auf dem Zielserver generiert, wenn Dateibereiche mit demselben Namen vorhanden sind.
Yes

Gibt an, dass importierte Daten auf dem Zielserver in den vorhandenen Dateibereich gemischt werden, wenn ein Dateibereich mit demselben Namen auf dem Zielserver vorhanden ist.

Der Standardwert ist NO.

PROXynodeassoc

Gibt an, ob Proxyknotenzuordnungen importiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Beispiel: Die Informationen für alle definierten Server von bestimmten Bändern importieren

Vom Server aus die Informationen für alle definierten Server von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist.

```
import server devclass=menu1 volumenames=tape01,tape02,tape03
```

AIX-BetriebssystemeLinux-Betriebssysteme

Beispiel: Informationen für alle definierten Server von bestimmten Bändern importieren und angeben, dass Dateien in vorhandene Dateibereiche gemischt werden

Vom Server aus die Informationen für alle definierten Server von den Banddatenträgern TAPE01, TAPE02 und TAPE03 importieren. Angeben, dass diese Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist, und dass Clientdateien in Dateibereiche auf dem Zielserver gemischt werden sollen, wenn Dateibereiche mit denselben Namen vorhanden sind.

```
import server devclass=menu1 volumenames=tape01,tape02,tape03 mergefilespaces=yes
```

Beispiel: Informationen für alle definierten Server von Bändern importieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Server von den Banddatenträgern importieren, die in der Datei TAPEVOL aufgelistet sind. Angeben, dass die Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Die Eingabedatei enthält diese Zeilen:

```
TAPE01
TAPE02
TAPE03

import server devclass=menu1 volumenames=file:tapevol
```

 Windows-Betriebssysteme

Beispiel: Informationen für alle definierten Server von Bändern importieren, die in einer Datei aufgelistet sind

Vom Server die Informationen für alle definierten Server von den Banddatenträgern importieren, die in der Datei TAPEVOL.DATA aufgelistet sind. Angeben, dass die Banddatenträger von einer Einheit gelesen werden, die der Einheitenklasse MENU1 zugeordnet ist. Die Eingabedatei enthält diese Zeilen:

```
TAPE01
TAPE02
TAPE03

import server devclass=menu1 volumenames=file:tapevol.data
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für IMPORT SERVER

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
EXPORT SERVER	Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT ADMIN	Schreibt Verwaltungsdaten von externen Datenträgern zurück.
IMPORT NODE	Schreibt Clientknotendaten von externen Datenträgern zurück.
IMPORT POLICY	Schreibt Maßnahmendaten von externen Datenträgern zurück.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.

INSERT MACHINE (Maschinenkenndaten oder Wiederh.-Anweisungen einfügen)

Mit diesem Befehl können vorhandenen Maschineninformationen in der Datenbank Client-Maschinenkenndaten oder Wiederherstellungsanweisungen hinzugefügt werden.

Sie können ein Programm schreiben, um Dateien mit den Informationen zu lesen und die entsprechenden INSERT MACHINE-Befehle zu generieren.

Mit den QUERY-Befehlen können die Informationen abgerufen werden, wenn ein schwerwiegender Fehler auftritt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-INsert MAchine--Maschinenname--Folgenummer------------------>

>--+-CHaracteristics--=--Text------+--------------------------><
   '-RECOVERYInstructions--=--Text-'
```

Parameter

Maschinenname (Erforderlich)
: Gibt den Namen der Client-Maschine an.

Folgenummer (Erforderlich)
: Gibt die Folgenummer für die Textzeile in der Datenbank an.

CHaracteristics
: Gibt die Maschinenkenndaten an. Der Benutzer muß die Kenndaten oder die Wiederherstellungsanweisungen angeben, jedoch nicht beides. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Der Text kann bis zu 1024 Zeichen umfassen.

RECOVERYInstructions
: Gibt die Wiederherstellungsanweisungen an. Der Benutzer muß die Kenndaten oder die Wiederherstellungsanweisungen angeben, jedoch nicht beides. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Der Text kann bis zu 1024 Zeichen umfassen.

Beispiel: Die Informationen einer Maschine aktualisieren

Für die Maschine DISTRICT5 den folgenden Kenndatentext in Zeile 1 einfügen: "Machine owner is Mary Smith".

```
insert machine district5 1
characteristics="Machine owner is Mary Smith"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für INSERT MACHINE

Befehl	Beschreibung
DEFINE MACHINE	Definiert eine Maschine für DRM.
DELETE MACHINE	Löscht eine Maschine.
QUERY MACHINE	Zeigt Informationen über Maschinen an.

Zugehörige Informationen:

Informationen zur Servermaschine und zu Clientknotenmaschinen angeben

ISSUE MESSAGE (Nachricht aus einem Server-Script ausgeben)

Diesen Befehl mit Rückkehrcodeverarbeitung in einem Script verwenden, um eine Nachricht aus einem Server-Script auszugeben, mit der die Fehlerquelle bei einem Befehl in dem Script bestimmt wird.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-ISSUE MESSAGE--Nachrichtenbewertung--Nachrichtentext--------><
```

Parameter

Nachrichtenbewertung (Erforderlich)
Gibt die Bewertung der Nachricht an. Die Anzeiger für die Nachrichtenbewertung sind:

I
Information. ANR1496I wird im Nachrichtentext angezeigt.
W
Warnung. ANR1497W wird im Nachrichtentext angezeigt.
E
Fehler. ANR1498E wird im Nachrichtentext angezeigt.
S
Schwer wiegender Fehler. ANR1499S wird im Nachrichtentext angezeigt.

Nachrichtentext (Erforderlich)
Gibt die Beschreibung der Nachricht an.

Beispiel: Eine Nachricht aus einem Server-Script ausgeben

Angenommen, Sie haben ein Script mit dem Namen backupscript, mit dem die Datenbank eines Clients stillgelegt wird, eine Sicherung dieser Datenbank vorgenommen wird und dann die Datenbank des Clients erneut gestartet wird. Zur Veranschaulichung resultiert das Script in einem Rückkehrcode ungleich Null. Den Befehl ISSUE MESSAGE mit der Nachrichtenbewertung und dem Nachrichtentext verwenden. Das folgende Beispiel ist ein Server-Script, das backupscript auf der Clientmaschine aufruft und Nachrichten auf der Basis des Rückkehrcodes von backupscript ausgibt.

```
issue message i "Starting backup"
define clientaction nodename action=command objects="c:\backupscript" wait=yes
if (101) goto qfail
if (102) goto qwarn
if (103) goto backupf
if (104) goto restartf
issue message i "Backup of database complete"
exit
qfail: issue message e "Quiesce of database failed"
exit
qwarn: issue message w "Quiesce of database failed, taking fuzzy backup"

exit
backupf: issue message e "Backup of database failed"
exit
restartf: issue message s "Database restart failed"
exit
```

Befehl

```
issue message e "quiesce of database failed"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ISSUE MESSAGE

Befehl	Beschreibung
COPY SCRIPT	Erstellt eine Kopie einer Prozedur.
DEFINE SCRIPT	Definiert eine Prozedur für den IBM Spectrum Protect-Server.
DELETE SCRIPT	Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur.
RENAME SCRIPT	Vergibt einen neuen Namen für eine Prozedur.
RUN	Führt ein Script aus.
UPDATE SCRIPT	Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.

LABEL LIBVOLUME (Datenträger im Kassettenarchiv Kennsatz zuordnen)

Mit diesem Befehl kann Banddatenträgern ein Kennsatz zugeordnet werden; in einem automatisierten Kassettenarchiv wird den Datenträgern automatisch beim Zurückstellen ein Kennsatz zugeordnet. Mit diesem Befehl verwendet der Server den Kennsatz mit vollständiger Länge, mit dem die Datenträger häufig vorgekennzeichnet sind.

Einschränkung: Verwenden Sie diesen Befehl nur für Kassettenarchive des Typs MANUAL, SCSI, ACSLS und 349X. Die Verarbeitung des Befehls wartet nicht darauf, dass ein Laufwerk verfügbar wird, auch wenn sich das Laufwerk nur im Status IDLE befindet. Falls erforderlich, kann ein

Kassettenarchivlaufwerk verfügbar gemacht werden, indem der Befehl DISMOUNT VOLUME ausgegeben wird, um den Datenträger in diesem speziellen Laufwerk zu entladen. Wird das Kassettenarchivlaufwerk verfügbar, können Sie den Befehl LABEL LIBVOLUME erneut ausgeben. Ausführliche und aktuelle Informationen zur Laufwerk- und Speicherarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

AIX-BetriebssystemeLinux-Betriebssysteme

Um den Befehl LABEL LIBVOLUME zu verwenden, muss mindestens ein Laufwerk vorhanden sein, das nicht von einem anderen IBM Spectrum Protect-Prozess verwendet wird. Dies schließt inaktive Datenträger ein, die bereitgestellt werden. Falls erforderlich, verwenden Sie den Befehl DISMOUNT VOLUME zur Aufhebung der Bereitstellung des inaktiven Datenträgers, um dieses Laufwerk verfügbar zu machen.

Standardmäßig überschreibt der Befehl LABEL LIBVOLUME keinen vorhandenen Kennsatz. Soll ein vorhandener Kennsatz jedoch überschrieben werden, können Sie die Option `OVERWRITE=YES` angeben.

Achtung:

- Beim Überschreiben eines Datenträgerkennsatzes werden alle Daten auf dem Datenträger gelöscht. Gehen Sie beim Überschreiben von Datenträgerkennsätzen mit Vorsicht vor, um das Löschen gültiger Daten zu vermeiden.
- Die Kennsätze auf VolSafe-Datenträgern können nur einmal überschrieben werden. Verwenden Sie daher den Befehl LABEL LIBVOLUME nur einmal für VolSafe-Datenträger. Sie können das Überschreiben des Kennsatzes vermeiden, indem Sie die Option `OVERWRITE=NO` mit dem Befehl LABEL LIBVOLUME verwenden.

Wenn Sie den Befehl LABEL LIBVOLUME verwenden, können Sie die Datenträger, die gekennzeichnet werden sollen, auf folgende Art und Weise angeben:

- Benennen Sie explizit einen Datenträger.
- Geben Sie mit dem Parameter VOLRANGE einen Bereich von Datenträgern ein.
- Verwenden Sie den Parameter VOLLIST, um eine Datei anzugeben, die eine Liste der Datenträgernamen enthält, oder um einen oder mehrere Datenträger explizit zu benennen.

Bei automatisierten Speicherarchiven werden Sie aufgefordert, den Datenträger in den Eingangs-/Ausgangsschacht des Speicherarchivs einzulegen. Ist keine Serviceein-/-ausgabestation verfügbar, legen Sie den Datenträger in einen leeren Schacht ein. Bei manuellen Speicherarchiven werden Sie aufgefordert, den Datenträger direkt in ein Laufwerk zu laden.

Tipp: Um Banddatenträger automatisch zu kennzeichnen, können Sie den Parameter AUTOLABEL in den Befehlen DEFINE LIBRARY und UPDATE LIBRARY verwenden. Wird der Parameter AUTOLABEL verwendet, ist es nicht erforderlich, eine Gruppe von Bändern vorab zu kennzeichnen. Diese Methode ist effizienter als die Verwendung des Befehls LABEL LIBVOLUME, der es erfordert, dass Datenträger separat bereitgestellt werden. Wenn Sie den Parameter AUTOLABEL mit einem SCSI-Speicherarchiv verwenden, müssen Sie Bänder zurückstellen, indem Sie `CHECKLABEL=BARCODE` im Befehl CHECKIN LIBVOLUME angeben. Der Parameter AUTOLABEL nimmt für alle Nicht-SCSI-Speicherarchive standardmäßig den Wert YES und für SCSI-Speicherarchive den Wert NO an.
Windows-Betriebssysteme

Um Datenträger mit dem Befehl LABEL LIBVOLUME zu kennzeichnen, geben Sie den Parameter CHECKIN an.

Um Banddatenträger in SCSI-Speicherarchiven automatisch zu kennzeichnen, verwenden Sie den Parameter AUTOLABEL in den Befehlen DEFINE LIBRARY und UPDATE LIBRARY. Wird dieser Parameter verwendet, ist es nicht erforderlich, eine Gruppe von Bändern vorab zu kennzeichnen. Diese Methode ist außerdem effizienter als die Verwendung des Befehls LABEL LIBVOLUME, der es erfordert, dass Datenträger separat bereitgestellt werden. Wenn Sie den Parameter AUTOLABEL verwenden, müssen Sie Bänder zurückstellen, indem Sie CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME angeben.

Ein Kennsatz darf keine eingebetteten Leerzeichen oder Punkte enthalten und muss gültig sein, wenn er als Dateiname auf den Datenträgern verwendet wird.

Sie müssen CD-ROM-, Zip- oder Jaz-Datenträger mit den Dienstprogrammen des Einheitenherstellers oder den Windows-Dienstprogrammen kennzeichnen. IBM Spectrum Protect stellt keine Dienstprogramme zum Formatieren oder Kennzeichnen dieser Datenträgertypen bereit. Die Dienstprogramme des Betriebssystems schließen das Plattenverwaltungsprogramm (Disk Administrator) (eine grafische Benutzerschnittstelle) und den Befehl zum Zuordnen von Kennsätzen ein.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax für manuelles Speicherarchiv

```
>>-LABEl LIBVolume--Speicherarchivname--------------------------->

                           .-OVERWRITE--=--No------.
>------Datenträgername------+-----------------------+----------->
                           '-OVERWRITE--=--+-No--+-'
```

```
                                                '-Yes-'

   .-WAITTime--=--60---.
>--+-------------------+---------------------------------------><
   '-WAITTime--=--Wert-'
```

Syntax für SCSI-Kassettenarchiv

```
>>-LABEl LIBVolume--Speicherarchivname-------------------------->

>----+-Datenträgername-------------------------------------------------+---->
     '-SEARCH--=--+-Yes--| A |--+--LABELSource--=--+-Barcode---------+-'
                  '-Bulk--| A |-'                 +-Prompt----------+
                                                  '-Vollist--| B |-'

                                .-OVERWRITE--=--No------.
>--+-------------------------+--+----------------------+------->
   '-CHECKIN--=--+-SCRatch-+-'  '-OVERWRITE--=--+-No--+-'
                 '-PRIvate-'                    '-Yes-'

   .-WAITTime--=--60---.
>--+-------------------+---------------------------------------><
   '-WAITTime--=--Wert-'

A (SEARCH=Yes, SEARCH=Bulk)

|--+-VOLRange--=----Datenträgername1,Datenträgername2---+-------|
   |               .-,---------------.                  |
   |               V                 |                  |
   '-VOLList--=--+---Datenträgername-+-+----------------'
                 '-FILE:--Dateiname----'

B (LABELSource=Vollist)

                 .-,---------------.
                 V                 |
|--VOLList--=--+---Datenträgername-+-+--------------------------|
               '-FILE:--Dateiname----'
```

Syntax für 349X-Kassettenarchiv

```
>>-LABEl LIBVolume--Speicherarchivname-------------------------->

>----+-Datenträgername-----------+------------------------------>
     '-SEARCH--=--Yes----| A |---'

                                .-OVERWRITE--=--No------.
>--+-------------------------+--+----------------------+------->
   '-CHECKIN--=--+-SCRatch-+-'  '-OVERWRITE--=--+-No--+-'
                 '-PRIvate-'                    '-Yes-'

   .-WAITTime--=--60---.
>--+-------------------+---------------------------------------><
   '-WAITTime--=--Wert-'

A (SEARCH=Yes)

|--+-VOLRange--=----Datenträgername1,Datenträgername2---+-------|
   |               .-,---------------.                  |
   |               V                 |                  |
   '-VOLList--=--+---Datenträgername-+-+----------------'
                 '-FILE:--Dateiname----'
```

Syntax für ACSLS-Kassettenarchiv

```
>>-LABEl LIBVolume--Speicherarchivname-------------------------->

>----+-Datenträgername-----------+------------------------------>
     '-SEARCH--=--Yes----| A |---'

                                .-OVERWRITE--=--No------.
>--+-------------------------+--+----------------------+------->
   '-CHECKIN--=--+-SCRatch-+-'  '-OVERWRITE--=--+-No--+-'
                 '-PRIvate-'                    '-Yes-'
```

```
   .-WAITTime----60---.
>--+-------------------+---------------------------------------><
   '-WAITTime----Wert-'

A (SEARCH=Yes)

|--+-VOLRange-------Datenträgername1,Datenträgername2---+-------|
   |                .-,---------------.                  |
   |                V                 |                  |
   '-VOLList-----+---Datenträgername-+-+----------------'
                 '-FILE:--Dateiname----'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das den Speicherdatenträger enthält.

Datenträgername
: Gibt den Namen des Datenträgers an, der gekennzeichnet werden soll.

  - Für SCSI-Speicherarchive: Der Server gibt die Anforderung aus, den Datenträger in einen Schacht in dem Speicherarchiv oder, falls verfügbar, in einen Eingangs-/Ausgangsanschluss einzulegen. Der Server identifiziert einen Schacht anhand der Elementadresse des Schachts. Wird ein Datenträger in einem SCSI-Speicherarchiv mit mehreren Eingangs-/Ausgangsanschlüssen gekennzeichnet, wird der Datenträger in dem Schacht mit der niedrigsten Nummer gekennzeichnet.
    Warnung: Wenn Sie einen Datenträgernamen angeben, überschreibt der angegebene Name den Kennsatz, der auf der Kassette gedruckt ist.
  - Für Speicherarchive des Typs MANUAL: Der Server gibt die Anforderung aus, den Datenträger in ein Laufwerk einzulegen.
  - Für 349X-Kassettenarchive: Der Datenträger befindet sich möglicherweise bereits in dem Kassettenarchiv, oder Sie werden möglicherweise aufgefordert, den Datenträger in die E/A-Station zu stellen.

  Hinweis: Ist der angegebene Datenträgername bereits in einem Speicherpool oder in einer Datenträgerhistorydatei definiert, erhält der Datenträger keinen Kennsatz und eine Nachricht wird angezeigt.

CHECKIN
: Gibt an, ob der Server den Datenträger zurückstellt. Dieser Parameter ist wahlfrei. Gültige Werte:

  SCRatch
  : Gibt an, dass der Server die Datenträger zurückstellt und die Datenträger dem Arbeitsdatenträgerpool des Kassettenarchivs hinzufügt. Hat ein Datenträger einen Eintrag in der Datenträger-History, können Sie den Datenträger nicht als Arbeitsdatenträger zurückstellen.

  PRIvate
  : Gibt an, dass der Server die Datenträger zurückstellt und die Datenträger als privat kennzeichnet. Private Datenträger sind nur verfügbar, wenn sie nach Namen angefordert werden.

  Wird kein Wert für diesen Parameter angegeben, wird mit dem Befehl der Datenträger gekennzeichnet, aber nicht zurückgestellt. Geben Sie für diesen Parameter keinen Wert ein und soll der Datenträger zurückgestellt werden, müssen Sie den Befehl CHECKIN LIBVOLUME ausgeben.

SEARCH
: Gibt an, dass der Server das Kassettenarchiv nach verwendbaren Datenträgern durchsucht, denen ein Kennsatz zugeordnet werden soll. Dieser Parameter gilt für SCSI-, 349X- und ACSLS-Kassettenarchive.
  Die folgenden Werte sind gültig:

  Yes
  : Gibt an, dass der Server nur den Datenträgern einen Kennsatz zuordnet, die in dem Kassettenarchiv aufbewahrt werden, es sei denn, dem Datenträger wurde bereits ein Kennsatz zugeordnet oder der Barcode des Datenträgers kann nicht gelesen werden.

    Wird die Option `LABELSOURCE=PROMPT` angegeben, wird der Datenträger aus seiner Position in dem Kassettenarchiv oder den Eingangs- und Ausgangsanschlüssen in das Laufwerk versetzt. Der Server fordert den Benutzer auf, den Befehl REPLY auszugeben, der die Kennsatzzeichenfolge enthält, und dieser Kennsatz wird auf das Band geschrieben.

  Bulk
  : Gibt an, dass der Server die Eingangs-/Ausgangsanschlüsse des Kassettenarchivs nach verwendbaren Datenträgern durchsucht, denen ein Kennsatz zugeordnet werden soll. Diese Option ist nur für SCSI-Kassettenarchive gültig.

    Wird LABELSOURCE=BARCODE angegeben, wird der Barcode des Datenträgers gelesen. Anschließend wird das Band aus seiner Position in dem Kassettenarchiv oder in den Eingangs-/Ausgangsanschlüssen in ein Laufwerk versetzt, in dem das Barcodeetikett geschrieben wird. Nachdem das Band mit einem Kennsatz versehen wurde, wird es zurück in seine Position in dem Kassettenarchiv, in die Eingangs-/Ausgangsanschlüsse oder in einen Speicherschacht versetzt, wenn die Option CHECKIN angegeben wurde. Für die korrekte Funktionsweise der Barcodeunterstützung für Kassettenarchive, die von IBM Spectrum Protect unterstützt werden, müssen der IBM Spectrum Protect-Server und der Einheitentreiber dieselbe Stufe aufweisen. Die Barcodeunterstützung ist für Kassettenarchive verfügbar, die von IBM Spectrum Protect unterstützt werden und die den IBM Spectrum Protect-Einheitentreiber oder den IBM® Magstar- oder LTO Ultrium-Einheitentreiber verwenden.

Tipp: Sie können den Parameter VOLRANGE oder VOLLIST verwenden, um die Suche zu begrenzen.

VOLRange
Gibt einen Bereich von Datenträgernamen an, die durch ein Komma voneinander getrennt sind. Verwenden Sie diesen Parameter, um die Suche nach Datenträgern zu begrenzen, die gekennzeichnet werden sollen, wenn SEARCH=YES (Kassettenarchive 349X, ACSLS und SCSI) oder SEARCH=BULK (nur SCSI-Kassettenarchive) angegeben wird. Sind keine Datenträger in dem Kassettenarchiv vorhanden, die sich in dem angegebenen Bereich befinden, wird der Befehl ohne Fehler beendet.

Es können nur Datenträgernamen angegeben werden, die numerisch erhöht werden können. Neben dem Bereich für den Erhöhungswert kann ein Datenträgername ein alphanumerisches Präfix und ein alphanumerisches Suffix enthalten.

Parameter	**Beschreibung**
`volrange=bar110,bar130`	Die folgenden 21 Datenträger werden mit einem Kennsatz versehen: bar110, bar111, bar112,...bar129, bar130.
`volrange=bar11a,bar13a`	Die 3 Datenträger werden wie folgt gekennzeichnet: bar11a, bar12a, bar13a.
`volrange=123400,123410`	Die 11 Datenträger werden gekennzeichnet: 123400, 123401, ...123409, 123410.

VOLList
Gibt eine Liste mit Datenträgern an. Verwenden Sie diesen Parameter, um die Suche nach Datenträgern zu begrenzen, die gekennzeichnet werden sollen, wenn SEARCH=YES (Kassettenarchive 349X, ACSLS und SCSI) oder SEARCH=BULK (nur SCSI-Kassettenarchive) angegeben wird. Sind keine Datenträger in dem Kassettenarchiv vorhanden, die sich in der Liste befinden, wird der Befehl ohne Fehler beendet. Der Parameter VOLLIST kann auch die Quelle der Namen sein, die zum Kennzeichnen von Datenträgern verwendet werden sollen, wenn der Parameter LABELSOURCE auf VOLLIST gesetzt ist. Bei LABELSOURCE=VOLLIST müssen Sie den Parameter VOLLIST angeben.
Die folgenden Werte sind gültig:

Datenträgername
Gibt die Namen der Datenträger an, die für den Befehl verwendet werden. Zum Beispiel: `VOLLIST=TAPE01,TAPE02`.
FILE: Dateiname
Gibt den Namen einer Datei an, die eine Liste der Datenträger für den Befehl enthält. In der Datei muss sich jeder Datenträgername auf einer separaten Zeile befinden. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert. Um beispielsweise die Datenträger TAPE01, TAPE02 und TAPE03 zu verwenden, erstellen Sie eine Datei mit dem Namen TAPEVOL, die die folgenden Zeilen enthält:

```
TAPE01
TAPE02
TAPE03
```

Die Datenträger können für den Befehl wie folgt angegeben werden: `VOLLIST=FILE:TAPEVOL`.

Hinweis: Bei dem Dateinamen muss die Groß-/Kleinschreibung beachtet werden.

LABELSource
Gibt an, wie oder ob der Server Kennsätze sequenzieller Datenträger liest. Diese Option ist nur für SCSI-Kassettenarchive gültig. Geben Sie diesen Parameter nur bei SEARCH=YES oder SEARCH=BULK an.
Sie können die folgenden Werte angeben:

Prompt
Der Server fordert bei Bedarf zur Eingabe von Datenträgernamen auf.
Barcode
Der Server versucht, das Barcode-Etikett zu lesen. Schlägt der Versuch fehl, wird der Datenträger von dem Server nicht mit einem Kennsatz versehen, und es wird eine Nachricht angezeigt.
Wichtig: Für die korrekte Funktionsweise der Barcode-Unterstützung müssen die entsprechenden Einheitentreiber für die Kassettenarchive installiert sein.
Vollist
Diese Option gilt nur für SCSI-Kassettenarchive. Der Server versucht, die angegebene Datei oder Dateiliste zu lesen. Schlägt der Versuch fehl, werden die Datenträger von dem Server nicht mit einem Kennsatz versehen, und es wird eine Nachricht angezeigt.

OVERWRITE
Gibt an, ob der Server versucht, vorhandene Kennsätze zu überschreiben. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

No
Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht. Für StorageTek-VolSafe-Datenträger muss der Wert NO lauten.
Yes
Gibt an, dass der Server vorhandene Kennsätze nur dann überschreibt, wenn sowohl der vorhandene Kennsatz als auch der angeforderte Kennsatz oder das Barcodeetikett noch nicht in dem Serverspeicherpool oder in der Datenträgerhistoryliste definiert sind.

WAITTime
: Gibt die Anzahl Minuten an, die der Server auf Ihre Antwort auf eine Anforderung wartet. Geben Sie einen Wert im Bereich 0-9999 an. Möchten Sie vom Server zur Eingabe aufgefordert werden, geben Sie eine Wartezeit größer als Null an. Der Standardwert ist 60 Minuten. Beispiel: Angenommen, Sie werden vom Server aufgefordert, ein Band in den Eingangs-/Ausgangsanschluss eines Kassettenarchivs einzulegen. Haben Sie eine Wartezeit von 60 Minuten angegeben, gibt der Server eine Anforderung aus und wartet 60 Minuten auf Ihre Antwort. Angenommen, Sie haben dagegen eine Wartezeit von 0 angegeben. Wenn Sie ein Band eingelegt haben, hat eine Wartezeit mit dem Wert Null zur Folge, dass die Operation ohne Aufforderung fortgesetzt wird. Haben Sie kein Band eingelegt, hat eine Wartezeit mit dem Wert Null zur Folge, dass die Operation fehlschlägt.

Beispiel: Datenträger im Kassettenarchiv automatisch mit einem Kennsatz versehen

Bänder in dem SCSI-Kassettenarchiv `AUTO` automatisch mit einem Kennsatz versehen, wenn die Datenträger zurückgestellt werden.

```
label libvolume auto checkin=scratch search=yes labelsource=barcode
overwrite=yes
```

Beispiel: Sequenzielle Datenträger im Kassettenarchiv mit einem Kennsatz versehen

Die 3 Datenträger `bar11a` bis `bar13a` in dem SCSI-Kassettenarchiv ABC mit einem Kennsatz versehen. Wird der folgende Befehl ausgegeben, werden die drei Datenträger wie folgt gekennzeichnet: `bar11a`, `bar12a`, `bar13a`.

```
label libvolume abc checkin=scratch search=yes volrange=bar11a,bar13a
labelsource=barcode
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für LABEL LIBVOLUME

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
CHECKIN LIBVOLUME	Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY LIBVOLUME	Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
REPLY	Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.
UPDATE LIBVOLUME	Ändert den Status eines Speicherdatenträgers.

LOAD DEFALERTTRIGGERS (Standardgruppe von Alertauslösern laden)

Verwenden Sie diesen Befehl, um die Standardgruppe von Alertauslösern auf den IBM Spectrum Protect-Server zu laden.

Für einen neu installierten Server ist eine Standardgruppe von Nachrichten zum Auslösen von Alerts definiert. Sie können die Standardalertauslöser ändern oder löschen. Verwenden Sie diesen Befehl, um die folgenden Tasks auszuführen:

- Die Standardgruppe von Alertauslösern laden und alle Standardalertauslöser, die gelöscht wurden, zurückschreiben.
- Alle Alertauslöser durch die ursprüngliche Standardgruppe ersetzen.

Standardmäßig werden mit diesem Befehl keine anderen erstellten Alertauslöser gelöscht; außerdem werden keine geänderten Standardalertauslöser ersetzt. Um alle Alertauslöser zu löschen und die ursprüngliche Gruppe von Standardalertauslösern zurückzuschreiben, geben Sie RESET=yes an.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                          .-REset----No------.
>>-LOad DEFALerttriggers--+------------------+----------------><
                          '-REset----+-No--+-'
                                     '-Yes-'
```

Parameter

REset
: Gibt an, ob alle Alertauslöser durch die Standardgruppe von Alertauslösern ersetzt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

  No
  : Gibt an, dass nur die Standardalertauslöser hinzugefügt werden. Die ursprünglichen Standardalertauslöser werden dem Server hinzugefügt. Vorhandene Auslöser werden nicht gelöscht. Wenn ein Standardauslöser auf dem Server vorhanden ist, wird er nicht ersetzt oder geändert.

  Yes
  : Gibt an, dass die Alertauslöser mit den ursprünglichen Standardwerten zurückgeschrieben werden. Alle Alertauslöser werden gelöscht; anschließend wird die ursprüngliche Gruppe von Standardalertauslösern hinzugefügt.

Beispiel: Standardalertauslöser auf den Server laden

Die Standardauslöser laden, um alle gelöschten Standardauslöser zurückzuschreiben. Den folgenden Befehl ausgeben:

```
load defalerttriggers
```

Beispiel: Alle Alertauslöser auf dem Server durch die Standardalertauslöser ersetzen

Alle Alertauslöser auf dem Server löschen und durch die ursprünglichen Standardwerte ersetzen. Den folgenden Befehl ausgeben:

```
load defalerttriggers reset=yes
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für für LOAD DEFALERTTRIGGERS

Befehl	Beschreibung
DEFINE ALERTTRIGGER (Alertauslöser definieren)	Ordnet angegebene Nachrichten einem Alertauslöser zu.
DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)	Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.
QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)	Zeigt Nachrichtennummern an, die einen Alert auslösen.
UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)	Aktualisiert die Attribute eines oder mehrerer Alertauslöser.

LOCK-Befehle

Mit den LOCK-Befehlen kann der Benutzerzugriff auf den Server verhindert werden.

- LOCK ADMIN (Administrator sperren)
- LOCK NODE (Clientknoten sperren)
- LOCK PROFILE (Profil sperren)

LOCK ADMIN (Administrator sperren)

Mit diesem Befehl kann der Zugriff eines Administrators auf den Server verhindert werden. Der Administrator bleibt gesperrt, bis ein Systemadministrator seine Zugriffsberechtigung mit dem Befehl UNLOCK ADMIN wiederherstellt.

Sie können den Authentifizierungsfilter verwenden, um alle Administratoren, außer Konsolenadministratoren, zu sperren. Nach der Konfiguration eines LDAP-Verzeichnisservers für die Kennwortauthentifizierung können Sie Administratoren sperren, um zu erzwingen, dass sie Kennwörter erstellen, die sich mit einem LDAP-Server authentifizieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-LOCK Admin--+-*-----------------+--+-----------------------------+-><
              '-Administratorname-'  '-AUTHentication--=--+-LOcal-+-'
                                                          '-LDap--'
```

Parameter

Administratorname (Erforderlich)
: Gibt den Namen des Administrators an, der gesperrt werden soll. Sie können Platzhalterzeichen verwenden, um den Administratornamen anzugeben. Sie müssen keinen Administratornamen eingeben, wenn alle Administratoren gemäß ihrer Authentifizierungsmethode gesperrt werden sollen. Verwenden Sie das Platzhalterzeichen mit einer Authentifizierungsmethode, um mehrere Administratoren zu sperren.

AUTHentication
: Gibt die Methode der Authentifizierung an, die der Administrator für die Anmeldung verwendet.

  LOcal
  : Gibt an, dass Administratoren gesperrt werden sollen, die sich mit dem IBM Spectrum Protect-Server authentifizieren.

  LDap
  : Gibt an, dass Administratoren gesperrt werden sollen, die sich mit dem LDAP-Verzeichnisserver authentifizieren.

Beispiel: Einen Administrator sperren

Den Administrator CLAUDIA sperren. Den folgenden Befehl ausgeben:

```
lock admin claudia
```

Beispiel: Alle Administratoren sperren, die sich mit der IBM Spectrum Protect-Serverdatenbank authentifizieren

Das Platzhalterzeichen (*) verwenden, um alle Administratoren zu sperren, die ihre Kennwörter lokal authentifizieren. Konsolenadministratoren sind von diesem Befehl nicht betroffen. Den folgenden Befehl ausgeben:

```
lock admin * authentication=local
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für LOCK ADMIN

Befehl	Beschreibung
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.
UNLOCK ADMIN	Ermöglicht einem gesperrten Administrator den Zugriff auf IBM Spectrum Protect.

LOCK NODE (Clientknoten sperren)

Mit diesem Befehl kann der Zugriff eines Clientknotens auf den Server verhindert werden. Ein gesperrter Clientknoten kann keine IBM Spectrum Protect-Operationen ausführen, auch wenn die Operationen geplant sind.

Nach der Konfiguration eines LDAP-Verzeichnisservers für die Kennwortauthentifizierung können Sie Knoten sperren, um zu erzwingen, dass sie Kennwörter verwenden, die sich mit einem LDAP-Server authentifizieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Clientknoten gehört.

Syntax

```
>>-LOCK Node--+-*----------+--+-----------------------------+-><
              '-Knotenname-'  '-AUTHentication--=--+-LOcal-+-'
                                                  '-LDap--'
```

Parameter

Knotenname
: Gibt den Namen des Clientknotens an, der gesperrt werden soll. Sie können ein Platzhalterzeichen anstelle eines Knotennamens verwenden, wenn alle Knoten gemäß ihrer Authentifizierungsmethode gesperrt werden sollen.

AUTHentication
: Gibt die Methode der Kennwortauthentifizierung an, die für die Anmeldung bei einem Knoten erforderlich ist.

  LOcal
  : Gibt an, dass Knoten gesperrt werden sollen, die sich mit dem IBM Spectrum Protect-Server authentifizieren.

  LDap
  : Gibt an, dass Knoten gesperrt werden sollen, die sich mit einem LDAP-Verzeichnisserver authentifizieren.

Beispiel: Einen bestimmten Clientknoten sperren

Den Clientknoten SMITH sperren.

```
lock node smith
```

Beispiel: Alle Knoten sperren, die sich mit der lokalen IBM Spectrum Protect-Datenbank authentifizieren

Geben Sie den folgenden Befehl aus, um alle Knoten zu sperren, die sich mit dem IBM Spectrum Protect-Server authentifizieren:

```
lock node * authentication=local
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für LOCK NODE

Befehl	Beschreibung
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
UNLOCK NODE	Ermöglicht einem gesperrten Benutzer in einer bestimmten Maßnahmendomäne wieder den Zugriff auf den Server.

LOCK PROFILE (Profil sperren)

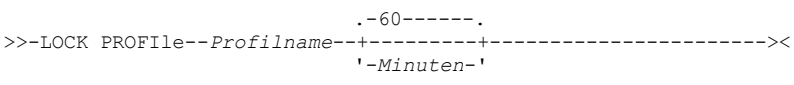
Mit diesem Befehl kann auf einem Konfigurationsmanager ein Profil vorübergehend gesperrt werden, so dass die Konfigurationsdaten nicht an subskribierende verwaltete Server verteilt werden.

Dieser Befehl kann verwendet werden, wenn mehrere Aktualisierungen an der Konfiguration vorgenommen werden und diese Informationen erst verteilt werden sollen, wenn die Änderungen abgeschlossen sind.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Profilname (Erforderlich)
: Gibt das Profil an, das gesperrt werden soll. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben.

Minuten
: Gibt die Zeit in Minuten an, bevor IBM Spectrum Protect das Konfigurationsprofil entsperrt. Eine ganze Zahl von 0 bis 10000 angeben. Der Standardwert ist 60 Minuten. Wenn 0 angegeben wird, wird das Konfigurationsprofil nicht automatisch entsperrt. Den Befehl UNLOCK PROFILE verwenden, um das Profil zu entsperren, bevor die Zeitperiode verstrichen ist, oder um das Profil zu entsperren, wenn der Wert 0 angegeben wurde. Dieser Parameter ist wahlfrei.

Beispiel: Ein Profil für eine bestimmte Zeit sperren

Das Profil DELTA 30 Minuten lang sperren.

```
lock profile delta 30
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für LOCK PROFILE

Befehl	Beschreibung
COPY PROFILE	Erstellt eine Kopie eines Profils.
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DELETE PROFASSOCIATION	Löscht die Zuordnung zwischen einem Objekt und einem Profil.
DELETE PROFILE	Löscht ein Profil aus einem Konfigurationsmanager.
QUERY PROFILE	Zeigt Informationen über Konfigurationsprofile an.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UNLOCK PROFILE	Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

MACRO (Makro aufrufen)

Mit diesem Befehl kann eine Datei über die Verwaltungsbefehlszeile aufgerufen werden, die auszuführende IBM Spectrum Protect-Verwaltungsbefehle enthält.

Einschränkung: Verwenden Sie diesen Befehl nur für Verwaltungsbefehlszeilenclients.

Ein Makro ist eine Datei, die IBM Spectrum Protect-Verwaltungsbefehle enthält. Ein Makro kann vom Verwaltungs-Client nur im Stapelmodus oder im interaktiven Modus ausgegeben werden. Ein Makro wird als Datei auf der Verwaltungs-Client-Maschine (oder dem System) gespeichert. Makros werden nicht an Server verteilt und können nicht auf dem Server geplant werden.

Die Erstellung eines Makros zur Eingabe von Befehlen kann hilfreich sein, wenn Befehle ausgegeben werden sollen, die wiederholt verwendet werden, wenn Befehle ausgegeben werden, die mehrere Parameter enthalten, oder wenn zugehörige Befehle in einer bestimmten Reihenfolge verarbeitet werden sollen. Nach der Erstellung eines Makros können die enthaltenen Informationen aktualisiert und wiederverwendet werden, oder die Makrodatei kann kopiert, die Kopie geändert und dann die Kopie ausgeführt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-MACRO--Makroname--+-----------------------+-----------------><
                     | .-------------------. |
                     | V                   | |
                     '---Substitutionswert-+-'
```

Parameter

Makroname (Erforderlich)
: Gibt den Namen des Makros an.

Substitutionswert
: Gibt den Wert einer Substitutionsvariablen in einem Makro an. Wenn eine Substitutionsvariable verwendet wird, kann ein Makro immer wieder verwendet werden, wenn dieselbe Task für verschiedene Objekte oder mit anderen Parameterwerten ausgeführt werden muß. Um einen Wert anzugeben, der Leerzeichen enthält, muß er in Anführungszeichen eingeschlossen werden. Dieser Parameter ist wahlfrei.

Beispiel: Ein Makro zum Registrieren eines neuen Administrators erstellen

Die Makrodatei REGNG erstellen. Mit Hilfe des Makros einen neuen Administrator registrieren und ihm eine Berechtigung erteilen. Das Makro wie folgt schreiben:

```
/* Neuen Administrator registrieren und Berechtigung erteilen */
REGister Admin jones passwd       -
CONtactinfo="x1235"
GRant AUTHority jones             -
CLasses=Policy
```

Den folgenden Befehl ausgeben, um das Makro auszuführen:

```
macro regng.mac
```

Beispiel: Ein Makro unter Verwendung von Substitutionsvariablen schreiben

Die Makrodatei AUTHRG erstellen, die Substitutionsvariablen enthält, um einen neuen Administrator zu registrieren und ihm eine Berechtigung zu erteilen. Das Makro wie folgt schreiben:

```
/* Neuen Administrator registrieren und Berechtigung erteilen */
REGister Admin %1 %2  -        /*  Benutzer-ID und Kennwort eingeben  */
CONtact=%3         /* Kontaktinfo eingeben (evtl. in Anführungszeichen) */
GRant AUTHority %1  -        /*  Server verwendet die definierte */
-                                    /*  Variable bereits */
CLasses=%4                    /*  Berechtigungsklasse eingeben */
```

Einen Befehl ausgeben, der dem folgenden Befehl ähnelt. Dabei die Werte eingeben, die an den Server übergeben werden sollen, um den Befehl zu verarbeiten, wenn das Makro ausgeführt wird.

```
macro authrg.mac jones passwd x1235 Policy
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für MACRO

Befehl	Beschreibung
COMMIT	Schreibt Änderungen in der Datenbank fest.
ROLLBACK	Löscht alle Änderungen, die seit dem letzten COMMIT nicht in der Datenbank festgeschrieben wurden.

Zugehörige Konzepte:
Makros des Verwaltungsclients

MIGRATE STGPOOL (Speicherpool in nächsten Speicherpool umlagern)

Mit diesem Befehl können Dateien aus einem Speicherpool in den nächsten Speicherpool in der Speicherhierarchie umgelagert werden.

Dieser Befehl kann nur mit primären Speicherpools verwendet werden. Das Datenformat des Speicherpools darf nicht NETAPPDUMP, CELERRADUMP oder NDMPDUMP sein. Daten können nicht in oder aus Speicherpools umgelagert werden, die mit einer Einheitenklasse CENTERA definiert sind.

Für einen bestimmten Speicherpool ist nur jeweils ein Umlagerungs- oder Wiederherstellungsprozess zulässig. Wird für den Speicherpool bereits ein Umlagerungs- oder Wiederherstellungsprozess ausgeführt, kann kein anderer Umlagerungsprozess für den Speicherpool gestartet werden.

Dieser Befehl sollte nur verwendet werden, wenn die automatische Umlagerung für den Speicherpool nicht verwendet wird. Um die Ausführung der automatischen Umlagerung zu verhindern, setzen Sie das Attribut HIGHMIG der Speicherpooldefinition auf 100.

Wird dieser Befehl verwendet, um einen Umlagerungsprozess zu starten, aber ist für den Speicherpool kein nächster Speicherpool in der Hierarchie angegeben, wird ein Wiederherstellungsprozess für den Quellenspeicherpool ausgelöst. Um den Wiederherstellungsprozess zu verhindern, definieren Sie den nächsten Speicherpool in der Hierarchie. Starten Sie dann den Umlagerungsprozess.

Der Befehl MIGRATE STGPOOL berücksichtigt die Werte der folgenden Parameter in den Befehlen DEFINE STGPOOL und UPDATE STGPOOL:

- MIGPROCESS
- MIGDELAY
- MIGCONTINUE
- NEXTPOOL
- LOWMIG
  Tipp: Sie können den Wert des Parameters LOWMIG in den Befehlen DEFINE STGPOOL und UPDATE STGPOOL überschreiben, indem Sie einen Wert für den Parameter LOWMIG im Befehl MIGRATE STGPOOL angeben.

Der Befehl MIGRATE STGPOOL ignoriert den Wert des Parameters HIGHMIG der Speicherpooldefinition. Die Umlagerung erfolgt unabhängig vom Wert des Parameters HIGHMIG.

Dieser Befehl erstellt einen oder mehrere Umlagerungsprozesse, die mit dem Befehl CANCEL PROCESS abgebrochen werden können. Die Anzahl der Prozesse wird durch das Attribut MIGPROCESS der Speicherpooldefinition begrenzt. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Hinweis: Beim Umlagern von Daten aus einem primären Speicherpool, der für die Deduplizierung von Daten definiert ist, in einen anderen primären Speicherpool, der ebenfalls für die Deduplizierung von Daten definiert ist, werden doppelte Daten entfernt.

Berechtigungsklasse

Um diesen Befehl auszugeben, benötigen Sie Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, aus dem die Dateien umgelagert werden sollen, und für den nächsten Speicherpool, in den Dateien umgelagert werden sollen.

Syntax

```
>>-MIGrate STGpool--Poolname--+-----------------+--------------->
                              '-LOwmig--=--Zahl-'

                             .-RECLaim--=--No------.
>--+----------------------+--+---------------------+------------>
   '-DUration--=--Minuten-'  '-RECLaim--=--+-No--+-'
                                           '-Yes-'

   .-Wait--=--No------.
>--+-----------------+-------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'
```

Parameter

Poolname (Erforderlich)
: Gibt den primären Speicherpool an, aus dem Dateien umgelagert werden sollen.

DUration
: Gibt die maximale Anzahl Minuten an, die die Umlagerung ausgeführt wird, bevor sie automatisch abgebrochen wird. Wenn die angegebene Anzahl Minuten verstrichen ist, bricht der Server automatisch alle Umlagerungsprozesse für diesen Speicherpool ab. Sobald die Prozesse den automatischen Abbruch erkennen, werden sie beendet. Aus diesem Grund kann die Umlagerung länger dauern als mit dem Wert für diesen Parameter angegeben ist. Es kann eine Zahl von 1 bis 9999 angegeben werden. Dieser Parameter ist wahlfrei. Falls nicht angegeben, stoppt der Server erst nach Erreichen der unteren Umlagerungsschwelle.

LOwmig
: Gibt für Plattenspeicherpools mit wahlfreiem Zugriff und mit sequenziellem Zugriff an, dass die Umlagerung gestoppt werden soll, wenn das Datenvolumen in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht oder unter diesem Prozentsatz liegt. Dieser Parameter ist wahlfrei.
  Die Berechnung für Plattenspeicherpools mit sequenziellem Zugriff schließt die Kapazität aller für den Pool angegebenen Arbeitsdatenträger ein. Da die Umlagerung je nach Kollokation nach Knoten oder Dateibereich erfolgt, kann die Belegung des Speicherpools unter den für diesen Parameter angegebenen Wert fallen. Um den Speicherpool zu leeren, definieren Sie LOWMIG=0. Für andere Typen von Speicherpools mit sequenziellem Zugriff stoppt der Server die Umlagerung, wenn das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool diesen Prozentsatz erreicht oder unter diesem Prozentsatz liegt. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Sie können eine Zahl von 0 bis 99 für diesen optionalen Parameter angeben. Der Standardwert ist das Attribut LOWMIG der Speicherpooldefinition.

RECLaim
: Gibt an, ob vor der Ausführung der Umlagerung die Wiederherstellung für den Speicherpool versucht wird. Dieser Parameter kann nur für einen Speicherpool mit sequenziellem Zugriff angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

  No
  : Gibt an, dass der Server keine Wiederherstellung vor dem Starten der Umlagerung ausführt.

  Yes
  : Gibt an, dass der Server vor dem Starten der Umlagerung eine Wiederherstellung ausführt. Alle Datenträger in dem Speicherpool, die der Wiederherstellungsschwelle entsprechen, die mit dem Attribut RECLAIM der Speicherpooldefinition angegeben wird, werden vor der Ausführung der Umlagerung wiederhergestellt. Entsprechen keine Datenträger der Wiederherstellungsschwelle, oder wurde nach der Wiederherstellung die LOWMIG-Schwelle nicht erreicht, beginnt der Server mit der Umlagerung. Bevor Speicherbereich für Speicherpools wiederhergestellt wird, die mit RECLAMATIONTYPE=SNAPLOCK definiert sind, löscht der Server während der Wiederherstellungsverarbeitung alle leeren WORM-FILE-Datenträger, die ihren Wiederherstellungszeitraum überschritten haben.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

  No
  : Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

    Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

    Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise bereits einige Dateien vor dem Abbruch umgelagert.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Der Server zeigt dann die Ausgabenachrichten dem Verwaltungsclient an, wenn die Operation beendet ist. Nachrichten werden auch im Aktivitätenprotokoll und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.
Anmerkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

Beispiel: Einen Speicherpool in den nächsten Speicherpool umlagern

Daten aus dem Speicherpool BACKUPPOOL in den nächsten Speicherpool umlagern. Angeben, dass der Server die Umlagerung so schnell wie möglich nach 90 Minuten beenden soll.

```
migrate stgpool backuppool duration=90
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für MIGRATE STGPOOL

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY PROCESS	Zeigt Informationen zu dem Hintergrundprozess an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
RECLAIM STGPOOL	Führt eine Wiederherstellung für den Speicherpool aus.

Zugehörige Informationen:
Dateien in einer Speicherpoolhierarchie umlagern

MOVE-Befehle

Mit den MOVE-Befehlen können Sicherungs- oder Archivierungsdaten zwischen Speicherpools oder Datenträger zur Wiederherstellung nach einem Katastrophenfall vor Ort und an einen ausgelagerten Standort versetzt werden.

- MOVE CONTAINER (Container versetzen)
- MOVE DATA (Dateien auf einem Speicherpooldatenträger versetzen)
- MOVE DRMEDIA (DRM-Datenträger aus- und einlagern)
- MOVE GRPMEMBER (Servergruppenteil versetzen)
- MOVE MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff versetzen)
- MOVE NODEDATA (Daten nach Knoten in einem Speicherpool mit sequenziellem Zugriff versetzen)

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

MOVE CONTAINER (Container versetzen)

Verwenden Sie diesen Befehl, um den Inhalt eines Speicherpoolcontainers in einen anderen Container zu versetzen, wenn ein Speicherpoolverzeichnis entfernt wird oder ein Container beschädigt ist.

Mit diesem Befehl können Sie auch den Inhalt eines Speicherpoolcontainers unter den folgenden Bedingungen versetzen:

- Wenn ein Upgrade für die Hardware durchgeführt wird
- Wenn E/A-Fehler auf einer Platte auftreten

Berechtigungsklasse

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-MOVe CONTainer--Containername------------------------------>

>--+-------------------------------------+--------------------->
   '-STGPOOLDIRectory--=--Verzeichnisname-'

   .-Wait--=--Yes-----.
>--+------------------+---------------------------------------><
   '-Wait--=--+-Yes-+-'
              '-No--'
```

Parameter

Containername (Erforderlich)
Gibt den Namen des Containers an, der versetzt werden soll. Sie müssen den vollständigen Pfadnamen des Containers angeben.

STGPOOLDIRectory
Gibt den Namen des Speicherpoolverzeichnisses an, in das der Container versetzt wird. Dieser Parameter ist wahlfrei.

Wenn Sie ein Speicherpoolverzeichnis angeben, muss es sich in demselben Speicherpool wie der ursprüngliche Container befinden. Das Speicherpoolverzeichnis wird für den neuen Container verwendet. Wenn Sie kein Speicherpoolverzeichnis angeben, wählt der IBM Spectrum Protect-Server ein Speicherpoolverzeichnis aus demselben Speicherpool aus.

Wait
Gibt an, ob darauf gewartet werden soll, dass der IBM Spectrum Protect-Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Geben Sie die folgenden Werte an:

No
Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden. Dies ist der Standardwert.

Yes
Der Server verarbeitet diesen Befehl im Vordergrund. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.
Einschränkung: Sie können den Parameter WAIT=YES nicht an der Serverkonsole angeben.

Beispiel: Einen Container versetzen

 AIX-Betriebssysteme  Linux-BetriebssystemeDen Container 0000000000000001.dcf aus dem Speicherpoolverzeichnis /data1/storage/dir1 in das Speicherpoolverzeichnis /data/storage/dir2 versetzen.

```
move container /data1/storage/dir1/00/0000000000000001.dcf
stgpooldir=/data/storage/dir2
```

 Windows-BetriebssystemeDen Container 0000000000000001.dcf aus dem Speicherpoolverzeichnis e:\data1\storage\dir1 in das Speicherpoolverzeichnis e:\data\storage\dir2 versetzen.

```
move container e:\data1\storage\dir1\00\0000000000000001.dcf
stgpooldir=e:\data\storage\dir2
```

Tabelle 1. Zugehörige Befehle für MOVE CONTAINER

Befehl	Beschreibung
AUDIT CONTAINER	Prüft einen Verzeichniscontainerspeicherpool.
QUERY CONTAINER	Zeigt Informationen zu einem Container an.

MOVE DATA (Dateien auf einem Speicherpooldatenträger versetzen)

Mit diesem Befehl können Dateien von einem Speicherpooldatenträger auf andere Speicherpooldatenträger versetzt werden.

Einschränkung: Sie können diesen Befehl nicht für Datenträger verwenden, die Containerkopienspeicherpools zugeordnet sind.
Dateien von einem Datenträger aus dem primären Speicherpool können nur auf Datenträger in demselben oder einem anderen primären Speicherpool versetzt werden. Dateien von einem Datenträger aus dem Kopienspeicherpool können nur auf Datenträger in demselben Kopienspeicherpool versetzt werden. Dateien von einem Datenträger aus dem Pool für aktive Daten können nur auf Datenträger in demselben Pool für aktive Daten versetzt werden.

Neben dem Versetzen von Daten von Datenträgern in Speicherpools mit dem Datenformat NATIVE oder NONBLOCK können Sie mit diesem Befehl auch Daten von Datenträgern in Speicherpools versetzen, die NDMP-Datenformate haben (NETAPPDUMP, CELERRADUMP oder NDMPDUMP). Der Zielspeicherpool muss dasselbe Datenformat wie der Quellenspeicherpool haben. Werden Daten aus einem Speicherpool zum Zweck eines Upgrades auf eine neue Bandtechnologie versetzt, muss der primäre Zielspeicherpool einem Speicherarchiv zugeordnet sein, das über die neue Einheit für die Bandlaufwerke verfügt. IBM Spectrum Protect unterstützt die Back-End-Datenversetzung für NDMP-Images.

Sie können keine Daten in einen Speicherpool oder aus einem Speicherpool versetzen, der mit einer Einheitenklasse CENTERA definiert ist.

Werden Dateien auf Datenträger in demselben Speicherpool versetzt, muss auf den Datenträgern genügend Speicherbereich verfügbar sein. Andernfalls schlägt die Operation fehl.

Werden Dateien von einem Datenträger mit sequenziellem Zugriff versetzt, sind mehrere Mountoperationen für Datenträger mit sequentiellem Zugriff erforderlich, um Dateien zu versetzen, die sich über mehrere Datenträger erstrecken.

Werden Dateien von einem Datenträger mit wahlfreiem Zugriff versetzt, löscht der Server alle Cachekopien von Dateien auf dem Datenträger.

Ein Datenträger ist möglicherweise nach dem Versetzen von Daten nicht leer, wenn Dateien aufgrund von Ein-/Ausgabefehlern auf der Einheit oder aufgrund von Fehlern in der Datei nicht auf einen anderen Datenträger verlagert werden können. Falls erforderlich, kann der Datenträger mit der Option zum Löschen aller Daten gelöscht werden. Die Dateien mit Ein-/Ausgabefehlern oder anderen Fehlern werden dann gelöscht.

Mit diesem Befehl können Dateien von einem ausgelagerten Datenträger in einen Kopienspeicherpool oder einen Pool für aktive Daten versetzt werden. Da der ausgelagerte Datenträger nicht geladen werden kann, ruft der Server die Dateien auf dem ausgelagerten Datenträger entweder aus einem primären Speicherpool oder einem anderen Kopienspeicherpool ab. Diese Dateien werden dann auf die Zieldatenträger im ursprünglichen Kopienspeicherpool oder Pool für aktive Daten geschrieben.

Während des Datenversetzungsprozesses können Pools für aktive Daten nicht verwendet werden, um Daten abzurufen.

Wenn Sie den Befehl MOVE DATA für einen ausgelagerten Datenträger angeben, der durch Kollokation zusammengefasste Daten enthält, müssen Sie den Befehl MOVE DATA möglicherweise mehrmals ausgeben, um alle Daten von dem Datenträger zu versetzen. Wenn Sie beispielsweise Dateibereichskollokationsgruppen mit einem ausgelagerten Datenträger verwenden, der Dateibereiche in einer Kollokationsgruppe und Dateibereiche, die nicht in der Gruppe sind, enthält, müssen Sie zwei Befehle MOVE DATA ausgeben. Mit jedem Befehl MOVE DATA werden die Daten für eine einzelne kollokierte oder nicht kollokierte Gruppe von Dateien versetzt.

Der Befehl MOVE DATA darf nicht verwendet werden, wenn ein Zurückschreibungsprozess (RESTORE STGPOOL oder RESTORE VOLUME) ausgeführt wird. Durch den Befehl MOVE DATA könnte die Zurückschreibung unvollständig sein. Wird der Befehl MOVE DATA während einer Zurückschreibungsoperation ausgegeben und empfangen Sie eine Fehlernachricht, die angibt, dass eine oder mehrere Dateien gesperrt sind und nicht versetzt werden können, müssen Sie den Befehl MOVE DATA nach Beendigung der Zurückschreibungsoperation erneut ausgeben, damit alle übrigen Dateien versetzt werden.

Hinweis:
Wird dieser Befehl ausgegeben, werden doppelte Daten entfernt, wenn:

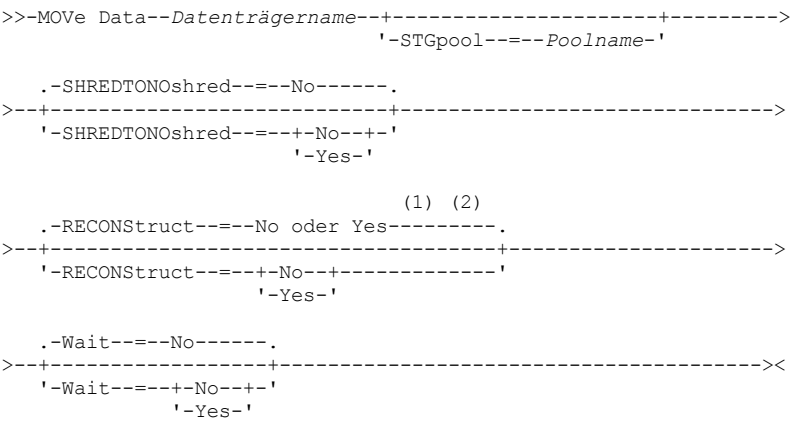
- Daten aus einem primären Speicherpool, der für die Deduplizierung von Daten definiert ist, in einen anderen primären Speicherpool versetzt werden, der ebenfalls für die Deduplizierung von Daten definiert ist.
- Daten innerhalb eines Kopienspeicherpools versetzt werden, der für die Deduplizierung von Daten definiert ist.
- Daten innerhalb eines Pools für aktive Daten versetzt werden, der für die Deduplizierung von Daten definiert ist.

Ein Datenträger in einem deduplizierten Speicherpool kann Dateien enthalten, die logisch gelöscht sind, aber dennoch mit Dateien auf anderen Datenträgern verknüpft sind. Wenn Sie den Befehl MOVE DATA verwenden, um den Inhalt eines deduplizierten Speicherpooldatenträgers in einen nicht deduplizierten Speicherpool zu versetzen, werden die logisch gelöschten Dateien nicht auf den neuen Datenträger geschrieben, da sie logisch nicht vorhanden sind. Die gelöschten Dateien werden zur Referenzierung anderer Dateien auf den Originaldatenträgern aufbewahrt. Der Prozess MOVE DATA wird erfolgreich beendet, aber die gelöschten Dateien werden nicht auf den neuen Zieldatenträger versetzt und der Quellendatenträger wird nicht gelöscht. Sie können den Befehl QUERY CONTENT mit dem Parameter FOLLOWLINKS=YES oder FOLLOWLINKS=JUSTLINKS ausgeben, um zu prüfen, ob der Datenträger Dateien enthält, die mit Dateien auf anderen Datenträgern verknüpft sind.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder die eingeschränkte Speicherberechtigung für den Speicherpool erforderlich, zu dem der Datenträger gehört, sowie für den neuen Speicherpool, sofern angegeben.

Syntax



Anmerkungen:

1. Der Standardwert ist NO, wenn entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff ist. Der Standardwert ist YES, wenn sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff ist.
2. Dieser Parameter ist nicht verfügbar oder wird ignoriert, wenn das Datenformat NETAPPDUMP, CELERRADUMP oder NDMPDUMP ist.

Parameter

Datenträgername (Erforderlich)
: Gibt den Speicherpooldatenträger an, von dem Dateien versetzt werden sollen.

STGpool
: Gibt den primären Speicherpool an, in den Dateien versetzt werden sollen (Zielspeicherpool). Dieser Parameter ist wahlfrei und gilt nur für das Versetzen von Daten von Datenträgern aus dem primären Speicherpool. Wird kein Wert für diesen Parameter angegeben, werden Dateien auf andere Datenträger in demselben Speicherpool versetzt.

SHREDTONOshred
: Gibt an, ob Daten aus einem Speicherpool, der das Schreddern erzwingt, in einen Speicherpool, der das Schreddern nicht erzwingt, versetzt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, dass es der Server nicht erlaubt, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, in einen Speicherpool, der das Schreddern nicht erzwingt, versetzt werden. Wenn der Quellenspeicherpool das Schreddern erzwingt und der Zielspeicherpool das Schreddern nicht erzwingt, schlägt die Operation fehl.

  Yes
  : Gibt an, dass es der Server erlaubt, dass Daten aus einem Speicherpool, der das Schreddern erzwingt, in einen Speicherpool, der das Schreddern nicht erzwingt, versetzt werden. Die Quellendaten werden geschreddert, wenn die Operation abgeschlossen ist. Die Zieldaten werden beim Löschen nicht geschreddert.

RECONStruct
: Gibt an, ob Dateiaggregate beim Versetzen von Daten wiederhergestellt werden sollen. Bei der Wiederherstellung wird leerer Speicherbereich entfernt, der sich durch das Löschen von logischen Dateien aus einem Aggregat angesammelt hat. Dieser Parameter ist wahlfrei. Ist sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff, ist der Standardwert YES. Ist entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff, ist der Standardwert NO. Der Parameter ist nicht verfügbar oder wird ignoriert, wenn eine der folgenden Bedingungen zutrifft:

  - Das Datenformat ist NETAPPDUMP, CELERRADUMP oder NDMPDUMP.
  - Die Daten befinden sich in einem Speicherpool, der für die Deduplizierung von Daten konfiguriert ist.
  - Der Zielspeicherpool für die Datenversetzung ist für die Deduplizierung von Daten konfiguriert.

  Achtung: Bei der Wiederherstellung werden inaktive Sicherungsdateien in Pools für aktive Daten entfernt. Geben Sie RECONSTRUCT=NO an, wenn die Daten in einen Pool für aktive Daten versetzt werden, der nicht für die Deduplizierung von Daten konfiguriert ist, verbleiben inaktive Sicherungsdateien in dem Speicherpool.

  Gültige Werte:

  No
  : Gibt an, dass die Wiederherstellung von Dateiaggregaten beim Versetzen von Daten nicht ausgeführt wird.

  Yes
  : Gibt an, dass die Wiederherstellung von Dateiaggregaten beim Versetzen von Daten ausgeführt wird. Sie können diese Option nur angeben, wenn Quellen- und Zielspeicherpool Speicherpools mit sequenziellem Zugriff sind.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

  No
  : Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

    Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

    Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird ein Hintergrundprozess MOVE DATA abgebrochen, wurden einige Dateien möglicherweise vor dem Abbruch bereits versetzt.

  Yes
  : Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist. Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

Beispiel: Dateien auf einem Speicherpooldatenträger versetzen

Dateien vom Speicherpooldatenträger STGVOL.1 auf alle verfügbaren Datenträger versetzen, die dem Speicherpool 8MMPOOL zugeordnet sind.

```
move data stgvol.1 stgpool=8mmpool
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für MOVE DATA

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
DELETE VOLUME	Löscht einen Datenträger aus einem Speicherpool.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY CONTENT	Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY SHREDSTATUS	Zeigt Informationen zu Daten an, die auf das Schreddern warten.
SHRED DATA	Startet manuell den Prozess zum Schreddern gelöschter Daten.

MOVE DRMEDIA (DRM-Datenträger aus- und einlagern)

Mit diesem Befehl können Datenträger verfolgt werden, die ausgelagert werden sollen, und verfallene oder leere Datenträger identifiziert werden, die vor Ort versetzt werden sollen. Sie können Datenbanksicherungsdatenträger und Datenträger in Kopienspeicherpools, Containerkopienspeicherpools und Speicherpools für aktive Daten verfolgen.

Die Verarbeitung von Datenträgern durch diesen Befehl hängt vom Verwendungszweck der Datenträger ab:

Sicherungen der Serverdatenbank
: Mit dem Parameter SOURCE in diesem Befehl kann gesteuert werden, ob der Befehl Datenbanksicherungsdatenträger verarbeitet. Der Befehl kann Datenträger verarbeiten, die für Gesamt- und Teilsicherungen oder Datenbankmomentaufnahmesicherungen verwendet werden. Es können keine virtuellen Datenträger angegeben werden (Sicherungsobjekte, die auf einem anderen Server gespeichert werden). Datenträger können von Status zu Status geändert werden, oder es können der Parameter TOSTATE verwendet und Status übersprungen werden, um die Bewegungen zu vereinfachen.

Kopienspeicherpools
: Der Befehl MOVE DRMEDIA verarbeitet immer Kopienspeicherpooldatenträger.

Containerkopienspeicherpools
: Standardmäßig sind Datenträger in Containerkopienspeicherpools nicht für die Verarbeitung mit dem Befehl MOVE DRMEDIA auswählbar. Um Datenträger in Containerkopienspeicherpools zu verarbeiten, müssen Sie zuerst den Befehl SET DRMCOPYCONTAINERSTGPOOL ausgeben oder den Parameter COPYCONTAINERSTGPOOL im Befehl MOVE DRMEDIA angeben.

Speicherpools für aktive Daten
: Standardmäßig sind Datenträger in Speicherpools für aktive Daten nicht für die Verarbeitung mit dem Befehl MOVE DRMEDIA auswählbar. Um Datenträger in Pools für aktive Daten zu verarbeiten, müssen Sie zuerst den Befehl SET DRMACTIVEDATASTGPOOL ausgeben oder den Parameter ACTIVEDATASTGPOOL im Befehl MOVE DRMEDIA angeben.

Mit dem Befehl QUERY ACTLOG kann abgefragt werden, ob der Befehl MOVE DRMEDIA erfolgreich ausgeführt wurde. Diese Informationen können auch über die Serverkonsole angezeigt werden.

Einschränkung: Führen Sie die Befehle MOVE DRMEDIA und BACKUP STGPOOL nicht gleichzeitig aus. Stellen Sie sicher, dass die Speicherpoolsicherungsprozesse abgeschlossen wurden, bevor der Befehl MOVE DRMEDIA ausgegeben wird.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Wenn der Parameter CMD angegeben wird und die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt ist: Bedienerberechtigung, uneingeschränkte Speicherberechtigung oder Systemberechtigung.
- Wenn der Parameter CMD angegeben wird und die Serveroption REQSYSAUTHOUTFILE auf YES (Standardwert) gesetzt ist: Systemberechtigung.

Syntax

```
>>-MOVe DRMedia--Datenträgername------------------------------->

>--+-------------------------------------+---------------------->
   '-WHERESTate--=--+-MOuntable-------+-'
                    +-NOTMOuntable----+
```

Parameter

Datenträgername (Erforderlich)

Gibt den Namen des Datenträgers an, der verarbeitet werden soll. Es können Platzhalterzeichen verwendet werden. Werden bei der Angabe dieses Namens Platzhalterzeichen verwendet, muss auch der Parameter WHERESTATE angegeben werden. Der Server sucht nach übereinstimmenden Namen unter den folgenden auswählbaren Datenträgern:

- Datenbanksicherungsdatenträger, die mit dem Parameter SOURCE dieses Befehls angegeben wurden.
- Kopienspeicherpooldatenträger in Speicherpools, die im Parameter COPYSTGPOOL angegeben wurden. Wird der Parameter COPYSTGPOOL nicht verwendet, verarbeitet der Server Datenträger aus Kopienspeicherpools, die zuvor im Befehl SET DRMCOPYSTGPOOL angegeben wurden.
- Containerkopienspeicherpooldatenträger in Speicherpools, die im Parameter COPYCONTAINERSTGPOOL angegeben wurden. Wenn der Parameter COPYCONTAINERSTGPOOL nicht verwendet wird, verarbeitet der Server Datenträger aus Containerkopienspeicherpools, die zuvor im Befehl SET DRMCOPYCONTAINERSTGPOOL angegeben wurden.
- Datenträger im Speicherpool für aktive Daten in Speicherpools, die im Parameter ACTIVEDATASTGPOOL angegeben wurden. Wird der Parameter ACTIVEDATASTGPOOL nicht verwendet, verarbeitet der Server Datenträger aus Speicherpools für aktive Daten, die zuvor im Befehl SET DRMACTIVEDATASTGPOOL angegeben wurden.

Andere Parameter können ebenfalls die Ergebnisse des Befehls begrenzen.

WHERESTate

Gibt den Status der zu verarbeitenden Datenträger an. Dieser Parameter ist erforderlich, wenn der Parameter TOSTATE nicht angegeben wird oder wenn ein Platzhalterzeichen in dem Datenträgernamen verwendet wird. Näheres dazu siehe Tabelle 2 und Tabelle 3. Geben Sie

einen der folgenden Werte an:

MOuntable

Diese Datenträger enthalten gültige Daten und sind für die Verarbeitung vor Ort verfügbar. Die Werte ändern sich in NOTMOUNTABLE, wenn der Parameter TOSTATE nicht angegeben wird.

Abhängig vom Ergebnis des Parameters REMOVE kann der Server Datenträger in einem automatisierten Kassettenarchiv ausgeben, bevor der Zielstatus geändert wird.

Bei externen Kassettenarchiven sendet der Server Anforderungen zur Ausgabe der Datenträger an den externen Kassettenarchivmanager. Es hängt vom externen Kassettenarchivmanager ab, ob die Datenträger aus dem Kassettenarchiv ausgegeben werden.

NOTMOuntable
Diese Datenträger befinden sich vor Ort, enthalten gültige Daten und stehen nicht für die Verarbeitung vor Ort zur Verfügung. Die Werte ändern sich in COURIER, wenn der Parameter TOSTATE nicht angegeben wird.

COUrier
Diese Datenträger werden mit dem Kurier ausgelagert. Die Werte ändern sich nur in VAULT.

VAULTRetrieve
Diese Datenträger befinden sich an dem ausgelagerten Aufbewahrungsort und enthalten keine gültigen Daten. Die Werte ändern sich in COURIERRETRIEVE, wenn der Parameter TOSTATE nicht angegeben wird.

COURIERRetrieve
Diese Datenträger werden mit dem Kurier vor Ort versetzt. Die Werte ändern sich nur in ONSITERETRIEVE. Der Server löscht die Datenträgersätze der Datenbanksicherungsdatenträger und Kopienspeicherpoolarbeitsdatenträger aus der Datenbank.

BEGINDate
Gibt das Anfangsdatum an, das zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach dem angegebenen Datum in seinen aktuellen Status ändert. Standardwert ist das früheste Datum, ab dem Datenträgerdaten vorliegen.
Sie können das Datum mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum.	`09/15/1998`
TODAY	Das aktuelle Datum.	`TODAY`
TODAY-Tage oder -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage.	`TODAY-7` oder `-7` Sollen Datenträger identifiziert werden, die vor einer Woche in ihren aktuellen Status geändert wurden, können Sie `TODAY-7` oder `-7` angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	`EOLM`
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	`EOLM-1` Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	`BOTM`
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	`BOTM+9` Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDDate
Gibt das Enddatum an, das zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder vor dem angegebenen Datum in seinen aktuellen Status ändert. Standardwert ist das aktuelle Datum.
Sie können das Datum mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum.	`09/15/1998`
TODAY	Das aktuelle Datum.	`TODAY` Sollen Datenträger identifiziert werden, die heute in ihren aktuellen Status geändert wurden, geben Sie `TODAY` an.

Wert	Beschreibung	Beispiel
TODAY-Tage oder -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage beträgt 9999.	`TODAY-1` oder `-1` Sollen Datenträger identifiziert werden, die vor einer Woche in ihren aktuellen Status geändert wurden, können Sie `TODAY-1` oder `-1` angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	`EOLM`
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	`EOLM-1` Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	`BOTM`
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	`BOTM+9` Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt die Anfangszeit an, die zum Auswählen der Datenträger für die Verarbeitung verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach der angegebenen Uhrzeit und dem angegebenen Datum in seinen aktuellen Status ändert. Der Standardwert ist Mitternacht (00:00:00) an dem mit dem Parameter BEGINDATE angegebenen Datum.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Anfangsdatum.	`12:33:28`
NOW	Die aktuelle Uhrzeit am angegebenen Anfangsdatum.	`NOW`
NOW+HH:MM oder +HH:MM	Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum.	`NOW+03:00` oder `+03:00`
NOW-HH:MM oder -HH:MM	Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Anfangsdatum.	`NOW-03:30` oder `-03:30` Wird der Befehl MOVE DRMEDIA um 9:00 Uhr mit der Angabe BEGINTIME=NOW-03:30 oder BEGINTIME=-03:30 ausgegeben, identifiziert der Server die Datenträger, die um 5:30 Uhr am angegebenen Anfangsdatum in ihren aktuellen Status geändert wurden.

ENDTime

Gibt die Endzeit an, die zum Auswählen der Datenträger für die Verarbeitung verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach der angegebenen Uhrzeit und dem angegebenen Datum in seinen aktuellen Status ändert. Der Standardwert ist 23:59:59.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Enddatum.	`12:33:28`
NOW	Die aktuelle Uhrzeit am angegebenen Enddatum.	`NOW`
NOW+HH:MM oder +HH:MM	Die aktuelle Uhrzeit plus der Anzahl Stunden und Minuten am angegebenen Enddatum.	`NOW+03:00` oder `+03:00` Wird der Befehl MOVE DRMEDIA um 9:00 Uhr mit der Angabe ENDTIME=NOW+03:30 oder ENDTIME=+03:30 ausgegeben, identifiziert der Server die Datenträger, die um 12:30 Uhr am angegebenen Enddatum in ihren aktuellen Status geändert wurden.
NOW-HH:MM oder -HH:MM	Die aktuelle Uhrzeit minus der Anzahl Stunden und Minuten am angegebenen Enddatum.	`NOW-03:30` oder `-03:30`

COPYCONtainerstgpool

Gibt den Namen des Containerkopienspeicherpools an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Werden bei der Angabe dieses Namens Platzhalterzeichen verwendet, muss auch der Parameter WHERESTATE angegeben werden.

Die mit diesem Parameter angegebenen Containerkopienspeicherpools überschreiben die mit dem Befehl SET DRMCOPYCONTAINERSTGPOOL angegebenen Speicherpools. Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

- Wenn der Befehl SET DRMCOPYCONTAINERSTGPOOL zuvor mit gültigen Containerkopienspeicherpoolnamen ausgegeben wurde, verarbeitet der Server nur diese Speicherpools.
- Wenn der Befehl SET DRMCOPYCONTAINERSTGPOOL nicht ausgegeben wurde oder alle Containerkopienspeicherpools mit dem Befehl SET DRMCOPYCONTAINERSTGPOOL entfernt wurden, verarbeitet der Server alle Containerkopienspeicherpooldatenträger auf der Basis der Einstellung des Parameters WHERESTATE. Wird der Parameter auf den Wert NOTMOUNTABLE, COURIER, VAULTRETRIEVE oder COURIERRETRIEVE gesetzt, werden die Datenträger verarbeitet. Lautet der Wert MOUNTABLE, werden die Datenträger nicht verarbeitet.

COPYstgpool
: Gibt den Namen des Kopienspeicherpools an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Werden bei der Angabe dieses Namens Platzhalterzeichen verwendet, muss auch der Parameter WHERESTATE angegeben werden.

  Die mit diesem Parameter angegebenen Kopienspeicherpools überschreiben die mit dem Befehl SET DRMCOPYSTGPOOL angegebenen Kopienspeicherpools. Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

  - Wurde der Befehl SET DRMCOPYSTGPOOL zuvor mit gültigen Kopienspeicherpoolnamen ausgegeben, verarbeitet der Server nur diese Speicherpools.
  - Wurde der Befehl SET DRMCOPYSTGPOOL nicht ausgegeben, oder werden alle Kopienspeicherpools mit dem Befehl SET DRMCOPYSTGPOOL entfernt, verarbeitet der Server alle Kopienspeicherpooldatenträger in dem angegebenen Status. Die verfügbaren Status sind MOUNTABLE, NOTMOUNTABLE, COURIER, VAULTRETRIEVE und COURIERRETRIEVE.

ACTIVEDatastgpool
: Gibt den Namen des Pools für aktive Daten an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Werden bei der Angabe dieses Namens Platzhalterzeichen verwendet, muss auch der Parameter WHERESTATE angegeben werden.

  Die mit diesem Parameter angegebenen Pools für aktive Daten überschreiben die mit dem Befehl SET DRMACTIVEDATASTGPOOL angegebenen Pools für aktive Daten. Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

  - Wurde der Befehl SET DRMACTIVEDATASTGPOOL zuvor mit gültigen Namen von Pools für aktive Daten ausgegeben, verarbeitet der Server nur diese Speicherpools.
  - Wurde der Befehl SET DRMACTIVEDATASTGPOOL nicht ausgegeben, oder werden alle Pools für aktive Daten mit dem Befehl SET DRMACTIVEDATASTGPOOL entfernt, verarbeitet der Server alle Datenträger im Pool für aktive Daten in dem angegebenen Status. Die verfügbaren Status sind NOTMOUNTABLE, COURIER, VAULTRETRIEVE und COURIERRETRIEVE. Datenträger im Status MOUNTABLE werden nicht verarbeitet.

Source
: Gibt an, ob Datenbanksicherungsdatenträger bei der Verarbeitung berücksichtigt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBACKUP. Geben Sie einen der folgenden Werte an:

  DBBackup
  : Gibt an, dass der Server Datenbanksicherungsdatenträger mit Gesamt- und Teilsicherungen bei der Verarbeitung berücksichtigt.

  DBSnapshot
  : Gibt an, dass der Server Sicherungsdatenträger mit Datenbankmomentaufnahmen bei der Verarbeitung berücksichtigt.

  DBNOne
  : Gibt an, dass der Server keine Datenbanksicherungsdatenträger bei der Verarbeitung berücksichtigt.

REMove
: Gibt an, dass der Server versucht, den Datenträger aus dem Kassettenarchiv in die Serviceein-/-ausgabestation oder die Eingangs-/Ausgangsanschlüsse zu versetzen. Dieser Parameter ist wahlfrei. Gültige Werte sind YES, NO, BULK und UNTILEEFULL. Der Standardwert ist BULK. Die Antwort des Servers auf jeden Wert und den Standardwert hängt vom Typ des Speicherarchivs ab. Einschränkung: Sie können die Option REMOVE=UNTILEEFULL nur mit dem Speicherarchivtyp SCSI verwenden.

  SCSI-Kassettenarchive
  : Die Antwort des Servers auf den Befehl ist davon abhängig, ob das Speicherarchiv Eingangs-/Ausgangsanschlüsse hat und, wenn dies der Fall ist, ob ein Anschluss für die Verwendung verfügbar ist. Siehe die folgende Tabelle.

Tabelle 1. Antwort des Servers für SCSI-Kassettenarchive

Kassettenarchiv-merkmal	**Antwort des Servers bei Angabe von REMOVE=YES**	**Antwort des Servers bei Angabe von REMOVE=BULK**	**Antwort des Servers bei Angabe von REMOVE=NO**	**Antwort des Servers bei Angabe von REMOVE=UNTILEEFULL**

Kassettenarchivmerkmal	**Antwort des Servers bei Angabe von REMOVE=YES**	**Antwort des Servers bei Angabe von REMOVE=BULK**	**Antwort des Servers bei Angabe von REMOVE=NO**	**Antwort des Servers bei Angabe von REMOVE=UNTILEEFULL**
Kassettenarchiv hat keine Eingangs-/Ausgangsanschlüsse	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.
Kassettenarchiv hat Eingangs-/Ausgangsanschlüsse und ein Eingangs-/Ausgangsanschluss ist verfügbar	Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an. Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.	Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.	Gibt der Server die Anschlussadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.	Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.
Kassettenarchiv hat Eingangs-/Ausgangsanschlüsse, aber es sind keine Anschlüsse verfügbar	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.	Wartet der Server auf einen verfügbaren Anschluss.	Gibt der Server die Anschlussadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.	Schlägt der Befehl fehl, und alle verbleibenden auswählbaren Datenträger werden nicht verarbeitet. Machen Sie den Anschluss verfügbar und wiederholen Sie den Befehl.

349X-Kassettenarchive

REMOVE=YES
Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Serviceein-/-ausgabestation aus.

REMOVE=BULK
Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Ausgabeeinrichtung mit hoher Speicherkapazität aus.

REMOVE=NO
Der 3494-Kassettenarchivmanager (Library Manager) gibt den Datenträger nicht aus. Der Server lässt die Kassette für die Verwendung durch andere Anwendungen in dem Kassettenarchiv in der Kategorie INSERT.

ACSLS-Kassettenarchive

REMOVE=YES oder REMOVE=BULK
Der Server gibt die Kassette an die Serviceein-/-ausgabestation aus.

Dann löscht der Server den Datenträgereintrag aus dem Serverdatenträgerbestand im Kassettenarchiv.

Wenn Sie Datenträger aus dem Status MOUNTABLE unter Angabe von REMOVE=YES versetzen, verwendet der Befehl MOVE MEDIA mehrere Schächte in dem CAP für ein StorageTek-Kassettenarchiv mit ACSLS.

REMOVE=NO
Der Server gibt die Kassette nicht aus.

Der Server löscht den Datenträgereintrag aus dem Kassettenarchivbestand des Servers und lässt den Datenträger in dem Kassettenarchiv.

Externe Kassettenarchive
Sie können REMOVE=YES, REMOVE=BULK oder REMOVE=NO angeben. Für jeden Wert fordert der Server den externen Kassettenarchivmanager zur Ausgabe des Datenträgers aus dem Kassettenarchiv auf.

Es hängt vom externen Kassettenarchivmanager ab, ob der Datenträger aus dem Kassettenarchiv ausgegeben wird. Lesen Sie in der Dokumentation zum externen Kassettenarchiv die Informationen zu den Prozeduren, die ausgeführt werden müssen, wenn Sie den Befehl MOVE DRMEDIA verwenden, um Datenträger zu verfolgen.

TOSTate
Gibt den Zielstatus der Datenträger an, die verarbeitet werden. Dieser Parameter ist erforderlich, wenn der Parameter WHERESTATE nicht angegeben wird. Wird der Parameter TOSTATE angegeben, aber der Parameter WHERESTATE nicht angegeben, müssen Sie den Datenträgernamen angeben. Platzhalterzeichen sind nicht zulässig.Siehe Tabelle 2 und Tabelle 3.
Geben Sie einen der folgenden Werte an:

NOTMOuntable
Gibt an, dass Datenträger in den Status NOTMOUNTABLE übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status MOUNTABLE haben.

Befinden sich Datenträger in einem automatisierten Kassettenarchiv, kann der Server die Datenträger abhängig vom Verhalten des Parameters REMOVE aus dem Kassettenarchiv ausgeben, bevor sie in den Status NOTMOUNTABLE geändert werden.

Bei externen Kassettenarchiven sendet der Server Anforderungen zur Ausgabe der Datenträger an den externen Kassettenarchivmanager. Es hängt vom externen Kassettenarchivmanager ab, ob die Datenträger aus dem Kassettenarchiv ausgegeben werden. Lesen Sie in der Dokumentation zum externen Kassettenarchiv die Informationen zu den Prozeduren, die ausgeführt werden müssen, wenn Sie den Befehl MOVE DRMEDIA verwenden, um die Datenträger zu verfolgen.

COUrier
Gibt an, dass Datenträger in den Status COURIER übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status MOUNTABLE oder NOTMOUNTABLE haben.

Abhängig vom Verhalten des Parameters REMOVE und davon, ob sich Datenträger in einem automatisierten Kassettenarchiv befinden, kann der Server die Datenträger aus dem Kassettenarchiv ausgeben, bevor sie in den Status COURIER geändert werden.

Bei externen Kassettenarchiven sendet der Server Anforderungen zur Ausgabe der Datenträger an den externen Kassettenarchivmanager. Es hängt vom externen Kassettenarchivmanager ab, ob die Datenträger aus dem Kassettenarchiv ausgegeben werden. Lesen Sie in der Dokumentation zum externen Kassettenarchiv die Informationen zu den Prozeduren, die ausgeführt werden müssen, wenn Sie den Befehl MOVE DRMEDIA verwenden, um die Datenträger zu verfolgen.

VAult
Gibt an, dass Datenträger in den Status VAULT übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status MOUNTABLE, NOTMOUNTABLE oder COURIER haben.

Abhängig vom Verhalten des Parameters REMOVE und davon, ob sich Datenträger in einem automatisierten Kassettenarchiv befinden, kann der Server die Datenträger aus dem Kassettenarchiv ausgeben, bevor sie in den Status VAULT geändert werden.

Bei externen Kassettenarchiven sendet der Server Anforderungen zur Ausgabe der Datenträger an den externen Kassettenarchivmanager. Es hängt vom externen Kassettenarchivmanager ab, ob die Datenträger aus dem Kassettenarchiv ausgegeben werden. Lesen Sie in der Dokumentation zum externen Kassettenarchiv die Informationen zu den Prozeduren, die ausgeführt werden müssen, wenn Sie den Befehl MOVE DRMEDIA verwenden, um die Datenträger zu verfolgen.

COURIERRetrieve
Gibt an, dass Datenträger in den Status COURIERRETRIEVE übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status VAULTRETRIEVE haben.

ONSITERetrieve
Gibt an, dass Datenträger in den Status ONSITERETRIEVE übergehen sollen. Dieser Wert ist nur gültig, wenn die Datenträger den Status VAULTRETRIEVE oder COURIERRETRIEVE haben. Für Datenbanksicherungsdatenträger und Arbeitsdatenträger aus Kopienspeicherpools, die in den Status ONSITERETRIEVE übergehen, löscht der Server die Datenträgersätze aus der Datenbank.

WHERELOcation
Gibt den aktuellen Standort der Datenträger an. Dieser Parameter ist wahlfrei. Die maximale Länge des Standorts beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

TOLOcation
Gibt den Zielstandort der Datenträger an. Dieser Parameter ist wahlfrei. Die maximale Länge des angegebenen Standorts beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.Wird kein Zielstandort angegeben, wird der mit dem

Befehl SET DRMNOTMOUNTABLE definierte Standort verwendet.

CMd

Gibt einen Befehl an, der für jeden Datenträger ausgegeben werden soll, der von dem Befehl MOVE DRMEDIA verarbeitet wird. DRM schreibt die Befehle in eine Datei, die mit dem Parameter CMDFILENAME angegeben wird. Nach Abschluss der Operation MOVE DRMEDIA können die Befehle in der Datei ausgegeben werden. Der Befehl kann bis zu 255 Zeichen enthalten. Enthält der Befehl mehr als 240 Zeichen, wird er in mehrere Zeilen geteilt und es werden Fortsetzungszeichen (+) hinzugefügt. Sie müssen möglicherweise das Fortsetzungszeichen auf der Basis des Betriebssystems ändern. Dieser Parameter ist wahlfrei.

Befehl

Die Befehlszeichenfolge, die in Anführungszeichen eingeschlossen wird. Die Zeichenfolge darf keine eingebetteten Anführungszeichen enthalten. Beispielsweise ist der folgende Parameter CMD gültig:

```
cmd="checkin libvol lib8mm &vol status=scratch"
```

Das folgende Beispiel zeigt eine ungültige Angabe des Parameters CMD:

```
cmd=""checkin libvol lib8mm" &vol status=scratch""
```

Der Befehl kann Substitutionsvariablen enthalten. Bei den Variablen muss die Groß-/Kleinschreibung nicht berücksichtigt werden. Die Variablen dürfen keine Leerstellen hinter dem Et-Zeichen (&) enthalten. Sie können die folgenden Werte angeben:

&VOL
: Ein Datenträgername.

&LOC
: Ein Datenträgerstandort.

&VOLDSN
: Der Dateiname, der in die Kennsätze der Datenträger mit sequenziellem Zugriff geschrieben werden soll. Wenn beispielsweise die entsprechende Einheitenklasse BKP als Präfix des Banddatenträgers definiert, könnte der Dateiname eines Kopienspeicherpoolbanddatenträgers BKP.BFS und der Dateiname eines Datenbanksicherungsbanddatenträgers BKP.DBB lauten.

&NL
: Das Zeilenvorschubzeichen. Wenn Sie das Zeilenvorschubzeichen verwenden, wird der Befehl bei der Variablen &NL geteilt. Falls erforderlich, muss das entsprechende Fortsetzungszeichen vor dem &NL-Zeichen angegeben werden. Wird das &NL-Zeichen nicht angegeben und hat die Befehlszeile mehr als 240 Zeichen, wird die Zeile in mehrere Zeilen geteilt und es werden Fortsetzungszeichen (+) hinzugefügt.

 AIX-Betriebssysteme  Linux-BetriebssystemeCMDFilename

AIX-Betriebssysteme  Linux-BetriebssystemeGibt den vollständig qualifizierten Namen der Datei an, die die durch den Parameter CMD angegebenen Befehle enthält. Dieser Parameter ist wahlfrei.

Wird kein Dateiname angegeben oder wird eine Nullzeichenfolge ("") angegeben, verwendet DRM den mit dem Befehl SET DRMCMDFILENAME angegebenen Dateinamen. Wird kein Dateiname mit dem Befehl SET DRMCMDFILENAME angegeben, generiert DRM einen Dateinamen, indem `exec.cmds` an den Namen des Verzeichnispfads des aktuellen Arbeitsverzeichnisses des Servers angehängt wird.

Schlägt die Operation fehl, nachdem die Befehlsdatei erstellt wurde, wird die Datei nicht gelöscht.

 Windows-BetriebssystemeCMDFilename

Windows-BetriebssystemeGibt den vollständig qualifizierten Namen der Datei an, die die durch den Parameter CMD angegebenen Befehle enthält. Dieser Parameter ist wahlfrei.

Die maximale Länge des Dateinamens beträgt 259 Zeichen. Wird kein Dateiname angegeben oder wird eine Nullzeichenfolge ("") angegeben, verwendet DRM den mit dem Befehl SET DRMCMDFILENAME angegebenen Dateinamen. Wird kein Dateiname mit dem Befehl SET DRMCMDFILENAME angegeben, generiert DRM einen Dateinamen, indem `exec.cmd` an das Verzeichnis angehängt wird, das diese Instanz des Servers darstellt (normalerweise das Verzeichnis, aus dem der Server installiert wurde). DRM ordnet den angegebenen oder generierten Dateinamen zu. Ist der Dateiname vorhanden, versucht DRM, den Namen zu verwenden; alle vorhandenen Daten werden überschrieben. Wenn dies eintritt und die ausführbaren Befehle in der Datei noch nicht ausgeführt wurden, geben Sie den Befehl QUERY DRMEDIA aus, um die ausführbaren Befehle für das gewünschte Datum und den gewünschten Datenträgerübergang wiederherzustellen.

Schlägt der Befehl MOVE DRMEDIA fehl und werden keine Informationen der mit dem Parameter CMD angegebenen Befehlszeichenfolge für den erfolgreich versetzten Datenträger geschrieben, wird der zugeordnete Dateiname gelöscht.

APPend

Gibt an, ob der vorhandene Inhalt der Befehlsdatei überschrieben werden soll oder ob die Befehle an die Datei angehängt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie einen der folgenden Werte an:

No
: DRM überschreibt den Inhalt der Datei.

Yes
: DRM hängt die Befehle an die Datei an.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie einen der folgenden Werte an:

No
: Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

  Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

  Um zu prüfen, ob die Operation erfolgreich war, den Befehl QUERY ACTLOG ausgeben.

Yes
: Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Erst nachdem der Befehl vollständig ausgeführt wurde, kann mit anderen Aufgaben fortgefahren werden. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an.
  Einschränkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

CAP
: Gibt an, welcher Cartridge Access Port (CAP) für die Ausgabe von Datenträgern verwendet werden soll, wenn REMOVE=YES angegeben wird. Dieser Parameter gilt nur für Datenträger in ACSLS-Kassettenarchiven. Wenn der CAP-Prioritätswert in dem Kassettenarchiv auf 0 gesetzt wird, ist dieser Parameter erforderlich. Ist ein CAP-Prioritätswert größer als Null in dem Kassettenarchiv definiert, ist dieser Parameter optional. Standardmäßig haben alle CAPs anfänglich den Prioritätswert 0, der bedeutet, dass ACSLS nicht automatisch den Kassettenzugriffsport auswählt.
  Zum Anzeigen der gültigen CAP-Kennungen (*x,y,z*) geben Sie den Befehl QUERY CAP mit der Option ALL von der ACSSA-Konsole (ACSSA = Automated Cartridge System System Administrator) auf dem ACSLS-Server-Host aus. Die Kennungen sind:

  x
  : Die ACS-ID (ACS = Automated Cartridge System). Diese Kennung kann eine Zahl im Bereich von 0 bis 126 sein.

  y
  : Die LSM-ID (LSM = Library Storage Module). Diese Kennung kann eine Zahl im Bereich von 0 bis 23 sein.

  z
  : Die CAP-ID. Diese Kennung kann eine Zahl im Bereich von 0 bis 11 sein.

  Weitere Informationen enthält die StorageTek-Dokumentation.

Regeln für Zielstatus und Zielstandorte

Die folgende Tabelle zeigt, wie DRM den Zielstatus und Zielstandort eines Datenträgers bestimmt.

Zielstatus

- Der Wert des Parameters TOSTATE, der angegeben wurde
- Der nächste Status des Parameters WHERESTATE, der angegeben wurde, wenn der Parameter TOSTATE nicht angegeben wurde

Zielstandort

- Der Wert des Parameters TOLOCATION, der angegeben wurde
- Der Standort des Parameters TOSTATE, der angegeben wurde, wenn der Parameter TOLOCATION nicht angegeben wurde
- Der Standort des nächsten Status des Parameters WHERESTATE, der angegeben wurde, wenn die Parameter TOLOCATION und TOSTATE nicht angegeben werden

Tabelle 2. Datenträgerzielstatus und -zielstandort

Angegebene Parameter	**Zielstatus**	**Zielstandort**
WHERESTATE	Der nächste Status von WHERESTATE	Standort des nächsten Status
WHERESTATE, TOSTATE	TOSTATE	Standort von TOSTATE
WHERESTATE, TOLOCATION	Der nächste Status von WHERESTATE	TOLOCATON
WHERESTATE, TOSTATE, TOLOCATION	TOSTATE	TOLOCATION
TOSTATE	TOSTATE	Standort von TOSTATE
TOSTATE, WHERELOCATION	TOSTATE	Standort von TOSTATE
TOSTATE, WHERELOCATION, TOLOCATION	TOSTATE	TOLOCATION

Regeln für Statusübergang

Die folgenden Tabellen zeigen die Statusübergänge, für die Datenträger auf der Basis ihres aktuellen Status ausgewählt werden können.

Tabelle 3. Statusübergänge für Datenträger

Der aktuelle Status des Datenträgers	**Zielstatus**

Der aktuelle Status des Datenträgers	MOUNTABLE	NOTMOUNTABLE	COURIER
	Zielstatus		
	MOUNTABLE	**NOTMOUNTABLE**	**COURIER**
MOUNTABLE	N	J	J
NOTMOUNTABLE	N	N	J
COURIER	N	N	N
VAULT	N	N	N
VAULTRETRIEVE	N	N	N
COURIERRETRIEVE	N	N	N
ONSITERETRIEVE	N	N	N

Tabelle 4. Statusübergänge für Datenträger

	Zielstatus	
Der aktuelle Status des Datenträgers	**VAULT**	**VAULTRETRIEVE**
MOUNTABLE	J	N
NOTMOUNTABLE	J	N
COURIER	J	N
VAULT	N	N
VAULTRETRIEVE	N	N
COURIERRETRIEVE	N	N
ONSITERETRIEVE	N	N

Tabelle 5. Statusübergänge für Datenträger

	Zielstatus	
Der aktuelle Status des Datenträgers	**COURIERRETRIEVE**	**ONSITERETRIEVE**
MOUNTABLE	N	N
NOTMOUNTABLE	N	N
COURIER	N	N
VAULT	N	N
VAULTRETRIEVE	J	J
COURIERRETRIEVE	N	J
ONSITERETRIEVE	N	N

Beispiel: Datenträger zur Wiederherstellung nach einem Katastrophenfall aus dem Status NOTMOUNTABLE versetzen

Datenträger zur Wiederherstellung nach einem Katastrophenfall, die sich im Status NOTMOUNTABLE befinden, in den Status COURIER versetzen und dann die Ergebnisse abfragen.

```
move drmedia * wherestate=notmountable
tostate=courier

query actlog search="MOVE DRMEDIA"

 08/11/1999 11:12:24      ANR0984I Prozess 10 für MOVE DRMEDIA
                        im BACKGROUND um 11:12:24 gestartet.
  08/11/1999 11:12:24     ANR0610I MOVE DRMEDIA von HSIAO als
                        Prozess 10 gestartet.
  08/11/1999 11:12:25     ANR6683I MOVE DRMEDIA: Datenträger TAPE0P
                        wurde von Status NOTMOUNTABLE in Status
                        COURIER versetzt.
  08/11/1999 11:12:25     ANR6683I MOVE DRMEDIA: Datenträger TAPE1P
                        wurde von Status NOTMOUNTABLE in Status
                        COURIER versetzt.
  08/11/1999 11:12:25     ANR6683I MOVE DRMEDIA: Datenträger DBTP02
                        wurde von Status NOTMOUNTABLE in Status
                        COURIER versetzt.
  08/11/1999 11:12:25     ANR6683I MOVE DRMEDIA: Datenträger DBTP01
                        wurde von Status NOTMOUNTABLE in Status
                        COURIER versetzt.
```

```
  08/11/1999 11:12:25      ANR6682I Befehl MOVE DRMEDIA beendet: 4
                          verarbeitet.
  08/11/1999 11:12:25      ANR0611I MOVE DRMEDIA, der von HSIAO als
                          Prozess 10 gestartet wurde, wurde beendet.
  08/11/1999 11:12:25      ANR0985I Prozess 10 für MOVE DRMEDIA, der
                          im BACKGROUND ausgeführt wird, hat 4 Objekte
                          mit Beendigungsstatus SUCCESS um
                          11:12:25 beendet.
```

Beispiel: Datenträger zur Wiederherstellung nach einem Katastrophenfall aus dem Status MOUNTABLE versetzen

Datenträger zur Wiederherstellung nach einem Katastrophenfall vom Status MOUNTABLE in den Status COURIER versetzen. Befinden sich die Datenträger in einem automatisierten Kassettenarchiv, gibt MOVE DRMEDIA die Datenträger aus, bevor der Status geändert wird.

```
move drmedia * wherestate=mountable tostate=courier wait=yes

ANR0984I Prozess 12 für MOVE DRMEDIA
  im FOREGROUND um 09:57:17 gestartet.
ANR0609I MOVE DRMEDIA als Prozess 12 gestartet.
ANR0610I MOVE DRMEDIA von HSIAO als
  Prozess 12 gestartet.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger TAPE01 in Kassettenarchiv LIB8MM wird gestartet.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger TAPE01 in Kassettenarchiv LIB8MM
  erfolgreich beendet.
ANR6683I MOVE DRMEDIA: Datenträger TAPE01 wurde von
  Status MOUNTABLE in Status COURIER versetzt.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger TAPE02 in Kassettenarchiv LIB8MM wird gestartet.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger TAPE02 in Kassettenarchiv LIB8MM
  erfolgreich beendet.
ANR6683I MOVE DRMEDIA: Datenträger TAPE02 wurde von
  Status MOUNTABLE in Status COURIER versetzt.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger DBTP05 in Kassettenarchiv LIB8MM wird gestartet.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger DBTP05 in Kassettenarchiv LIB8MM
  erfolgreich beendet.
ANR6683I MOVE DRMEDIA: Datenträger DBTP05 wurde von
  Status MOUNTABLE in Status COURIER versetzt.
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger DBTP04 in Kassettenarchiv LIB8MM wird gestartet.
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME für
  Datenträger DBTP04 in Kassettenarchiv LIB8MM
  erfolgreich beendet.
ANR6683I MOVE DRMEDIA: Datenträger DBTP04 wurde von
  Status MOUNTABLE in Status COURIER versetzt.
ANR6682I Befehl MOVE DRMEDIA beendet: 4 Datenträger
 verarbeitet.
ANR0611I MOVE DRMEDIA, der von HSIAO als
  Prozess 12 gestartet wurde, wurde beendet.
ANR0985I Prozess 12 für MOVE DRMEDIA, der im
  FOREGROUND ausgeführt wird, hat 4 Objekte mit
  Beendigungsstatus SUCCESS um 10:12:25 beendet.
```

Beispiel: Datenträger zur Wiederherstellung nach einem Katastrophenfall aus dem Status VAULTRETRIEVE versetzen

Datenträger zur Wiederherstellung nach einem Katastrophenfall, die sich im Status VAULTRETRIEVE befinden, sollen in den Status ONSITERETRIEVE versetzt werden. Einen Befehl CHECKIN LIBVOLUME für jeden Datenträger generieren, der erfolgreich verarbeitet wird, und die Befehle in einer Datei speichern:

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=/drm/move/exec.cmds
cmd="checkin libvol lib8mm &vol status=scratch"
```

Windows-Betriebssysteme

```
move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=c:\drm\move\exec.cmd
cmd="checkin libvol lib8mm &vol status=scratch"
```

Die Ergebnisse abfragen:

```
query actlog search="MOVE DRMEDIA"

08/13/1999 09:12:24   ANR0984I Prozess 15 für MOVE DRMEDIA
                      im BACKGROUND um 09:12:24 gestartet
08/13/1999 09:12:24   ANR0610I MOVE DRMEDIA von HSIAO als Prozess
                      15 gestartet.
08/13/1999 09:12:24   ANR6684I MOVE DRMEDIA: Datenträger CSTP01
                      wurde gelöscht.
08/13/1999 09:12:24   ANR6684I MOVE DRMEDIA: Datenträger CSTP02
                      wurde gelöscht.
08/13/1999 09:12:24   ANR6684I MOVE DRMEDIA: Datenträger DBTP10
                      wurde gelöscht.
08/13/1999 09:12:24   ANR6684I MOVE DRMEDIA: Datenträger DBTP11
                      wurde gelöscht.
08/13/1999 09:12:27   ANR6682I Befehl MOVE DRMEDIA beendet: 4 Datenträger
                      verarbeitet.
08/13/1999 09:12:42   ANR0611I MOVE DRMEDIA, der von HSIAO als Prozess
                       15 gestartet wurde, wurde beendet.
08/13/1997 09:12:42   ANR0985I Prozess 15 für MOVE DRMEDIA, der im
                      im BACKGROUND ausgeführt wird, hat 4 Objekte
                      Beendigungsstatus SUCCESS um 09:12:42 beendet.
```

Die Befehle zum Zurückstellen der Datenträger wurden ebenfalls in der Datei erstellt, die mit dem Parameter CMDFILENAME angegeben wurde:

- AIX-BetriebssystemeLinux-Betriebssysteme/drm/move/exec.cmds
- Windows-Betriebssystemec:\drm\move\exec.cmd

Die Datei enthält diese Zeilen:

```
checkin libvol lib8mm CSTP01 status=scratch
checkin libvol lib8mm CSTP02 status=scratch
checkin libvol lib8mm DBTP10 status=scratch
checkin libvol lib8mm DBTP11 status=scratch
```

Tipp: Um die Befehle CHECKIN LIBVOLUME zu verarbeiten, geben Sie den Befehl MACRO mit dem Dateinamen als Makronamen aus.

Zugehörige Befehle

Tabelle 6. Zugehörige Befehle für MOVE DRMEDIA

Befehl	Beschreibung
BACKUP DB	Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff.
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
DISMOUNT VOLUME	Entlädt einen sequenziellen entfernbaren Datenträger anhand des Datenträgernamens.
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
SET DRMACTIVEDATASTGPOOL	Gibt an, dass Speicherpools für aktive Daten von DRM verwaltet werden.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeSET DRMCOPYCONTAINERSTGPOOL	AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeGibt die Containerkopienspeicherpools an, die in DRM-Befehlen verwendet werden.
SET DRMCOPYSTGPOOL	Gibt an, dass Kopienspeicherpools von DRM verwaltet werden.
SET DRMCOURIERNAME	Gibt den Kuriernamen für DRM an.
SET DRMDBBACKUPEXPIREDAYS	Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.
SET DRMVAULTNAME	Gibt den Namen des Aufbewahrungsorts an, an dem DRM-Datenträger gespeichert werden.

Befehl	Beschreibung
SET DRMCMDFILENAME	Gibt den Namen einer Datei an, in die ausführbare DRM-Befehle gestellt werden sollen.
SET DRMFILEPROCESS	Gibt an, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Dateien verarbeitet, die den Einheitentyp FILE aufweisen.
SET DRMNOTMOUNTABLENAME	Gibt den Standortnamen der DRM-Datenträger an, die ausgelagert werden sollen.

MOVE GRPMEMBER (Servergruppenteil versetzen)

Mit diesem Befehl kann ein Teil aus einer Servergruppe in eine andere Servergruppe versetzt werden. Der Befehl schlägt fehl, wenn das Teil, das versetzt wird, denselben Namen wie ein aktuelles Teil der Gruppe hat.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-MOVe GRPMEMber--Name_des_Teils--aus_Gruppe--in_Gruppe------><
```

Parameter

Name_des_Teils (Erforderlich)
: Gibt das Teil an (Server oder Servergruppe), das versetzt werden soll.

aus_Gruppe (Erforderlich)
: Gibt die Servergruppe an, der das Teil gegenwärtig zugeordnet ist.

in_Gruppe (Erforderlich)
: Gibt die neue Servergruppe des Teils an.

Beispiel: Einen Server in eine andere Servergruppe versetzen

Teil PAYSON aus Gruppe REGION1 in Gruppe REGION2 versetzen.

```
move grpmember payson region1 region2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für MOVE GRPMEMBER

Befehl	Beschreibung
DEFINE GRPMEMBER	Definiert einen Server als Teil einer Servergruppe.
DEFINE SERVERGROUP	Definiert eine neue Servergruppe.
DELETE GRPMEMBER	Löscht einen Server aus einer Servergruppe.
DELETE SERVERGROUP	Löscht eine Servergruppe.
QUERY SERVER	Zeigt Informationen über Server an.
QUERY SERVERGROUP	Zeigt Informationen über Servergruppen an.
RENAME SERVERGROUP	Benennt eine Servergruppe um.
UPDATE SERVERGROUP	Aktualisiert eine Servergruppe.

MOVE MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff versetzen)

Mit diesem Befehl können übergelaufene Speicherpools verwaltet werden. Die Datenbank verfolgt Datenträger, die mit diesem Befehl versetzt werden.

Dieser Befehl gilt für Datenträger mit sequenziellem Zugriff aus primären Speicherpools und Kopienspeicherpools, die durch ein automatisiertes Kassettenarchiv (einschließlich externes Kassettenarchiv) verwaltet werden. Das Kassettenarchiv muss nicht voll sein. Ein oder mehrere Speicherpooldatenträger mit sequenziellem Zugriff können gleichzeitig verarbeitet werden.

Den Parameter DAYS verwenden, um auswählbare Datenträger zu identifizieren, die versetzt werden sollen. Den Parameter OVERFLOW LOCATION verwenden, um den Aufbewahrungsort der versetzten Datenträger aufzuzeichnen.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl QUERY PROCESS angezeigt werden kann. Zum Abbrechen den Befehl CANCEL PROCESS ausgeben.

Um zu bestimmen, ob der Befehl erfolgreich war, den Befehl QUERY ACTLOG ausgeben oder die Serverkonsole verwenden.

Die Datenträger, die mit dem Befehl MOVE DRMEDIA für die Wiederherstellung an einen anderen Standort versetzt werden, werden nicht mit dem Befehl MOVE MEDIA verarbeitet.

Der Befehl MOVE MEDIA verarbeitet keine Kopienspeicherpooldatenträger mit dem DRM STATUS-Wert NOTMOUNTABLE, COURIER oder VAULT.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Ist der Parameter CMD nicht angegeben: Bediener- oder Systemberechtigung.
- Wenn der Parameter CMD angegeben wird und die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt ist: Bedienerberechtigung, uneingeschränkte Speicherberechtigung oder Systemberechtigung.
- Wenn der Parameter CMD angegeben wird und die Serveroption REQSYSAUTHOUTFILE auf YES (Standardwert) gesetzt ist: Systemberechtigung.

Syntax

```
>>-MOVe MEDia--Datenträgername--STGpool--=--Poolname------------>

   .-Days--=--0----.
>--+---------------+---------------------------------------------->
   '-Days--=--Tage-'

>--+-------------------------------------+---------------------->
   '-WHERESTate--=--+-MOUNTABLEInlib----+-'
                    '-MOUNTABLENotinlib-'

>--+-----------------------------------+-------------------------->
   |                 .-,-----------.   |
   |                 V             | |
   '-WHERESTATUs--=----+-FULl----+-+-'
                       +-FILling-+
                       '-EMPty---'

>--+--------------------------+--+--------------------------+--->
   '-ACCess--=--+-READWrite-+-'  '-OVFLOcation--=--Standort-'
                '-READOnly--'

   .-REMove--=--Bulk-----.
>--+---------------------+--+------------------+---------------->
   '-REMove--=--+-No---+-'  '-CMd--=--"Befehl"-'
                +-Yes--+
                '-Bulk-'

                                  .-APPend--=--No------.
>--+---------------------------+--+--------------------+-------->
   '-CMDFilename--=--Dateiname-'  '-APPend--=--+-No--+-'
                                               '-Yes-'

   .-CHECKLabel--=--Yes-----.
>--+------------------------+--+------------------+----------><
   '-CHECKLabel--=--+-Yes-+-'  '-CAP--=----x,y,z---'
                    '-No--'
```

Parameter

Datenträgername (Erforderlich)
: Gibt den Namen des zu verarbeitenden Datenträgers mit sequenziellem Zugriff aus einem primären Speicherpool oder einem Kopienspeicherpool an. Es kann ein Platzhalterzeichen verwendet werden, um den Namen anzugeben. Alle übereinstimmenden Datenträger werden bei der Verarbeitung berücksichtigt.

STGpool (Erforderlich)
: Gibt den Namen des primären Speicherpools oder Kopienspeicherpools mit sequenziellem Zugriff an, aus dem die Datenträger für die Verarbeitung ausgewählt werden. Es kann ein Platzhalterzeichen verwendet werden, um den Namen anzugeben. Alle übereinstimmenden Speicherpools werden verarbeitet. Wird der angegebene Speicherpool nicht durch ein automatisiertes Kassettenarchiv verwaltet, werden keine Datenträger verarbeitet.

Days

Gibt die Anzahl Tage an, die nach dem Schreiben oder Lesen des Datenträgers verstreichen müssen, bevor der Datenträger durch den Befehl verarbeitet werden kann. Dieser Parameter ist wahlfrei. Es kann eine Zahl von 0 bis 9999 angegeben werden. Der Standardwert ist 0. Die Anzahl der verstrichenen Tage wird anhand des letzten Lese- oder Schreibdatums (das aktuellere von beiden) der Datenträger berechnet.

WHERESTate

Gibt den aktuellen Status der zu verarbeitenden Datenträger an. Mit diesem Parameter wird die Verarbeitung auf die Datenträger beschränkt, die den angegebenen Status haben. Dieser Parameter ist wahlfrei. Der Standardwert ist MOUNTABLEINLIB.
Gültige Werte:

MOUNTABLEInlib
: Gibt an, dass Speicherpooldatenträger vom Status MOUNTABLEINLIB in den Status MOUNTABLENOTINLIB versetzt werden sollen. Datenträger mit dem Status MOUNTABLEINLIB enthalten gültige Daten und befinden sich im Kassettenarchiv.

MOUNTABLENotinlib
: Gibt an, dass Speicherpooldatenträger vom Status MOUNTABLENOTINLIB wieder in den Status MOUNTABLEINLIB übergehen sollen. Datenträger mit dem Status MOUNTABLENOTINLIB können gültige Daten enthalten und befinden sich am Überlaufstandort.

- Bei leeren Arbeitsdatenträgern löscht der Befehl MOVE MEDIA die Datenträgersätze, so dass sie wiederverwendet werden können.
- Bei privaten Datenträgern setzt der Befehl MOVE MEDIA den Datenträgerstandort auf leer (blank) zurück, ändert den Datenträgerstatus in CHECKIN und das letzte Aktualisierungsdatum in das aktuelle Datum.
- Bei Arbeitsdatenträgern mit Daten setzt der Befehl MOVE MEDIA den Datenträgerstandort auf leer (blank) zurück, ändert den Datenträgerstatus in CHECKIN und das letzte Aktualisierungsdatum in das aktuelle Datum.

Achtung: Datenträger mit dem Status CHECKIN können gültige Daten enthalten und müssen in das Kassettenarchiv zurückgestellt werden.

WHERESTATUs

Gibt an, dass der Versetzungsprozess auf einen bestimmten Datenträgerstatus beschränkt werden muss. Dieser Parameter ist wahlfrei. Es können mehrere Status in einer Liste angegeben werden, indem jeder Status ohne Leerzeichen durch ein Komma voneinander getrennt wird. Wird dieser Parameter nicht angegeben, sind Datenträger, die vom Status MOUNTABLEINLIB in den Status MOUNTABLENOTINLIB versetzt werden, nur auf volle Datenträger beschränkt, und sind Datenträger, die vom Status MOUNTABLENOTINLIB in den Status MOUNTABLEINLIB versetzt werden, nur auf leere Datenträger beschränkt.

Gültige Werte:

FULl
: Datenträger mit dem Status FULL werden versetzt.

FILling
: Datenträger mit dem Status FILLING werden versetzt.

EMPty
: Datenträger mit dem Status EMPTY werden versetzt.

ACCess

Gibt an, wie Benutzer und Systemprozesse auf Dateien auf dem Speicherpooldatenträger zugreifen, der durch den Befehl MOVE MEDIA aus einem automatisierten Kassettenarchiv versetzt und an einem Überlaufstandort gespeichert wird. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird der Zugriffsmodus der Datenträger durch das Versetzen von Datenträgern vom Status MOUNTABLEINLIB in den Status MOUNTABLENOTINLIB in READONLY geändert und durch das Versetzen von Datenträgern vom Status MOUNTABLENOTINLIB in den Status MOUNTABLEINLIB in READWRITE.

Gültige Werte:

READWrite
: Gibt an, dass Benutzer und Systemprozesse Dateien auf dem Datenträger, der sich am Überlaufstandort befindet, lesen und in diese schreiben können. Wenn dieser Wert angegeben wird, fordert IBM Spectrum Protect das Zurückstellen des Datenträgers in das Kassettenarchiv an, wenn er für eine Lese- oder Schreiboperation benötigt wird.

READOnly
: Gibt an, dass Benutzer und Systemprozesse Dateien auf dem Datenträger, der sich am Überlaufstandort befindet, lesen, aber nicht in diese schreiben können. Der Server fordert das Zurückstellen des Datenträgers in das Kassettenarchiv nur an, wenn er für eine Leseoperation benötigt wird.

OVFLOcation

Gibt den Überlaufstandort an, der der Zielort für die Datenträger ist, die gerade verarbeitet werden. Der Standortname darf maximal 255 Zeichen lang sein. Wenn der Standortname Leerzeichen enthält, muss er in Anführungszeichen stehen. Wird kein Überlaufstandort angegeben und hat auch der Speicherpool keinen Überlaufstandort identifiziert, ändert der Server den Standort des ausgegebenen Datenträgers in eine leere Zeichenfolge ("").

REMove

Gibt an, dass der Server versucht, den Datenträger aus dem Kassettenarchiv in die Serviceein-/-ausgabestation oder die Eingangs-/Ausgangsanschlüsse zu versetzen. Dieser Parameter ist wahlfrei. Gültige Werte sind YES, BULK und NO. Der Standardwert ist BULK. Die Antwort des Servers auf jede dieser Optionen und die Standardwerte werden in den folgenden Tabellen beschrieben.

349X-Kassettenarchive: Die folgende Tabelle zeigt, wie der Server für 349X-Kassettenarchive antwortet.

Tabelle 1. Antwort des Servers für 349X-Kassettenarchive

REMOVE=YES	REMOVE=BULK	REMOVE=NO
Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Serviceein-/-ausgabestation aus.	Der 3494-Kassettenarchivmanager (Library Manager) gibt die Kassette an die Ausgabeeinrichtung mit hoher Speicherkapazität aus.	Der 3494-Kassettenarchivmanager (Library Manager) gibt den Datenträger nicht aus. Der Server lässt die Kassette für die Verwendung durch andere Anwendungen in dem Kassettenarchiv in der Kategorie INSERT.

SCSI-Kassettenarchive: Die folgende Tabelle zeigt, wie der Server für SCSI-Kassettenarchive auf YES, BULK und NO antwortet.

Tabelle 2. Antwort des Servers für SCSI-Kassettenarchive

Wenn ein Kassettenarchiv...	Und REMOVE=YES...	Und REMOVE=BULK...	Und REMOVE=NO
Keine Eingangs-/Ausgangsanschlüsse hat	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.
Eingangs-/Ausgangsanschlüsse hat und ein Eingangs-/Ausgangsanschluss verfügbar ist	Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an. Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.	Versetzt der Server die Kassette in den verfügbaren Eingangs-/Ausgangsanschluss und gibt die Anschlussadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.
Eingangs-/Ausgangsanschlüsse hat, aber keine Anschlüsse verfügbar sind	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden dann vom Server aufgefordert, die Kassette aus dem Schacht zu entnehmen und einen Befehl REPLY auszugeben.	Wartet der Server auf einen verfügbaren Eingangs-/Ausgangsanschluss.	Lässt der Server die Kassette in dem aktuellen Schacht in dem Kassettenarchiv und gibt die Schachtadresse in einer Nachricht an. Sie werden nicht vom Server aufgefordert, die Kassette zu entnehmen, und müssen keinen Befehl REPLY ausgeben.

ACSLS-Kassettenarchive: Die folgende Tabelle zeigt, wie der Server für ACSLS-Kassettenarchive antwortet.

Tabelle 3. Antwort des Servers für ACSLS-Kassettenarchive

REMOVE=YES oder REMOVE=BULK	REMOVE=NO
Der Server gibt die Kassette an die Serviceein-/-ausgabestation aus. Dann löscht der Server den Datenträgereintrag aus dem Serverdatenträgerbestand im Kassettenarchiv. Beim Versetzen von Datenträgern aus dem Status MOUNTABLE unter Angabe von REMOVE=YES verwendet der Befehl MOVE MEDIA mehrere Schächte in dem CAP für ein StorageTek-Kassettenarchiv mit ACSLS.	Der Server gibt die Kassette nicht aus. Der Server löscht den Datenträgereintrag aus dem Kassettenarchivbestand des Servers und lässt den Datenträger in dem Kassettenarchiv.

Externe Kassettenarchive: Die folgende Tabelle zeigt, wie der Server für externe Kassettenarchive antwortet.

Tabelle 4. Antwort des Servers für externe Kassettenarchive

REMOVE=YES oder REMOVE=BULK	REMOVE=NO

REMOVE=YES oder REMOVE=BULK	REMOVE=NO
Der Server gibt die Kassette an die Serviceein-/-ausgabestation aus. Dann löscht der Server den Datenträgereintrag aus dem Serverdatenträgerbestand im Kassettenarchiv.	Der Server gibt die Kassette nicht aus. Der Server löscht den Datenträgereintrag aus dem Kassettenarchivbestand des Servers und lässt den Datenträger in dem Kassettenarchiv.

CMd

Gibt an, dass ausführbare Befehle erstellt werden. Dieser Parameter ist wahlfrei. Die Befehlsangabe muss in Anführungszeichen eingeschlossen werden. Die maximale Länge der Befehlsangabe beträgt 255 Zeichen. Für jeden Datenträger, den der Befehl MOVE MEDIA erfolgreich verarbeitet hat, schreibt der Server die zugeordneten Befehle in eine Datei. Den Dateinamen mit dem Parameter CMDFILENAME angeben.

 AIX-Betriebssysteme  Linux-BetriebssystemeWird der Dateiname nicht angegeben, generiert der Befehl MOVE MEDIA einen Standarddateinamen, indem die Zeichenfolge exec.cmds.media an das IBM Spectrum Protect-Serververzeichnis angehängt wird.

 Windows-BetriebssystemeWird der Dateiname nicht angegeben, generiert der Befehl MOVE MEDIA einen Standarddateinamen, indem die Zeichenfolge exec.cmd.media an das IBM Spectrum Protect-Serververzeichnis angehängt wird.

Wenn die Länge des Befehls, der in die Datei geschrieben wird, 255 Zeichen überschreitet, wird er in mehrere Zeilen aufgeteilt, wobei an das Ende jeder Zeile (mit Ausnahme der letzten Befehlszeile) ein Fortsetzungszeichen (+) eingefügt wird. Sie müssen das Fortsetzungszeichen entsprechend den Anforderungen des Produkts, das die Befehle ausführt, ändern.

Wird CMD nicht angegeben, generiert der Befehl MOVE MEDIA möglicherweise keine ausführbaren Befehle.

Zeichenfolge

Gibt die Zeichenfolge für die Erstellung eines ausführbaren Befehls an. Für die Zeichenfolge kann beliebiger Text im freien Format angegeben werden. Die gesamte Zeichenfolge muss in Anführungszeichen eingeschlossen werden. Das folgende Beispiel zeigt eine gültige Angabe eines ausführbaren Befehls:

```
CMD="UPDATE VOLUME &VOL"
```

Die folgende Angabe ist ungültig:

```
CMD=""UPDATE VOLUME" &VOL"
```

Substitution

Gibt eine Variable an, für die der Befehl einen Wert ersetzen soll. Gültige Substitutionsvariablen:

&VOL

Den Datenträgernamen für &VOL ersetzen. Kleinbuchstaben können angegeben werden (&vol). Zwischen Et-Zeichen (&) und VOL dürfen keine Leerschritte oder Leerzeichen stehen. Befinden sich an dieser Stelle Leerzeichen, behandelt der Befehl MOVE MEDIA diese Zeichen als Zeichenfolge, und es wird keine Substitution definiert. Wird &VOL nicht angegeben, wird in dem ausführbaren Befehl kein Datenträgername definiert.

&LOC

Den Datenträgerstandort für &LOC ersetzen. Kleinbuchstaben können angegeben werden (&loc). Zwischen Et-Zeichen (&) und LOC dürfen keine Leerschritte oder Leerzeichen stehen. Befinden sich an dieser Stelle Leerzeichen, behandelt der Befehl MOVE MEDIA diese Zeichen als Zeichenfolge, und es wird keine Substitution definiert. Wird &LOC nicht angegeben, wird in dem ausführbaren Befehl kein Standortname definiert.

&VOLDSN

Den Datenträgerdateinamen für &VOLDSN ersetzen. Ein Beispiel für einen Dateinamen eines Banddatenträgers aus dem Speicherpool, der das Standardpräfix ADSM verwendet, ist ADSM.BFS. Wird &VOLDSN nicht angegeben, wird in dem ausführbaren Befehl kein Datenträgerdateiname definiert.

&NL

Ein Zeilenvorschubzeichen für &NL ersetzen. Wenn &NL angegeben wird, teilt der Befehl MOVE MEDIA den Befehl an der Position, an der sich &NL befindet; es werden keine Fortsetzungszeichen angehängt. Die Angabe des richtigen Fortsetzungszeichens (falls erforderlich) vor &NL ist Aufgabe des Benutzers. Der Benutzer ist außerdem verantwortlich für die Länge der Zeile. Wenn &NL nicht angegeben wird und die Länge der Befehlszeile 255 Zeichen überschreitet, wird sie in mehrere Zeilen aufgeteilt, wobei an das Ende jeder Zeile (mit Ausnahme der letzten Befehlszeile) ein Fortsetzungszeichen (+) eingefügt wird.

CMDFilename

Gibt den vollständigen Pfadnamen einer Datei an, die die mit CMD angegebenen Befehle enthält. Dieser Parameter ist wahlfrei. Die maximale Länge des Dateinamens beträgt 1279 Zeichen.

 AIX-Betriebssysteme  Linux-BetriebssystemeWird kein Dateiname angegeben, generiert der Befehl MOVE MEDIA einen Standarddateinamen, indem die Zeichenfolge `exec.cmds.media` an das IBM Spectrum Protect-Serververzeichnis angehängt wird. Das Serververzeichnis ist das aktuelle Arbeitsverzeichnis des IBM Spectrum Protect-Serverprozesses.

 Windows-BetriebssystemeWird kein Dateiname angegeben, generiert der Befehl MOVE MEDIA einen Standarddateinamen, indem die Zeichenfolge *`exec.cmd.media`* an das IBM Spectrum Protect-Serververzeichnis angehängt wird. Das Serververzeichnis ist das aktuelle Arbeitsverzeichnis des IBM Spectrum Protect-Serverprozesses.

Der Befehl MOVE MEDIA ordnet den angegebenen oder generierten Dateinamen automatisch zu. Ist der Dateiname vorhanden, kann mit dem Parameter APPEND=YES an die Datei angefügt werden. Andernfalls wird die Datei überschrieben. Wird eine Datei versehentlich überschrieben und müssen die Befehle, die in der Datei enthalten waren, ausgeführt werden, geben Sie den Befehl QUERY MEDIA aus, um die ausführbaren Befehle für die gewünschten Datenträger wiederherzustellen. Wenn der Befehl MOVE MEDIA nach der Zuordnung der Befehlsdatei fehlschlägt, wird die Datei nicht gelöscht.

APPend
Gibt an, dass am Anfang oder Ende der Befehlsdateidaten geschrieben werden soll. Der Standardwert ist NO. Gültige Werte:

No
Gibt an, dass die Daten an den Anfang der Befehlsdatei geschrieben werden sollen. Wenn die Befehlsdatei vorhanden ist, wird ihr Inhalt überschrieben.
Yes
Gibt an, dass die Befehlsdatei angehängt werden soll, indem am Ende der Befehlsdateidaten geschrieben wird.

CHECKLabel
Gibt an, ob der Server Datenträgerkennsätze für sequenzielle Datenträger liest. Bei SCSI-Einheiten kann die Kennsatzprüfung unterdrückt werden, indem CHECKLabel auf NO gesetzt wird. Dieser Parameter gilt nicht für 349X-Kassettenarchive. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Gültige Werte:

Yes
Gibt an, dass der Server versucht, den Datenträgerkennsatz zu lesen. Das Lesen des Datenträgerkennsatzes bestätigt, dass der richtige Datenträger entnommen wird.
No
Gibt an, dass der Server nicht versucht, den Datenträgerkennsatz zu lesen. Da der Lesevorgang entfällt, verbessert sich die Leistung.

CAP
Gibt an, welcher Cartridge Access Port (CAP) für die Ausgabe von Datenträgern verwendet werden soll, wenn REMOVE=YES angegeben wird. Dieser Parameter gilt nur für Datenträger in ACSLS-Kassettenarchiven. Wenn der CAP-Prioritätswert in dem Kassettenarchiv auf 0 gesetzt wird, ist dieser Parameter erforderlich. Ist ein CAP-Prioritätswert größer als Null in dem Kassettenarchiv definiert, ist dieser Parameter optional. Standardmäßig haben alle CAPs anfänglich den Prioritätswert 0, der bedeutet, dass ACSLS nicht automatisch den Kassettenzugriffsport auswählt.
Zum Anzeigen der gültigen CAP-Kennungen (*x,y,z*) geben Sie den Befehl QUERY CAP mit der Option ALL von der ACSSA-Konsole (ACSSA = Automated Cartridge System System Administrator) auf dem ACSLS-Server-Host aus. Die Kennungen sind:

x
Die ACS-ID (ACS = Automated Cartridge System). Diese Kennung kann eine Zahl im Bereich von 0 bis 126 sein.
y
Die LSM-ID (LSM = Library Storage Module). Diese Kennung kann eine Zahl im Bereich von 0 bis 23 sein.
z
Die CAP-ID. Diese Kennung kann eine Zahl im Bereich von 0 bis 11 sein.

Weitere Informationen enthält die StorageTek-Dokumentation.

Beispiel: Alle vollen Datenträger aus dem Kassettenarchiv versetzen

Alle vollen Datenträger, die sich im sequenziellen primären Speicherpool ARCHIVE befinden, aus dem Kassettenarchiv versetzen.

```
move media * stgpool=archive
```

Beispiel: Die Befehle zum Zurückstellen generieren

Die Befehle CHECKIN LIBVOLUME für volle und teilweise volle Datenträger generieren, die sich im primären Speicherpool ONSITE.ARCHIVE befinden und im Überlaufstandort Room 2948/Bldg31 aufbewahrt werden.

AIX-BetriebssystemeLinux-BetriebssystemeMOVE MEDIA erstellt die ausführbaren Befehle in /tsm/move/media/checkin.vols.

Windows-BetriebssystemeMOVE MEDIA erstellt die ausführbaren Befehle in c:\tsm\move\media\checkin.vols.

```
move media * stgpool=onsite.archive
wherestate=mountablenotinlib wherestatus=full,filling
ovflocation=room2948/bldg31
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols

checkin libvolume lib3494 TAPE04 status=private
checkin libvolume lib3494 TAPE13 status=private
checkin libvolume lib3494 TAPE14 status=private
```

Tipp: Führen Sie die Befehle CHECKIN LIBVOLUME aus, indem Sie den Befehl MACRO mit dem folgenden Wert als Makronamen ausgeben:

-  AIX-Betriebssysteme  Linux-Betriebssysteme/tsm/move/media/checkin.vols
-  Windows-Betriebssystemec:\tsm\move\media\checkin.vols

Zugehörige Befehle

Tabelle 5. Zugehörige Befehle für MOVE MEDIA

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY MEDIA	Zeigt Informationen über Speicherpooldatenträger an, die mit dem Befehl MOVE MEDIA versetzt wurden.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.

MOVE NODEDATA (Daten nach Knoten in einem Speicherpool mit sequenziellem Zugriff versetzen)

Verwenden Sie diesen Befehl, um Daten zu versetzen, die sich in einem Speicherpool mit sequenziellem Zugriff befinden. Sie können Daten für einen oder mehrere Knoten, eine Gruppe von Dateibereichen oder eine Gruppe von zusammengefassten Knoten versetzen. Sie können auch ausgewählte Dateibereiche für einen einzelnen Knoten versetzen. Die Daten können sich in einem primären Speicherpool, einem Kopienspeicherpool oder einem Pool für aktive Daten befinden.

Mit diesem Befehl kann die Anzahl der Datenträgerladevorgänge bei Zurückschreibungs- oder Abrufoperationen des Clients reduziert werden, indem Daten für einen bestimmten Knoten innerhalb eines Speicherpools zusammengefasst werden. Außerdem können Daten in einen anderen Speicherpool versetzt werden. Beispielsweise kann der Befehl zum Versetzen von Daten in einen Speicherpool mit wahlfreiem Zugriff als Vorbereitung für eine Client-Zurückschreibungsverarbeitung verwendet werden.

Stellen Sie sicher, dass der Zugriffsmodus der Datenträger, von denen die Knotendaten versetzt werden, "Lesen/Schreiben" oder "Lesezugriff" lautet, und der Zugriffsmodus der Datenträger, auf die die Knotendaten versetzt werden, auf "Lesen/Schreiben" gesetzt ist. Diese Operation versetzt keine Daten auf Datenträgern mit den Zugriffsmodi "Ausgelagert", "Nicht verfügbar" oder "Zerstört".

Der Befehl MOVE NODEDATA hat zwei Formen, je nachdem, ob Daten nur für ausgewählte Dateibereiche versetzt werden. Syntax und Parameter der jeweiligen Form werden separat definiert.

Einschränkung: Sie können keine Knotendaten in einen Speicherpool oder aus einem Speicherpool versetzen, der mit einer Einheitenklasse CENTERA definiert ist.

Tabelle 1. Zugehörige Befehle für MOVE NODEDATA

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
DEFINE COLLOCGROUP	Definiert eine Kollokationsgruppe.
DEFINE COLLOCMEMBER	Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.
DELETE COLLOCGROUP	Löscht eine Kollokationsgruppe.
DELETE COLLOCMEMBER	Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.
MOVE DATA	Versetzt Daten aus einem angegebenen Speicherpooldatenträger in einen anderen Speicherpooldatenträger.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY OCCUPANCY	Zeigt Dateibereichsdaten anhand des Speicherpools an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
QUERY VOLUME	Zeigt Informationen über Speicherpooldatenträger an.
UPDATE COLLOCGROUP	Aktualisiert die Beschreibung einer Kollokationsgruppe.

- MOVE NODEDATA (Daten in Dateibereichen für einen oder mehrere Knoten oder eine Kollokationsgruppe versetzen)
  Verwenden Sie diesen Befehl, um Daten in Dateibereichen zu versetzen, die zu einem oder mehreren Knoten, einer

Knotenkollokationsgruppe oder einer Dateibereichskollokationsgruppe gehören.

- MOVE NODEDATA (Daten aus ausgewählten Dateibereichen eines einzelnen Knotens versetzen)
  Verwenden Sie diesen Befehl, um Daten für ausgewählte Dateibereiche zu versetzen, die zu einem einzelnen Knoten gehören.

MOVE NODEDATA (Daten in Dateibereichen für einen oder mehrere Knoten oder eine Kollokationsgruppe versetzen)

Verwenden Sie diesen Befehl, um Daten in Dateibereichen zu versetzen, die zu einem oder mehreren Knoten, einer Knotenkollokationsgruppe oder einer Dateibereichskollokationsgruppe gehören.

Berechtigungsklasse

Um diesen Befehl auszugeben, benötigen Sie die Systemberechtigung, die uneingeschränkte Speicherberechtigung oder die eingeschränkte Speicherberechtigung für den Quellenspeicherpool. Wenn Ihre Berechtigung die eingeschränkte Speicherberechtigung ist und Sie Daten in einen anderen Speicherpool versetzen, benötigen Sie die entsprechende Berechtigung für den Zielspeicherpool.

Syntax

Anmerkungen:

1. Der Standardwert ist NO, wenn entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff ist. Der Standardwert ist YES, wenn sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff ist.

Parameter

Knotenname (Erforderlich, wenn nicht der Parameter COLLOCGROUP angegeben ist)
: Gibt den Knotennamen für die Daten an, die mit diesem Befehl versetzt werden. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

COLLOCGroup (Erforderlich, wenn nicht der Parameter für den Knotennamen angegeben ist)
: Gibt den Namen der Kollokationsgruppe an, deren Daten versetzt werden müssen. Daten für alle Knoten und Dateibereiche, die zu der Kollokationsgruppe gehören, werden versetzt.

FROMstgpool (Erforderlich)
: Gibt den Namen eines Speicherpools mit sequenziellem Zugriff an, der Daten enthält, die versetzt werden sollen. Dieser Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben.

TOstgpool
: Gibt den Namen eines Speicherpools an, in den die Daten versetzt werden. Dieser Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben.Dieser Parameter ist optional und gilt nicht, wenn der Quellenspeicherpool ein Kopienspeicherpool oder ein Pool für aktive Daten ist. Ist der Quellenspeicherpool ein Kopienspeicherpool, muss das Ziel derselbe Kopienspeicherpool sein. Ist der Quellenspeicherpool ein Pool für aktive Daten, muss das Ziel ebenfalls derselbe Pool für aktive Daten sein. Wird kein Wert angegeben, werden Daten auf andere Datenträger innerhalb des Quellenpools versetzt.
  Wichtig: Werden Daten innerhalb desselben Speicherpools versetzt, müssen Datenträger verfügbar sein, die nicht die Knotendaten enthalten, die versetzt werden. Der Server kann nicht Datenträger, die die zu versetzenden Daten enthalten, als Zieldatenträger

verwenden.

Type

Gibt den Typ der Dateien an, die versetzt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Ist der Quellenspeicherpool ein Pool für aktive Daten, sind nur die Werte ANY und BACKUP gültig. Bei TYPE=ANY werden jedoch nur die aktiven Versionen von Sicherungsdaten versetzt. Geben Sie einen der folgenden Werte an:

ANY
: Gibt an, dass alle Typen der Dateien versetzt werden.

Backup
: Gibt an, dass Sicherungsdateien versetzt werden.

ARchive
: Gibt an, dass Archivierungsdateien versetzt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

SPacemanaged
: Gibt an, dass speicherverwaltete Dateien (Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden) versetzt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

MAXPRocess

Gibt die maximale Anzahl paralleler Prozesse an, die zum Versetzen von Daten verwendet werden. Dieser Parameter ist wahlfrei. Sie können einen Wert von 1 bis einschließlich 999 angeben. Der Standardwert ist 1. Bei einer Erhöhung der Anzahl paralleler Prozesse wird normalerweise der Durchsatz verbessert.

Bei der Bestimmung dieses Werts ist die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden kann. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Systemaktivitäten abhängig. Die Mountpunkte und Laufwerke sind auch von den Grenzwerten für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Versetzung betroffen sind. Jeder Prozess benötigt einen Mountpunkt für Speicherpooldatenträger und, falls der Einheitentyp nicht FILE lautet, außerdem ein Laufwerk.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Geben Sie einen der folgenden Werte an:

No
: Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

  Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

  Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird ein Hintergrundprozess abgebrochen, wurden einige Dateien möglicherweise vor dem Abbruch versetzt.

Yes
: Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist. Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

RECONStruct

Gibt an, ob Dateiaggregate beim Versetzen von Daten wiederhergestellt werden sollen. Bei der Wiederherstellung wird leerer Speicherbereich entfernt, der sich durch das Löschen von logischen Dateien aus einem Aggregat angesammelt hat. Dieser Parameter ist wahlfrei. Ist sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff, ist der Standardwert YES. Ist entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff, ist der Standardwert NO. Der Parameter ist nicht verfügbar oder wird ignoriert, wenn eine der folgenden Bedingungen zutrifft:

- Das Datenformat ist NETAPPDUMP, CELERRADUMP oder NDMPDUMP.
- Die Daten befinden sich in einem Speicherpool, der für die Deduplizierung von Daten konfiguriert ist.
- Der Zielspeicherpool für die Datenversetzung ist für die Deduplizierung von Daten konfiguriert.

Achtung: Bei der Wiederherstellung werden inaktive Sicherungsdateien in Pools für aktive Daten entfernt. Geben Sie RECONSTRUCT=NO an, wenn die Daten in einen Pool für aktive Daten versetzt werden, der nicht für die Deduplizierung von Daten konfiguriert ist, verbleiben inaktive Sicherungsdateien in dem Speicherpool.
Sie können einen der folgenden Werte angeben:

No
: Gibt an, dass die Wiederherstellung von Dateiaggregaten beim Versetzen von Daten nicht ausgeführt wird.

Yes
: Gibt an, dass die Wiederherstellung von Dateiaggregaten beim Versetzen von Daten ausgeführt wird. Sie können diese Option nur angeben, wenn die Quellen- und Zielspeicherpools Speicherpools mit sequenziellem Zugriff sind.

Die Daten eines bestimmten Knotens aus einem Bandspeicherpool in einen Plattenspeicherpool versetzen

Alle Daten für Knoten MARY versetzen, die im Speicherpool TAPEPOOL gespeichert sind. Die Daten können in den Plattenspeicherpool BACKUPPOOL versetzt werden.

```
move nodedata mary
 fromstgpool=tapepool tostgpool=backuppool
```

Daten für eine Knotenkollokationsgruppe aus einem Speicherpool in einen anderen Speicherpool versetzen

Alle Daten für die Knotenkollokationsgruppe NODEGROUP1 aus dem Speicherpool SOURCEPOOL in den Speicherpool TARGETPOOL versetzen.

```
move nodedata collocgroup=nodegroup1 fromstgpool=sourcespool tostgpool=targetpool
```

Daten für eine Dateibereichskollokationsgruppe aus einem Speicherpool in einen anderen Speicherpool versetzen

Alle Daten für die Dateibereichskollokationsgruppe FSGROUP1 aus dem Speicherpool SOURCEPOOL2 in den Speicherpool TARGETPOOL2 versetzen.

```
move nodedata collocgroup=fsgroup1 fromstgpool=sourcespool2 tostgpool=targetpool2
```

MOVE NODEDATA (Daten aus ausgewählten Dateibereichen eines einzelnen Knotens versetzen)

Verwenden Sie diesen Befehl, um Daten für ausgewählte Dateibereiche zu versetzen, die zu einem einzelnen Knoten gehören.

Berechtigungsklasse

Um diesen Befehl auszugeben, benötigen Sie die Systemberechtigung, die uneingeschränkte Speicherberechtigung oder die eingeschränkte Speicherberechtigung für den Quellenspeicherpool. Ist Ihre Berechtigung die eingeschränkte Speicherberechtigung und möchten Sie Daten in einen anderen Speicherpool versetzen, benötigen Sie auch die entsprechende Berechtigung für den Zielspeicherpool.

Syntax

```
   .-RECONStruct--=--No oder Yes-----.
>--+---------------------------------+------------------------><
   '-RECONStruct--=--+-No--+---------'
                     '-Yes-'
```

Anmerkungen:

1. Der Standardwert ist NO, wenn entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff ist. Der Standardwert ist YES, wenn sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff ist.

Parameter

Knotenname (Erforderlich)
: Gibt den Knotennamen für die Daten an, die mit diesem Befehl versetzt werden. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

FROMstgpool (Erforderlich)
: Gibt den Namen eines Speicherpools mit sequenziellem Zugriff an, der Daten enthält, die versetzt werden sollen. Dieser Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben.

TOstgpool
: Gibt den Namen eines Speicherpools an, in den Daten versetzt werden. Dieser Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben.Dieser Parameter ist optional und gilt nicht, wenn der Quellenspeicherpool ein Kopienspeicherpool oder ein Pool für aktive Daten ist. Ist der Quellenspeicherpool ein Kopienspeicherpool, muss das Ziel derselbe Kopienspeicherpool sein. Ist der Quellenspeicherpool ein Pool für aktive Daten, muss das Ziel ebenfalls derselbe Pool für aktive Daten sein. Wird kein Wert angegeben, werden Daten auf andere Datenträger innerhalb des Quellenpools versetzt.
  Wichtig: Werden Daten innerhalb desselben Speicherpools versetzt, müssen Datenträger verfügbar sein, die nicht die Knotendaten enthalten, die versetzt werden. Der Server kann nicht Datenträger, die die zu versetzenden Daten enthalten, als Zieldatenträger verwenden.

FILespace
: Gibt den Namen des Nicht-Unicode-Dateibereichs an, der Daten enthält, die versetzt werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Geben Sie für diesen Parameter und für UNIFILESPACE und/oder FSID keine Werte an, werden Nicht-Unicode-Dateibereiche nicht versetzt.

UNIFILESpace
: Gibt den Namen des Unicode-Dateibereichs an, der Daten enthält, die versetzt werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Geben Sie für diesen Parameter und für FILESPACE und/oder FSID keine Werte an, werden Nicht-Unicode-Dateibereiche nicht versetzt.

FSID
: Gibt die Dateibereich-IDs (FSIDs) für die Dateibereiche an, die versetzt werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

Type
: Gibt den Typ der Dateien an, die versetzt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Ist der Quellenspeicherpool ein Pool für aktive Daten, sind nur die Werte ANY und BACKUP gültig. Bei TYPE=ANY werden jedoch nur die aktiven Versionen von Sicherungsdaten versetzt. Gültige Werte:

  ANY
  : Gibt an, dass alle Typen der Dateien versetzt werden.

  Backup
  : Gibt an, dass Sicherungsdateien versetzt werden.

  ARchive
  : Gibt an, dass Archivierungsdateien versetzt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

  SPacemanaged
  : Gibt an, dass speicherverwaltete Dateien (Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden) versetzt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

MAXPRocess
: Gibt die maximale Anzahl paralleler Prozesse an, die zum Versetzen von Daten verwendet werden. Dieser Parameter ist wahlfrei. Mögliche Werte sind 1–999 einschließlich. Der Standardwert ist 1. Eine Erhöhung der Anzahl paralleler Prozesse sollte den Durchsatz verbessern.

  Bei der Bestimmung dieses Werts ist die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden kann. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Systemaktivitäten sowie von den Grenzwerten für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von dem Versetzen betroffen sind. Jeder Prozess benötigt einen Mountpunkt für Speicherpooldatenträger und, falls der Einheitentyp nicht FILE lautet, außerdem ein Laufwerk.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

  No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird ein Hintergrundprozess abgebrochen, wurden einige Dateien möglicherweise vor dem Abbruch bereits versetzt.

Yes
Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist. Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

RECONStruct
Gibt an, ob Dateiaggregate beim Versetzen von Daten wiederhergestellt werden sollen. Bei der Wiederherstellung wird leerer Speicherbereich entfernt, der sich durch das Löschen von logischen Dateien aus einem Aggregat angesammelt hat. Dieser Parameter ist wahlfrei. Ist sowohl der Quellenspeicherpool als auch der Zielspeicherpool ein Speicherpool mit sequenziellem Zugriff, ist der Standardwert YES. Ist entweder der Quellen- oder der Zielspeicherpool ein Speicherpool mit wahlfreiem Zugriff, ist der Standardwert NO. Der Parameter ist nicht verfügbar oder wird ignoriert, wenn eine der folgenden Bedingungen zutrifft:

- Das Datenformat ist NETAPPDUMP, CELERRADUMP oder NDMPDUMP.
- Die Daten befinden sich in einem Speicherpool, der für die Deduplizierung von Daten konfiguriert ist.
- Der Zielspeicherpool für die Datenversetzung ist für die Deduplizierung von Daten konfiguriert.

Achtung: Bei der Wiederherstellung werden inaktive Sicherungsdateien in Pools für aktive Daten entfernt. Geben Sie RECONSTRUCT=NO an, wenn die Daten in einen Pool für aktive Daten versetzt werden, der nicht für die Deduplizierung von Daten konfiguriert ist, verbleiben inaktive Sicherungsdateien in dem Speicherpool.
Gültige Werte:

No
Gibt an, dass die Wiederherstellung von Dateiaggregaten beim Versetzen von Daten nicht ausgeführt wird.

Yes
Gibt an, dass die Wiederherstellung von Dateiaggregaten beim Versetzen von Daten ausgeführt wird. Sie können diese Option nur angeben, wenn Quellen- und Zielspeicherpool Speicherpools mit sequenziellem Zugriff sind.

Beispiel: Nicht-Unicode- und Unicode-Daten eines Knotens versetzen

Daten für Knoten TOM im Speicherpool TAPEPOOL versetzen. Das Versetzen von Daten auf Dateien in Nicht-Unicode-Dateibereichen und Unicode-Dateibereichen \\jane\d$ beschränken. Die Daten sollen in den Plattenspeicherpool BACKUPPOOL versetzt werden.

```
move nodedata tom
 fromstgpool=tapepool tostgpool=backuppool
 filespace=* unifilespace=\\jane\d$
```

Beispiel: Alle Knotendaten aus Bandspeicherpools in einen Plattenspeicherpool versetzen

Alle Daten für Knoten SARAH aus allen primären Speicherpools mit sequenziellem Zugriff (in diesem Beispiel TAPEPOOL*) nach DISKPOOL versetzen. Um eine Liste der Speicherpools zu erhalten, die Daten für Knoten SARAH enthalten, geben Sie einen der folgenden QUERY OCCUPANCY- oder SELECT-Befehle aus:

```
query occupancy sarah
```

```
SELECT * from OCCUPANCY where node_name='sarah'
```

Achtung: In diesem Beispiel wird angenommen, dass die Ergebnisse TAPEPOOL1, TAPEPOOL4 und TAPEPOOL5 lauten.

```
move nodedata sarah
 fromstgpool=tapepool1 tostgpool=DISKPOOL

move nodedata sarah
 fromstgpool=tapepool4 tostgpool=DISKPOOL

move nodedata sarah
 fromstgpool=tapepool5 tostgpool=DISKPOOL
```

Beispiel: Nicht-Unicode- und Unicode-Dateibereiche eines Knotens versetzen

Das folgende Beispiel zeigt das Versetzen von Nicht-Unicode-Dateibereichen und Unicode-Dateibereichen für einen Knoten. Für Knoten NOAH den Nicht-Unicode-Dateibereich \\servtuc\d$ und den Unicode-Dateibereich \\tsmserv1\e$ mit der Dateibereichs-ID 2 aus dem Speicherpool TAPEPOOL mit sequenziellem Zugriff in den Speicherpool DISKPOOL mit wahlfreiem Zugriff versetzen.

```
move nodedata noah
 fromstgpool=tapepool tostgpool=diskpool
```

```
filespace=\\tsmserv1\d$ fsid=2
```

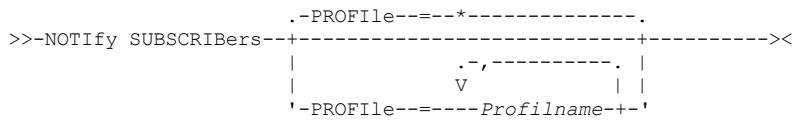
NOTIFY SUBSCRIBERS (Verwaltete Server auf Profilaktualisierung hinweisen)

Mit diesem Befehl können auf einem Konfigurationsmanager ein oder mehrere verwaltete Server benachrichtigt werden, dass ihre Konfigurationsdaten sofort aktualisiert werden müssen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

PROFIle (Erforderlich)
: Gibt den Namen des Profils an. Alle verwalteten Server, die für das Profil subskribieren, werden benachrichtigt. Es können Platzhalterzeichen verwendet werden, um mehrere Profile anzugeben. Sollen mehrere Profile angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Standardmäßig werden alle Subskribenten benachrichtigt.

Beispiel: Verwaltete Server zum Aktualisieren von Profilen benachrichtigen

Alle verwalteten Server, die für das Profil DELTA subskribieren, darauf hinweisen, die Aktualisierung ihrer Konfigurationsdaten anzufordern.

```
notify subscribers profile=delta
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für NOTIFY SUBSCRIBERS

Befehl	Beschreibung
DEFINE SUBSCRIPTION	Subskribiert einen verwalteten Server für ein Profil.
DELETE SUBSCRIBER	Löscht veraltete Subskriptionen verwalteter Server.
DELETE SUBSCRIPTION	Löscht eine angegebene Profilsubskription.
QUERY SUBSCRIBER	Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.
QUERY SUBSCRIPTION	Zeigt Informationen über Profilsubskriptionen an.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
SET CONFIGREFRESH	Gibt das Zeitintervall an, in dem verwaltete Server die Konfigurationsmanager ansprechen sollen.

PERFORM LIBACTION (Alle Laufwerke und Pfade für ein Kassettenarchiv definieren oder löschen)

Verwenden Sie diesen Befehl, um alle Laufwerke und ihre Pfade für ein einzelnes Kassettenarchiv in einem Schritt zu definieren oder zu löschen.

Dieser Befehl kann verwendet werden, wenn eine Kassettenarchivumgebung definiert oder eine vorhandene Hardwarekonfiguration, die Änderungen an vielen Laufwerkdefinitionen erfordert, geändert wird. Nachdem Sie ein Kassettenarchiv definiert haben, geben Sie den Befehl PERFORM LIBACTION aus, um die Laufwerke und ihre Pfade für das Kassettenarchiv zu definieren. Sie können auch alle Laufwerke und Pfade für ein Kassettenarchiv löschen, indem Sie den Befehl mit ACTION=DELETE ausgeben.

Dieser Befehl ist nur für die Speicherarchivtypen SCSI und VTL gültig. Um diesen Befehl mit ACTION=DEFINE verwenden zu können, muss die Option SANDISCOVERY unterstützt werden und aktiviert sein.

Ausführliche und aktuelle Informationen zur Kassettenarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-PERForm LIBACTion--Kassettenarchivname----------------------->

>----ACTion--=--+-DEFine--| A |-+------------------------------->
                +-DELete--------+
                +-RESet--| B |--+
                '-QUIesce-------'

                                .-PREView--=--No------.
>--+-------------------------+--+---------------------+---------><
   '-SOURCe--=--Quellenname-'  '-PREView--=--+-Yes-+-'
                                             '-No--'

A (DEFine)

|--+---------------------------------------------+--------------->
   '-DEVIce--=--Name der Kassettenarchiveinheit-'

   .-PREFix--=--Kassettenarchivname-.
>--+--------------------------------+--------------------------|
   '-PREFix--=--Laufwerkpräfix------'

B (RESet)

                          .-DRIVEsonly--=--No------.
|----ACTion--=--RESet-----+------------------------+-------------|
                          '-DRIVEsonly--=--+-Yes-+-'
                                           '-No--'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das definiert oder gelöscht werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen, es sei denn, Sie geben den Befehl PERFORM LIBACTION mit ACTION=DEFINE aus und verwenden den PREFIX-Standardwert. In diesem Fall beträgt die maximale Länge des Namens 25 Zeichen.

ACTion
: Gibt die Aktion für den Befehl PERFORM LIBACTION an. Gültige Werte:

  DEFine
  : Gibt an, dass Laufwerke und ihre Pfade für das angegebene Kassettenarchiv definiert werden. Die SAN-Erkennung muss aktiviert sein, bevor dieser Parameterwert angegeben wird.

  DELete
  : Gibt an, dass Laufwerke und ihre Pfade für das angegebene Kassettenarchiv gelöscht werden.

  RESet
  : Gibt an, dass Laufwerke und ihre Pfade für das angegebene Kassettenarchiv in 'online' aktualisiert werden.

    DRIVEsonly
    : Gibt an, dass nur Laufwerke für das angegebene Kassettenarchiv in 'online' aktualisiert werden.
      Gültige Werte:

      No
      : Gibt an, dass die Laufwerke und Pfade in 'online' aktualisiert werden.

      Yes
      : Gibt an, dass nur die Laufwerke in 'online' aktualisiert werden.

  QUIesce
  : Gibt an, dass die Laufwerke in 'offline' aktualisiert werden.

DEVIce
: Gibt den Namen der Kassettenarchiveinheit an, der beim Definieren von Pfaden verwendet wird, wenn noch kein Pfad zu dem Kassettenarchiv definiert wurde. Ist bereits ein Pfad definiert, wird der Parameter DEVICE ignoriert. Die maximale Länge für diesen Wert beträgt 64 Zeichen. Dieser Parameter ist wahlfrei.

PREFix

Gibt das Präfix an, das für alle Laufwerkdefinitionen verwendet wird. Beispielsweise werden mit dem PREFIX-Wert *DR* Laufwerke *DR0, DR1, DR2* für so viele Laufwerke erstellt, wie erstellt werden sollen. Wird für den Parameter PREFIX kein Wert angegeben, wird der Kassettenarchivname als Präfix für Laufwerkdefinitionen verwendet. Die maximale Länge für diesen Wert beträgt 25 Zeichen.

SOURCe

Gibt den Namen des Quellenservers an, der beim Definieren oder Löschen von Laufwerkpfaddefinitionen auf einem Kassettenarchivclient oder einem LAN-unabhängigen Client verwendet werden soll. Verwenden Sie diesen Parameter nur, wenn die Laufwerke in dem Kassettenarchiv für den lokalen Server definiert sind. Wenn kein Wert für den Parameter SOURCE angegeben wird, wird der Name des lokalen Servers (Standardwert) verwendet. Die maximale Länge für den Quellennamen beträgt 64 Zeichen.

Wird der Parameter SOURCE angegeben, können Sie nur Pfade für angegebene SOURCE-Werte zurücksetzen. Der Parameter SOURCE ist mit den Optionen RESET DRIVESONLY=YES und QUIESCE nicht kompatibel.

Wird ein anderer Quellenname als der Name des lokalen Servers mit ACTION=DEFINE angegeben, werden Laufwerkpfaddefinitionen mit dem Tokenwert UNDISCOVERED definiert. Die Pfaddefinitionen werden dann dynamisch von Kassettenarchivclients, die die SAN-Erkennung unterstützen, aktualisiert, wenn das Laufwerk zum ersten Mal angehängt wird.

PREView

Gibt die Ausgabe aller Befehle an, die für PERFORM LIBACTION verarbeitet werden, bevor der Befehl ausgegeben wird. Der Parameter PREVIEW ist mit dem Parameter DEVICE nicht kompatibel. Wenn Sie den Befehl PERFORM LIBACTION ausgeben, um ein Kassettenarchiv zu definieren, können Sie nicht beide Parameter PREVIEW und DEVICE angeben.
Gültige Werte:

No

Gibt an, dass keine Voranzeige der Befehle, die für PERFORM LIBACTION ausgegeben werden, angezeigt wird.

Yes

Gibt an, dass eine Voranzeige der Befehle, die für PERFORM LIBACTION ausgegeben werden, angezeigt wird.

Beispiel: Ein gemeinsam genutztes Kassettenarchiv definieren

Angenommen, Sie arbeiten in einem SAN und haben einen Kassettenarchivmanager mit dem Namen LIBMGR1 konfiguriert. Definieren Sie jetzt ein Kassettenarchiv mit dem Namen SHAREDTSM für einen Kassettenarchivclientserver mit dem Namen LIBCL1.

Geben Sie den Befehl DEFINE LIBRARY auf dem Kassettenarchivclientserver LIBCL1 aus:

```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

Geben Sie dann den Befehl PERFORM LIBACTION auf dem Kassettenarchivmanager LIBMGR1 aus, um die Laufwerkpfade für den Kassettenarchivclient zu definieren:

```
perform libaction sharedtsm action=define source=libcl1
```

Anmerkung: Die Option SANDISCOVERY muss unterstützt werden und auf dem Kassettenarchivclientserver aktiviert sein.

Beispiel: Kassettenarchiv mit vier Laufwerken definieren

Ein SCSI-Kassettenarchiv mit dem Namen KONA definieren:

```
define library kona libtype=scsi
```

Anschließend den Befehl PERFORM LIBACTION ausgeben, um Laufwerke und Pfade für das Kassettenarchiv zu definieren:
AIX-Betriebssysteme

```
perform libaction kona action=define device=/dev/lb3
prefix=dr
```

Der Server führt dann die folgenden Befehle aus:

```
define path server1 kona srct=server destt=library
device=/dev/lb3
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=/dev/mt1
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=/dev/mt2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=/dev/mt3define drive kona dr3
define path server1 dr3 srct=server destt=drive library=kona
device=/dev/mt4
```

Linux-Betriebssysteme

```
perform libaction kona action=define device=/dev/tsmscsi/lb3
prefix=dr
```

Der Server führt dann die folgenden Befehle aus:

```
define path server1 kona srct=server destt=library
device=/dev/tsmscsi/lb3
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=/dev/tsmscsi/mt1
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=/dev/tsmscsi/mt2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=/dev/tsmscsi/mt3define drive kona dr3
define path server1 dr3 srct=server destt=drive library=kona
device=/dev/tsmscsi/mt4
```


Windows-Betriebssysteme

```
perform libaction kona action=define device=lb0.0.0.2
prefix=dr
```

Der Server führt dann die folgenden Befehle aus:

```
define path server1 kona srct=server destt=library
device=lb0.0.0.2
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=mt0.1.0.2
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=mt0.2.0.2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=mt0.3.0.2
define drive kona dr3
define path server1 dr3 srct=server destt=drive library=kona
device=mt0.4.0.2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für PERFORM LIBACTION

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DELETE DRIVE	Löscht ein Laufwerk aus einem Kassettenarchiv.
DELETE LIBRARY	Löscht ein Kassettenarchiv.
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
QUERY DRIVE	Zeigt Informationen zu Laufwerken an.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE DRIVE	Ändert die Attribute eines Laufwerks.
UPDATE LIBRARY	Ändert die Attribute eines Kassettenarchivs.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.

PING SERVER (Verbindung zwischen Servern testen)

Mit diesem Befehl kann die Verbindung zwischen dem lokalen Server und einem fernen Server getestet werden.

Wichtig: Name und Kennwort des Administrator-Clients, der diesen Befehl ausgibt, müssen auch auf dem fernen Server definiert sein. Verfügt der ferne Server über die aktuelle Version, werden die Serverberechtigungsnachweise automatisch geprüft, wenn der Befehl PING SERVER ausgeführt wird. Verfügt der ferne Server nicht über die aktuelle Version, werden die Serverberechtigungsnachweise nicht geprüft.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-PING SERVER--Servername-------------------------------------><
```

Parameter

Servername (Erforderlich)
: Gibt den Namen des fernen Servers an.

Beispiel: Mit Ping einen Server überprüfen

Die Verbindung zu Server FRED testen.

```
ping server fred
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für PING SERVER

Befehl	Beschreibung
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
QUERY SERVER	Zeigt Informationen über Server an.

PREPARE (Wiederherstellungsplandatei erstellen)

Mit diesem Befehl kann eine Wiederherstellungsplandatei erstellt werden, die die für die Wiederherstellung eines IBM Spectrum Protect-Servers erforderlichen Daten enthält. Eine Wiederherstellungsplandatei kann in einem Dateisystem gespeichert werden, auf das vom Quellenserver oder einem Zielserver zugegriffen werden kann.

Mit dem Befehl QUERY ACTLOG kann abgefragt werden, ob der Befehl PREPARE erfolgreich ausgeführt wurde.

Diese Informationen können auch von der Serverkonsole oder, wenn für den Parameter WAIT der Wert YES angegeben wird, von einer Verwaltungsclientsitzung aus abgefragt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
            .-Source--=--DBBackup-------.
>>-Prepare--+---------------------------+----------------------->
            '-Source--=--+-DBBackup---+-'
                         '-DBSnapshot-'

>--+-----------------------------------+----------------------->
   '-DEVclass--=--Einheitenklassenname-'

>--+-----------------------+--+-----------------------+-------->
   '-PLANPrefix--=--Präfix-'  '-INSTRPrefix--=--Präfix-'

>--+-------------------------------+----------------------------->
   |                 .-,--------. |
   |                 V          | |
   '-COPYstgpool--=----Poolname-+-'

>--+---------------------------------------+----------------------->
   |                       .-,--------. |
   |                       V          | |
   '-ACTIVEDatastgpool--=----Poolname-+-'

                                    .-Wait--=--No------.
>--+-------------------------------+--+-----------------+------><
   |                 .-,--------. |  '-Wait--=--+-No--+-'
   |                 V          | |             '-Yes-'
```

```
'-PRIMstgpool--=----Poolname-+-'
```

Parameter

Source
: Gibt die Art der Datenbanksicherungsserie an, die IBM Spectrum Protect beim Generieren der Wiederherstellungsplandatei annimmt. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBACKUP. Unter folgenden Möglichkeiten kann gewählt werden:

  DBBackup
  : Gibt an, dass IBM Spectrum Protect die letzte vollständige Datenbanksicherungsserie annimmt.

  DBSnapshot
  : Gibt an, daß IBM Spectrum Protect die letzte Sicherungsserie mit Datenbankmomentaufnahmen annimmt.

DEVclass
: Gibt den Namen der Einheitenklasse an, mit der ein Wiederherstellungsplandateiobjekt auf einem Ziel-Server erstellt wird. Die Einheitenklasse muß den Einheitentyp SERVER haben.
  Wichtig: Die maximale Kapazität für die Einheitenklasse muß größer als die Größe der Wiederherstellungsplandatei sein. Überschreitet die Größe der Wiederherstellungsplandatei die maximale Kapazität, schlägt der Befehl fehl.
  Die Namenskonvention für das Archivierungsobjekt mit der Wiederherstellungsplandatei auf dem Ziel-Server lautet:

  - **Dateibereichsname:**
    - ADSM.SERVER
  - **Qualifikationsmerkmal der oberen Ebene:**
    -  AIX-Betriebssysteme  Linux-Betriebssystemedevclassprefix/servername.yyyymmdd.hhmmss
    -  Windows-Betriebssystemedevclassprefix\servername.yyyymmdd.hhmmss
  - **Qualifikationsmerkmal der unteren Ebene:**
    - RPF.OBJ.1

  Der Name des virtuellen Bereichs der Wiederherstellungsplandatei, der in der Datenträger-History-Tabelle auf dem Quellen-Server aufgezeichnet ist, hat das Format `servername.yyyymmdd.hhmmss`.

  Wird der Parameter DEVCLASS nicht angegeben, wird die Wiederherstellungsplandatei auf der Basis des Planpräfix in eine Datei geschrieben.

  Wird SOURCE=DBBACKUP angegeben oder als Standardwert verwendet, gibt der Datenträger-History-Eintrag für das Wiederherstellungsplandateiobjekt den Datenträgertyp RPFILE an. Wird SOURCE=DBSNAPSHOT angegeben, gibt der Datenträger-History-Eintrag den Datenträgertyp RPFSNAPSHOT an.

PLANPrefix
: Gibt das Pfadnamenpräfix an, das im Namen der Wiederherstellungsplandatei verwendet wird. Dieser Parameter ist wahlfrei.

  -  AIX-Betriebssysteme  Linux-BetriebssystemeDie maximale Länge beträgt 250 Zeichen.
  -  Windows-BetriebssystemeDie maximale Länge beträgt 200 Zeichen.

   Windows-BetriebssystemeGibt das Pfadnamenpräfix an, das im Namen der Wiederherstellungsplandatei verwendet wird.

  IBM Spectrum Protect hängt an das Präfix das sortierbare Datums- und Zeitformat `jjjjmmtt.hhmmss`. Beispiel: 20081115.051421.

   AIX-Betriebssysteme  Linux-BetriebssystemeDas Präfix kann Folgendes sein:

  Verzeichnispfad
  : Das Präfix mit dem Schrägstrich (/) beenden. Beispiel:

    ```
    PLANPREFIX=/adsmsrv/recplans/
    ```

    Der daraus resultierende Dateiname würde wie folgt aussehen:

    ```
    /adsmsrv/recplans/20081115.051421
    ```

  Verzeichnispfad, gefolgt von einer Zeichenfolge
  : IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

    ```
    PLANPREFIX=/adsmsrv/recplans/accounting
    ```

    Der daraus resultierende Dateiname sieht wie folgt aus:

    ```
    /adsmsrv/recplans/accounting.20081115.051421
    ```

    Den Punkt vor dem Datum und der Uhrzeit beachten.

  Nur Zeichenfolge
  : IBM Spectrum Protect gibt den Verzeichnispfad an. IBM Spectrum Protect verwendet den Namen des aktuellen Arbeitsverzeichnisses. Beispiel: Das aktuelle Arbeitsverzeichnis lautet /opt/tivoli/tsm/server/bin und es wird der folgende Parameter angegeben:

```
PLANPREFIX=shipping
```

Der daraus resultierende Dateiname sieht wie folgt aus:

```
/opt/tivoli/tsm/server/bin/shipping.20081115.051421
```

Den Punkt vor dem Datum und der Uhrzeit beachten.

 Das Präfix kann Folgendes sein:

Verzeichnispfad
: Das Präfix mit dem umgekehrten Schrägstrich (\) beenden. Beispiel:

```
PLANPREFIX=c:\adsmsrv\recplans\
```

Der daraus resultierende Dateiname sieht wie folgt aus:

```
c:\adsmsrv\recplans\20081115.051421
```

Tipp: Wenn Sie den Befehl PREPARE über den Verwaltungsbefehlszeilenclient ausgeben und das letzte Zeichen in der Befehlszeile ein umgekehrter Schrägstrich ist, wird er als Fortsetzungszeichen interpretiert. Um dies zu vermeiden, den Präfixwert in Anführungszeichen setzen. Beispiel:

```
PLANPREFIX="c:\adsmsrv\recplans\"
```

Verzeichnispfad, gefolgt von einer Zeichenfolge
: IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

```
PLANPREFIX=c:\adsmsrv\recplans\accounting
```

Der daraus resultierende Dateiname sieht wie folgt aus:

```
c:\adsmsrv\recplans\accounting.20081115.051421
```

Den Punkt vor dem Datum und der Uhrzeit beachten.

Nur Zeichenfolge
: IBM Spectrum Protect hängt das Datum und die Uhrzeit im Format *.yyyymmdd.hhmmss* (den Punkt vor dem Datum und der Uhrzeit beachten) an das Präfix an. Der von dem Befehl PREPARE verwendete Verzeichnispfad ist das Verzeichnis, das dieses “Exemplar” des IBM Spectrum Protect-Servers darstellt. Dabei handelt es sich normalerweise um das ursprüngliche Installationsverzeichnis des IBM Spectrum Protect-Servers. Im folgenden Beispiel stellt c:\Programme\Tivoli\TSM;\server2 dieses Verzeichnis dar, und der Befehl PREPARE wird mit folgendem Parameter ausgegeben:

```
PLANPREFIX=shipping
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
c:\Programme\Tivoli\TSM;\server2\shipping.20081115.051421
```

Wird der Parameter PLANPREFIX nicht angegeben, wählt IBM Spectrum Protect das Präfix wie folgt aus:

- Wurde der Befehl SET DRMPLANPREFIX ausgegeben, verwendet IBM Spectrum Protect das in diesem Befehl angegebene Präfix.
-  Ist der Befehl SET DRMPLANPREFIX nicht definiert, verwendet IBM Spectrum Protect als Pfad das Verzeichnis, das dieses “Exemplar” des IBM Spectrum Protect-Servers darstellt. Hierbei handelt es sich normalerweise um das ursprüngliche Installationsverzeichnis des IBM Spectrum Protect-Servers. Beispiel: Folgendes Verzeichnis bildet das vorliegende Exemplar des Servers:

  ```
  c:\Programme\Tivoli\TSM;\server2
  ```

  Der daraus resultierende Name der Wiederherstellungsplandatei lautet wie folgt:

  ```
  c:\Programme\Tivoli\TSM;\server2\2008115.051421
  ```

-   Wurde der Befehl SET DRMPLANPREFIX nicht ausgegeben, verwendet IBM Spectrum Protect den Verzeichnispfadnamen des aktuellen Arbeitsverzeichnisses. Das aktuelle Arbeitsverzeichnis lautet beispielsweise:

  ```
  /opt/tivoli/tsm/server/bin
  ```

  Der daraus resultierende Dateiname sieht wie folgt aus:

  ```
  /opt/tivoli/txm/server/bin/20081115.051421
  ```

INSTRPrefix
: Gibt das Präfix des Pfadnamens an, das von IBM Spectrum Protect zum Lokalisieren der Dateien verwendet wird, die die Wiederherstellungsanweisungen enthalten. Die maximale Länge beträgt   250  200 Zeichen.
 Das Präfix kann Folgendes sein:

Verzeichnispfad
Das Präfix mit dem Schrägstrich (/) beenden. Beispiel:

```
INSTRPREFIX=/adsmsrv/recinstr/
```

```
/adsmsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
```

Verzeichnispfad, gefolgt von einer Zeichenfolge
IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

```
INSTRPREFIX=/adsmsrv/recinstr/accounts
```

IBM Spectrum Protect hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. Für die Datei RECOVERY.INSTRUCTIONS.GENERAL lautet der daraus resultierende Dateiname wie folgt:

```
/adsmsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

Nur Zeichenfolge

- IBM Spectrum Protect gibt den Verzeichnispfad an und hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. IBM Spectrum Protect verwendet den Namen des aktuellen Arbeitsverzeichnisses. Beispiel: Das aktuelle Arbeitsverzeichnis lautet /opt/tivoli/tsm/server/bin und es wird der folgende Parameter angegeben:

  ```
  INSTRPREFIX=shipping
  ```

  Für die Datei RECOVERY.INSTRUCTIONS.GENERAL sieht der daraus resultierende Dateiname wie folgt aus:

  ```
  /opt/tivoli/tsm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
  ```

Windows-BetriebssystemeDas Präfix kann Folgendes sein:

Verzeichnispfad
Das Präfix mit dem umgekehrten Schrägstrich (\) beenden. Beispiel:

```
INSTRPREFIX=c:\adsmsrv\recinstr\
```

IBM Spectrum Protect hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. Für die Datei RECOVERY.INSTRUCTIONS.GENERAL lautet der daraus resultierende Dateiname wie folgt:

```
c:\adsmsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
```

Tipp: Wenn Sie den Befehl PREPARE über den Verwaltungsbefehlszeilenclient ausgeben und das letzte Zeichen in der Befehlszeile ein umgekehrter Schrägstrich ist, wird er als Fortsetzungszeichen interpretiert. Um dies zu vermeiden, den Präfixwert in Anführungszeichen setzen. For example:

```
INSTRPREFIX="c:\adsmserv\recinstr\"
```

Verzeichnispfad, gefolgt von einer Zeichenfolge
IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

```
INSTRPREFIX=c:\adsmsrv\recinstr\accounts
```

IBM Spectrum Protect hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. Für die Datei RECOVERY.INSTRUCTIONS.GENERAL lautet der daraus resultierende Dateiname wie folgt:

```
c:\adsmsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

Nur Zeichenfolge
IBM Spectrum Protect gibt den Verzeichnispfad an und hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. IBM Spectrum Protect hängt den Namen der Zeilengruppe für die Wiederherstellungsplandatei an das Präfix an. Ist das Präfix nur eine Zeichenfolge, ist der von dem Befehl PREPARE verwendete Verzeichnispfad das Verzeichnis, das dieses Exemplar des IBM Spectrum Protect-Servers darstellt. Dabei handelt es sich normalerweise um das ursprüngliche Installationsverzeichnis des IBM Spectrum Protect-Servers. Im folgenden Beispiel stellt c:\Programme\Tivoli\TSM;\server2 dieses Verzeichnis dar, und der Befehl PREPARE wird mit folgendem Parameter ausgegeben:

```
INSTRPREFIX=dock
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

```
c:\Programme\Tivoli\TSM;\server2\shipping.20081115.051421
```

Wird der Parameter INSTRPREFIX nicht angegeben, wählt IBM Spectrum Protect das Präfix wie folgt aus:

- Wurde der Befehl SET DRMINSTRPREFIX ausgegeben, verwendet IBM Spectrum Protect das in diesem Befehl angegebene Präfix.
- Windows-BetriebssystemeWenn der Befehl SET DRMINSTRPREFIX nicht ausgegeben wurde, verwendet IBM Spectrum Protect das Verzeichnis, das diese "Instanz" des IBM Spectrum Protect-Servers darstellt, als Pfad; hierbei handelt es sich normalerweise um das ursprüngliche Installationsverzeichnis des Servers. Beispiel: Folgendes Verzeichnis bildet das vorliegende Exemplar des Servers:

```
c:\Programme\Tivoli\TSM;\server2
```

Der daraus resultierende Name der Wiederherstellungsplandatei lautet wie folgt:

```
c:\Programme\Tivoli\TSM;\server2\RECOVERY.INSTRUCTIONS.GENERAL
```

- AIX-BetriebssystemeLinux-BetriebssystemeWurde der Befehl SET DRMINSTRPREFIX nicht ausgegeben, verwendet IBM Spectrum Protect das aktuelle Arbeitsverzeichnis.
  Lautet beispielsweise das aktuelle Arbeitsverzeichnis /opt/tivoli/tsm/server/bin, würde für die Datei RECOVERY.INSTRUCTIONS.GENERAL der daraus resultierende Dateiname wie folgt lauten:

  ```
  /opt/tivoli/tsm/server/bin/RECOVERY.INSTRUCTIONS.GENERAL
  ```

PRIMstgpool
: Gibt die Namen der primären Speicherpools an, die wiederhergestellt werden sollen. Die Speicherpoolnamen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden. Wird dieser Parameter nicht angegeben, wählt IBM Spectrum Protect die Speicherpools wie folgt aus:

  - Wurde der Befehl SET DRMPRIMSTGPOOL ausgegeben, berücksichtigt IBM Spectrum Protect die in diesem Befehl angegebenen primären Speicherpools.
  - Wurde der Befehl SET DRMPRIMSTGPOOL nicht ausgegeben, berücksichtigt IBM Spectrum Protect alle primären Speicherpools.

COPYstgpool
: Gibt die Namen der Kopienspeicherpools an, die zum Sichern der primären Speicherpools verwendet wurden, die wiederhergestellt werden sollen (siehe Parameter PRIMSTGPOOL). Die Speicherpoolnamen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden. Wird dieser Parameter nicht angegeben, wählt IBM Spectrum Protect die Speicherpools wie folgt aus:

  - Wurde der Befehl SET DRMCOPYSTGPOOL ausgegeben, berücksichtigt IBM Spectrum Protect diese Kopienspeicherpools.
  - Wurde der Befehl SET DRMCOPYSTGPOOL nicht ausgegeben, berücksichtigt IBM Spectrum Protect alle Kopienspeicherpools.

ACTIVEDatastgpool
: Gibt die Namen der Speicherpools für aktive Daten an, die für den Zugriff an einem anderen Standort verfügbar sein sollen. Die Namen der Speicherpools für aktive Daten sind ohne Leerzeichen durch Kommas voneinander zu trennen. Es können Platzhalterzeichen verwendet werden. Wird dieser Parameter nicht angegeben, wählt IBM Spectrum Protect die Speicherpools wie folgt aus:

  - Wurde der Befehl SET ACTIVEDATASTGPOOL zuvor mit gültigen Namen von Speicherpools für aktive Daten ausgegeben, verarbeitet IBM Spectrum Protect diese Speicherpools.
  - Wurde der Befehl SET ACTIVEDATASTGPOOL nicht ausgegeben, oder wurden alle Speicherpools für aktive Daten mit dem Befehl SET ACTIVEDATASTGPOOL entfernt, verarbeitet IBM Spectrum Protect nur die Datenträger im Pool für aktive Daten, die zum Zeitpunkt der Ausführung des Befehls PREPARE als ONSITE markiert waren. IBM Spectrum Protect markiert diese Datenträger als UNAVAILABLE.

Wait
: Gibt an, ob dieser Befehl im Hintergrund oder Vordergrund verarbeitet wird.

  No
  : Gibt die Hintergrundverarbeitung an. Dies ist der Standardwert.

  Yes
  : Gibt die Vordergrundverarbeitung an.

    AIX-BetriebssystemeLinux-BetriebssystemeYES kann nicht von der Server-Konsole aus angegeben werden.

Beispiel: Eine Wiederherstellungsplandatei erstellen

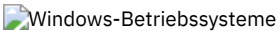
Den Befehl PREPARE ausgeben und das Aktivitätenprotokoll abfragen, um die Ergebnisse zu prüfen.

```
prepare
query actlog search=prepare
```

AIX-BetriebssystemeLinux-Betriebssysteme

```
05/03/2008 12:01:13  ANR0984I Prozess 3 für PREPARE im
                      BACKGROUND um 12:01:13 gestartet.
05/03/2008 12:01:13  ANR6918W PREPARE: Datei mit Wiederherstellungsanweisungen
                      /home/guest/drmtest/prepare/tservr/DSM1509/
                      RECOVERY.INSTRUCTIONS.DATABASE nicht gefunden.
05/03/2008 12:01:13  ANR6918W PREPARE: Datei mit Wiederherstellungsanweisungen
                      /home/guest/drmtest/prepare/tservr/DSM1509/
                      RECOVERY.INSTRUCTIONS.STGPOOL nicht gefunden.
05/03/2008 12:01:13  ANR6913W PREPARE: Keine Datenträger mit Sicherungsdaten
                      im Kopienspeicherpool CSTORAGEP vorhanden.
05/03/2008 12:01:13  ANR6913W PREPARE: Keine Datenträger mit Sicherungsdaten
                      im Kopienspeicherpool CSTORAGEPSM vorhanden.
05/03/2008 12:01:14  ANR6920W PREPARE: Generierter Ersatzdatenträger
                      BACK4X@ für Einheitentyp 8MM ungültig.
```

```
                      Originaldatenträgername: BACK4X. Zeilengruppe
                      ist Makro PRIMARY.VOLUMES.REPLACEMENT.
05/03/2008 12:01:14   ANR6900I PREPARE: Wiederherstellungsplandatei
                      /home/guest/drmtest/prepare/plandir/DSM1509/
                      r.p.20080503.120113 wurde erstellt.
05/03/2008 12:01:14   ANR0985I Prozess 3 für PREPARE, der im
                      BACKGROUND ausgeführt wird, wurde mit Status
                      SUCCESS um 12:01:14 beendet.
```


Windows-Betriebssysteme

```
05/03/2008 12:01:13   ANR0984I Prozess 3 für PREPARE im
                      BACKGROUND um 12:01:13 gestartet.
05/03/2008 12:01:13   ANR6918W PREPARE: Datei mit Wiederherstellungsanweisungen
                      c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.DATABASE
                      nicht gefunden.
05/03/2008 12:01:13   ANR6918W PREPARE: Datei mit Wiederherstellungsanweisungen
                      c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.STGPOOL
                      nicht gefunden.
05/03/2008 12:01:13   ANR6913W PREPARE: Keine Datenträger mit Sicherungsdaten
                      im Kopienspeicherpool CSTORAGEP vorhanden.
05/03/2008 12:01:13   ANR6913W PREPARE: Keine Datenträger mit Sicherungsdaten
                      im Kopienspeicherpool CSTORAGEPSM vorhanden.
05/03/2008 12:01:14   ANR6920W PREPARE: Generierter Ersatzdatenträger
                      BACK4X@ für Einheitenklasse 8MM ungültig.
                      Originaldatenträgername: BACK4X. Zeilengruppe
                      ist Makro PRIMARY.VOLUMES.REPLACEMENT.
05/03/2008 12:01:14   ANR6900I PREPARE: Wiederherstellungsplandatei
                      c:\drmtest\prepare\r.p.20080503.120113
                      wurde erstellt.
05/03/2008 12:01:14   ANR0985I Prozess 3 für PREPARE, der im
                      BACKGROUND ausgeführt wird, wurde mit Status
                      SUCCESS um 12:01:14 beendet.
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für PREPARE

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
DELETE VOLHISTORY	Löscht History-Daten sequenzieller Datenträger aus der Datenträger-History-Datei.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.
QUERY RPFCONTENT	Zeigt den Inhalt einer Wiederherstellungsplandatei an.
QUERY RPFILE	Zeigt Informationen über Wiederherstellungsplandateien an.
QUERY SERVER	Zeigt Informationen über Server an.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.
SET DRMACTIVEDATASTGPOOL	Gibt an, dass Speicherpools für aktive Daten von DRM verwaltet werden.
SET DRMCOPYSTGPOOL	Gibt an, dass Kopienspeicherpools von DRM verwaltet werden.
SET DRMINSTRPREFIX	Gibt das Präfix des Pfadnamens für die Wiederherstellungsplananweisungen an.
SET DRMPLANVPOSTFIX	Gibt die Namen der Ersatzdatenträger in der Wiederherstellungsplandatei an.
SET DRMPLANPREFIX	Gibt das Präfix des Pfadnamens für den Wiederherstellungsplan an.
SET DRMPRIMSTGPOOL	Gibt an, dass primäre Speicherpools von DRM verwaltet werden.
SET DRMRPFEXPIREDAYS	Definiert Verfallskriterien für Wiederherstellungsplandateien.
UPDATE VOLHISTORY	Ändert Standortinformationen für einen Datenträger in der Datenträger-History-Datei oder fügt Informationen hinzu.


AIX-Betriebssysteme 
Linux-Betriebssysteme 
Windows-Betriebssysteme

PROTECT STGPOOL (Daten schützen, die zu einem Speicherpool gehören)

Verwenden Sie diesen Befehl, um Daten in einem Verzeichniscontainerspeicherpool zu schützen, indem eine Kopie der Daten in einem anderen Speicherpool auf einem Zielreplikationsserver oder auf demselben Server gespeichert wird und die Daten auf Band geschützt werden. Wenn Sie

den Verzeichniscontainerspeicherpool schützen, können Sie später mithilfe des Befehls REPAIR STGPOOL versuchen, beschädigte Daten in dem Speicherpool zu reparieren.

Wenn Sie den Befehl PROTECT STGPOOL für einen Verzeichniscontainerspeicherpool ausgeben, werden in diesem Speicherpool gespeicherte Daten in dem Zielpool gesichert, den Sie angeben. Die Daten können in den folgenden Zielpools gesichert werden:

- Verzeichniscontainerspeicherpool auf dem Zielreplikationsserver.
  Voraussetzung: Für den Speicherpool, der geschützt wird, müssen Sie den Zielpool angeben, indem Sie den Parameter PROTECTSTGPOOL im Befehl DEFINE STGPOOL oder UPDATE STGPOOL verwenden.

  Wenn Sie den Befehl PROTECT STGPOOL regelmäßig verwenden, können Sie in der Regel die Verarbeitungszeit für den Befehl REPLICATE NODE verringern. Die Datenbereiche, die bereits durch Speicherpoolschutzoperationen auf den Zielreplikationsserver kopiert wurden, werden übersprungen, wenn die Knotenreplikation gestartet wird.

  Als Teil der Operation PROTECT STGPOOL können Prozesse ausgeführt werden, um beschädigte Bereiche im Speicherpool des Zielservers zu reparieren. Die Reparaturoperation wird unter den folgenden Bedingungen ausgeführt:
  - Sowohl der Quellenserver als auch der Zielserver müssen über Version 7.1.5 oder eine höhere Version verfügen.
  - Bereiche, die auf dem Zielserver bereits als beschädigt markiert sind, werden repariert. Der Reparaturprozess führt keinen Prüfprozess aus, um beschädigte Daten zu identifizieren.
  - Nur Zielbereiche, die mit Quellenbereichen übereinstimmen, werden repariert. Zielbereiche, die beschädigt sind, aber keine Entsprechung auf dem Quellenserver haben, werden nicht repariert.

  Einschränkungen: Für die Reparaturoperation, die als Teil der Operation PROTECT STGPOOL ausgeführt wird, gelten die folgenden Einschränkungen:
  - Bereiche, die zu verschlüsselten Objekten gehören, werden nicht repariert.
  - Der Zeitpunkt des Auftretens der Beschädigung in dem Zielspeicherpool und die Reihenfolge der Befehle REPLICATE NODE und PROTECT STGPOOL können Auswirkungen darauf haben, ob der Reparaturprozess erfolgreich ist. Einige Bereiche, die mit einem Befehl REPLICATE NODE in dem Zielspeicherpool gespeichert wurden, werden möglicherweise nicht repariert.
- Durch Kopieren auf Band geschützte Containerkopienspeicherpools auf demselben Server.
  Voraussetzung: Für den Speicherpool, der geschützt wird, müssen Sie den Zielspeicherpool angeben, indem Sie den Parameter PROTECTLOCALSTGPOOLS verwenden. Details zu dem Parameter finden Sie unter den Befehlen zum Definieren und Aktualisieren von Verzeichniscontainerspeicherpools (Befehle DEFINE STGPOOL und UPDATE STGPOOL).

  Als Teil der Operation PROTECT STGPOOL können Datenträger in dem Zielpool konsolidiert werden. Der Wert des Parameters RECLAIM für den Containerkopienspeicherpool hat Auswirkungen darauf, ob Datenträger konsolidiert werden. Details zu dem Parameter finden Sie unter den Befehlen zum Definieren und Aktualisieren von Containerkopienspeicherpools (Befehle DEFINE STGPOOL und UPDATE STGPOOL).

Einschränkung: Es ist nicht möglich, eine gleichzeitige Ausführung mehrerer Operationen PROTECT STGPOOL zu planen. Warten Sie auf die Beendigung einer Operation PROTECT STGPOOL, bevor Sie eine weitere Operation starten.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

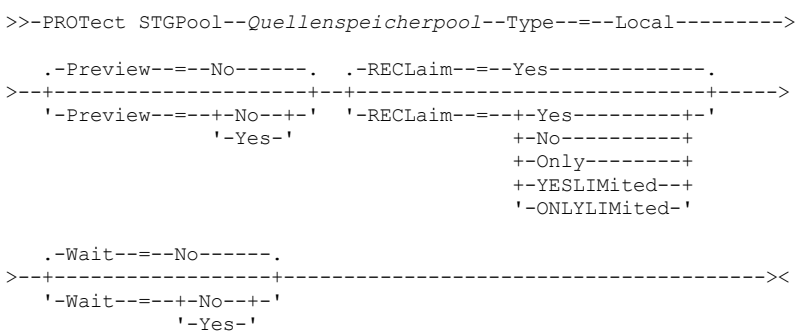
Syntax, wenn das Ziel der Replikationsserver ist

```
>>-PROTect STGPool--Quellenspeicherpool-------------------------->

   .-Type--=--Replserver-.  .-FORCEREConcile--=--No------.
>--+---------------------+--+----------------------------+------>
   '-Type--=--Replserver-'  '-FORCEREConcile--=--+-No--+-'
                                                 '-Yes-'

                      (1)
   .-MAXSESSions--=--10-------------------.
>--+-------------------------------------+--------------------->
   '-MAXSESSions--=----Anzahl Sitzungen---'

   .-Preview--=--No------.  .-PURGEdata--=--No----------.
>--+--------------------+--+---------------------------+------->
   '-Preview--=--+-No--+-'  '-PURGEdata--=--+-No------+-'
                 '-Yes-'                    +-All-----+
                                            '-Deleted-'

   .-Wait--=--No------.  .-TRANSFERMethod--=--Tcpip---------.
>--+-----------------+--+---------------------------------+--><
   '-Wait--=--+-No--+-'  |                            (2) |
              '-Yes-'    '-TRANSFERMethod--=--+-Tcpip-+-----'
                                              '-Fasp--'
```

Anmerkungen:

1. Linux-BetriebssystemeWird der Parameter TRANSFERMETHOD auf den Standardwert TCPIP gesetzt, ist der Standardwert des Parameters MAXSESSIONS 10. Wird der Parameter TRANSFERMETHOD auf FASP gesetzt, ist der Standardwert des Parameters MAXSESSIONS 2.
2. Linux-BetriebssystemeDer Parameter TRANSFERMETHOD ist nur auf Betriebssystemen Linux x86_64 verfügbar.

Syntax, wenn das Ziel ein Bandspeicherpool auf demselben Server ist



Parameter

Quellenspeicherpool (Erforderlich)
Gibt den Namen des Verzeichniscontainerspeicherpools auf dem Quellenserver an.

Type
Gibt den Typ des Ziels für die Schutzoperation an. Dieser Parameter ist wahlfrei. Der Standardwert ist REPLSERVER. Geben Sie einen der folgenden Werte an:

Replserver
Gibt an, dass das Ziel der Speicherpool auf dem Zielreplikationsserver ist, der für den Quellenspeicherpool mit dem Parameter PROTECTSTGPOOL im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert wurde.

Local
Gibt an, dass sich das Ziel auf demselben Server wie der Quellenspeicherpool befindet. Das Ziel ist der Containerkopienspeicherpool, der mit dem Parameter PROTECTLOCALSTGPOOLS im Befehl DEFINE STGPOOL oder UPDATE STGPOOL für den Quellenspeicherpool definiert wird.
Tipp: Standardmäßig verwendet der Server maximal zwei parallele Prozesse, um Daten in ein lokales Ziel zu kopieren. Sie können die maximale Anzahl paralleler Prozesse ändern, indem Sie den Containerkopienspeicherpool aktualisieren, der das Ziel ist. Verwenden Sie den Befehl UPDATE STGPOOL mit dem Parameter PROTECTPROCESS.

FORCEREConcile
Gibt an, ob die Unterschiede zwischen Datenbereichen in dem Verzeichniscontainerspeicherpool auf dem Quellenserver und dem Zielserver abgeglichen werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie einen der folgenden Werte an:

No
Gibt an, dass bei der Datensicherung nicht alle Datenbereiche in dem Verzeichniscontainerspeicherpool auf dem Quellenserver mit Datenbereichen auf dem Zielserver verglichen werden. Stattdessen werden bei der Datensicherung Änderungen an den Datenbereichen auf dem Quellenserver seit der letzten Sicherung verfolgt und diese Änderungen auf dem Zielserver synchronisiert.

Yes
Gibt an, dass bei der Datensicherung alle Datenbereiche auf dem Quellenserver mit Datenbereichen auf dem Zielserver verglichen und die Datenbereiche auf dem Zielserver mit den Datenbereichen auf dem Quellenserver synchronisiert werden.

MAXSESSions
Gibt die maximale Anzahl der Datensitzungen an, die Daten an einen Zielserver senden können. Dieser Parameter ist wahlfrei. Der angegebene Wert kann im Bereich 1 - 100 liegen.

AIX-BetriebssystemeWindows-BetriebssystemeDer Standardwert ist 10.

Linux-BetriebssystemeDer Standardwert variiert:

- Bei TRANSFERMETHOD=TCPIP ist der Standardwert des Parameters MAXSESSIONS 10.
- Bei TRANSFERMETHOD=FASP ist der Standardwert des Parameters MAXSESSIONS 2.

Wenn Sie die Anzahl der Sitzungen erhöhen, können Sie den Durchsatz für den Speicherpool verbessern.

Wenn Sie einen Wert für den Parameter MAXSESSIONS definieren, stellen Sie sicher, dass die verfügbare Bandbreite und die Prozessorkapazität des Quellen- und Zielservers ausreichend sind.

Tipps:

- Wird ein Befehl QUERY SESSION ausgegeben, kann die Gesamtzahl der Sitzungen die Anzahl der Datensitzungen überschreiten. Die Differenz resultiert aus kurzen Steuersitzungen, die zum Abfragen und Definieren von Operationen verwendet werden.
- Die Anzahl der Sitzungen, die für den Schutz verwendet werden, hängt vom Datenvolumen ab, das gesichert wird. Wird nur ein geringes Datenvolumen gesichert, wird durch die Erhöhung der Anzahl Sitzungen kein Vorteil erzielt.

Preview
Gibt an, ob eine Voranzeige der Daten aufgerufen werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Geben Sie einen der folgenden Werte an:

No
Gibt an, dass die Daten auf dem Zielserver gesichert, aber nicht vorangezeigt werden.
Yes
Gibt an, dass die Daten vorangezeigt, aber nicht gesichert werden.

PURGEdata
Gibt an, dass Datenbereiche auf dem Zielserver gelöscht werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass Datenbereiche auf dem Zielserver nicht gelöscht werden.
All
Gibt an, dass alle Datenbereiche auf dem Zielserver gelöscht werden. Datenbereiche, die von anderen Daten im Zielspeicherpool referenziert werden, werden nicht gelöscht.
Deleted
Gibt an, dass Datenbereiche, die auf dem Quellenserver gelöscht wurden, vom Zielserver gelöscht werden. Neue Datenbereiche werden nicht geschützt.

RECLaim
Gibt an, ob die Konsolidierung ausgeführt wird, wenn der Befehl PROTECT STGPOOL verarbeitet wird. Die Konsolidierung wird für den lokalen Containerkopienspeicherpool ausgeführt, der das Ziel der Schutzoperation ist. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass die Konsolidierung zusammen mit der Speicherpoolschutzoperation ausgeführt wird, wenn der Befehl ausgegeben wird. Die Konsolidierung wird vollständig ausgeführt; die Anzahl der Datenträger im Speicherpool, die für die Konsolidierung verarbeitet werden, ist hierbei nicht begrenzt.
No
Gibt an, dass die Konsolidierung nicht ausgeführt wird, wenn der Befehl ausgegeben wird. Nur die Speicherpoolschutzoperation wird ausgeführt.
Only
Gibt an, dass ausschließlich die Konsolidierung ausgeführt wird, wenn der Befehl ausgegeben wird. Die Speicherpoolschutzoperation wird nicht ausgeführt. Daten im Verzeichniscontainerspeicherpool, die seit der letzten Schutzoperation aktualisiert wurden, werden daher nicht geschützt. Die Konsolidierung wird vollständig ausgeführt; die Anzahl der Datenträger im Speicherpool, die für die Konsolidierung verarbeitet werden, ist hierbei nicht begrenzt.
YESLIMited
Gibt an, dass die Konsolidierung zusammen mit der Speicherpoolschutzoperation ausgeführt wird, wenn der Befehl ausgegeben wird. Die Konsolidierung wird ausgeführt, bis sie den Konsolidierungsgrenzwert erreicht, der für den Containerkopienspeicherpool definiert ist. Der Konsolidierungsgrenzwert wird mit dem Parameter RECLAIMLIMIT im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert.
ONLYLIMited
Gibt an, dass ausschließlich die Konsolidierung ausgeführt wird, wenn der Befehl ausgegeben wird. Die Speicherpoolschutzoperation wird nicht ausgeführt. Daten im Verzeichniscontainerspeicherpool, die seit der letzten Schutzoperation aktualisiert wurden, werden daher nicht geschützt. Die Konsolidierung wird ausgeführt, bis sie den Konsolidierungsgrenzwert erreicht, der für den Containerkopienspeicherpool definiert ist. Der Konsolidierungsgrenzwert wird mit dem Parameter RECLAIMLIMIT im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert.

Wait
Gibt an, ob darauf gewartet werden soll, dass der Server diesen Befehl im Vordergrund verarbeitet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass der Befehl im Hintergrund verarbeitet wird. Um die Hintergrundprozesse dieses Befehls zu überwachen, geben Sie den Befehl QUERY PROCESS aus.
Yes
Gibt an, dass der Befehl im Vordergrund verarbeitet wird. Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist.
Einschränkung: Sie können nicht `WAIT=YES` an der Serverkonsole angeben.

Linux-BetriebssystemeTRANSFERMethod

Linux-BetriebssystemeGibt die Methode an, die für die Datenübertragung zwischen Servern verwendet wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Tcpip
: Gibt an, dass TCP/IP für die Übertragung von Daten verwendet wird. Dieser Wert ist der Standardwert.

Fasp
: Gibt an, dass die Aspera FASP-Technologie (Fast Adaptive Secure Protocol) für die Übertragung von Daten verwendet wird. Mit der Aspera FASP-Technologie kann die Datenübertragung in einem Weitverkehrsnetz (WAN) optimiert werden. Wenn Sie TRANSFERMETHOD=FASP angeben, werden alle Parameter TRANSFERMETHOD überschrieben, die Sie im Befehl DEFINE SERVER oder UPDATE SERVER angegeben haben.
Einschränkungen:

- Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie bestimmen, ob die Technologie für Ihre Systemumgebung geeignet ist, und die entsprechenden Lizenzen installieren. Anweisungen finden Sie unter Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann. Wenn die Lizenzen fehlen oder abgelaufen sind, schlagen Operationen zum Schützen von Speicherpools fehl.
- Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.

Beispiel: Alle Datenbereiche auf dem Zielserver löschen

Löschen Sie alle Datenbereiche in einem Verzeichniscontainerspeicherpool auf dem Zielserver. Der Verzeichniscontainerspeicherpool mit dem Namen POOL1 auf dem Quellenserver wird nicht mehr durch den Verzeichniscontainerspeicherpool auf dem Zielserver geschützt. Sie können alle Bereiche löschen, um den Verzeichniscontainerspeicherpool auf dem Zielserver zu bereinigen, der den Quellenserver nicht mehr schützt.

```
protect stgpool pool1 purgedata=all
```

Beispiel: Einen Speicherpool schützen und eine maximale Anzahl Datensitzungen angeben

Schützen Sie einen Speicherpool mit dem Namen SPOOL1 auf dem Quellenserver, indem Sie die Daten auf dem Zielserver TPOOL1 sichern. Geben Sie maximal 20 Datensitzungen an.

```
update stgpool spool1 protectstgpool=tpool1
protect stgpool spool1 maxsessions=20
```

Beispiel: Die Speicherpooldaten auf Band kopieren

Schützen Sie einen Verzeichniscontainerspeicherpool, indem Sie die Daten in einen Containerkopienspeicherpool auf demselben Server kopieren. In diesem Beispiel hat der Verzeichniscontainerspeicherpool den Namen SPOOL1 und der Containerkopienspeicherpool, der Band für die Speicherung verwendet, den Namen TAPES1.

1. Aktualisieren Sie den Verzeichniscontainerspeicherpool, um TAPES1 als lokalen Speicherpool für den Schutz hinzuzufügen. Der Speicherpool TAPES1 muss ein Containerkopienspeicherpool sein. Geben Sie den folgenden Befehl aus:

   ```
   update stgpool spool1 protectlocalstgpools=tapes1
   ```

2. Schützen Sie die Daten in dem Verzeichniscontainerspeicherpool mit einer lokalen Kopie, indem Sie den folgenden Befehl ausgeben:

   ```
   protect stgpool type=local spool1
   ```

   Die Daten werden in den Speicherpool TAPES1 kopiert.

Beispiel: Speicherbereich auf Banddatenträgern vor dem Schutz eines Speicherpools konsolidieren

Konsolidieren Sie Speicherbereich auf den Banddatenträgern, die zum Schutz eines Verzeichniscontainerspeicherpools verwendet werden. Schützen Sie anschließend die Daten im Verzeichniscontainerspeicherpool. In diesem Beispiel hat der Verzeichniscontainerspeicherpool den Namen SPOOL1.

1. Konsolidieren Sie Speicherbereich im lokalen Containerkopienspeicherpool, der als Zielschutzpool für SPOOL1 definiert ist.

   ```
   protect stgpool spool1 type=local reclaim=only
   ```

2. Schützen Sie die Daten im Verzeichniscontainerspeicherpool namens SPOOL1, ohne eine Konsolidierung auszuführen.

   ```
   protect stgpool spool1 type=local reclaim=no
   ```

Tabelle 1. Zugehörige Befehle für PROTECT STGPOOL

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
DEFINE STGPOOL (Containerkopie)	Definiert einen Containerkopienspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden.
DEFINE STGPOOL (Verzeichniscontainer)	Definiert einen Verzeichniscontainerspeicherpool.
DEFINE STGPOOLDIRECTORY	Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.

Befehl	Beschreibung
REPAIR STGPOOL	Repariert einen Verzeichniscontainerspeicherpool.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
SET REPLSERVER	Gibt einen Zielreplikationsserver an.
UPDATE STGPOOL (Containerkopie)	Aktualisiert einen Containerkopienspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden.

QUERY-Befehle

Mit den QUERY-Befehlen können Informationen zu IBM Spectrum Protect-Objekten angefordert oder angezeigt werden.

- QUERY ACTLOG (Aktivitätenprotokoll abfragen)
- QUERY ADMIN (Administratorinformationen anzeigen)
- QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)
- QUERY ALERTSTATUS (Status eines Alert abfragen)
- QUERY ASSOCIATION (Zuordnung zwischen Clientknoten und Zeitplan abfragen)
- QUERY AUDITOCCUPANCY (Speicherauslastung des Clientknotens abfragen)
- QUERY BACKUPSET (Sicherungsgruppe abfragen)
- QUERY BACKUPSETCONTENTS (Inhalt einer Sicherungsgruppe abfragen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY CLEANUP (Bereinigung abfragen, die in einem Quellenspeicherpool erforderlich ist)
- QUERY CLOPTSET (Clientoptionsgruppe abfragen)
- QUERY COLLOCGROUP (Kollokationsgruppe abfragen)
- QUERY CONTENT (Inhalt eines Speicherpooldatenträgers abfragen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY CONTAINER (Container abfragen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY CONVERSION (Konvertierungsstatus eines Speicherpools abfragen)
- QUERY COPYGROUP (Kopiengruppen abfragen)
- QUERY DATAMOVER (Definitionen der Einheit zum Versetzen von Daten anzeigen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abfragen)
- QUERY DB (Datenbankinformationen anzeigen)
- QUERY DBSPACE (Datenbankspeicherbereich anzeigen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen)
- QUERY DEVCLASS (Informationen über Einheitenklassen anzeigen)
- QUERY DIRSPACE (Speichernutzung von FILE-Verzeichnissen abfragen)
- QUERY DOMAIN (Maßnahmendomäne abfragen)
- QUERY DRIVE (Informationen über ein Laufwerk abfragen)
- QUERY DRMEDIA (Fehlerbehebungsdatenträger abfragen)
- QUERY DRMSTATUS (Disaster Recovery Manager-Systemparameter abfragen)
- QUERY ENABLED (Aktivierte Ereignisse abfragen)
- QUERY EVENT (Geplante und abgeschlossene Ereignisse abfragen)
- QUERY EVENTRULES (Regeln für Server- oder Clientereignisse abfragen)
- QUERY EVENTSERVER (Ereignisserver abfragen)
- QUERY EXPORT (Aktive oder ausgesetzte Exportoperationen abfragen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)
- QUERY FILESPACE (Dateibereiche abfragen)
- QUERY LIBRARY (Kassettenarchiv abfragen)
- QUERY LIBVOLUME (Datenträger im Kassettenarchiv abfragen)
- QUERY LICENSE (Lizenzinformationen anzeigen)
- QUERY LOG (Informationen zum Wiederherstellungsprotokoll anzeigen)
- QUERY MACHINE (Maschineninformationen abfragen)
- QUERY MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff abfragen)
- QUERY MGMTCLASS (Verwaltungsklasse abfragen)
- QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)
- QUERY MONITORSTATUS (Überwachungsstatus abfragen)
- QUERY MOUNT (Informationen zu bereitgestellten Datenträgern mit sequenziellem Zugriff anzeigen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY NASBACKUP (NAS-Sicherungsimages abfragen)
- QUERY NODE (Knoten abfragen)
- QUERY NODEDATA (Clientdaten auf Datenträgern abfragen)
- QUERY NODEGROUP (Knotengruppe abfragen)
- QUERY OCCUPANCY (Clientdateibereiche in Speicherpools abfragen)

- QUERY OPTION (Serveroptionen abfragen)
- QUERY PATH (Pfaddefinition anzeigen)
- QUERY POLICYSET (Maßnahmengruppe abfragen)
- QUERY PROCESS (Serverprozesse abfragen)
- QUERY PROFILE (Profil abfragen)
- QUERY PROTECTSTATUS (Status des Speicherpoolschutzes abfragen)
- QUERY PROXYNODE (Proxyberechtigung für einen Clientknoten abfragen)
- QUERY PVUESTIMATE (Prozessor-Value-Unit-Schätzung anzeigen)
- QUERY RECOVERYMEDIA (Wiederherstellungsdatenträger abfragen)
- QUERY REPLICATION (Knotenreplikationsprozesse abfragen)
- QUERY REPLNODE (Informationen zum Replikationsstatus für einen Clientknoten anzeigen)
- QUERY REPLRULE (Replikationsregeln abfragen)
- QUERY REPLSERVER (Replikationsserver abfragen)
- QUERY REQUEST (Anstehende Ladeanforderungen abfragen)
- QUERY RESTORE (Wiederanlauffähige Zurückschreibungssitzungen abfragen)
- QUERY RPFCONTENT (Inhalt der auf Zielserver gespeicherten Plandatei abfragen)
- QUERY RPFILE (Auf Zielserver gespeicherte Infos über Plandateien abfragen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY SAN (Einheiten in dem SAN abfragen)
- QUERY SCHEDULE (Zeitpläne abfragen)
- QUERY SCRIPT (IBM Spectrum Protect-Prozeduren abfragen)
- QUERY SERVER (Server abfragen)
- QUERY SERVERGROUP (Servergruppe abfragen)
- QUERY SESSION (Clientsitzungen abfragen)
- QUERY SHREDSTATUS (Status für Schreddern abfragen)
- QUERY SPACETRIGGER (Speicherbereichsauslöser abfragen)
- QUERY STATUS (Systemparameter abfragen)
- QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)
- QUERY STGPOOL (Speicherpools abfragen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY STGPOOLDIRECTORY (Speicherpoolverzeichnis abfragen)
- QUERY SUBSCRIBER (Informationen zu Subskribenten anzeigen)
- QUERY SUBSCRIPTION (Subskriptionsinformationen anzeigen)
- QUERY SYSTEM (Systemkonfiguration und Kapazität abfragen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY TAPEALERTMSG (Status des Befehls SET TAPEALERTMSG anzeigen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeQUERY TOC (Inhaltsverzeichnis für ein Sicherungsimage anzeigen)
- QUERY VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs abfragen)
- QUERY VOLHISTORY (History-Daten für sequentielle Datenträger anzeigen)
- QUERY VOLUME (Speicherpooldatenträger abfragen)

QUERY ACTLOG (Aktivitätenprotokoll abfragen)

Mit diesem Befehl können Nachrichten angezeigt werden, die von dem Server und dem Client generiert wurden. Dieser Befehl stellt Filteroptionen bereit, mit denen die Anzahl der angezeigten Nachrichten und die Zeit begrenzt werden kann, die für die Verarbeitung dieser Abfrage benötigt wird. Werden keine Parameter in diesem Befehl angegeben, werden alle Nachrichten angezeigt, die in der vorhergehenden Stunde generiert wurden.

Das Aktivitätenprotokoll enthält alle Nachrichten, die bei normalem Betrieb an die Serverkonsole gesendet werden. Die Ergebnisse der Befehle, die an der Serverkonsole eingegeben werden, werden nicht im Aktivitätenprotokoll aufgezeichnet, es sei denn, der Befehl betrifft oder startet einen Hintergrundprozess oder eine Clientsitzung. Fehlernachrichten werden im Aktivitätenprotokoll angezeigt.

Einschränkung: Der Befehl QUERY ACTLOG kann nicht mit Hilfe des Befehls DEFINE SCHEDULE geplant werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                .-BEGINDate--=--aktuelles_Datum-.
>>-Query ACtlog--+-------------------------------+-------------->
                 '-BEGINDate--=--Datum-----------'

   .-BEGINTime--=--aktuelle_Uhrzeit_minus_1_Stunde-.
>--+--------------------------------------------+------------>
   '-BEGINTime--=--Zeit---------------------------'

   .-ENDDate--=--aktuelles_Datum-.
```

```
>--+----------------------------+----------------------------->
   '-ENDDate--=--Datum----------'

   .-ENDTime--=--aktuelle_Uhrzeit-.
>--+-------------------------------+---------------------------->
   '-ENDTime--=--Zeit-------------'

>--+----------------------------+----------------------------->
   '-MSGno--=--Nachrichtennummer-'

>--+-------------------------+--+-------------------------+----->
   '-Search--=--Zeichenfolge-'  '-NODEname--=--Knotenname-'

   .-ORiginator--=--ALL---------------.
>--+-----------------------------------+-----------------------><
   '-ORiginator--=--+-ALL-----------+-'
                    +-SErver--------+
                    '-CLient--| A |-'

A

|--+-------------------------+-------------------------------->
   '-OWNERname--=--Eignername-'

>--+----------------------------+----------------------------->
   '-SCHedname--=--Zeitplanname-'

>--+----------------------------+----------------------------->
   '-DOmainname--=--Domänenname-'

>--+----------------------------+-----------------------------|
   '-SESsnum--=--Sitzungsnummer-'
```

Parameter

BEGINDate

Gibt das Anfangsdatum des Bereichs an, für den Nachrichten angezeigt werden sollen. Es werden alle Nachrichten angezeigt, die die Zeitkriterien erfüllen und nach diesem Datum aufgetreten sind. Standardwert ist das aktuelle Datum. Dieser Parameter ist wahlfrei.
Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–7 *oder* –7. Sollen Informationen beginnend mit den Nachrichten angezeigt werden, die vor einer Woche erstellt wurden, kann BEGINDATE=TODAY-7 oder BEGINDATE= -7 angegeben werden.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt die Anfangszeit des Bereichs an, für den Nachrichten angezeigt werden sollen. Es werden alle Nachrichten angezeigt, die die Zeitkriterien erfüllen und nach dieser Uhrzeit aufgetreten sind. Wird keine Zeit angegeben, werden alle Nachrichten angezeigt, die in der letzten Stunde aufgetreten sind.
Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Anfangsdatum	10:30:08

Wert	Beschreibung	Beispiel
NOW	Die aktuelle Uhrzeit am angegebenen Anfangsdatum	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum	NOW+03:00 *oder* +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW+3 oder BEGINTIME=+3 ausgegeben, zeigt IBM Spectrum Protect Nachrichten mit der Uhrzeit 12:00 Uhr oder später am Anfangsdatum an.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum	NOW-04:00 *oder* -04:00. Wird der Befehl QUERY ACTLOG um 9:00 Uhr mit der Angabe BEGINTime=NOW-3:30 oder BEGINTime= -3:30 ausgegeben, zeigt IBM Spectrum Protect Nachrichten mit der Uhrzeit 5:30 Uhr oder später am Anfangsdatum an.

ENDDate

Gibt das Enddatum des Bereichs an, für den Nachrichten angezeigt werden sollen. Es werden alle Nachrichten angezeigt, die die Zeitkriterien erfüllen und vor dem Enddatum aufgetreten sind. Wird kein Wert angegeben, wird das aktuelle Datum verwendet. Dieser Parameter ist wahlfrei.

Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–1 *oder* –1. Sollen Informationen angezeigt werden, die bis gestern erstellt wurden, kann ENDDATE=TODAY-1 oder einfach ENDDATE= -1 angegeben werden.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDTime

Gibt die Endzeit des Bereichs an, für den Nachrichten angezeigt werden sollen. Es werden alle Nachrichten angezeigt, die die Zeitkriterien erfüllen und vor dieser Uhrzeit aufgetreten sind. Wird kein Wert angegeben, werden alle Nachrichten angezeigt, die bis zum Zeitpunkt der Ausgabe dieses Befehls aufgetreten sind. Dieser Parameter ist wahlfrei.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Enddatum	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Enddatum	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum	NOW+03:00 *oder* +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+3:00 oder ENDTIME= +3:00 ausgegeben, zeigt IBM Spectrum Protect Nachrichten mit der Uhrzeit 12:00 Uhr oder früher am angegebenen Enddatum an.

Wert	Beschreibung	Beispiel
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum	NOW-03:30 *oder* -03:30. Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME= -3:30 ausgegeben, zeigt IBM Spectrum Protect Nachrichten mit der Uhrzeit 5:30 Uhr oder früher am angegebenen Enddatum an.

MSGno
Gibt eine ganze Zahl an, die die Nachrichtennummer der aus dem Aktivitätenprotokoll anzuzeigenden Nachricht definiert. Diese ganze Zahl ist nur der numerische Teil der Nachricht. Dieser Parameter ist wahlfrei.

Search
Gibt eine Zeichenfolge an, nach der im Aktivitätenprotokoll gesucht werden soll. Die Zeichenfolge in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Sie können Text und ein Platzhalterzeichen verwenden, um diese Zeichenfolge anzugeben. Dieser Parameter ist wahlfrei.
Anmerkung: Geben Sie als Zeichenfolge nicht den IBM Spectrum Protect-Servernamen oder Text und ein Platzhalterzeichen an, mit dem der Servername gefunden würde. Die Ausgabe enthält sonst Nachrichten, die den Suchbegriff nicht enthalten.

NODEname
Gibt an, dass die Abfrage Nachrichten anzeigt, die für diesen Knoten protokolliert wurden. Wird kein Wert für diesen Parameter angegeben, werden Nachrichten für alle Knoten angezeigt.

ORiginator
Gibt an, dass die Abfrage Nachrichten anzeigt, die vom Server und/oder Client protokolliert wurden. Standardwert ist ALL. Gültige Werte:

ALL
Gibt an, dass die Abfrage Nachrichten anzeigt, die vom Client und vom Server stammen.

SErver
Gibt an, dass die Abfrage Nachrichten anzeigt, die vom Server stammen.

CLient
Gibt an, dass die Abfrage Nachrichten anzeigt, die vom Client stammen.
Es kann einer der folgenden Werte angegeben werden, um die Verarbeitungszeit zu minimieren, wenn das Aktivitätenprotokoll nach Nachrichten abgefragt wird, die vom Client protokolliert wurden:

OWNERname
Gibt an, dass die Abfrage Nachrichten anzeigt, die für einen bestimmten Eigner protokolliert wurden. Wird kein Wert für diesen Parameter angegeben, werden Nachrichten für alle Eigner angezeigt.

SCHedname
Gibt an, dass die Abfrage Nachrichten anzeigt, die für eine bestimmte geplante Clientaktivität protokolliert wurden. Wird kein Wert für diesen Parameter angegeben, werden Nachrichten für alle Zeitpläne angezeigt.

DOmainname
Gibt an, dass die Abfrage Nachrichten anzeigt, die für eine bestimmte Maßnahmendomäne protokolliert wurden, zu der ein angegebener Zeitplan gehört. Dieser Parameter ist wahlfrei, es sei denn, es wird ein Zeitplanname angegeben.

SESsnum
Gibt an, dass die Abfrage Nachrichten anzeigt, die aus einer bestimmten Clientsitzung protokolliert wurden. Wird kein Wert für diesen Parameter angegeben, werden Nachrichten für alle Clientsitzungen angezeigt.

Beispiel: Das Aktivitätenprotokoll nach Nachrichten mit bestimmtem Text durchsuchen

Das Aktivitätenprotokoll nach allen Nachrichten durchsuchen, die die Zeichenfolge "löschen" enthalten. Die Ausgabe schließt nur die Nachrichten mit ein, die während der letzten Stunde ausgegeben wurden. Den folgenden Befehl ausgeben:

```
query actlog search=löschen

Datum/Uhrzeit        Nachricht
-------------------- ----------------------------------------
08/27/1998 15:19:43  ANR0812I Verfallsprozess für Bestandsdateien
                      abgeschlossen: 0 Dateien wurden gelöscht.
```

Beispiel: Das Aktivitätenprotokoll nach Nachrichten innerhalb eines bestimmten Zeitrahmens durchsuchen

Nachrichten anzeigen, die gestern zwischen 9:30 Uhr und 12:30 Uhr aufgetreten sind. Den folgenden Befehl ausgeben:

```
query actlog begindate=today-1
begintime=09:30:00 endtime=12:30:00

Datum/Uhrzeit        Nachricht
-------------------- ----------------------------------------------
10/21/1998 10:52:36 ANR0407I Sitzung 3921 für Administrator ADMIN
                    gestartet (WebBrowser) (HTTP 9.115.20.100(2315)).
10/21/1998 11:06:08 ANR0405I Sitzung 3922 für Administrator ADMIN
                    beendet (WebBrowser).
```

```
10/21/1998 12:16:50 ANR0405I Sitzung 3934 für Administrator ADMIN
                    beendet (WebBrowser).
```

Beispiel: Das Aktivitätenprotokoll nach Nachrichten von einem bestimmten Clientknoten durchsuchen

Das Aktivitätenprotokoll nach IBM Spectrum Protect-Nachrichten vom Client für Knoten JEE durchsuchen. Den folgenden Befehl ausgeben:

```
query actlog originator=client node=jee
```

```
Datum/Uhrzeit        Nachricht
------------------- ----------------------------------------------
06/10/1998 15:46:22 ANE4007E (Sitzungsnummer: 3 Knoten: JEE) Fehler
                    beim Verarbeiten von '/jee/report.out': Zugriff
                    auf Objekt wird verweigert
06/11/1998 15:56:56 ANE4009E (Sitzungsnummer: 4 Knoten: JEE) Fehler
                    beim Verarbeiten von '/jee/work.lst': Platte
                    vollständig belegt.
```

Beispiel: Das Aktivitätenprotokoll nach Client- und Servernachrichten von einem bestimmten Clientknoten und einer bestimmten Sitzung durchsuchen

Das Aktivitätenprotokoll nach IBM Spectrum Protect-Nachrichten vom Client und Server für Knoten A, der der Sitzung 1 zugeordnet ist, durchsuchen. Die Ausgabe umfasst alle Nachrichten mit der definierten Zeichenfolge "SITZUNG: 1". Den folgenden Befehl ausgeben:

```
query actlog search="(SITZUNG:1)"
```

```
Datum/Uhrzeit        Nachricht
-------------------  ----------------------------------------------
02/13/2012 12:13:42    ANR0406I Sitzung 1 für Knoten A gestartet (WinNT)
                       (Tcp/Ip colind(2463)). (SITZUNG: 1)
02/13/2012 12:13:56  ANE4952I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
                       Gesamtzahl geprüfter Objekte:            34
                       (SITZUNG: 1)
02/13/2012 12:13:56  ANE4954I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
                       Gesamtzahl gesicherter Objekte:          34
                       (SITZUNG: 1)
02/13/2012 12:13:56  ANE4958I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
                       Gesamtzahl aktualisierter Objekte:        0
                       (SITZUNG: 1)
02/13/2012 12:13:56  ANE4964I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
                       Abgelaufene Verarbeitungszeit:     00:00:02
                       (SITZUNG: 1)
02/13/2012 12:13:59  ANR0403I Sitzung 1 für Knoten A beendet (WinNT).
                       (SITZUNG: 1)
```

Beispiel: Das Aktivitätenprotokoll nach Clientnachrichten aus einer Clientsitzung durchsuchen

Das Aktivitätenprotokoll nach IBM Spectrum Protect-Nachrichten aus einer bestimmten Clientsitzung durchsuchen. Die Ausgabe umfasst nur Nachrichten, die vom Client generiert wurden. Den folgenden Befehl ausgeben:

```
query actlog sessnum=1
```

```
Datum/Uhrzeit        Nachricht
-------------------  ----------------------------------------------
02/13/2012 12:13:56  ANE4952I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
                       Gesamtzahl geprüfter Objekte:            34
                       (SITZUNG: 1)
02/13/2012 12:13:56  ANE4954I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
                       Gesamtzahl gesicherter Objekte:          34
                       (SITZUNG: 1)
02/13/2012 12:13:56  ANE4958I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
                       Gesamtzahl aktualisierter Objekte:        0
                       (SITZUNG: 1)
02/13/2012 12:13:56  ANE4964I (ANE4985I Sitzung: 1, ANE4986I Knoten: A)
                       Abgelaufene Verarbeitungszeit:     00:00:02
                       (SITZUNG: 1)
```

Feldbeschreibungen

Datum/Uhrzeit
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die Nachricht vom Server oder Client generiert wurde.

Nachricht
: Gibt die Nachricht an, die vom Server oder Client generiert wurde.

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für QUERY ACTLOG

Befehl	Beschreibung
SET ACTLOGRETENTION	Gibt die Anzahl Tage an, die Protokollsätze im Aktivitätenprotokoll aufbewahrt werden sollen.

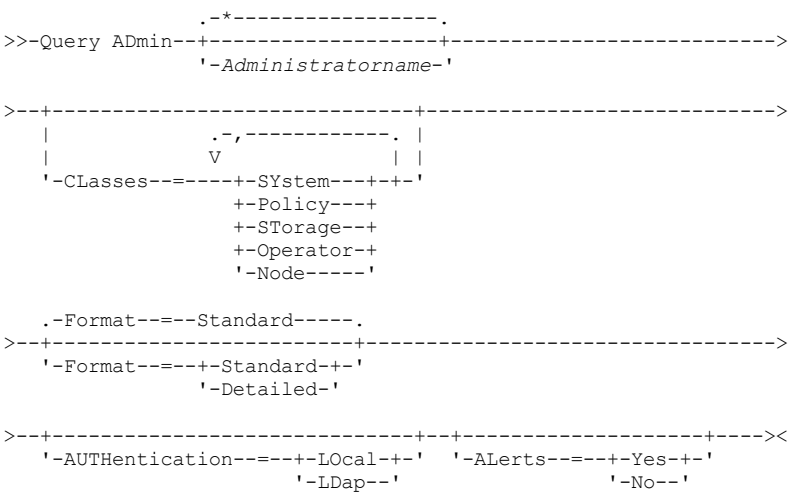
QUERY ADMIN (Administratorinformationen anzeigen)

Mit diesem Befehl können Informationen zu einem oder zu mehreren Administratoren angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Administratorname
: Gibt den Namen des Administrators an, für den Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird für diesen Parameter kein Wert angegeben, werden alle Administratoren angezeigt.

CLasses
: Gibt an, dass die Ausgabe auf Administratoren beschränkt werden soll, die über die angegebenen Berechtigungsklassen verfügen. Dieser Parameter ist wahlfrei. Es können mehrere Berechtigungsklassen in einer Liste angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, werden unabhängig von der Berechtigungsklasse Informationen zu allen Administratoren angezeigt. Gültige Werte:

  SYstem
  : Informationen über Administratoren mit Systemberechtigung anzeigen.

  Policy
  : Informationen über Administratoren mit Maßnahmenberechtigung anzeigen.

  STorage
  : Informationen über Administratoren mit Speicherberechtigung anzeigen.

  Operator
  : Informationen über Administratoren mit Bedienerberechtigung anzeigen.

  Node
  : Informationen über Benutzer mit Client-Knotenberechtigung anzeigen.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen für die angegebenen Administratoren angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen für die angegebenen Administratoren angezeigt werden.

Authentication
: Gibt die Kennwortauthentifizierungsmethode für den Administrator an.

LOcal
: Zeigt die Administratoren an, die sich mit dem IBM Spectrum Protect-Server authentifizieren.

LDap
: Zeigt die Administratoren an, die sich mit einem LDAP-Verzeichnisserver authentifizieren. Bei dem Administratorkennwort muss die Groß-/Kleinschreibung beachtet werden.

ALert
: Gibt an, ob Alerts an die E-Mail-Adresse eines Administrators gesendet werden.

Yes
: Gibt an, dass Alerts an die E-Mail-Adresse des angegebenen Administrators gesendet werden.

No
: Gibt an, dass Alerts nicht an die E-Mail-Adresse des angegebenen Administrators gesendet werden. Dies ist der Standardwert.

Tipp: Die Alertüberwachung muss aktiviert sein und die E-Mail-Einstellungen müssen korrekt definiert sein, damit Alerts erfolgreich als E-Mail empfangen werden können. Um die aktuellen Einstellungen anzuzeigen, geben Sie den Befehl QUERY MONITORSETTINGS aus.

Beispiel: Informationen zu allen Administratoren anzeigen

Teilinformationen zu allen Administratoren anzeigen. Den folgenden Befehl ausgeben:

```
query admin
```

```
Administrator- Tage seit     Tage seit  Gesperrt   Berechtigungsklasse
name           ltzt. Zugriff Kennwort-
                                 vergabe
-------------  ------------  ----------  ---------  ------------------
ADMIN                 <1        <1       No     System
SERVER_CONSOLE                                No     System
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Vollständige Informationen zu einem Administrator anzeigen

Von einem verwalteten Server aus vollständige Informationen für den Administrator ADMIN anzeigen. Den folgenden Befehl ausgeben:

```
query admin admin format=detailed
```

```
                      Administratorname: ADMIN
                      Letzter Zugriff: 1998.06.04 17.10.52
           Tage seit letztem Zugriff: <1
         Datum/Zeit der Kennwortvergabe: 1998.06.04 17.10.52
           Tage seit Kennwortvergabe: 26
     Zahl der ungültigen Anmeldeversuche: 0
                           Gesperrt?: No
                 Kontaktinformationen:
                   Systemberechtigung: Yes
                Maßnahmenberechtigung: **Enthalten in Systemberechtigung.**
                 Speicherberechtigung: **Enthalten in Systemberechtigung.**
                 Bedienerberechtigung: **Enthalten in Systemberechtigung.**
            Client-Zugriffsberechtigung: **Enthalten in Systemberechtigung.**
              Client-Eignerberechtigung: **Enthalten in Systemberechtigung.**
                        Registriert am: 05/09/1998 23:54:20
                    Registriert durch: SERVER_CONSOLE
                  Verwaltendes Profil:
                  Kennwortablaufdauer: 90 Tag(e)
                       E-Mail-Adresse:
             Alerts als E-Mail senden: Yes
                    Authentifizierung: Local
                     SSL erforderlich: No
         Sitzungssicherheit: Strict
                    Transportmethode: TLS 1.2
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Administratorname
: Gibt den Namen des Administrators an.

Letzter Zugriff
: Gibt an, wann der Administrator zuletzt auf den Server zugegriffen hat (Datum und Uhrzeit).

Tage seit letztem Zugriff
: Gibt die Anzahl Tage seit des letzten Zugriffs des Administrators auf den Server an.

Datum/Zeit der Kennwortvergabe
: Gibt an, wann das Kennwort des Administrators definiert bzw. zuletzt aktualisiert wurde (Datum und Uhrzeit).

Tage seit Kennwortvergabe

Gibt die Anzahl Tage seit der Definition oder der letzten Aktualisierung des Administratorkennworts an.

Zahl der ungültigen Anmeldeversuche

Gibt die Anzahl der ungültigen Anmeldeversuche an, die seit der letzten erfolgreichen Anmeldung unternommen wurden. Diese Anzahl kann nur ungleich Null sein, wenn das Limit für ungültige Kennworteingaben (SET INVALIDPWLIMIT) größer Null ist. Entspricht die Anzahl der ungültigen Versuche dem durch den Befehl SET INVALIDPWLIMIT definierten Limit, wird der betreffende Administrator gesperrt.

Gesperrt?

Gibt an, ob der Administrator für das System gesperrt ist.

Kontaktinformationen

Gibt Kontaktinformationen für den Administrator an.

Systemberechtigung

Gibt an, ob dem Administrator Systemberechtigung erteilt wurde.

Maßnahmenberechtigung

Gibt an, ob dem Administrator uneingeschränkte Maßnahmenberechtigung erteilt wurde, oder gibt die Namen der Maßnahmendomänen an, die der Administrator mit eingeschränkter Maßnahmenberechtigung verwalten kann.

Speicherberechtigung

Gibt an, ob dem Administrator uneingeschränkte Speicherberechtigung erteilt wurde, oder gibt die Namen der Speicherpools an, die der Administrator mit eingeschränkter Speicherberechtigung verwalten kann.

Bedienerberechtigung

Gibt an, ob dem Administrator Bedienerberechtigung erteilt wurde.

Clientzugriffsberechtigung

Gibt an, dass einem Benutzer mit Knotenberechtigung Clientzugriffsberechtigung erteilt wurde.

Clienteignerberechtigung

Gibt an, dass einem Benutzer mit Knotenberechtigung Clienteignerberechtigung erteilt wurde.

Registriert am

Gibt an, wann der Administrator registriert wurde (Datum und Uhrzeit).

Registriert durch

Gibt den Namen des Administrators an, der den Administrator registriert hat. Enthält dieses Feld $$CONFIG_MANAGER$$, ist der Administrator einem Profil zugeordnet, das von dem Konfigurationsmanager verwaltet wird.

Verwaltendes Profil

Gibt die Profile an, für die der verwaltete Server subskribiert hat, um die Definition dieses Administrators zu erhalten.

Kennwortablaufdauer

Gibt die Ablaufdauer des Administratorkennworts an.

E-Mail-Adresse

Gibt die E-Mail-Adresse für den Administrator an.

Alerts als E-Mail senden

Gibt an, ob Alerts als E-Mail an den angegebenen Administrator gesendet werden.

Authentifizierung

Gibt die Kennwortauthentifizierungsmethode an: LOCAL, LDAP oder LDAP (künftig).

Authentifizierungsziel	**Authentifizierungsmethode**
IBM Spectrum Protect-Server	LOCAL
LDAP-Verzeichnisserver	LDAP
Dieser Administrator ist für die Authentifizierung mit einem LDAP-Verzeichnisserver konfiguriert, aber der Administrator hat sich noch nicht über einen Clientknoten authentifiziert.	LDAP (künftig)

SSL erforderlich (veraltet)

Gibt an, ob die Sicherheitseinstellung für die Administrator-ID das Protokoll Secure Sockets Layer (SSL) erfordert. Die gültigen Werte sind YES, NO oder Default. Sie müssen über die Berechtigung auf Systemebene verfügen, um die Einstellung von SSLREQUIRED für den Administrator zu aktualisieren. Dieser Parameter wird nicht mehr verwendet.

Sitzungssicherheit

Gibt die Stufe der Sitzungssicherheit an, die für die Administrator-ID durchgesetzt wird. Die gültigen Werte sind STRICT und TRANSITIONAL.

Transportmethode

Gibt die Transportmethode an, die zuletzt für den angegebenen Administrator verwendet wurde. Die gültigen Werte sind TLS 1.2, TLS 1.1 und NONE. Ein Fragezeichen (?) wird angezeigt, bis eine erfolgreiche Authentifizierung ausgeführt wird.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ADMIN

Befehl	**Beschreibung**
GRANT AUTHORITY	Ordnet einem Administrator Berechtigungsklassen zu.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER ADMIN	Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.
REMOVE ADMIN	Löscht einen Administrator aus der Liste der registrierten Administratoren.
RENAME ADMIN	Ändert den Namen eines IBM Spectrum Protect-Administrators.
RESET PASSEXP	Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.
REVOKE AUTHORITY	Widerruft eine oder mehrere Berechtigungsklassen oder schränkt den Zugriff auf Maßnahmendomänen und Speicherpools ein.
SET INVALIDPWLIMIT	Definiert die Anzahl ungültiger Anmeldeversuche, die zulässig sind, bevor ein Knoten gesperrt wird.
SET MINPWLENGTH	Legt die Mindestlänge für Clientkennwörter fest.
SET PASSEXP	Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.

QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)

Verwenden Sie diesen Befehl, um die Servernachrichten anzuzeigen, die als Alerts definiert sind.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                        .-*---------------------.
>>-Query ALERTTrigger--+-----------------------+---------------><
                        '---Nachrichtennummer---'
```

Parameter

Nachrichtennummer
: Gibt die Nachrichtennummer an, die abgefragt werden soll. Geben Sie mehrere Nachrichtennummern durch Kommas getrennt und ohne Leerzeichen an. Nachrichtennummern haben eine maximale Länge von acht Zeichen. Platzhalterzeichen können verwendet werden, um Nachrichtennummern anzugeben. Wenn Sie keine Nachrichtennummer angeben, werden alle Alertauslöser angezeigt.

Alertauslöser abfragen, um die Nachrichten anzuzeigen, die als Alerts angegeben sind

Mit dem folgenden Befehl alle Nachrichten anzeigen, die als Alerts angegeben sind:

```
query alerttrigger
```

Beispielausgabe:

```
Alertauslöser        Kategorie      Administrator
--------------       ---------      -------------------------------
ANR1067E              SERVER         HARRYH
ANR1073E              SERVER         CSDADMIN,DJADMIN,HARRYH
ANR1074E              STORAGE        CSDADMIN,DJADMIN,HARRYH
ANR1096E              STORAGE        CSDADMIN,DJADMIN,HARRYH,MHAYE
```

Alertauslöser nach einer bestimmten Nachrichtennummer abfragen

Den folgenden Befehl ausgeben, um alle Alertauslöser anzuzeigen, für die die Nachrichtennummer ANR1067E angegeben ist:

```
query alerttrigger ANR1067E
```

Beispielausgabe:

```
Alertauslöser        Kategorie      Administrator
--------------       ---------      -------------
```

```
ANR1067E              SERVER         HARRYH
```

Feldbeschreibungen

Alertauslöser
: Die Nachrichtennummer für den Alertauslöser.

Kategorie
: Die Kategorie des Alertauslösers.

Administrator
: Der Name des Administrators, der Alerts von diesem Alertauslöser empfängt.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ALERTTRIGGER

Befehl	Beschreibung
DEFINE ALERTTRIGGER (Alertauslöser definieren)	Ordnet angegebene Nachrichten einem Alertauslöser zu.
DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)	Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.
QUERY ALERTSTATUS (Status eines Alert abfragen)	Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.
UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)	Aktualisiert die Attribute eines oder mehrerer Alertauslöser.
UPDATE ALERTSTATUS (Status eines Alert aktualisieren)	Aktualisiert den Status eines zurückgemeldeten Alert.

QUERY ALERTSTATUS (Status eines Alert abfragen)

Mit diesem Befehl können Informationen zu Alerts angezeigt werden, die auf dem IBM Spectrum Protect-Server zurückgemeldet werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

Parameter

Status

Gibt den Statustyp an, der angezeigt werden soll. Wenn Sie keinen Status angeben, werden alle Alerts abgefragt und angezeigt. Geben Sie einen der folgenden Werte an:

ACtive
: Zeigt Alerts an, die in der IBM Spectrum Protect-Serverdatenbank als aktiv angegeben sind.

INactive
: Zeigt Alerts an, die sich im Status 'inaktiv' befinden.

CLosed
: Zeigt Alerts an, die sich im Status 'geschlossen' befinden.

ANy
: Zeigt alle Alerts unabhängig vom Status an.

MSGnum
: Gibt die Nachrichtennummer an, die angezeigt werden soll. Geben Sie den numerischen Teil einer IBM Spectrum Protect-Servernachricht an. Die Werte liegen im Bereich von 0 bis 9999. Beispielsweise lautet die Nachrichtennummer in Nachricht ANR2044E 2044. Mehrere Nachrichtennummern können angegeben werden, indem sie ohne Leerzeichen durch Kommas voneinander getrennt werden.

CATegory
: Gibt den Kategorietyp für den Alert an, der durch die Nachrichtentypen bestimmt wird. Geben Sie einen der folgenden Werte an:

APplication
: Der Alert wird als Anwendungskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Anwendungsclients (TDP) zugeordnet sind.

INventory
: Der Alert wird als Bestandskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die der Datenbank, der aktiven Protokolldatei oder der Archivprotokolldatei zugeordnet sind.
Anmerkung: Die Kategorie `CAtalog` wird anstelle von `INventory` in Alerts von Servern verwendet, für die kein Upgrade auf IBM Spectrum Protect 7.1.0 oder höher durchgeführt wurde.

CLient
: Der Alert wird als Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Clientaktivitäten zugeordnet sind.

DEvice
: Der Alert wird als Einheitenkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Einheitenklassen, Kassettenarchiven, Laufwerken oder Pfaden zugeordnet sind.

SErver
: Der Alert wird als allgemeine Serverkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Serveraktivitäten oder -ereignissen zugeordnet sind.

STorage
: Der Alert wird als Speicherkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Speicherpools zugeordnet sind.

SYstems
: Der Alert wird als Systemclientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Systemsicherungs- und -archivierungsclients oder HSM-Clients zugeordnet sind.

VMclient
: Der Alert wird als VM-Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die VM-Clients zugeordnet sind.

SOURCEType
: Gibt den Quellentyp an, der abgefragt wird. Geben Sie einen der folgenden Werte an:

LOcal
: Zeigt Alerts an, die von dem lokalen IBM Spectrum Protect-Server stammen.

CLient
: Zeigt Alerts an, die von dem IBM Spectrum Protect-Client stammen.

REmote
: Zeigt Alerts an, die von einem anderen IBM Spectrum Protect-Server stammen.

SOURCEName
: Gibt den Namen der Quelle an, von der der Alert stammt. SOURCENAME kann der Name eines lokalen oder fernen IBM Spectrum Protect-Servers oder eines IBM Spectrum Protect-Clients sein.

ID
: Dieser optionale Parameter gibt die eindeutige ID des Alert an, der angezeigt werden soll. Geben Sie einen Wert von 1 bis 9223372036854775807 an.

ASSigned
: Gibt den Namen des Administrators an, dem der Alert zugeordnet ist, der abgefragt werden soll.

RESolvedby
: Gibt den Namen des Administrators an, der den Alert behoben hat, der abgefragt werden soll.

Aktive Alerts abfragen

Den folgenden Befehl ausgeben, um nur Alerts anzuzeigen, die in der Serverdatenbank aktiv sind:

```
query alertstatus status=active
```

Aktive Alerts für zwei Nachrichten abfragen, die vom lokalen Server ausgegeben wurden

Den folgenden Befehl ausgeben, um nur aktive Alerts für die Nachrichtennummern ANE4958I und ANR4952E anzuzeigen, die vom lokalen Server ausgegeben wurden:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=local
```

Aktive Alerts für die Nachrichten ANR4958I und ANR4952E abfragen, die von einem Client ausgegeben wurden

Den folgenden Befehl ausgeben, um nur aktive Alerts für die Nachrichtennummern ANE4958I und ANE4952I anzuzeigen, die von einem Client ausgegeben wurden:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=client
```

Alle Alerts auf einem Server abfragen

Den folgenden Befehl ausgeben, um alle Alerts auf dem Server anzuzeigen:

```
query alertstatus
```

Beispielausgabe: Alle Alerts auf dem Server anzeigen

```
               Alert-ID: 83
  Alertnachrichtennummer: 293
            Quellenname: SEDONA
             Quellentyp: LOCAL
       Erstes Auftreten: 03/07/2013 17:08:35
      Letztes Auftreten: 03/07/2013 17:08:35
                 Anzahl: 1
                 Status: ACTIVE
   Letzte Statusänderung: 12/31/1969 17:00:00
              Kategorie: INVENTORY
              Nachricht: ANR0293I Reorganisation für Tabelle AF_BITFILES gestartet.
             Zugeordnet:
            Behoben von:
              Anmerkung:

               Alert-ID: 85
  Alertnachrichtennummer: 293
            Quellenname: SEDONA
             Quellentyp: LOCAL
       Erstes Auftreten: 03/08/2013 05:45:00
      Letztes Auftreten: 03/08/2013 05:45:00
                 Anzahl: 1
                 Status: ACTIVE
   Letzte Statusänderung: 12/31/1969 17:00:00
              Kategorie: INVENTORY
              Nachricht: ANR0293I Reorganisation für Tabelle BF_AGGREGATED_BITFILES gestartet.
             Zugeordnet:
            Behoben von:
              Anmerkung:

               Alert-ID: 1282
  Alertnachrichtennummer: 293
            Quellenname: ALPINE
             Quellentyp: LOCAL
       Erstes Auftreten: 02/13/2013 15:47:50
      Letztes Auftreten: 02/13/2013 15:47:50
                 Anzahl: 1
                 Status: CLOSED
   Letzte Statusänderung: 02/26/2013 09:46:39
              Kategorie: INVENTORY
              Nachricht: ANR0293I Reorganisation für Tabelle TSMMON_ALERT gestartet.
             Zugeordnet:
            Behoben von:
              Anmerkung:


               Alert-ID: 1792
  Alertnachrichtennummer: 293
            Quellenname: ALPINE
             Quellentyp: LOCAL
       Erstes Auftreten: 02/19/2013 08:58:14
      Letztes Auftreten: 02/19/2013 08:58:14
                 Anzahl: 1
                 Status: CLOSED
```

```
Letzte Statusänderung: 03/01/2013 12:39:21
            Kategorie: INVENTORY
            Nachricht: ANR0293I Reorganisation für Tabelle ACTIVITY_LOG gestartet.
           Zugeordnet:
         Behoben von:
            Anmerkung:
```

Feldbeschreibungen

Alert-ID
: Die eindeutige ID für den Alert.

Alertnachrichtennummer
: Die Nachrichtennummer für den Alert.

Quellenname
: Der Name der Quelle, aus der der Alert stammte.

Quellentyp
: Der Typ dieser Quelle.

Erstes Auftreten
: Der Zeitpunkt (Datum und Uhrzeit), an dem der Alert erstmalig aufgetreten ist.

Letztes Auftreten
: Der Zeitpunkt (Datum und Uhrzeit), an dem der Alert zum letzten Mal aufgetreten ist.

Anzahl
: Gibt an, wie häufig der Alert insgesamt ausgelöst wurde.

Status
: Gibt den Status des Alerts an.

Letzte Statusänderung
: Gibt den Zeitpunkt (Uhrzeit und Datum) an, an dem der Status für den Alert zuletzt geändert wurde.

Kategorie
: Die Kategorie für den Alert.

Nachricht
: Die Nachricht, die den Alert auslöst.

Zugeordnet
: Gibt den Benutzer an, den dieser Alert betrifft.

Behoben von
: Gibt den Benutzer an, der den Alert überprüft und behoben hat.

Anmerkung
: Eine optional vom Auflöser hinterlassene Anmerkung.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ALERTSTATUS

Befehl	Beschreibung
DEFINE ALERTTRIGGER (Alertauslöser definieren)	Ordnet angegebene Nachrichten einem Alertauslöser zu.
DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)	Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.
QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)	Zeigt Nachrichtennummern an, die einen Alert auslösen.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)	Aktualisiert die Attribute eines oder mehrerer Alertauslöser.
UPDATE ALERTSTATUS (Status eines Alert aktualisieren)	Aktualisiert den Status eines zurückgemeldeten Alert.

QUERY ASSOCIATION (Zuordnung zwischen Clientknoten und Zeitplan abfragen)

Mit diesem Befehl können Informationen darüber angezeigt werden, welche Clientknoten einem oder mehreren Zeitplänen zugeordnet sind. Clientknoten, die einem Zeitplan zugeordnet sind, führen Operationen wie Sichern oder Archivieren gemäß diesem Zeitplan aus.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                        .-*--*--------------------------.
>>-Query ASSOCiation--+-------------------------------+--------><
```

```
|              .-*------------. |
'-Domänenname--+--------------+-'
               '-Zeitplanname-'
```

Parameter

Domänenname
: Gibt den Namen der Maßnahmendomäne an, die angezeigt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.Alle übereinstimmenden Maßnahmendomänennamen werden angezeigt. Wird kein Wert für diesen Parameter angegeben, werden alle vorhandenen Maßnahmendomänen abgefragt. Wird ein Domänenname angegeben, ist kein Zeitplanname erforderlich.

Zeitplanname
: Gibt den Namen des Zeitplans an, der angezeigt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.Alle übereinstimmenden Zeitplannamen werden angezeigt. Wird kein Wert für diesen Parameter angegeben, werden alle vorhandenen Zeitpläne abgefragt. Wird ein Zeitplanname angegeben, ist gleichzeitig auch ein Domänenname erforderlich.

Beispiel: Clientknoten anzeigen, die einem Zeitplan zugeordnet sind

Alle Client-Knoten anzeigen, die allen Zeitplänen zugeordnet sind, die zu der Maßnahmendomäne EMPLOYEE_RECORDS gehören. Den folgenden Befehl ausgeben:

```
query association employee_records *
```

```
           Name der Maßnahmendomäne: EMPLOYEE_RECORDS
            Zeitplanname: WEEKLY_BACKUP
      Zugeordnete Knoten: JOE JOHNSON LARRY SMITH SMITHERS TOM
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Name der Maßnahmendomäne
: Gibt den Namen der Maßnahmendomäne an, zu der der Zeitplan gehört.

Zeitplanname
: Gibt den Namen des Zeitplans an.

Zugeordnete Knoten
: Gibt die Namen der Client-Knoten an, die dem angegebenen Zeitplan zugeordnet sind.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ASSOCIATION

Befehl	Beschreibung
DEFINE ASSOCIATION	Ordnet Clients einem Zeitplan zu.
DELETE ASSOCIATION	Löscht die Zuordnung zwischen Clients und einem Zeitplan.

QUERY AUDITOCCUPANCY (Speicherauslastung des Clientknotens abfragen)

Mit diesem Befehl können Informationen über die Server-Speicherauslastung des Client-Knotens angezeigt werden. Sollen aktuelle Lizenzprüfungsinformationen vom Server angezeigt werden, den Befehl AUDIT LICENSE verwenden, bevor der Befehl QUERY AUDITOCCUPANCY ausgegeben wird.

Als Teil einer Lizenzprüfung berechnet der Server den Umfang des belegten Sicherungs-, Archivierungs- und Speicherverwaltungsspeichers nach Knoten. Bei Servern, die umfangreiche Datenmengen verwalten, kann diese Berechnung sehr viel Prozessorzeit beanspruchen und andere Serveraktivitäten blockieren. Mit der Serveroption AUDITSTORAGE kann angegeben werden, dass bei der Lizenzprüfung der Speicher nicht berechnet werden soll.

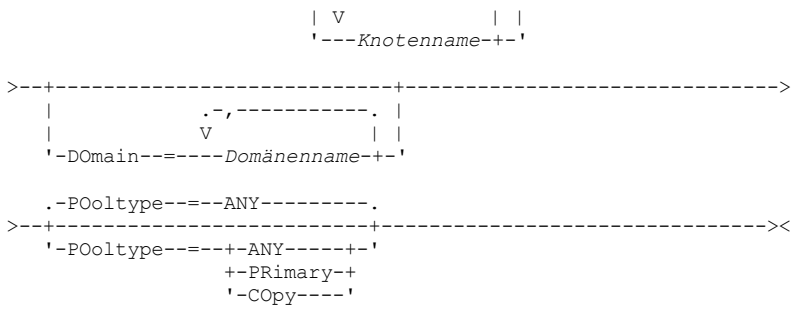
Mit Hilfe der Informationen aus dieser Abfrage kann festgestellt werden, ob und wo die Speicherauslastung des Clientknotens ausgeglichen werden muss. Diese Informationen können auch für die Berechnung der Speicherbelegungskosten für Clients verwendet werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query AUDITOccupancy--+----------------+---------------------->
                         | .-,----------. |
```



Parameter

Knotenname
: Gibt eine Liste der Knoten an, für die Informationen über die Serverspeicherbelegung angezeigt werden sollen. Es können mehrere Knoten angegeben werden, indem die Knotennamen ohne Leerzeichen durch Kommas voneinander getrennt werden. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Standardmäßig (*) werden alle Clientknoten abgefragt. Verwenden Sie den Parameter DOMAIN, um diese Liste nach Maßnahmendomäne einzugrenzen. Dieser Parameter ist wahlfrei.

DOmain
: Gibt eine Liste mit Maßnahmendomänen an, die die Anzeige von Knoten einschränken soll. Knoten, die zu den angegebenen Maßnahmendomänen gehören, werden angezeigt. Es können mehrere Maßnahmendomänen angegeben werden, indem die Namen der Maßnahmendomänen ohne Leerzeichen durch Kommas voneinander getrennt werden. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei.

POoltype
: Gibt den Typ des Speicherpools an, der angezeigt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Gültige Werte:

  ANY
  : Gibt primäre Speicherpools und Kopienspeicherpools an. Der angezeigte Wert gibt die Summe beider Pools an.

  PRimary
  : Gibt nur primäre Speicherpools an.

  COpy
  : Gibt nur Kopienspeicherpools an.

Beispiel: Speicherbelegung anzeigen

Die kombinierte Speicherbelegung in primären Speicherpools und Kopienspeicherpools anzeigen. Den folgenden Befehl ausgeben:

```
query auditoccupancy
```

```
Lizenzinformationen
z. Zt. der letzten Prüfung 05/22/1996 14:49:51.
```

Knotenname	Belegter Sicherungs-speicher (MB)	Belegter Archivierungs-speicher (MB)	Belegter Speicherver-waltungs-speicher (MB)	Belegter Gesamt-speicher (MB)
CLIENT	245	20	0	265
SMITH	245	20	0	265
SMITHERS	245	20	0	265
JOHNSON	300	15	0	320
JOE	245	20	0	265
TOM	300	15	0	320
LARRY	245	20	0	265

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Knotenname
: Gibt den Namen des Clientknotens an.

Belegter Sicherungsspeicher (MB)
: Gibt die gesamte Sicherungsspeicherbelegung des Knotens an. Bei diesem Wert ist ein MB = 1048576 Byte.

Belegter Archivierungsspeicher (MB)
: Gibt die gesamte Archivierungsspeicherbelegung des Knotens an. Bei diesem Wert ist ein MB = 1048576 Byte.

Belegter Speicherverwaltungsspeicher (MB)
: Gibt die Größe des Serverspeichers an, der zum Speichern von Dateien verwendet wird, die von einem IBM Spectrum Protect for Space Management-Client aus dem Clientknoten umgelagert werden. Bei diesem Wert ist ein MB = 1048576 Byte.

Belegter Gesamtspeicher (MB)
: Gibt die gesamte Speicherbelegung des Knotens an. Bei diesem Wert ist ein MB = 1048576 Byte.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY AUDITOCCUPANCY

Befehl	Beschreibung
AUDIT LICENSES	Prüft die Einhaltung der definierten Lizenzen.
QUERY LICENSE	Zeigt Informationen über Lizenzen und Prüfvorgänge an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER LICENSE	Registriert eine Lizenz für den IBM Spectrum Protect-Server.
SET LICENSEAUDITPERIOD	Gibt die Anzahl Tage zwischen den automatischen Lizenzprüfungen an.

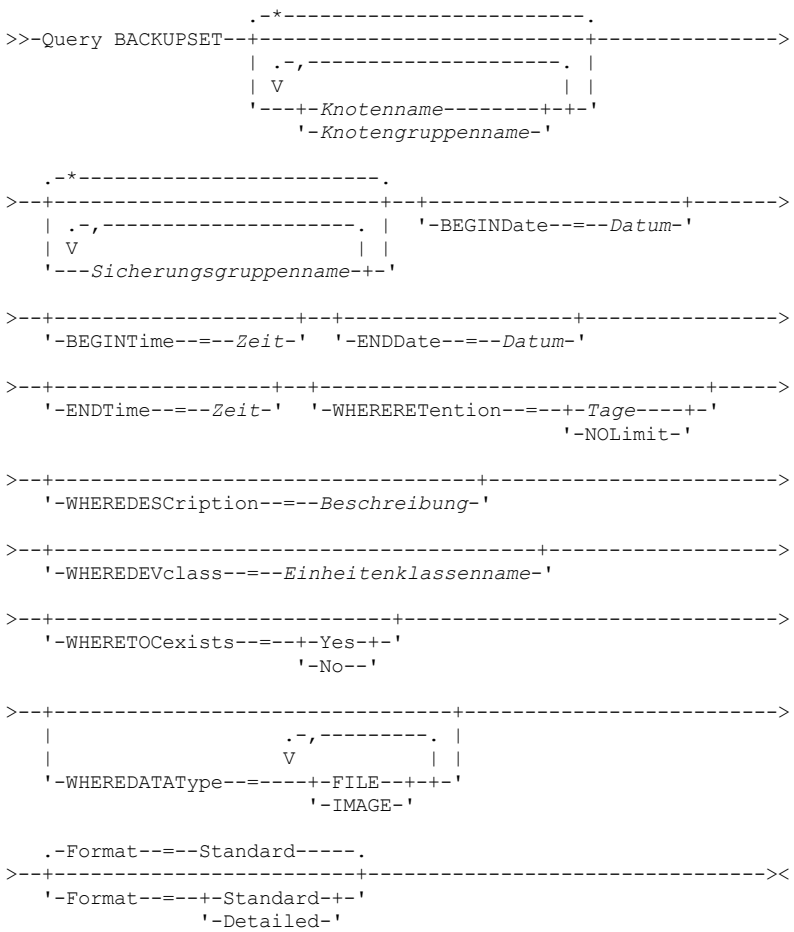
QUERY BACKUPSET (Sicherungsgruppe abfragen)

Mit diesem Befehl können Informationen über eine oder mehrere Sicherungsgruppen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Knotenname oder Knotengruppenname
: Gibt den Namen des Clientknotens und der Knotengruppen an, dessen bzw. deren Daten in der Sicherungsgruppe enthalten sind, die angezeigt werden soll. Sollen mehrere Knotennamen und Knotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen für Knotennamen, aber nicht für Knotengruppennamen verwenden.

Sicherungsgruppenname

Gibt den Namen der Sicherungsgruppe an, deren Informationen angezeigt werden sollen. Der angegebene Sicherungsgruppenname kann Platzhalterzeichen enthalten. Es können mehrere Sicherungsgruppennamen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

BEGINDate

Gibt das Anfangsdatum des Bereichs an, in den das zeitpunktgesteuerte Datum der Sicherungsgruppe, die angezeigt werden soll, fallen muss. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Anfangsdatum ohne eine Anfangszeit angegeben, lautet die Zeit 24:00 (Mitternacht) an dem angegebenen Datum.

Sie können das Datum mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1999
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage *oder* +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage.	TODAY +3 *oder* +3.
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage.	TODAY -3 *oder* -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt die Anfangszeit des Bereichs an, in den das zeitpunktgesteuerte Datum der Sicherungsgruppe, die angezeigt werden soll, fallen muss. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Anfangszeit ohne ein Anfangsdatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Uhrzeit.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten	NOW+02:00 *oder* +02:00.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW-02:00 *oder* –02:00.

ENDDate

Gibt das Enddatum des Bereichs an, in den das zeitpunktgesteuerte Datum der Sicherungsgruppe, die angezeigt werden soll, fallen muss. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDTIME verwendet werden, um ein Enddatum und eine Endzeit anzugeben. Wird ein Enddatum ohne eine Endzeit angegeben, lautet die Zeit 23:59:59 am angegebenen Enddatum.

Sie können das Datum mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1999
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage *oder* +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY +3 *oder* +3.
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage.	TODAY -3 *oder* -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM

Wert	Beschreibung	Beispiel
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDTime
Gibt die Endzeit des Bereichs an, in den das zeitpunktgesteuerte Datum der Sicherungsgruppe, die angezeigt werden soll, fallen muss. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDDATE verwendet werden, um ein Datum und eine Uhrzeit anzugeben. Wird eine Endzeit ohne ein Enddatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Zeit.
Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten	NOW+02:00 *oder* +02:00.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW-02:00 *oder* –02:00.

WHERERETention
Gibt den Aufbewahrungszeitraum in Tagen an, der den Sicherungsgruppen zugeordnet sein muss, die angezeigt werden sollen. Sie können eine ganze Zahl von 0 bis 30000 angeben. Gültige Werte:

Tage
Gibt an, dass Sicherungsgruppen, die diese Anzahl Tage aufbewahrt werden, angezeigt werden.
NOLimit
Gibt an, dass Sicherungsgruppen, die unbegrenzt aufbewahrt werden, angezeigt werden.

WHEREDESCription
Gibt die Beschreibung an, die der Sicherungsgruppe zugeordnet sein muss, die angezeigt werden soll. Die angegebene Beschreibung kann Platzhalterzeichen enthalten. Dieser Parameter ist wahlfrei. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.
WHEREDEVclass
Gibt den Namen der Einheitenklasse an, die der Sicherungsgruppe zugeordnet sein muss, die angezeigt werden soll. Es können Platzhalterzeichen verwendet werden, um einen Einheitenklassennamen anzugeben. Dieser Parameter ist wahlfrei.
WHERETOCexists
Gibt an, ob eine Sicherungsgruppe ein Inhaltsverzeichnis haben muss, damit sie angezeigt wird. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass alle Sicherungsgruppen angezeigt werden sollen, unabhängig davon, ob sie ein Inhaltsverzeichnis haben.
WHEREDATAType
Gibt den Datentyp einer Sicherungsgruppe an, der angezeigt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass alle Typen von Sicherungsgruppen angezeigt werden sollen. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden.

FILE
Gibt an, dass eine Sicherungsgruppe auf Dateiebene angezeigt werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Client für Sichern/Archivieren gesichert wurden.
IMAGE
Gibt an, dass eine Imagesicherungsgruppe angezeigt werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Clients für Sichern/Archivieren erstellt wurden.

Format
Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard
Gibt an, dass Teilinformationen für die angegebenen Sicherungsgruppen angezeigt werden.
Detailed
Gibt an, dass die gesamten Informationen für die angegebenen Sicherungsgruppen angezeigt werden.

Beispiel: Eine Sicherungsgruppe abfragen

Informationen zu Sicherungsgruppen anzeigen, deren Namen mit PERS_DATA beginnen. Die Sicherungsgruppen gehören zum Knoten JANE und sind der Einheitenklasse DVLMENT zugeordnet.

```
query backupset jane pers_data*

                     Knotenname: JANE
                Sicherungsgruppenname: PERS_DATA.3089
                       Datentyp: File
                  Datum/Uhrzeit: 03/17/2007 16:17:47
                Aufbewahrungszeitraum: 60
                 Einheitenklassenname: DVLMENT
                        Beschreibung: backupset created from /srvr
              Hat Inhaltsverzeichnis?: Yes
```

Feldbeschreibungen

Knotenname
: Gibt den Namen des Clientknotens an, dessen Daten in der Sicherungsgruppe enthalten sind.

Sicherungsgruppenname
: Gibt den Namen der Sicherungsgruppe an.

Datentyp
: Zeigt den Datentyp der Sicherungsgruppen. Mögliche Typen sind file (Datei), image (Image) und application (Anwendung).

Datum/Uhrzeit
: Gibt das Datum und die Uhrzeit (PITDate und PITTime) des Befehls GENERATE BACKUPSET an. PITDate und PITTime geben an, dass Dateien, die an dem angegebenen Datum und zu der angegebenen Zeit aktiv waren und die noch auf dem IBM Spectrum Protect-Server gespeichert sind, in die Sicherungsgruppe eingeschlossen werden sollen, auch wenn sie zum Zeitpunkt der Ausgabe des Befehls GENERATE BACKUPSET inaktiv sind. Der Standardwert ist das Datum, an dem der Befehl GENERATE BACKUPSET ausgeführt wird.

Aufbewahrungszeitraum
: Gibt die Anzahl Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt wird.

Einheitenklassenname
: Gibt den Namen der Einheitenklasse an, der die Datenträger, die die Sicherungsgruppe enthalten, zugeordnet sind.

Beschreibung
: Gibt die Beschreibung an, die der Sicherungsgruppe zugeordnet ist.

Hat Inhaltsverzeichnis?
: Gibt an, ob die Sicherungsgruppe ein Inhaltsverzeichnis hat.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY BACKUPSET

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
GENERATE BACKUPSETTOC	Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUP	Löscht eine Knotengruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
QUERY BACKUPSETCONTENTS	Zeigt den Inhalt in Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

QUERY BACKUPSETCONTENTS (Inhalt einer Sicherungsgruppe abfragen)

Mit diesem Befehl können Informationen zu Dateien und Verzeichnissen angezeigt werden, die in einer Sicherungsgruppe eines Clientknotens enthalten sind.

Hinweis: Die Verarbeitung dieses Befehls kann erhebliche Netzressourcen und Mountpunkte erfordern.

Berechtigungsklasse

Um diesen Befehl ausgeben zu können, müssen Benutzer die Systemberechtigung oder Maßnahmenberechtigung für die Domäne haben, der der Client-Knoten zugeordnet ist.

Syntax

```
>>-Query BACKUPSETCONTENTS--Knotenname--Sicherungsgruppenname--->

   .-DATAType--=--FILE------.
>--+------------------------+----------------------------------><
   '-DATAType--=--+-FILE--+-'
                  '-IMAGE-'
```

Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, dessen Daten in der Sicherungsgruppe enthalten sind, die angezeigt werden soll. Der angegebene Name darf keine Platzhalterzeichen enthalten oder darf keine Liste mit Knotennamen sein, die durch Kommas voneinander getrennt sind.

Sicherungsgruppenname (Erforderlich)
: Gibt den Namen der Sicherungsgruppe an, die angezeigt werden soll. Der angegebene Name darf keine Platzhalterzeichen enthalten oder darf keine Liste mit Knotennamen sein, die durch Kommas voneinander getrennt sind.

DATAType
: Gibt an, dass die Sicherungsgruppe mit den angegebenen Typen von Daten abgefragt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass eine Sicherungsgruppe auf Dateiebene abgefragt werden soll. Gültige Werte:

  FILE
  : Gibt an, dass eine Sicherungsgruppe auf Dateiebene abgefragt werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Client für Sichern/Archivieren gesichert wurden.

  IMAGE
  : Gibt an, dass eine Imagesicherungsgruppe abgefragt werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Clients für Sichern/Archivieren erstellt wurden.

Beispiel: Inhalt einer Sicherungsgruppe für einen bestimmten Knoten abfragen

Den Inhalt der Sicherungsgruppe PERS_DATA.3099 anzeigen, die zum Clientknoten JANE gehört. Den folgenden Befehl ausgeben:

```
query backupsetcontents jane pers_data.3099
```

```
Knotenname              Dateibe-   Dateiname des Clients
                        klasse
----------------------- ---------- ------------------------
JANE                    /srvr      /deblock
JANE                    /srvr      /deblock.c
JANE                    /srvr      /dsmerror.log
JANE                    /srvr      /dsmxxxxx.log
JANE                    ...        ......
```

Feldbeschreibungen

Knotenname
: Gibt den Namen des Clientknotens an, dessen Daten in der Sicherungsgruppe enthalten sind.

Dateibereichsname
: Gibt den Namen des Dateibereichs an, zu dem die angegebene Datei gehört.

  Dateibereichsnamen können eine andere Zeichenumsetztabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

  Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

Dateiname des Clients
: Gibt den Namen der Datei an.

  Dateibereichsnamen und Dateinamen, die eine andere Zeichenumsetztabelle oder Locale als der Server haben können, werden im Operations Center oder in der Verwaltungsbefehlszeilenschnittstelle nicht korrekt angezeigt. Die Daten selbst werden korrekt gesichert und können korrekt zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname in Unicode, wird der Name zur Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Die Ergebnisse der Konvertierung für Zeichen, die von der aktuellen Zeichenumsetztabelle nicht unterstützt werden, hängen von dem Betriebssystem ab. Bei Namen, die IBM Spectrum Protect teilweise konvertieren kann, werden möglicherweise Fragezeichen (??), Leerzeichen, nicht druckbare Zeichen oder "..." angezeigt. Diese Zeichen zeigen dem Administrator, dass Dateien vorhanden sind. Ist die Konvertierung nicht erfolgreich, wird der Name als "..." angezeigt. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

Ein Dateiname, der als "....." angezeigt wird, gibt an, dass sowohl der Dateipfad als auch der Dateiname nicht erfolgreich konvertiert wurden. Ein Beispiel für den Pfad und Namen ist:

```
my\dir\...
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY BACKUPSETCONTENTS

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
GENERATE BACKUPSETTOC	Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

QUERY CLEANUP (Bereinigung abfragen, die in einem Quellenspeicherpool erforderlich ist)

Mit diesem Befehl können Informationen zu beschädigten Dateien angezeigt werden, die während eines Speicherpoolkonvertierungsprozesses identifiziert werden.

Wenn Sie den Befehl CONVERT STGPOOL ausgeben, um eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) in einen Verzeichniscontainerspeicherpool zu konvertieren, werden einige Dateien in dem Quellenspeicherpool aufgrund von beschädigten Daten möglicherweise nicht konvertiert. Geben Sie den Befehl QUERY CLEANUP für einen Quellenspeicherpool aus, um beschädigte Daten anzuzeigen, die während des Konvertierungsprozesses identifiziert werden.

Um eine unbeschädigte Version der Daten aus einem Kopienspeicherpool oder Speicherpool für aktive Daten wiederherzustellen, geben Sie den Befehl RESTORE STGPOOL aus. Um eine unbeschädigte Version der Daten von einem Zielreplikationsserver wiederherzustellen, geben Sie den Befehl REPLICATE NODE aus und geben Sie den Parameter RECOVERDAMAGED=YES an.

Berechtigungsklasse

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-Query CLeanup--Poolname-------------------------------------><
```

Parameter

Poolname (Erforderlich)
: Gibt den Speicherpool an, der abgefragt werden soll.

Beispiel: Beschädigte Dateien anzeigen, die bei einem Speicherpoolkonvertierungsprozess identifiziert werden

Beschädigte Dateien in einem Speicherpool mit dem Namen POOL1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query cleanup pool1

              Dateiname: \RTC\BDAT\GIGFILES\BF1.GB
                 Status: Aktiv
          Gespeicherte Größe: 1 GB
```

```
Dateibereichsname: \\ibm838-r90gf0gx\c$
              Typ: Backup
       Clientname: CAKINProtection
Datum des Schutzes: 03/25/2016 16:47:57
```

Feldbeschreibungen

Dateiname
: Der Name der beschädigten Datei.

Status
: Der Status der Daten im Bestand. Die folgenden Status sind gültig:

  Aktiv
  : Die Version der Datei im Bestand ist aktiv. Es kann nur eine aktive Version der Datei im Bestand vorhanden sein.

  Inaktiv
  : Die Version der Datei im Bestand ist inaktiv. Es können mehrere inaktive Versionen der Datei im Bestand vorhanden sein.

Gespeicherte Größe
: Die Größe der Daten in Megabyte (MB) oder Gigabyte (GB), die in dem Speicherpool gespeichert werden.

Dateibereichsname
: Der Name des Dateibereichs, dem die Datei zugeordnet ist.

Typ
: Der Typ der Operation, die zum Speichern der Datei verwendet wurde. Die folgenden Typen sind gültig:

  Backup
  : Dateien, die gesichert werden.

  Archive
  : Dateien, die archiviert werden.

  SpaceMg
  : Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert werden.

Clientname
: Der Name des Clients, der Eigner der Datei ist.

Datum des Schutzes
: Die Uhrzeit und das Datum, zu der bzw. an dem die Datei von einem IBM Spectrum Protect for Space Management-Client gesichert, archiviert oder umgelagert wurde.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY CLEANUP

Befehl	Beschreibung
CONVERT STGPOOL	Konvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool.
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.
QUERY CONVERSION	Fragt den Konvertierungsstatus eines Speicherpools ab.
REMOVE DAMAGED	Entfernt beschädigte Daten aus einem Quellenspeicherpool.
REPAIR STGPOOL	Repariert einen Verzeichniscontainerspeicherpool.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
RESTORE STGPOOL	Schreibt Dateien aus Kopienspeicherpools in einen primären Speicherpool zurück.

QUERY CLOPTSET (Clientoptionsgruppe abfragen)

Mit diesem Befehl kann eine Clientoptionsgruppe abgefragt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
.-*------------------.
```

```
>>-Query CLOptset--+--------------------+---------------------->
                  '-Optionsgruppenname-'

>--+-----------------------------+---------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Optionsgruppenname
: Gibt den Namen der Clientoptionsgruppe an, die abgefragt werden soll. Dieser Name kann mithilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert lautet Optionsgruppennamen.

DESCription
: Gibt die im Befehl DEFINE oder UPDATE CLOPTSET verwendete Beschreibung an, die als Filter verwendet werden soll. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Dieser Parameter ist wahlfrei.

Beispiel: Eine Clientoptionsgruppe abfragen

Von einem verwalteten Server die Clientoptionsgruppe ENG abfragen. Geben Sie den folgenden Befehl aus:

```
query cloptset eng
```

```
                      Optionsgruppe: ENG
                                     Beschreibung:
             Letzte Aktualisierung durch
                          (Administrator): $$CONFIG_MANAGER$$
                          Verwaltendes Profil:
                                                          Replikatoptionsgruppe: Yes

                               Option: SCROLLINES
                          Folgenummer: 0
  Optionsgruppenwert verwenden (FORCE): No
                          Optionswert: 40

                               Option: SCROLLPROMPT
                          Folgenummer: 0
  Optionsgruppenwert verwenden (FORCE): No
                          Optionswert: yes
```

Feldbeschreibungen

Optionsgruppe
: Gibt den Namen der Optionsgruppe an.

Beschreibung
: Gibt die Beschreibung der Clientoptionsgruppe an.

Letzte Aktualisierung durch (Administrator)
: Gibt den Namen des Administrators an, der die Optionsgruppe zuletzt aktualisiert hat. Enthält dieses Feld $$CONFIG_MANAGER$$, ist die Clientoptionsgruppe einem Profil zugeordnet, das von dem Konfigurationsmanager verwaltet wird.

Verwaltendes Profil
: Gibt das Profil an, für das der verwaltete Server subskribiert hat, um die Definition der Clientoptionsgruppe zu erhalten.

Replikatoptionsgruppe
: Gibt an, dass die Replikatoptionsgruppe durch den Quellenreplikationsserver repliziert wird.

Option
: Gibt den Namen der Option an.

Folgenummer
: Gibt die Folgenummer der Option an.

Optionsgruppenwert verwenden (FORCE)
: Gibt an, ob die Serveroptionseinstellung die Optionseinstellung für den Client überschreibt. NO gibt an, dass die Serveroptionseinstellung die Clientoption nicht überschreibt. YES gibt an, dass die Serveroptionseinstellung die Clientoptionseinstellung überschreibt. Diese Option wird mit dem Parameter FORCE im Befehl DEFINE CLIENTOPT definiert.

Optionswert
: Gibt den Wert der Option an.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY CLOPTSET

Befehl	Beschreibung
COPY CLOPTSET	Kopiert eine Clientoptionsgruppe.
DEFINE CLIENTOPT	Fügt einer Clientoptionsgruppe eine Clientoption hinzu.
DEFINE CLOPTSET	Definiert eine Clientoptionsgruppe.

Befehl	Beschreibung
DELETE CLIENTOPT	Löscht eine Clientoption aus einer Clientoptionsgruppe.
DELETE CLOPTSET	Löscht eine Clientoptionsgruppe.
UPDATE CLIENTOPT	Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe.
UPDATE CLOPTSET	Aktualisiert die Beschreibung einer Clientoptionsgruppe.
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.

QUERY COLLOCGROUP (Kollokationsgruppe abfragen)

Verwenden Sie diesen Befehl, um die Kollokationsgruppen anzuzeigen, die auf dem Server definiert sind.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                        .-*-----------.
>>-Query COLLOCGroup--+-------------+--------------------------->
                      '-Gruppenname-'

   .-Format--=--Standard-----.
>--+-------------------------+---------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Gruppenname
: Gibt den Namen der Kollokationsgruppe an, die angezeigt werden soll. Sollen mehrere Namen angegeben werden, ein Platzhalterzeichen verwenden. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Kollokationsgruppen angezeigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.Um die Clientknoten in der Kollokationsgruppe anzuzeigen, müssen Sie FORMAT=DETAILED angeben.

Definierte Kollokationsgruppen anzeigen

Die Kollokationsgruppen anzeigen, die auf dem Server definiert sind. Den folgenden Befehl ausgeben:

```
query collocgroup

Name der Kollokationsgruppe    Beschreibung der Kollokationsgruppe
---------------------------    -------------------------------
DEPT_ED                        Ausbildungsabteilung
GROUP1                         Clientknoten mit geringer Kap.
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Ausführliche Informationen zu Kollokationsgruppen anzeigen

Vollständige Informationen zu allen Kollokationsgruppen anzeigen und bestimmen, welche Clientknoten zu welchen Kollokationsgruppen gehören. Den folgenden Befehl ausgeben:

```
query collocgroup format=detailed

               Name der Kollokationsgruppe: DEPT_ED
         Beschreibung der Kollokationsgruppe: Ausbildungsabteilung
  Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
       Datum/Zeit der letzten Aktualisierung: 04/21/2013 10:59:03
            Kollokationsgruppenmitglied(er): EDU_1 EDU_7
                  Dateibereichsmitglied(er):
```

```
                Name der Kollokationsgruppe: GROUP1
          Beschreibung der Kollokationsgruppe: Knoten mit ger. Kap.
  Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
        Datum/Zeit der letzten Aktualisierung: 04/21/2013 10:59:16
             Kollokationsgruppenmitglied(er): CHESTER
                   Dateibereichsmitglied(er): alpha

                Name der Kollokationsgruppe: GROUP1
          Beschreibung der Kollokationsgruppe: Knoten mit ger. Kap.
  Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
        Datum/Zeit der letzten Aktualisierung: 04/21/2013 10:59:16
             Kollokationsgruppenmitglied(er): CHESTER
                   Dateibereichsmitglied(er): beta

                Name der Kollokationsgruppe: GROUP1
          Beschreibung der Kollokationsgruppe: Knoten mit ger. Kap.
  Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
        Datum/Zeit der letzten Aktualisierung: 04/21/2013 10:59:16
             Kollokationsgruppenmitglied(er): CHESTER
                   Dateibereichsmitglied(er): gamma
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Name der Kollokationsgruppe
: Der Name der Kollokationsgruppe.

Beschreibung der Kollokationsgruppe
: Die Beschreibung der Kollokationsgruppe.

Letzte Aktualisierung durch (Administrator)
: Der Name des Administrators, der die Kollokationsgruppe definiert oder zuletzt aktualisiert hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der ein Administrator die Kollokationsgruppe definiert oder zuletzt aktualisiert hat.

Kollokationsgruppenmitglied(er)
: Die Mitglieder der Kollokationsgruppe.

Dateibereichsmitglied(er)
: Die Dateibereiche, die Mitglieder der Kollokationsgruppe sind. Sind mehrere Dateibereiche vorhanden, wird jeder Dateibereich in einem separaten Eintrag angezeigt.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY COLLOCGROUP

Befehl	Beschreibung
DEFINE COLLOCGROUP	Definiert eine Kollokationsgruppe.
DEFINE COLLOCMEMBER	Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE COLLOCGROUP	Löscht eine Kollokationsgruppe.
DELETE COLLOCMEMBER	Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.
MOVE NODEDATA	Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
UPDATE COLLOCGROUP	Aktualisiert die Beschreibung einer Kollokationsgruppe.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

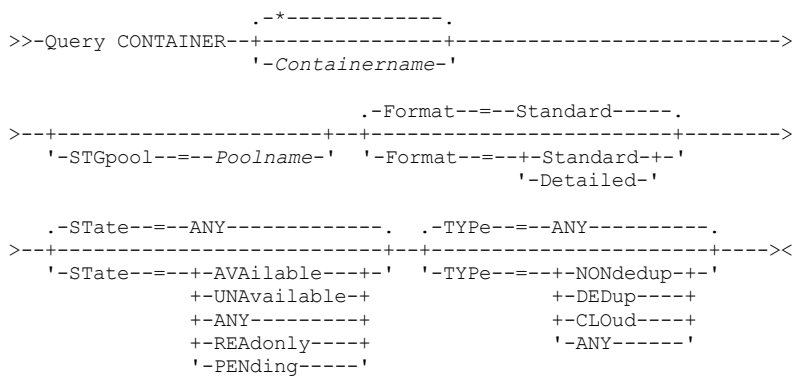
QUERY CONTAINER (Container abfragen)

Mit diesem Befehl können Informationen zu einem oder zu mehreren Containern angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Containername
: Gibt den Namen des Containers an. Geben Sie einen der folgenden Werte an:

  *
  : Gibt an, dass ein Stern (*) ein Platzhalterzeichen darstellt. Verwenden Sie Platzhalterzeichen, wie z. B. einen Stern, für die Übereinstimmung mit beliebigen Zeichen. Alternativ können Sie ein Fragezeichen (?) oder ein Prozentzeichen (%) verwenden, die exakt einem Zeichen entsprechen. Wenn Sie einen Stern angeben, werden alle Containernamen angezeigt. Dieser Wert ist der Standardwert.

  Containername
  : Gibt den Namen des Containers an. Die maximale Länge des Containernamens beträgt 1024 Zeichen.

STGpool
: Gibt den Namen des Verzeichniscontainerspeicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge des Speicherpoolnamens beträgt 30 Zeichen.

Format
: Gibt die Detaillierungsebene der Abfrageergebnisse an. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

  Standard
  : Gibt an, dass eine Zusammenfassung der Informationen angezeigt wird. Dieser Wert ist der Standardwert.

  Detailed
  : Gibt an, dass ausführliche Informationen angezeigt werden.

STate
: Gibt den Status des Containers an, der abgefragt wird. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

  AVAilable
  : Gibt an, dass nur verfügbare Container angezeigt werden.

  UNAvailable
  : Gibt an, dass nur Container angezeigt werden, die nicht verfügbar sind. Beispielsweise kann ein Container nicht verfügbar sein, wenn der Header beschädigt ist oder der Container nicht geöffnet werden kann.

  ANY
  : Gibt an, dass Container mit einem beliebigen Status angezeigt werden. Dieser Wert ist der Standardwert.

  REAdonly
  : Gibt an, dass nur Container mit Lesezugriff angezeigt werden. Daten in dem Container können gelesen werden, aber es können keine Daten in den Container geschrieben werden.

  PENding
  : Gibt an, dass nur Container im Wartestatus angezeigt werden.

TYPe
: Gibt den Typ des Containers an, der abgefragt wird. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

NONdedup
: Zeigt Container an, die Daten enthalten, die nicht dedupliziert werden. Dieser Datentyp schließt Metadaten, verschlüsselte Daten und Daten ein, die für die Datendeduplizierung zu klein sind.

DEDup
: Zeigt Container an, die deduplizierte Daten enthalten.

CLOud
: Zeigt Container an, die in einem Cloudspeicherpool gespeichert sind.

ANY
: Zeigt jeden Typ von Container an. Dieser Wert ist der Standardwert.

 AIX-Betriebssysteme  Linux-Betriebssysteme

Beispiel: Informationen zu einem Container anzeigen

Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query container /Containers/09/0000000000000943.ncf
```

```
Container                                Speicher-       Container-    Status
                                         poolname        typ
---------------------------------- -------------- ------------  ---------
/Containers/09/0000000000000943.ncf       STGPOOL1       Non Dedup      Available
```

 Windows-Betriebssysteme

Beispiel: Informationen zu einem Container anzeigen

Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query container C:\abc\00\0000000000000005.ncf
```

```
Container                           Speicher-       Container-    Status
                                    poolname        typ
------------------------------    -----------  ----------  ---------
C:\abc\00\0000000000000005.ncf       STGPOOL1       Non Dedup      Available
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

Beispiel: Ausführliche Informationen zu einem Container anzeigen

Ausführliche Informationen zu Containern anzeigen, die deduplizierte Daten im Speicherpool STGPOOL1 enthalten:

```
query container stgpool=STGPOOL1 type=dedup format=detail
```

```
                          Container: /abc/00/0000000000000001.dcf
                                 Speicherpoolname: STGPOOL1
                                     Containertyp: Dedup
                                           Status: Available
                              Maximale Größe (MB): 40.960
                        Freier Speicherbereich (MB): 39.700
              Ungefähres Datum des letzten Schreibens: 11/10/2014 15:17:09
                 Ungefähres Datum der letzten Prüfung:
                                       Cloudtyp:
                                      Cloud-URL:
                    Belegter Speicherbereich (MB):
                                  Anzahl Objekte:
```

 Windows-Betriebssysteme

Beispiel: Ausführliche Informationen zu einem Container anzeigen

Ausführliche Informationen zu Containern anzeigen, die deduplizierte Daten im Speicherpool STGPOOL1 enthalten:

```
query container stgpool=STGPOOL1 type=dedup format=detail
```

```
                          Container: C:\abc\00\0000000000000001.dcf
                                 Speicherpoolname: STGPOOL1
                                     Containertyp: Dedup
                                           Status: Available
                              Maximale Größe (MB): 40.960
                        Freier Speicherbereich (MB): 39.700
              Ungefähres Datum des letzten Schreibens: 11/10/2014 15:17:09
                 Ungefähres Datum der letzten Prüfung:
                                       Cloudtyp:
                                      Cloud-URL:
                    Belegter Speicherbereich (MB):
                                  Anzahl Objekte:
```

Beispiel: Ausführliche Informationen zu Containern anzeigen, die in einem Cloudspeicherpool gespeichert sind

Ausführliche Informationen zu Containern anzeigen, die im Cloudspeicherpool CLOUDPOOL gespeichert sind:

```
query container stgpool=CLOUDPOOL format=detail
```

```
                        Container: 7-64a1261000c811e58e8f005056c00008
                                    Speicherpoolname: CLOUDPOOL
                                        Containertyp: Cloud
                                              Status:
                                  Freier Speicherbereich (MB):
                               Maximale Größe (MB):
              Ungefähres Datum des letzten Schreibens: 05/22/2015 14:36:57
                 Ungefähres Datum der letzten Prüfung:
                                           Cloudtyp: SWIFT
                                       Cloud-URL: http://cloudurl:5000/v2.0
                     Belegter Speicherbereich: 7104
                               Anzahl Objekte: 2472
```

Feldbeschreibungen

Container
: Der Name des Containers.

Speicherpoolname
: Der Name des Speicherpools.

Containertyp
: Der Typ des Containers.

Status
: Der Status der Daten in dem Container. Das Feld kann einen der folgenden Werte enthalten:

  Available
  : Der Container ist für die Verwendung verfügbar.

  Unavailable
  : Der Container kann nicht geöffnet oder geprüft werden.
  Tipp: Geben Sie den Befehl AUDIT CONTAINER aus, um den Inhalt des Containers zu prüfen.

  Read only
  : Der Container kann gelesen werden, aber es können keine Daten in den Container geschrieben werden.

  Pending
  : Das Löschen des Containers ist anstehend. Wenn der für den Parameter REUSEDELAY im Befehl DEFINE STGPOOL oder UPDATE STGPOOL angegebene Wert abläuft, wird der Container gelöscht.

  Dieses Feld gilt nicht für Container, die in Cloudspeicherpools gespeichert sind.

Maximale Größe (MB)
: Die maximale Größe des Containers in Megabyte.

  Dieses Feld gilt nicht für Container, die in Cloudspeicherpools gespeichert sind.

Freier Speicherbereich (MB)
: Der Gesamtumfang des freien Speicherbereichs (in Megabyte), der im Container verfügbar ist.

  Dieses Feld gilt nicht für Container, die in Cloudspeicherpools gespeichert sind.

Ungefähres Datum des letzten Schreibens
: Das ungefähre Datum und die Uhrzeit, an dem bzw. zu der Daten in den Container geschrieben wurden.

Ungefähres Datum der letzten Prüfung
: Das ungefähre Datum und die Uhrzeit, an dem bzw. zu der Daten in dem Container geprüft wurden.

Cloudtyp
: Wenn der Container in einem Cloudspeicherpool gespeichert ist, der Typ der Cloudplattform.

Cloud-URL
: Wenn der Container in einem Cloudspeicherpool gespeichert ist, die URL für den Zugriff auf die private On-Premises-Cloud oder die öffentliche Off-Premises-Cloud.

Belegter Speicherbereich (MB)
: Wenn der Container in einem Cloudspeicherpool gespeichert ist, der Umfang des Speicherbereichs, der von dem Container in der privaten On-Premises-Cloud oder der öffentlichen Off-Premises-Cloud belegt wird.

Anzahl Objekte
: Wenn der Container in einem Cloudspeicherpool gespeichert ist, die Anzahl Objekte, die von der privaten On-Premises-Cloud oder der öffentlichen Off-Premises-Cloud für den Container verwaltet wird.

Tabelle 1. Zugehörige Befehle für QUERY CONTAINER

Befehl	Beschreibung

Befehl	Beschreibung
AUDIT CONTAINER	Prüft einen Verzeichniscontainerspeicherpool.
MOVE CONTAINER	Versetzt den Inhalt eines Speicherpoolcontainers in einen anderen Container.
QUERY DAMAGED	Zeigt Informationen zu beschädigten Dateien an.

QUERY CONTENT (Inhalt eines Speicherpooldatenträgers abfragen)

Mit diesem Befehl können Informationen zu Dateien auf einem Speicherpooldatenträger und die Namen von Clientdateien angezeigt werden, die die Verknüpfung zu einer deduplizierten Gruppe von Dateien herstellen.

Mit diesem Befehl können Dateien identifiziert werden, die vom Server als beschädigt erkannt wurden, sowie Dateien bestimmt werden, die in einem Kopienspeicherpool gesichert oder in einen Pool für aktive Daten kopiert wurden. Dieser Befehl ist nützlich bei einem beschädigten Datenträger oder bevor

- eine Anforderung an den Server gesendet wird, Inkonsistenzen zwischen einem Datenträger und der Datenbank zu beseitigen.
- Dateien von einem Datenträger auf einen anderen Datenträger versetzt werden.
- ein Datenträger aus einem Speicherpool gelöscht wird.

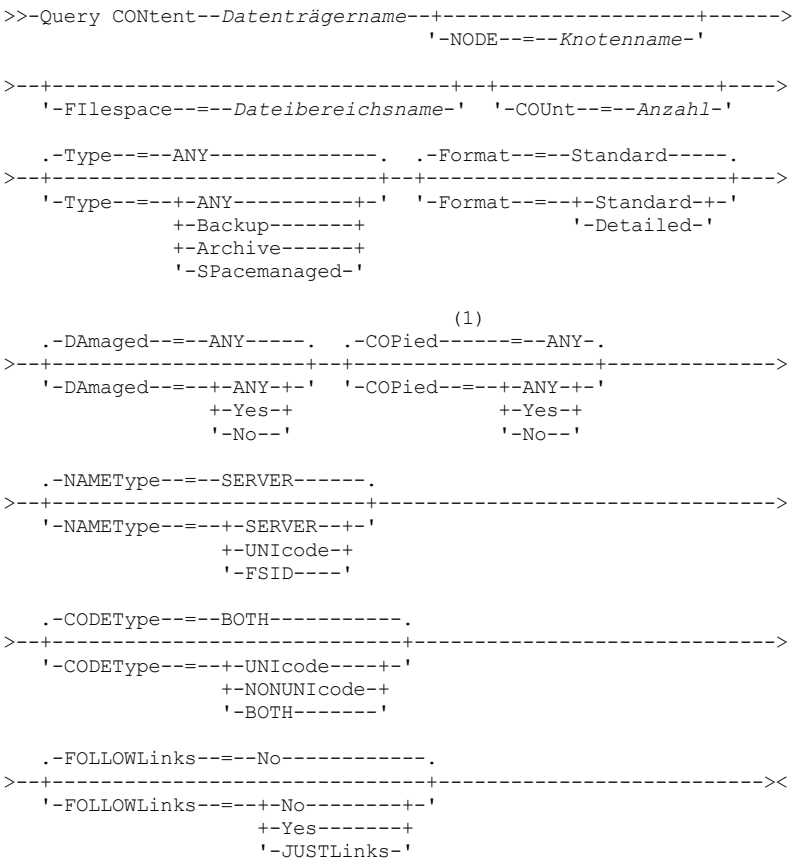
Da die Ausführung dieses Befehls sehr lange dauern kann und die Ergebnisse umfangreich sein können, sollte der Parameter COUNT verwendet werden, um die Anzahl der angezeigten Dateien zu begrenzen.

Anmerkung: Cache-Dateien in einem Plattendatenträger, die als beschädigt markiert sind, sind in den Ergebnissen nicht enthalten.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Anmerkungen:

1. Dieser Parameter ist nur für Datenträger in primären Speicherpools zu verwenden.

Parameter

Datenträgername (Erforderlich)
Gibt den Datenträger an, der abgefragt werden soll.

NODE
Gibt den Client für Sichern/Archivieren oder den IBM Spectrum Protect for Space Management an, der dem Dateibereich zugeordnet ist, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Name angegeben, werden alle Clients für Sichern/Archivieren und IBM Spectrum Protect for Space Management-Clients berücksichtigt.

FIlespace
Gibt den Dateibereich an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Wird kein Dateibereichsname angegeben, werden alle Dateibereiche berücksichtigt.

Ein Server, der über Clients mit Unicode-Unterstützung verfügt, muss möglicherweise den Dateibereichsnamen, den Sie eingeben, konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich unter dem Parameter NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

COUnt
Gibt die Anzahl der Dateien an, die angezeigt werden sollen. Dieser Parameter ist wahlfrei. Zulässig ist die Angabe einer positiven ganzen Zahl oder einer negativen ganzen Zahl. Wird eine positive ganze Zahl *n* angegeben, werden die ersten `n` Dateien angezeigt. Wird eine negative ganze Zahl *-n* angegeben, werden die letzten `n` Dateien in `umgekehrter` Reihenfolge angezeigt. Sie dürfen COUNT=0 nicht angeben. Wird für diesen Parameter kein Wert angegeben, werden alle Dateien angezeigt.

Type
Gibt die Dateitypen an, die abgefragt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Ist der Datenträger, der abgefragt wird, einem Pool für aktive Daten zugeordnet, sind nur die Werte ANY und BACKUP gültig. Gültige Werte:

ANY
Gibt an, dass alle Dateitypen in dem Speicherpooldatenträger abgefragt werden: Sicherungsversionen von Dateien, Archivierungskopien von Dateien und Dateien, die von IBM Spectrum Protect for Space Management-Clients aus Clientknoten umgelagert wurden.

Backup
Gibt an, dass nur Sicherungsdateien abgefragt werden.

Archive
Gibt an, dass nur Archivierungsdateien abgefragt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

SPacemanaged
Gibt an, dass nur speicherverwaltete Dateien (Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden) abgefragt werden. Dieser Wert ist für Pools für aktive Daten nicht gültig.

Format
Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard
Gibt an, dass Teilinformationen angezeigt werden.Unicode-Namen werden in die Server-Zeichenumsetztabelle konvertiert.

Detailed
Gibt an, dass die gesamten Informationen angezeigt werden.Unicode-Namen werden in hexadezimalen Zeichen angezeigt.

DAmaged
Gibt Kriterien an, um die Ausgabe der Abfrage auf der Basis von Dateien, die als beschädigt markiert werden, zu begrenzen. Zu diesem Zweck überprüft der Server nur physische Dateien (eine Datei, die eine einzelne logische Datei oder ein Aggregat aus logischen Dateien sein kann). Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Gültige Werte:

ANY
Gibt an, dass Dateien unabhängig davon angezeigt werden, ob der Server die Dateien als beschädigt festgestellt hat.

Yes
Gibt an, dass nur Dateien angezeigt werden, die als beschädigt markiert werden. Hierbei handelt es sich um Dateien, in denen der Server Fehler festgestellt hat, als versucht wurde, sie zurückzuschreiben, abzurufen oder zurückzurufen oder als ein Befehl AUDIT VOLUME ausgeführt wurde.

No
Gibt an, dass nur Dateien angezeigt werden, von denen nicht bekannt ist, dass sie beschädigt sind.

COPied
Gibt Kriterien an, um die Ausgabe der Abfrage auf der Basis von Dateien, die in einem Kopienspeicherpool gesichert wurden, zu begrenzen. Ob Dateien in einem Pool für aktive Daten gespeichert werden, hat keinen Einfluss auf die Ausgabe. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Gültige Werte:

ANY
Gibt an, daß Dateien unabhängig davon angezeigt werden, ob sie in einem Kopienspeicherpool gesichert werden. Kopien von Primär- und Cache-Dateien werden angezeigt.

Yes

Gibt an, daß nur Dateien angezeigt werden, für die mindestens eine verwendbare Sicherungskopie in einem Kopienspeicherpool vorhanden ist. Eine Datei wird nicht angezeigt, wenn bei ihrer Kopie im Kopienspeicherpool Fehler festgestellt wurden. Kopien von Cache-Dateien werden nicht angezeigt, weil diese Dateien nie zurückgeschrieben werden.

Verwenden Sie COPIED=YES, um Primärdateien zu identifizieren, die mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL zurückgeschrieben werden können.

No
Gibt an, daß nur Dateien angezeigt werden, für die keine verwendbaren Sicherungskopien in einem Kopienspeicherpool vorhanden sind. Kopien von Cache-Dateien werden nicht angezeigt, weil diese Dateien nie zurückgeschrieben werden.

Verwenden Sie COPIED=NO, um Primärdateien zu identifizieren, die mit dem Befehl RESTORE VOLUME oder RESTORE STGPOOL nicht zurückgeschrieben werden können.

NAMEType
Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unicode-Unterstützung verfügt. Ein Client für Sichern/Archivieren mit Unicode-Unterstützung ist gegenwärtig nur für Windows, Macintosh OS 9, Macintosh OS X und NetWare verfügbar. Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen angeben.

Der Standardwert lautet SERVER. Gültige Werte:

SERVER
Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.
UNIcode
Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in den Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.
FSID
Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

CODEType
Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben.

Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass die Dateibereiche unabhängig von der Art der Zeichenumsetztabelle eingeschlossen werden. Gültige Werte:

UNIcode
Nur Dateibereiche einschließen, die in Unicode sind.
NONUNIcode
Dateibereiche einschließen, die nicht nur in Unicode sind.
BOTH
Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

FOLLOWLinks
Gibt an, ob nur die Dateien angezeigt werden sollen, die auf dem Datenträger gespeichert sind, oder nur Dateien angezeigt werden sollen, die mit dem Datenträger verknüpft sind. Sie können auch gespeicherte Dateien und verknüpfte Dateien anzeigen. Der Standardwert ist NO. Gültige Werte:

No
Nur die Dateien anzeigen, die auf dem Datenträger gespeichert sind. Keine Dateien anzeigen, die Verknüpfungen mit dem Datenträger haben.
Yes
Alle Dateien anzeigen, einschließlich Dateien, die auf dem Datenträger gespeichert sind, und aller Dateien, die Verknüpfungen mit dem Datenträger haben.
JUSTLinks
Nur die Dateien anzeigen, die Verknüpfungen mit dem Datenträger haben. Keine Dateien anzeigen, die auf dem Datenträger gespeichert sind.

Beispiel: Den Inhalt eines Datenträgers für einen bestimmten Clientknoten anzeigen

Den Inhalt eines Datenträgers abfragen und die Ergebnisse auf Dateien begrenzen, die auf dem Clientknoten PEGASUS gesichert wurden.
AIX-Betriebssysteme  Linux-BetriebssystemeFür den Datenträger /tsmstg/diskvol1.dsm den folgenden Befehl ausgeben:

```
query content /tsmstg/diskvol1.dsm node=pegasus
  type=backup
```

Windows-BetriebssystemeFür den Datenträger f:\tsmstg\diskvol1.dsm den folgenden Befehl ausgeben:

```
query content f:\tsmstg\diskvol1.dsm node=pegasus
  type=backup
```

Die Ergebnisse des Befehls umfassen alle logischen Dateien, die ein beliebiges Aggregat auf dem Datenträger bilden, auch wenn das Aggregat auf mehreren Datenträgern gespeichert ist. Bei Aggregaten wird von der Abfrage nicht bestimmt, welche logischen Dateien tatsächlich auf dem Datenträger gespeichert sind, für den die Abfrage ausgeführt wird.

```
Knotenname       Typ   Dateibe-    FSID  Dateiname des Clients
                         klasse
-----------  ----  ----------   ----  ---------------------
PEGASUS         Bkup  \\pegasus\e$   1   \UNI_TEST\ SM01.DAT
PEGASUS         Bkup  \\pegasus\e$   1   \UNI_TEST\ SM02.DAT
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Informationen zu einem Banddatenträger anzeigen

Den Inhalt des Banddatenträgers mit dem Namen WPD001 abfragen. Nur die Dateien anzeigen, die von dem Knoten MARK gesichert werden, und die Dateien anzeigen, die entweder auf dem Datenträger gespeichert oder mit dem Datenträger verknüpft sind. Nur die ersten vier Dateien auf dem Datenträger anzeigen.

```
query content wpd001 node=mark count=4 type=backup followlinks=yes
 format=detailed

                             Knotenname: MARK
                                    Typ: Bkup
                      Dateibereichsname: \\mark\e$
          Hexadezimaler Dateibereichsname:
                                   FSID: 1
                 Dateiname des Clients: \UNI_TEST\ SM01.DAT
      Hexadezimaler Dateiname des Clients:
                               Aggregat?: 1/3
                    Gespeicherte Größe: 2.746
                         Segmentnummer:
                          Cache-Kopie?: No
                              Verknüpft: No
                     Fragmentnummer:

                             Knotenname: MARK
                                    Typ: Bkup
                      Dateibereichsname: \\mark\e$
          Hexadezimaler Dateibereichsname:
                                   FSID: 1
                 Dateiname des Clients: \UNI_TEST\ SM02.DAT
      Hexadezimaler Dateiname des Clients:
                               Aggregat?: 2/3
                    Gespeicherte Größe: 2.746
                         Segmentnummer:
                          Cache-Kopie?: No
                              Verknüpft: No
                     Fragmentnummer: 2

                             Knotenname: MARK
                                    Typ: Bkup
                      Dateibereichsname: \\mark\e$
          Hexadezimaler Dateibereichsname:
                                   FSID: 1
                 Dateiname des Clients: \UNI_TEST\ SM03.DAT
      Hexadezimaler Dateiname des Clients:
                               Aggregat?: 3/3
                    Gespeicherte Größe: 2.746
                         Segmentnummer:
                          Cache-Kopie?: No
                              Verknüpft: No
                     Fragmentnummer: 3
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Knotenname
: Der Knoten, zu dem die Datei gehört.

Type
: Der Dateityp: archive (Arch), backup (Bkup) oder space-managed (SpMg) (durch einen IBM Spectrum Protect for Space Management-Client).

Dateibereichsname
: Der Dateibereich, zu dem die Datei gehört.

  Dateibereichsnamen können eine andere Zeichenumsetztabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal

gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

Hexadezimaler Dateibereichsname
: Der Dateibereich, zu dem die Datei gehört. Ist der Dateibereichsname in Unicode, wird der Name in hexadezimalem Format angezeigt.

FSID
: Die Dateibereichs-ID (FSID) des Dateibereichs. Der Server ordnet eine eindeutige FSID zu, wenn ein Dateibereich zum ersten Mal auf dem Server gespeichert wird.

Dateiname des Clients
: Der Dateiname des Clients.

Dateibereichsnamen und Dateinamen, die eine andere Zeichenumsetztabelle oder Locale als der Server haben können, werden im Operations Center oder in der Verwaltungsbefehlszeilenschnittstelle nicht korrekt angezeigt. Die Daten selbst werden korrekt gesichert und können korrekt zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden. Die Ergebnisse der Konvertierung für Zeichen, die von der aktuellen Zeichenumsetztabelle nicht unterstützt werden, hängen von dem Betriebssystem ab. Bei Namen, die IBM Spectrum Protect teilweise konvertieren kann, werden möglicherweise Fragezeichen (??), Leerzeichen, nicht druckbare Zeichen oder "..." angezeigt. Diese Zeichen zeigen dem Administrator, dass Dateien vorhanden sind.

Hexadezimaler Dateiname des Clients
: Der Dateiname des Clients, der in hexadezimalem Format angezeigt wird.

Aggregat?
: Die Angabe, ob es sich um eine logische Datei handelt, die als Teil eines Aggregats gespeichert ist. Ist die Datei ein Teil eines Aggregats, werden die Folgenummer dieser Datei innerhalb des Aggregats und die Gesamtzahl der logischen Dateien in dem Aggregat angezeigt.Die Ergebnisse des Befehls umfassen alle logischen Dateien, die ein beliebiges Aggregat auf dem Datenträger bilden, auch wenn das Aggregat auf mehreren Datenträgern gespeichert ist. Die Abfrage bestimmt nicht, welche logischen Dateien tatsächlich auf dem Datenträger gespeichert sind, für den die Abfrage ausgeführt wird.

Ist die Datei nicht Teil eines Aggregats, zeigt dieses Feld "Nein" (No) an.

Gespeicherte Größe
: Die Größe der physischen Datei in Byte. Ist die Datei eine logische Datei, die als Teil eines Aggregats gespeichert ist, gibt dieser Wert die Größe des gesamten Aggregats an.

Segmentnummer
: Gibt bei Datenträgern in Speicherpools mit sequenziellem Zugriff an, ob die physische Datei (entweder eine einzelne logische Datei oder ein Aggregat aus logischen Dateien) auf mehreren Datenträgern gespeichert ist. Ist die logische Datei beispielsweise in einem Aggregat gespeichert, das sich über zwei Datenträger erstreckt, gibt die Segmentnummer `1/2` an (der erste Teil der physischen Datei ist auf dem Datenträger gespeichert) oder `2/2` an (der zweite Teil der physischen Datei ist auf dem Datenträger gespeichert). Lautet die Segmentnummer `1/1`, ist die physische Datei vollständig auf dem Datenträger gespeichert. Bei Datenträgern in Speicherpools mit wahlfreiem Zugriff wird für dieses Feld kein Wert angezeigt.

Cache-Kopie?
: Die Angabe, ob die physische Datei eine Cache-Kopie einer Datei ist, die in den nächsten Speicherpool umgelagert wurde. Ist die Datei ein Teil eines Aggregats, bezieht sich dieser Wert auf das Aggregat.

Verknüpft
: Gibt an, ob die Datei auf dem Datenträger gespeichert ist oder ob die Datei mit dem Datenträger verknüpft ist.

Fragmentnummer
: Gibt die Fragmentnummer an. Ist die Fragmentnummer leer, ist das Fragment entweder das erste Fragment oder kein Fragment.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY CONTENT

Befehl	Beschreibung
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
DELETE VOLUME	Löscht einen Datenträger aus einem Speicherpool.
RESTORE STGPOOL	Schreibt Dateien aus Kopienspeicherpools in einen primären Speicherpool zurück.

Befehl	Beschreibung
RESTORE VOLUME	Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopienspeicherpools zurück.
UPDATE VOLUME	Aktualisiert die Attribute der Speicherpooldatenträger.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

QUERY CONVERSION (Konvertierungsstatus eines Speicherpools abfragen)

Verwenden Sie diesen Befehl, um Informationen zu einer Konvertierungsoperation anzuzeigen. Sie können einen primären Speicherpool, der eine Einheitenklasse des Typs FILE oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet, in einen Verzeichniscontainerspeicherpool konvertieren.

Berechtigungsklasse

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-Query CONVERSion--+----------+------------------------------>
                     '-Poolname-'

   .-Format--=--Standard-----.
>--+-------------------------+---------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Poolname
: Gibt den Quellenspeicherpool an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert für diesen Parameter angegeben, werden Informationen für alle Speicherpools angezeigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Geben Sie einen der folgenden Werte an:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Konvertierungsinformationen für alle Speicherpools anzeigen

Konvertierungsinformationen für alle Speicherpools anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query conversion
```

```
Quellen-        Zielspeicher-   Anfangs-   Summe       Zuletzt
speicherpool    pool            volumen    konvertiert konvertiert
------------  ---------------  ---------  ----------  ----------
FILEPOOL       CTR              3 GB       3 GB        3 GB
FPOOL          CTR              333 MB     333 MB      267 MB
```

Beispiel: Ausführliche Informationen zur Speicherpoolkonvertierung anzeigen

Ausführliche Informationen zur Speicherpoolkonvertierung anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query conversion format=detailed
```

```
    Quellenspeicherpool: FILEPOOL
              Zielspeicherpool: CTR
      Maximale Anzahl Prozesse: 4
                        Dauer: 60 Minuten
                Anfangsvolumen: 333 MB
            Summe konvertiert: 333 MB
          Zuletzt konvertiert: 333 MB
             Startdatum/-zeit: 03/24/2016 13:22:32
```

Feldbeschreibungen

Quellenspeicherpool
: Der Name des Speicherpools, der konvertiert wird.

Zielspeicherpool
: Der Name des Zielspeicherpools, in dem die konvertierten Daten gespeichert werden.

Maximale Anzahl Prozesse
: Gibt die maximale Anzahl Konvertierungsprozesse an.

Dauer
: Gibt die Zeit in Minuten für die Konvertierung an.

Anfangsvolumen
: Das Anfangsdatenvolumen in Megabyte (MB), Gigabyte (GB) oder Terabyte (TB), das konvertiert werden soll.

Summe konvertiert
: Das Gesamtdatenvolumen in Megabyte (MB), Gigabyte (GB) oder Terabyte (TB), das konvertiert wurde.

Zuletzt konvertiert
: Das Datenvolumen in Megabyte (MB), Gigabyte (GB) oder Terabyte (TB), das während dieses Konvertierungsprozesses konvertiert wurde.

Startdatum/-zeit
: Die Uhrzeit und das Datum, zu der bzw. an dem der Befehl CONVERT STGPOOL zum ersten Mal für den Speicherpool ausgegeben wurde.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY CONVERSION

Befehl	Beschreibung
CONVERT STGPOOL	Konvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool.
QUERY CLEANUP	Fragt den Bereinigungsstatus eines Quellenspeicherpools ab.

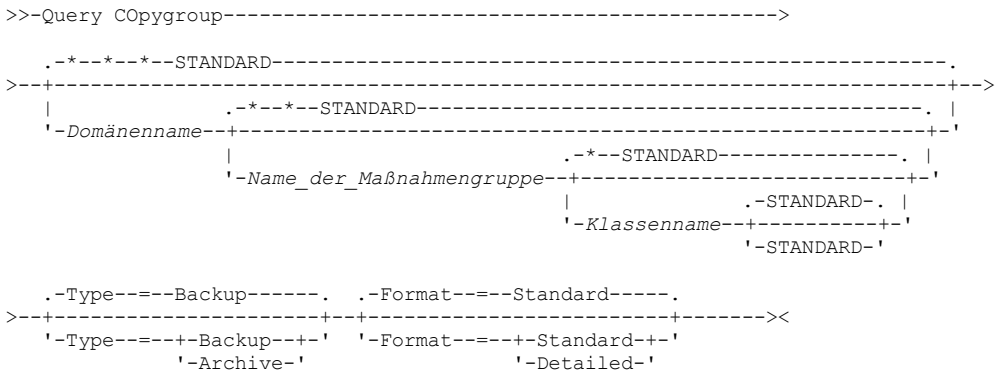
QUERY COPYGROUP (Kopiengruppen abfragen)

Mit diesem Befehl können Informationen über eine oder mehrere Kopiengruppen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Domänenname
: Gibt die Maßnahmendomäne an, die der Kopiengruppe zugeordnet ist, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Maßnahmendomänen abgefragt. Dieser Parameter muss angegeben werden, wenn explizit der Name einer Kopiengruppe angegeben wird.

Name_der_Maßnahmengruppe
: Gibt die Maßnahmengruppe an, die der Kopiengruppe zugeordnet ist, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Maßnahmengruppen abgefragt. Dieser Parameter muss angegeben werden, wenn explizit der Name einer Kopiengruppe angegeben wird.

Klassenname
: Gibt die Verwaltungsklasse an, die der Kopiengruppe zugeordnet ist, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Verwaltungsklassen abgefragt. Dieser Parameter muss angegeben werden, wenn explizit der Name einer Kopiengruppe angegeben wird.

STANDARD

Gibt den Namen der Kopiengruppe an. Dieser Parameter ist wahlfrei. Der Name der Kopiengruppe muss STANDARD lauten. Der Standardwert ist STANDARD.

Type

Gibt den Typ der Kopiengruppe an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist BACKUP. Gültige Werte:

Backup
: Gibt an, dass Sicherungskopiengruppen abgefragt werden sollen.

Archive
: Gibt an, dass Archivierungskopiengruppen abgefragt werden sollen.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard
: Gibt an, dass Teilinformationen angezeigt werden.

Detailed
: Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Informationen zur Standardsicherungskopiengruppe anzeigen

Informationen zur Standardsicherungskopiengruppe in der Maßnahmendomäne ENGPOLDOM anzeigen. Geben Sie den folgenden Befehl aus:

```
query copygroup engpoldom * *
```

Die folgenden Daten zeigen die Ausgabe der Abfrage. Die Ausgabe zeigt, dass die Maßnahmengruppe ACTIVE zwei Sicherungskopiengruppen enthält, die zu den Verwaltungsklassen MCENG und STANDARD gehören.

```
Name d.     Name d.     Name d.     Name d.  Versionen   Versionen  Extra-    Einzige
Maßnahmen-  Maßnahmen-  Verw.-      Kopien-  bestehender gelöschter versionen Version
domäne      gruppe      Klasse      gruppe   Daten       Daten      aufbew.   aufbew.
---------- ---------  ---------   -------  ---------  -------  -------  -------
ENGPOLDOM   ACTIVE      MCENG       STANDARD         5         4        90      600
ENGPOLDOM   ACTIVE      STANDARD    STANDARD         2         1        30       60
ENGPOLDOM   STANDARD    MCENG       STANDARD         5         4        90      600
ENGPOLDOM   STANDARD    STANDARD    STANDARD         2         1        30       60
ENGPOLDOM   TEST        STANDARD    STANDARD         2         1        30       60
```

Beispiel: Ausführliche Informationen zu einer Sicherungskopiengruppe anzeigen

Die gesamten Informationen für die Sicherungskopiengruppe anzeigen, die zur Verwaltungsklasse ACTIVEFILES in der Maßnahmengruppe VACATION der Maßnahmendomäne EMPLOYEE_RECORDS gehört. Den folgenden Befehl ausgeben:

```
query copygroup employee_records vacation
activefiles format=detailed
```

Beispiel: Informationen zu der Sicherungskopiengruppe in der Verwaltungsklasse und Maßnahmengruppe STANDARD anzeigen

Von einem verwalteten Server die vollständigen Informationen für die Sicherungskopiengruppe anzeigen, die der Verwaltungsklasse STANDARD in der Maßnahmengruppe STANDARD der Maßnahmendomäne ADMIN_RECORDS zugeordnet ist. Den folgenden Befehl ausgeben:

```
query copygroup admin_records
standard standard format=detailed
```

```
                          Name der Maßnahmendomäne: ADMIN_RECORDS
                          Name der Maßnahmengruppe: STANDARD
                            Verwaltungsklassenname: STANDARD
                             Name der Kopiengruppe: STANDARD
                              Typ der Kopiengruppe: Backup
                     Versionen bestehender Daten: 2
                      Versionen gelöschter Daten: 1
                      Extraversionen aufbewahren: 30
                     Einzige Version aufbewahren: 60
                                 Kopienmodus: Modified
                           Kopiennumerierung: Shared Static
                            Kopienhäufigkeit: 0
                               Kopienzielort: BACKUPPOOL
           Zielort für Inhaltsverzeichnis:
              Letzte Aktualisierung durch
                                 (Administrator): $$CONFIG_MANAGER$$
Datum/Zeit der letzten Aktualisierung: 2002.10.02 17.51.49
                            Verwaltendes Profil: ADMIN_INFO
                          Änderungen anstehend: Yes
```

Beispiel: Informationen zu einer Archivierungskopiengruppe anzeigen

Von einem verwalteten Server die vollständigen Informationen über die Archivierungskopiengruppe STANDARD anzeigen, die der Verwaltungsklasse MCLASS1 in der Maßnahmengruppe SUMMER der Maßnahmendomäne PROG1 zugeordnet ist. Den folgenden Befehl ausgeben:

```
query copygroup prog1 summer mclass1
type=archive format=detailed
```

```
                         Name der Maßnahmendomäne: PROG1
                         Name der Maßnahmengruppe: SUMMER
                      Name der Verwaltungsklasse: MCLASS1
                           Name der Kopiengruppe: STANDARD
                            Typ der Kopiengruppe: Archive
                              Version aufbewahren: 730
                               Aufbewahrungsstart: Creation
                              Mindestaufbewahrung:
                                 Kopiennumerierung: Shared Static
                                  Kopienhäufigkeit: Cmd
                                       Kopienmodus: Absolute
                                     Kopienzielort: ARCHPOOL
                    Letzte Aktualisierung durch
                                 (Administrator): $$CONFIG_MANAGER$$
          Datum/Zeit der letzten Aktualisierung: 2002.10.02 17.42.49
                              Verwaltendes Profil: ADMIN_INFO
```

Beispiel: Informationen zu der Kopiengruppe für eine NAS-Sicherung anzeigen

Die Kopiengruppe für die NAS-Sicherung abfragen. Den folgenden Befehl ausgeben:

```
query copygroup nasdomain
 type=backup
```

```
               Name der Maßnahmendomäne: NASDOMAIN
                         Name der Maßnahmengruppe: ACTIVE
                           Verwaltungsklassenname: STANDARD
                            Name der Kopiengruppe: STANDARD
                             Typ der Kopiengruppe: Backup
                    Versionen bestehender Daten: 2
                     Versionen gelöschter Daten: 1
                     Extraversionen aufbewahren: 30
                    Einzige Version aufbewahren: 60
                                 Kopienmodus: Modified
                            Kopiennumerierung: Shared Static
                             Kopienhäufigkeit: 0
                                Kopienzielort: NASPOOL
             Zielort für Inhaltsverzeichnis: BACKUPPOOL
    Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
          Datum/Zeit der letzten Aktualisierung: 10/02/2002 12:16:52
                              Verwaltendes Profil:
                           Änderungen anstehend: Yes
```

Feldbeschreibungen

Name der Maßnahmendomäne
: Der Name der Maßnahmendomäne.

Name der Maßnahmengruppe
: Der Name der Maßnahmengruppe.

Name der Verwaltungsklasse
: Der Name der Verwaltungsklasse.

Name der Kopiengruppe
: Der Name der Kopiengruppe. Dieser Name lautet immer STANDARD.

Typ der Kopiengruppe
: Der Typ der Kopiengruppe.

Versionen bestehender Daten
: Die maximale Anzahl Sicherungsversionen, die für Dateien aufbewahrt werden sollen, die sich momentan im Clientdateisystem befinden.

Versionen gelöschter Daten
: Die maximale Anzahl Sicherungsversionen, die für Dateien aufbewahrt werden sollen, die aus dem Clientdateisystem gelöscht wurden, nachdem sie mit IBM Spectrum Protect gesichert wurden.

Extraversionen aufbewahren
: Die Anzahl Tage, die eine Sicherungsversion aufbewahrt werden soll, nachdem diese Version inaktiv wurde.

Einzige Version aufbewahren
: Die Anzahl Tage, die die letzte Sicherungsversion einer Datei aufbewahrt werden soll, die aus dem Clientdateisystem gelöscht wurde.

Kopiennumerierung
: Angabe, ob eine Datei während einer Archivierungsoperation verwendet werden darf.

Kopienhäufigkeit
: Die Kopienhäufigkeit der Kopiengruppe. Bei Archivierungskopiengruppen lautet dieser Wert immer CMD.

Kopienmodus

Gibt an, daß Dateien in der Kopiengruppe ohne Rücksicht darauf, ob sie geändert wurden, archiviert werden sollen. Bei Archivierungskopiengruppen lautet dieser Wert immer ABSOLUTE.

Kopienzielort
: Der Name des Speicherpools, in dem der Server Dateien anfänglich speichert, die dieser Archivierungskopiengruppe zugeordnet sind.

Zielort für Inhaltsverzeichnis
: Der Name des primären Speicherpools, in dem Inhaltsverzeichnisse für Imagesicherungsoperationen anfänglich gespeichert werden, bei denen die Generierung eines Inhaltsverzeichnisses angefordert wird.

Letzte Aktualisierung durch (Administrator)
: Der Name des Administrators oder Servers, der die Kopiengruppe zuletzt aktualisiert hat. Enthält dieses Feld $$CONFIG_MANAGER$$, ist die Kopiengruppe einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der die Kopiengruppe definiert oder zuletzt aktualisiert wurde.

Verwaltendes Profil
: Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition dieser Maßnahmengruppe zu erhalten.

Änderungen anstehend
: Angabe, ob Änderungen vorgenommen, aber nicht aktiviert werden. Sobald die Änderungen aktiviert werden, wird das Feld auf No zurückgesetzt.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY COPYGROUP

Befehl	Beschreibung
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DELETE COPYGROUP	Löscht eine Sicherungs- oder Archivierungskopiengruppe aus einer Maßnahmendomäne und Maßnahmengruppe.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

QUERY DAMAGED (Beschädigte Daten in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool abfragen)

Mit diesem Befehl können Informationen zu beschädigten Datenbereichen in einem Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool angezeigt werden. Verwenden Sie diesen Befehl zusammen mit dem Befehl AUDIT CONTAINER, um eine Wiederherstellungsmethode für die beschädigten Daten festzulegen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                            .-Type--=--Status---------------.
>>-Query DAMaged--Poolname--+-------------------------------+--><
                            '-Type--=--+-INVentory--------+-'
                                       +-Node--| A |------+
                                       '-CONTAiner--| A |-'

A (Zusätzlicher Filter nach Knotenname)

|--+-------------------------+---------------------------------|
   '-Nodename--=--Knotenname-'
```

Parameter

Poolname (Erforderlich)
: Gibt den Namen des Verzeichniscontainer- oder Cloudspeicherpools an.

Type
: Gibt den Typ der Informationen an, die angezeigt werden sollen. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

  Status
  : Gibt an, dass Informationen zu beschädigten Datenbereichen angezeigt werden. Für Cloudspeicherpools werden auch verwaiste Bereiche angezeigt. Dies ist der Standardwert.

  Knoten

Gibt an, dass Informationen zur Anzahl beschädigter Dateien pro Knoten angezeigt werden sollen.

INVentory
: Gibt an, dass Informationen zum Bestand für jede beschädigte Datei angezeigt werden.

CONTAiner
: Gibt an, dass die Container, die beschädigte Datenbereiche oder verwaiste Bereiche in Cloudspeicherpools enthalten, angezeigt werden. Für Verzeichniscontainerspeicherpools werden auch Speicherpoolverzeichnisse angezeigt.

Nodename
: Gibt an, dass Informationen zu beschädigten Dateien für einen einzelnen Knoten angezeigt werden.
Einschränkung: Sie können diesen Parameter nicht angeben, wenn der Parameter TYPE=CONTAINER oder TYPE=STATUS angegeben wird.

Beispiel: Statusinformationen zu beschädigten oder verwaisten Datenbereichen anzeigen

Informationen zum Status beschädigter Datenbereiche anzeigen, die in einem Container gespeichert sind.

```
query damaged pool1 type=status

Speicherpool-    Anzahl nicht      Anzahl         Anzahl verwaister
name             deduplizierter    deduplizierter Bereiche in Cloud-
                 Datenbereiche     Datenbereiche  speicherpools
---------------  -------------     ----------     -------------
POOL1                  58               145
```

Für Cloudspeicherpools wird auch die Anzahl verwaister Bereiche angezeigt.

```
Speicherpool-    Anzahl nicht      Anzahl         Anzahl verwaister
name             deduplizierter    deduplizierter Bereiche in Cloud-
                 Datenbereiche     Datenbereiche  speicherpools
---------------  -------------     ----------     -------------
POOL1                  65               238           18
```

Beispiel: Informationen zu einer beschädigten Datei für einen Knotentyp anzeigen

Informationen zu beschädigten Dateien anzeigen, die in einem Knoten gespeichert werden.

```
query damaged pool1 type=node

Knotenname          Anzahl beschädigter
                    Dateien
-------------  -----------------
POOL1                  37
```

Beispiel: Informationen zu einer beschädigten Datei für einen Bestandstyp anzeigen

Informationen zu beschädigten Dateien anzeigen, die in einem Bestand gespeichert werden.

```
query damaged pool2 type=inventory

       Dateiname des Clients: /data/files/10.out
                                 Typ: Bkup
                          Knotenname: NODE1
                      Dateibereichsname: /data/space
                                Status: Available
                         Einfügezeit: 01/19/2015 16:01:35
                           Objekt-ID: 2073
```

Beispiel: Informationen zu einer beschädigten Datei für einen Containertyp anzeigen

Informationen zu beschädigten Dateien anzeigen, die in einem Container gespeichert werden.

```
query damaged pool3 type=container

         Verzeichnis-ID: 1
            Verzeichnis: /abc/space/container1
              Container: /abc/space/container1/00/0000000000000022.dcf
                 Status: Unavailable
```

Für Cloud-Container wird nur der Name des Containers angezeigt.

```
         Verzeichnis-ID:
            Verzeichnis:
              Container: ibmsp.12520ae05b4011e613320a0027000000/
                         001-10006a3278bc34f0e4118a850090fa3dcb48/
                         00000000000001.ncf
                 Status:
```

Für den lokalen Speicher werden die folgenden Informationen zu einem beschädigten Container angezeigt.

```
Verzeichnis-ID: 1
   Verzeichnis: localdirectory
     Container: localdirectory/00/00000000000011.ncf
        Status: Unavailable
```

Feldbeschreibungen

Dateiname des Clients (nur bei TYPE=INVENTORY)
: Der Name der Datei.

Anzahl verwaister Bereiche in Cloudspeicherpools (nur bei TYPE=STATUS)
: Die Anzahl verwaister Bereiche in einem Cloudspeicherpool. Bereiche werden als verwaist betrachtet, wenn sie keinen entsprechenden Datenbankeintrag haben.

Container (nur bei TYPE=CONTAINER)
: Der Name des Containers.

Anzahl deduplizierter Bereiche (nur bei TYPE=STATUS)
: Die Anzahl beschädigter Bereiche im Speicherpool für deduplizierte Daten.

Verzeichnis (nur bei TYPE=CONTAINER)
: Der Name des Speicherpoolverzeichnisses.

Verzeichnis-ID (nur bei TYPE=CONTAINER)
: Die Identifikationsnummer des Speicherpoolverzeichnisses.

Dateibereichsname (nur bei TYPE=INVENTORY)
: Der Name des Dateibereichs.

Einfügezeit (nur bei TYPE=INVENTORY)
: Das Datum und die Uhrzeit, an dem bzw. zu der das Objekt auf dem Server gespeichert wurde.

Knotenname (nur bei TYPE=INVENTORY oder TYPE=NODE)
: Der Name des Knotens.

Anzahl nicht deduplizierter Bereiche (nur bei TYPE=STATUS)
: Die Anzahl beschädigter Bereiche im Speicherpool für nicht deduplizierte Daten, wie beispielsweise Metadaten und vom Client verschlüsselte Daten.

Anzahl beschädigter Dateien (nur bei TYPE=NODE)
: Die Anzahl beschädigter Dateien pro Knoten.

Objekt-ID (nur bei TYPE=INVENTORY)
: Die Identifikationsnummer des Objekts.

Status (nur bei TYPE=INVENTORY oder TYPE=CONTAINER)
: Der Status der Daten im Bestand oder Container, abhängig vom Typ der Daten, die abgefragt werden. Das Feld kann einen der folgenden Werte enthalten:

  Active
  : Die Version der Datei im Bestand ist aktiv. Es kann nur eine aktive Version der Datei im Bestand vorhanden sein.

  Inactive
  : Die Version der Datei im Bestand ist inaktiv. Es können mehrere inaktive Versionen der Datei im Bestand vorhanden sein.

  Available
  : Der Status des Containers ist 'verfügbar'.

  Unavailable
  : Der Status des Containers ist 'nicht verfügbar'. Beispielsweise kann ein Container nicht verfügbar sein, wenn der Header beschädigt ist oder der Container nicht geöffnet werden kann.

  Read-Only
  : Der Container hat den Status 'Nur lesen'. Daten in dem Container können gelesen werden, aber es können keine Daten in den Container geschrieben werden.

  Pending
  : Das Löschen des Containers ist anstehend. Der Inhalt des Containers wurde in einen anderen Container versetzt und der Container kann jetzt gelöscht werden.

Typ (nur bei TYPE=INVENTORY)
: Der Typ der Daten in der Datei.

Tabelle 1. Zugehörige Befehle für QUERY DAMAGED

Befehl	Beschreibung
AUDIT CONTAINER	Prüft einen Verzeichniscontainerspeicherpool.
QUERY CLEANUP	Fragt den Bereinigungsstatus eines Quellenspeicherpools ab.
QUERY CONTAINER	Zeigt Informationen zu einem Container an.

Befehl	Beschreibung
REMOVE DAMAGED	Entfernt beschädigte Daten aus einem Quellenspeicherpool.

QUERY DATAMOVER (Definitionen der Einheit zum Versetzen von Daten anzeigen)

Verwenden Sie diesen Befehl, um Definitionen der Einheit zum Versetzen von Daten anzuzeigen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query DATAMover-------------------------------------------->

   .-*---------------------------------------.
>--+-----------------------------------------+----------------->
   '-Name_der_Einheit_zum_Versetzen_von_Daten-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------->
   '-Format--=--+-Standard-+-'
                '-Detailed-'

   .-Type--=--*----------------------.
>--+--------------------------------+------------------------><
   |                          (1) (2) |
   '-Type--=--+-NAS--------+---------'
              +-NASCLUSTER-+
              '-NASVSERVER-'
```

Anmerkungen:

1. Bei `FORMAT=DETAILED` müssen Sie den Parameter TYPE angeben.
2. Sie können `TYPE=NASCLUSTER` und `TYPE=NASVSERVER` nur auf einem AIX-, Linux- oder Windows-Betriebssystem angeben.

Parameter

Name der Einheit zum Versetzen von Daten
: Gibt den Namen der Einheit zum Versetzen von Daten an, die angezeigt werden soll. Sie können mehrere Namen mit einem Platzhalterzeichen angeben. Standardmäßig werden alle Einheiten zum Versetzen von Daten angezeigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD.

  Standard
  : Gibt an, dass Informationen zum Namen und zur Adresse angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Type
: Gibt den Typ der Einheit zum Versetzen von Daten an, die angezeigt werden soll. Wenn Sie `FORMAT=DETAILED` angeben, müssen Sie einen Wert für den Parameter TYPE angeben.

  NAS
  : Gibt einen NAS-Dateiserver an.

  AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeNASCLUSTER
  : AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeGibt einen NAS-Dateiserver in einem Cluster an.

  AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeNASVSERVER
  : AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeGibt eine virtuelle Speichereinheit innerhalb eines Clusters an.

Beispiel: Informationen zu allen Einheiten zum Versetzen von Daten anzeigen

Die Einheiten zum Versetzen von Daten auf dem Server anzeigen. Den folgenden Befehl ausgeben:

```
query datamover

Name der Einheit  Typ der Einheit
zum Versetzen     zum Versetzen
von Daten         von Daten          Online
```

```
-------------     -------------      ------
 NASMOVER1             NAS              Yes
 NASMOVER2             NAS               No
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Informationen zu einer Einheit zum Versetzen von Daten anzeigen

Teilinformationen zu der Einheit zum Versetzen von Daten DATAMOVER6 anzeigen. Den folgenden Befehl ausgeben:

```
query datamover datamover6 type=nas
```

```
 Quellenname      Typ            Online
-------------     -------        ------
DATAMOVER6        NAS            Yes
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Informationen zu einer Einheit zum Versetzen von Daten anzeigen

Ausführliche Informationen zur Einheit zum Versetzen von Daten DATAMOVER6 anzeigen. Der Parameter TYPE ist bei FORMAT = DETAILED erforderlich. Den folgenden Befehl ausgeben:

```
query datamover datamover6 format=detailed type=nas
```

```
               Name der Einheit zum Versetzen von Daten:   DataMover6
                Typ der Einheit zum Versetzen von Daten:   NAS
                                          IP-Adresse:      198.51.100.0
                           TCP/IP-Anschlussnummer:         10000
                                     Benutzername:         NDMPadmin
                           Speicherpooldatenformat:        NDMPDUMP
                                          Online:          Yes
            Letzte Aktualisierung durch (Administrator):   ADMIN
                  Datum/Zeit der letzten Aktualisierung:   05/23/2015 09:26:33
```

Für Feldbeschreibungen siehe Feldbeschreibungen.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Beispiel: Ausführliche Informationen zu einer NAS-Einheit zum Versetzen von Daten in einem Cluster anzeigen

Beispiel: Ausführliche Informationen zu einer NAS-Einheit zum Versetzen von Daten (mit dem Namen CLUSTERA) in einem Cluster anzeigen. Geben Sie den folgenden Befehl aus:

```
query datamover clustera format=detailed type=nascluster
```

```
               Name der Einheit zum Versetzen von Daten:   CLUSTERA
                Typ der Einheit zum Versetzen von Daten:   NASCLUSTER
                                          IP-Adresse:      192.0.2.255
                           TCP/IP-Anschlussnummer:         10000
                                     Benutzername:         ndmp
                           Speicherpooldatenformat:        NETAPPDUMP
                                          Online:          Yes
            Letzte Aktualisierung durch (Administrator):   ADMIN
                  Datum/Zeit der letzten Aktualisierung:   04/28/2015 09:26:33
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Name der Einheit zum Versetzen von Daten
: Gibt den Namen der Einheit zum Versetzen von Daten an.

Typ der Einheit zum Versetzen von Daten
: Gibt den Typ der Einheit zum Versetzen von Daten an.

IP-Adresse
: Gibt die IP-Adresse der Einheit zum Versetzen von Daten an.

TCP/IP-Anschlussnummer
: Gibt die TCP-Anschlussnummer für die Einheit zum Versetzen von Daten an.

Benutzername
: Gibt die Benutzer-ID an, die der Server verwendet, um auf die Einheit zum Versetzen von Daten zuzugreifen.

Speicherpooldatenformat
: Gibt das Datenformat an, das von der Einheit zum Versetzen von Daten verwendet wird.

Online
: Gibt an, ob die Einheit zum Versetzen von Daten online und für die Verwendung verfügbar ist.

Letzte Aktualisierung durch (Administrator)

Gibt die ID des Administrators an, der die letzte Aktualisierung ausgeführt hat.

Datum/Zeit der letzten Aktualisierung
Gibt das Datum und die Uhrzeit der letzten Aktualisierung an.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DATAMOVER

Befehl	Beschreibung
DEFINE DATAMOVER	Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.
DELETE DATAMOVER	Löscht eine Einheit zum Versetzen von Daten.
UPDATE DATAMOVER	Ändert die Definition einer Einheit zum Versetzen von Daten.

QUERY DB (Datenbankinformationen anzeigen)

Mit diesem Befehl können Informationen über die Datenbank angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
             .-Format--=--Standard-----.
>>-Query DB--+-------------------------+----------------------><
             '-Format--=--+-Standard-+-'
                          '-Detailed-'
```

Parameter

Format
Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Die folgenden Werte sind gültig:

Standard
Gibt an, dass Teilinformationen angezeigt werden.

Detailed
Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Übersichtsstatistik zur Datenbank anzeigen

Statistikdaten zur Datenbank anzeigen. Den folgenden Befehl ausgeben:

```
query db
```

```
Datenbank-     Gesamt-      Verwendbare   Belegte     Freie
name           seitenzahl   Seiten        Seiten      Seiten
-------------  -----------  ------------  ----------  ----------
       TSMDB1       32.776        32.504      24.220       8.284
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Datenbankinformationen anzeigen

Ausführliche statistische Informationen zur Datenbank anzeigen. Den folgenden Befehl ausgeben:

```
query db format=detailed
```

```
                                  Datenbankname: TSM_DB2
      Gesamtspeicherbereich des Dateisystems (MB): 1.748.800
    Verwendeter Speicherbereich im Dateisystem (MB): 2.304.355
     Von Datenbank verwendeter Speicherbereich (MB): 448
            Freier verfügbarer Speicherbereich (MB): 235.609
                               Gesamtseitenzahl: 32.776
                            Verwendbare Seiten: 32.504
                                Belegte Seiten: 24.220
                                  Freie Seiten: 8.284
                          Pufferpooltrefferquote: 99,3
```

```
                  Pufferanforderungen insgesamt: 204.121
                              Sortierüberlauf: 0
                         Paketcachetrefferquote: 89,8
                    Letzte Datenbankreorganisation: 05/25/2009 16:44:06
      Einheitenklassenname für Gesamtsicherungen: FILE
           Anzahl Datenbanksicherungsdatenströme: 4
  Teilsicherungen seit letzter Gesamtsicherung: 0
       Datum/Zeit der letzten Gesamtsicherung: 05/18/2009 22:55:19
          Datenbanksicherungen komprimieren: Yes
   Masterverschlüsselungsschlüssel schützen: No
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Datenbankname
: Der Name der Datenbank, die für die Verwendung durch den IBM Spectrum Protect-Server definiert und konfiguriert ist.

 AIX-Betriebssysteme  Linux-BetriebssystemeGesamtspeicherbereich des Dateisystems (MB)
:  AIX-Betriebssysteme  Linux-BetriebssystemeDer Gesamtspeicherbereich in Megabyte der Dateisysteme, in denen sich die Datenbank befindet.

 Windows-BetriebssystemeGesamtspeicherbereich des Dateisystems (MB)
:  Windows-BetriebssystemeDer Gesamtspeicherbereich in Megabyte der Laufwerke, auf denen sich die Datenbank befindet.

Verwendeter Speicherbereich im Dateisystem (MB)
: Der Datenbankbereich in Megabyte, der verwendet wird.

Von der Datenbank verwendeter Speicherbereich (MB)
: Die Größe der Datenbank in Megabyte. Der Wert schließt keinen Tabellenbereich für temporäre Tabellen ein. Die Größe der Datenbank wird anhand der Größe des Speicherbereichs berechnet, der auf dem Dateisystem, das die Datenbank enthält, belegt ist.

Freier verfügbarer Speicherbereich (MB)
: Der Datenbankbereich in Megabyte, der nicht verwendet wird.

Gesamtseitenzahl
: Die Gesamtzahl der Seiten im Tabellenbereich.

Verwendbare Seiten
: Die Anzahl der verwendbaren Seiten im Tabellenbereich.

Belegte Seiten
: Die Anzahl der belegten Seiten im Tabellenbereich.

Freie Seiten
: Die Gesamtzahl der freien Seiten in allen Tabellenbereichen. Die IBM Spectrum Protect-Datenbank hat bis zu 10 Tabellenbereiche.

Pufferpooltrefferquote
: Die Gesamttrefferquote in Prozent.

Pufferanforderungen insgesamt
: Die Gesamtzahl der logischen Lesevorgänge für Pufferpooldaten und der logischen Lesevorgänge für Indexeinträge seit dem letzten Start der Datenbank oder seit dem Zurücksetzen des Datenbankmonitors.

Sortierüberlauf
: Die Gesamtzahl der Sortiervorgänge, die den Sortierspeicher überschritten haben und möglicherweise Plattenspeicherplatz für temporären Speicher erfordert haben.

Paketcachetrefferquote
: Ein Prozentsatz, der angibt, in welchem Umfang der Paketcache hilft, das erneute Laden von Paketen und Abschnitten für statisches SQL aus den Systemkatalogen zu vermeiden. Außerdem gibt der Prozentsatz an, inwieweit der Paketcache dabei hilft, das erneute Kompilieren von Anweisungen für dynamisches SQL zu vermeiden. Eine hohe Trefferquote gibt eine erfolgreiche Unterstützung bei der Vermeidung dieser Aktivitäten an.

Letzte Datenbankreorganisation
: Der Zeitpunkt, zu dem der Datenbankmanager zuletzt eine automatische Reorganisationsaktivität ausgeführt hat.

Einheitenklassenname für Gesamtsicherungen
: Der Name der Einheitenklasse, die für Datenbankgesamtsicherungen verwendet wird.

Anzahl Datenbanksicherungsdatenströme
: Die Anzahl der parallelen Datenversetzungsdatenströme, die während der Datenbanksicherung verwendet wurden.

Teilsicherungen seit letzter Gesamtsicherung
: Die Anzahl der Teilsicherungen, die seit der letzten Gesamtsicherung ausgeführt wurden.

Datum/Zeit der letzten Gesamtsicherung
: Das Datum und die Uhrzeit der letzten Gesamtsicherung.

Datenbanksicherungen komprimieren
: Gibt an, ob Datenbanksicherungen komprimiert werden.

Masterverschlüsselungsschlüssel schützen
: Gibt an, ob Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels des Servers einschließen.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DB

Befehl	Beschreibung

Befehl	Beschreibung
BACKUP DB	Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff.
EXTEND DBSPACE	Fügt Verzeichnisse hinzu, um den Speicherbereich für die Verwendung durch die Datenbank zu vergrößern.
QUERY DBSPACE	Zeigt Informationen zum Speicherplatz an, der für die Datenbank definiert ist.

QUERY DBSPACE (Datenbankspeicherbereich anzeigen)

Verwenden Sie diesen Befehl, um Informationen zu den Verzeichnissen anzuzeigen, die von der Datenbank zum Speichern von Daten verwendet werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-QUERY DBSpace-----------------------------------------------><
```

Parameter

Keine.

Beispiel: Informationen zum Datenbankspeicherbereich anzeigen

Informationen zum Datenbankspeicherbereich anzeigen. Den folgenden Befehl ausgeben:

```
query dbspace
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
Position             Gesamtspeicherber. Verw. Sp.-Ber.    Freier verfügbarer
                     des Dateisystems   im Dateisystem    Speicherbereich
                     (MB)               (MB)              (MB)
-----------------  ----------------   ---------------   --------------
/tsmdb001                  1,748,800    1,513,191.125       117,804.422
/tsmdb002                  1.748.800      1.513.191,125       117.804,422
```

 Windows-Betriebssysteme

```
Position             Gesamtspeicherber. Verw. Sp.-Ber.    Freier verfügbarer
                     des Dateisystems   im Dateisystem    Speicherbereich
                     (MB)               (MB)              (MB)
----------------   ----------------   ---------------   --------------
d:\tsm\db001         1.748.800            1.513.191,125              117.804,422
e:\tsm\db002         1.748.800            1.513.191,125              117.804,422
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Position
: Gibt die Positionen der Datenbankverzeichnisse an.

 AIX-BetriebssystemeGesamtspeicherbereich des Dateisystems (MB)
:  AIX-BetriebssystemeDer Gesamtspeicherbereich in Megabyte des Dateisystems, in dem sich die Datenbank befindet.

 Windows-BetriebssystemeGesamtspeicherbereich des Dateisystems (MB)
:  Windows-BetriebssystemeDer Gesamtspeicherbereich in Megabyte der Laufwerke, auf denen sich die Datenbank befindet.

Verwendeter Speicherbereich im Dateisystem (MB)
: Der Speicherbereich in Megabyte, der verwendet wird.

   AIX-Betriebssysteme  Linux-BetriebssystemeWenn Sie den Befehl QUERY DBSPACE ausführen, kann der Wert in der Ausgabe größer als der Wert sein, den Sie bei der Ausführung des Systembefehls df erhalten. Die Ausgabe des Systembefehls df enthält nicht den Speicherbereich, der für den Rootbenutzer reserviert ist.

   Linux-BetriebssystemeWenn Sie den Systembefehl df ausführen, beträgt der Standardprozentsatz des Speicherbereichs, der für den Rootbenutzer reserviert ist, 5 %. Sie können diesen Standardwert ändern.

Freier verfügbarer Speicherbereich (MB)
: Der Speicherbereich in Megabyte, der nicht verwendet wird.

Windows-BetriebssystemeFreier verfügbarer Speicherbereich (MB)
: Windows-BetriebssystemeDer Speicherbereich, der auf dem Laufwerk verbleibt, auf dem sich das Verzeichnis befindet.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DBSPACE

Befehl	Beschreibung
BACKUP DB	Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff.
EXTEND DBSPACE	Fügt Verzeichnisse hinzu, um den Speicherbereich für die Verwendung durch die Datenbank zu vergrößern.
QUERY DB	Zeigt Zuordnungsinformationen zu der Datenbank an.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

QUERY DEDUPSTATS (Datendeduplizierungsstatistikdaten abfragen)

Verwenden Sie diesen Befehl, um Informationen zu Datendeduplizierungsstatistikdaten für einen Verzeichniscontainerspeicherpool oder einen Cloudspeicherpool anzuzeigen.

Sie müssen den Befehl GENERATE DEDUPSTATS ausgeben, bevor Sie den Befehl QUERY DEDUPSTATS ausgeben können.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query DEDUPSTats--+----------+--+------------+--------------->
                     '-Poolname-'  '-Knotenname-'

   .-*--------------------.  .-Format--=--Standard-----.
>--+----------------------+--+-------------------------+------->
   | .-,-----------------. |  '-Format--=--+-Standard-+-'
   | V                   | |               '-Detailed-'
   +---Dateibereichsname-+-+
   | .-,---------.         |
   | V           |         |
   '-----FSID----+---------'

   .-CODEType--=--BOTH-----------.
>--+-----------------------------+------------------------------>
   '-CODEType--=--+-UNIcode----+-'
                  +-NONUNIcode-+
                  '-BOTH-------'

   .-NAMEType--=--SERVER------.
>--+--------------------------+--+--------------------+-------->
   '-NAMEType--=--+-SERVER--+-'  '-BEGINDate--=--Datum-'
                  +-UNIcode-+
                  '-FSID----'

>--+--------------------+--+-------------------+---------------->
   '-BEGINTime--=--Zeit-'  '-ENDDate--=--Datum-'

                         .-ALLSTats--=--No------.
>--+-------------------+--+----------------------+-------------><
   '-ENDTime--=--Zeit-'  '-ALLSTats--=--+-Yes-+-'
                                        '-No--'
```

Parameter

Poolname
: Gibt den Namen des Verzeichniscontainerspeicherpools an, dessen Daten in den Datendeduplizierungsstatistikdaten enthalten sind. Dieser Parameter ist wahlfrei. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherpools angezeigt. Für den Speicherpoolnamen können bis zu 30 Zeichen angegeben werden. Wenn Sie mehr als 30 Zeichen angeben, schlägt der Befehl fehl. Einschränkung: Sie können nur Verzeichniscontainerspeicherpools oder Cloudspeicherpools angeben.

Knotenname

Gibt den Namen des Clientknotens an, dessen Daten in den Datendeduplizierungsstatistikdaten enthalten sind. Dieser Parameter ist wahlfrei. Wird für diesen Parameter kein Wert angegeben, werden alle Knoten angezeigt. Für den Knotennamen können bis zu 64 Zeichen angegeben werden. Wenn Sie mehr als 64 Zeichen angeben, schlägt der Befehl fehl.

Dateibereichsname oder FSID

Gibt die Namen der Dateibereiche an, die die Daten enthalten, die in den Datendeduplizierungsstatistikdaten berücksichtigt werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden.Wird kein Wert für diesen Parameter angegeben, werden alle Dateibereiche angezeigt. Es können mehrere Dateibereiche angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.
Für einen Server, der über Clients mit Unterstützung für Dateibereiche im Unicode-Format verfügt, können Sie entweder einen Dateibereichsnamen oder eine Dateibereichs-ID (FSID) angeben. Wird ein Dateibereichsname eingegeben, muss der Server möglicherweise den eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Zeichenumsetztabelle des Servers in Unicode konvertieren.
Einschränkungen: Die folgenden Einschränkungen gelten für Dateibereichsnamen und FSIDs:

- Ein Knotenname muss angegeben werden, wenn ein Dateibereichsname angegeben wird.
- Mischen Sie nicht Dateibereichsnamen und FSIDs in demselben Befehl.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

Standard
: Gibt an, dass Teilinformationen für die angegebenen Datendeduplizierungsgruppen angezeigt werden. Dies ist der Standardwert.

Detailed
: Gibt an, dass vollständige Information für die angegebenen Datendeduplizierungsgruppen angezeigt werden.

CODEType

Geben Sie an, welcher Typ von Dateibereichen in der Operation berücksichtigt werden soll. Der Standardwert lautet BOTH. Dieser Standardwert gibt an, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Geben Sie einen der folgenden Werte an:

UNIcode
: Dateibereiche einschließen, die ein Unicode-Format haben.

NONUNIcode
: Dateibereiche einschließen, die kein Unicode-Format haben.

BOTH
: Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen. Dies ist der Standardwert.

NAMEType

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Dateibereiche im Unicode-Format verfügt. Sie können diesen Parameter für IBM Spectrum Protect-Clients angeben, die die Betriebssysteme Windows, NetWare oder Macintosh OS X verwenden.
Verwenden Sie diesen Parameter nur, wenn Sie einen Knotennamen und einen Dateibereichsnamen oder eine FSID eingeben.
Einschränkung: Wenn Sie diesen Parameter angeben, darf der Dateibereichsname kein Platzhalterzeichen enthalten.

Geben Sie einen der folgenden Werte an:

SERVER
: Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren. Dies ist der Standardwert.

UNIcode
: Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

FSID
: Der Server interpretiert die Dateibereichsnamen als ihre FSIDs.

BEGINDate

Gibt das Startdatum zum Abfragen von Datendeduplizierungsstatistikdaten an. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Anfangsdatum ohne eine Anfangszeit angegeben, lautet die Zeit 24:00 (Mitternacht) an dem angegebenen Datum.
Einschränkung: Sie können diesen Parameter nur angeben, wenn Sie den Parameter ALLSTATS=YES angeben.
Geben Sie einen der folgenden Werte an:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum.	09/15/2015
TODAY	Das aktuelle Datum.	TODAY
TODAY-Tage oder -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage.	TODAY -3 oder -3.

Wert	Beschreibung	Beispiel
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Sätze einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Sätze einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt die Startzeit zum Abfragen der Datendeduplizierungsstatistikdaten an. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter BEGINDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Anfangszeit ohne ein Anfangsdatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Uhrzeit.
Einschränkung: Sie können diesen Parameter nur angeben, wenn Sie den Parameter ALLSTATS=YES angeben.
Geben Sie einen der folgenden Werte an:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit.	10:30:08
NOW	Die aktuelle Uhrzeit.	NOW
NOW+HH:MM oder +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten.	NOW+02:00 oder +02:00.
NOW-HH:MM oder -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten.	NOW-02:00 oder –02:00.

ENDDate

Gibt das Enddatum zum Abfragen von Datendeduplizierungsstatistikdaten an. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Enddatum ohne eine Endzeit angegeben, lautet die Zeit 23:59:59 am angegebenen Enddatum.
Einschränkung: Sie können diesen Parameter nur angeben, wenn Sie den Parameter ALLSTATS=YES angeben.
Geben Sie einen der folgenden Werte an:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1999
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage oder -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage.	TODAY -3 oder -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Sätze einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Sätze einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDTime

Gibt die Endzeit des Bereichs an, für den die Datendeduplizierungsstatistikdaten abgefragt werden sollen. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Endzeit ohne ein Enddatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Zeit.
Einschränkung: Sie können diesen Parameter nur angeben, wenn Sie den Parameter ALLSTATS=YES angeben.
Geben Sie einen der folgenden Werte an:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit.	10:30:08
NOW	Die aktuelle Uhrzeit.	NOW

Wert	Beschreibung	Beispiel
NOW+HH:MM oder +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum	NOW+02:00 oder +02:00.
NOW-HH:MM oder -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum	NOW-02:00 oder -02:00.

ALLSTats
: Gibt an, ob alle Datendeduplizierungsstatistikdaten oder nur die zuletzt generierten Datendeduplizierungsstatistikdaten angezeigt werden sollen. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

  No
  : Zeigt nur die zuletzt generierten Datendeduplizierungsstatistikdaten für jeden Knoten und Dateibereich an.

  Yes
  : Zeigt alle Datendeduplizierungsstatistikdaten an.

Beispiel: Datendeduplizierungsstatistikdaten im Standardformat anzeigen

Datendeduplizierungsstatistikdaten für einen Speicherpool mit dem Namen POOL1 anzeigen. Die Datendeduplizierungsstatistikdaten gelten für den Knoten NODE1; es werden die Statistikdaten vom 8. Mai 2015 angezeigt. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query dedupstats pool1 node1 begindate=05/08/2015
```

```
                                          Datum/Zeit: 05/05/2015 15:15:23
                                      Speicherpoolname: POOL1
                                            Knotenname: NODE1
                                     Dateibereichsname: \\fs1\a1
                                                  FSID: 41
                                                   Typ: Bkup
                            Gesamteinsparung in Prozent: 86,62
                         Geschützte Daten insgesamt (MB): 311
```

Beispiel: Ausführliche Datendeduplizierungsstatistikdaten anzeigen

Ausführliche Informationen zur Datendeduplizierung für einen Speicherpool mit dem Namen POOL1 anzeigen.

```
query dedupstats pool1 format=detailed
```

```
                                          Datum/Zeit: 05/05/2015 15:15:23
                                      Speicherpoolname: POOL1
                                            Knotenname: NODE1
                                     Dateibereichsname: \\fs1\a1
                                                  FSID: 41
                                                   Typ: Bkup
                         Geschützte Daten insgesamt (MB): 47.646
                      Gesamtspeicherbereichsbelegung (MB): 10.139
                  Eingesparter Gesamtspeicherbereich (MB): 37.507
                              Gesamteinsparung in Prozent: 78,72
                              Deduplizierungseinsparungen: 21.278.892.501
                                Deduplizierung in Prozent: 42,59
                    Anzahl nicht deduplizierter Bereiche: 1.658
Von nicht deduplizierten Bereichen belegter Speicherbereich: 732.626
                              Anzahl eindeutiger Bereiche: 189.791
           Vom eindeutigen Bereich belegter Speicherbereich: 23.385.014.635
                       Anzahl gemeinsam genutzter Bereiche: 178.712
                 Geschützte gemeinsam genutzte Datenbereiche: 26.575.010.669
          Von gemeinsam genutzten Bereichen belegter Speicherbereich: 5.267.815.421
                               Komprimierungseinsparungen: 5.267.815.421
                                 Komprimierung in Prozent: 62,93
                             Anzahl komprimierter Bereiche: 352.498
                          Anzahl nicht komprimierter Bereiche: 17.663
      Von verschlüsselten Bereichen belegter Speicherbereich: 52.901.672
                               Verschlüsselung in Prozent: 100,00
                            Anzahl verschlüsselter Bereiche: 188
                         Anzahl nicht verschlüsselter Bereiche: 0
```

Feldbeschreibungen

Datum/Zeit
: Zeigt das Datum und die Uhrzeit an, am dem bzw. zu der die Datendeduplizierungsstatistikdaten generiert werden.

Speicherpoolname
: Der Name des Speicherpools.

Knotenname
: Der Name des Clientknotens, dessen Daten in den Datendeduplizierungsstatistikdaten enthalten sind.

Dateibereichsname

Der Name des Dateibereichs.

FSID
: Der Name der Dateibereichs-ID.

Typ
: Der Datentyp. Die folgenden Werte sind gültig:

  Arch
  : Daten, die archiviert wurden.

  Bkup
  : Daten, die gesichert wurden.

  SpMg
  : Daten, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Geschützte Daten insgesamt (MB)
: Das logische Datenvolumen (in Megabyte), das im Speicherpool geschützt wird, vor der Datendeduplizierung und -komprimierung. Dieser Wert stellt die Summe der Werte für Gesamtspeicherbereichsbelegung (MB) und Eingesparter Gesamtspeicherbereich (MB) dar.

Gesamtspeicherbereichsbelegung (MB)
: Der im Speicherpool belegte Gesamtspeicherbereich in Megabyte. Dieser Wert ist das physische Datenvolumen, das nach der Datendeduplizierung und -komprimierung gesichert wird.

Eingesparter Gesamtspeicherbereich (MB)
: Der Gesamtspeicherbereich in Megabyte der Daten, die aufgrund der Datendeduplizierung und Komprimierung aus dem Speicherpool entfernt werden. Dieser Wert stellt die Summe der Werte für Deduplizierungseinsparungen und Komprimierungseinsparungen dar.

Gesamteinsparung in Prozent
: Der Prozentsatz der Daten, die aufgrund der Komprimierung und Datendeduplizierung aus dem Speicherpool entfernt werden.

Deduplizierungseinsparungen
: Der Umfang des belegten Speicherbereichs, der im Speicherpool aufgrund der Datendeduplizierung eingespart wird.

Deduplizierung in Prozent
: Der Prozentsatz der Daten, die aufgrund der Datendeduplizierung aus dem Speicherpool entfernt werden.

Anzahl nicht deduplizierter Bereiche
: Die Anzahl nicht deduplizierter Datenbereiche im Speicherpool.

Von nicht deduplizierten Bereichen belegter Speicherbereich
: Der Umfang des Speicherbereichs, der von Datenbereichen belegt wird, die im Speicherpool nicht dedupliziert werden. Dieser Wert gilt Container mit dem Dateityp .ncf, die keine deduplizierten Daten enthalten.
  Tipp: Datenbereiche, die nicht dedupliziert sind, bestehen aus den folgenden Daten- oder Dateitypen:

  - Dateimetadaten
  - Dateien mit einer Größe von weniger als 2 KB
  - Dateien, die die Clientverschlüsselung verwenden

Anzahl eindeutiger Bereiche
: Die Anzahl Datenbereiche, die nicht von einem Knoten gemeinsam genutzt werden.

Vom eindeutigen Bereich belegter Speicherbereich
: Der Umfang des Speicherbereichs im Speicherpool, der von einem Knoten nicht gemeinsam genutzt wird. Dieser Wert gilt Container mit dem Dateityp .dcf, die keine deduplizierten Daten enthalten.

Anzahl gemeinsam genutzter Bereiche
: Die Anzahl Datenbereiche, die aufgrund der Datendeduplizierung mehrmals von demselben Knoten oder von unterschiedlichen Knoten verwendet werden.

Geschützte gemeinsam genutzte Datenbereiche
: Der Umfang des Speicherbereichs im Speicherpool, der von gemeinsam genutzten Datenbereichen schützt wird, vor der Datendeduplizierung.

Von gemeinsam genutzten Bereichen belegter Speicherbereich
: Der Umfang des Speicherbereichs im Speicherpool, der von gemeinsam genutzten Datenbereichen belegt ist, nach der Datendeduplizierung.

Komprimierungseinsparungen
: Der Umfang des belegten Speicherbereichs, der im Speicherpool aufgrund einer Komprimierung nach der Datendeduplizierung eingespart wird.

Komprimierung in Prozent
: Der Prozentsatz der Daten, die aufgrund der Komprimierung aus dem Speicherpool entfernt werden.

Anzahl komprimierter Bereiche
: Die Anzahl der komprimierten Datenbereiche.

Anzahl nicht komprimierter Bereiche
: Die Anzahl der nicht komprimierten Datenbereiche.

Von verschlüsselten Bereichen belegter Speicherbereich
: Der Umfang des Speicherbereichs im Speicherpool, der von verschlüsselten Datenbereichen belegt ist.

Verschlüsselung in Prozent
: Der Prozentsatz der verschlüsselten Daten im Speicherpool.

Anzahl verschlüsselter Bereiche
: Die Anzahl der verschlüsselten Datenbereiche.

Anzahl nicht verschlüsselter Bereiche
: Die Anzahl der nicht verschlüsselten Datenbereiche.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DEDUPSTATS

Befehl	Beschreibung
DELETE DEDUPSTATS	Löscht Datendeduplizierungsstatistikdaten.
GENERATE DEDUPSTATS	Generiert Datendeduplizierungsstatistikdaten.

QUERY DEVCLASS (Informationen über Einheitenklassen anzeigen)

Mit diesem Befehl können Informationen über eine oder mehrere Einheitenklassen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                    .-*---------------------.
>>-Query DEVclass--+-----------------------+---------------------><
                    '-Einheitenklassenname-'

   .-Format--=--Standard-----.
><-+-------------------------+-------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Einheitenklassenname
: Gibt den Namen der abzufragenden Einheitenklasse an. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Einheitenklassen werden angezeigt. Wird für diesen Parameter kein Wert angegeben, werden alle Einheitenklassen angezeigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen für die angegebene Einheitenklasse angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen für die angegebene Einheitenklasse angezeigt werden.

Beispiel: Alle Einheitenklassen auflisten

Informationen über alle Einheitenklassen anzeigen.

```
query devclass
```



```
Einheiten-   Einheiten- Anzahl    Ein-  Format  Gesch./  Grenzwert
klassen-     zugriffs-  Speicher- hei-          Max. Ka- für Ladean-
name         strategie  pools     tentyp        pazität  forderung
                                                  (MB)
-----------  ---------- -------  ------ ------  -------- -----
8MMTAPE      Sequenziell      1  8MM    DRIVE   6.144,0  2
DISK         Wahlfrei         4
PLAINFILES   Sequenziell    1     FILE                  50,0       1
8MMSP2       Sequenziell      2  8MM    DRIVE      44,4  DRIVES
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Informationen zu einer bestimmten Einheitenklasse FILE anzeigen

Ausführliche Informationen über die Einheitenklasse PLAINFILES anzeigen.

```
query devclass plainfiles format=detailed
```

```
                      Einheitenklassenname: PLAINFILES
                   Einheitenzugriffsstrategie: Sequenziell
                         Anzahl Speicherpools: 1
                                 Einheitentyp: FILE
                                       Format:
                   Gesch./Max. Kapazität (MB): 50,0
                     Grenzwert für Ladeanforderung: 1
                          Ladewartezeit (Min):
                              Ladedauer (Min):
                               Kennsatzpräfix:
Windows-Betriebssysteme                                Laufwerkbuchstabe:
                              Kassettenarchiv:
                                  Verzeichnis:
                                   Servername:
                       Wiederholungszeitlimit:
                       Wiederholungsintervall:
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme                                Gemeinsam
benutzt:
AIX-Betriebssysteme Linux-Betriebssysteme       Primäre Bereichszuordnung (MB):
             Sekundäre Bereichszuordnung (MB):
                               Komprimierung:
                      Aufbewahrungszeitraum:
                                     Schutz:
                                Verfallsdatum:
                                      Einheit:
                    Schutz logischer Blöcke:
Letzte Aktualisierung durch (Administrator):   ADMIN
          Datum/Zeit der letzten Aktualisierung: 05/31/2000 13:15:36
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Informationen zu einer bestimmten Einheitenklasse 3592 anzeigen

Ausführliche Informationen zur Einheitenklasse 3592 anzeigen.

```
query devclass 3592 format=detailed
```

```
                         Einheitenklassenname: 3592
                   Einheitenzugriffsstrategie: Sequenziell
                         Anzahl Speicherpools: 1
                                 Einheitentyp: 3592
                                       Format: 3592
                   Gesch./Max. Kapazität (MB):
                     Grenzwert für Ladeanforderung: DRIVES
                          Ladewartezeit (Min): 60
                              Ladedauer (Min): 60
                               Kennsatzpräfix: ADSM
Windows-Betriebssysteme                                Laufwerkbuchstabe:
                              Kassettenarchiv: MANLIB
                                  Verzeichnis:
                                   Servername:
                       Wiederholungszeitlimit:
                       Wiederholungsintervall:
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme                                Gemeinsam
benutzt:
                          Adresse der oberen Ebene:
                                          WORM: No
                             Skalierte Kapazität: 90
                       Laufwerkverschlüsselung: On
AIX-Betriebssysteme Linux-Betriebssysteme       Primäre Bereichszuordnung (MB):
             Sekundäre Bereichszuordnung (MB):
                               Komprimierung:
                      Aufbewahrungszeitraum:
                                     Schutz:
                                Verfallsdatum:
                                      Einheit:
                    Schutz logischer Blöcke: Read/Write
   Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
         Datum/Zeit der letzten Aktualisierung: 08/04/03 14:28:31
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Einheitenklassenname
: Der Name der Einheitenklasse.

Einheitenzugriffsstrategie
: Gibt an, wie Daten in die Einheitenklasse geschrieben werden.

Anzahl Speicherpools

Die Anzahl der Speicherpools, die der Einheitenklasse zugeordnet sind.

Einheitentyp
: Der Einheitentyp der Einheitenklasse.

Format
: Das Aufzeichnungsformat.

Gesch./Max. Kapazität (MB)
: Die geschätzte oder die maximale Kapazität eines Datenträgers, der der Einheitenklasse zugeordnet ist.

Grenzwert für Ladeanforderung
: Die maximale Anzahl Datenträger mit sequenziellem Zugriff, die gleichzeitig geladen sein kann, oder gibt an, dass DRIVES der Grenzwert für Ladeanforderungen ist.

Ladewartezeit (Min)
: Die maximale Wartezeit in Minuten für das Laden eines Datenträgers mit sequenziellem Zugriff.

Ladedauer (Min)
: Die Anzahl Minuten, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten werden soll, bevor er entladen wird.

Kennsatzpräfix
: Die Kennung der oberen Ebene des Dateinamens, die der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt.

Windows-BetriebssystemeLaufwerkbuchstabe
: Windows-BetriebssystemeDer Laufwerkbuchstabe für einen austauschbaren Datenträger.

Kassettenarchiv
: Der Name des definierten Kassettenarchivobjekts, das die von der Einheitenklasse verwendeten Laufwerke enthält.

Verzeichnis
: Das Verzeichnis bzw. die Verzeichnisse für eine gemeinsam benutzte Einheitenklasse FILE.

Servername
: Der Name eines definierten Servers.

Wiederholungszeitlimit
: Das Intervall, in dem der Server versucht, eine Verbindung zu einem Zielserver herzustellen, falls ein Übertragungsfehler vermutet wird.

Wiederholungsintervall
: Gibt an, wie oft die Wiederholungen in einem Wiederholungszeitraum erfolgen.

Gemeinsam benutzt
: Gibt an, ob diese Einheitenklasse FILE von dem Server und von einem oder mehreren Speicheragenten gemeinsam benutzt wird.

Adresse der höheren Ebene
: Die IP-Adresse der Einheit in Schreibweise mit Trennzeichen.

Mindestkapazität
: Die Mindestkapazität eines Datenträgers, der der Einheitenklasse zugeordnet ist.

WORM
: Die Angabe, ob dieses Laufwerk eine WORM-Einheit ist (WORM = Write Once, Read Many).

Laufwerkverschlüsselung
: Die Angabe, ob die Laufwerkverschlüsselung zulässig ist. Dieses Feld gilt nur für Datenträger in einem Speicherpool, dem der Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet ist.

Skalierte Kapazität
: Der Prozentsatz der Datenträgerkapazität, der zum Speichern von Daten verwendet werden kann.

AIX-Betriebssysteme Linux-BetriebssystemePrimäre Bereichszuordnung (MB)
: AIX-Betriebssysteme Linux-BetriebssystemeFür Einheitenklassen FILE, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt den anfänglichen Speicherbereich an, der dynamisch zugeordnet wird, wenn ein neuer Datenträger geöffnet wird.

AIX-Betriebssysteme Linux-BetriebssystemeSekundäre Bereichszuordnung (MB)
: AIX-Betriebssysteme Linux-BetriebssystemeFür Einheitenklassen FILE, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt den Speicherbereich an, um den ein Dateidatenträger erweitert wird, wenn der Speicherbereich, der dem Dateidatenträger bereits zugeordnet ist, verbraucht ist.

AIX-Betriebssysteme Linux-BetriebssystemeKomprimierung
: AIX-Betriebssysteme Linux-BetriebssystemeFür Bandeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt an, ob die Daten komprimiert werden.

AIX-Betriebssysteme Linux-BetriebssystemeAufbewahrungszeitraum
: AIX-Betriebssysteme Linux-BetriebssystemeFür Bandeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll, wenn die Aufbewahrung verwendet wird.

AIX-Betriebssysteme Linux-BetriebssystemeSchutz
: AIX-Betriebssysteme Linux-BetriebssystemeFür Bandeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt an, ob die Datenträger durch das RACF-Programm geschützt werden.

AIX-Betriebssysteme Linux-BetriebssystemeVerfallsdatum
: AIX-Betriebssysteme Linux-BetriebssystemeFür Bandeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt das Verfallsdatum an, das auf Bandkennsätzen für diese Einheitenklasse erscheint, wenn die Verfallsverarbeitung verwendet wird.

AIX-Betriebssysteme Linux-BetriebssystemeEinheit
: AIX-Betriebssysteme Linux-BetriebssystemeFür Bandeinheitenklassen, die Speicher darstellen, der von einem z/OS Media-Server verwaltet wird. Gibt den privaten Einheitennamen für die Gruppe der Bandeinheiten an.

Schutz logischer Blöcke
: Gibt an, ob der Schutz logischer Blöcke aktiviert ist, und gibt den Modus an, wenn dies der Fall ist. Gültige Werte sind 'Read/Write', 'Write-only' und 'No'. Sie können den Schutz logischer Blöcke nur mit den folgenden Typen von Laufwerken und Datenträgern verwenden:

  - IBM® LTO5 und höher

- IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
- Oracle StorageTek T10000C- und T10000D-Laufwerke

Letzte Aktualisierung durch (Administrator)
: Der Administrator, der die letzte Aktualisierung der Einheitenklasse vorgenommen hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit der letzten Aktualisierung.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DEVCLASS

Befehl	Beschreibung
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
AIX-BetriebssystemeLinux-BetriebssystemeDEFINE DEVCLASS (z/OS Media-Server)	AIX-BetriebssystemeLinux-BetriebssystemeDefiniert eine Einheitenklasse für die Verwendung von Speicher, der von einem z/OS Media-Server verwaltet wird.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DELETE DEVCLASS	Löscht eine Einheitenklasse.
QUERY DIRSPACE	Zeigt Informationen zu Verzeichnissen FILE an.
QUERY SERVER	Zeigt Informationen über Server an.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.
AIX-BetriebssystemeLinux-BetriebssystemeUPDATE DEVCLASS (z/OS Media-Server)	AIX-BetriebssystemeLinux-BetriebssystemeÄndert die Attribute einer Einheitenklasse für Speicher, der von einem z/OS Media-Server verwaltet wird.

QUERY DIRSPACE (Speichernutzung von FILE-Verzeichnissen abfragen)

Verwenden Sie diesen Befehl, um Informationen zum freien Speicherbereich in den Verzeichnissen anzuzeigen, die einer Einheitenklasse mit dem Einheitentyp FILE zugeordnet sind.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query DIRSPace--+----------------------+--------------------><
                   '-Einheitenklassenname-'
```

Parameter

Einheitenklassenname
: Gibt den Namen der abzufragenden Einheitenklasse an. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Einheitenklassen mit dem Einheitentyp FILE werden angezeigt. Wird für diesen Parameter kein Wert angegeben, werden alle Einheitenklassen mit dem Einheitentyp FILE angezeigt.

Beispiel: Einheitenklassen des Typs FILE auflisten

Informationen für alle Einheitenklassen mit dem Einheitentyp FILE anzeigen. Im folgenden Beispiel steht M für Megabyte und G für Gigabyte.

```
query dirspace
```

Windows-Betriebssysteme

```
Einheiten-   Verzeichnis                  Geschätzte  Geschätzt
klasse                                    Kapazität   verfügbar
-----------  ---------------------------  ----------  ----------
DBBKUP       /This/is/a/large/directory    13.000 M     5.543 M
DBBKUP       /This/is/directory2           13.000 M     7.123 M
DBBKUP2      /This/is/a/huge/directory      2.256 G     2.200 G
```

Windows-Betriebssysteme

```
Einheiten-   Verzeichnis                   Geschätzte  Geschätzt
klasse                                     Kapazität   verfügbar
-----------  ---------------------------  ----------  ----------
DBBKUP       G:\This\is\a\large\directory    13.000 M     5.543 M
DBBKUP       G:\This\is\directory2           13.000 M     7.123 M
DBBKUP2      G:\This\is\a\huge\directory      2.256 G     2.200 G
```

Feldbeschreibungen

Einheitenklassenname
: Der Name der Einheitenklasse.

Verzeichnis
: Der Pfad des Verzeichnisses auf dem Server.

Geschätzte Kapazität
: Die geschätzte Gesamtkapazität für das Verzeichnis.

Geschätzt verfügbar
: Der geschätzte verbleibende verfügbare Speicherplatz für das Verzeichnis.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DIRSPACE

Befehl	Beschreibung
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
DELETE DEVCLASS	Löscht eine Einheitenklasse.
QUERY DEVCLASS	Zeigt Informationen zu Einheitenklassen an.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.

QUERY DOMAIN (Maßnahmendomäne abfragen)

Mit diesem Befehl können Informationen über eine oder mehrere Maßnahmendomänen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                .-*-----------.  .-Format--=--Standard-----.
>>-Query DOmain--+-------------+--+-------------------------+--><
                '-Domänenname-'  '-Format--=--+-Standard-+-'
                                              '-Detailed-'
```

Parameter

Domänenname
: Gibt die Maßnahmendomäne an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Maßnahmendomänen angezeigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Eine Zusammenfassung der Maßnahmendomänen anzeigen

Teilinformationen für alle Maßnahmendomänen auf dem Server anzeigen. Den folgenden Befehl ausgeben:

```
query domain

Name der     Aktivierte   Aktivierte   Anzahl        Beschreibung
Maßnahmen-   Maßnahmen-   Standard-    registrierter
domäne       gruppe       verwaltungs- Knoten
                          klasse
---------    ---------    ---------    ----------    -----------------
```

```
EMPLOYEE-     VACATION     ACTIVEFI-            6    Employee Records
  _RECORDS                   LES                      Domain
PROG1                                             0    Programming Group
                                                        Test Domain
PROG2                                             0    Programming Group
                                                        Test Domain
STANDARD      STANDARD     STANDARD             1    Installed default
                                                        Maßnahmendomäne
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Die Liste der Pools für aktive Daten anzeigen

Die Liste der Pools für aktive Daten anzeigen. Den folgenden Befehl ausgeben:

```
query domain format=detailed
```

```
                      Name der Maßnahmendomäne: STANDARD
                    Aktivierte Maßnahmengruppe: STANDARD
                       Aktivierungsdatum/-zeit: 05/16/2006 16:18:05
                         Tage seit Aktivierung: 15
           Aktivierte Standardverwaltungsklasse: STANDARD
                    Anzahl registrierter Knoten: 1
                                  Beschreibung: Inst. default policy domain.
            Aufbewahrungszeitraum für Sicherung: 30
         Aufbewahrungszeitraum für Archivierung: 365
    Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
          Datum/Zeit der letzten Aktualisierung: 05/31/2006 15:17:48
                          Verwaltendes Profil:

                      Änderungen anstehend: Yes
               Liste der Pools für aktive Daten: ADPPOOL
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Name der Maßnahmendomäne
: Der Name der Maßnahmendomäne.

Aktivierte Maßnahmengruppe
: Der Name der Maßnahmengruppe, die zuletzt in der Domäne aktiviert wurde.

  Die Definitionen in der letzten aktivierten Maßnahmengruppe und in der AKTIVEN Maßnahmengruppe sind nicht notwendigerweise identisch. Wird eine Maßnahmengruppe aktiviert, kopiert der Server den Inhalt der Maßnahmengruppe in die Maßnahmengruppe mit dem speziellen Namen ACTIVE. Die kopierten Definitionen in der Maßnahmengruppe ACTIVE können nur durch Aktivieren einer anderen Maßnahmengruppe geändert werden. Die ursprüngliche Maßnahmengruppe kann ohne Auswirkungen auf die Maßnahmengruppe ACTIVE geändert werden. Aus diesem Grund sind Definitionen in der Maßnahmengruppe, die zuletzt aktiviert wurde, möglicherweise nicht mit den Definitionen in der Maßnahmengruppe ACTIVE identisch.

Aktivierungsdatum/-zeit
: Das Datum und die Uhrzeit, an dem bzw. zu der die Maßnahmengruppe aktiviert wurde.

Tage seit Aktivierung
: Die Anzahl Tage seit der Aktivierung der Maßnahmengruppe.

Aktivierte Standardverwaltungsklasse
: Die zugeordnete Standardverwaltungsklasse für die Maßnahmengruppe.

Anzahl registrierter Knoten
: Die Anzahl Client-Knoten, die in der Maßnahmendomäne registriert sind.

Beschreibung
: Die Beschreibung der Maßnahmendomäne.

Aufbewahrungszeitraum für Sicherung
: Die Anzahl der Tage, die inaktive Sicherungsversionen von Dateien aufbewahrt werden sollen, wenn eine der folgenden Bedingungen zutrifft:

  - Eine Datei wird an eine neue Verwaltungsklasse erneut gebunden, aber weder die neue Verwaltungsklasse noch die Standardverwaltungsklasse enthält eine Sicherungskopiengruppe.
  - Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden, und die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.
  - Die Sicherungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist, und die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.

Aufbewahrungszeitraum für Archivierung
: Gibt die Anzahl der Tage an, die eine Archivierungsdatei aufbewahrt werden soll, die eine der folgenden Bedingungen erfüllt:

- Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden, und die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.
- Die Archivierungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist, und die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.

Letzte Aktualisierung durch (Administrator)
: Der Administrator, der die Maßnahmendomäne definiert oder zuletzt aktualisiert hat. Enthält dieses Feld $$CONFIG_MANAGER$$, ist die Maßnahmendomäne einem Profil zugeordnet, das von dem Konfigurationsmanager verwaltet wird.

Datum/Zeit der letzten Aktualisierung
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die Maßnahmendomäne definiert oder zuletzt aktualisiert wurde.

Verwaltendes Profil
: Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition dieser Maßnahmendomäne zu erhalten.

Änderungen anstehend
: Angabe, ob Änderungen vorgenommen, aber nicht aktiviert werden. Sobald die Änderungen aktiviert werden, wird das Feld auf No zurückgesetzt.

Liste der Pools für aktive Daten
: Die Liste der Pools für aktive Daten in der Domäne.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DOMAIN

Befehl	Beschreibung
COPY DOMAIN	Erstellt eine Kopie einer Maßnahmendomäne.
DEFINE DOMAIN	Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.
DELETE DOMAIN	Löscht eine Maßnahmendomäne und, falls vorhanden, Maßnahmenobjekte in der Maßnahmendomäne.
UPDATE DOMAIN	Ändert die Attribute einer Maßnahmendomäne.

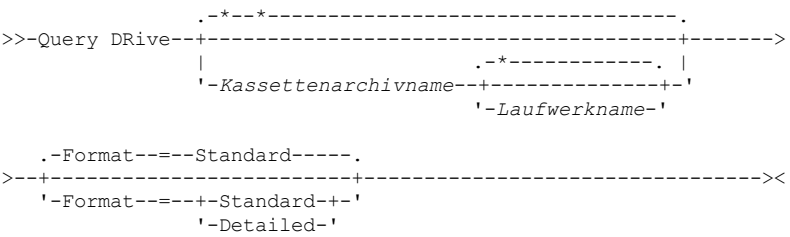
QUERY DRIVE (Informationen über ein Laufwerk abfragen)

Verwenden Sie diesen Befehl, um Informationen über die Laufwerke anzuzeigen, die einem Kassettenarchiv zugeordnet sind.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Kassettenarchivname
: Gibt den Namen des Kassettenarchivs an, in dem sich das abgefragte Laufwerk befindet. Dieser Parameter ist wahlfrei. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

  Sie müssen für diesen Parameter einen Wert angeben, wenn Sie einen Laufwerknamen angeben.

Laufwerkname
: Gibt den Namen an, der dem Laufwerk zugeordnet ist. Dieser Parameter ist wahlfrei. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.Wird ein Laufwerkname angegeben, muss auch ein *Kassettenarchivname* angegeben werden.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, daß Teilinformationen für das Laufwerk angezeigt werden.

Detailed
Gibt an, daß die gesamten Informationen für das Laufwerk angezeigt werden.

Beispiel: Laufwerke auflisten, die dem Server zugeordnet sind

Informationen über alle Laufwerke anzeigen, die dem Server zugeordnet sind. Den folgenden Befehl ausgeben:

```
query drive

Kassetten-  Laufwerk-  Einheiten-  Angehängt
archivname  name       typ
--------  ------   --------  -----
LIB1        DRIVE01    3590        Yes
LIB2        DRIVE02    3590        Yes
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Informationen zu einem bestimmten Laufwerk und Kassettenarchiv anzeigen

Ausführliche Informationen über das Laufwerk DRIVE02 anzeigen, das Kassettenarchiv LIB2 zugeordnet ist. Den folgenden Befehl ausgeben:

```
query drive lib2 drive02 format=detailed

                                  Kassettenarchivname: LIB2
                                        Laufwerkname: DRIVE02
                                        Einheitentyp: 3590
                                              Online: Yes
                                    Laufwerkstatus: Leer
                                     Zugeordnet zu:
          Letzte Aktualisierung durch (Administrator): ADMIN
                    Datum/Zeit der letzten Aktualisierung: 02/29/2002 09:26:23
          Reinigungshäufigk. (Gigabyte/ASNEEDED/NONE): NONE
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Kassettenarchivname
Der Name des Kassettenarchivs, dem das Laufwerk zugeordnet ist.

Laufwerkname
Der Name, der dem Laufwerk zugeordnet ist.

Einheitentyp
Der Einheitentyp, der in der zugehörigen Einheitenklasse angegeben ist. Für den Server muss ein Pfad von dem Server zu dem Laufwerk definiert sein, damit der Server den wahren Einheitentyp bestimmen kann. Solange ein Pfad von dem Server zu dem Laufwerk definiert ist, zeigt der Server den wahren Einheitentyp des Laufwerks an, auch wenn andere Pfade zu diesem Laufwerk definiert sind. Ausnahmen treten auf, wenn der Einheitentyp "remote" oder "unknown" lautet.

REMOTE
Der Server hat keinen Pfad zu der Einheit. Es sind nur Pfade von den Einheiten zum Versetzen von Daten zu der Einheit definiert.

UNKNOWN
Es ist kein Pfad vorhanden.

Tipp: Überprüfen Sie die Ausgabe des Befehls QUERY PATH, um zu bestimmen, ob die gewünschten Pfade definiert sind. Sind sie nicht definiert, definieren Sie die gewünschten Pfade mit dem Befehl DEFINE PATH. Wird eine Einheit zum Versetzen von Daten verwendet, überprüfen Sie auch die Ausgabe des Befehls QUERY DATAMOVER, um den Typ der Einheit zum Versetzen von Daten zu bestimmen. Wird ein Pfad von dem Server zu einem Laufwerk verwendet, müssen die Einheitentypen der Einheitenklasse und des Laufwerks übereinstimmen. Wird ein Pfad von einer Einheit zum Versetzen von Daten zu einem Laufwerk verwendet, lesen Sie die Informationen in der Dokumentation zu Ihrer Einheit zum Versetzen von Daten, um sicherzustellen, dass der Einheitentyp der Einheitenklasse mit dem Typ der Einheit zum Versetzen von Daten kompatibel ist.

Online
Gibt den Status des Laufwerks an:

Yes
Das Laufwerk ist angehängt und für Serveroperationen verfügbar.

No
Das Laufwerk ist abgehängt. Das Laufwerk wurde von einem Administrator, der den Status aktualisiert, in diesen Status gesetzt.

Nicht verfügbar seit
Gibt an, dass das Laufwerk seit *mm/tt/jj hh:mm:ss* nicht verfügbar ist. Die Ausgabe zeigt die Zeit, zu der der Server das Laufwerk als nicht verfügbar markiert hat.

Sendeaufruf seit
Gibt an, daß der Server das Laufwerk aufruft, da das Laufwerk nicht mehr antwortet. Die Ausgabe zeigt die Zeit, zu der der Server einen Fehler erkannt und mit dem Aufrufen des Laufwerks begonnen hat. Der Server ruft ein Laufwerk auf, bevor es als nicht verfügbar markiert wird. Die Zeitausgabe hat das Format: mm/dd/yy hh:mm:ss.

Leseformate
: Die Leseformate für das Laufwerk.

Schreibformate
: Die Schreibformate für das Laufwerk.

Element
: Die Elementnummer für das Laufwerk.

Laufwerkstatus
: Gibt den aktuellen Status dieses spezifischen Laufwerks auf der Basis des Ergebnisses des letzten SCSI-Befehls für das Laufwerk oder Kassettenarchiv an. Der Server verfolgt den Status des Laufwerks, um die Auswahl eines Laufwerks für eine Operation und die Fehlerbehebungsoperationen zu erleichtern. Gültige Werte:

  Unavailable
  : Das Laufwerk steht dem Kassettenarchiv für Operationen nicht zur Verfügung.

  Empty
  : Das Laufwerk ist leer und steht für Operationen zur Verfügung.

  Loaded
  : Das Laufwerk ist gegenwärtig geladen, und der Server führt gerade Operationen mit dem Laufwerk aus.

  Unloaded
  : Der Datenträger wurde vom Laufwerk ausgegeben.

  Reserved
  : Das Laufwerk ist für eine Ladeanforderung reserviert.

  Unknown
  : Das Laufwerk beginnt mit dem Anfangsstatus 'Unbekannt', da es gerade definiert wird, da der Server initialisiert wird oder da sein Status in 'Angehängt' aktualisiert wird.

Datenträgername
: Der Datenträgername für das Laufwerk.

Zugeordnet zu
: Der Name des Kassettenarchiv-Clients, der gegenwärtig das Laufwerk verwendet. Dieses Feld gilt nur für gemeinsam benutzte SCSI-Kassettenarchive; für alle anderen Kassettenarchive bleibt das Feld leer.

WWN
: Der weltweite Name für das Laufwerk.

Letzte Aktualisierung durch (Administrator)
: Gibt an, wer die letzte Aktualisierung des Laufwerks ausgeführt hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit der letzten Aktualisierung.

Reinigungshäufigk. (Gigabyte/ASNEEDED/NONE)
: Gibt an, wie oft der Server die Laufwerkreinigung aktiviert. Dieser Wert kann die Anzahl der Gigabyte, ASNEEDED oder NONE sein.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DRIVE

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE DRIVE	Löscht ein Laufwerk aus einem Kassettenarchiv.
DELETE LIBRARY	Löscht ein Kassettenarchiv.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
UPDATE DRIVE	Ändert die Attribute eines Laufwerks.

QUERY DRMEDIA (Fehlerbehebungsdatenträger abfragen)

Mit diesem Befehl können Informationen zu Datenbanksicherungsdatenträgern und Datenträgern in Kopienspeicherpools, Containerkopienspeicherpools und Speicherpools für aktive Daten angezeigt werden. Der Befehl kann auch verwendet werden, um eine Datei mit ausführbaren Befehlen zu erstellen, um die Datenträger zu verarbeiten.

Die Verarbeitung von Datenträgern durch diesen Befehl hängt vom Verwendungszweck der Datenträger ab:

Sicherungen der Serverdatenbank
: Mit dem Parameter SOURCE kann gesteuert werden, ob der Befehl Datenbanksicherungsdatenträger verarbeitet. Der Befehl kann Datenträger verarbeiten, die für Gesamt- und Teilsicherungen oder Datenbankmomentaufnahmesicherungen verwendet werden. Es

können keine virtuellen Datenträger angegeben werden (Sicherungsobjekte, die auf einem anderen Server gespeichert werden). Datenträger können von Status zu Status geändert werden, oder es können der Parameter TOSTATE verwendet und Status übersprungen werden, um die Bewegungen zu vereinfachen.

Kopienspeicherpools
: Der Befehl QUERY DRMEDIA verarbeitet immer auswählbare Kopienspeicherpooldatenträger.

Containerkopienspeicherpools
: Standardmäßig sind Datenträger in Containerkopienspeicherpools nicht für die Verarbeitung mit dem Befehl QUERY DRMEDIA auswählbar. Um Datenträger in Containerkopienspeicherpools zu verarbeiten, müssen Sie zuerst den Befehl SET DRMCOPYCONTAINERSTGPOOL ausgeben oder den Parameter COPYCONTAINERSTGPOOL im Befehl QUERY DRMEDIA angeben.

Speicherpools für aktive Daten
: Standardmäßig sind Datenträger in Speicherpools für aktive Daten nicht für die Verarbeitung mit dem Befehl QUERY DRMEDIA auswählbar. Um Datenträger in Pools für aktive Daten zu verarbeiten, müssen Sie zuerst den Befehl SET DRMACTIVEDATASTGPOOL ausgeben oder den Parameter ACTIVEDATASTGPOOL im Befehl QUERY DRMEDIA angeben.

Wenn Sie ein externes Kassettenarchiv verwenden und einen Datenträger mit dem Befehl MOVE DRMEDIA in den Status NOTMOUNTBLE versetzt haben, kann der Befehl QUERY DRMEDIA den Datenträgerstatus dennoch als MOUNTABLE zurückmelden, wenn er feststellt, dass sich der Datenträger in dem Kassettenarchiv befindet. Lesen Sie in der Dokumentation zum externen Kassettenarchiv die Informationen zu den Prozeduren, denen Sie folgen sollten, wenn Sie die Befehle MOVE DRMEDIA und QUERY DRMEDIA verwenden.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- *Ist der Parameter CMD nicht angegeben:* Bediener- oder Systemberechtigung.
- *Wenn der Parameter CMD angegeben wird und die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt ist:* Bedienerberechtigung, uneingeschränkte Speicherberechtigung oder Systemberechtigung.
- *Wenn der Parameter CMD angegeben wird und die Serveroption REQSYSAUTHOUTFILE auf YES (Standardwert) gesetzt ist:* Systemberechtigung.

Syntax

```
                  .-*---------------.
>>-Query DRMedia--+-----------------+--------------------------->
                  '-Datenträgername-'

   .-WHERESTate--=--All-----------------.
>--+-----------------------------------+---------------------->
   '-WHERESTate--=--+-----------------+-'
                    +-All-------------+
                    +-MOuntable-------+
                    +-NOTMOuntable----+
                    +-COUrier---------+
                    +-VAult-----------+
                    +-VAULTRetrieve---+
                    +-COURIERRetrieve-+
                    '-REmote----------'

>--+---------------------+--+-------------------+--------------->
   '-BEGINDate--=--Datum-'  '-ENDDate--=--Datum-'

>--+---------------------+--+-------------------+----------------->
   '-BEGINTime--=--Zeit-'  '-ENDTime--=--Zeit-'

>--+---------------------------+--------------------------------->
   '-COPYstgpool--=--Poolname-'

>--+--------------------------------+--------------------------->
   '-ACTIVEDatastgpool--=--Poolname-'

>--+-----------------------------------+----------------------->
   '-COPYCONtainerstgpool--=--Poolname-'

   .-Source--=--DBBackup-------.  .-Format--=--Standard-----.
>--+---------------------------+--+-------------------------+--->
   '-Source--=--+-DBBackup---+-'  '-Format--=--+-Standard-+-'
                +-DBSnapshot-+                 +-Detailed-+
                '-DBNone-----'                 '-Cmd------'

>--+-----------------------------+--+----------------------+----->
   '-WHERELOCation--=--Standort-'  |         .----------. |
                                   |         V          | |
                                   '-CMd--=----"Befehl"-+-'

                                  .-APPend--=--No------.
>--+-----------------------------+--+-------------------+------><
```

```
'-CMDFilename--=--Dateiname-'  '-APPend--=--+-No--+-'
                                            '-Yes-'
```

Parameter

Datenträgername
: Gibt die Namen der Datenträger an, die abgefragt werden sollen. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben. Dieser Parameter ist wahlfrei. Der Server sucht nach übereinstimmenden Namen unter den folgenden auswählbaren Datenträgern:

  - Datenbanksicherungsdatenträger, die mit dem Parameter SOURCE dieses Befehls ausgewählt wurden.
  - Kopienspeicherpooldatenträger aus Kopienspeicherpools, die mit dem Parameter COPYSTGPOOL angegeben wurden. Wird der Parameter COPYSTGPOOL nicht verwendet, fragt der Server Datenträger aus Kopienspeicherpools ab, die zuvor mit dem Befehl SET DRMCOPYSTGPOOL angegeben wurden.
  - Datenträger im Speicherpool für aktive Daten aus Speicherpools für aktive Daten, die mit dem Parameter ACTIVEDATASTGPOOL angegeben wurden. Wird der Parameter ACTIVEDATASTGPOOL nicht verwendet, fragt der Server Datenträger aus Speicherpools für aktive Daten ab, die zuvor mit dem Befehl SET DRMACTIVEDATASTGPOOL angegeben wurden.
  - Containerkopienspeicherpooldatenträger aus Containerkopienspeicherpools, die mit dem Parameter COPYCONTAINERSTGPOOL angegeben wurden. Wenn der Parameter COPYCONTAINERSTGPOOL nicht verwendet wird, fragt der Server Datenträger aus Containerkopienspeicherpools ab, die zuvor im Befehl SET DRMCOPYCONTAINERSTGPOOL angegeben wurden.

  Andere Parameter können ebenfalls die Ergebnisse der Abfrage begrenzen.

WHERE State
: Gibt den Status der zu verarbeitenden Datenträger an. Dieser Parameter ist wahlfrei. Standardwert ist ALL. Gültige Werte:

  All
  : Gibt alle Datenträger in allen Status an.

  MOuntable
  : Datenträger in diesem Status enthalten gültige Daten und stehen für die Verarbeitung vor Ort zur Verfügung.

  NOTMOuntable
  : Datenträger in diesem Status befinden sich vor Ort, enthalten gültige Daten und stehen nicht für die Verarbeitung vor Ort zur Verfügung.

  COUrier
  : Datenträger in diesem Status werden gerade an einen ausgelagerten Standort versetzt.

  VAult
  : Datenträger in diesem Status sind ausgelagert, enthalten gültige Daten und stehen nicht für die Verarbeitung vor Ort zur Verfügung.

  VAULTRetrieve
  : Datenträger in diesem Status befinden sich an dem ausgelagerten Aufbewahrungsort, enthalten keine gültigen Daten und können zur Wiederverwendung oder Entsorgung wieder vor Ort versetzt werden:

    - Für einen Kopienspeicherpooldatenträger wird der Status VAULTRETRIEVE angenommen, wenn er für mindestens die Anzahl Tage leer war, die mit dem Parameter REUSEDELAY im Befehl DEFINE STGPOOL angegeben wurde.
    - Für einen Datenbanksicherungsdatenträger wird der Status VAULTRETRIEVE angenommen, wenn er einer Datenbanksicherungsserie zugeordnet ist, die auf der Basis des mit dem Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Werts als verfallen gekennzeichnet wurde.

    Wichtig: Wenn Sie QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE ausgeben, bestimmt der Server dynamisch, welche Datenträger zur Wiederverwendung oder Aussonderung wieder vor Ort transportiert werden können. Um sicherzustellen, dass alle Datenträger im Status VAULTRETRIEVE identifiziert werden, müssen Sie daher den Befehl QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE ohne die Parameter BEGINDATE, ENDDATE, BEGINTIME und ENDTIME ausgeben. Das Feld `Datum/Zeit der letzten Aktualisierung` in der Ausgabe für QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE zeigt das Datum und die Uhrzeit an, an dem bzw. zu der ein Datenträger in den Status VAULT, nicht VAULTRETRIEVE, versetzt wurde.

  COURIERRetrieve
  : Datenträger in diesem Status werden wieder an den Standort vor Ort versetzt.

  REmote
  : Datenträger in diesem Status enthalten gültige Daten und befinden sich auf dem ausgelagerten fernen Server.

BEGINDate
: Gibt das Anfangsdatum an, das zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach dem angegebenen Datum in seinen aktuellen Status geändert hat. Standardwert ist das früheste Datum, ab dem Datenträgerdaten vorliegen.
  Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY

Wert	Beschreibung	Beispiel
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage beträgt 9999.	TODAY-7 *oder* -7. Sollen Datenträger abgefragt werden, deren Sätze vor einer Woche in den aktuellen Status geändert wurden, kann BEGINDATE=TODAY-7 oder BEGINDATE=-7 angegeben werden.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDDate

Gibt das Enddatum an, das zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder vor dem angegebenen Datum in seinen aktuellen Status geändert hat. Standardwert ist das aktuelle Datum.

Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage beträgt 9999.	TODAY-7 *oder* -7. Sollen Datenträger abgefragt werden, deren Sätze vor einer Woche in den aktuellen Status geändert wurden, kann BEGINDATE=TODAY-7 oder BEGINDATE=-7 angegeben werden.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt die Anfangszeit an, die zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder nach der angegebenen Uhrzeit und dem angegebenen Datum in seinen aktuellen Status geändert hat. Der Standardwert ist Mitternacht (00:00:00) an dem mit dem Parameter BEGINDATE angegebenen Datum.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Anfangsdatum	12:33:28
NOW	Die aktuelle Uhrzeit am angegebenen Anfangsdatum	NOW

Wert	Beschreibung	Beispiel
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum	NOW+03:00 *oder* +03:00. Wird der Befehl QUERY DRMEDIA um 9:00 Uhr mit der Angabe BEGINTIME=NOW+03:00 oder BEGINTIME=+03:00 ausgegeben, zeigt der Server Datenträger an, die um 12:00 Uhr am angegebenen Anfangsdatum in ihren aktuellen Status geändert wurden.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum	NOW-03:30 *oder* -03:30. Wird der Befehl QUERY DRMEDIA um 9:00 Uhr mit der Angabe BEGINTIME=NOW-03:30 oder BEGINTIME=-03:30 ausgegeben, zeigt der Server Datenträger an, die um 5:30 Uhr am angegebenen Anfangsdatum in ihren aktuellen Status geändert wurden.

ENDTime

Gibt die Endzeit an, die zum Auswählen der Datenträger verwendet wird. Dieser Parameter ist wahlfrei. Datenträger sind auswählbar, wenn der Befehl MOVE DRMEDIA den Datenträger an oder vor der angegebenen Uhrzeit und dem angegebenen Datum in seinen aktuellen Status geändert hat. Der Standardwert ist 23:59:59.
Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Enddatum	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Enddatum	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum	NOW+03:00 *oder* +03:00. Wird der Befehl QUERY DRMEDIA um 9:00 Uhr mit der Angabe ENDTIME=NOW+03:00 oder ENDTIME=+03:00 ausgegeben, verarbeitet IBM Spectrum Protect Datenträger, die um 12:00 Uhr am angegebenen Enddatum in ihren aktuellen Status geändert wurden.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum	NOW-03:30 *oder* -03:30 Wird der Befehl QUERY DRMEDIA um 9:00 Uhr mit der Angabe ENDTIME=NOW-03:00 oder ENDTIME=-03:00 ausgegeben, verarbeitet IBM Spectrum Protect Datenträger, die um 6:00 Uhr am angegebenen Enddatum in ihren aktuellen Status geändert wurden.

COPYstgpool

Gibt den Namen des Kopienspeicherpools an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Die mit diesem Parameter angegebenen Kopienspeicherpools überschreiben die mit dem Befehl SET DRMCOPYSTGPOOL angegebenen Kopienspeicherpools.

Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

- Wurde der Befehl SET DRMCOPYSTGPOOL zuvor mit gültigen Kopienspeicherpoolnamen ausgegeben, verarbeitet der Server nur diese Speicherpools.
- Wurde der Befehl SET DRMCOPYSTGPOOL nicht ausgegeben, oder wurden alle Kopienspeicherpools mit dem Befehl SET DRMCOPYSTGPOOL entfernt, verarbeitet der Server alle Kopienspeicherpooldatenträger in dem angegebenen Status (ALL, MOUNTABLE, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE oder REMOTE).

Source

Gibt an, ob Datenbanksicherungsdatenträger ausgewählt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBACKUP. Gültige Werte:

DBBackup
: Datenbanksicherungsdatenträger mit Gesamt- und Teilsicherungen werden ausgewählt.

DBSnapshot
: Datenbanksicherungsdatenträger mit Momentaufnahmen werden ausgewählt.

DBNone
: Es werden keine Datenbanksicherungsdatenträger ausgewählt.

ACTIVEDatastgpool

Gibt den Namen des Speicherpools für aktive Daten an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Die mit diesem Parameter angegebenen Speicherpools für aktive Daten überschreiben die mit dem Befehl SET DRMACTIVEDATASTGPOOL angegebenen Speicherpools für aktive Daten.

Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

- Wurde der Befehl SET DRMACTIVEDATASTGPOOL zuvor mit gültigen Namen von Speicherpools für aktive Daten ausgegeben, verarbeitet der Server nur diese Speicherpools.
- Wurde der Befehl SET DRMACTIVEDATASTGPOOL nicht ausgegeben, oder wurden alle Speicherpools für aktive Daten mit dem Befehl SET DRMACTIVEDATASTGPOOL entfernt, verarbeitet der Server alle Datenträger im Speicherpool für aktive Daten in dem angegebenen Status (ALL, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE oder REMOTE). Datenträger im Status MOUNTABLE werden nicht verarbeitet.

COPYCONtainerstgpool
Gibt den Namen des Containerkopienspeicherpools an, dessen Datenträger verarbeitet werden sollen. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Die in diesem Parameter angegebenen Containerkopienspeicherpools überschreiben die im Befehl SET DRMCOPYCONTAINERSTGPOOL angegebenen Speicherpools.

Wird dieser Parameter nicht angegeben, wählt der Server die Speicherpools wie folgt aus:

- Wenn der Befehl SET DRMCOPYCONTAINERSTGPOOL zuvor mit Namen gültiger Containerkopienspeicherpools ausgegeben wurde, verarbeitet der Server nur diese Speicherpools.
- Wenn der Befehl SET DRMCOPYCONTAINERSTGPOOL nicht ausgegeben wurde oder alle Containerkopienspeicherpools mit dem Befehl SET DRMCOPYCONTAINERSTGPOOL entfernt wurden, verarbeitet der Server alle Containerkopienspeicherpooldatenträger auf der Basis des Werts im Parameter WHERESTATE. Ist der Parameter auf den Wert ALL, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE oder REMOTE gesetzt, werden die Datenträger verarbeitet. Lautet der Wert MOUNTABLE, werden die Datenträger nicht verarbeitet.

Format
Gibt die Informationen an, die angezeigt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard
Gibt an, dass Teilinformationen angezeigt werden.
Detailed
Gibt an, dass ausführliche Informationen angezeigt werden.
Cmd
Gibt an, dass ausführbare Befehle für die ausgewählten Datenträger erstellt werden. Wenn Sie FORMAT=CMD angeben, müssen Sie auch den Parameter CMD angeben.

WHERELOcation
Gibt den Standort der Datenträger an, die abgefragt werden sollen. Dieser Parameter ist wahlfrei. Die maximale Länge des Standorts beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.Wird der Name eines Zielservers angegeben, zeigt Disaster Recovery Manager alle Datenbanksicherungsdatenträger und Kopienspeicherpooldatenträger an, die sich auf dem Zielserver befinden.
CMd
Gibt die Erstellung von ausführbaren Befehlen an, um den mit diesem Befehl erhaltenen Datenträgernamen und Standort zu verarbeiten. Dieser Parameter ist wahlfrei. Die Befehlsangabe muss in Anführungszeichen eingeschlossen werden. Die maximale Länge dieses Parameters beträgt 255 Zeichen. Disaster Recovery Manager schreibt die Befehle in eine Datei, die mit dem Parameter CMDFILENAME oder dem Befehl SET DRMCMDFILENAME angegeben oder mit dem Befehl QUERY DRMEDIA generiert wurde. Ist der Befehl länger als 240 Zeichen, wird er in mehrere Zeilen geteilt und es werden Fortsetzungszeichen (+) hinzugefügt. Das Fortsetzungszeichen muss möglicherweise entsprechend dem Produkt, das die Befehle ausführt, geändert werden.

Wenn der Parameter FORMAT=CMD nicht angegeben wird, werden von diesem Befehl keine Befehlszeilen erstellt.

Zeichenfolge
Die Befehlszeichenfolge. Die Zeichenfolge darf keine eingebetteten Anführungszeichen enthalten. Dies ist beispielsweise ein gültiger CMD-Parameter:

```
cmd="checkin libvol lib8mm &vol status=scratch"
```

Dies ist ein Beispiel eines CMD-Parameters, der *nicht* gültig ist:

```
cmd=""checkin libvolume lib8mm" &vol status=scratch""
```

Substitution
Gibt eine Substitutionsvariable an, mit der QUERY DRMEDIA angewiesen wird, einen Wert für die Variable einzusetzen. Bei den Variablen muss die Groß-/Kleinschreibung nicht berücksichtigt werden. Die Variablen dürfen keine Leerstellen hinter dem Et-Zeichen (&) enthalten. Gültige Variablen sind:

&VOL
Eine Variable für den Datenträgernamen.
&LOC
Ein Datenträgerstandort.

&VOLDSN
: Der Name der Datei, in die der Server die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Ein Beispiel für einen Dateinamen eines Banddatenträgers aus dem Kopienspeicherpool unter Verwendung des Standardpräfix TSM lautet TSM.BFS. Ein Beispiel für einen Dateinamen eines Banddatenträgers für die Datenbanksicherung unter Verwendung des Präfix TSM310 lautet TSM310.DBB.

&NL
: Das Zeilenvorschubzeichen. Wird &NL angegeben, teilt der Befehl QUERY DRMEDIA den Befehl bei der Variablen &NL und fügt kein Fortsetzungszeichen hinzu. Es muss das korrekte Fortsetzungszeichen vor &NL angegeben werden, sofern ein Fortsetzungszeichen erforderlich ist. Wird &NL nicht angegeben und hat die Befehlszeile mehr als 240 Zeichen, wird die Zeile in mehrere Zeilen geteilt und es werden Fortsetzungszeichen (+) hinzugefügt.

 AIX-Betriebssysteme  Linux-BetriebssystemeCMDFilename
:  AIX-Betriebssysteme  Linux-BetriebssystemeGibt den vollständig qualifizierten Namen der Datei an, die die mit dem Parameter CMD angegebenen Befehle enthalten soll. Dieser Parameter ist wahlfrei.

  Wenn kein Name mit dem Befehl SET DRMCMDFILENAME angegeben wird, erstellt der Server einen Dateinamen, indem `exec.cmds` an den absoluten Verzeichnispfadnamen des IBM Spectrum Protect-Instanzverzeichnisses angehängt wird. Wird eine Nullzeichenfolge ("") angegeben, werden die Befehle nur an der Konsole angezeigt. Die Befehle können an eine Datei umgeleitet werden, indem das Umleitungszeichen für das Betriebssystem verwendet wird.

  Schlägt die Operation fehl, nachdem die Befehlsdatei erstellt wurde, wird die Datei nicht gelöscht.

 Windows-BetriebssystemeCMDFilename
:  Windows-BetriebssystemeGibt den vollständig qualifizierten Namen der Datei an, die die mit dem Parameter CMD angegebenen Befehle enthalten soll. Dieser Parameter ist wahlfrei.

  Wenn kein Dateiname mit dem Befehl SET DRMCMDFILENAME angegeben wird, erstellt der Server einen Dateinamen, indem `exec.cmd` an das Verzeichnis angehängt wird, das diese Instanz des Servers darstellt (normalerweise das Verzeichnis, in dem der IBM Spectrum Protect-Server ursprünglich installiert wurde). Wird eine Nullzeichenfolge ("") angegeben, werden die Befehle nur an der Konsole angezeigt. Die Befehle können an eine Datei umgeleitet werden, indem die Zeichen > und >> verwendet werden, die vom System zur Verfügung gestellt werden. Disaster Recovery Manager ordnet den angegebenen oder generierten Dateinamen zu. Ist die Datei vorhanden, versucht Disaster Recovery Manager, die Datei zu verwenden, und es werden alle vorhandenen Daten überschrieben.

  Schlägt die Operation fehl, nachdem die Befehlsdatei erstellt wurde, wird die Datei nicht gelöscht.

APPend
: Gibt an, ob der vorhandene Inhalt der Befehlsdatei überschrieben werden soll oder ob die Befehle an die Datei angehängt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Disaster Recovery Manager überschreibt den Inhalt der Datei.

  Yes
  : Disaster Recovery Manager hängt die Befehle an die Datei an.

Beispiel: Datenträger auflisten, die zur Speicherung ausgelagert werden sollen

Es sollen alle Datenträger angezeigt werden, die einem Kurier für die ausgelagerte Speicherung übergeben werden sollen.

```
query drmedia wherestate=notmountable
format=standard

Datenträger-     Status          Dat./Zeit             Automat.
name             d.letz.Akt.     Kassettenarchiv
---------------  --------------  --------------------  ---------
TAPE01           Not mountable    01/20/1998 14:25:22
DBTP01           Not mountable    01/20/1998 14:25:22
DBTP03           Not mountable    01/20/1998 14:31:53
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Informationen zu Datenträgern am Aufbewahrungsort anzeigen

Ausführliche Informationen über alle Datenträger an dem Aufbewahrungsort anzeigen.

```
query drmedia wherestate=vault format=detailed

                                Datenträgername: DBTP02
                                         Status: Vault
          Datum/Zeit der letzten Aktualisierung: 01/20/1998 13:29:02
                                       Standort: Ironmnt
                                 Datenträgerart: DBBackup
                        Kopienspeicherpoolname:
   Name des Speicherpools für aktive Daten: TSMACTIVEPOOL
                       Automat. Kassettenarchiv:
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Datenträgername
: Der Name des Datenbanksicherungs- oder Kopienspeicherpooldatenträgers.

Status
: Der Status des Datenträgers.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der der Datenträgerstatus zuletzt aktualisiert wurde. Für Datenträger im Status VAULTRETRIEVE zeigt dieses Feld das Datum und die Uhrzeit an, an dem bzw. zu der ein Datenträger in den Status VAULT, nicht VAULTRETRIEVE, versetzt wurde. Der Server "aktualisiert" keine Datenträger nach VAULTRETRIEVE. Zum Zeitpunkt der Ausgabe des Befehls QUERY DRMEDIA bestimmt der Server dynamisch, ob die Daten auf den Kopienspeicherpooldatenträgern und Datenbanksicherungsdatenträgern nicht mehr gültig sind und ob der Datenträger zur Wiederverwendung oder Entsorgung wieder an den Standort vor Ort versetzt werden kann.

Standort
: Das Feld Standort wird angezeigt, wenn der Datenträger nicht mountfähig ist oder sich nicht im Speicherarchiv befindet. Das Feld Standort ist leer, wenn der Datenträger mountfähig ist und sich im Speicherarchiv befindet.

Datenträgertyp
: Gibt den Datenträgertyp an. Gültige Werte:

  DBBackup
  : Datenträger mit vollständiger Datenbanksicherung oder Teilsicherung der Datenbank.

  DBSnapshot
  : Datenträger mit Datenbankmomentaufnahmesicherung.

  CopyStgPool
  : Ein Kopienspeicherpooldatenträger.

  ContcopyStgPool
  : Ein Datenträger im Containerkopienspeicherpool.

Kopienspeicherpoolname
: Für einen Kopienspeicherpooldatenträger der Name des Kopienspeicherpools.

Name des Speicherpools für aktive Daten
: Für einen Datenträger im Speicherpool für aktive Daten der Name des Speicherpools für aktive Daten.

Name des Containerkopienspeicherpools
: Für einen Datenträger im Containerkopienspeicherpool der Name des Containerkopienspeicherpools.

Automat. Kassettenarchiv
: Der Name des automatisierten Kassettenarchivs, wenn sich der Datenträger in einem Kassettenarchiv befindet.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DRMEDIA

Befehl	Beschreibung
BACKUP DB	Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff.
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.
SET DRMACTIVEDATASTGPOOL	Gibt an, dass Speicherpools für aktive Daten von DRM verwaltet werden.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeSET DRMCOPYCONTAINERSTGPOOL	Gibt die Containerkopienspeicherpools an, die in DRM-Befehlen verwendet werden.
SET DRMCOPYSTGPOOL	Gibt an, dass Kopienspeicherpools von DRM verwaltet werden.
SET DRMDBBACKUPEXPIREDAYS	Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.
SET DRMCMDFILENAME	Gibt den Namen einer Datei an, in die ausführbare DRM-Befehle gestellt werden sollen.
SET DRMFILEPROCESS	Gibt an, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Dateien verarbeitet, die den Einheitentyp FILE aufweisen.

QUERY DRMSTATUS (Disaster Recovery Manager-Systemparameter abfragen)

Mit diesem Befehl können Informationen über die Systemparameter angezeigt werden, die für Disaster Recovery Manager (DRM) definiert sind.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query DRMSTatus-----------------------------------------><
```

Parameter

Keine.

Beispiel: Informationen zu DRM-Systemparametern anzeigen

Informationen zu den DRM-Systemparametern anzeigen:

```
query drmstatus

                    Wiederherstellungsplanpräfix:
                            Plananweisungspräfix:
                    Ersatzdatenträgererweiterung: @
                           Primäre Speicherpools: PRIM1 PRIM2
                             Kopienspeicherpools: COPY*
          Speicherpools für aktive Daten: TSMACTIVEPOOL
       Containerkopienspeicherpools: COPYCNTRPOOL
                 Nicht mount-fähiger Standortname: Local
                                      Kuriername: Fedex
                            Aufbewahrungsortname: Ironmnt
          Verfallszeitraum für DB-Sicherungsserie: 30 Tag(e)
Verfallszeitraum für Wiederherstellungsplandatei: 30 Tag(e)
                                Kennsatzprüfung?: No
                  Einheitentyp FILE verarbeiten?: No
                                Befehlsdateiname:
```

Feldbeschreibungen

Wiederherstellungsplanpräfix
: Benutzerdefinierter Präfixabschnitt des Dateinamens für die Wiederherstellungsplandatei.

Plananweisungspräfix
: Benutzerdefinierter Präfixabschnitt der Dateinamen für die Wiederherstellungsanweisungsdateien des Servers.

Ersatzdatenträgererweiterung
: Das Zeichen, das an das Ende der Ersatzdatenträgernamen in der Wiederherstellungsplandatei hinzugefügt wird.

Primäre Speicherpools
: Die primären Speicherpools, die für die Verarbeitung durch den Befehl PREPARE ausgewählt werden können. Ist dieses Feld leer, können alle primären Speicherpools ausgewählt werden.

Kopienspeicherpools
: Die Kopienspeicherpools, die für die Verarbeitung durch die Befehle MOVE DRMEDIA, PREPARE und QUERY DRMEDIA ausgewählt werden können. Ist dieses Feld leer, können alle Kopienspeicherpools ausgewählt werden.

Speicherpools für aktive Daten
: Die Pools für aktive Daten, die für die Verarbeitung durch die Befehle MOVE DRMEDIA, PREPARE und QUERY DRMEDIA ausgewählt werden können. Ist dieses Feld leer, sind keine Pools für aktive Daten auswählbar.

Containerkopienspeicherpools
: Die Containerkopienspeicherpools, die für die Verarbeitung durch die Befehle MOVE DRMEDIA, PREPARE und QUERY DRMEDIA ausgewählt werden können. Ist dieses Feld leer, sind keine Containerkopienspeicherpools auswählbar.

Nicht mount-fähiger Standortname
: Der Name des ausgelagerten Standorts, an dem die zu liefernden Datenträger aufbewahrt werden.

Kuriername
: Der Name des Kuriers, mit dem die Datenträger an den Aufbewahrungsort befördert werden.

Aufbewahrungsortname
: Der Name des Aufbewahrungsorts, an dem die Datenträger aufbewahrt werden.

Verfallszeitraum für DB-Sicherungsserie
: Die Mindestanzahl Tage, die seit der Erstellung einer Datenbankserie vergangen sein müssen, bevor sie für den Verfall ausgewählt werden kann. Unter dem Befehl SET DRMDBBACKUPEXPIREDAYS befinden sich Informationen zu den Kriterien, die für den Verfall von Datenbanksicherungsserien erfüllt sein müssen.

Verfallszeitraum für Wiederherstellungsplandatei
: Die Mindestanzahl Tage, die seit der Erstellung einer Wiederherstellungsplandatei, die auf einem Zielserver gespeichert ist, vergangen sein müssen, bevor die Datei für den Verfall ausgewählt werden kann. Unter dem Befehl SET DRMRPFEXPIREDAYS befinden sich Informationen zu den Kriterien, die für den Verfall einer Wiederherstellungsplandatei erfüllt sein müssen.

Kennsatzprüfung?
: Die Angabe, ob Datenträgerkennsätze für sequenzielle Datenträger gelesen werden, die durch den Befehl MOVE DRMEDIA entnommen wurden. Gültige Werte sind Yes oder No.

Einheitentyp FILE verarbeiten?
: Die Angabe, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Datenbanksicherungs- und Kopienspeicherpooldatenträger verarbeitet, die einer Einheitenklasse mit dem Einheitentyp FILE zugeordnet sind. Gültige Werte sind Yes oder No.

Befehlsdateiname
: Der vollständige Pfad und Dateiname, in dem sich die durch den Befehl MOVE DRMEDIA oder QUERY DRMEDIA generierten ausführbaren Befehle befinden.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY DRMSTATUS

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
SET DRMCHECKLABEL	Gibt an, ob IBM Spectrum Protect während der Verarbeitung des Befehls MOVE DRMEDIA Datenträgerkennsätze lesen soll.
SET DRMACTIVEDATASTGPOOL	Gibt an, dass Speicherpools für aktive Daten von DRM verwaltet werden.
AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeSET DRMCOPYCONTAINERSTGPOOL	Gibt die Containerkopienspeicherpools an, die in DRM-Befehlen verwendet werden.
SET DRMCOPYSTGPOOL	Gibt an, dass Kopienspeicherpools von DRM verwaltet werden.
SET DRMCMDFILENAME	Gibt den Namen einer Datei an, in die ausführbare DRM-Befehle gestellt werden sollen.
SET DRMCOURIERNAME	Gibt den Kuriernamen für DRM an.
SET DRMDBBACKUPEXPIREDAYS	Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.
SET DRMFILEPROCESS	Gibt an, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Dateien verarbeitet, die den Einheitentyp FILE aufweisen.
SET DRMINSTRPREFIX	Gibt das Präfix des Pfadnamens für die Wiederherstellungsplananweisungen an.
SET DRMPLANVPOSTFIX	Gibt die Namen der Ersatzdatenträger in der Wiederherstellungsplandatei an.
SET DRMPLANPREFIX	Gibt das Präfix des Pfadnamens für den Wiederherstellungsplan an.
SET DRMPRIMSTGPOOL	Gibt an, dass primäre Speicherpools von DRM verwaltet werden.
SET DRMRPFEXPIREDAYS	Definiert Verfallskriterien für Wiederherstellungsplandateien.
SET DRMVAULTNAME	Gibt den Namen des Aufbewahrungsorts an, an dem DRM-Datenträger gespeichert werden.
SET DRMNOTMOUNTABLENAME	Gibt den Standortnamen der DRM-Datenträger an, die ausgelagert werden sollen.

QUERY ENABLED (Aktivierte Ereignisse abfragen)

Mit diesem Befehl kann eine Liste der aktivierten Ereignisse oder eine Liste der inaktivierten Ereignisse (die kürzere Liste) angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query--ENabled--+-CONSOLE--------+--------------------------->
                   +-ACTLOG---------+
                   +-EVENTSERVER----+
                   +-FILE-----------+
                   +-FILETEXT-------+
```

```
                    |            (1) |
                    +-NTEVENTLOG-----+
                    |         (2)    |
                    +-SYSLOG---------+
                    +-TIVOLI---------+
                    '-USEREXIT-------'

>--+--------------------------+-------------------------------><
   +-NODEname--=--Knotenname---+
   '-SERVername--=--Servername-'
```

Anmerkungen:

1. Dieser Parameter ist nur für das Windows-Betriebssystem verfügbar.
2. Dieser Parameter ist nur für das Linux-Betriebssystem verfügbar.

Parameter

Empfänger
: Gibt eine Art des Empfängers für aktivierte Ereignisse an. Dieser Parameter ist erforderlich. Gültige Werte sind:

  ACTLOG
  : Gibt das IBM Spectrum Protect-Aktivitätenprotokoll als Empfänger an.

  CONSOLE
  : Gibt die Standardserverkonsole als Empfänger an.

  EVENTSERVER
  : Gibt den Ereignisserver als Empfänger an.

  FILE
  : Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist ein Satz in der Datei, und eine Person kann jedes protokollierte Ereignis nicht einfach lesen.

  FILETEXT
  : Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

  Windows-BetriebssystemeNTEVENTLOG
  : Windows-BetriebssystemeGibt das Windows-Anwendungsprotokoll als Empfänger an.

  Linux-BetriebssystemeSYSLOG
  : Linux-BetriebssystemeGibt das Linux-Systemprotokoll als Empfänger an.

  TIVOLI
  : Gibt Tivoli Management Environment (TME) als Empfänger an.

  USEREXIT
  : Gibt eine benutzerdefinierte Routine, in die IBM Spectrum Protect Informationen schreibt, als Empfänger an.

NODEname
: Gibt einen Knotennamen an, der abgefragt werden soll. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, bezieht sich die Abfrage auf die Ereignisse, die für den Server aktiviert sind, der diesen Befehl ausführt.

SERVername
: Gibt einen Servernamen an, der abgefragt werden soll. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, bezieht sich die Abfrage auf die Ereignisse, die für den Server aktiviert sind, der diesen Befehl ausführt.

Beispiel: Den Server nach Konsolereignissen abfragen

Den Server nach Serverereignissen abfragen, die für die Konsole aktiviert sind. Es gibt 10000 mögliche Serverereignisse. Es wird eine Liste der aktivierten Ereignisse oder der inaktivierten Ereignisse (die kürzere Liste) angezeigt.

```
query enabled console

9998
Ereignisse für Empfänger CONSOLE aktiviert. Folgende
Ereignisse sind für Empfänger CONSOLE inaktiviert:

ANR8409, ANR8410
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ENABLED

Befehl	Beschreibung
BEGIN EVENTLOGGING	Startet das Ereignisprotokoll für einen bestimmten Empfänger.
DISABLE EVENTS	Inaktiviert bestimmte Ereignisse für Empfänger.
ENABLE EVENTS	Aktiviert bestimmte Ereignisse für Empfänger.
END EVENTLOGGING	Beendet das Ereignisprotokoll für einen bestimmten Empfänger.

Befehl	Beschreibung
QUERY EVENTRULES	Zeigt Informationen über Regeln für Server- und Clientereignisse an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

QUERY EVENT (Geplante und abgeschlossene Ereignisse abfragen)

Mit diesem Befehl kann der Status geplanter Ereignisse angezeigt werden. Mit den Parametern für Uhrzeit und Datum können Sie die Abfrage auf Ereignisse begrenzen, die innerhalb der angegebenen Uhrzeiten und Datumsangaben stattfinden sollten. Wird die Ausgabe auf Ereignisse begrenzt, deren geplante Startzeiten innerhalb eines Datums- und Zeitbereichs liegen, wird auch die Zeit für die Verarbeitung dieser Abfrage verkürzt.

Die Befehlssyntax unterscheidet sich bei Abfragen, die sich auf geplante Client-Operationen und geplante Verwaltungsbefehle beziehen.

Tabelle 1. Zugehörige Befehle für QUERY EVENT

Befehl	Beschreibung
DEFINE SCHEDULE	Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.
DELETE EVENT	Löscht Ereignissätze, die vor einem bestimmten Zeitpunkt erstellt wurden.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
SET EVENTRETENTION	Gibt die Anzahl Tage für die Aufbewahrung von Sätzen geplanter Operationen an.
SET RANDOMIZE	Gibt die Zufallsgenerierung von Startzeiten innerhalb eines Fensters für Zeitpläne im Clientsendeaufrufmodus an.

- QUERY EVENT (Clientzeitpläne anzeigen)
  Mit dem Befehl QUERY EVENT können geplante und abgeschlossene Ereignisse für ausgewählte Clients angezeigt werden.
- QUERY EVENT (Ereignisse für Verwaltungszeitpläne anzeigen)
  Mit dem Befehl QUERY EVENT können geplante und abgeschlossene Ereignisse für ausgewählte Verwaltungsbefehlszeitpläne angezeigt werden.

QUERY EVENT (Clientzeitpläne anzeigen)

Mit dem Befehl QUERY EVENT können geplante und abgeschlossene Ereignisse für ausgewählte Clients angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query EVent--Domänenname--Zeitplanname----------------------->

   .-Type--=--Client-.
>--+-----------------+--+-------------------------+------------>
                       |           .-,----------. |
                       |           V            | |
                       '-Nodes--=----Knotenname-+-'

   .-BEGINDate--=--aktuelles_Datum-.  .-BEGINTime--=--00:00-.
>--+-------------------------------+--+---------------------+--->
   '-BEGINDate--=--Datum-----------'  '-BEGINTime--=--Zeit--'

   .-ENDDate--=--Enddatum-.  .-ENDTime--=--23:59-.
>--+---------------------+--+------------------+-------------->
   '-ENDDate--=--Datum----'  '-ENDTime--=--Zeit--'

   .-EXceptionsonly--=--No------.
>--+----------------------------+------------------------------>
   '-EXceptionsonly--=--+-No--+-'
                        '-Yes-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
```

```
'-Detailed-'
```

Parameter

Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an, zu der die Zeitpläne gehören. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

Zeitplanname (Erforderlich)
: Gibt den Namen des Zeitplans an, für den Ereignisse angezeigt werden. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

Type=Client
: Gibt an, dass die Abfrage Ereignisse für Clientzeitpläne anzeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT.

Nodes
: Gibt den Namen des Client-Knotens an, der zur angegebenen Maßnahmendomäne, für die Ereignisse angezeigt werden, gehört. Es können mehrere Client-Knoten angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.Es können Platzhalterzeichen verwendet werden, um Knoten anzugeben. Wird kein Clientname angegeben, werden Ereignisse für alle Clients angezeigt, die mit dem Domänennamen und dem Zeitplannamen übereinstimmen.

BEGINDate
: Gibt das Anfangsdatum des Zeitraums an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieses Zeitraums geplant ist, werden angezeigt. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum.
Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage **oder** +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY +3 **oder** +3.
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage	TODAY-7 **oder** -7. Sollen Ereignisse abgefragt werden, deren Start während der vergangenen sieben Tage geplant war, BEGINDATE=TODAY-7 ENDDATE=TODAY oder BEGINDATE=-7 ENDDATE=TODAY angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime
: Gibt die Anfangszeit des Bereichs an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieses Zeitraums geplant ist, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 00:00.
Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Anfangsdatum	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Anfangsdatum	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum	NOW+03:00 **oder** +03:00. Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start in 3 Stunden geplant ist, kann entweder BEGINTIME=NOW+03:00 oder BEGINTIME=+03:00 angegeben werden. IBM Spectrum Protect zeigt dann Ereignisse um 12:00 Uhr am angegebenen Anfangsdatum an.

Wert	Beschreibung	Beispiel
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum	NOW-04:00 **oder** -04:00. Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start während der letzten 4 Stunden geplant war, kann entweder BEGINTIME=NOW-04:00 ENDTIME=NOW oder BEGINTIME=-04:00 ENDTIME=NOW angegeben werden. IBM Spectrum Protect zeigt dann Ereignisse um 5:00 Uhr am angegebenen Anfangsdatum an.

ENDDate

Gibt das Enddatum des Zeitraums an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start während dieser Zeit geplant war, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist der für BEGINDATE verwendete Wert.
Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage **oder** +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY +3 **oder** +3.
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage	TODAY-8 **oder** -8. Sollen Ereignisse abgefragt werden, deren Start während einer einwöchigen Periode, die gestern zu Ende ging, geplant war, kann entweder BEGINDATE=TODAY-8 ENDDATE=TODAY-1 oder BEGINDATE=-8 ENDDATE=-1 angegeben werden.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDTime

Gibt die Endzeit des Bereichs an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieser Zeitspanne geplant war, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 23:59.
Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Enddatum	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Enddatum	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum	NOW+03:00 **oder** +03:00. Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start in 3 Stunden geplant ist, kann entweder BEGINTIME=NOW ENDTIME=NOW+03:00 oder BEGINTIME=NOW ENDTIME=+03:00 angegeben werden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum	NOW-04:00 **oder** -04:00

EXceptionsonly

Gibt die Art der Informationen an, die über geplante oder abgeschlossene Ereignisse gewünscht werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No

Gibt an, daß die Informationen zu vergangenen und projektierten Ereignissen angezeigt werden.

Yes

Gibt an, daß die Ereignisse angezeigt werden, die fehlgeschlagen sind oder nicht wie geplant verarbeitet wurden.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Die folgenden Werte sind gültig:

Standard

Gibt an, dass Teilinformationen für Ereignisse angezeigt werden.

Detailed

Gibt an, dass die gesamten Informationen für Ereignisse angezeigt werden.

Teilinformationen zu nicht erfolgreichen Ereignissen anzeigen

Teilinformationen zu allen für DOMAIN1 geplanten Ereignissen, deren Ausführung nicht erfolgreich war, anzeigen. Die Suche soll sich auf den Client JOE beschränken. Außerdem sollen nur die Ereignisse angezeigt werden, deren Ausführung in der Zeit vom 11. Februar 2001 (02/11/2001) bis 12. Februar 2001 (02/12/2001) geplant war.

```
query event domain1 * nodes=joe begindate=02/11/2001
enddate=02/12/2001 exceptionsonly=yes
```

```
Geplanter Start      Ist-Start            Zeitplan-  Knoten- Status
                                            name         name
-------------------- -------------------- --------- ----   ---------
02/11/1999 01:00:00  02/11/1999 01:13:55   BACK1      JOE    Failed
02/12/1999 01:00:00                       DAILYBKP   JOE    Missed
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Teilinformationen zu geplanten Ereignissen für einen Client anzeigen

Die gesamten Informationen für alle Ereignisse anzeigen, die für die Verarbeitung geplant sind. Als Startdatum 10 Tage vor dem heutigen Datum definieren und beim Enddatum den heutigen Tag einschließen.

```
query event * * begindate=today-10 enddate=today
```

```
Geplanter Start         Ist-Start               Zeitplan-        Knoten-          Status
                                                  name             name
--------------------    --------------------    -------------    -------------    ---------
02/04/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/04/2013 14:00:00     02/04/2013 14:12:49     VDATAMVR1-IN1    VDATAMVR1-T1     Completed
02/04/2013 14:30:00     02/04/2013 14:33:10     VDATAMVR1-IN2    VDATAMVR1-T2     Completed
02/04/2013 15:00:00     02/04/2013 15:01:49     VDATAMVR1-IN3    VDATAMVR1-T3     Completed
02/04/2013 15:30:00     02/04/2013 15:42:00     VDATAMVR1-IN4    VDATAMVR1-T4     Completed
02/05/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/05/2013 14:00:00     02/05/2013 14:05:22     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/05/2013 14:30:00     02/05/2013 14:32:53     VDATAMVR1-F2     VDATAMVR1-F2     Failed 12
02/05/2013 15:00:00     02/05/2013 15:00:38     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/05/2013 15:30:00     02/05/2013 15:36:41     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/06/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/06/2013 14:00:00     02/06/2013 14:06:42     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/06/2013 14:30:00     02/06/2013 14:35:41     VDATAMVR1-F2     VDATAMVR1-F2     Completed
02/06/2013 15:00:00     02/06/2013 15:08:56     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/06/2013 15:30:00     02/06/2013 15:40:49     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/07/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/07/2013 14:00:00     02/07/2013 14:03:43     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/07/2013 14:30:00     02/07/2013 14:35:10     VDATAMVR1-F2     VDATAMVR1-F2     Completed
02/07/2013 15:00:00     02/07/2013 15:09:12     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/07/2013 15:30:00     02/07/2013 15:40:21     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/08/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/08/2013 14:00:00     02/08/2013 14:10:17     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/08/2013 14:30:00     02/08/2013 14:39:16     VDATAMVR1-F2     VDATAMVR1-F2     Completed
02/08/2013 15:00:00     02/08/2013 15:08:17     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/08/2013 15:30:00     02/08/2013 15:41:16     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/09/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/09/2013 14:02:16                             VDATAMVR1-F1     VDATAMVR1-F1     Failed 12
02/09/2013 14:30:00     02/09/2013 14:44:26     VDATAMVR1-F2     VDATAMVR1-F2     Failed 12
02/09/2013 15:00:00     02/09/2013 15:06:24     VDATAMVR1-F3     VDATAMVR1-F3     Failed 12
02/09/2013 15:30:00     02/09/2013 15:32:18     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/11/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/11/2013 14:00:00     02/11/2013 14:01:05     VDATAMVR1-F1     VDATAMVR1-F1     Failed 12
02/11/2013 14:30:00     02/11/2013 14:31:42     VDATAMVR1-F2     VDATAMVR1-F2     Failed 12
02/11/2013 15:00:00     02/11/2013 15:06:17     VDATAMVR1-F3     VDATAMVR1-F3     Failed 12
02/11/2013 15:30:00     02/11/2013 15:30:19     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/12/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/12/2013 14:00:00     02/12/2013 14:03:37     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/12/2013 14:30:00     02/12/2013 14:33:07     VDATAMVR1-F2     VDATAMVR1-F2     Completed
02/12/2013 15:00:00     02/12/2013 15:03:56     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/12/2013 15:30:00     02/12/2013 15:36:44     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/13/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Missed
02/13/2013 14:00:00     02/13/2013 14:06:24     VDATAMVR1-F1     VDATAMVR1-F1     Completed
02/13/2013 14:30:00     02/13/2013 14:34:50     VDATAMVR1-F2     VDATAMVR1-F2     Completed
```

```
02/13/2013 15:00:00     02/13/2013 15:15:01     VDATAMVR1-F3     VDATAMVR1-F3     Completed
02/13/2013 15:30:00     02/13/2013 15:30:18     VDATAMVR1-F4     VDATAMVR1-F4     Completed
02/14/2013 14:00:00                             SCHD_INCR-DM1    TSM_CET_DM1      Future
02/14/2013 14:00:00                             VDATAMVR1-F1     VDATAMVR1-F1     Future
02/14/2013 14:30:00                             VDATAMVR1-F2     VDATAMVR1-F2     Future
02/14/2013 15:00:00                             VDATAMVR1-F3     VDATAMVR1-F3     Future
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Ausführliche Informationen zu geplanten Ereignissen für einen Client anzeigen

Die ausführlichen Informationen zu Ereignissen anzeigen, deren Verarbeitung durch den Client DOC zwischen 10:00 Uhr und 11:00 Uhr am 1. November 2005 (11/01/2005) geplant ist. Lautet der Status FAILED (Fehlgeschlagen), wird der Ergebniscode angezeigt.

```
query event domain1 * nodes=doc begindate=11/01/2005
begintime=10:00 endtime=11:00 enddate=11/01/2005
exceptionsonly=yes format=detailed
```

```
Geplanter Start      Ist-Start            Zeitplan-  Knoten- Status
                                          name         name
-------------------- -------------------- ---------  ------  -------
11/01/2005 10:01:01  11/01/2005 10:03:46  T1            DOC  Failed 8
11/01/2005 10:16:01  11/01/2005 10:16:10  T1            DOC  Failed 4
11/01/2005 10:31:01  11/01/2005 10:33:08  T1            DOC  Completed
11/01/2005 10:46:01                       T1            DOC  Missed
11/01/2005 10:57:49  11/01/2005 10:58:07  T0            DOC  Failed 12
```

Feldbeschreibungen

Name der Maßnahmendomäne
: Gibt den Namen der Maßnahmendomäne an, der der Zeitplan zugeordnet ist.

Zeitplanname
: Gibt den Namen des Zeitplans an, der dieses Ereignis eingeleitet hat.

Knotenname
: Gibt den Client an, der für die Ausführung der Operation geplant ist.

Geplanter Start
: Gibt das geplante Startdatum und die geplante Uhrzeit für das Ereignis an.

Ist-Start
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Client mit der Verarbeitung der geplanten Operation begonnen hat. Wurde die geplante Operation nicht gestartet, werden keine Informationen angezeigt.

Completed
: Gibt an, wann das geplante Ereignis abgeschlossen wurde (Datum und Uhrzeit).

Status
: Gibt den Status des Ereignisses zu dem Zeitpunkt an, zu dem der Befehl QUERY EVENT ausgegeben wird. Die folgenden Werte sind gültig:

  Completed
  : Gibt an, dass das geplante Ereignis abgeschlossen ist.

  Failed
  : Gibt an, dass der Client bei der Ausführung der geplanten Operation einen Fehler festgestellt hat und aufeinanderfolgende Wiederholungsversuche fehlgeschlagen sind.

  Failed - no restart
  : Gibt einen temporären Status an, wenn eine Clientsitzung durch einen Übertragungsfehler oder eine Zeitlimitüberschreitung auf dem Server unterbrochen wird. Dieser Status kann in den endgültigen Status "Completed" oder "Failed" geändert werden, wenn das Ereignis abgeschlossen ist.

  Future
  : Gibt an, dass der Beginn des Startfensters für das Ereignis in der Zukunft liegt. Dieser Status gibt außerdem an, dass kein Ereignissatz für dieses Ereignis erstellt wurde.

  In Progress
  : Gibt an, dass das geplante Ereignis gerade ausgeführt wird, aber die Beendigung noch nicht an den Server gemeldet wurde.

    Überprüfen Sie regelmäßig den Status auf Beendigung des geplanten Ereignisses. Wird dieser Status nicht in einer angemessenen Zeit aktualisiert, überprüfen Sie dsmsched.log und dsmerror.log des Clients, um zu bestimmen, warum der Client das Ergebnis dieses Ereignisses nicht an den Server gemeldet hat. Ist die geplante Sicherung fehlgeschlagen, führen Sie das geplante Ereignis erneut aus oder führen Sie eine manuelle Teilsicherung aus, um die Datensicherung zu gewährleisten.

  Missed
  : Gibt an, dass das geplante Startfenster für dieses Ereignis abgelaufen ist und mit der Ausführung nicht begonnen wurde.

  Pending
  : Gibt an, dass der Befehl QUERY EVENT innerhalb des Startfensters für das Ereignis ausgegeben wurde, die Verarbeitung der geplanten Operation jedoch nicht begonnen hat.

  Restarted
  : Gibt an, dass der Client versucht hat, die geplante Operation erneut zu verarbeiten.

  Severed

Gibt an, dass die Übertragung zum Client unterbrochen wurde, bevor das Ereignis abgeschlossen werden konnte.

Started
: Gibt an, dass die Verarbeitung des Ereignisses begonnen hat.

Uncertain
: Gibt an, dass der Status des Ereignisses nicht ermittelt werden kann. Der Server gibt immer dann `Uncertain` an, wenn der Befehl QUERY EVENT keinen Ereignissatz finden kann. Ein Ereignissatz wird nicht gefunden, wenn der Satz gelöscht wurde oder der Server während des geplanten Startfensters nicht verfügbar war (der Zeitplan wurde nie gestartet). Sätze mit dem Status "Uncertain" werden nicht in der Datenbank gespeichert. Sollen diese Sätze nicht angezeigt werden, ist entweder EXCEPTIONSONLY=YES anzugeben oder der Zeitplan zu löschen, wenn er nicht mehr benötigt wird.

Achtung: Wenn eine geplante Operation verarbeitet wird und innerhalb der angegebenen Dauer nicht erneut gestartet wird, zeigt das Feld Status `Gestartet` an. Wird die Operation über die angegebene Dauer hinaus fortgesetzt, wird kein Ereignissatz erstellt. Wird nach Ablauf der angegebenen Dauer eine Abfrage ausgegeben, wird der Status als `Fehlgeschlagen` angezeigt, auch wenn die Operation noch ausgeführt wird. Nach Abschluss der Operation wird ein Ereignissatz erstellt, und eine nachfolgende Abfrage zeigt das Ergebnis in dem Statusfeld an.

Ergebnis
: Gibt den Rückkehrcode an, der anzeigt, ob der Zeitplan erfolgreich verarbeitet wurde. Wenn der Rückkehrcode einen anderen Wert als 0 hat, prüfen Sie das Serveraktivitätenprotokoll sowie das Fehlerprotokoll und das Planungsprotokoll des Clients.

Rückkehrcode	Erläuterung
0	Alle Operationen wurden erfolgreich abgeschlossen.
4	Die Operation wurde abgeschlossen, einige Dateien wurden jedoch nicht verarbeitet.
8	Die Operation wurde mit mindestens einer Warnung abgeschlossen.
12	Die Operation wurde mit mindestens einer Fehlernachricht abgeschlossen. Die Anzahl Fehlernachrichten schließt keine Benachrichtigungen über übersprungene Dateien ein.
-99	Die Operation ist fehlgeschlagen, da die Sitzung zwischen dem Client und dem Server aus einem unbekannten Grund beendet wurde. Es ist nicht bekannt, ob der Client die Verbindung zum Server wiederherstellen kann, um das geplante Ereignis auszuführen.

Verfügt ein Zeitplan über ACTION=COMMAND als Parameter, und ist der Befehl kein IBM Spectrum Protect-Befehl, kann der Befehl andere Werte im Feld Ergebnis generieren.

Ursache
: Gibt die Ursache des Rückkehrcodes an.

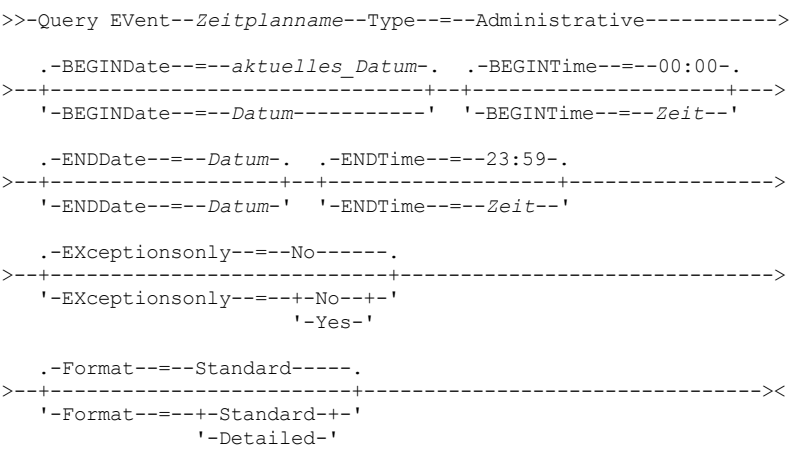
QUERY EVENT (Ereignisse für Verwaltungszeitpläne anzeigen)

Mit dem Befehl QUERY EVENT können geplante und abgeschlossene Ereignisse für ausgewählte Verwaltungsbefehlszeitpläne angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Zeitplanname (Erforderlich)

Gibt den Namen des Zeitplans an, für den Ereignisse angezeigt werden. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

Type=Administrative (Erforderlich)

Gibt an, dass die Abfrage Ereignisse für Verwaltungszeitpläne anzeigt.

BEGINDate

Gibt das Anfangsdatum des Zeitraums an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieses Zeitraums geplant ist, werden angezeigt. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage **oder** +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY +3 **oder** +3.
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage	TODAY-7 **oder** -7. Sollen Ereignisse abgefragt werden, deren Start während der vergangenen sieben Tage geplant war, BEGINDATE=TODAY-7 ENDDATE=TODAY oder BEGINDATE=-7 ENDDATE=TODAY angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt die Anfangszeit des Bereichs an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieses Zeitraums geplant ist, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 00:00.

Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Anfangsdatum	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Anfangsdatum	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum	NOW+03:00 **oder** +03:00. Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start in 3 Stunden geplant ist, kann entweder BEGINTIME=NOW+03:00 oder BEGINTIME=+03:00 angegeben werden. IBM Spectrum Protect zeigt dann Ereignisse um 12:00 Uhr am angegebenen Anfangsdatum an.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum	NOW-04:00 **oder** -04:00. Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start während der letzten 4 Stunden geplant war, kann entweder BEGINTIME=NOW-04:00 ENDTIME=NOW oder BEGINTIME=-04:00 ENDTIME=NOW angegeben werden. IBM Spectrum Protect zeigt dann Ereignisse um 5:00 Uhr am angegebenen Anfangsdatum an.

ENDDate

Gibt das Enddatum des Zeitraums an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start während dieser Zeit geplant war, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist der für BEGINDATE verwendete Wert.

Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage **oder** +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY +3 **oder** +3.
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage	TODAY-8 **oder** -8. Sollen Ereignisse abgefragt werden, deren Start während einer einwöchigen Periode, die gestern zu Ende ging, geplant war, kann entweder BEGINDATE=TODAY-8 ENDDATE=TODAY-1 oder BEGINDATE=-8 ENDDATE=-1 angegeben werden.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDTime

Gibt die Endzeit des Bereichs an, für den Ereignisse angezeigt werden sollen. Alle Ereignisse, deren Start innerhalb dieser Zeitspanne geplant war, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 23:59.
Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Enddatum	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Enddatum	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum	NOW+03:00 **oder** +03:00. Wird dieser Befehl um 9:00 Uhr ausgegeben, um Ereignisse abzufragen, deren Start in 3 Stunden geplant ist, kann entweder BEGINTIME=NOW ENDTIME=NOW+03:00 oder BEGINTIME=NOW ENDTIME=+03:00 angegeben werden.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum	NOW-04:00 **oder** -04:00

EXceptionsonly

Gibt die Art der Informationen an, die über geplante oder abgeschlossene Ereignisse gewünscht werden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No
: Gibt an, daß die Informationen zu vergangenen und projektierten Ereignissen angezeigt werden.

Yes
: Gibt an, daß die Ereignisse angezeigt werden, die fehlgeschlagen sind oder nicht wie geplant verarbeitet wurden.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard
: Gibt an, dass Teilinformationen für Ereignisse angezeigt werden.

Detailed
: Gibt an, dass die gesamten Informationen für Ereignisse angezeigt werden.

Beispiel: Ereignisse für einen bestimmten Verwaltungszeitplan auflisten

Teilinformationen für alle Ereignisse anzeigen, die für den Verwaltungszeitplan DOSADMIN geplant waren. Die Abfrage auf Ereignisse begrenzen, die am 30. März 1999 (03/30/1999) geplant sind. Den folgenden Befehl ausgeben:

```
query event dosadmin type=administrative
begindate=03/30/1999
enddate=03/30/1999

Geplanter Start      Ist-Start             Zeitplan-  Status
                                           klasse
-------------------- --------------------  ---------  ---------
03/30/1999 00:00:00  03/30/1999 00:00:01   DOSADMIN   Completed
03/30/1999 04:00:00  03/30/1999 04:00:01   DOSADMIN   Completed
03/30/1999 12:00:00                        DOSADMIN   Future
03/30/1999 16:00:00                        DOSADMIN   Future
```

Feldbeschreibungen

Geplanter Start
: Gibt das geplante Startdatum und die geplante Uhrzeit für das Ereignis an.

Ist-Start
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Client mit der Verarbeitung der geplanten Operation begonnen hat. Wurde die Ausführung des Zeitplans noch nicht gestartet, werden keine Informationen angezeigt.

Zeitplanname
: Gibt den Namen des Zeitplans an, der dieses Ereignis eingeleitet hat.

Status
: Für Verwaltungsbefehle oder Scripts, die WAIT=YES angeben, ist der Status eines geplanten Ereignisses STARTED, bis die mit dem Befehl oder dem Script angegebene Operation abgeschlossen ist. Der endgültige Status des geplanten Ereignisses hängt vom Rückkehrcode der Operation ab. Ist jedoch WAIT=YES angegeben und führt der Zeitplan ein Script aus, das PREVIEW=YES angibt, lautet der endgültige Status COMPLETED, es sei denn, das Script enthielt einen Syntaxfehler.

  Für Verwaltungsbefehle oder Scripts, die WAIT=NO angeben, ist der Status eines geplanten Ereignisses COMPLETED, wenn der geplante Befehl oder das Script gestartet wurde. Der Erfolg des Zeitplans ist nicht vom Erfolg der Operation abhängig, die mit dem Befehl oder dem Script ausgeführt wurde.

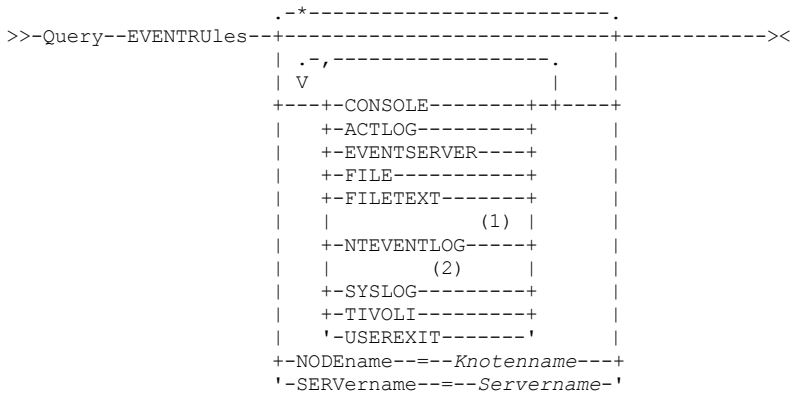
QUERY EVENTRULES (Regeln für Server- oder Clientereignisse abfragen)

Mit diesem Befehl kann die History von Ereignissen, die von einem bestimmten Empfänger aktiviert oder inaktiviert wurden, für den Server oder einen Client-Knoten angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Anmerkungen:

1. Dieser Parameter ist nur für das Windows-Betriebssystem verfügbar.
2. Dieser Parameter ist nur für das Linux-Betriebssystem verfügbar.

Parameter

Empfänger
: Gibt den Namen eines oder mehrerer Empfänger für aktivierte Ereignisse an. Dieser Parameter ist wahlfrei.

  Es kann ein Platzhalterzeichen verwendet werden, um alle Empfänger anzugeben.

Gültige Werte sind:

CONSOLE
: Gibt die Standardkonsole als Empfänger an.

ACTLOG
: Gibt das IBM Spectrum Protect-Aktivitätenprotokoll als Empfänger an.

EVENTSERVER
: Gibt den Ereignisserver als Empfänger an.

FILE
: Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist ein Satz in der Datei, und eine Person kann jedes protokollierte Ereignis nicht einfach lesen.

FILETEXT
: Gibt eine Benutzerdatei als Empfänger an. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.


NTEVENTLOG
: Gibt das Windows-Anwendungsprotokoll als Empfänger an.


SYSLOG
: Gibt das Linux-Systemprotokoll als Empfänger an.

TIVOLI
: Gibt Tivoli Management Environment (TME) als Empfänger an.

USEREXIT
: Gibt eine benutzerdefinierte Routine, in die IBM Spectrum Protect Informationen schreibt, als Empfänger an.

NODEname
: Gibt einen Knotennamen an, der abgefragt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, bezieht sich die Abfrage auf Ereignisregeln für den Server, der diesen Befehl ausführt.

SERver
: Gibt einen Servernamen an, der abgefragt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um einen Namen anzugeben. Der Benutzer kann NODENAME oder SERVERNAME angeben. Wird keiner der Parameter angegeben, bezieht sich die Abfrage auf Ereignisregeln für den Server, der diesen Befehl ausführt.

Beispiel: Die History von Clientereignissen für die Serverkonsole anzeigen

Die History von Clientereignissen anzeigen, die für die Serverkonsole und für Aktivitätenprotokollempfänger aktiviert oder inaktiviert sind.

```
query eventrules console,actlog nodename=*

Datum/Zeit           Client-Ereignisregeln

-------------------- ------------------------------------------------
05/29/97 13:39:58    ENABLE EVENTS CONSOLE ANE4001 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4962 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4963 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4965 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4966 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4967 NODENAMES=JEE
05/30/97 13:46:25    DISABLE EVENTS ACTLOG ANE4968 NODENAMES=JEE
05/30/97 14:24:20    ENABLE EVENTS CONSOLE ANE4015 NODENAMES=RON
05/30/97 14:24:50    ENABLE EVENTS CONSOLE ANE4026 NODENAMES=DONNA
05/30/97 14:25:59    ENABLE EVENTS CONSOLE ANE4015 NODENAMES=DONNA
```

Beispiel: Die History von Clientereignissen für alle Empfänger anzeigen

Die History von Serverereignissen anzeigen, die für alle Empfänger aktiviert oder inaktiviert sind.

```
query eventrules

Datum/Zeit           Server-Ereignisregeln
-------------------- ------------------------------------------------
05/22/97 14:35:13    ENABLE EVENTS CONSOLE ANR2578
05/30/97 14:29:31    ENABLE EVENTS CONSOLE ANR0272
05/30/97 14:31:46    ENABLE EVENTS USEREXIT ANR0130
05/30/97 14:31:54    ENABLE EVENTS USEREXIT ANR0131
05/30/97 14:50:28    ENABLE EVENTS USEREXIT ANR0266
```

Feldbeschreibungen

Datum/Zeit
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der das Ereignis aktiviert oder inaktiviert wurde.

Client-Ereignisregeln
: Gibt die Clientereignisse an, die für die angegebenen Empfänger aktiviert oder inaktiviert wurden.

Server-Ereignisregeln
: Gibt die Serverereignisse an, die für die angegebenen Empfänger aktiviert oder inaktiviert wurden.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY ENABLED

Befehl	Beschreibung
BEGIN EVENTLOGGING	Startet das Ereignisprotokoll für einen bestimmten Empfänger.
DISABLE EVENTS	Inaktiviert bestimmte Ereignisse für Empfänger.
ENABLE EVENTS	Aktiviert bestimmte Ereignisse für Empfänger.
END EVENTLOGGING	Beendet das Ereignisprotokoll für einen bestimmten Empfänger.
QUERY ENABLED	Zeigt aktivierte bzw. inaktivierte Ereignisse für einen bestimmten Empfänger an.

QUERY EVENTSERVER (Ereignisserver abfragen)

Mit diesem Befehl kann der Name des Ereignisservers angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query EVENTSERVer-------------------------------------------><
```

Beispiel: Den Namen des Ereignisservers anzeigen

Den Namen des Ereignisservers anzeigen.

```
query eventserver

ANR1669I Server EVENT
ist als Ereignisserver definiert.
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY EVENTSERVER

Befehl	Beschreibung
BEGIN EVENTLOGGING	Startet das Ereignisprotokoll für einen bestimmten Empfänger.
DEFINE EVENTSERVER	Definiert einen Server als Ereignisserver.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DELETE EVENTSERVER	Löscht Verweise auf den Ereignisserver.
DELETE SERVER	Löscht die Definition eines Servers.
END EVENTLOGGING	Beendet das Ereignisprotokoll für einen bestimmten Empfänger.

QUERY EXPORT (Aktive oder ausgesetzte Exportoperationen abfragen)

Mit diesem Befehl können alle wieder anlauffähigen Exportoperationen aufgelistet werden. Ein wiederanlauffähiger Export ist eine Exportoperation zwischen Servern, deren Wert für FILEDATA nicht NONE ist. Es werden nur aktive Exportoperationen zwischen Servern angezeigt, die ausgesetzt werden können.

EXPORT NODE- oder EXPORT SERVER-Operationen mit FILEDATA=NONE werden nicht angezeigt. Außerdem zeigt der Befehl QUERY EXPORT keine Exportoperationen, bei denen die Zieleinheit eine Einheit mit sequenziellen oder virtuellen Datenträgern ist.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                .-*-------------.
>>-Query EXPort--+---------------+------------------------------>
                 '---Export-ID---'

   .-STate--=--ALl-----------.
>--+-------------------------+--+---------------------------+--->
   '-STate--=--+-ALl-------+-'  '-PROCess-----Prozessnummer-'
               +-RUnning---+
               '-SUSpended-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Export-ID
: Dieser optionale Parameter ist die eindeutige Zeichenfolge-ID für die Exportoperation zwischen Servern. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. In diesem Fall werden alle übereinstimmenden Exportoperationen abgefragt. Wird kein Wert für diesen Parameter angegeben und wird auch keine PROZESS-ID angegeben, werden alle Exportoperationen abgefragt.

STate
: Dieser optionale Parameter fragt den Status der gültigen Exportoperationen zwischen Servern ab. Der Standardwert ist ALL. Gültige Werte sind:

  ALl
  : Alle aktiven und ausgesetzten Exportoperationen zwischen Servern werden aufgelistet.

  RUnning
  : Alle aktiven Exportoperationen zwischen Servern, die auswählbare Dateien angeben oder Dateien auf den Zielserver exportieren, werden aufgelistet.

  SUSpended
  : Alle ausgesetzten Exportoperationen zwischen Servern werden aufgelistet. Die Ausführung dieser ausgesetzten Operationen wurde durch einen Fehler oder durch die Ausgabe des Befehls SUSPEND EXPORT gestoppt.

PROCess
: Dieser optionale Parameter gibt die Nummer einer aktiven Exportoperation zwischen Servern an, die Sie abfragen wollen. Wird PROCESS angegeben, zeigt IBM Spectrum Protect nur die aktive Exportoperation zwischen Servern an, die der Prozessnummer zugeordnet ist. Wird PROCESS nicht angegeben, zeigt IBM Spectrum Protect Informationen zu allen Exportoperationen zwischen Servern an. Sie können diesen Parameter nicht angeben, wenn Sie eine Export-ID oder den Parameter STATE mit dem Wert SUSPENDED angeben.

Format
: Dieser optionale Parameter gibt an, wie die Informationen angezeigt werden. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen für die angegebenen Exportoperationen angezeigt werden.

  Detailed
  : Falls angegeben, werden alle verfügbaren Informationen für die Exportoperationen angezeigt.

Beispiel: Aktive und ausgesetzte Exportoperationen anzeigen

Informationen für alle Exportoperationen auflisten, die momentan aktiv oder ausgesetzt sind. Geben Sie den folgenden Befehl aus:

```
query export state=all

Export-          Startzeit     Status     Prozess-    Befehl
ID                                          ID
-------------  -----------  ---------  --------  ------------------
MYEXPORTNODE   01/24/2007   Ausgesetzt    --     Export NODE
               10:30:03                          me,you,them
                                                 filespace=c$
                                                 nametype=unicode
                                                 filedata=all
                                                 durunits=indefinite
                                                 toserver=athens
                                                 exportid=MYEXPORTNODE

EXPORT_HOME_    01/25/2007   Aktiv         11    Export NODE n2,n3,n4
DIRS           09:30:03                          filespace=/home
                                                 nametype=server
                                                 filedata=all
                                                 durunits=indefinite
                                                 toserver=athens
                                                 exportid=EXPORT_HOME_DIRS

EXPORT_NODE_    01/25/2007   Aktiv, nicht  --    Export NODE n5,n6,n7
```

```
0001          14:30:33      aussetzbar          filespace=d$
                                                nametype=unicode
                                                filedata=archive
                                                durunits=indefinite
                                                toserver=athens
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Informationen zu einer aktiven Exportoperation anzeigen

Informationen für die momentan aktive Exportoperation mit Prozessnummer "7" auflisten. Den folgenden Befehl ausgeben:

```
query export process=7
```

```
Export-         Startzeit     Status     Prozess-    Befehl
ID                                         ID
----------    ----------  ------  ------   --------
MYEXPORTNODE  01/24/2007  Aktiv     7      Export NODE
              10:30:03                     me,you,them
                                           filespace=c$
                                           nametype=unicode
                                           filedata=all
                                           toserver=athens
                                           exportid=MYEXPORTNODE
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Informationen zu allen ausgesetzten Exportoperationen anzeigen

Informationen für alle Exportoperationen auflisten, die momentan ausgesetzt sind. Geben Sie den folgenden Befehl aus:

```
query export state=suspended format=detailed
```

```
                                Export-ID :  MyExportNode
                                Startzeit :  01/24/2007 10:30:03
                                   Status :  Ausgesetzt
                                Prozess-ID :  --
                                     Befehl: Export NODE m* filespace=c$
                                             nametype=unicode
                                             filedata=all durunits=indefinite
                                             toserver=athens
                                     Phase :  Dateiliste vollständig.
                                              Auswählbare Dateien werden exportiert
                    Gesamtausführungszeit :  3 Tag 0 Stunden 24 Minuten
    Ausführungszeit des aktuellen Prozesses :
        Anzahl Neustarts der Exportoperation:  0
    Datum und Uhrzeit des letzten Neustarts :  --
   Datum und Uhrzeit der letzten Aussetzung :  01/25/2007 08:30:11
              Exportierte Maßnahmendomänen :  0
              Exportierte Maßnahmengruppen :  0
                     Exportierte Zeitpläne :  0
            Exportierte Verwaltungsklassen :  0
                 Exportierte Kopiengruppen :  0
               Exportierte Administratoren :  1
                Exportierte Optionsgruppen :  0
            Exportierte Knotendefinitionen :  3
      Exportierte Dateibereichsdefinitionen :  7
           Exportierte Archivierungsdateien :  50.000
              Exportierte Sicherungsdateien :  150.000
     Exportierte speicherverwaltete Dateien :  0
         Übersprungene Archivierungsdateien :  0
            Übersprungene Sicherungsdateien :  25
   Übersprungene speicherverwaltete Dateien :  0
           Summe der übertragenen Byte (MB) :  7.000
         Summe der zu übertragenden Dateien :  900.000
                        Verbleibende Dateien :  700.000
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Informationen zu Exportoperation zwischen Servern anzeigen

Listen Sie detaillierte Informationen zu allen Exportoperationen auf, die momentan aktiv sind. Geben Sie den folgenden Befehl aus:

```
query export state=running format=detailed
```

```
                                Export-ID :  export_HOME_Dirs
                                Startzeit :  01/25/2007 09:30:03
                                   Status :  Aktiv
                                Prozess-ID :  11
                                     Befehl:  Export NODE n2,n3,n4
```

```
                                        filespace=/home nametype=
                                      server filedata=all
                                      toserver=athens
                                Phase :  Auswählbare Dateien angeben
                                         und exportieren
                  Gesamtausführungszeit :  0 Tage 22 Stunden 0 Minuten
 Ausführungszeit des aktuellen Prozesses :  01:30:00
     Anzahl Neustarts der Exportoperation:  4
 Datum und Uhrzeit des letzten Neustarts :  02/01/2007 11:00:03
Datum und Uhrzeit der letzten Aussetzung :  01/31/2007 05:01:00
           Exportierte Maßnahmendomänen :  0
           Exportierte Maßnahmengruppen :  0
                  Exportierte Zeitpläne :  0
          Exportierte Verwaltungsklassen :  0
               Exportierte Kopiengruppen :  0
             Exportierte Administratoren :  1
              Exportierte Optionsgruppen :  0
          Exportierte Knotendefinitionen :  3
   Exportierte Dateibereichsdefinitionen :  7
        Exportierte Archivierungsdateien :  0
           Exportierte Sicherungsdateien :  1000
  Exportierte speicherverwaltete Dateien :  0
      Übersprungene Archivierungsdateien :  0
         Übersprungene Sicherungsdateien :  0
Übersprungene speicherverwaltete Dateien :  0
        Summe der übertragenen Byte (MB) :  50
      Summe der zu übertragenden Dateien :  400.000
                   Verbleibende Dateien :  399.000
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Export-ID
: Die eindeutige ID, die dieser Exportoperation zwischen Servern zugeordnet ist.

Startzeit
: Der Zeitpunkt (Datum und Uhrzeit), an dem diese Exportoperation zum ersten Mal eingeleitet wurde.

Status
: Der aktuelle Status dieser Exportoperation. Mögliche Werte sind:

  Aktiv - Nicht aussetzbar
  : Die Operation ist aktiv und überträgt gerade Definitionen an den Zielserver. Der Prozess kann nicht ausgesetzt werden. Wenn in diesem Status ein Prozessfehler auftritt, können Sie den Prozess nicht erneut starten.

  Aktiv
  : Die Operation ist aktiv und sucht gerade nach auswählbaren Dateien oder überträgt gerade Dateidaten an den Zielserver.

  Aktiv - Aussetzen wird ausgeführt
  : Die Operation wird gerade als Folge eines Befehls SUSPEND EXPORT ausgesetzt. Die Exportoperation ist vollständig ausgesetzt, wenn alle Daten aus der Exportoperation gesichert sind. Eine Exportoperation in diesem Status antwortet nicht auf die folgenden Befehle:

    - CANCEL PROCESS
    - CANCEL EXPORT
    - RESTART EXPORT
    - SUSPEND EXPORT

  Ausgesetzt
  : Die Ausführung der Operation wurde durch einen Fehler gestoppt oder durch den Befehl SUSPEND EXPORT ausgesetzt.

Prozess-ID
: Die Prozess-ID für die Exportoperation im Status "Wird initialisiert" oder "Aktiv".

Befehl
: Der vollständig ausgegebene Befehl zum Starten dieser Exportoperation zwischen Servern.

Phase
: Der aktuelle Schritt, der von der Operation gerade ausgeführt wird. Die gültigen Phasen sind in der Reihenfolge aufgeführt, in der sie ausgeführt werden:

  Definitionen auf Zielserver erstellen
  : Die Operation exportiert Definitionen. Der Prozess kann nicht ausgesetzt werden. Schlägt der Prozess in dieser Phase fehl, kann er nicht erneut gestartet werden.

  Auswählbare Dateien angeben und exportieren
  : Die Operation erstellt eine Liste der auswählbaren Dateien für den Export. Einige Dateien können in dieser Phase auch an den Zielserver übertragen werden. Der Prozess kann in dieser Phase ausgesetzt werden. Schlägt der Prozess in dieser Phase fehl, kann er erneut gestartet werden.

  Dateiliste vollständig. Auswählbare Dateien werden exportiert.

Die Erstellung der Liste der auswählbaren Dateien für den Export ist beendet. Die Dateien werden jetzt an das Ziel übertragen. Der Prozess kann in dieser Phase ausgesetzt werden. Schlägt der Prozess in dieser Phase fehl, kann er erneut gestartet werden.

Gesamtausführungszeit
: Die Gesamtausführungszeit für diese Exportoperation zwischen Servern. Beispiel: Wurde diese Operation gestartet und dann zweimal ausgesetzt und erneut gestartet, gibt dieser Wert die Gesamtausführungszeit aller drei aktiven Prozesse der Exportoperation an.

Ausführungszeit des aktuellen Prozesses
: Die Ausführungszeit des aktiven Prozesses einer Exportoperation zwischen Servern. Für eine ausgesetzte Operation wird kein Wert angezeigt, weil kein aktiver Prozess vorhanden ist.

Anzahl Neustarts der Exportoperation
: Gibt an, wie oft die Exportoperation zwischen Servern erneut gestartet wurde.

Datum und Uhrzeit des letzten Neustarts
: Das Datum und die Uhrzeit des letzten Neustarts dieser Exportoperation zwischen Servern.

Datum und Uhrzeit der letzten Aussetzung
: Das Datum und die Uhrzeit der letzten Aussetzung dieser Exportoperation zwischen Servern.

Exportierte Maßnahmendomänen
: Die Anzahl der Maßnahmendomänendefinitionen, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Maßnahmengruppen
: Die Anzahl der Maßnahmengruppendefinitionen, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Zeitpläne
: Die Anzahl der Zeitplandefinitionen, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Verwaltungsklassen
: Die Anzahl der Verwaltungsklassendefinitionen, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Kopiengruppen
: Die Anzahl der Kopiengruppendefinitionen, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Administratoren
: Die Anzahl der Administratordefinitionen, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Optionsgruppen
: Die Anzahl der Optionsgruppendefinitionen, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Knotendefinitionen
: Die Anzahl der Knotendefinitionen, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Dateibereichsdefinitionen
: Die Anzahl der Dateibereichsdefinitionen, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die erfolgreich auf den Zielserver exportiert wurden.

Exportierte speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die erfolgreich auf den Zielserver exportiert wurden.

Übersprungene Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die zum Exportieren ausgewählt werden konnten, aber übersprungen wurden.

Übersprungene Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die zum Exportieren ausgewählt werden konnten, aber übersprungen wurden.

Übersprungene speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die zum Exportieren ausgewählt werden konnten, aber übersprungen wurden.

Summe der übertragenen Byte (MB)
: Die Gesamtzahl der bisher an den Zielserver übertragenen Byte für diese Exportoperation.

Summe der zu übertragenden Dateien
: Die Gesamtzahl der an den Zielserver zu übertragenden Dateien für diese Exportoperation.

Verbleibende Dateien
: Die Gesamtzahl der Dateien, die für diese Exportoperation noch an den Zielserver übertragen werden müssen.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY EXPORT

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
CANCEL EXPORT	Löscht eine ausgesetzte Exportoperation.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT SERVER	Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server.
IMPORT NODE	Schreibt Clientknotendaten von externen Datenträgern zurück.
IMPORT SERVER	Schreibt den gesamten Server oder einen Teil davon von externen Datenträgern zurück.

Befehl	Beschreibung
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
RESTART EXPORT	Startet eine ausgesetzte Exportoperation erneut.
SUSPEND EXPORT	Setzt eine aktive Exportoperation aus.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

QUERY EXTENTUPDATES (Aktualisierte Datenbereiche abfragen)

Verwenden Sie diesen Befehl, um Informationen zu Aktualisierungen an Datenbereichen in Verzeichniscontainerspeicherpools anzuzeigen und zu bestimmen, welche Datenbereiche gelöscht werden und welche Datenbereiche zum Löschen auswählbar sind.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query EXTENTUPDates--Poolname------------------------------><
```

Parameter

Poolname (Erforderlich)
: Gibt den Speicherpool an, der abgefragt werden soll. Sie können zur Angabe dieses Namens keine Platzhalterzeichen verwenden.

Beispiel: Informationen zu Aktualisierungen an Datenbereichen anzeigen

Zeigen Sie Informationen zu Aktualisierungen an Datenbereichen an, indem Sie den folgenden Befehl ausgeben:

```
query extentupdates

     Anzahl Bereiche mit anstehender Aktualisierung: 0
            Anzahl nicht referenzierter Bereiche: 0
    Anzahl der zum Löschen auswählbaren Bereiche: 0
               Wiederverwendungsverzögerung (Tage) für Bereiche: 1
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Anzahl Bereiche mit anstehender Aktualisierung
: Gibt die Anzahl Datenbereichsreferenzen an, für die eine Aktualisierung im Verzeichniscontainerspeicherpool ansteht. Daten, die im Verzeichniscontainerspeicherpool gespeichert werden, erhöhen die Anzahl Referenzen; Daten, die gelöscht werden, verringern die Anzahl Referenzen.

Anzahl nicht referenzierter Bereiche
: Gibt die Anzahl Datenbereiche an, die nicht im Verzeichniscontainerspeicherpool referenziert werden. Sie können die Datenbereiche löschen, wenn sie nicht erneut innerhalb des im Befehl DEFINE STGPOOL angegebenen Verzögerungszeitraums für Wiederverwendung referenziert werden.

Anzahl der zum Löschen auswählbaren Bereiche
: Gibt die Anzahl Datenbereiche an, die aus dem Speicherpool gelöscht werden können. Für die Datenbereiche wird der im Befehl DEFINE STGPOOL angegebene Verzögerungszeitraum für Wiederverwendung überschritten.

Wiederverwendungsverzögerung (Tage) für Bereiche
: Gibt die Wiederverwendungsverzögerung für Datenbereiche in Tagen an.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY EXTENTUPDATES

Befehl	Beschreibung
DEFINE STGPOOL (Verzeichniscontainer)	Definiert einen Verzeichniscontainerspeicherpool.
DELETE STGPOOLDIRECTORY	Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool.

QUERY FILESPACE (Dateibereiche abfragen)

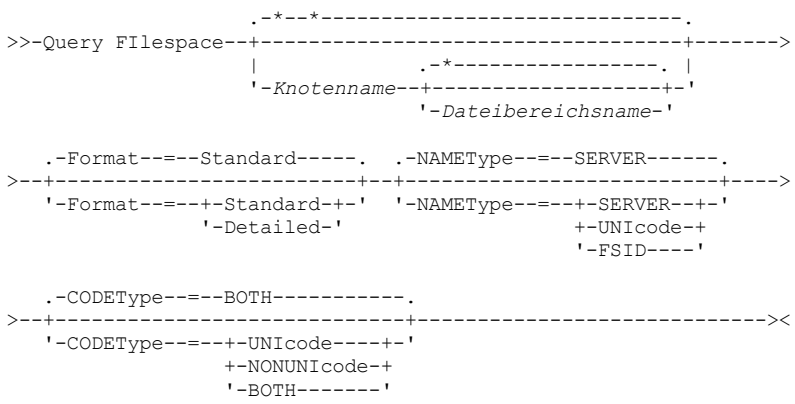
Mit diesem Befehl können Informationen über Dateibereiche angezeigt werden, die zu einem Clientknoten gehören. Die Ausgabe dieses Befehls schließt die Ergebnisse der letzten Teilsicherung oder Replikation ein.

Tipp: Verfügt ein Knoten über mehrere Dateibereiche, können Sie einen Befehl DELETE FILESPACE für einen der Dateibereiche ausgeben. Geben Sie jedoch während des Löschprozesses einen Befehl QUERY FILESPACE für den Knoten aus, zeigt die Ausgabe keine Dateibereiche an. Um genaue Informationen zu den verbleibenden Dateibereichen zu erhalten, geben Sie den Befehl QUERY FILESPACE aus, nachdem der Löschprozess beendet wurde.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Knotenname
: Gibt den Clientknoten an, zu dem der Dateibereich gehört. Dieser Name kann mithilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert ist alle Clientknotennamen.

  Für diesen Parameter muss ein Wert angegeben werden, wenn ein Dateiname angegeben wird.

Dateibereichsname
: Gibt den Namen des Dateibereichs an, der abgefragt werden soll. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden alle Dateibereiche abgefragt.

  Wenn ein Server Clients einschließt, die Unicode-fähige Dateibereiche verwenden, muss der Server möglicherweise den eingegebenen Namen konvertieren. Beispielsweise muss der Server gegebenenfalls den Dateibereichsnamen, den Sie eingeben, aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Weitere Informationen enthält die Beschreibung des Parameters NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

  Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Mit dem Befehl QUERY FILESPACE kann die korrekte Schreibweise für den abzufragenden Dateibereich bestimmt werden.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Sie können einen der folgenden Werte angeben:

  Standard
  : Gibt an, dass Teilinformationen für den angegebenen Dateibereich angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen für den angegebenen Dateibereich angezeigt werden.

NAMEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode verfügt. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients verwenden, die über die Betriebssysteme Windows, Macintosh OS X und NetWare verfügen.

  Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

  SERVER
  : Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

UNIcode
: Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

FSID
: Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

CODEType
: Angeben, welche Art von Dateibereichen in der Operation berücksichtigt werden soll. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Sie können einen der folgenden Werte angeben:

  UNIcode
  : Nur Dateibereiche einschließen, die in Unicode sind.

  NONUNIcode
  : Nur Dateibereiche einschließen, die nicht in Unicode sind.

  BOTH
  : Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

Beispiel: Alle Dateibereiche auflisten

Alle Dateibereiche abfragen, die allen Clientknoten zugeordnet sind.

```
query filespace
```

```
Knoten- Dateibe-   FSID  Platt-   Dateibe-  Ist        Kapazi-   %
name    reichsname       form     reichstyp Dateiber.  tät      Ausl.
                                            Unicode?
------ ----------- ----  -------   --------  --------  -------- ----
JOE        \\joe\c$    1  WinNT     NTFS        Yes     2.502,3  75,2
JOE        \\joe\d$    2  WinNT     NTFS        Yes     6.173,4  59,6
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Dateibereichsinformationen zu einem virtuellen Dateibereich anzeigen

Ausführliche Informationen zu dem Dateibereich /HomeDir anzeigen, der eine virtuelle Dateibereichszuordnung ist und zu dem NAS-Knoten NAS1 gehört.

```
query filespace nas1 /HomeDir
```

```
Knoten- Dateibe-   FSID  Platt-   Dateibe-  Ist        Kapazi-   %
name    reichsname       form     reichstyp Dateiber.  tät      Ausl.
                                            Unicode?
----   ----------- ----  -------   --------  ---------  -------- ----
NAS1    /HomeDir     1    NetApp  WAFL (VFS)     No     2.502,3  75,2
```

Für Feldbeschreibungen siehe Feldbeschreibungen.
Wichtig: Möglicherweise werden die erwarteten Ergebnisse nicht angezeigt, nachdem ein ausführliches Format angefordert wurde, da einige Felder von der API-Anwendung ausgefüllt werden müssen. Zu diesen Feldern gehören:

- Dateibereichstyp
- Plattform
- Kapazität
- Auslastung in %
- Startdatum/-zeit der letzten Sicherung
- Fertigstellungsdatum/-zeit der letzten Sicherung

Weitere Informationen zu bestimmten Feldern, die von der API aktualisiert werden, befinden sich im Handbuch *IBM Spectrum Protect: Verwendung der Anwendungsprogrammierschnittstelle*.

Beispiel: Ausführliche Dateibereichsinformationen zu einem bestimmten Dateibereich und Knoten anzeigen

Ausführliche Informationen zu dem Dateibereich \\joe\c$ anzeigen, der zum Clientknoten JOE gehört.

```
query filespace joe \\joe\c$ nametype=unicode format=detailed
```

```
                                    Knotenname: JOE
                                         Dateibereichsname: \\joe\c$
                                Hexadezimaler Dateibereichsname: 5c5c6a6f655c6324
                                                          FSID: 1
                                   Name der Kollokationsgruppe: FSGRP1
```

```
                                        Plattform: WinNT
                                   Dateibereichstyp: NTFS
                               Ist Dateibereich Unicode?: Yes
                                        Kapazität: 2.502,3
                                    Auslastung in %: 75,2
                              Start der letzten Sicherung:
                          Tage seit Start der letzten Sicherung:
                                Abschluss der letzten Sicherung:
                     Tage seit Abschluss der letzten Sicherung:
                      Startdatum/-zeit der letzten Replikation: 12/02/2012, 12:42:00
           Tage seit Start der letzten Knotenreplikation: 30
        Fertigstellungsdatum/-zeit der letzten Replikation: 12/02/2012, 12:42:00
               Tage seit Abschluss der letzten Replikation: 30
        Datum/Zeit der letzten Sicherung des Clients (UTC): 06/02/2013, 09:10:00
     Datum/Zeit der letzten Archivierung des Clients (UTC): 06/02/2013, 09:10:00
              Name der Replikationsregel für Sicherungsdaten: ACTIVE_DATA
            Status der Replikationsregel für Sicherungsdaten: ENABLED
          Name der Replikationsregel für Archivierungsdaten: DEFAULT
       Status der Replikationsregel für Archivierungsdaten: ENABLED
    Name der Replikationsregel für speicherverwaltete Daten: NONE
  Status der Replikationsregel für speicherverwaltete Daten: DISABLED

                                      Typ für Gefährdung: Angepasstes Intervall
                                   Gefährdungsintervall: 2,222
                                             Stillgelegt: Nein
                                   Datum der Stilllegung:
                                             MAC-Adresse:
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Wichtig: Möglicherweise werden die erwarteten Ergebnisse nicht angezeigt, nachdem ein ausführliches Format angefordert wurde, da einige Felder von der API-Anwendung ausgefüllt werden müssen. Zu diesen Feldern gehören:

- Dateibereichstyp
- Plattform
- Kapazität
- Auslastung in %
- Startdatum/-zeit der letzten Sicherung
- Abschluss der letzten Sicherung

Weitere Informationen zu bestimmten Feldern, die von der API aktualisiert werden, befinden sich im Handbuch *IBM Spectrum Protect: Verwendung der Anwendungsprogrammierschnittstelle*.

Knotenname
: Gibt den Namen des Clientknotens an.

Dateibereichsname
: Der Name des Dateibereichs, der zu dem Knoten gehört.

  Dateibereichsnamen können eine andere Zeichenumsetztabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

  Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

Hexadezimaler Dateibereichsname
: Gibt den hexadezimalen Namen des Dateibereichs für den Clientknoten im UTF-8-Format an.

FSID
: Gibt die Dateibereichs-ID des Dateibereichs an.

Name der Kollokationsgruppe
: Der Name der Kollokationsgruppe (sofern vorhanden), zu der der Dateibereich gehört.

Plattform
: Gibt die Plattform für den Clientknoten an.

Dateibereichstyp
: Gibt den Typ des Dateibereichs an.

  Ein Dateibereichstyp, dem "(VFS)" angehängt ist, gibt an, dass dieser Dateibereichsname eine virtuelle Dateibereichszuordnung für einen Verzeichnispfad auf einer NAS-Einheit ist.

Ist Dateibereich Unicode?
: Gibt an, ob der Dateibereich in Unicode ist.

Kapazität
: Gibt den Speicherbereich in Megabyte an, der diesem Dateibereich auf dem Clientknoten zugeordnet ist.

  Bei einem Dateibereich, der eine virtuelle Dateibereichszuordnung für einen Verzeichnispfad ist, gibt dieses Feld die Kapazität des Dateibereichs an, in dem sich der Verzeichnispfad befindet.

Auslastung in %
: Gibt den Prozentsatz des belegten Dateibereichs an.

  Bei einem Dateibereich, der eine virtuelle Dateibereichszuordnung für einen Verzeichnispfad ist, wird die prozentuale Auslastung als Prozentsatz der Kapazität des Dateibereichs berechnet, der von dem Verzeichnis zum Zeitpunkt der letzten Gesamtsicherung belegt wurde.

Startdatum/-zeit der letzten Sicherung
: Gibt das Startdatum und die Startzeit der letzten Teilsicherung des Dateibereichs an.

Tage seit Start der letzten Sicherung
: Gibt die Anzahl der Tage seit dem Start der letzten Teilsicherung des Dateibereichs an.

Abschluss der letzten Sicherung
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die letzte Teilsicherung des Dateibereichs abgeschlossen wurde.

Tage seit Abschluss der letzten Sicherung
: Gibt die Anzahl der Tage seit dem Abschluss der letzten Teilsicherung des Dateibereichs an.

Startdatum/-zeit der letzten Replikation
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die letzte Replikation der Dateibereichsdaten gestartet wurde.

Tage seit Start der letzten Replikation
: Gibt die Anzahl der Tage seit dem Start der letzten Replikation der Dateibereichsdaten an.

Fertigstellungsdatum/-zeit der letzten Replikation
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die letzte Replikation der Dateibereichsdaten beendet wurde.

Tage seit Abschluss der letzten Replikation
: Gibt die Anzahl der Tage seit dem Ende der letzten Replikation der Dateibereichsdaten an.

Datum/Zeit der letzten Sicherung des Clients (UTC)
: Das Datum und die Uhrzeit (in koordinierter Weltzeit - UTC) der letzten Sicherungsoperation für diesen Dateibereich.

Datum/Zeit der letzten Archivierung des Clients (UTC)
: Das Datum und die Uhrzeit (in koordinierter Weltzeit - UTC) der letzten Archivierungsoperation für diesen Dateibereich.

Name der Replikationsregel für Sicherungsdaten
: Gibt die Replikationsregel an, die für Sicherungsdaten in dem Dateibereich gilt. Die folgenden Werte sind gültig:

  ALL_DATA
  : Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

  ACTIVE_DATA
  : Repliziert nur aktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert.
    Achtung: Wenn Sie ACTIVE_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

    - Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
    - Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
    - Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

    Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

  ALL_DATA_HIGH_PRIORITY
  : Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit einer hohen Priorität repliziert.

  ACTIVE_DATA_HIGH_PRIORITY

    Diese Regel entspricht der Replikationsregel ACTIVE_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

  DEFAULT
  : Repliziert Sicherungsdaten gemäß der Clientknotenregel für Sicherungsdaten. Lautet die Clientknotenregel für Sicherungsdaten DEFAULT, werden Sicherungsdaten gemäß der Serverregel für Sicherungsdaten repliziert.

  NONE
  : Sicherungsdaten in dem Dateibereich werden nicht repliziert.

Status der Replikationsregel für Sicherungsdaten
: Gibt an, ob die Replikation der Sicherungsdaten in dem Dateibereich aktiviert oder inaktiviert ist. Lautet der Status 'Aktiviert', können Sicherungsdateien für die Replikation ausgewählt werden. Lautet der Status 'Inaktiviert', können Sicherungsdateien nicht für die Replikation ausgewählt werden.

Name der Replikationsregel für Archivierungsdaten
: Gibt die Replikationsregel an, die für Archivierungsdaten in dem Dateibereich gilt. Die folgenden Werte sind gültig:

  ALL_DATA
  : Repliziert Archivierungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

  ALL_DATA_HIGH_PRIORITY
  : Repliziert Archivierungsdaten. Die Daten werden mit einer hohen Priorität repliziert.

  DEFAULT
  : Repliziert Archivierungsdaten gemäß der Clientregel für Archivierungsdaten. Lautet die Clientregel für Archivierungsdaten DEFAULT, werden Archivierungsdaten gemäß der Serverregel für Archivierungsdaten repliziert.

  NONE
  : Archivierungsdaten in dem Dateibereich werden nicht repliziert.

Status der Replikationsregel für Archivierungsdaten
: Gibt an, ob die Replikation der Archivierungsdaten in dem Dateibereich aktiviert oder inaktiviert ist. Lautet der Status 'Aktiviert', können Archivierungsdateien für die Replikation ausgewählt werden. Lautet der Status 'Inaktiviert', können Archivierungsdateien nicht für die Replikation ausgewählt werden.

Name der Replikationsregel für speicherverwaltete Daten
: Gibt die Replikationsregel an, die für speicherverwaltete Daten in dem Dateibereich gilt. Die folgenden Werte sind gültig:

  ALL_DATA
  : Repliziert speicherverwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.

  ALL_DATA_HIGH_PRIORITY
  : Repliziert speicherverwaltete Daten. Die Daten werden mit einer hohen Priorität repliziert.

  DEFAULT
  : Repliziert speicherverwaltete Daten gemäß der Clientregel für speicherverwaltete Daten. Lautet die Clientregel für speicherverwaltete Daten DEFAULT, werden speicherverwaltete Daten gemäß der Serverregel für speicherverwaltete Daten repliziert.

  NONE
  : Speicherverwaltete Daten in dem Dateibereich werden nicht repliziert.

Status der Replikationsregel für speicherverwaltete Daten
: Gibt an, ob die Replikation der speicherverwalteten Daten in dem Dateibereich aktiviert oder inaktiviert ist. Lautet der Status 'Aktiviert', können speicherverwaltete Dateien für die Replikation ausgewählt werden. Lautet der Status 'Inaktiviert', können speicherverwaltete Dateien nicht für die Replikation ausgewählt werden.

Typ für Gefährdung
: Gibt den Auswertungstyp für Gefährdung an. Die gültigen Werte sind 'Standard', 'Übergangen' oder 'Angepasst'. 'Standard' gibt an, dass der Knoten mit demselben Intervall ausgewertet wird, das für die Knotenklassifizierung mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde. 'Übergangen' gibt an, dass der Gefährdungsstatus für den Knoten nicht vom Statusmonitor ausgewertet wird. 'Angepasst' gibt an, dass der Knoten mit dem Intervall ausgewertet wird, das mit dem Befehl SET VMATRISKINTERVAL angegeben wurde, und nicht mit dem Intervall, das mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde.

Gefährdungsintervall
: Gibt die Zeit in Stunden zwischen Clientsicherungsaktivitäten an, bevor der Statusmonitor den Client als gefährdet ansieht. Dieses Feld gilt nur, wenn der Typ für Gefährdung 'Angepasst' ist.

Stillgelegt
: Gibt an, ob die virtuelle Maschine, die der Dateibereich darstellt, stillgelegt ist.

Datum der Stilllegung
: Gibt das Datum an, an dem die virtuelle Maschine, die der Dateibereich darstellt, stillgelegt wurde.

MAC-Adresse
: Gibt die MAC-Adresse (MAC = Media Access Control) der Dateibereiche an, die für virtuelle VMware-Maschinen gesichert werden. Wenn die virtuelle Maschine über mehrere MAC-Adressen verfügt, ist dies die Adresse mit dem niedrigsten Wert.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY FILESPACE

Befehl	Beschreibung
DEFINE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs definieren.
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.

Befehl	Beschreibung
RENAME FILESPACE	Vergibt einen neuen Namen für einen Clientdateibereich auf dem Server.
UPDATE FILESPACE	Ändert Knotenreplikationsregeln für Dateibereiche.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

QUERY LIBRARY (Kassettenarchiv abfragen)

Mit diesem Befehl können Informationen über Kassettenarchive angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                .-*-------------------.
>>-Query LIBRary--+---------------------+----------------------->
                  '-Kassettenarchivname-'

   .-Format--=--Standard-----.
>--+-------------------------+---------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Kassettenarchivname
: Gibt den Namen des Kassettenarchivs an, das abgefragt werden soll. Es können Platzhalterzeichen verwendet werden, um Namen anzugeben. Dieser Parameter ist wahlfrei.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen für das Kassettenarchiv angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen für das Kassettenarchiv angezeigt werden.

Beispiel: Übersichtsdaten zu einem bestimmten Kassettenarchiv anzeigen

Informationen über das Kassettenarchiv AUTO anzeigen. Den folgenden Befehl ausgeben:

```
query library auto
```

```
                Kassettenarchivname: AUTO
                          Kassettenarchivtyp: SCSI
                                      ACS-ID:
                         Private Kategorie:
                     Arbeitsdatenträgerkategorie:
                WORM-Arbeitsdatenträgerkategorie:
                           Externer Manager:
                         Gemeinsam benutzt: No
                            LAN-unabhängig:
                   Ladeverzögerung beachten:
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Informationen zu einem bestimmten Kassettenarchiv anzeigen

Ausführliche Informationen über das Kassettenarchiv EZLIFE anzeigen. Den folgenden Befehl ausgeben: AIX-Betriebssysteme Linux-Betriebssysteme

```
query library ezlife format=detailed
```

AIX-Betriebssysteme Linux-Betriebssysteme

```
                  Kassettenarchivname: EZLIFE
                              Kassettenarchivtyp: SCSI
                                          ACS-ID:
```

```
                        Private Kategorie:
                  Arbeitsdatenträgerkategorie:
             WORM-Arbeitsdatenträgerkategorie:
                         Externer Manager:
                        Gemeinsam benutzt: Yes
                           LAN-unabhängig:
                  Ladeverzögerung beachten:
           Primärer Kassettenarchivmanager: EZSERVER
                                      WWN:
                              Seriennummer:
                  Automatisch kennzeichnen: OVERWRITE
   Arbeitsdatenträger mit einem neuen Kennsatz versehen: Yes
Letzte Aktualisierung durch (Administrator): DOCTOR_MIKE
      Datum/Zeit der letzten Aktualisierung: 2002-12-05 15:24:53
```


Windows-Betriebssysteme

```
               Kassettenarchivname: EZLIFE
                         Kassettenarchivtyp: SCSI
                                    ACS-ID:
                        Private Kategorie:
                  Arbeitsdatenträgerkategorie:
             WORM-Arbeitsdatenträgerkategorie:
                         Externer Manager:
                        Gemeinsam benutzt: YES
                           LAN-unabhängig:
                  Ladeverzögerung beachten:
           Primärer Kassettenarchivmanager: EZSERVER
                                      WWN:
                              Seriennummer:
                  Automatisch kennzeichnen: OVERWRITE
                    Laufwerke zurücksetzen: No
   Arbeitsdatenträger mit einem neuen Kennsatz versehen: Yes
Letzte Aktualisierung durch (Administrator): DOCTOR_MIKE
      Datum/Zeit der letzten Aktualisierung: 2000-12-05 15:24:53
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Kassettenarchivname
: Der Name des Kassettenarchivs.

Kassettenarchivtyp
: Der Typ des Kassettenarchivs.

ACS-ID
: Gibt an, dass es sich bei dem Kassettenarchiv um ein StorageTek-Kassettenarchiv handelt, das durch StorageTek Automated Cartridge System Library Software (ACSLS) gesteuert wird.

Private Kategorie
: Die Kategorienummer für private Datenträger, die nach Namen geladen werden müssen.

  Die Informationen, die in diesem Feld angezeigt werden, gelten nur für einen IBM® 3494 oder 3495 Tape Library Dataserver.

Arbeitsdatenträgerkategorie
: Die Kategorienummer, die für Arbeitsdatenträger in dem Kassettenarchiv verwendet werden soll.

  Die Informationen, die in diesem Feld angezeigt werden, gelten nur für einen IBM 3494 oder 3495 Tape Library Dataserver.

WORM-Arbeitsdatenträgerkategorie
: Die Kategorienummer, die für WORM-Arbeitsdatenträger in dem Kassettenarchiv verwendet wird.

  Die Informationen, die in diesem Feld angezeigt werden, gelten nur für einen IBM 3494 oder 3495 Tape Library Dataserver.

Externer Manager
: Der Standort des externen Kassettenarchivmanagers, an den der Server Zugriffsanforderungen für Datenträger senden kann.

Gemeinsam benutzt
: Gibt an, ob dieses Kassettenarchiv mit anderen IBM Spectrum Protect-Servern in einem Speicherbereichsnetz (Storage Area Network = SAN) gemeinsam benutzt wird.

LAN-unabhängig
: Gibt an, ob ein externes Kassettenarchiv für LAN-unabhängige Operationen verwendet wird.

Ladeverzögerung beachten
: Gibt an, ob der Server den Wert verwendet, der für Ladeverzögerung in der Einheitenklasse definiert ist, die diesem externen Kassettenarchiv zugeordnet ist.

Primärer Kassettenarchivmanager
: Der Name des Servers, der für die Steuerung des Zugriffs auf Kassettenarchivressourcen zuständig ist.

WWN
: Der weltweit verwendete Fibre Channel-Name für das Kassettenarchiv.

Seriennummer
: Gibt die Seriennummer des Kassettenarchivs an, das abgefragt wird.

Automatisch kennzeichnen
: Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen.

AIX-BetriebssystemeWindows-BetriebssystemeLaufwerke zurücksetzen
: AIX-BetriebssystemeWindows-BetriebssystemeGibt an, ob der Server das Ziel zurücksetzt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

Arbeitsdatenträger mit einem neuen Kennsatz versehen
: Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden.

Letzte Aktualisierung durch (Administrator)
: Gibt an, wer die letzte Aktualisierung des Kassettenarchivs ausgeführt hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit der letzten Aktualisierung.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY LIBRARY

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE LIBRARY	Löscht ein Kassettenarchiv.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE LIBRARY	Ändert die Attribute eines Kassettenarchivs.

QUERY LIBVOLUME (Datenträger im Kassettenarchiv abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Datenträger angezeigt werden, die in ein automatisiertes Kassettenarchiv zurückgestellt werden, damit sie vom IBM Spectrum Protect-Server verwendet werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                    .-*-------------------.
>>-Query LIBVolume--+---------------------+---------------------><
                    '-Kassettenarchivname-'

   .-*---------------.  .-Format--=--Standard-----.
>--+-----------------+--+-------------------------+------------><
   '-Datenträgername-'  '-Format--=--+-Standard-+-'
                                     '-Detailed-'
```

Parameter

Kassettenarchivname
: Gibt den Namen des Kassettenarchivs an. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Kassettenarchive.

Datenträgername
: Gibt den Datenträgernamen an. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Datenträger.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Zurückgestellte Datenträger für ein bestimmtes Kassettenarchiv auflisten

Informationen über alle Datenträger anzeigen, die in das Kassettenarchiv TAPE zurückgestellt werden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query libvolume tape
```

```
Kassetten-    Datenträger- Status   Eigner  Letzte     Ausgangs-  Einheiten-
archivname    name                        Verwendung element    typ
------------  -----------  -------- ------- --------   ------  ------
TAPE          000114       Scratch                      1,000      LTO
TAPE          NY1602       Scratch                     1,001    DLT
```

Beispiel: Ausführliche Informationen zu einem bestimmten Kassettenarchiv anzeigen

Ausführliche Informationen zu dem Datenträger JJY008 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query libvolume jjy008 format=detailed
```

```
                          Kassettenarchivname: HPW3494
                              Datenträgername: JJY008
                                       Status: Private
                                       Eigner: SUNSET
                         Letzte Verwendung: Data
                            Ausgangselement:
                               Einheitentyp:
                  Verbleibende Reinigungen:
                           Datenträgertyp:
```

Feldbeschreibungen

Kassettenarchivname
: Der Name des Kassettenarchivs, in dem sich der Speicherdatenträger befindet.

Datenträgername
: Der Name des Speicherdatenträgers.

Status
: Der Status des Speicherdatenträgers laut Datenträgerbestand im Kassettenarchiv. Lautet der Status 'Private', wird der Datenträger von IBM Spectrum Protect verwendet. Lautet der Status 'Scratch', steht der Datenträger für andere Benutzer zur Verfügung.

Owner
: Der Eignerserver des Datenträgers, wenn der Datenträger den Status 'Private' hat.

Letzte Verwendung
: Der Typ der Daten auf dem Datenträger. Dieses Feld gilt nur für Datenträger im Status 'Private'. Für Speicherpooldatenträger zeigt dieses Feld **Data**. Für Datenbanksicherungsdatenträger (Gesamt-, Teil- oder Momentaufnahmesicherung) zeigt dieses Feld **DbBackup**.

Ausgangselement
: Die Elementadresse des Kassettenarchivschachts, der den Datenträger enthält.

Einheitentyp
: Der Typ der Einheit, auf der der Datenträger verwendet wird. Dieses Feld zeigt einen Wert nur für Datenträger an, die in ein Kassettenarchiv zurückgestellt wurden, das gemischte Datenträger verwenden kann.

Verbleibende Reinigungen
: Für Reinigungskassetten die Anzahl der verbleibenden Reinigungen.

Datenträgertyp
: Der Typ des Datenträgers (z. B. 8-mm-Band).

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY LIBVOLUME

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.
CHECKIN LIBVOLUME	Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.

Befehl	Beschreibung
LABEL LIBVOLUME	Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
UPDATE LIBVOLUME	Ändert den Status eines Speicherdatenträgers.

QUERY LICENSE (Lizenzinformationen anzeigen)

Mit diesem Befehl können Informationen über die Lizenzprüfung, die Lizenzbedingungen und ihre Einhaltung angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query LICense-----------------------------------------------><
```

Parameter

Keine.

Um die Lizenzinformationen anzuzeigen, geben Sie den folgenden Befehl aus:

```
query license
```

Die folgende Beispielausgabe wird angezeigt:

```
ANR2017I Administrator SERVER_CONSOLE hat folgenden Befehl ausgegeben: QUERY LICENSE
                                          Letzte Lizenzprüfung: 10/17/2016 14:28:08
                    Anzahl Data Protection for Oracle im Gebrauch: 0
                  Anzahl Data Protection for Oracle im Testmodus: 0
              Anzahl Data Protection for Microsoft SQL im Gebrauch: 0
           Anzahl of Data Protection for Microsoft SQL im Testmodus: 0
         Anzahl Data Protection for Microsoft Exchange im Gebrauch: 0
               Anzahl Data Protection for MS Exchange im Testmodus: 0
                          Anzahl TDP for Lotus Notes in Gebrauch: 12
                          Anzahl TDP for Lotus Notes im Testmodus: 0
               Anzahl Data Protection for Lotus Domino im Gebrauch: 0
             Anzahl Data Protection for Lotus Domino im Testmodus: 0
                               Anzahl TDP for Informix in Gebrauch: 1
                             Anzahl TDP for Informix im Testmodus: 0
                               Anzahl TDP for SAP R/3 in Gebrauch: 0
                              Anzahl TDP for SAP R/3 im Testmodus: 0
                                   Anzahl TDP for ESS in Gebrauch: 0
                                  Anzahl TDP for ESS im Testmodus: 0
                                Anzahl TDP for ESS R/3 in Gebrauch: 0
                               Anzahl TDP for ESS R/3 im Testmodus: 0
                          Anzahl TDP for EMC Symmetrix in Gebrauch: 0
                         Anzahl TDP for EMC Symmetrix im Testmodus: 0
                       Anzahl TDP for EMC Symmetrix R/3 in Gebrauch: 6
                      Anzahl TDP for EMC Symmetrix R/3 im Testmodus: 0
                                       Anzahl TDP for WAS in Gebrauch: 0
                                      Anzahl TDP for WAS im Testmodus: 0
    Ist IBM Spectrum Protect for Data Retention im Gebrauch?: Nein
     Ist IBM Spectrum Protect for Data Retention lizenziert?: Ja
         Ist IBM Spectrum Protect Basic Edition im Gebrauch?: Ja
          Ist IBM Spectrum Protect Basic Edition lizenziert?: Ja
  Ist IBM Spectrum Protect Extended Edition im Gebrauch?: Nein
   Ist IBM Spectrum Protect Extended Edition lizenziert?: Ja
                                    Serverlizenzeinhaltung: Gültig
```

Feldbeschreibungen

Letzte Lizenzprüfung
: Gibt an, wann die Lizenzprüfung zuletzt durchgeführt wurde (Datum und Uhrzeit).

Anzahl Data Protection for Oracle im Gebrauch
: Gibt die Anzahl der Instanzen von Data Protection for Oracle an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl Data Protection for Oracle im Testmodus
: Gibt die Anzahl der Instanzen von Data Protection for Oracle an, die im Testmodus sind.

Anzahl Data Protection for Microsoft SQL im Gebrauch
: Gibt die Anzahl der Instanzen von Data Protection for Microsoft SQL an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl Data Protection for Microsoft SQL im Testmodus
: Gibt die Anzahl der Instanzen von Data Protection for Microsoft SQL an, die im Testmodus sind.

Anzahl Data Protection for Microsoft Exchange im Gebrauch
: Gibt die Anzahl der Instanzen von Data Protection for Microsoft Exchange an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl Data Protection for Microsoft Exchange im Testmodus
: Gibt die Anzahl der Instanzen von Data Protection for Microsoft Exchange an, die im Testmodus sind.

Anzahl TDP for Lotus Notes in Gebrauch
: Gibt die Anzahl von TDP for Lotus Notes an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl TDP for Lotus Notes im Testmodus
: Gibt die Anzahl von TDP for Lotus Notes an, die im Testmodus sind.

Anzahl Data Protection for Lotus Domino im Gebrauch
: Gibt die Anzahl der Instanzen von Data Protection for Lotus Domino an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl Data Protection for Lotus Domino im Testmodus
: Gibt die Anzahl der Instanzen von Data Protection for Lotus Domino an, die im Testmodus sind.

Anzahl TDP for Informix in Gebrauch
: Gibt die Anzahl von TDP for Informix an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl TDP for Informix im Testmodus
: Gibt die Anzahl von TDP for Informix an, die im Testmodus sind.

Anzahl TDP for SAP R/3 in Gebrauch
: Gibt die Anzahl von TDP for SAP R/3 an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl TDP for SAP R/3 im Testmodus
: Gibt die Anzahl von TDP for SAP R/3 an, die im Testmodus sind.

Anzahl TDP for ESS in Gebrauch
: Gibt die Anzahl von TDP for ESS an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl TDP for ESS im Testmodus
: Gibt die Anzahl von TDP for ESS an, die im Testmodus sind.

Anzahl TDP for ESS R/3 in Gebrauch
: Gibt die Anzahl von TDP for ESS R/3 an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl TDP for ESS R/3 im Testmodus
: Gibt die Anzahl von TDP for ESS R/3 an, die im Testmodus sind.

Anzahl TDP for EMC Symmetrix in Gebrauch
: Gibt die Anzahl von TDP for EMC Symmetrix an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl TDP for EMC Symmetrix im Testmodus
: Gibt die Anzahl von TDP for EMC Symmetrix an, die im Testmodus sind.

Anzahl TDP for EMC Symmetrix R/3 in Gebrauch
: Gibt die Anzahl von TDP for EMC Symmetrix R/3 an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl TDP for EMC Symmetrix R/3 im Testmodus
: Gibt die Anzahl von TDP for EMC Symmetrix R/3 an, die im Testmodus sind.

Anzahl TDP for WAS in Gebrauch
: Gibt die Anzahl von TDP for WAS an, die im Gebrauch sind. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Anzahl TDP for WAS im Testmodus
: Gibt die Anzahl von TDP for WAS an, die im Testmodus sind.

Ist IBM Spectrum Protect for Data Retention im Gebrauch?
: Gibt an, ob IBM Spectrum Protect for Data Retention im Gebrauch ist. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Ist IBM Spectrum Protect for Data Retention lizenziert?
: Gibt an, ob IBM Spectrum Protect for Data Retention lizenziert ist.

Ist IBM Spectrum Protect Basic Edition im Gebrauch?
: Gibt an, ob IBM Spectrum Protect Basic Edition im Gebrauch ist. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Ist IBM Spectrum Protect Basic Edition lizenziert?
: Gibt an, ob IBM Spectrum Protect Basic Edition lizenziert ist.

Ist IBM Spectrum Protect Extended Edition im Gebrauch?

Gibt an, ob IBM Spectrum Protect Extended Edition im Gebrauch ist. Ein Produkt ist im Gebrauch, wenn Sie das Produkt gekauft und die Lizenz registriert haben.

Ist IBM Spectrum Protect Extended Edition lizenziert?

Gibt an, ob IBM Spectrum Protect Extended Edition lizenziert ist.

Serverlizenzeinhaltung

Gibt an, ob die Serverlizenz gültig ist.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY LICENSE

Befehl	Beschreibung
AUDIT LICENSES	Prüft die Einhaltung der definierten Lizenzen.
QUERY AUDITOCCUPANCY	Zeigt die Serverspeicherauslastung für einen Clientknoten an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY PVUESTIMATE	Zeigt Prozessor-Value-Unit-Schätzungen an. Hinweis: Mit dem Befehl QUERY PVUESTIMATE werden Lizenzen zurückgemeldet, indem PVU-Informationen auf Knotenbasis für Servereinheiten bereitgestellt werden.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER LICENSE	Registriert eine Lizenz für den IBM Spectrum Protect-Server.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
SET CPUINFOREFRESH	Gibt die Anzahl der Tage zwischen Clientsuchläufen nach Workstationinformationen an, die für PVU-Schätzungen verwendet werden.
SET LICENSEAUDITPERIOD	Gibt die Anzahl Tage zwischen den automatischen Lizenzprüfungen an.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

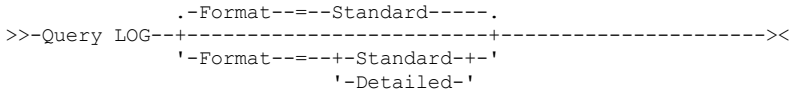
QUERY LOG (Informationen zum Wiederherstellungsprotokoll anzeigen)

Mit diesem Befehl können Informationen über das Wiederherstellungsprotokoll angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Die folgenden Werte sind gültig:

Standard

Gibt an, dass Teilinformationen angezeigt werden.

Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Übersichtsdaten zu dem Wiederherstellungsprotokoll anzeigen

Die Übersichtsdaten zu dem Wiederherstellungsprotokoll anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query log
```

```
Gesamtspeicher-     Verw. Speicher-     Freier Speicher-
bereich (MB)        bereich (MB)        bereich (MB)
----------------    ---------------     ---------------
          38.912              543,3            38.368,7
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

Beispiel: Ausführliche Informationen zu dem Wiederherstellungsprotokoll anzeigen

Ausführliche Informationen zu dem Wiederherstellungsprotokoll anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query log format=detailed
```

```
                     Verzeichnis für aktive Protokolldateien: /actlog
                                 Gesamtspeicherbereich (MB): 524.032
                           Verwendeter Speicherbereich (MB): 3.517
                                Freier Speicherbereich (MB): 520.515

                           Gesamtgröße des Dateisystems (MB): 564.443
                Verwendeter Speicherbereich im Dateisystem (MB): 527.049
                     Freier Speicherbereich im Dateisystem (MB): 8.722

                      Verzeichnis für Archivprotokolle: /archlog
                           Gesamtgröße des Dateisystems (MB): 603.751,82
                Verwendeter Speicherbereich im Dateisystem (MB): 80.642,30
                     Freier Speicherbereich im Dateisystem (MB): 523.109,52
                               Archivprotokoll komprimiert: Ja

                               Spiegelprotokollverzeichnis: /mirrorlog
                           Gesamtgröße des Dateisystems (MB): 564.443
                Verwendeter Speicherbereich im Dateisystem (MB): 527.049
                     Freier Speicherbereich im Dateisystem (MB): 8.722

                    Übernahmeverzeichnis für Archivprotokolle: /archfaillog
                           Gesamtgröße des Dateisystems (MB): 301.372,06
                Verwendeter Speicherbereich im Dateisystem (MB): 44.741,80
                     Freier Speicherbereich im Dateisystem (MB): 256.630,26
```

 Windows-Betriebssysteme

Beispiel: Ausführliche Informationen zu dem Wiederherstellungsprotokoll anzeigen, wenn das Spiegelprotokoll und das Archivübernahmeprotokoll nicht definiert sind

Die Ausgabe dieses Befehls auf Windows-Systemen hat ein anderes Aussehen. Beispielsweise enthält die Ausgabe Leerzeichen für das Spiegelprotokoll und das Archivübernahmeprotokoll.
Informationen zu dem Wiederherstellungsprotokoll anzeigen, wenn das Spiegelprotokoll und das Archivübernahmeprotokoll nicht definiert sind.

```
query log format=detailed
```

 Windows-Betriebssysteme

```
                  Verzeichnis für aktive Protokolldateien: d:\actlog
                              Gesamtspeicherbereich (MB): 524.032
                        Verwendeter Speicherbereich (MB): 3.517
                             Freier Speicherbereich (MB): 520.515

                        Gesamtgröße des Dateisystems (MB): 564.443
             Verwendeter Speicherbereich im Dateisystem (MB): 527.049
                  Freier Speicherbereich im Dateisystem (MB): 8.722

                   Verzeichnis für Archivprotokolle: e:\archlog
                        Gesamtgröße des Dateisystems (MB): 603.751,82
             Verwendeter Speicherbereich im Dateisystem (MB): 80.642,30
                  Freier Speicherbereich im Dateisystem (MB): 523.109,52
                            Archivprotokoll komprimiert: Ja

                            Spiegelprotokollverzeichnis:
                        Gesamtgröße des Dateisystems (MB):
             Verwendeter Speicherbereich im Dateisystem (MB):
                  Freier Speicherbereich im Dateisystem (MB):

                  Übernahmeverzeichnis für Archivprotokolle:
                        Gesamtgröße des Dateisystems (MB):
             Verwendeter Speicherbereich im Dateisystem (MB):
                  Freier Speicherbereich im Dateisystem (MB):
```

Feldbeschreibungen

Gesamtspeicherbereich
: Gibt die maximale Größe der aktiven Protokolldatei in Megabyte an.

Verwendeter Speicherbereich
: Gibt den verwendeten Speicherbereich (in MB) für aktive Protokolldateien an.

Freier Speicherbereich
: Gibt den Speicherbereich (in MB) für aktive Protokolldateien an, der nicht von nicht festgeschriebenen Transaktionen verwendet wird.

Gesamtgröße des Dateisystems
: Gibt die Gesamtgröße des Dateisystems in Megabyte an.

Verwendeter Speicherbereich im Dateisystem
: Gibt den verwendeten Speicherbereich im Dateisystem in Megabyte an.

Freier Speicherbereich im Dateisystem
: Gibt den Speicherbereich in Megabyte an, der im Dateisystem verfügbar ist.

Archivprotokoll komprimiert
: Gibt an, ob die Archivprotokolle komprimiert sind.

Verzeichnis für aktive Protokolldateien
: Gibt die Position an, an der aktive Protokolldateien gespeichert werden. Wird das Verzeichnis für aktive Protokolldateien geändert, versetzt der Server alle archivierten Protokolle in das Verzeichnis für Archivprotokolle und alle aktiven Protokolldateien in ein neues Verzeichnis für aktive Protokolldateien.

Spiegelprotokollverzeichnis
: Gibt die Position an, an der der Spiegel der aktiven Protokolldatei aufbewahrt wird.

Übernahmeverzeichnis für Archivprotokolle
: Gibt die Position an, an der der Server Archivprotokolle sichert, wenn die Protokolle nicht im Verzeichnis für Archivprotokolle archiviert werden können.

Verzeichnis für Archivprotokolle
: Gibt die Position an, an der der Server eine Protokolldatei archivieren kann, nachdem alle in dieser Protokolldatei angegebenen Transaktionen abgeschlossen wurden.

QUERY MACHINE (Maschineninformationen abfragen)

Mit diesem Befehl können Informationen über eine oder mehrere Maschinen angezeigt werden. Mit Hilfe dieser Informationen können IBM Spectrum Protect-Client-Maschinen bei einem schwerwiegenden Fehler wiederhergestellt werden.

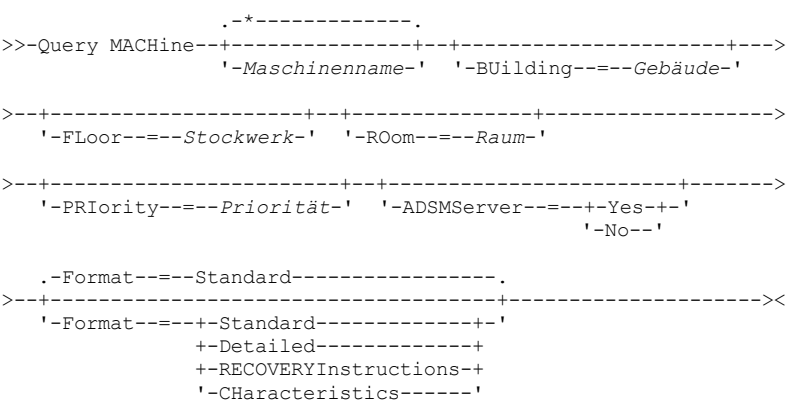
Achtung: Die Informationen werden von IBM Spectrum Protect nicht verwendet. Sie dienen nur zur Planung der Fehlerbehebung bei Client-Maschinen.
IBM Spectrum Protect zeigt Informationen für mehrere Maschinen in der folgenden Reihenfolge an:

- Entsprechend der angegebenen Priorität.
- Innerhalb einer Priorität, entsprechend dem angegebenen Standort und Maschinennamen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Maschinenname
: Gibt den Namen einer oder mehrerer Maschinen an, die abgefragt werden sollen. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert umfaßt alle Maschinen, die die angegebenen Kriterien erfüllen.

BUilding

Gibt den Namen oder die Nummer des Gebäudes an, in dem sich die Maschinen befinden. Dieser Parameter ist wahlfrei. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

FLoor
Gibt den Namen oder die Nummer des Stockwerks an, auf dem sich die Maschinen befinden. Dieser Parameter ist wahlfrei. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

ROom
Gibt den Namen oder die Nummer des Raums an, in dem sich die Maschinen befinden. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

PRIority
Gibt die Prioritätsnummer der Maschinen an. Dieser Parameter ist wahlfrei.

ADSMServer
Gibt an, ob die Maschine einen IBM Spectrum Protect-Server enthält. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Maschinen angezeigt, die die anderen Kriterien erfüllen. Gültige Werte:

Yes
Die Maschine enthält einen IBM Spectrum Protect-Server.

No
Die Maschinen enthalten keinen IBM Spectrum Protect-Server.

Format
Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard
Zeigt Teilinformationen für die Maschinen an.

Detailed
Zeigt alle Informationen für die Maschinen an.

RECOVERYInstructions
Zeigt nur Wiederherstellungsanweisungen für die Maschine an. Diese Option ist nur gültig, wenn eine bestimmte Maschine abgefragt wird.

CHaracteristics
Zeigt nur Maschinenkenndaten an. Diese Option ist nur gültig, wenn eine bestimmte Maschine abgefragt wird.

Beispiel: Informationen zu einer bestimmten Maschine anzeigen

Informationen für die Maschine MACH1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query machine MACH1
```

```
Maschi-  Maschinen- Gebäude Stock- Raum Knotenname Wiederherstellungs-
nenname  priorität          werk                  datenträgername
-------  -------- -------- ----- ----- ---------  ----------
MACH1       1         21      2    2929  VIRGINIA    RECMED1
```

Beispiel: Ausführliche Informationen zu Maschinen mit Priorität 1 anzeigen

Ausführliche Informationen über alle Maschinen mit der Priorität 1 anzeigen, die sich im zweiten Stockwerk des Gebäudes 21 befinden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query machine * building=21 floor=2 priority=1
format=detailed
```

```
                            Maschinenname: MACH1
                        Maschinenpriorität: 1
                                  Gebäude: 21
                                Stockwerk: 2
                                     Raum: 2929
                                  Server?: Yes
                               Beschreibung: TSM-Server-Maschine
                                 Knotenname: VIRGINIA
          Wiederherstellungsdatenträgername: RECMED1
                                Kenndaten?: Yes
             Wiederherstellungsanweisungen?: Yes
```

Feldbeschreibungen

Maschinenname
Der Name der Maschine.

Maschinenpriorität
Die Wiederherstellungspriorität der Maschine.

Gebäude
Das Gebäude, in dem sich die Maschine befindet.

Stockwerk
Das Stockwerk, auf dem sich die Maschine befindet.

Raum
: Der Raum, in dem sich die Maschine befindet.

Server?
: Angabe, ob die Maschine einen IBM Spectrum Protect-Server enthält.

Beschreibung
: Eine Beschreibung der Maschine.

Knotenname
: Die IBM Spectrum Protect-Client-Knoten, die dieser Maschine zugeordnet sind.

Wiederherstellungsdatenträgername
: Die Wiederherstellungsdatenträger, die dieser Maschine zugeordnet sind.

Kenndaten?
: Angabe, ob die Kenndaten der Maschine in der Datenbank gespeichert sind.

Wiederherstellungsanweisungen?
: Gibt an, ob Wiederherstellungsanweisungen für eine Maschine in der IBM Spectrum Protect-Datenbank gespeichert sind.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MACHINE

Befehl	Beschreibung
DEFINE MACHINE	Definiert eine Maschine für DRM.
DEFINE MACHNODEASSOCIATION	Ordnet einen IBM Spectrum Protect-Knoten einer Maschine zu.
DEFINE RECMEDMACHASSOCIATION	Ordnet Wiederherstellungsdatenträger einer Maschine zu.
DELETE MACHINE	Löscht eine Maschine.
INSERT MACHINE	Fügt Maschinenkenndaten oder Wiederherstellungsanweisungen in die IBM Spectrum Protect-Datenbank ein.
UPDATE MACHINE	Ändert die Informationen zu einer Maschine.

QUERY MEDIA (Speicherpooldatenträger mit sequenziellem Zugriff abfragen)

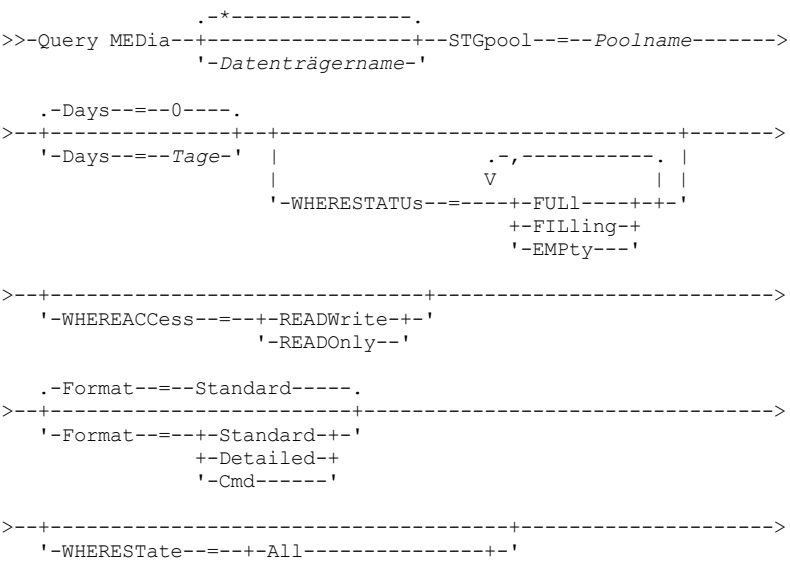
Mit diesem Befehl können Informationen zu Datenträgern mit sequenziellem Zugriff aus primären Speicherpools und Kopienspeicherpools angezeigt werden, die durch den Befehl MOVE MEDIA versetzt wurden.

Berechtigungsklasse

Jeder Administrator mit System- oder Bedienerberechtigung kann diesen Befehl ausgeben, es sei denn, der Befehl enthält den Parameter CMD. Wird der Parameter CMD angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator Bedienerberechtigung, uneingeschränkte Speicherberechtigung oder Systemberechtigung haben. Wird der Parameter CMD angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf YES (Standardwert) gesetzt, muss der Administrator Systemberechtigung haben.

Mit dem Befehl QUERY MEDIA werden nur Datenträger mit dem ACCESS MODE-Wert READONLY oder READWRITE angezeigt.

Syntax



```
                    +-MOUNTABLEInlib----+
                    '-MOUNTABLENotinlib-'

>--+-------------------------------+--+------------------+------>
   '-WHEREOVFLOcation--=--Standort-'  '-CMd---=--"Befehl"-'

                                  .-APPend--=--No------.
>--+----------------------------+--+--------------------+-------><
   '-CMDFilename--=--Dateiname-'  '-APPend--=--+-No--+-'
                                               '-Yes-'
```

Parameter

Datenträgername
: Gibt den Namen des anzuzeigenden Datenträgers mit sequenziellem Zugriff aus einem primären Speicherpool oder einem Kopienspeicherpool an. Dieser Parameter ist wahlfrei. Es kann ein Platzhalterzeichen verwendet werden, um den Namen anzugeben. Alle übereinstimmenden Datenträger werden bei der Verarbeitung berücksichtigt.Wenn dieser Parameter nicht angegeben wird, werden alle Datenträger angezeigt, die in dem durch den Parameter STGPOOL angegebenen Speicherpool definiert sind.

STGpool (Erforderlich)
: Gibt den Namen des primären Speicherpools oder Kopienspeicherpools mit sequenziellem Zugriff an, aus dem die Datenträger für die Verarbeitung ausgewählt werden. Es können Platzhalterzeichen verwendet werden, um den Namen anzugeben. Alle übereinstimmenden Speicherpools werden verarbeitet. Wird der angegebene Speicherpool nicht durch ein automatisiertes Kassettenarchiv verwaltet, werden keine Datenträger angezeigt.

Days
: Gibt die Anzahl Tage an, die nach dem Schreiben oder Lesen des Datenträgers verstreichen müssen, bevor der Datenträger für die Verarbeitung ausgewählt werden kann. Dieser Parameter ist wahlfrei. Es kann eine Zahl von 0 bis 9999 angegeben werden. Der Standardwert ist 0. Die Anzahl der verstrichenen Tage wird anhand des letzten Lese- oder Schreibdatums (das aktuellere von beiden) des Datenträgers berechnet.

WHERESTATUs
: Gibt an, dass die Ausgabe der Abfrage auf einen bestimmten Datenträgerstatus beschränkt werden soll. Dieser Parameter ist wahlfrei. Es können mehrere Status in einer Liste angegeben werden, indem jeder Status ohne Leerzeichen durch ein Komma voneinander getrennt wird. Wird für diesen Parameter kein Wert angegeben, werden alle Datenträger in dem angegebenen Speicherpool unabhängig von ihrem Status angezeigt.

  Gültige Werte:

  FULl
  : Gibt an, dass Datenträger mit dem Status FULL angezeigt werden.

  FILling
  : Gibt an, dass Datenträger mit dem Status FILLING angezeigt werden.

  EMPty
  : Gibt an, dass Datenträger mit dem Status EMPTY angezeigt werden.

WHEREACCess
: Gibt an, dass die Ausgabe auf bestimmte Datenträgerzugriffsmodi beschränkt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert für diesen Parameter angegeben, wird die Ausgabe nicht auf bestimmte Zugriffsmodi beschränkt.

  Gültige Werte:

  READWrite
  : Gibt an, dass Datenträger mit dem Zugriffsmodus READWRITE angezeigt werden.

  READOnly
  : Gibt an, dass Datenträger mit dem Zugriffsmodus READONLY angezeigt werden.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen für die angegebenen Datenträger mit sequenziellem Zugriff aus dem Speicherpool angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen für die angegebenen Datenträger mit sequenziellem Zugriff aus dem Speicherpool angezeigt werden.

  Cmd
  : Gibt an, dass ausführbare Befehle für die Speicherpooldatenträger erstellt werden, die von dem Befehl QUERY MEDIA verarbeitet werden. Diese Befehle befinden sich in der Datei, die mit dem Parameter CMDFILENAME des Befehls QUERY MEDIA angegeben wird. Sollen die Befehle nur an der Konsole angezeigt werden, geben Sie eine Nullzeichenfolge ("") für den Parameter CMDFILENAME an. Wenn FORMAT=CMD, aber keine Befehlsfolge im Parameter CMD angegeben wird, schlägt der Befehl QUERY MEDIA fehl.

WHERESTate

Gibt den Status der zu verarbeitenden Datenträger an. Mit diesem Parameter wird die Verarbeitung auf Datenträger beschränkt, die den angegebenen Status haben. Dieser Parameter ist wahlfrei. Standardwert ist ALL. Gültige Werte:

All
: Gibt an, dass Datenträger mit jedem Status abgefragt werden. Gültige Statusangaben sind MOUNTABLEINLIB und MOUNTABLENOTINLIB.

MOUNTABLEInlib
: Gibt an, dass Datenträger abgefragt werden, die momentan den Status MOUNTABLEINLIB haben. Datenträger mit dem Status MOUNTABLEINLIB befinden sich im Kassettenarchiv, sind vor Ort, enthalten gültige Daten und stehen für die Verarbeitung vor Ort zur Verfügung.

MOUNTABLENotinlib
: Gibt an, dass Datenträger abgefragt werden, die momentan den Status MOUNTABLENOTINLIB haben. Datenträger mit dem Status MOUNTABLENOTINLIB befinden sich nicht im Kassettenarchiv, enthalten keine gültigen Daten und stehen für die Verarbeitung vor Ort nicht zur Verfügung.

WHEREOVFLOcation
: Gibt den Überlaufstandort der Datenträger an, die angezeigt werden sollen. Dieser Parameter ist wahlfrei. Mit diesem Parameter wird die Verarbeitung auf Datenträger beschränkt, die sich an dem angegebenen Standort befinden. Die maximale Länge des Standorts beträgt 255 Zeichen. Wenn der Standort Leerzeichen enthält, muss er in Anführungszeichen eingeschlossen werden.

CMd
: Gibt an, dass ausführbare Befehle erstellt werden. Die Befehlsangabe in Anführungszeichen einschließen. Die maximale Länge der Befehlsangabe beträgt 255 Zeichen. Dieser Parameter ist wahlfrei.

  Für jeden Datenträger, den der Befehl QUERY MEDIA erfolgreich verarbeitet hat, schreibt der Server die zugeordneten Befehle in eine Datei. Den Dateinamen mit dem Parameter CMDFILENAME angeben.

  AIX-BetriebssystemeLinux-BetriebssystemeWird kein Dateiname angegeben, generiert der Befehl einen Standarddateinamen, indem die Zeichenfolge exec.cmds.media an das Serververzeichnis angehängt wird.

  Windows-BetriebssystemeWird kein Dateiname angegeben, generiert der Befehl einen Standarddateinamen, indem die Zeichenfolge exec.cmd.media an das Serververzeichnis angehängt wird.

  Hinweis:

  1. Wenn der Befehl, der in die Datei geschrieben wird, 255 Zeichen überschreitet, wird er in mehrere Zeilen aufgeteilt, und an das Ende jeder Zeile (mit Ausnahme der letzten Zeile) wird ein Fortsetzungszeichen (+) eingefügt. Das Fortsetzungszeichen muss möglicherweise entsprechend den Anforderungen des Produkts, das die Befehle ausführt, geändert werden.
  2. Wird ein ausführbarer Befehl mit einem anderen Wert als CMD für FORMAT angegeben, wird die Befehlszeichenfolge ignoriert, und der Befehl QUERY MEDIA schreibt keine Befehlszeile.

  Geben Sie eine Befehlszeichenfolge und Substitutionsvariablen an:

  Zeichenfolge
  : Gibt die Zeichenfolge an, mit der ein ausführbarer Befehl erstellt wird, um den Datenträgernamen und/oder Datenträgerstandort zu verarbeiten. Für die Zeichenfolge kann beliebiger Text im freien Format angegeben werden. Keine eingebetteten Anführungszeichen verwenden. Das folgende Beispiel zeigt eine gültige Angabe eines ausführbaren Befehls:

    ```
    cmd="checkin libvolume &vol"
    ```

    Die folgende Angabe ist ungültig:

    ```
    cmd="checkin libvolume "&vol""
    ```

  Substitution
  : Gibt eine Variable an, für die der Befehl QUERY MEDIA einen Wert ersetzen soll. Gültige Substitutionsvariablen:

    &VOL
    : Den Datenträgernamen für &VOL ersetzen. Kleinbuchstaben können angegeben werden (&vol). Zwischen Et-Zeichen (&) und VOL dürfen keine Leerschritte oder Leerzeichen stehen. Befinden sich an dieser Stelle Leerzeichen, behandelt der Befehl QUERY MEDIA diese Zeichen als Zeichenfolge, und es wird keine Substitution definiert. Wird &VOL nicht angegeben, wird in dem ausführbaren Befehl kein Datenträgername definiert.

    &LOC
    : Den Datenträgerstandort für &LOC ersetzen. Kleinbuchstaben können angegeben werden (&loc). Zwischen Et-Zeichen (&) und LOC dürfen keine Leerschritte oder Leerzeichen stehen. Befinden sich an dieser Stelle Leerzeichen, behandelt der Befehl QUERY MEDIA diese Zeichen als Zeichenfolge, und es wird keine Substitution definiert. Wird &LOC nicht angegeben, wird in dem ausführbaren Befehl kein Standortname definiert.

    &VOLDSN
    : Den Datenträgerdateinamen für &VOLDSN ersetzen. Ein Beispiel für einen Dateinamen eines Banddatenträgers aus dem Kopienspeicherpool unter Verwendung des definierten Präfix IBM Spectrum Protect310 lautet IBM Spectrum Protect310.BFS. Wird &VOLDSN nicht angegeben, wird in dem ausführbaren Befehl kein Datenträgerdateiname definiert.

    &NL

Das Zeilenvorschubzeichen für &NL ersetzen. Wenn &NL angegeben wird, teilt der Befehl QUERY MEDIA den Befehl an der Position, an der sich &NL befindet; es werden keine Fortsetzungszeichen angehängt. Die Angabe des richtigen Fortsetzungszeichens (falls erforderlich) vor &NL ist Aufgabe des Benutzers. Der Benutzer ist außerdem verantwortlich für die Länge der Zeile. Wird &NL nicht angegeben und überschreitet der Befehl 255 Zeichen, wird der Befehl in mehrere Zeilen aufgeteilt, und an das Ende jeder Zeile (mit Ausnahme der letzten Zeile) wird ein Fortsetzungszeichen (+) eingefügt.

CMDFilename
Gibt den vollständigen Pfadnamen an, der die durch CMD angegebenen Befehle enthalten wird, wenn FORMAT=CMD angegeben wird. Dieser Parameter ist wahlfrei. Die maximale Länge des Dateinamens beträgt 1279 Zeichen.

 AIX-Betriebssysteme  Linux-BetriebssystemeWird "" im Parameter CMDFILENAME angegeben, generiert der Befehl QUERY MEDIA einen Dateinamen, indem die Zeichenfolge "exec.cmds.media" an das Serververzeichnis angehängt wird. Das Serververzeichnis ist das aktuelle Arbeitsverzeichnis des Serverprozesses.

 Windows-BetriebssystemeWird "" im Parameter CMDFILENAME angegeben, generiert der Befehl QUERY MEDIA einen Dateinamen, indem die Zeichenfolge "exec.cmd.media" an das Serververzeichnis angehängt wird. Das Serververzeichnis ist das aktuelle Arbeitsverzeichnis des Serverprozesses.

Wird für CMDFILENAME eine Nullzeichenfolge ("") angegeben, werden die erstellten Befehle nur an der Konsole angezeigt. Die angezeigten Befehle können mit den Umleitungszeichen des Betriebssystems (> oder >>) in eine Datei umgeleitet werden.

 AIX-Betriebssysteme  Linux-BetriebssystemeWird der Dateiname nicht angegeben, generiert der Befehl einen Standarddateinamen, indem die Zeichenfolge "exec.cmds.media" an das Serververzeichnis angehängt wird.

 Windows-BetriebssystemeWird der Dateiname nicht angegeben, generiert der Befehl einen Standarddateinamen, indem die Zeichenfolge "exec.cmd.media" an das Serververzeichnis angehängt wird.

Der Befehl QUERY MEDIA ordnet den angegebenen oder generierten Dateinamen automatisch zu. Wenn der Dateiname vorhanden ist, versucht der Befehl QUERY MEDIA ihn zu verwenden, und die eventuell vorhandenen Daten in der Datei werden überschrieben. APPEND=YES kann angegeben werden, um zu verhindern, dass die vorhandenen Daten überschrieben werden. Schlägt der Befehl QUERY MEDIA fehl, nachdem die Befehlsdatei zugeordnet wurde, wird die Datei nicht gelöscht.

APPend
Gibt an, dass am Anfang oder Ende der Befehlsdateidaten geschrieben werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No
Gibt an, dass die Daten an den Anfang der Befehlsdatei geschrieben werden sollen. Wenn die betreffende Befehlsdatei vorhanden ist, wird ihr Inhalt überschrieben.

Yes
Gibt an, dass die Befehlsdatei angehängt werden soll, indem am Ende der Befehlsdateidaten geschrieben wird.

Beispiel: Informationen zu einem bestimmten Speicherpool mit sequenziellem Zugriff anzeigen

Alle vollen und teilweise vollen Datenträger anzeigen, die sich im primären Speicherpool mit sequenziellem Zugriff ARCHIVE befinden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query media * stgpool=archive wherestatus=full, filling


Daten-      Status               Standort             Name des autom.
                                                      trägername
Speicherarchivs
----------- -------------------  -------------------  -----------
TAPE01      Mountable in Library                      LIB3494
TAPE03      Mountable not in Lib. Room1234/Bldg31
TAPE07      Mountable in Library                      LIB3494
TAPE09      Mountable not in Lib. Room1234/Bldg31
```

Beispiel: Informationen zu einem Speicherpool mit sequenziellem Zugriff mit einem bestimmten Präfix anzeigen

Alle vollen Datenträger mit dem Status MOUNTABLENOTINLIB für Speicherpools mit sequenziellem Zugriff, die den Präfixnamen ONSITE haben, detailliert anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query media wherestate=mountablenotinlib stgpool=onsite*
wherestatus=full format=detailed

                        Datenträgername: TAPE21
                                 Status: Mountable not in library
                    Datenträgerstatus: Full
                                Zugriff: ReadOnly
                        Letztes Referenzdatum: 01/30/98
          Datum/Zeit der letzten Aktualisierung: 08/20/1996 13:29:02
```

```
                                Standort: Rm569/bldg31
                           Speicherpoolname: ONSITE.ARCHIVE
      Name des automatisierten Kassettenarchivs:

                            Datenträgername: TAPE22
                                     Status: Mountable not in library
                          Datenträgerstatus: Full
                                    Zugriff: ReadOnly
                      Letztes Referenzdatum: 01/30/98
          Datum/Zeit der letzten Aktualisierung: 08/20/1996 15:29:02
                                Standort: Rm569/bldg31
                           Speicherpoolname: ONSITE.ARCHIVEPOOL
      Name des automatisierten Kassettenarchivs:
```

Beispiel: Befehle zum Zurückstellen generieren

Die Befehle CHECKIN LIBVOLUME für volle und teilweise volle Datenträger generieren, die sich im primären Speicherpool ONSITE.ARCHIVE befinden und im Überlaufstandort Room 2948/Bldg31 aufbewahrt werden.

```
query media * stgpool=onsite.archive format=cmd
wherestatus=full,filling wherestate=mountablenotinlib
whereovflocation=room2948/bldg31
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols
```

Der Befehl QUERY MEDIA hat die ausführbaren Befehle CHECKIN LIBVOLUME in /tsm/move/media/checkin.vols erstellt, die durch Ausgabe des Befehls MACRO mit /tsm/move/media/checkin.vols als Makronamen ausgeführt werden können.

```
checkin libvol lib3494 TAPE04 status=private
checkin libvol lib3494 TAPE13 status=private
checkin libvol lib3494 TAPE14 status=private
```

Feldbeschreibungen

Datenträgername
: Gibt den Namen des Datenträgers aus dem primären Speicherpool mit sequenziellem Zugriff an.

Status
: Gibt den Status des Datenträgers an.

Datenträgerstatus
: Gibt den Status des Datenträgers an.

Zugriff
: Gibt den Zugriffsmodus des Datenträgers an.

Letztes Referenzdatum
: Gibt das letzte Lese- oder Schreibdatum (das aktuellere von beiden) des Datenträgers an.

Datum/Zeit der letzten Aktualisierung
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Datenträger zuletzt aktualisiert wurde.

Standort
: Gibt den Speicherort des Datenträgers an. Wenn der Datenträger aus dem Kassettenarchiv ausgegeben wurde und sein Speicherort nicht angegeben oder definiert ist, wird ein Fragezeichen (?) als Standort angezeigt.

Speicherpoolname
: Gibt den Namenn des Speicherpools mit sequenziellem Zugriff an, in dem der Datenträger definiert ist.

Automat. Kassettenarchiv
: Gibt den Namen des automatisierten Kassettenarchivs an, wenn sich der Datenträger im Kassettenarchiv befindet.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MEDIA

Befehl	Beschreibung
AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeMOVE MEDIA	Versetzt Speicherpooldatenträger, die von einem automatisierten Kassettenarchive verwaltet werden.

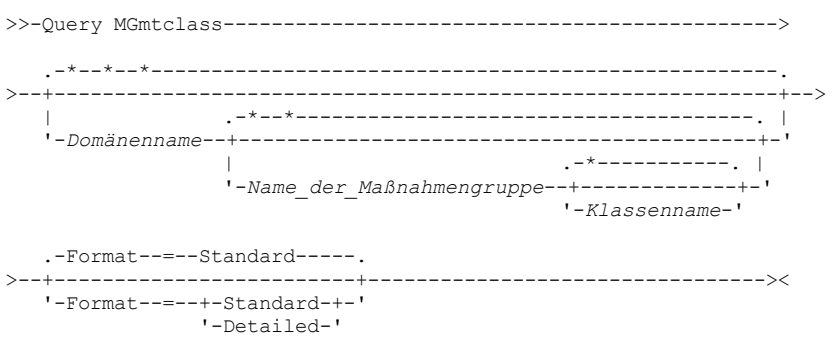
QUERY MGMTCLASS (Verwaltungsklasse abfragen)

Mit diesem Befehl können Informationen über Verwaltungsklassen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Domänenname
: Gibt die Maßnahmendomäne an, die der Verwaltungsklasse zugeordnet ist, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden Verwaltungsklassen in allen Maßnahmendomänen abgefragt. Dieser Parameter muß angegeben werden, wenn explizit der Name einer Verwaltungsklasse angegeben wird.

Name_der_Maßnahmengruppe
: Gibt die Maßnahmengruppe an, die der Verwaltungsklasse zugeordnet ist, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden Verwaltungsklassen in allen Maßnahmengruppen abgefragt. Dieser Parameter muß angegeben werden, wenn explizit der Name einer Verwaltungsklasse angegeben wird.

Klassenname
: Gibt die Verwaltungsklasse an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Verwaltungsklassen abgefragt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Informationen zu allen Verwaltungsklassen anzeigen

Alle Verwaltungsklassen für alle Maßnahmendomänen abfragen. Die Ausgabe soll im Standardformat erstellt werden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query mgmtclass

Name der     Name der     Name         Standard    Beschreibung
Maßnahmen-   Maßnahmen-   Verwal-      verwal-
domäne       gruppe       tungskl.     tungskl.?
---------    ---------    ---------    ---------   ------------------
EMPLOYEE-    ACTIVE       ACTIVEFI-    Yes         Modified default
  _RECORDS                  LES                      management class
EMPLOYEE-    HOLIDAY      ACTIVEFI-    Yes         Modified default
  _RECORDS                  LES                      management class
EMPLOYEE-    HOLIDAY      FILEHIST-    No          Test modified
  _RECORDS                  ORY                      management class
EMPLOYEE-    VACATION     ACTIVEFI-    Yes         Original default
  _RECORDS                  LES                      management class
EMPLOYEE-    VACATION     FILEHIST-    No          Test modified
  _RECORDS                  ORY                      management class
PROG1        SUMMER       MCLASS1      No          Technical Support
                                                     Mgmt Class
PROG2        SUMMER       MCLASS1      No          Technical Support
                                                     Mgmt Class
STANDARD     ACTIVE       STANDARD     Yes         Installed default
                                                     management class
STANDARD     STANDARD     STANDARD     Yes         Installed default
                                                     management class
```

Um Informationen zu Verwaltungsklassen in einer bestimmten Maßnahmendomäne (z. B. in der Domäne ENGPOLDOM) anzuzeigen, geben Sie den folgenden Befehl aus:

```
query mgmtclass engpoldom * *
```

Beispiel: Ausführliche Informationen zu einer bestimmten Verwaltungsklasse anzeigen

Die Verwaltungsklasse ACTIVEFILES abfragen, die der Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE_RECORDS zugeordnet ist. Die Ausgabe soll im ausführlichen Format erstellt werden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query mgmtclass employee_records vacation
activefiles format=detailed
```

```
                    Name der Maßnahmendomäne: EMPLOYEE_RECORDS
                 Name der Maßnahmengruppe: VACATION
              Name der Verwaltungsklasse: ACTIVEFILES
              Standardverwaltungsklasse?: Yes
                           Beschreibung: Inst. def. management class
             Speicherverwaltungstechnik: None
       Auto-Umlagerung bei Nichtbenutzung: 0
    Sicherung vor Umlagerung erforderl.?: Yes
         Zielort für umgelagerte Dateien: SPACEMGPOOL
            Letzte Aktualisierung durch
                        (Administrator): $$CONFIG_MANAGER$$
     Datum/Zeit der letzten Aktualisierung: 05/31/1998 13:15:45
                  Verwaltendes Profil: EMPLOYEE
                Änderungen anstehend: Yes
```

Feldbeschreibungen

Name der Maßnahmendomäne
: Die Maßnahmendomäne.

Name der Maßnahmengruppe
: Die Maßnahmengruppe.

Name der Verwaltungsklasse
: Die Verwaltungsklasse.

Standardverwaltungsklasse?
: Angabe, ob die Verwaltungsklasse die Standardverwaltungsklasse für die Maßnahmengruppe ist.

Beschreibung
: Die Beschreibung der Verwaltungsklasse.

Speicherverwaltungstechnik
: Die Speicherverwaltungstechnik für die Verwaltungsklasse für IBM Spectrum Protect for Space Management-Clients.

Auto-Umlagerung bei Nichtbenutzung
: Die Anzahl Tage, die nach dem letzten Zugriff auf eine Datei verstreichen müssen, bevor die Datei für die automatische Umlagerung durch IBM Spectrum Protect for Space Management-Clients ausgewählt werden kann.

Sicherung vor Umlagerung erforderlich?
: Angabe, ob eine Sicherungsversion einer Datei vorhanden sein muss, bevor eine Datei durch IBM Spectrum Protect for Space Management-Clients umgelagert werden kann.

Zielort für umgelagerte Dateien
: Der Speicherpool, der der Zielort für Dateien ist, die von IBM Spectrum Protect for Space Management-Clients umgelagert werden.

Letzte Aktualisierung durch (Administrator)
: Der Administrator oder Server, der die Verwaltungsklasse zuletzt aktualisiert hat. Enthält dieses Feld $$CONFIG_MANAGER$$, ist die Verwaltungsklasse einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der die Verwaltungsklasse definiert oder zuletzt aktualisiert wurde.

Verwaltendes Profil
: Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition dieser Verwaltungsklasse zu erhalten.

Änderungen anstehend
: Angabe, ob Änderungen vorgenommen, aber nicht aktiviert werden. Sobald die Änderungen aktiviert werden, wird das Feld auf No zurückgesetzt.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MGMTCLASS

Befehl	Beschreibung
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DELETE MGMTCLASS	Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
UPDATE MGMTCLASS	Ändert die Attribute einer Verwaltungsklasse.

QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)

Verwenden Sie diesen Befehl, um Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus anzuzeigen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query MONITORSEttings---------------------------------------><
```

Überwachungseinstellungen anzeigen

Ausführliche Informationen zu den Überwachungseinstellungen anzeigen. Ausführliche Informationen befinden sich in Feldbeschreibungen.

```
query monitorsettings
```

Beispielausgabe:

```
                                        Status überwachen: On
                    Statusaktualisierungsintervall (Minuten): 5
                                Statusbeibehaltung (Stunden): 48
                                Nachrichtenalerts überwachen: On
                     Alertaktualisierungsintervall (Minuten): 10
                                    Alert an E-Mail-Adresse: On
               Alertzusammenfassung an Administratoren senden: On
                                Alert von E-Mail-Adresse: DJADMIN@MYDOMAIN.COM
                                        Alert-SMTP-Host: DJHOST.MYDOMAIN.COM
                                    Alert-SMTP-Anschluss: 25
                  Dauer des Alertstatus 'aktiv' (Minuten): 480
                Dauer des Alertstatus 'inaktiv' (Minuten): 480
             Dauer des Alertstatus 'geschlossen' (Minuten): 60
                                Überwachungsadministrator: ADMINISTRATOR
                                        Überwachte Gruppe: MONGROUP
                                        Überwachte Server: SERVER2
                           Gefährdungsintervall für Anwendungen: 24
    Übersprungene Dateien als Gefährdung für Anwendungen ansehen?: Yes
                      Gefährdungsintervall für virtuelle Maschinen: 24
Übersprungene Dateien als Gefährdung für virtuelle Maschinen ansehen?: Yes
                                Gefährdungsintervall für Systeme: 24
        Übersprungene Dateien als Gefährdung für Systeme ansehen?: Yes
```

Feldbeschreibungen

Status überwachen
: Gibt an, ob die Alertüberwachung auf dem Server aktiviert oder inaktiviert ist.

Statusaktualisierungsintervall (Minuten)
: Gibt die Anzahl Minuten zwischen Intervallen an, in denen der Überwachungsserver Ereignisdaten zusammenstellt.

Statusbeibehaltung (Stunden)
: Gibt die Anzahl Stunden an, die Statusüberwachungsanzeiger beibehalten werden.

Nachrichtenalerts überwachen
: Gibt an, ob Alerts in einer E-Mail an Administratoren gesendet werden.

Alertaktualisierungsintervall (Minuten)
: Gibt die Zeit in Minuten an, die der Alertmonitor wartet, bevor der Alert auf dem Server aktualisiert und bereinigt wird.

Alert an E-Mail-Adresse
: Gibt an, ob Alerts in einer E-Mail an Administratoren gesendet werden.

Alertzusammenfassung an Administratoren senden
: Gibt die Administratoren an, die in einer E-Mail eine Zusammenfassung der vorhandenen Alerts auf dem Server empfangen.

Alert von E-Mail-Adresse
: Gibt die E-Mail-Adresse des Absenders an.

Alert-SMTP-Host
: Gibt den SMTP-Host-Mail-Server (SMTP = Simple Mail Transfer Protocol) an, der zum Senden von Alerts in einer E-Mail verwendet wird.

Alert-SMTP-Anschluss
: Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.

Dauer des Alertstatus 'aktiv' (Minuten)
: Gibt die Zeit in Minuten an, die ein Alert aktiv bleibt.

Dauer des Alertstatus 'inaktiv' (Minuten)

Gibt die Zeit in Minuten an, die ein Alert inaktiv bleibt.

Dauer des Alertstatus 'geschlossen' (Minuten)

Gibt die Zeit in Minuten an, die ein Alert geschlossen bleibt, bevor der Alert auf dem Server gelöscht wird.

Überwachungsadministrator

Gibt den Namen des Überwachungsadministrators an, der verwendet wird, um die Verbindung zu den Servern in der überwachten Gruppe herzustellen.

Überwachte Gruppe

Gibt den Namen der überwachten Servergruppe an.

Überwachte Server

Gibt die Namen der Server in der überwachten Servergruppe an. Die Überwachungseinstellungen können auf den überwachten Servern unterschiedlich sein. Ist dies der Fall, geben Sie für jeden Server den Abfragebefehl aus, um die Überwachungseinstellungen anzuzeigen.

Gefährdungsintervall für Anwendungen

Gibt die Anzahl Stunden an, die ein Anwendungsclient keine Aktivität protokollieren kann, bevor er als gefährdet angesehen wird.

Übersprungene Dateien als Gefährdung für Anwendungen ansehen?

Gibt an, dass der Server vom Client übersprungene Dateien als Fehler ansieht und den Client als gefährdet markiert.

Gefährdungsintervall für virtuelle Maschinen

Gibt die Anzahl Stunden an, die ein virtueller Client keine Aktivität protokollieren kann, bevor er als gefährdet angesehen wird.

Übersprungene Dateien als Gefährdung für virtuelle Maschinen ansehen?

Gibt an, dass der Server vom Client übersprungene Dateien als Fehler ansieht und den Client als gefährdet markiert.

Gefährdungsintervall für Systeme

Gibt die Anzahl Stunden an, die ein Systemclient keine Aktivität protokollieren kann, bevor er als gefährdet angesehen wird.

Übersprungene Dateien als Gefährdung für Systeme ansehen?

Gibt an, dass der Server vom Client übersprungene Dateien als Fehler ansieht und den Client als gefährdet markiert.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MONITORSETTINGS

Befehl	Beschreibung
DEFINE ALERTTRIGGER (Alertauslöser definieren)	Ordnet angegebene Nachrichten einem Alertauslöser zu.
DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)	Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.
DELETE GRPMEMBER (Server aus einer Servergruppe löschen)	Löscht einen Server aus einer Servergruppe.
DELETE SERVER (Server-Definition löschen)	Löscht die Definition eines Servers.
QUERY ALERTSTATUS (Status eines Alert abfragen)	Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.
QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)	Zeigt Nachrichtennummern an, die einen Alert auslösen.
SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)	Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.
UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)	Aktualisiert die Attribute eines oder mehrerer Alertauslöser.
UPDATE ALERTSTATUS (Status eines Alert aktualisieren)	Aktualisiert den Status eines zurückgemeldeten Alert.

QUERY MONITORSTATUS (Überwachungsstatus abfragen)

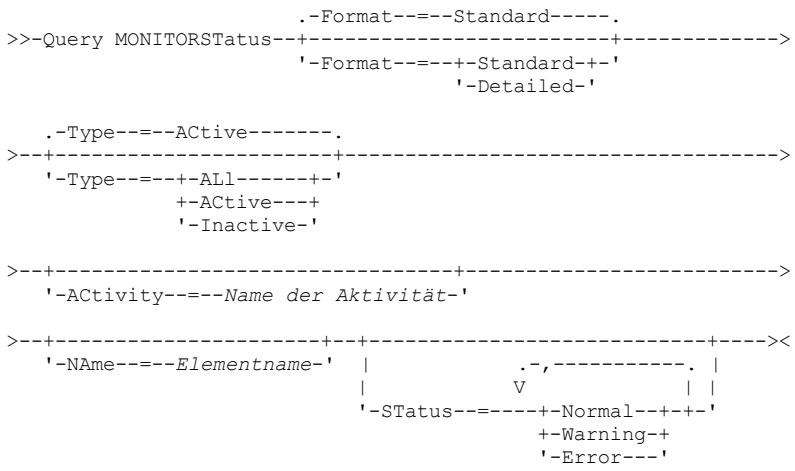
Mit diesem Befehl können Sie Überwachungsnachrichten anzeigen, die innerhalb des definierten Zeitraums für die Statusbeibehaltung liegen.

Sie können die Ausgabe auf einen angegebenen Status begrenzen, wie z. B. auf Nachrichten mit dem Status 'aktiv'. Werden keine Parameter angegeben, werden alle Nachrichten angezeigt.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Format
: Gibt den Umfang der Informationen an, die angezeigt werden. Der Standardwert ist STANDARD. Geben Sie einen der folgenden Werte an:

  Standard
  : Gibt an, dass nur Teilinformationen für die angegebenen Nachrichten angezeigt werden.

  Detailed
  : Gibt an, dass alle Informationen für die angegebenen Nachrichten angezeigt werden.

Type
: Dieser Parameter begrenzt die Ausgabe auf Nachrichten mit dem angegebenen Wert für den Typ. Geben Sie einen der folgenden Werte an:

  ALl
  : Zeigt alle Informationen an.

  ACtive
  : Zeigt alle aktiven Nachrichten an. Dies ist der Standardwert.

  Inactive
  : Zeigt alle inaktiven Nachrichten an.

ACtivity
: Gibt die Aktivität an, die abgefragt werden soll. Die Beschreibung des Befehls DEFINE STATUSTHRESHOLD enthält ausführliche Informationen zu den verfügbaren Aktivitäten für die Abfrage.

NAme
: Gibt den Namen an, der abgefragt werden soll. Der Wert für NAME bezieht sich auf den Namen des Elements mit der angegebenen Aktivität. Beispiel: Für einen Statusanzeiger, der Informationen zu einem Speicherpool mit dem Namen `backuppool` enthält, wird NAME auf BACKUPPOOL gesetzt.

STatus
: Gibt den Status der Nachrichten an, der abgefragt werden soll. Es können mehrere Statuswerte in einer Liste angegeben werden, indem die Werte ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, werden Informationen zu allen Statuswerten angezeigt. Geben Sie einen der folgenden Werte an:

  Normal
  : Zeigt alle Nachrichten mit einem normalen Status an.

  Warning
  : Zeigt alle Nachrichten mit einem Warnstatus an.

  Error
  : Zeigt alle Nachrichten mit einem Fehlerstatus an.

Überwachungseinstellungen anzeigen

Ausführliche Informationen zum Überwachungsstatus anzeigen.

```
Query MONITORStatus type=active
```

Beispielausgabe:

```
            Servername: SERVER1
     Datum der Aktivität: 05.03.2013 15:57:37
      Name der Aktivität: Kapazität des primären Platten- und
                          Dateispeichers
           Elementname: Kapazität des primären Platten- und
```

```
                            Dateispeichers
Numerischer Wert des Elements: 0
Zeichenfolgewert des Elements:
               Elementstatus: NORMAL

                  Servername: SERVER1
          Datum der Aktivität: 05.03.2013 15:57:37
           Name der Aktivität: Verwendete Kapazität des primären Platten-
                               und Dateispeichers
                 Elementname: Verwendete Kapazität des primären Platten-
                               und Dateispeichers
Numerischer Wert des Elements: 0
Zeichenfolgewert des Elements:
               Elementstatus: NORMAL

                  Servername: SERVER1
          Datum der Aktivität: 05.03.2013 15:57:37
           Name der Aktivität: Kapazität des primären Bandspeichers
                 Elementname: Kapazität des primären Bandspeichers
Numerischer Wert des Elements: 0
Zeichenfolgewert des Elements:
               Elementstatus: NORMAL

                  Servername: SERVER1
          Datum der Aktivität: 05.03.2013 15:57:37
           Name der Aktivität: Verwendete Kapazität des primären Bandspeichers
                 Elementname: Verwendete Kapazität des primären Bandspeichers
Numerischer Wert des Elements: 0
Zeichenfolgewert des Elements:
               Elementstatus: NORMAL
```

Überwachungseinstellungen anzeigen

Ausführliche Informationen zum Überwachungsstatus anzeigen.

```
query monitorstatus f=d type=active
```

Beispielausgabe:

```
                                       Servername: SERVER1
                     Datum der Aktivität: 05.03.2013 15:57:37
                      Name der Aktivität: Kapazität des primären Platten- und Dateispeichers
                             Elementname: Kapazität des primären Platten- und Dateispeichers
           Numerischer Wert des Elements: 0
           Zeichenfolgewert des Elements:
                         Elementstatus: NORMAL
                        Elementdetails:
             Primärer Reparaturvorschlag:
    Erster alternativer Reparaturvorschlag:
  Zweiter alternativer Reparaturvorschlag:

                                       Servername: SERVER1
                     Datum der Aktivität: 05.03.2013 15:57:37
                      Name der Aktivität: Verwendete Kapazität des primären Platten- und Dateispeichers
                             Elementname: Verwendete Kapazität des primären Platten- und Dateispeichers
           Numerischer Wert des Elements: 0
           Zeichenfolgewert des Elements:
                         Elementstatus: NORMAL
                        Elementdetails:
             Primärer Reparaturvorschlag:
    Erster alternativer Reparaturvorschlag:
  Zweiter alternativer Reparaturvorschlag:

                                       Servername: SERVER1
                     Datum der Aktivität: 05.03.2013 15:57:37
                      Name der Aktivität: Kapazität des primären Bandspeichers
                             Elementname: Kapazität des primären Bandspeichers
           Numerischer Wert des Elements: 0
           Zeichenfolgewert des Elements:
                         Elementstatus: NORMAL
                        Elementdetails:
             Primärer Reparaturvorschlag:
    Erster alternativer Reparaturvorschlag:
  Zweiter alternativer Reparaturvorschlag:

                                       Servername: SERVER1
                     Datum der Aktivität: 05.03.2013 15:57:37
                      Name der Aktivität: Verwendete Kapazität des primären Bandspeichers
                             Elementname: Verwendete Kapazität des primären Bandspeichers
           Numerischer Wert des Elements: 0
           Zeichenfolgewert des Elements:
```

```
                          Elementstatus: NORMAL
                         Elementdetails:
              Primärer Reparaturvorschlag:
    Erster alternativer Reparaturvorschlag:
  Zweiter alternativer Reparaturvorschlag:
```

Feldbeschreibungen

Servername
: Der Name des Servers.

Datum der Aktivität
: Gibt an, wann die Aktivität zuletzt zurückgemeldet wurde.

Name der Aktivität
: Der Name der Aktivität.

Elementname
: Der Name des Elements.

Numerischer Wert des Elements
: Der numerische Wert des Elements.

Zeichenfolgewert des Elements
: Der Zeichenfolgewert des Elements.

Elementstatus
: Der Status des Elements.

Elementdetails
: Die detaillierten Informationen des Elements.

Primärer Reparaturvorschlag
: Der primäre Reparaturvorschlag.

Erster alternativer Reparaturvorschlag
: Der zu befolgende Reparaturvorschlag, falls der primäre Vorschlag nicht geeignet ist.

Zweiter alternativer Reparaturvorschlag
: Der zu befolgende Reparaturvorschlag, falls der primäre und der erste alternative Vorschlag nicht geeignet sind.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MONITORSTATUS

Befehl	Beschreibung
DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)	Definiert einen Schwellenwert für die Statusüberwachung.
DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)	Löscht einen Schwellenwert für die Statusüberwachung.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)	Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.
UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)	Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.

QUERY MOUNT (Informationen zu bereitgestellten Datenträgern mit sequenziellem Zugriff anzeigen)

Mit diesem Befehl können Informationen zum Status eines oder mehrerer bereitgestellter Datenträger mit sequenziellem Zugriff angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                .-*---------------.
>>-Query MOunt--+-----------------+----------------------------->
                '-Datenträgername-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Datenträgername
: Gibt den Namen des bereitgestellten Datenträgers mit sequenziellem Zugriff an. Dieser Name kann mithilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert sind alle bereitgestellten Datenträger.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Alle geladenen sequenziellen Datenträger auflisten

Informationen zu allen geladenen sequenziellen Datenträgern anzeigen.

```
query mount
```

 AIX-Betriebssysteme

```
ANR8330I 3590 Datenträger D6W992 wurde im Modus R/O
in Laufwerk RMT1 (/dev/rmt1) geladen, Status: IN USE.
ANR8334I  1 Datenträger gefunden.
ANR8331I 8MMTAPE Datenträger WPD000 wurde im Modus
R/W in Laufwerk 8MM.1 (/dev/mt0) geladen, Status: DISMOUNTING.
ANR8334I  1 Datenträger gefunden.
```

 Linux-Betriebssysteme

```
ANR8330I 3590 Datenträger D6W992 wurde im Modus R/O
in Laufwerk RMT1/dev/IBMtape1 geladen, Status: IN USE.
ANR8334I  1 Datenträger gefunden.
ANR8331I 8MMTAPE Datenträger WPD000 wurde im Modus
R/W in Laufwerk 8MM.1 (/dev/tsmscsi/mt0) geladen, Status: DISMOUNTING.
ANR8334I  1 Datenträger gefunden.
```

 Windows-Betriebssysteme

```
ANR8330I 3590 Datenträger D6W992 wurde im Modus R/O
in Laufwerk RMT1 (/dev/rmt1) geladen, Status: IN USE.
ANR8334I  1 Datenträger gefunden.
ANR8331I 8MMTAPE Datenträger WPD000 wurde im Modus
R/W in Laufwerk 8MM.1 (mt3.0.0.0) geladen, Status: DISMOUNTING.
ANR8334I  1 Datenträger gefunden.
```

Hinweis:

1. Lautet der Status eines Datenträgers FULL oder lautet sein Zugriffsmodus READ-ONLY (R/O), ist der Lademodus des Datenträgers R/O. Um den Status und Zugriffsmodus eines Datenträgers zu bestimmen, geben Sie den Befehl QUERY VOLUME FORMAT=DETAILED aus. Kann ein Datenträger beschrieben werden (d. h., der Status lautet FILLING oder EMPTY), ist der Lademodus des Datenträgers READ/WRITE (R/W), auch wenn der Datenträger nur gelesen wird.
2. In einem Speicherpool, dem der Einheitentyp FILE oder CENTERA zugeordnet ist, kann der Server gleichzeitig mehrere Lesezugriffe und einen Schreibzugriff auf denselben Datenträger ausführen. Daher kann ein Datenträger in einem Speicherpool mit einem Einheitentyp FILE oder CENTERA mehrmals als geladen angezeigt werden.
3. In der Nachricht ANR8448I wird der Laufwerkname als `UNKNOWN` für Datenträger des Einheitentyps FILE mit einer nicht gemeinsam genutzten Einheitenklasse aufgelistet. Der Grund liegt darin, dass den Datenträgern kein Laufwerk zugeordnet ist; Laufwerknamen werden in dem dateibasierten Speicherarchiv angezeigt.

4. Wenn Sie den Befehl QUERY MOUNT ausgeben, während das Laufwerk gereinigt wird, zeigt die Befehlsausgabe weiterhin den Status `DISMOUNTING` für den entladenen Datenträger an, bis die Reinigung abgeschlossen ist.

Beispiel: Ausführliche Informationen zu geladenen sequenziellen Datenträgern anzeigen

Ausführliche Informationen zu geladenen Datenträgern anzeigen.

```
query mount format=detailed

ANR2017I Administrator SERVER_CONSOLE hat folgenden Befehl ausgegeben: QUERY
MOUNT format=detailed
ANR8487I Mountpunkt in Einheitenklasse FILE wartet auf die Beendigung
des Datenträgerladevorgangs -- Eignerserver: SERVER1, Status: WAITING
FOR VOLUME (Sitzung: 0, Prozess: 1).
ANR8488I LTO-Datenträger 015005L4 wurde im Modus R/W in Laufwerk
IBMVTL1 (/dev/rmt37) geladen -- Eignerserver: SERVER1, Status: IN
USE (Sitzung: 0, Prozess: 2).
ANR8486I Mountpunkt in Einheitenklasse FILE ist reserviert --
Eignerserver: SERVER1, Status: RESERVED (Sitzung: 5, Prozess: 0).
ANR8334I         3 Übereinstimmungen gefunden.
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY MOUNT

Befehl	Beschreibung
DISMOUNT VOLUME	Entlädt einen sequenziellen entfernbaren Datenträger anhand des Datenträgernamens.
REPLY	Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.

QUERY NASBACKUP (NAS-Sicherungsimages abfragen)

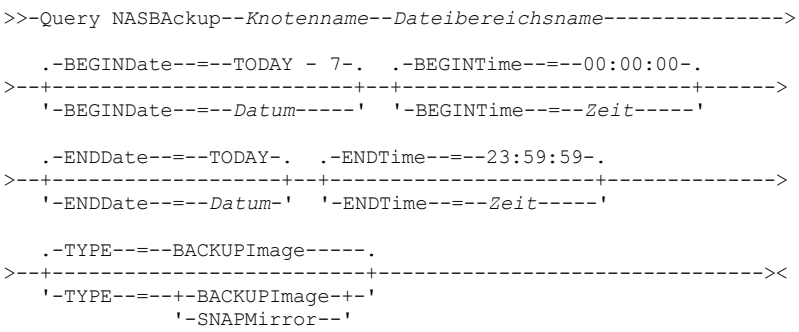
Mit diesem Befehl können Informationen zu Dateisystemimageobjekten angezeigt werden, die für einen bestimmten NAS-Knoten und Dateibereich gesichert wurden. Sie können diesen Befehl nur verwenden, um Objekte anzuzeigen, die mit NDMP für einen NAS-Knoten gesichert wurden.

Der Server zeigt alle übereinstimmenden Objekte an, die Daten, an denen diese Objekte gesichert wurden, und Informationen zu einem Inhaltsverzeichnis (TOC) für das Objekt.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Knotenname (Erforderlich)
: Gibt den Namen des NAS-Knotens an, für den Sicherungsobjekte angezeigt werden. Sie können zur Angabe dieses Namens keine Platzhalterzeichen verwenden.

Dateibereichsname (Erforderlich)
: Gibt den Namen des Dateibereichs an, für den Sicherungsobjekte angezeigt werden. Sie können zur Angabe dieses Namens Platzhalterzeichen verwenden.

BEGINDate

Gibt das Anfangsdatum an, ab dem Sicherungsobjekte angezeigt werden sollen. Alle Sicherungsobjekte, die an oder nach dem angegebenen Datum erstellt wurden, werden angezeigt. Der Standardwert ist sieben Tage vor dem aktuellen Datum. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Dieser Parameter ist wahlfrei.
Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/2002
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–7 *oder* –7. Sollen Informationen zu den Imageobjekten angezeigt werden, die vor einer Woche erstellt wurden, können Sie BEGINDATE=TODAY-7 oder BEGINDATE= -7 angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt die Anfangszeit an, ab der Sicherungsobjekte angezeigt werden sollen. Alle Sicherungsobjekte, die zu oder nach der angegebenen Zeit erstellt wurden, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist Mitternacht (00:00:00) an dem Datum, das als BEGINDATE angegeben wurde.
Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Anfangsdatum	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Anfangsdatum	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum	NOW+03:00 *oder* +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW+3 oder BEGINTIME=+3 ausgegeben, zeigt der Server Imageobjekte mit der Uhrzeit 12:00 Uhr oder später am Anfangsdatum an.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum	NOW-04:00 *oder* -04:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTime=NOW-3:30 oder BEGINTime= -3:30 ausgegeben, zeigt der Server Imageobjekte mit der Uhrzeit 5:30 Uhr oder später am Anfangsdatum an.

ENDDate

Gibt das Enddatum an, das zum Auswählen der Sicherungsobjekte verwendet wird, die angezeigt werden sollen. Alle Sicherungsobjekte, die an oder vor dem angegebenen Datum erstellt wurden, werden angezeigt. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Dieser Parameter kann mit dem Parameter ENDTIME verwendet werden, um ein Enddatum und eine Endzeit anzugeben.
Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/2002
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY–1 *oder* –1. Sollen Informationen angezeigt werden, die bis gestern erstellt wurden, kann ENDDATE=TODAY-1 oder einfach ENDDATE= -1 angegeben werden.

Wert	Beschreibung	Beispiel
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDTime

Gibt die Endzeit an, die zum Auswählen der Sicherungsobjekte verwendet wird, die angezeigt werden sollen. Alle Sicherungsobjekte, die zu oder vor der angegebenen Zeit erstellt wurden, werden angezeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist 23:59:59. Dieser Parameter kann zusammen mit dem Parameter ENDDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Enddatum	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Enddatum	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum	NOW+03:00 *oder* +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+3:00 oder ENDTIME= +3:00 ausgegeben, zeigt der Server Imageobjekte mit der Uhrzeit 12:00 Uhr oder später am angegebenen Enddatum an.
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum	NOW-03:30 *oder* -03:30. Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME= -3:30 ausgegeben, zeigt der Server Imageobjekte mit der Uhrzeit 5:30 Uhr oder später am angegebenen Enddatum an.

TYPE

Gibt den Typ der NDMP-Sicherungsimages an, für die Informationen angezeigt werden sollen. Der Standardwert für diesen Parameter ist BACKUPIMAGE. Andere Imagetypen stellen Sicherungsmethoden dar, die für einen bestimmten Dateiserver spezifisch sein können. Gültige Werte:

BACKUPImage
: Gibt an, dass die Ausgabe nur die standardmäßigen NAS-Basis- und -Differenzsicherungsimages zeigen soll. Dies ist der Standardwert für diesen Parameter.

SNAPMirror
: Gibt an, ob Informationen zu NetApp SnapMirror-Images angezeigt werden sollen. SnapMirror-Images sind Gesamtsicherungsimages auf Blockebene eines Dateisystems. Ein SnapMirror-Image kann nur in ein Dateisystem zurückgeschrieben werden, das als SnapMirror-Zieldatenträger vorbereitet wurde. Weitere Informationen enthält die Dokumentation zu Ihrem NetApp-Dateiserver. Dieser Parameter ist nur für NetApp- und IBM N-Series-Dateiserver gültig.

Beispiel:

Geben Sie den Befehl QUERY NASBACKUP aus, um Informationen zu dem Knoten nas1 und dem Dateibereich /vol/vol1 anzuzeigen.

```
query nasbackup nas1 /vol/vol1

Knoten- Dateiber.- Objekt-   Objekt- Erstell.-  Hat         Verwalt.-   Image-
name    Name       typ       größe   Datum      Inhalts-    Klassen-    speicher-
                   (MB)      (MB)               verzeichnis name        poolname
------ --------  ---------   -----   ---------- --------  --------  --------
NAS1   vol/vol1  Gesamtimage 1050,5  10/22/2002  YES        DEFAULT     NASBACKUPS
                                      10:50:57
NAS1   vol/vol1  Differenz-    9,1   10/22/2002  YES        DEFAULT     NASBACKUPS
                 image                11:03:21
NAS1   vol/vol1  Gesamtimage 1050,5  10/22/2006  YES        STANDARD    FILEPOOL
                                      10:43:00
```

```
NAS1   vol/vol1   Differenz-     9,1    10/25/2006  YES         STANDARD     FILEPOOL
                  image                   11:53:21
```

Beispiel:

Geben Sie den Befehl QUERY NASBACKUP aus, um Informationen zu allen NetApp SnapMirror-auf-Band-Images für den Knoten nas2 und den Dateibereich /vol/vol2 anzuzeigen.

```
query nasbackup nas2 /vol/vol2 type=snapmirror

Knoten- Dateiber.- Objekt-   Objekt- Erstell.-   Verwalt.-   Image-
name    Name       typ       größe   Datum       Klassen-    speicher-
                             (MB)                name        poolname
------  ---------  -------   ------  ---------   --------    --------
NAS2    vol/vol2   SnapMirror  1050,5  04/02/2008  STANDARD    MYPOOL
                                       10:50:57
NAS2    vol/vol2   SnapMirror  1450,5  04/02/2008  STANDARD    MYPOOL
                                       11:03:21
```

Feldbeschreibungen

Knotenname
: Der Name des Clientknotens.

Dateibereichsname
: Der Name des Dateibereichs.

Objekttyp
: Der Typ des gesicherten Objekts.

Objektgröße (MB)
: Die Größe des Objekts in Megabyte.

Erstellungsdatum
: Das Datum, an dem die Sicherung erstellt wurde.

Name der Verwaltungsklasse
: Der Name der Verwaltungsklasse.

Imagespeicherpoolname
: Der Name des Speichers, in dem sich die Sicherung befindet.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY NASBACKUP

Befehl	Beschreibung
BACKUP NODE	Sichert einen NAS-Knoten (NAS = Network Attached Storage).
BACKUP NAS (IBM Spectrum Protect-Clientbefehl)	Erstellt eine Sicherung der NAS-Knotendaten.
QUERY TOC	Zeigt Details zum Inhaltsverzeichnis für ein angegebenes Sicherungsimage an.
RESTORE NODE	Schreibt einen NAS-Knoten (NAS = Network Attached Storage) zurück.

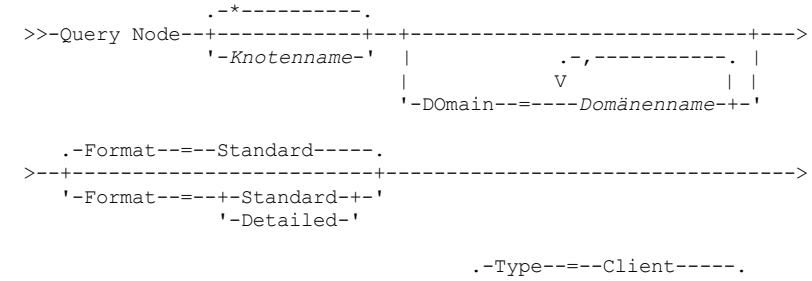
QUERY NODE (Knoten abfragen)

Mit diesem Befehl können Informationen zu einem oder zu mehreren registrierten Knoten angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



```
>--+-----------------------------+--+---------------------+--->< 
   '-AUTHentication--=--+-LOcal-+-'  '-Type--=--+-Client-+-'
                        '-LDap--'               +-NAS----+
                                                +-Server-+
                                                '-Any----'
```

Parameter

Knotenname
: Gibt den Namen des abzufragenden Clientknotens an. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Clientknoten werden abgefragt. Wird kein Wert für diesen Parameter angegeben, werden alle Clientknoten abgefragt. Der Parameter ist wahlfrei.

DOmain
: Gibt eine Liste mit Maßnahmendomänen an, auf die sich die Clientknotenabfrage beschränken soll. In diesem Fall werden dann nur Knoten angezeigt, die einer der angegebenen Maßnahmendomänen zugeordnet sind. Dieser Parameter ist wahlfrei. Die Einträge in der Liste ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden, um eine Domäne anzugeben. Alle Clients, die einer übereinstimmenden Domäne zugeordnet sind, werden angezeigt. Wird kein Wert für diesen Parameter angegeben, wird die Abfrage für alle Maßnahmendomänen ausgeführt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Sie können einen der folgenden Werte angeben:

  Standard
  : Gibt an, dass Teilinformationen für die angegebenen Clientknoten angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen für die angegebenen Clientknoten angezeigt werden.

Type
: Gibt den Typ des Knotens an, der in den Abfrageergebnissen berücksichtigt werden soll. Der Parameter ist wahlfrei. Der Standardwert ist CLIENT. Sie können einen der folgenden Werte angeben:

  Any
  : Gibt einen beliebigen Typ des Knotens an.

  Client
  : Gibt Clientknoten an, die Clients für Sichern/Archivieren, IBM Spectrum Protect for Space Management-Clients oder Anwendungsclients sind.

  NAS
  : Gibt NAS-Knoten an.

  Server
  : Gibt Clientknoten an, die andere -Server sind.

Authentication
: Gibt die Kennwortauthentifizierungsmethode für den Knoten an.

  LOcal
  : Zeigt die Knoten an, die sich mit dem IBM Spectrum Protect-Server authentifizieren.

  LDap
  : Zeigt die Knoten an, die sich mit einem LDAP-Verzeichnisserver authentifizieren. Bei dem Knotenkennwort muss die Groß-/Kleinschreibung beachtet werden.

Beispiel: Informationen zu registrierten Clientknoten anzeigen

Informationen zu allen registrierten Clientknoten anzeigen.

```
query node

Knotenname  Plattform Maßnah-         Tage seit   Tage seit  Gesperrt?
                      mendomäne       letz. Zugr. Kennwort-
                                                  vergabe
---------   --------  --------        ---------   ---------- -------
CLIENT1       AIX     STANDARD              6            6    No
GEORGE        AIX     STANDARD              1            1    No
JANET         AIX     STANDARD              1            1    No
JARED       Linux86   STANDARD              1            1    No

JOE2        Mac       STANDARD             <1           <1    No
TOMC        WinNT     STANDARD              1            1    No
```

Beispiel: Ausführliche Informationen zu einem Clientknoten anzeigen

Die gesamten Informationen zum Clientknoten Joe anzeigen.

```
query node joe format=detailed

                                  Knotenname: JOE
                                   Plattform: WinNT
                              Client-OS-Stufe: 4.00
                               Client-Version: Version 5, Release 4, Stufe 0.0
                           Anwendungsversion: Version 6, Release 4, Stufe 0.4
                     Name der Maßnahmendomäne: STANDARD
                              Letzter Zugriff: 09/24/2012 18:55:46
                    Tage seit letztem Zugriff: 6
                Datum/Zeit der Kennwortvergabe: 09/24/2012 18:26:43
                     Tage seit Kennwortvergabe: 6
            ahl der ungültigen Anmeldeversuche: 0
                                  Gesperrt?: No
                          Kontaktinformationen:
                                 Komprimierung: Client
                        Archivierung löschen?: Yes
                           Sicherung löschen?: No
                               Registriert am: 09/24/2012 18:26:43
                            Registriert durch: SERVER_CONSOLE
       Zuletzt verwendete Übertragungsmethode: Tcp/Ip
              Byte empfangen (letzte Sitzung): 108.731
               Byte gesendet (letzte Sitzung): 698
                    Dauer der letzten Sitzung: 0,00
  Inaktiver Wartestatus in % (letzte Sitzung): 0,00
Auf Übertragung warten in % (letzte Sitzung): 0,00
Auf Datenträger warten in % (letzte Sitzung): 0,00
                                Optionsgruppe:
                                    URL: http://joe.host.name:1581
                                  Knotentyp: Client
                         Kennwortablaufdauer: 60
                      Mountpunkt beibehalten?: No
                  Max. zulässige Mountpunkte: 2
              Auto. Dateibereichsumbenennung: No
                        Protokoll auswerten: No
                                TCP/IP-Name:
                             TCP/IP-Adresse: 9.11.153.39
                       Global eindeutige ID: 11.9c.54.e0.8a.b5.11.d6.b3.c3.00.06.29.45.cl
                    Max. Transaktionsgruppe: 0
                Pfad zum Schreiben von Daten: ANY
                    Pfad zum Lesen von Daten: ANY
                                Sitzungsstart: ClientOrServer
                    Adresse der oberen Ebene:
                   Adresse der unteren Ebene: 1501
                Name der Kollokationsgruppe:
                             Proxyknotenziel:
                           Proxyknotenagent:
                              Knotengruppen:
                             E-Mail-Adresse:
                                                          Deduplizierung: ServerOnly

AIX-BetriebssystemeLinux-BetriebssystemeBenutzer, die Sicherung ausführen dürfen: ALL
                                Replikationsstatus: Aktiviert
                                 Replikationsmodus: Send
            Replikationsregel für Sicherungsdaten: DEFAULT
          Replikationsregel für Archivierungsdaten: ALL_DATA
   Replikationsregel für speicherverwaltete Daten: None
                     Primärer Replikationsserver: PRODSERVER1
                  Zuletzt repliziert auf Server: DRSERVER1
                           Client-OS-Name: WIN: Windows XP
                        Clientprozessorarchitektur: x86
                        Installierte Clientprodukte: WIN, FCM, VE
                                 Clientzielversion: Version 6, Release 2, Stufe 0.0
                                 Authentifizierung: Local
                                  SSL erforderlich: No
    Sitzungssicherheit: Strict
                                 Transportmethode: TLS 1.2
                          Große Objekte aufteilen: Yes
                               Typ für Gefährdung: Standardintervall
                            Gefährdungsintervall:
                              Dienstprogramm-URL:
Replikationswiederherstellung beschädigter Dateien: Yes
                                       Stillgelegt:
                          Datum der Stilllegung:
```

Feldbeschreibungen

Knotenname
: Der Name des Clientknotens.

Plattform

Das Betriebssystem des Clientknotens zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat. Ein Fragezeichen (?) wird angezeigt, bis der Clientknoten zum ersten Mal auf den Server zugreift und seinen Betriebssystemtyp angibt.

Client-OS-Stufe
Die Stufe des Betriebssystems für den Client zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat.

Client-Version
Die Version des Clients, die auf dem Clientknoten installiert ist.

Dieses Feld gilt nicht für NAS-Knoten.

Anwendungsversion
Die Version des Data Protection for VMware-Clients.

Name der Maßnahmendomäne
Die zugeordnete Maßnahmendomäne des Clientknotens.

Letzter Zugriff
Das Datum und die Uhrzeit, an dem bzw. zu der der Clientknoten zuletzt auf den Server zugegriffen hat.

Tage seit letztem Zugriff
Die Anzahl der Tage, die vergangen sind, seit der Clientknoten das letzte Mal auf den Server zugegriffen hat.

Datum/Zeit der Kennwortvergabe
Das Datum und die Uhrzeit, an dem bzw. zu der das Kennwort für den Clientknoten definiert wurde.

Tage seit Kennwortvergabe
Die Anzahl der Tage, die vergangen sind, seit das Kennwort für den Clientknoten definiert wurde.

Zahl der ungültigen Anmeldeversuche
Die Anzahl der ungültigen Anmeldeversuche seit der letzten erfolgreichen Anmeldung. Diese Anzahl kann nur dann ungleich Null sein, wenn der Grenzwert für ungültige Kennworteingaben (SET INVALIDPWLIMIT) größer Null ist. Ist die Anzahl der ungültigen Versuche gleich dem mit dem Befehl SET INVALIDPWLIMIT definierten Grenzwert, wird der Knoten gesperrt.

Gesperrt?
Angabe, ob dem Clientknoten der Zugriff auf IBM Spectrum Protect verweigert wird.

Kontaktinformationen
Kontaktinformationen für den Clientknoten.

Komprimierung
Gibt an, ob die Komprimierung auf dem Clientknoten aktiviert ist.

Dieses Feld gilt nicht für NAS-Knoten.

Archivierung löschen?
Angabe, ob der Clientknoten seine eigenen Archivierungsdateien löschen darf.

Sicherung löschen?
Gibt an, ob der Clientknoten seine eigenen Sicherungsdateien löschen darf.

Registriert am
Das Datum und die Uhrzeit, an dem bzw. zu der der Clientknoten registriert wurde.

Registriert durch
Der Name des Administrators, der den Clientknoten registriert hat.

Zuletzt verwendete Übertragungsmethode
Die Übertragungsmethode, die zuletzt vom Clientknoten verwendet wurde, um den Server anzusprechen.

Byte empfangen (letzte Sitzung)
Die Anzahl der Byte, die während der letzten Sitzung des Clientknotens vom Server empfangen wurden.

Dieses Feld gilt nicht für NAS-Knoten.

Byte gesendet (letzte Sitzung)
Die Anzahl Byte, die an den Clientknoten gesendet wurden.

Dieses Feld gilt nicht für NAS-Knoten.

Dauer der letzten Sitzung
Die Dauer der letzten Sitzung des Clientknotens in Sekunden.

Dieses Feld gilt nicht für NAS-Knoten.

Inaktiver Wartestatus in % (letzte Sitzung)
Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client keine Funktionen ausgeführt hat.

Dieses Feld gilt nicht für NAS-Knoten.

Auf Übertragung warten in % (letzte Sitzung)
Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client auf eine Übertragungsantwort von dem Server gewartet hat.

Dieses Feld gilt nicht für NAS-Knoten.

Auf Datenträger warten in % (letzte Sitzung)
Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client auf das Laden eines austauschbaren Datenträgers gewartet hat.

Dieses Feld gilt nicht für NAS-Knoten.

Optionsgruppe
: Der Name der Clientoptionsgruppe.

URL
: Die URL des IBM Spectrum Protect-Web-Clients, die auf dem Clientsystem konfiguriert ist. Sie können die URL in einem Web-Browser und im Operations Center verwenden, um den Clientknoten über Fernzugriff zu verwalten.

Knotentyp
: Der Typ des Clientknotens. Die folgenden Werte sind gültig:

  - Client: Client für Sichern/Archivieren, IBM Spectrum Protect for Space Management-Client oder Anwendungsclient
  - Server: IBM Spectrum Protect-Server
  - NAS: NAS-Dateiserver

Kennwortablaufdauer
: Die Kennwortablaufdauer des Clientknotens.

Mountpunkt beibehalten?
: Die Angabe, ob der Clientknoten während einer Sitzung einen Mountpunkt beibehält.

Max. zulässige Mountpunkte
: Die Anzahl der Mountpunkte, die ein Clientknoten für die IBM Spectrum Protect for Space Management-Umlagerung sowie für Sicherungs- und Archivierungsoperationen auf dem Server verwenden kann. Dieser Parameter gilt nicht für Knoten mit dem Typ NAS oder SERVER. Wurde ein Clientknoten für einen Server mit Version 3.7 oder höher registriert, liegt der Wert im Bereich von 0 bis 999, abhängig von dem Wert, der mit dem Parameter MAXNUMMP des Befehls REGISTER NODE definiert wird. Wurde der Clientknoten unter vorherigen Versionen des Servers registriert und wurde der Parameter MAXNUMMP nicht explizit mit dem Befehl UPDATE NODE definiert, wird der Wert auf NOLIMIT gesetzt. Der MAXNUMMP-Wert wird während der Operationen zum Lesen von Clientdaten, wie beispielsweise Zurückschreiben, Abrufen und Zurückrufen durch IBM Spectrum Protect for Space Management, nicht ausgewertet oder umgesetzt. Mountpunkte, die für Operationen zum Lesen von Daten verwendet werden, werden jedoch in Bezug auf versuchte gleichzeitig ablaufende Datenspeicherungsoperationen für denselben Clientknoten ausgewertet. Diese Auswertung kann verhindern, dass die Datenspeicherungsoperationen Mountpunkte anfordern können.

Auto. Dateibereichsumbenennung
: Gibt an, ob IBM Spectrum Protect den Client zum Umbenennen von Dateibereichen auffordert, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt. Dieses Feld ist nur für Clientsysteme gültig, die die Betriebssysteme Windows, Macintosh OS X oder NetWare verwenden.

Protokoll auswerten (veraltet)
: Gibt an, ob für den Client die Datenprüfung aktiviert ist. Ist für den Client die Datenprüfung aktiviert, gibt dieses Feld an, ob IBM Spectrum Protect nur die Dateidaten oder alle Daten, einschließlich Dateimetadaten, auswertet. Sie können die Datenprüfung aktivieren, indem Sie den Befehl REGISTER NODE oder UPDATE NODE verwenden. Dieses Feld wird nicht mehr verwendet.

TCP/IP-Name
: Der Hostname des Clientknotens zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat. Das Feld ist leer, wenn die Clientsoftware das Melden dieser Informationen an den Server nicht unterstützt.

TCP/IP-Adresse
: Die TCP/IP-Adresse des Clientknotens zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat. Das Feld ist leer, wenn die Clientsoftware das Melden dieser Informationen an den Server nicht unterstützt.

Global eindeutige ID
: Die global eindeutige ID (Globally Unique Identifer = GUID) zu dem Zeitpunkt, als der Clientknoten das letzte Mal den Server angesprochen hat. Diese GUID identifiziert den Host-Computer, auf dem sich der Knoten befindet.

Max. Transaktionsgruppe
: Gibt die Anzahl der Dateien pro festgeschriebener Transaktion an, die zwischen einem Client und einem Server übertragen werden. Die Clientleistung kann verbessert werden, indem ein höherer Wert für diese Option verwendet wird.

Pfad zum Schreiben von Daten
: Gibt den Übertragungspfad an, der verwendet wird, wenn der Client während Speicheroperationen Daten an den Server und/oder den Speicheragenten sendet. Ist kein Pfad verfügbar, kann der Knoten keine Daten senden.

  AIX-BetriebssystemeLinux-BetriebssystemeGültige Datenübertragungsoptionen sind ANY, LAN oder LAN-unabhängig.

Pfad zum Lesen von Daten
: Gibt den Übertragungspfad an, der verwendet wird, wenn der Server und/oder Speicheragent während Operationen wie Zurückschreiben oder Abrufen Daten für einen Client lesen. Ist kein Pfad verfügbar, können keine Daten gelesen werden.

  AIX-BetriebssystemeLinux-BetriebssystemeGültige Datenübertragungsoptionen sind ANY, LAN oder LAN-unabhängig.

Sitzungsstart
: Steuert, ob der Server oder der Client Sitzungen einleitet. Die beiden folgenden Optionen sind verfügbar:

  - ClientOrServer
  - Serveronly

Adresse der höheren Ebene

Gibt die Client-IP-Adresse an, die der Server anspricht, um geplante Ereignisse einzuleiten, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist.

Adresse der unteren Ebene

Gibt die Clientanschlussnummer an, an der der Client für Sitzungen von dem Server empfangsbereit ist, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist.

Name der Kollokationsgruppe

Gibt den Namen der Kollokationsgruppe an, zu der ein Knoten gehört. Gehört ein Knoten nicht zu einer Kollokationsgruppe, ist dieses Feld leer.

Tipp: Wenn der Knoten Dateibereiche enthält, die Mitglieder einer Dateibereichskollokationsgruppe sind, bleibt dieses Feld leer. Sie können Dateibereichsnamen suchen, indem Sie den Befehl QUERY FILESPACE ausgeben.

Proxyknotenziel

Gibt in einer durch Leerzeichen getrennten Liste an, welche Knoten Proxyknoten (Agenten) für andere Knoten sind. Sind für diesen Typ der Zuordnung keine Knoten vorhanden, ist dieses Feld leer.

Proxyknotenagent

Gibt in einer durch Leerzeichen getrennten Liste den ursprünglichen Knotennamen (Zielknotennamen) für eine Proxyknotensitzung an. Sind für diesen Typ der Zuordnung keine Knoten vorhanden, ist dieses Feld leer.

Knotengruppen

Gibt den Namen der Knotengruppe an, zu der ein Knoten gehört. Gehört ein Knoten nicht zu einer Knotengruppe, ist dieses Feld leer.

E-Mail-Adresse

Gibt die E-Mail-Adresse des Clientknotens an.

Deduplizierung

Die Position, an der Daten dedupliziert werden. Der Wert ServerOnly gibt an, dass von diesem Knoten gespeicherte Daten nur auf dem Server dedupliziert werden können. Der Wert Clientorserver gibt an, dass von diesem Knoten gespeicherte Daten entweder auf dem Client oder auf dem Server dedupliziert werden können.

 AIX-Betriebssysteme  Linux-BetriebssystemeBenutzer, die Sicherung ausführen dürfen

 AIX-Betriebssysteme  Linux-BetriebssystemeGibt an, ob die ID eines Benutzers ohne Rootberechtigung oder nur eine Rootbenutzer-ID Dateien auf dem Server sichern kann. ALL gibt alle Benutzer an, während ROOT angibt, dass nur die Rootbenutzer-ID Dateien auf dem Server sichern kann. Diese Ausgabe ist nicht verfügbar, wenn das Betriebssystem des Clientknotens als Betriebssystem für einen einzelnen Benutzer betrachtet wird.

Replikationsstatus

Gibt an, ob der Knoten für die Replikation aktiviert ist. Die folgenden Werte sind gültig:

Aktiviert
: Der Knoten ist für die Replikation konfiguriert und für die Replikation bereit.

Inaktiviert
: Der Knoten ist für die Replikation konfiguriert, aber nicht für die Replikation bereit.

Keine.
: Der Knoten ist nicht für die Replikation konfiguriert.

Replikationsmodus

Gibt an, ob der Knoten als Quelle oder als Ziel der replizierten Daten konfiguriert ist. Ist dieses Feld leer, ist der Knoten nicht für die Replikation konfiguriert. Die folgenden Werte sind gültig:

Send
: Der Knoten ist als Quelle der Daten für die Replikation konfiguriert.

Receive
: Der Knoten ist als Ziel der Daten für die Replikation konfiguriert.

SyncSend
: Die Daten, die zu dem Knoten gehören, müssen mit den Knotendaten synchronisiert werden, die sich auf dem Zielreplikationsserver befinden. Die Synchronisation gilt nur für Knoten, deren Daten von einem Quellenreplikationsserver importiert und auf den Zielreplikationsserver importiert wurden. Die Synchronisation erfolgt während der Replikation.

SyncReceive
: Die Daten, die zu dem Knoten gehören, müssen mit den Knotendaten synchronisiert werden, die sich auf dem Quellenreplikationsserver befinden. Die Synchronisation gilt nur für Knoten, deren Daten von einem Quellenreplikationsserver importiert und auf den Zielreplikationsserver importiert wurden. Die Synchronisation erfolgt während der Replikation.

Keine.
: Der Knoten ist nicht für die Replikation konfiguriert.

Primärer Replikationsserver

Gibt den Quellenreplikationsserver für den Clientknoten an.

Replikationsregel für Sicherungsdaten

Replikationsregel für Archivierungsdaten

Replikationsregel für speicherverwaltete Daten

Die Replikationsregel, die für Sicherungsdaten, Archivierungsdaten und speicherverwaltete Daten gilt, die zu dem Knoten gehören. Die folgenden Werte sind gültig:

ALL_DATA
: Repliziert Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Die Daten werden mit normaler Priorität repliziert.

ACTIVE_DATA
: Repliziert aktive Sicherungsdaten. Die Daten werden mit normaler Priorität repliziert.

Achtung: Wenn Sie ACTIVE_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

ALL_DATA_HIGH_PRIORITY
: Repliziert Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Die Daten werden mit hoher Priorität repliziert.

ACTIVE_DATA_HIGH_PRIORITY

Diese Regel entspricht der Replikationsregel ACTIVE_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

DEFAULT
: Repliziert Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten gemäß der Domänenregel für den Datentyp.

NONE
: Es werden keine Daten repliziert. Lautet beispielsweise die Replikationsregel für Archivierungsdaten NONE, werden Archivierungsdaten, die zu dem Knoten gehören, nicht repliziert.

Zuletzt repliziert auf Server
: Gibt den Namen des Servers an, auf den der Knoten zuletzt repliziert wurde, und den Namen des Servers an, der während der Ausführung von Zurückschreibungsoperationen für die Übernahme des Clients verwendet wird.

Client-OS-Name
: Das Betriebssystem des Clients. Der Assistent für die Clientimplementierung verwendet diese Informationen zum Implementieren eines Pakets auf dem Client. Dieses Feld wird nur für IBM Spectrum Protect-Clients mit Version 6.2.0.0 und höher aufgelistet.

Clientprozessorarchitektur
: Die Architektur des Clients. Der Assistent für die Clientimplementierung verwendet diesen Wert, um das Paket zu bestimmen, das beim Aktualisieren des Clients implementiert werden soll. Dieses Feld wird nur für IBM Spectrum Protect-Clients mit Version 6.2.0.0 und höher aufgelistet.

Installierte Clientprodukte
: Die Produkte, die sich auf dem Knoten befinden. Die folgenden Produkte können aufgelistet werden:

- BA (Client für Sichern/Archivieren)
- VE (Virtual Environments)
- FCM (FlashCopy Manager)

Clientzielversion
: Die Version des Clients, die zu einem Zeitpunkt installiert wird, der mit dem Befehl DEFINE SCHEDULE oder UPDATE SCHEDULE geplant wird. Dieses Feld wird nur für IBM Spectrum Protect-Clients mit Version 6.2.0.0 und höher aufgelistet.

Authentifizierung
: Gibt die Kennwortauthentifizierungsmethode an: LOCAL, LDAP oder LDAP (künftig).

Authentifizierungsziel	**Authentifizierungsmethode**
IBM Spectrum Protect-Server	LOCAL
LDAP-Verzeichnisserver	LDAP
Dieser Knoten ist für die Authentifizierung mit einem LDAP-Verzeichnisserver konfiguriert, aber der Knoten hat sich noch nicht authentifiziert.	LDAP (künftig)

SSL erforderlich (veraltet)

Gibt an, ob die Sicherheitseinstellung für den Knoten das Protokoll Secure Sockets Layer (SSL) erfordert. Die gültigen Werte sind YES, NO oder Default. Sie müssen über die Berechtigung auf Systemebene verfügen, um die Einstellung von SSLREQUIRED für den Knoten zu aktualisieren. Dieses Feld wird nicht mehr verwendet.

Sitzungssicherheit
: Gibt die Stufe der Sitzungssicherheit an, die für den Knoten durchgesetzt wird. Die gültigen Werte sind STRICT und TRANSITIONAL.

Transportmethode
: Gibt die Transportmethode an, die zuletzt für den angegebenen Knoten verwendet wurde. Die gültigen Werte sind TLS 1.2, TLS 1.1 und NONE. Ein Fragezeichen (?) wird angezeigt, bis eine erfolgreiche Authentifizierung ausgeführt wird.

Große Objekte aufteilen
: Gibt an, ob große Objekte, die von diesem Knoten gespeichert werden, automatisch vom Server in kleinere Teile aufgeteilt werden, um die Serververarbeitung zu optimieren. 'Yes' gibt an, dass der Server große Objekte (über 10 GB) in kleinere Teile aufteilt, wenn sie von einem Clientknoten gespeichert werden. 'No' gibt an, dass dieser Prozess übergangen wird. Der Standardwert ist 'Yes'.

Typ für Gefährdung

Gibt den Auswertungstyp für Gefährdung an. Die gültigen Werte sind 'Standard', 'Übergangen' oder 'Angepasst'. 'Standard' gibt an, dass der Knoten mit demselben Intervall ausgewertet wird, das für die Knotenklassifizierung mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde. 'Übergangen' gibt an, dass der Gefährdungsstatus für den Knoten nicht vom Statusmonitor ausgewertet wird. 'Angepasst' gibt an, dass der Knoten mit dem Intervall ausgewertet wird, das mit dem Befehl SET NODEATRISKINTERVAL angegeben wurde, und nicht mit dem Intervall, das mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde.

Gefährdungsintervall
: Gibt die Anzahl der Stunden zwischen zwei Clientsicherungsaktivitäten oder zwei Replikationsaktivitäten an, nach denen der Statusmonitor angibt, dass die Aktivität gefährdet ist. Dieses Feld enthält nur dann einen Wert, wenn das Feld `Typ für Gefährdung` den Wert `Angepasst` enthält.

Dienstprogramm-URL
: Gibt die Adresse der IBM Spectrum Protect-Clientverwaltungsservices an, die auf dem Clientsystem konfiguriert sind. Diese URL wird vom Operations Center verwendet, um auf Clientprotokolldateien zuzugreifen, sodass Sie im Operations Center Clientprobleme über Fernzugriff diagnostizieren können.

Replikationswiederherstellung beschädigter Dateien
: Gibt an, ob beschädigte Dateien für diesen Knoten von einem Zielreplikationsserver wiederhergestellt werden können.

Stillgelegt
: Gibt an, ob der Clientknoten stillgelegt ist. Die folgenden Werte sind gültig:

  YES
  : Gibt an, dass der Knoten stillgelegt ist.

  Nullwert
  : Gibt an, dass der Knoten nicht stillgelegt ist.

  PENDING
  : Gibt an, dass der Knoten gerade stillgelegt wird oder der Stilllegungsprozess fehlgeschlagen ist.

  Tipp: Wenn Sie den Status eines anstehenden Stilllegungsprozesses bestimmen möchten, führen Sie die Anweisungen in Clientknoten stilllegen aus.

Datum der Stilllegung
: Gibt das Datum an, an dem der Clientknoten stillgelegt wurde.

Beispiel: Informationen zu Knotenrollen anzeigen

Die Beispielausgabe ist nur ein Teil der Gesamtanzeige.

```
query node alvin f=d
```

```
                              Proxyknotenagent:
                                 Knotengruppen:
                                E-Mail-Adresse:
                                                        Deduplizierung: ServerOnly
      Benutzer, die Sicherung ausführen dürfen: All
                                       Rolle: Server
                           Rollenüberschreibung: UseReported
                            Prozessorhersteller: ORACLE
                                 Prozessormarke: UltraSPARC-T2
                                   Prozessortyp: 4
                               Prozessormodell:
                             Anzahl Prozessoren: 1
                                     Hypervisor:
                                  API-Anwendung: NO
                          Fehler bei der Suche: NO
                                    MAC-Adresse:
```

Feldbeschreibungen

Rolle
: Die vom Client zurückgemeldete Prozessorrolle.

Rollenüberschreibung
: Der mit dem Befehl UPDATE NODE angegebene Überschreibungswert für 'Rolle'.

Prozessorhersteller
: Der vom Client zurückgemeldete Prozessorhersteller.

Prozessormarke
: Die vom Client zurückgemeldete Prozessormarke.

Prozessortyp
: Der vom Client zurückgemeldete Prozessortyp. Dieser Wert gibt die Anzahl der Prozessorkerne an, die für die PVU-Berechnung verwendet werden.

Prozessormodell
: Das vom Client zurückgemeldete Prozessormodell.

Anzahl Prozessoren
: Die vom Client zurückgemeldete Anzahl Prozessoren.

Hypervisor

Der vom Client zurückgemeldete Hypervisor.

API-Anwendung
: Der Clientanzeiger, der angibt, dass der Client eine API-Anwendung ist.

Fehler bei der Suche
: Gibt an, ob die letzte Suche nach Prozessorinformationen möglicherweise fehlerhaft ist und untersucht werden muss.

MAC-Adresse
: Die vom Client zurückgemeldete MAC-Adresse.

Beispiel: Alle Knoten anzeigen, die sich mit dem IBM Spectrum Protect-Server authentifizieren

Sollen alle Knoten angezeigt werden, die sich lokal authentifizieren, geben Sie den folgenden Befehl an:

```
query node * authentication=local
```

```
Knotenname  Plattform         Name der        Tage seit     Tage seit    Gesperrt?
                              Maßnahmen-      letz. Zugr.   Kennwort-
                              domäne                        vergabe
_____________________________________________________________________
NODE1             WinNT       STANDARD           3             3          No
LOCAL             (?)         STANDARD           7             7          No
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY NODE

Befehl	Beschreibung
LOCK NODE	Verhindert, dass ein Client auf den Server zugreift.
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.
QUERY REPLNODE	Zeigt Informationen zum Replikationsstatus eines Clientknotens an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
REMOVE REPLNODE	Entfernt einen Knoten aus der Replikation.
RENAME NODE	Ändert den Namen eines Clientknotens.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
RESET PASSEXP	Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.
SET INVALIDPWLIMIT	Definiert die Anzahl ungültiger Anmeldeversuche, die zulässig sind, bevor ein Knoten gesperrt wird.
SET MINPWLENGTH	Legt die Mindestlänge für Clientkennwörter fest.
SET PASSEXP	Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.
UNLOCK NODE	Ermöglicht einem gesperrten Benutzer in einer bestimmten Maßnahmendomäne wieder den Zugriff auf den Server.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

QUERY NODEDATA (Clientdaten auf Datenträgern abfragen)

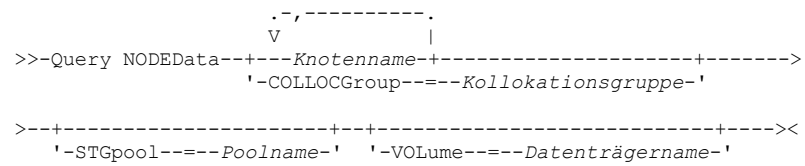
Verwenden Sie diesen Befehl, um Informationen zu den Daten für einen oder mehrere Knoten in einem Speicherpool mit sequenziellem Zugriff anzuzeigen. QUERY NODEDATA zeigt den Namen des Datenträgers, auf den die Daten eines Knotens geschrieben sind, und den Speicherbereich, der von den Daten auf diesem Datenträger belegt wird. Diese Informationen sind nützlich, wenn bestimmt wird, wie Knoten in zusammengefasste Speicherpools gruppiert werden können.

Berechtigungsklasse

Einschränkung: Sie können diesen Befehl nicht verwenden, um Informationen für Containerspeicherpools anzuzeigen.

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Knotenname
: Gibt den Namen des Clientknotens an, für den Daten lokalisiert werden sollen. Sie können einen oder mehrere Namen angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können auch Platzhalterzeichen verwenden, um mehrere Namen anzugeben. Sie müssen entweder einen Knotennamen oder den Namen einer Kollokationsgruppe, aber nicht beide Namen angeben.

COLLOCGroup
: Gibt den Namen der Kollokationsgruppe an, für die Daten lokalisiert werden sollen. Sie müssen entweder einen Knotennamen oder den Namen einer Kollokationsgruppe, aber nicht beide Namen angeben.
Wichtig: Wenn der Speicherbereich, der für die Ausführung der Abfrage bezüglich einer Kollokationsgruppe erforderlich ist, den SQL-Puffergrenzwert überschreitet, kann der Befehl QUERY NODEDATA fehlschlagen. Schlägt der Befehl aus diesem Grund fehl, geben Sie den Befehl QUERY COLLOCGROUP aus, um eine Liste der Knoten in der Gruppe anzuzeigen. Geben Sie dann den Befehl QUERY NODEDATA für jeden Knoten in der Gruppe aus.

STGpool
: Gibt den Namen des sequenziellen Speicherpools an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Es können Platzhalterzeichen verwendet werden, um die Namen anzugeben. Stimmt ein Platzhalterzeichen mit dem Namen eines Plattenspeicherpools überein, wird der Name des Plattenspeicherpools ignoriert. Wird kein Wert für diesen Parameter angegeben, werden alle sequenziellen Speicherpools abgefragt.

VOLume
: Gibt den Datenträger an, der die Daten enthält. Dieser Parameter ist wahlfrei. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben. Wird kein Wert für diesen Parameter angegeben, werden alle Datenträger in dem Speicherpool abgefragt.

Platzhalterzeichen verwenden, um Knotendaten für einen Speicherpool mit sequenziellem Zugriff anzuzeigen

Informationen zur Position anzeigen, an der Knotendaten in einem sequenziellen Speicherpool gespeichert sind. Verwenden Sie ein Platzhalterzeichen, um Knotennamen anzugeben. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query nodedata e*
```

```
   Knotenname  Datenträgername                 Speicherpool-  Physischer
                                               name           Speicher
                                                              belegt
                                                              (MB)
   ---------   ----------------------------   ------------   --------
      EDU_J2      E:\tsm\server\00000117.BFS      EDU512         0.01
      EDU_J2      E:\tsm\server\00000122.BFS      EDU319         0.01
      EDU_J3      E:\tsm\server\00000116.BFS      EDU512         0.01
      EDU_J3      E:\tsm\server\00000120.BFS      EDU319         0.01
      EDU_J7      E:\tsm\server\00000118.BFS      EDU512         0.04
      EDU_J7      E:\tsm\server\00000123.BFS      EDU319         0.04
      EDU_JJ1     E:\tsm\server\00000116.BFS      EDU512         0.01
      EDU_JJ1     E:\tsm\server\00000121.BFS      EDU512         0.01
```

Informationen zu Knotendaten für eine bestimmte Kollokationsgruppe anzeigen

Informationen zur Position von Knotendaten in einem sequenziellen Speicherpool für eine bestimmte Kollokationsgruppe anzeigen. In diesem Beispiel sind die Knoten EDU_J3 und EDU_JJ1 die einzigen Knoten, die zur Kollokationsgruppe grp1 gehören und Daten in einem Speicherpool mit sequenziellem Zugriff haben.

```
query nodedata collocgroup=grp1
```

```
   Knotenname  Datenträgername                 Speicherpool-  Physischer
                                               name           Speicher
                                                              belegt
                                                              (MB)
   ---------   ----------------------------   ------------   --------
      EDU_J3      E:\tsm\server\00000116.BFS      EDU512         0.01
      EDU_J3      E:\tsm\server\00000120.BFS      EDU319         0.01
```

```
EDU_JJ1      E:\tsm\server\00000116.BFS       EDU512          0.01
EDU_JJ1      E:\tsm\server\00000121.BFS       EDU512          0.01
```

Wenn Sie eine Dateibereichskollokationsgruppe angeben, werden nur die Datenträger der Dateibereiche angezeigt, die zu der Kollokationsgruppe gehören. Wenn Sie eine Dateibereichskollokationsgruppe und einen Datenträger angeben, werden die Dateibereiche innerhalb der Kollokationsgruppe, die sich auch auf dem angegebenen Datenträger befinden, angezeigt.

Feldbeschreibungen

Knotenname
: Gibt den Namen des Knotens an.

Datenträgername
: Gibt den Namen des Datenträgers an, der die Knotendaten enthält.

Speicherpoolname
: Gibt den Namen des Speicherpools an, in dem sich der Datenträger befindet.

Physischer Speicher belegt (MB)
: Gibt den physischen Speicherbereich an, der von den Knotendaten belegt wird. Der physische Speicherbereich schließt leeren Speicherbereich innerhalb von Aggregaten ein, aus denen Dateien möglicherweise gelöscht oder als verfallen gekennzeichnet wurden.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY NODEDATA

Befehl	Beschreibung
DEFINE COLLOCGROUP	Definiert eine Kollokationsgruppe.
DEFINE COLLOCMEMBER	Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE COLLOCGROUP	Löscht eine Kollokationsgruppe.
DELETE COLLOCMEMBER	Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.
MOVE NODEDATA	Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
UPDATE COLLOCGROUP	Aktualisiert die Beschreibung einer Kollokationsgruppe.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

QUERY NODEGROUP (Knotengruppe abfragen)

Verwenden Sie diesen Befehl, um die Knotengruppen anzuzeigen, die auf dem Server definiert sind.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                    .-*-----------.
>>-Query NODEGroup--+-------------+----------------------------->
                    '-Gruppenname-'

   .-Format--=--Standard-----.
>--+-----------------------+---------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Gruppenname
: Gibt den Namen der Knotengruppe an, die angezeigt werden soll. Sollen mehrere Namen angegeben werden, ein Platzhalterzeichen verwenden. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Knotengruppen angezeigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.Um die Knoten in der Knotengruppe anzuzeigen, müssen Sie FORMAT=DETAILED angeben.

Beispiel: Knotengruppen auf dem Server auflisten

Die Knotengruppen anzeigen, die auf dem Server definiert sind. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query nodegroup

Name der Knotengruppe          Beschreibung der Knotengruppe
-------------------------     ------------------------------
DEPT_ED                        Ausbildungsabteilung
GROUP1                         Clientknoten mit geringer Kap.
```

Beispiel: Ausführliche Informationen zu Knotengruppen anzeigen

Vollständige Informationen zu allen Knotengruppen anzeigen und bestimmen, welche Clientknoten zu welchen Knotengruppen gehören. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query nodegroup format=detailed

               Name der Knotengruppe: DEPT_ED
                 Beschreibung der Knotengruppe: Ausbildungsabteilung
   Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
         Datum/Zeit der letzten Aktualisierung: 04/21/2006 10:59:03
                       Knoten in Knotengruppe: EDU_1 EDU_7

                        Name der Knotengruppe: GROUP1
                  Beschreibung der Knotengruppe: Clientknoten mit geringer Kap.
   Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
         Datum/Zeit der letzten Aktualisierung: 04/21/2006 10:59:16
                       Knoten in Knotengruppe: CHESTER REX NOAH JARED
```

Feldbeschreibungen

Name der Knotengruppe
: Der Name der Knotengruppe.

Beschreibung der Knotengruppe
: Die Beschreibung der Knotengruppe.

Letzte Aktualisierung durch (Administrator)
: Der Name des Administrators, der die Knotengruppe definiert oder zuletzt aktualisiert hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der ein Administrator die Knotengruppe definiert oder zuletzt aktualisiert hat.

Knoten in Knotengruppe
: Die Clientknoten in der Knotengruppe.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY NODEGROUP

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUP	Löscht eine Knotengruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.

Befehl	Beschreibung
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

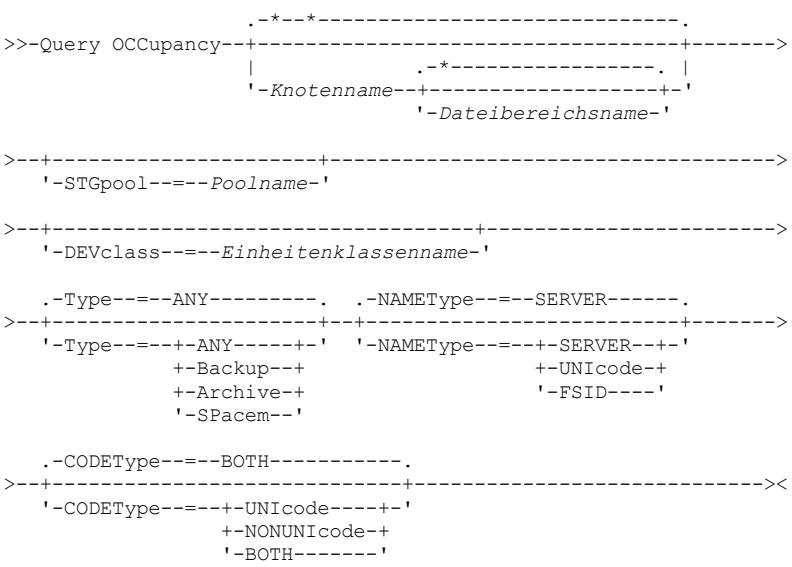
QUERY OCCUPANCY (Clientdateibereiche in Speicherpools abfragen)

Mit diesem Befehl kann angezeigt werden, wo Clientdateibereiche gespeichert sind und wieviel Speicherbereich sie belegen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Knotenname
: Gibt den Knoten an, der Eigner der zu suchenden Dateibereiche ist. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Knoten abgefragt.

Dateibereichsname
: Gibt den zu suchenden Dateibereich an. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Dateibereiche abgefragt. Ein Knotenname muß angegeben werden, wenn ein Dateibereichsname angegeben wird.

  Ein Server, der über Clients mit Unicode-Unterstützung verfügt, muss möglicherweise den Dateibereichsnamen, den Sie eingeben, konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich unter dem Parameter NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

STGpool
: Gibt den Speicherpool an, der nach Dateien aus dem angegebenen Dateibereich abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherpools abgefragt.

DEVclass
: Gibt die Einheitenklasse an, die den Einheiten zugeordnet ist, auf denen die Dateibereiche gespeichert sind. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden Speicherpools abgefragt, die einer beliebigen Einheitenklasse zugeordnet sind.

Type
: Gibt die Dateitypen an, die in den Dateibereichen abgefragt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Gültige Werte:

ANY
: Gibt an, dass alle Typen von Dateien abgefragt werden: Sicherungsversionen von Dateien, archivierte Kopien von Dateien und Dateien, die von IBM Spectrum Protect for Space Management-Clients umgelagert werden.

Backup
: Gibt an, daß Sicherungsdateien abgefragt werden.

Archive
: Gibt an, daß Archivierungsdateien abgefragt werden.

SPacem
: Gibt an, dass speicherverwaltete Dateien (Dateien, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden) abgefragt werden.

NAMEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unicode-Unterstützung verfügt. Ein Client für Sichern/Archivieren mit Unicode-Unterstützung ist nur für Windows, Macintosh OS 9, Macintosh OS X und NetWare verfügbar. Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen angeben.

  Der Standardwert lautet SERVER. Gültige Werte:

  SERVER
  : Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

  UNIcode
  : Der Server konvertiert die Dateibereichsnamen aus der Server-Codepage in die Codepage UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in den Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

  FSID
  : Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

CODEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben oder wenn Sie keinen Dateibereichsnamen angeben.

  Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass die Dateibereiche unabhängig von der Art der Zeichenumsetztabelle eingeschlossen werden. Gültige Werte:

  UNIcode
  : Nur Dateibereiche einschließen, die Unicode-fähig sind.

  NONUNIcode
  : Nur Dateibereiche einschließen, die nicht Unicode-fähig sind.

  BOTH
  : Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

Beispiel: Dateibereiche anzeigen, die einem bestimmten Knoten zugeordnet sind

Informationen zum Speicherstandort aller Dateibereiche anzeigen, die dem Knoten DAISY zugeordnet sind. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query occupancy daisy
```

```
Knoten-  Typ  Dateiber.- FSID   Speicher- Anzahl   Physischer Logischer
name          Name              pool-     der      Speicher   Speicher
                                name      Dateien  belegt     belegt
                                                   (MB)       (MB)
------- ----  ---------- -----  --------  -------- -------    --------
 DAISY   Bkup  DRIVED       1    COPYFILE     38     0,45       0,42
```

Beispiel: Dateibereiche anzeigen, die einem bestimmten Knoten mit dem Dateityp 'backup' zugeordnet sind

Informationen zu den Dateibereichen anzeigen, die zum Knoten WAYNE gehören und den Dateityp 'backup' haben. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query occupancy wayne type=backup
```

```
Knoten-  Typ  Dateiber.- FSID   Speicher- Anzahl   Physischer Logischer
 name         Name              pool-     der      Speicher   Speicher
                                name      Dateien  belegt     belegt
                                                   (MB)       (MB)
 ------ ----- --------- -----  ---------- ------- ---------  --------
  WAYNE  Bkup  DWG1        1    BACKUPPOOL1 2.330   53,19      50,01
  WAYNE  Bkup  OS2C        2    BACKUPPOOL1 1.554   32,00      31,30
```

Feldbeschreibungen

Knotenname
: Der Knoten, der Eigner des Dateibereichs ist.Wurde der Knoten zuvor gelöscht, wird der Knotenname DELETED angezeigt.

Type
: Der Datentyp. Gültige Werte:

  Arch
  : Daten, die archiviert wurden.

  Bkup
  : Daten, die gesichert wurden.

  SpMg
  : Daten, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Dateibereichsname
: Der Name des Dateibereichs, der zu dem Knoten gehört.

  Wurde der Dateibereich zuvor gelöscht, wird der Dateibereichsname DELETED angezeigt.

  Dateibereichsnamen können eine andere Zeichenumsetztabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

  Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

Speicherpoolname
: Der Speicherpool, in dem sich der Dateibereich befindet.

Anzahl Dateien
: Die Anzahl der logischen Dateien, die zum Dateibereich gehören und in diesem Speicherpool gespeichert sind.Wird eine Datei mit mehr als 10 GB gespeichert, teilt der Server die Datei in 10-GB-Fragmente auf. Die Anzahl der Fragmente ist ebenfalls in diesem Wert für die Berechnung der Belegung enthalten.

Belegung des physischen Speichers (MB)
: Der physische Speicherbereich, der vom Dateibereich belegt wird. Der physische Speicherbereich schließt leeren Speicherbereich innerhalb von Aggregaten ein, aus denen Dateien möglicherweise gelöscht oder als verfallen gekennzeichnet wurden. Bei diesem Wert ist 1 MB = 1048576 Byte.
  Tipp: Dieses Feld zeigt keinen Wert für Speicherpools, die für die Deduplizierung von Daten definiert sind. Wird die Deduplizierung von Daten für einen Speicherpool inaktiviert, wird ein Wert für die physische Belegung erst angezeigt, wenn sich keine deduplizierten Dateien mehr in dem Speicherpool befinden.

Belegung des logischen Speichers (MB)
: Der Speicherbereich, der von logischen Dateien in dem Dateibereich belegt wird. Der logische Speicherbereich ist der Speicherbereich, der tatsächlich zum Speichern von Dateien verwendet wird, ausschließlich des leeren Speicherbereichs innerhalb von Aggregaten. Bei diesem Wert ist 1 MB = 1048576 Byte.

FSID
: Die Dateibereichs-ID (FSID) des Dateibereichs. Der Server ordnet eine eindeutige FSID zu, wenn ein Dateibereich zum ersten Mal auf dem Server gespeichert wird.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY OCCUPANCY

Befehl	Beschreibung
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.

QUERY OPTION (Serveroptionen abfragen)

Mit diesem Befehl können Informationen zu Serveroptionen angezeigt werden.

Die Serveroptionen können durch Editieren der Serveroptionsdatei oder mit dem Befehl SETOPT geändert werden. Wenn die Serveroptionsdatei editiert wird, muss der Server erneut gestartet werden, damit die Änderungen wirksam werden. Alle mit dem Befehl SETOPT vorgenommenen Änderungen werden sofort wirksam.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                .-*-----------.
>>-Query OPTion--+-------------+-------------------------------><
                '-Optionsname-'
```

Parameter

Optionsname
: Gibt den Namen einer Option in der Serveroptionsdatei an. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden.Alle übereinstimmenden Serveroptionen werden angezeigt. Wird dieser Parameter nicht angegeben, werden Informationen für alle Optionen angezeigt.

Beispiel: Alle Serveroptionen anzeigen

Allgemeine Informationen zu allen Serveroptionen anzeigen. Die Ausgabe listet alle Optionen mit ihren angegebenen Werten auf.

```
query option
```

Beispiel: Optionseinstellungen unter Verwendung eines Platzhalterzeichens anzeigen

Die Optionseinstellungen für alle Optionen anzeigen, die mit L beginnen.

```
query option l*

Serveroption         Optionswert
-----------------     --------------------
Language              AMENG
```

Beispiel: LDAP-Verzeichnisserver anzeigen

Die Einstellungen für alle LDAP-Verzeichnisserver anzeigen.

```
query option ldapurl

Serveroption         Optionswert
-----------------     --------------------
LDAP URL               ldap:\\tophoy.tucson.com\cn=tsmdata
LDAP URL               ldap:\\krypton.ibm.com\ou=tsmdata,dc=ibm,dc=com
```

Feldbeschreibungen

Serveroption
: Gibt den Namen der Option in der Serveroptionsdatei an.

Optionswert
: Gibt den Wert der Option in der Serveroptionsdatei an.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY OPTION

Befehl	Beschreibung
SETOPT	Aktualisiert eine Serveroption, ohne den Server zu stoppen und erneut zu starten.

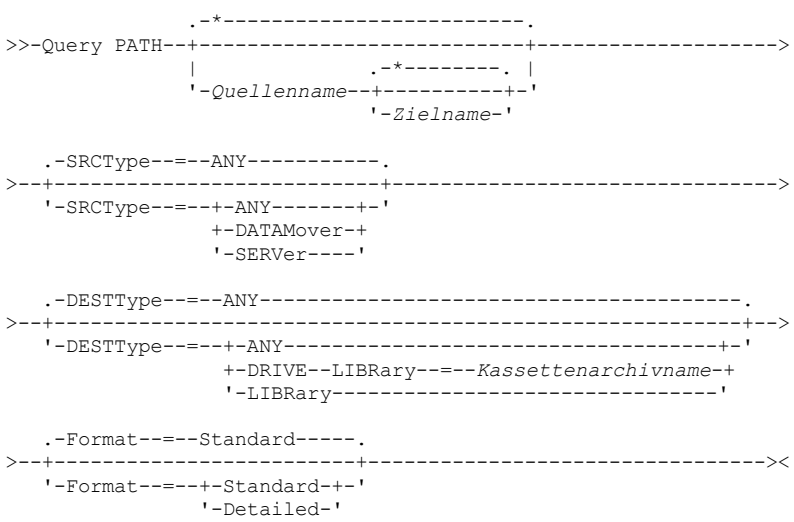
QUERY PATH (Pfaddefinition anzeigen)

Verwenden Sie diesen Befehl, um den Pfad zwischen einer Quelle und einem Ziel anzuzeigen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Quellenname
: Gibt den Namen einer Quelle an, für die Pfade angezeigt werden sollen. Dieser Parameter ist wahlfrei. Sie können Platzhalterzeichen angeben. Standardmäßig werden Pfade für alle Quellen angezeigt.

  Eine Quelle ist eine Einheit zum Versetzen von Daten, ein Server oder ein Speicheragent.

Zielname
: Gibt den Namen eines Ziels an, für das Pfade angezeigt werden sollen. Dieser Parameter ist wahlfrei. Sie können Platzhalterzeichen angeben. Standardmäßig werden Pfade für alle Ziele angezeigt.

SRCType
: Gibt den Typ der Quelle an. Dieser Parameter ist wahlfrei. Standardmäßig werden Pfade für alle Quellentypen angezeigt. Gültige Werte:

  ANY
  : Gibt an, dass Pfade mit einem beliebigen Quellentyp angezeigt werden sollen.

  DATAMover
  : Gibt an, dass nur Pfade mit dem Quellentyp DATAMOVER angezeigt werden sollen.

  SERVer
  : Gibt an, dass nur Pfade mit dem Quellentyp SERVER angezeigt werden sollen. (Eine Quelle, die den Quellentyp SERVER hat, ist ein Speicheragent.)

DESTType
: Gibt den Typ des Ziels an. Dieser Parameter ist wahlfrei. Standardmäßig werden Pfade für alle Zieltypen angezeigt. Gültige Werte:

  ANY
  : Gibt an, dass Pfade mit einem beliebigen Zieltyp angezeigt werden sollen.

  DRive
  : Gibt an, dass nur Pfade mit dem Zieltyp DRIVE angezeigt werden sollen. Ist der Zieltyp ein Laufwerk, müssen Sie den Kassettenarchivnamen angeben. Durch die Eingabe eines Namens in dem Parameter LIBRARY können Sie genauer spezifizieren, welche Pfade angezeigt werden.

  LIBRary
  : Gibt an, dass nur Pfade mit dem Zieltyp LIBRARY angezeigt werden.

LIBRary
: Gibt den Namen des Kassettenarchivs an, zu dem das Laufwerk gehört. Dieser Parameter ist erforderlich, wenn der Zieltyp ein Laufwerk ist (DESTTYPE=DRIVE).

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed

Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Übersichtsdaten zu Pfaden anzeigen

Informationen zu Pfaden für die Quelle `NETAPP1` anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query path netapp1
```

```
Quellenname  Quellentyp   Zielname          Zieltyp           Online
-----------  -----------  ----------------  ----------------  ------
NETAPP1      DATAMOVER    DRIVE1            DRIVE             Yes
NETAPP1      DATAMOVER    NASLIB            LIBRARY           Yes
```

Beispiel: Ausführliche Informationen zu Pfaden anzeigen

Ausführliche Informationen zu Pfaden für die Quelle `NETAPP1` anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query path netapp1 format=detailed
```

 Linux-Betriebssysteme

```
                                     Quellenname: NETAPP1
                                      Quellentyp: DATAMOVER
                                        Zielname: NASLIB
                                         Zieltyp: LIBRARY
                                  Kassettenarchiv:
                                         Einheit: /dev/tsmscsi/mc0
                                     Verzeichnis:
                                          Online: Yes
   Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
               Datum/Zeit der letzten Aktualisierung: 06/21/2002 20:52:56

                                     Quellenname: NETAPP1
                                      Quellentyp: DATAMOVER
                                        Zielname: DRIVE1
                                         Zieltyp: DRIVE
                                  Kassettenarchiv: NASLIB
                                         Einheit: rst01
                                     Verzeichnis:
                                          Online: Yes
   Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
               Datum/Zeit der letzten Aktualisierung: 06/21/2002 20:55:23
```

 AIX-Betriebssysteme  Windows-Betriebssysteme

```
                                     Quellenname: NETAPP1
                                      Quellentyp: DATAMOVER
                                        Zielname: NASLIB
                                         Zieltyp: LIBRARY
                                  Kassettenarchiv:
                                         Einheit: mc0
                                     Verzeichnis:
                                          Online: Yes
   Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
               Datum/Zeit der letzten Aktualisierung: 06/21/2001 20:52:56

                                     Quellenname: NETAPP1
                                      Quellentyp: DATAMOVER
                                        Zielname: DRIVE1
                                         Zieltyp: DRIVE
                                  Kassettenarchiv: NASLIB
                                         Einheit: rst01
                                     Verzeichnis:
                                          Online: Yes
   Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
               Datum/Zeit der letzten Aktualisierung: 06/21/2001 20:55:23
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

Beispiel: Ausführliche Informationen zu Pfaden für einen z/OS Media-Server anzeigen

Ausführliche Informationen zu einem Pfad für einen z/OS Media-Server anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query path format=detailed
```

```
                  Quellenname: SERVER1
                                      Quellentyp: SERVER
                                        Zielname: ZOSMEDIA
                                         Zieltyp: LIBRARY
                                  Kassettenarchiv:
```

```
                                  Knotenname:
                                     Einheit:
                               Externer Manager:
                              z/OS Media-Server: MEDSERV1
                             Übertragungsmethode:
                                             LUN:
                                       Initiator: 0
                                     Verzeichnis:
                                          Online: Yes
Letzte Aktualisierung durch (Administrator): ADMIN
      Datum/Zeit der letzten Aktualisierung: 06/08/2011 15:33:39
```

Feldbeschreibungen

Quellenname
: Der Name der Quelle.

Zielname
: Der Name des Ziels.

Quellentyp
: Der Typ der Quelle.

Zieltyp
: Der Typ des Ziels.

Kassettenarchiv
: Der Name des Kassettenarchivs, das das Laufwerk als Ziel enthält.

  Dieses Feld ist leer, wenn der Zieltyp ein Kassettenarchiv ist. Der Kassettenarchivname befindet sich im Feld für den Zielnamen, wenn das Ziel ein Kassettenarchiv ist.

Knotenname
: Der Name der Einheit, die das Ziel ist.

Einheit
: Der Name der Einheit, die das Ziel ist.

Externer Manager
: Der Name des externen Managers.

z/OS Media-Server
: Der Name des z/OS Media-Servers.

Übertragungsmethode
: Gibt den Typ der Übertragungsmethode an.

LUN
: Gibt den Namen der logischen Einheit an, über den von der Quelle auf die Platte zugegriffen werden kann.

Initiator
: Gibt den Initiator der Übertragung an.

Verzeichnis
: Gibt die Verzeichnisposition einer Datei in der Quelle an.

Online
: Gibt an, ob der Pfad online und für die Verwendung verfügbar ist.

Letzte Aktualisierung durch (Administrator)
: Die ID des Administrators, der die letzte Aktualisierung ausgeführt hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit der letzten Aktualisierung.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY PATH

Befehl	Beschreibung
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.

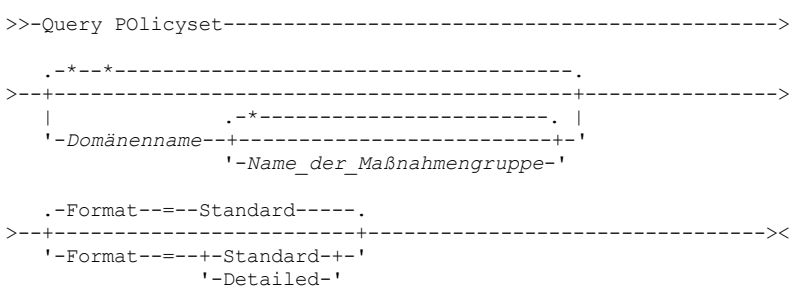
QUERY POLICYSET (Maßnahmengruppe abfragen)

Mit diesem Befehl können Informationen über eine oder mehrere Maßnahmengruppen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Domänenname
: Gibt die Maßnahmendomäne an, die der Maßnahmengruppe zugeordnet ist, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Maßnahmendomänen abgefragt. Dieser Parameter muß angegeben werden, wenn eine explizit benannte Maßnahmengruppe abgefragt wird.

Name_der_Maßnahmengruppe
: Gibt die Maßnahmengruppe an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.Wird nicht ACTIVE oder der Name einer Maßnahmengruppe angegeben, werden alle Maßnahmengruppen abgefragt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Die Maßnahmengruppen für alle Maßnahmendomänen auflisten

Alle Maßnahmengruppen für alle Maßnahmendomänen abfragen. Die Ausgabe soll im Standardformat erstellt werden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query policyset

Name der      Name der      Standard-     Beschreibung
Maßnah-       Maßnah-       verwal-
mendomäne     mengruppe     tungs-
                            klasse
---------     ---------     ---------     ------------------------
EMPLOYEE-     ACTIVE        ACTIVEFI-     Personnel Department
  _RECORDS                  LES
EMPLOYEE-     HOLIDAY       ACTIVEFI-     Personnel Department
  _RECORDS                  LES
EMPLOYEE-     VACATION      ACTIVEFI-     Personnel Department
  _RECORDS                  LES
PROG1         SUMMER                      Programming Group
                                           Policies
PROG2         SUMMER                      Programming Group
                                           Policies
STANDARD      ACTIVE        STANDARD      Installed default policy
                                           set.
STANDARD      STANDARD      STANDARD      Installed default policy
                                           set.
```

Beispiel: Ausführliche Informationen zu einer bestimmten Maßnahmengruppe anzeigen

Die Maßnahmengruppe VACATION abfragen, die sich in der Maßnahmendomäne EMPLOYEE_RECORDS befindet. Die Ausgabe soll im ausführlichen Format erstellt werden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query policyset employee_records vacation
format=detailed

                    Name der Maßnahmendomäne: EMPLOYEE_RECORDS
                Name der Maßnahmengruppe: VACATION
                    Standardverwaltungsklasse: ACTIVEFILES
                                Beschreibung: Personnel Department
            Letzte Aktualisierung durch
                         (Administrator): $$CONFIG_MANAGER$$
```

```
Datum/Zeit der letzten Aktualisierung: 05/31/1998 13:15:50
                  Verwaltendes Profil: ADSM_INFO
                Änderungen anstehend: Yes
```

Feldbeschreibungen

Name der Maßnahmendomäne
: Der Name der Maßnahmendomäne.

Name der Maßnahmengruppe
: Der Name der Maßnahmengruppe.

Standardverwaltungsklasse
: Die Verwaltungsklasse, die der Maßnahmengruppe standardmäßig zugeordnet ist.

Beschreibung
: Die Beschreibung der Maßnahmengruppe.

Letzte Aktualisierung durch (Administrator)
: Der Name des Administrators oder Servers, der die Maßnahmengruppe zuletzt aktualisiert hat. Enthält dieses Feld $$CONFIG_MANAGER$$, ist die Maßnahmengruppe einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der die Maßnahmengruppe definiert oder zuletzt aktualisiert wurde.

Verwaltendes Profil
: Das Profil oder die Profile, die die Domäne verwalten, zu der diese Maßnahmengruppe gehört.

Änderungen anstehend
: Angabe, ob Änderungen vorgenommen, aber nicht aktiviert werden. Sobald die Änderungen aktiviert werden, wird das Feld auf No zurückgesetzt.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY POLICYSET

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
COPY POLICYSET	Erstellt eine Kopie einer Maßnahmengruppe.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
DELETE POLICYSET	Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
UPDATE POLICYSET	Ändert die Beschreibung einer Maßnahmengruppe.
VALIDATE POLICYSET	Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert.

QUERY PROCESS (Serverprozesse abfragen)

Mit diesem Befehl können Informationen zu aktiven Hintergrundprozessen angezeigt werden.

Geben Sie den Befehl CANCEL PROCESS aus, um Hintergrundprozesse abzubrechen. Um ausführliche Informationen zu Knotenreplikationsprozessen anzuzeigen, geben Sie den Befehl QUERY REPLICATION aus.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query PRocess--+---------------+----------------------------->
                  '-Prozessnummer-'

>--+-----------------------------+----------------------------->
   '-DESCription--=--Zeichenfolge-'

>--+-------------------------+--------------------------------><
   '-STATus--=--Zeichenfolge-'
```

Parameter

Prozessnummer
: Gibt die Nummer des Hintergrundprozesses an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird keine Prozessnummer angegeben, werden Informationen zu allen Hintergrundprozessen angezeigt.

DESCription
: Gibt eine Textzeichenfolge an, nach der in der Liste der Beschreibungen von aktiven Prozessen gesucht werden soll. Die Zeichenfolge in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Sie können Text und ein Platzhalterzeichen verwenden, um diese Zeichenfolge anzugeben. Dieser Parameter ist wahlfrei.

STATus
: Gibt eine Textzeichenfolge an, nach der in der Liste der Status von aktiven Prozessen gesucht werden soll. Die Zeichenfolge in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Sie können Text und ein Platzhalterzeichen verwenden, um diese Zeichenfolge anzugeben. Dieser Parameter ist wahlfrei.

Beispiel: Einen einzelnen Hintergrundprozess abfragen

Informationen zu Hintergrundprozess 202 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query process 202
```

```
Prozess-  Prozess-             Prozess-
nummer    beschreibung         status
--------  -------------        ---------
     202  EXPORT SERVER         ANR0NNNI EXPORT-
                               ID MYEXPORTSERVER
                               ANR0648I Folgendes wurde
                               kopiert: 8 Domänen 2
                               Maßnahmengruppen, 10
                               Verwaltungsklassen, 4
                               Kopiengruppen, 1 Admi-
                               nistrator 746 Byte
                               (0 Fehler erkannt) Akt. Eingabe-
                               datenträger: C:\BUILD\540\
                               GA\BUILD\NT\I386\DEBUG\
                               -00000014.BFS,(6 Sekunden)
```

Beispiel: Alle Hintergrundprozesse abfragen

Informationen zu allen Hintergrundprozessen anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query process
```

```
Prozess-  Prozess-             Prozess-
nummer    beschreibung         status
--------  --------------       ---------
     304  IDENTIFY DUPLICATES  Speicherpool
                               FILEPOOL, Datenträger
                               /tsmpool2/00006664.
                               BFS, Verarbeitete Dateien:
                               2000, Doppelte Erweiterungen
                               gefunden: 344, Doppelte
                               Byte gefunden: 3.238.123,
                               Aktuelle physische Datei
                               (Byte): 2.626.676.296.
                               Status: Wird verarbeitet

     284  IDENTIFY DUPLICATES  Speicherpool
                               FILEPOOL, Datenträger
                               /tsmpool2/00006666.
                               BFS, Verarbeitete Dateien:
                               2000, Doppelte Erweiterungen
                               gefunden: 344, Doppelte
                               Byte gefunden: 3.238.123,
                               Aktuelle physische Datei
                               (Byte): Keine.
                               Status: Inaktiv

       4  Replicate Node       Replizieren von Knoten IRONMAN.
                               Abgeschlossene Dateibereiche: 0.
                                Identifizieren und Replizieren
                               von Dateibereichen: 1. Replizieren
                               von Dateibereichen: 0. Nicht gestartete
                               Dateibereiche: 3. Aktuelle Dateien:
                               11.920. Replizierte Dateien: 0 von
                               0. Aktualisierte Dateien: 0 von 0.
                               Gelöschte Dateien: 0 von 0. Repliziertes
                               Volumen: 11.482 KB von 11.482 KB.
                               Übertragenes Volumen: 11.482 KB.
```

```
                              Abgelaufene Zeit: 0 Tag(e), 0 Stunde(n),
                              1 Minute(n).

      37  Expiration          12 Knoten von insgesamt 30 Knoten verarbeitet,
                              411 Objekte geprüft,
                              411 Sicherungsobjekte,
                              0 Archivierungsobjekte,
                              0 DB-Sicherungsdatenträger,
                              0 Wiederherstellungsplandateien werden gelöscht;
                              Die Verarbeitung von 0 Objekten wurde wiederholt und
                              0 Fehler wurden gefunden.
```

Beispiel: Alle Hintergrundreplikationsprozesse abfragen

Informationen zu allen Hintergrundreplikationsprozessen anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query process desc="replicate node"

Prozess-  Prozess-            Prozess-
nummer    beschreibung        status
--------  --------------      ---------
       4  Replicate Node      Replizieren von Knoten IRONMAN.
                              Abgeschlossene Dateibereiche: 0.
                               Identifizieren und Replizieren
                              von Dateibereichen: 1. Replizieren
                              von Dateibereichen: 0. Nicht gestartete
                              Dateibereiche: 3. Aktuelle Dateien:
                              11.920. Replizierte Dateien: 0 von
                              0. Aktualisierte Dateien: 0 von 0.
                              Gelöschte Dateien: 0 von 0. Repliziertes
                              Volumen: 11.482 KB von 11.482 KB.
                              Übertragenes Volumen: 11.482 KB.
                              Abgelaufene Zeit: 0 Tag(e), 0 Stunde(n),
                                      1 Minute(n).
```

Beispiel: Alle Hintergrundreplikationsprozesse für einen bestimmten Knoten abfragen

Informationen zu allen Hintergrundreplikationsprozessen anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query process desc="replicate node" status=ironman

Prozess-  Prozess-            Prozess-
nummer    beschreibung        status
--------  --------------      ---------
       4  Replicate Node      Replizieren von Knoten IRONMAN.
                              Abgeschlossene Dateibereiche: 0.
                               Identifizieren und Replizieren
                              von Dateibereichen: 1. Replizieren
                              von Dateibereichen: 0. Nicht gestartete
                              Dateibereiche: 3. Aktuelle Dateien:
                              11.920. Replizierte Dateien: 0 von
                              0. Aktualisierte Dateien: 0 von 0.
                              Gelöschte Dateien: 0 von 0. Repliziertes
                              Volumen: 11.482 KB von 11.482 KB.
                              Übertragenes Volumen: 11.482 KB.
                              Abgelaufene Zeit: 0 Tag(e), 0 Stunde(n),
                                      1 Minute(n).
```

Beispiel: Prüfen, ob ein Replikationswiederherstellungsprozess eingeleitet wurde

Prüfen Sie nach dem Start eines Knotenreplikationsprozesses mit aktivierter Dateiwiederherstellung, ob der Zielreplikationsserver den Dateiwiederherstellungsprozess eingeleitet hat. Geben Sie den Befehl QUERY PROCESS auf dem Zielreplikationsserver aus. Beschreibungen der Felder befinden sich in Feldbeschreibungen.

```
query process

Prozess-    Prozess-             Prozess-
nummer      beschreibung         status
--------  ------------------   ------------------------------------
4           Replicate Node -     Replizieren von Knoten 3MAUTOIMPORT.
            Recovery            Abgeschlossene Dateibereiche: 87.
                                Identifizieren und Replizieren von
                                Dateibereichen: 0.
                                Replizieren von Dateibereichen: 6.
                                Nicht gestartete Dateibereiche: 0.
                                Aktuelle Dateien: 0.
                                Replizierte Dateien: 0 von 14.
                                Aktualisierte Dateien: 0 von 0.
                                Gelöschte Dateien: 0 von 0. Repliziertes
                                Volumen: 0 KB von 11.688 Byte. Übertragenes
```

```
                                    Volumen: 0 KB.
                                    Abgelaufene Zeit: 0 Tag(e), 0 Stunde(n), 1 Minute(n).
```

Beispiel: Prüfen, ob beschädigte Dateien während eines Replikationsprozesses wiederhergestellt werden

Prüfen Sie nach dem Start eines Knotenreplikationsprozesses mit aktivierter Dateiwiederherstellung, ob beschädigte Dateien wiederhergestellt werden. Geben Sie den Befehl QUERY PROCESS auf dem Quellenreplikationsserver aus. Beschreibungen der Felder befinden sich in Feldbeschreibungen.

```
query process

Prozess-    Prozess-             Prozess-
nummer      beschreibung         status
-------   -------------------   ------------------------
6           Replicate Node       Wiederherstellen beschädigter Dateien
          ( As Secondary         von Server SERVER2,
           Recovery )            Prozess 4, Anzahl aktiver Sitzungen 10.
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Beispiel: Prüfen, ob die Dateien konvertiert werden

Prüfen Sie nach dem Start eines Speicherpoolkonvertierungsprozesses, ob die Dateien konvertiert werden. Beschreibungen der Felder befinden sich in Feldbeschreibungen.

```
query process

Prozess-  Prozess-             Prozess-
nummer    beschreibung         status
-------  ---------------   ------------------------------------
6         Convert Stgpool   Speicherpool FILEPOOL1 wird in Verzeichniscontainer-
                            speicherpool NEWDEDUP1 konvertiert. Konvertierte
                            Datenträger: 1 von 6, Fehlgeschlagene Datenträger: 0,
                            Konvertierte Dateien: 975, Konvertierte Byte: 196,27 MB,
                            Übersprungene Dateien: 0, Übersprungene Byte: 0 B,
                            Summe übertragener Byte: 151,27 MB

7         Convert Stgpool   Speicherpool DEDUPPOOL wird in Verzeichniscontainer-
                            speicherpool DIRPOOL konvertiert. Konvertierte
                            Dateien:  150 von 360, Konvertierte Byte: 79.598 KB
                            von 388 MB.Nicht konvertierte Dateien: 12.
                            Nicht konvertierte Byte: 27 MB. Aktueller Eingabe-
                            datenträger: /fvt/srv/BK01. Abgelaufene Zeit: 0 Tag(e),
                            0 Stunde(n), 1 Minute(n).

8          Convert Stgpool  Speicherpool FILEPOOL1 wird in Verzeichniscontainer-
                            speicherpool NEWDEDUP1 konvertiert. Konvertierte
                            Dateien: 0, Konvertierte Byte: 0 B von 1,00 GB,
                            Übersprungene Dateien: 0, Übersprungene Byte: 0 B,
                            Summe übertragener Byte: 0 B, Aktueller Eingabe-
                            datenträger: /STORAGE/file1/00000005.BFS,
                            Abgelaufene Zeit: 0 Tage, 0 Stunden, 1 Minute.

10         Convert Stgpool  Speicherpool FILEPOOL1 wird in Verzeichniscontainer-
                            speicherpool NEWDEDUP1 konvertiert. Konvertierte
                            Dateien: 1007, Konvertierte Byte: 285,44 MB von 1,33 GB,
                            Übersprungene Dateien: 0, Übersprungene Byte: 0 B,
                            Summe übertragener Byte: 196,28 MB, Aktueller Eingabe-
                            datenträger: /STORAGE/file1/00000004.BFS,
                            Abgelaufene Zeit: 0 Tage, 0 Stunden, 1 Minute.
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Beispiel: Versetzung von der lokalen Platte in die Cloud prüfen

Nach dem Start der Datenübertragung von der lokalen Platte in die Cloud prüfen, ob die Daten versetzt werden. Beschreibungen der Felder befinden sich in Feldbeschreibungen.

```
query process


Prozess-  Prozess-                Prozess-
nummer    beschreibung            status
-------   --------------   ---------------------------------------
4         Übertragung von lokaler  Übertragung von lokaler Platte nach Cloud
          Platte nach Cloud        für Verzeichniscontainerspeicherpool CLOUDPOOL.
                                   1 Container verarbeitet. 2.100 KB in 4 Datenbereichen
```

```
übertragen.
Abgelaufene Zeit: 0 Tag(e), 0 Stunde(n),
1 Minute(n).
```

Feldbeschreibungen

Prozessnummer
: Gibt die Nummer an, die dem aktiven Hintergrundprozess zugeordnet ist.

Prozessbeschreibung
: Gibt eine Beschreibung des aktiven Hintergrundprozesses an.

Prozessstatus
: Gibt den Status des aktiven Hintergrundprozesses an.

Tipp: Wenn ein Knotenreplikationsprozess auf dem Zielreplikationsserver beendet wird, werden nur Informationen zur Prozessbeendigung in der Aktivitätsübersichtstabelle gespeichert. Die vollständige Übersicht für den Replikationsprozess wird in der Aktivitätsübersichtstabelle auf dem Quellenreplikationsserver gespeichert.

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für QUERY PROCESS

Befehl	Beschreibung
CANCEL EXPORT	Löscht eine ausgesetzte Exportoperation.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
IDENTIFY DUPLICATES	Identifiziert doppelte Daten in einem Speicherpool.
QUERY EXPORT	Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY REPLNODE	Zeigt Informationen zum Replikationsstatus eines Clientknotens an.
RESTART EXPORT	Startet eine ausgesetzte Exportoperation erneut.
SUSPEND EXPORT	Setzt eine aktive Exportoperation aus.

QUERY PROFILE (Profil abfragen)

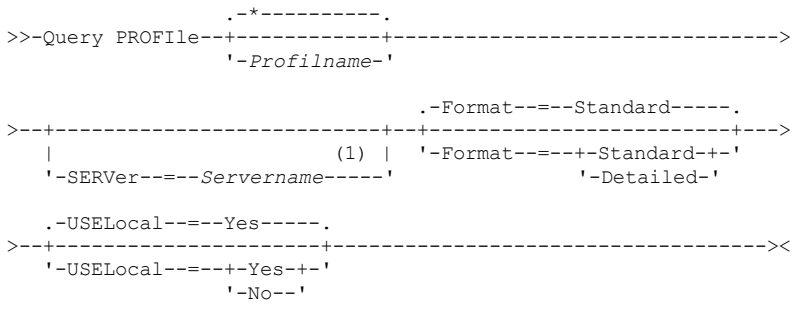
Mit diesem Befehl können Informationen über Profile und zugeordnete Objekte angezeigt werden. Geben Sie diesen Befehl von einem Konfigurationsmanager oder von einem verwalteten Server aus. Mit diesem Befehl können Profilinformationen von jedem Konfigurationsmanager abgerufen werden, der für den Server definiert ist, auch wenn der Server für kein Profil subskribiert.

Wird ein gesperrtes Profil von dem Konfigurationsmanager abgefragt, zu dem das Profil gehört, werden vollständige Profilinformationen angezeigt. Wird ein gesperrtes Profil von einem anderen Server abgefragt, zeigt die Abfrage nur an, daß das Profil gesperrt ist.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Anmerkungen:

1. Der angegebene Servername hängt von dem Server ab, von dem aus der Befehl ausgegeben wird. Siehe die Beschreibung des Parameters SERVER.

Parameter

Profilname
: Gibt das Profil an, das angezeigt werden soll. Sollen mehrere Namen angegeben werden, ein Platzhalterzeichen verwenden. Dieser Parameter ist wahlfrei. Standardmäßig werden alle Profile angezeigt.

SERVer
: Gibt den Konfigurationsmanager an, dessen Profilinformationen angezeigt werden. Die Anforderungen für den Namen sind davon abhängig, wo die Abfrage ausgegeben wird:

  - Von einem Konfigurationsmanager: Dieser Parameter ist wahlfrei. Der Standardwert ist der Name des Konfigurationsmanagers.
  - Von einem verwalteten Server: Dieser Parameter ist wahlfrei. Der Standardwert ist der Name des Konfigurationsmanagers für diesen verwalteten Server.
  - Von einem Server, der weder ein Konfigurationsmanager noch ein verwalteter Server ist: Sie müssen einen Namen angeben.

Format
: Gibt an, ob Teilinformationen oder ausführliche Informationen angezeigt werden. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass ausführliche Informationen angezeigt werden.

USELocal
: Wird die Abfrage von einem verwalteten Server ausgeführt, gibt dieser Parameter an, ob die Profilinformationen von dem Konfigurationsmanager oder dem verwalteten Server abgerufen werden. Sind die Profilinformationen auf dem verwalteten Server nicht vorhanden, werden die Informationen unabhängig von dem Wert dieses Parameters von dem Konfigurationsmanager abgerufen.

  Wenn dieser Parameter auf einem Server verwendet wird, der nicht durch den Konfigurationsmanager verwaltet wird, der Eigner des Profils ist, wird der Parameter ignoriert. Der Standardwert ist YES. Gültige Werte:

  Yes
  : Gibt an, dass die Profilinformationen, falls verfügbar, vom verwalteten Server abgerufen werden. Sind keine Informationen von dem verwalteten Server verfügbar, wird Kontakt mit dem Konfigurationsmanager aufgenommen.

  No
  : Gibt an, dass die Profilinformationen von dem Konfigurationsmanager abgerufen werden, auch wenn die Informationen auf dem verwalteten Server verfügbar sind. Damit wird sichergestellt, daß aktuelle Informationen über das Profil empfangen werden.

Beispiel: Profile von einem Konfigurationsmanager auflisten

Profilinformationen von einem Konfigurationsmanager anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query profile

Konfigurations-     Profilname            Gesperrt?
manager---------------     ---------------       ------
SERVER1             DEFAULT_PROFILE       No
SERVER1             ADMIN_INFO            No
SERVER1             EMPLOYEE              No
SERVER1             PERSONNEL             Yes
```

Beispiel: Ausführliche Profilinformationen für einen verwalteten Server anzeigen

Von einem verwalteten Server aktuelle ausführliche Informationen über das Profil ADMIN_INFO anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.
Anmerkung: Ist das Profil gesperrt, werden die meisten Felder nicht angezeigt.

```
query profile admin_info
format=detailed uselocal=no

           Konfigurationsmanager: SERVER1
                     Profilname: ADMIN_INFO
                       Gesperrt: No
                  Beschreibung: Distributed admin. schedules
     Server-Administratoren: DENNIS EMILY ANDREA
           Maßnahmendomänen: ADMIN RECORDS
   Zeitpläne für Verwaltungsbefehle: ** alle Objekte **
          Server-Befehlsprozeduren:
             Client-Optionsgruppen:
                                Server:
                  Server-Gruppen:
```

Feldbeschreibungen

Konfigurationsmanager

Der Name des Konfigurationsmanagers, der Eigner des Profils ist.

Profilname
: Der Name des Profils.

Gesperrt?
: Angabe, ob das Profil gesperrt ist.

Beschreibung
: Die Beschreibung des Profils.

Server-Administratoren
: Die Administratoren, die dem Profil zugeordnet sind.

Maßnahmendomänen
: Die Maßnahmendomänen, die dem Profil zugeordnet sind.

Zeitpläne für Verwaltungsbefehle
: Die Verwaltungszeitpläne, die dem Profil zugeordnet sind.

Server-Befehlsprozeduren
: Die Server-Befehlsprozeduren, die dem Profil zugeordnet sind.

Client-Optionsgruppen
: Die Client-Optionsgruppen, die dem Profil zugeordnet sind.

Server
: Die Server, die dem Profil zugeordnet sind.

Server-Gruppen
: Die Namen der Server-Gruppen, die dem Profil zugeordnet sind.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY PROFILE

Befehl	Beschreibung
COPY PROFILE	Erstellt eine Kopie eines Profils.
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DEFINE SUBSCRIPTION	Subskribiert einen verwalteten Server für ein Profil.
DELETE PROFASSOCIATION	Löscht die Zuordnung zwischen einem Objekt und einem Profil.
DELETE PROFILE	Löscht ein Profil aus einem Konfigurationsmanager.
LOCK PROFILE	Verhindert die Verteilung eines Konfigurationsprofils.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UNLOCK PROFILE	Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

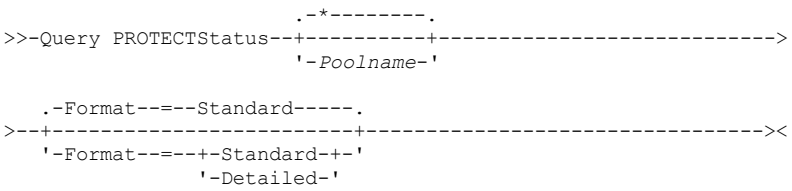
QUERY PROTECTSTATUS (Status des Speicherpoolschutzes abfragen)

Mit diesem Befehl können Informationen zum Status des Speicherpoolschutzes für Verzeichniscontainerspeicherpools angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Poolname

Gibt den Namen des Verzeichniscontainerspeicherpools an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert angegeben, wird der Status aller Verzeichniscontainerspeicherpools angezeigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Geben Sie einen der folgenden Werte an:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Übersichtsdaten zu einem bestimmten Speicherpool anzeigen

Informationen zum Speicherpool mit dem Namen POOL1 anzeigen. Den folgenden Befehl ausgeben:

```
query protectstatus pool1
```

```
Name des       Quellen-      Name des       Ziel-           Prozent     Letzter ausgeführter
Quellenservers speicherpool  Zielservers    speicherpool    geschützt   Schutz
-------------  ------------  ------------   ------------    ----------  --------------
NEXT           POOL1         NEXT           POOL1COPY       96,55       02/17/2017 11:15:07
NEXT           POOL1         NEXT1          POOL2           99,99       02/17/2017 11:14:53
NEXT           POOL1         UNKNOWN        UNKNOWN         UNKNOWN     02/17/2017 11:13:44
NEXT1          POOL2         NEXT           POOL1           100,00      02/17/2017 12:56:58
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Beispiel: Ausführliche Informationen zu einem bestimmten Speicherpool anzeigen

Ausführliche Informationen zum Speicherpool mit dem Namen POOL1 anzeigen. Den folgenden Befehl ausgeben:

```
query protectstatus pool1 format=detailed
```

```
       Name des Quellenservers: NEXT
                  Quellenspeicherpool: POOL1
                Name des Zielservers: NEXT
                    Zielspeicherpool: POOL1COPY
                  Prozent geschützt: 96,55
              Geschützte Datenbereiche: 1.747
          Gesamtzahl der Datenbereiche: 1.852
                       Geschützte MB: 165,33
                       Gesamtzahl MB: 171,23
            Letzter ausgeführter Schutz: 02/17/2017 11:15:07
   Datum/Zeit der letzten Aktualisierung: 02/19/2017 00:27:12
```

Für Feldbeschreibungen siehe Feldbeschreibungen.

Feldbeschreibungen

Name des Quellenservers
: Der Name des Quellenservers.

Quellenspeicherpool
: Der Name des Verzeichniscontainerspeicherpools auf dem Quellenserver.

Name des Zielservers
: Der Name des Zielservers.

Zielspeicherpool
: Der Name des Verzeichniscontainerspeicherpools auf dem Zielserver.

Prozent geschützt
: Der Prozentsatz der geschützten Daten im Verzeichniscontainerspeicherpool.

Geschützte Datenbereiche
: Die Anzahl Datenbereiche, die im Verzeichniscontainerspeicherpool geschützt werden.

Gesamtzahl der Datenbereiche
: Die Gesamtzahl der Datenbereiche im Verzeichniscontainerspeicherpool.

Geschützte MB
: Das Gesamtvolumen der geschützten Daten im Verzeichniscontainerspeicherpool in Megabyte.

Gesamtzahl MB
: Das Gesamtvolumen der Daten im Verzeichniscontainerspeicherpool in Megabyte.

Letzter ausgeführter Schutz
: Das Datum und die Uhrzeit, an dem bzw. zu der der Verzeichniscontainerspeicherpool zuletzt geschützt wurde.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der der Verzeichniscontainerspeicherpool zuletzt aktualisiert wurde.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY PROTECTSTATUS

Befehl	Beschreibung
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.

QUERY PROXYNODE (Proxyberechtigung für einen Clientknoten abfragen)

Verwenden Sie diesen Befehl, um Clientknoten anzuzeigen, die die Berechtigung als Proxy für andere Clientknoten auf dem IBM Spectrum Protect-Server haben.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                                .-*--------------.
>>-Query PROXynode----TArget--=--+----------------+------------><
                                '-Zielknotenname-'
```

Parameter

TArget
: Gibt den Namen des Knotens an, der Ziel des Knotens mit Proxyberechtigung ist. Die Angabe eines Zielknotennamens ist optional. Namen mit Platzhalterzeichen können zur Angabe des Zielknotennamens verwendet werden. Eine durch Kommas getrennte Auflistung von Knotennamen ist ebenfalls zulässig.

Beispiel: Clientknoten mit Proxy-Berechtigung auflisten

Um alle IBM Spectrum Protect-Clientknoten mit Proxy-Berechtigung für den Zielknoten MYCLUSTER anzuzeigen, geben Sie den folgenden Befehl aus.

```
query proxynode target=mycluster
```

```
Zielknoten          Agentenknoten
---------------     ----------------
FRED                MOE MINIE MICKEY
ALPHA               BETA GAMMA DELTA
```

Feldbeschreibungen

Zielknoten
: Gibt den Namen des Knotens an, der Ziel des Knotens mit Proxyberechtigung ist.

Agentenknoten
: Gibt den Namen des Agentenknotens an.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY PROXYNODE

Befehl	Beschreibung
GRANT PROXYNODE	Erteilt einem Agentenknoten die Proxyberechtigung.
REVOKE PROXYNODE	Entzieht einem Agentenknoten die Proxyberechtigung.

QUERY PVUESTIMATE (Prozessor-Value-Unit-Schätzung anzeigen)

Verwenden Sie diesen Befehl, um eine Schätzung der Clienteinheiten und Servereinheiten anzufordern, die von dem IBM Spectrum Protect-Server verwaltet werden. Außerdem wird mit diesem Befehl eine Schätzung der Prozessor-Value-Unit-Summen (PVU-Summen) für die Servereinheiten bereitgestellt.

Dieser Befehl generiert eine PVU-Schätzung, die auf der Anzahl logischer Knoten basiert, die für den IBM Spectrum Protect-Server definiert sind. Dagegen basiert die Berechnung der Lizenzpflichten auf der Anzahl physischer Computer. Möglicherweise ist keine 1:1-Korrelation zwischen der Anzahl logischer Knoten und der Anzahl physischer Computer vorhanden. Der von dem Befehl QUERY PVUESTIMATE generierte Bericht ist eine Schätzung, die rechtlich nicht bindend ist.

Für den Befehl QUERY PVUESTIMATE wird angenommen, dass Knoten auf Microsoft Windows 7-, Microsoft Windows XP Professional- und Apple-Systemen Clienteinheiten sind. Knoten auf allen anderen Plattformen werden als Servereinheiten betrachtet. Der Server, auf dem IBM Spectrum Protect ausgeführt wird, wird ebenfalls als Servereinheit klassifiziert. Sie können jedoch Servereinheiten wieder als Clienteinheiten klassifizieren, falls dies erforderlich ist. Wenn Ihr System Workstations im Ruhezustand, Testworkstations oder andere Workstations umfasst, die bei der PVU-Berechnung ignoriert werden können, können Sie diese als Typ 'Andere' angeben. Um eine Knotenklassifikation zu ändern, verwenden Sie den Befehl UPDATE NODE oder den Befehl REGISTER NODE.

Anmerkung: Die von IBM Spectrum Protect zurückgemeldeten PVU-Informationen werden nicht als annehmbarer Ersatz für das IBM® License Metric Tool angesehen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                       .-Format--=--Standard-----.
>>-Query PVUESTIMate--+------------------------+--------------><
                       '-Format--=--+-Standard-+-'
                                    '-Detailed-'
```

Parameter

Format
: Gibt das Ausgabeformat an. Dieser Parameter ist wahlfrei. Der Standardwert ist Standard. Die folgenden Werte können verwendet werden:

  Standard
  : Gibt die Standardausgabe an.

  Detailed
  : Gibt die Detailausgabe an.

Beispiel: Die geschätzte Anzahl der Einheiten und PVU anzeigen

Die geschätzte Anzahl der Clienteinheiten und Servereinheiten sowie die geschätzte PVU für die Servereinheiten für einen IBM Spectrum Protect-Server anzeigen. Den folgenden Befehl ausgeben:

```
query pvuestimate
```

Tabelle 1. Beispielausgabe für mehrere Produkte, die von einem IBM Spectrum Protect-Server verwaltet werden

Produkt	Anzahl Clienteinheiten	Anzahl Servereinheiten	Prozessor-Value-Unit (PVU) der Servereinheiten
IBM Spectrum Protect Extended Edition	1.000	905	90.500
IBM Spectrum Protect for Storage Area Networks	50	10	1.000
IBM Spectrum Protect for Space Management	0	0	0
IBM Spectrum Protect for Mail	0	25	5.000
IBM Spectrum Protect for Databases	0	1.025	20.500
IBM Spectrum Protect for Enterprise Resource Planning	0	25	5.000
IBM Spectrum Protect for System Backup and Recovery	0	0	0

Andere Knotenklassifikationen	Anzahl
Knoten vor Version 6.3, für die momentan keine PVU-Informationen verfügbar sind	10
Knoten mit Version 6.3 oder höher ohne PVU-Abgleich	9
Vom Administrator als "andere Einheit" klassifizierte Knoten	8
Als nicht lizenzierte API-Anwendung definierte Knoten	6

Die folgende Liste enthält Details zu den Beispielfeldern:

Produkt
: Der Name des IBM Spectrum Protect-Produkts.

Anzahl Clienteinheiten

Die geschätzte Anzahl der Clienteinheiten, die von dem Produkt verwaltet werden. Standardmäßig werden nur Knoten auf Microsoft Windows 7-, Microsoft Windows XP Professional- und Apple-Systemen als Clienteinheiten betrachtet.

Anzahl Servereinheiten

Die geschätzte Anzahl der Servereinheiten, die von dem Produkt verwaltet werden. Standardmäßig werden Knoten auf allen Plattformen mit Ausnahme von Microsoft Windows 7-, Microsoft Windows XP Professional- und Apple-Systemen als Servereinheiten betrachtet. Diese Anzahl enthält auch den Server, auf dem IBM Spectrum Protect ausgeführt wird.

Prozessor-Value-Unit (PVU) der Servereinheiten

Die geschätzten PVUs aller Knoten, die als Servereinheiten verbunden sind.

Knoten vor Version 6.3, für die momentan keine PVU-Informationen verfügbar sind

Einheiten, die keine Prozessorinformationen an den Server zurückmelden.

Knoten mit Version 6.3 oder höher ohne PVU-Abgleich

Einheiten, die nicht alle erforderlichen Werte zurückmelden, oder einige Werte wurden als "Unbekannt" zurückgemeldet.

Vom Administrator als "andere Einheit" klassifizierte Knoten

Knoten, die vom Administrator mit dem Befehl update node roleoverride=other von der PVU-Berechnung ausgeschlossen werden.

Als nicht lizenzierte API-Anwendung definierte Knoten

Knoten, wie beispielsweise DB2-Sicherungsanwendungen oder angepasste API-Anwendungen.

Beispiel: Ausführliche Knoteninformationen anzeigen

Informationen zu einzelnen Knoten anzeigen, indem der Wert 'Detailed' (d) für den Parameter Format angegeben wird. Den folgenden Befehl ausgeben:

```
tsm: PATMOS_630> query pvuestimate f=d
```

Tabelle 2. Knotenklassifikationen für bestimmte Produkte

Produkt	Anzahl Clienteinheiten	Anzahl Servereinheiten	Prozessor-Value-Unit (PVU) der Servereinheiten
IBM Spectrum Protect Extended Edition	1.000	905	90.500
- banode1	1		
- banode2		1	200
- banode3	1		
- banode3		1	100
IBM Spectrum Protect for Storage Area Networks	50	10	1.000
- stagent1		1	50
- stagent2		1	100
IBM Spectrum Protect for Space Management	0	0	0
IBM Spectrum Protect for Mail	0	25	5.000
- mailnode1		1	200
- mailnode2		1	100
IBM Spectrum Protect for Databases	0	1.025	20.500
- dbnode1		1	200
- dbnode2		1	100
IBM Spectrum Protect for Enterprise Resource Planning	0	25	5.000
- erpnode1		1	50
- erpnode2		1	100
IBM Spectrum Protect for System Backup and Recovery	0	0	0

Andere Knotenklassifikationen	Anzahl

Andere Knotenklassifikationen	Anzahl
Knoten vor Version 6.3, für die momentan keine PVU-Informationen verfügbar sind	10
- oldnode1	1
- oldnode2	1
- mailnote44	1
- erpnode66	1
Knoten mit Version 6.3 oder höher ohne PVU-Abgleich	10
- badcitnode1	1
- badcitnode2	1
- mailnode23	1
- erpnode34	1
Vom Administrator als "andere Einheit" klassifizierte Knoten	8
- overriddennode1	1
- overriddennode2	1
- mailnode77	
Als nicht lizenzierte API-Anwendung definierte Knoten	6
- vendorapinode1	1
- vendorapinode2	1

Zugehörige Befehle

Tabelle 3. Zugehörige Befehle für QUERY PVUESTIMATE

Befehl	Beschreibung
AUDIT LICENSES	Prüft die Einhaltung der definierten Lizenzen.
QUERY LICENSE	Zeigt Informationen über Lizenzen und Prüfvorgänge an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
REGISTER LICENSE	Registriert eine Lizenz für den IBM Spectrum Protect-Server.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
SET CPUINFOREFRESH	Gibt die Anzahl der Tage zwischen Clientsuchläufen nach Workstationinformationen an, die für PVU-Schätzungen verwendet werden.
SET LICENSEAUDITPERIOD	Gibt die Anzahl Tage zwischen den automatischen Lizenzprüfungen an.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

QUERY RECOVERYMEDIA (Wiederherstellungsdatenträger abfragen)

Mit diesem Befehl können Informationen über die Datenträger (beispielsweise Boot-Datenträger) angezeigt werden, die für die Wiederherstellung einer Maschine benötigt werden. Datenträger werden in alphabetischer Reihenfolge nach Namen angezeigt.

Hinweis: Die Informationen werden von IBM Spectrum Protect nicht verwendet. Sie dienen nur zur Planung der Fehlerbehebung bei Client-Maschinen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                        .-*---------------.
>>-Query RECOVERYMedia--+-----------------+--------------------><
                        '-Datenträgername-'

>--+--------------------+--+-----------------------+------------><
   '-Type--=--+-BOot--+-'  '-LOcation--=--Position-'
              '-OTher-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Datenträgername
: Gibt den Namen des Wiederherstellungsdatenträgers an. Es können Platzhalterzeichen verwendet werden, um den Namen anzugeben. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Wiederherstellungsdatenträger.

Type
: Gibt den Typ des Datenträgers an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden alle Wiederherstellungsdatenträger abgefragt. Gültige Werte:

  BOot
  : Nur Boot-Datenträger werden abgefragt.

  OTher
  : Alle Datenträger, außer Boot-Datenträger, werden abgefragt.

LOcation
: Gibt den Standort des Wiederherstellungsdatenträgers an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Es können bis zu 255 Zeichen angegeben werden. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Gültige Werte:

  Standard
  : Zeigt Teilinformationen an. Dies ist der Standardwert.

  Detailed
  : Zeigt alle Informationen an.

Beispiel: Übersichtsdaten zu einem bestimmten Wiederherstellungsdatenträger anzeigen

Informationen für den Wiederherstellungsdatenträger RECMED1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query recoverymedia RECMED1
```

```
Wiederherstellungs-
datenträgername       Datenträgernamen  Standort          Maschinenname
--------------------  ----------------  ----------------  ------------
RECMED1               vol1 vol2 vol3    IRONMOUNTAIN      MACH1
                                              vol4
```

Beispiel: Ausführliche Informationen zu einem bestimmten Wiederherstellungsdatenträger anzeigen

Ausführliche Informationen für den Wiederherstellungsdatenträger RECMED1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query recoverymedia RECMED1 format=detailed
```

```
Wiederherstellungsdatenträgername: RECMED1
                              Typ: Boot
                 Datenträgernamen: vol1 vol2 vol3 vol4
                         Standort: IRONMOUNTAIN
                     Beschreibung:
                          Produkt:
               Produktinformation:
                    Maschinenname: MACH1
```

Feldbeschreibungen

Wiederherstellungsdatenträgername
: Der Name des Wiederherstellungsdatenträgers.

Typ
: Angabe, ob es sich bei den Wiederherstellungsdatenträgern um Boot-Datenträger oder um einen anderen Datenträgertyp handelt. Gültige Werte:

Boot
: Die Wiederherstellungsdatenträger sind Boot-Datenträger.

Other
: Die Wiederherstellungsdatenträger sind keine Boot-Datenträger.

Datenträgernamen
: Die Gruppe der Datenträger, die die Daten enthalten, die zum Wiederherstellen der Maschinen benötigt werden, die diesem Datenträger zugeordnet sind.

Standort
: Der Speicherort des Wiederherstellungsdatenträgers.

Beschreibung
: Eine Beschreibung des Wiederherstellungsdatenträgers.

Produkt
: Das Produkt, das zum Erstellen der Boot-Datenträger verwendet wurde.

Produktinformation
: Informationen über das Produkt, das die Boot-Datenträger erstellt hat. Diese Informationen werden eventuell zum Zurückschreiben der Maschine benötigt.

Maschinenname
: Die Maschinen, die diesem Wiederherstellungsdatenträger zugeordnet sind.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY RECOVERYMEDIA

Befehl	Beschreibung
DEFINE RECMEDMACHASSOCIATION	Ordnet Wiederherstellungsdatenträger einer Maschine zu.
DEFINE RECOVERYMEDIA	Definiert die Datenträger, die für die Wiederherstellung einer Maschine erforderlich sind.
DELETE RECOVERYMEDIA	Löscht Wiederherstellungsdatenträger.
UPDATE RECOVERYMEDIA	Ändert die Attribute von Wiederherstellungsdatenträgern.

QUERY REPLICATION (Knotenreplikationsprozesse abfragen)

Verwenden Sie diesen Befehl, um Informationen zu aktiven und beendeten Knotenreplikationsprozessen anzuzeigen.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Wichtig: Es können keine Informationen zu aktiven Replikationsprozessen für Clientknoten angezeigt werden, die aus Import- und Exportoperationen in Replikationsoperationen konvertiert werden. Der Konvertierungsprozess kann lange dauern, aber er erfolgt nur einmal für einen Clientknoten, der konvertiert wird.

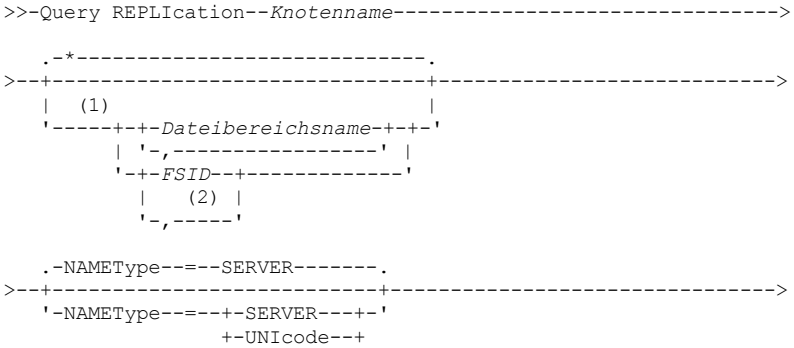
Standardmäßig werden Datensätze zu abgeschlossenen Knotenreplikationsprozessen 30 Kalendertage aufbewahrt. Ein *Kalendertag* besteht aus 24 Stunden, von Mitternacht bis Mitternacht.

Um den Aufbewahrungszeitraum anzuzeigen, geben Sie den Befehl QUERY STATUS aus. Überprüfen Sie den Wert im Feld Aufbewahrungszeitraum für Replikationsdatensätze. Um den Aufbewahrungszeitraum zu ändern, geben Sie den Befehl SET REPLRETENTION aus.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



```
                  |      (2) |
                  '-FSID-----'

   .-CODEType--=--BOTH-----------.
>--+-----------------------------+-----------------------------><
   '-CODEType--=--+-BOTH-------+-'
                  +-UNIcode----+
                  '-NONUNIcode-'

   .-DISplay--=--1-----------.
>--+-------------------------+--+-------------------------+----><
   '-DISplay--=--Anzahl Tage-'  '-PROCessid--=--Prozess-ID-'

   .-STatus--=--ALl---------.  .-Format--=--Standard-----.
>--+----------------------+--+-------------------------+-----><
   '-STatus--=--+-ALl-----+-'  '-Format--=--+-Standard-+-'
                +-RUnning-+                 '-Detailed-'
                +-ENded---+
                '-FAiled--'
```

Anmerkungen:

1. Mischen Sie nicht FSIDs (Dateibereichs-IDs) und Dateibereichsnamen in demselben Befehl.
2. Geben Sie nicht die FSID an, wenn Sie Platzhalterzeichen für den Clientknotennamen verwenden.

Parameter

Knotenname (Erforderlich)

Gibt den Namen des abzufragenden Clientknotens an. Mit einer Ausnahme können Sie Platzhalterzeichen verwenden, wenn Sie diesen Namen angeben. Wenn der Parameter NAMETYPE den Wert FSID hat, geben Sie keine Platzhalterzeichen für den Clientknotennamen an. Der Wert FSID gibt die Dateibereichs-ID an. Dateibereiche mit identischen Namen können verschiedene IDs in verschiedenen Clientknoten haben.

Dateibereichsname oder FSID

Gibt den Namen des Dateibereichs oder die ID des Dateibereichs (FSID) an, der abgefragt werden soll. Ein Name oder eine FSID ist optional. Wenn Sie keinen Namen oder keine FSID angeben, werden alle Dateibereiche abgefragt.

Dateibereichsname
: Gibt den Namen des Dateibereichs an, der Daten enthält, die abgefragt werden sollen. Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Um die korrekte Schreibweise für den Dateibereich zu bestimmen, geben Sie den Befehl QUERY FILESPACE aus. Mehrere Namen sind ohne Leerzeichen durch Kommas voneinander zu trennen. Wenn Sie einen Namen angeben, können Sie Platzhalterzeichen verwenden.

  Ein Server, der über Clients mit Unicode-fähigen Dateibereichen verfügt, muss möglicherweise den Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls einen Namen aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich in der Beschreibung des Parameters NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie nur ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

FSID
: Gibt die Dateibereichs-ID für den Dateibereich an, der abgefragt werden soll. Der Server verwendet FSIDs zum Lokalisieren der Dateibereiche, die repliziert werden sollen. Um die FSID für einen Dateibereich zu bestimmen, geben Sie den Befehl QUERY FILESPACE aus. Mehrere FSIDs sind ohne Leerzeichen durch Kommas voneinander zu trennen. Wenn Sie eine FSID angeben, muss der Wert des Parameters NAMETYPE FSID lauten.

NAMEType

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients verwenden, die über die Betriebssysteme Windows, Macintosh OS X und NetWare verfügen.

Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

SERVER
: Der Server verwendet die Zeichenumsetztabelle des Servers, um Dateibereichsnamen zu interpretieren.

UNIcode
: Der Server konvertiert Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind. Die Konvertierung kann auch fehlschlagen, wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

FSID
: Der Server interpretiert Dateibereichsnamen unter Verwendung ihrer Dateibereichs-IDs.

CODEType

Gibt den Typ der Dateibereiche an, die in der Abfrage berücksichtigt werden sollen. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig von der Art der Zeichenumsetztabelle eingeschlossen werden. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Sie können einen der folgenden Werte angeben:

UNIcode
: Nur Dateibereiche einschließen, die in Unicode sind.

NONUNIcode
: Dateibereiche einschließen, die nicht nur in Unicode sind.

BOTH
: Alle Dateibereiche unabhängig von der Art der Zeichenumsetztabelle einschließen.

DISplay

Gibt die Anzahl der Tage an, für die das Knotenreplikationsprotokoll angezeigt werden soll. Der Standardwert ist 1. Mit diesem Standardwert werden Informationen zu aktiven Knotenreplikationsprozessen und zu Prozessen angezeigt, die während des aktuellen Kalendertags abgeschlossen wurden. Der Maximalwert ist 9999.

Sie können eine Zahl angeben, die kleiner-gleich der Anzahl der Tage ist, die als Aufbewahrungszeitraum für die Replikationsprotokollsätze angegeben wird. Wenn Sie einen Wert angeben, der größer als der Wert des Aufbewahrungszeitraums für die Replikation ist oder größer als die Anzahl der Tage ist, die Replikationsdatensätze erfasst werden, zeigt der Server nur die Anzahl der verfügbaren Replikationsprotokollsätze an. Beispiel: Angenommen, der Aufbewahrungszeitraum für die Replikation beträgt 30 Tage und der Replikationsprozess wird nur 10 Tage ausgeführt. Wenn Sie `DISPLAY=20` angeben, werden nur 10 Tage des Replikationsprotokolls angezeigt.

PROCessid
: Gibt das Knotenreplikationsprotokoll an, das einem bestimmten Prozess zugeordnet ist, der durch die Prozess-ID angegeben ist. Dieser Parameter ist wahlfrei. Wenn dieser Parameter nicht angegeben wird, werden alle Prozesse für die mit dem Parameter DISPLAY angegebene Anzahl der Tage angezeigt.

Ein Neustart des Servers kann zur Folge haben, dass der Server Prozess-IDs wiederverwendet. Die Wiederverwendung von Prozess-IDs kann zu doppelten Prozess-IDs für separate Prozesse führen.

STatus
: Gibt den Status der Dateibereiche an, die abgefragt werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist ALL. Sie können einen der folgenden Werte angeben:

ALl
: Gibt alle Dateibereiche, die gerade repliziert werden, Dateibereiche, die erfolgreich repliziert wurden, und Dateibereiche an, deren Replikation nicht beendet wurde oder die mit Fehlern repliziert wurden.

RUnning
: Gibt alle Dateibereiche an, die auf den Zielreplikationsserver repliziert werden.

ENded
: Gibt alle Dateibereiche, die erfolgreich repliziert wurden, und Dateibereiche an, deren Replikation nicht beendet wurde oder die mit Fehlern repliziert wurden.

FAiled
: Gibt alle Dateibereiche an, deren Replikation nicht beendet wurde oder die mit Fehlern repliziert wurden.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Sie können einen der folgenden Werte angeben:

Standard
: Gibt an, dass Teilinformationen für Knotenreplikationsprozesse angezeigt werden.

Detailed
: Gibt an, dass alle verfügbaren Informationen für die Knotenreplikationsprozesse angezeigt werden.

Beispiel: Informationen zu Replikationsprozessen für einen Dateibereich anzeigen

Informationen zu Replikationsprozessen für einen Dateibereich im Clientknoten PAYROLL anzeigen. Die Dateibereichs-ID ist 10.

```
query replication ironman

Knotenname Dateiber.-  FSID   Startzeit    Endzeit    Status  Phase
           klasse
-----------------------------------------------------------------
IRONMAN    /space      2      02/08/11     02/08/11   Beendet Keine
                              21:44:19     21:48:14

query replication ironman format=detailed

                                  Knotenname: IRONMAN
                                   Dateibereichsname: /space
```

```
                                        FSID: 2
                                  Startzeit: 02/08/11 21:44:19
                                    Endzeit: 02/08/11 21:48:14
                                      Status: Beendet
                                Prozessnummer: 4
                                      Befehl: replicate node ironman
                                       Phase: Keine
                  Ausführungszeit des Prozesses: 0 Tag(e) 0 Stunde(n)
                                              4 Minute(n)
                              Beendigungsstatus: Beendet
                    Ursache der Nicht-Beendigung: Keine
               Datum/Zeit der letzten Aktual. von Sicherungsdateien:
                                          Zielserver für Sicherung:
                Sicherungsdateien, die keine Aktion erfordert haben: 0
                                 Zu replizierende Sicherungsdateien: 0
                                      Replizierte Sicherungsdateien: 0
            Aufgrund von Fehlern nicht replizierte Sicherungsdateien: 0
                                Noch nicht replizierte Sicherungsdateien: 0
                                   Zu löschende Sicherungsdateien: 0
                                      Gelöschte Sicherungsdateien: 0
             Aufgrund von Fehlern nicht gelöschte Sicherungsdateien: 0
                                 Zu aktualisierende Sicherungsdateien: 0
                                   Aktualisierte Sicherungsdateien: 0
          Aufgrund von Fehlern nicht aktualisierte Sicherungsdateien: 0
                    Zu replizierende Byte für Sicherungsdateien (MB): 0
                         Replizierte Byte für Sicherungsdateien (MB): 0
                         Übertragene Byte für Sicherungsdateien (MB): 0
Aufgrund von Fehlern nicht replizierte Byte für Sicherungsdateien (MB): 0
              Noch nicht replizierte Byte für Sicherungsdateien (MB): 0

            Datum/Zeit der letzten Aktual. von Archivierungsdateien: 02/08/11 21:48:14
                                    Zielserver für Archivierung: NIGLINA
             Archivierungsdateien, die keine Aktion erfordert haben: 0
                           Zu replizierende Archivierungsdateien: 39.416
                                Replizierte Archivierungsdateien: 39.206
        Aufgrund von Fehlern nicht replizierte Archivierungsdateien: 210
                             Noch nicht replizierte Archivierungsdateien: 0
                                Zu löschende Archivierungsdateien: 0
                                   Gelöschte Archivierungsdateien: 0
          Aufgrund von Fehlern nicht gelöschte Archivierungsdateien: 0
                           Zu aktualisierende Archivierungsdateien: 0
                                Aktualisierte Archivierungsdateien: 0


      Aufgrund von Fehlern nicht aktualisierte Archivierungsdateien: 0
                Zu replizierende Byte für Archivierungsdateien (MB): 4.335
                     Replizierte Byte für Archivierungsdateien (MB): 4.335
                     Übertragene Byte für Archivierungsdateien (MB): 0
Aufgrund von Fehlern nicht replizierte Byte für Archivierungsdateien (MB): 0
           Noch nicht replizierte Byte für Archivierungsdateien (MB): 0

     Datum/Zeit der letzten Aktual. von speicherverwalteten Dateien:
                                  Zielserver für Speicherverwaltung:
       Speicherverwaltete Dateien, die keine Aktion erfordert haben: 0
                        Zu replizierende speicherverwaltete Dateien: 0
                             Replizierte speicherverwaltete Dateien: 0
          Aufgrund von Fehlern nicht replizierte speicherverwaltete Dateien: 0
            Noch nicht replizierte speicherverwaltete Dateien: 0
                      Zu löschende speicherverwaltete Dateien: 0
                         Gelöschte speicherverwaltete Dateien: 0
            Aufgrund von Fehlern nicht gelöschte speicherverwaltete Dateien: 0
                Zu aktualisierende speicherverwaltete Dateien: 0
                     Aktualisierte speicherverwaltete Dateien: 0
         Aufgrund von Fehlern nicht aktualisierte speicherverwaltete Dateien: 0
       Zu replizierende Byte für speicherverwaltete Dateien (MB): 0
            Replizierte Byte für speicherverwaltete Dateien (MB): 0
            Übertragene Byte für speicherverwaltete Dateien (MB): 0
Aufgrund von Fehlern nicht replizierte Byte für speicherverwaltete Dateien (MB): 0
    Noch nicht replizierte Byte für speicherverwaltete Dateien (MB): 0
          Gesamtzahl der Dateien, die keine Aktion erfordert haben: 0
                       Gesamtzahl der zu replizierenden Dateien: 39.416
                            Gesamtzahl der replizierten Dateien: 39.206
    Gesamtzahl der aufgrund von Fehlern nicht replizierten Dateien: 210
                 Gesamtzahl der noch nicht replizierten Dateien: 0
                          Gesamtzahl der zu löschenden Dateien: 0
                             Gesamtzahl der gelöschten Dateien: 0
      Gesamtzahl der aufgrund von Fehlern nicht gelöschten Dateien: 0
                       Gesamtzahl der zu aktualisierenden Dateien: 0
                            Gesamtzahl der aktualisierten Dateien: 0
  Gesamtzahl der aufgrund von Fehlern nicht aktualisierten Dateien: 0
                          Summe der zu replizierenden Byte (MB): 4.335
                               Summe der replizierten Byte (MB): 4.335
```

```
                    Summe übertragener Byte (MB):
   Summe der aufgrund von Fehlern nicht replizierten Byte (MB):
Summe der noch nicht replizierten Byte (MB):
       Geschätzte Fertigstellung in Prozent: 100
               Geschätzte verbleibende Zeit:
         Geschätzte Zeit der Fertigstellung:
```

Feldbeschreibungen

Knotenname
: Der Name des Clientknotens, dessen Daten angezeigt werden.

Dateibereichsname
: Der Name des Clientdateibereichs, dessen Daten angezeigt werden.

FSID
: Die Dateibereichs-ID.

Startzeit
: Das Datum und die Uhrzeit, an dem bzw. zu der der Knotenreplikationsprozess gestartet wurde.

Endzeit
: Das Datum und die Uhrzeit, an dem bzw. zu der der Knotenreplikationsprozess beendet wurde.

Status
: Der Status des Knotenreplikationsprozesses. Die folgenden Werte sind gültig:

  Aktiv
  : Der Prozess ist aktiv und sucht nach auswählbaren Daten oder sendet Daten an den Zielreplikationsserver.

  Beendet
  : Der Prozess wurde beendet oder ist fehlgeschlagen.

  Fehlgeschlagen
  : Der Prozess ist fehlgeschlagen.

Prozessnummer
: Die ID für den Knotenreplikationsprozess.

  Dieselbe Prozessnummer kann verschiedene Startzeiten haben. Wenn ein Replikationsprozess gestartet und der Server erneut gestartet wird, ordnet der Server Prozessnummern zu, wobei mit Nummer 1 begonnen wird. Replikationsprozesse, die nach einem Serverneustart gestartet werden, können Prozessnummern erhalten, die bereits anderen Replikationsprozessen im Replikationsprotokoll zugeordnet sind. Um eindeutige Replikationsprozesse anzugeben, verwenden Sie die Startzeit.

Befehl
: Der Befehl, der ausgegeben wurde, um den Knotenreplikationsprozess zu starten.

Phase
: Die Phase eines aktiven Knotenreplikationsprozesses. Die folgenden Phasen sind in der Reihenfolge ihres Auftretens aufgelistet:

  Wird identifiziert
  : Der Knotenreplikationsprozess hat mit dem Identifizieren von Daten begonnen, die repliziert werden sollen, aber die Daten werden noch nicht an den Zielreplikationsserver gesendet.

  Wird identifiziert und repliziert
  : Der Knotenreplikationsprozess identifiziert Daten, die repliziert werden sollen, und überträgt die Daten an den Zielreplikationsserver.

  Wird repliziert
  : Der Knotenreplikationsprozess hat die Daten identifiziert und überträgt Dateien an den Zielreplikationsserver.

  Keine.
  : Der Knotenreplikationsprozess ist nicht aktiv.

Ausführungszeit des Prozesses
: Die Ausführungszeit des Knotenreplikationsprozesses.

Beendigungsstatus
: Der Status des Knotenreplikationsprozesses. Die folgenden Werte sind gültig:

  Beendet
  : Der Knotenreplikationsprozess wurde abgeschlossen.

  Nicht beendet
  : Der Knotenreplikationsprozess wurde nicht bis zum Abschluss ausgeführt. Um die Ursache zu bestimmen, überprüfen Sie den Wert im Feld 'Ursache der Nicht-Beendigung'.

Ursache der Nicht-Beendigung
: Der Grund, warum der Knotenreplikationsprozess nicht bis zum Abschluss ausgeführt wurde. Mögliche Werte sind *abgebrochen* und *andere*. Der Wert *andere* kann angeben, dass der Server während der Replikation angehalten wurde oder der Server fehlgeschlagen ist.

Datum/Zeit der letzten Aktual. von Sicherungsdateien
: Das Datum und die Uhrzeit, an dem bzw. zu der Statistikdaten für Sicherungsdateien zuletzt aktualisiert wurden. Die angegebene Zeit ist die Zeit, zu der die Dateien in dem Dateibereich für die Replikation identifiziert wurden, oder die Zeit, zu der jeder Dateistapel an den Zielreplikationsserver gesendet wurde.

Datum/Zeit der letzten Aktual. von Archivierungsdateien
: Das Datum und die Uhrzeit, an dem bzw. zu der Statistikdaten für Archivierungsdateien zuletzt aktualisiert wurden. Die angegebene Zeit ist die Zeit, zu der die Dateien in dem Dateibereich für die Replikation identifiziert wurden, oder die Zeit, zu der jeder Dateistapel an den Zielreplikationsserver gesendet wurde.

Datum/Zeit der letzten Aktual. von speicherverwalteten Dateien
: Das Datum und die Uhrzeit, an dem bzw. zu der Statistikdaten für speicherverwaltete Dateien zuletzt aktualisiert wurden. Die angegebene Zeit ist die Zeit, zu der die Dateien in dem Dateibereich für die Replikation identifiziert wurden, oder die Zeit, zu der jeder Dateistapel an den Zielreplikationsserver gesendet wurde.

Zielserver für Sicherung
: Der Name des Zielreplikationsservers für Sicherungsdateien.

Zielserver für Archivierung
: Der Name des Zielreplikationsservers für Archivierungsdateien.

Zielserver für Speicherverwaltung
: Der Name des Zielreplikationsservers für speicherverwaltete Dateien.

Sicherungsdateien, die keine Aktion erfordert haben
: Die Anzahl der Sicherungsdateien in dem Dateibereich, die nicht repliziert, aktualisiert oder gelöscht werden mussten.

Archivierungsdateien, die keine Aktion erfordert haben
: Die Anzahl der Archivierungsdateien in dem Dateibereich, die nicht repliziert, aktualisiert oder gelöscht werden mussten.

Speicherverwaltete Dateien, die keine Aktion erfordert haben
: Die Anzahl der speicherverwalteten Dateien in dem Dateibereich, die nicht repliziert, aktualisiert oder gelöscht werden mussten.

Zu replizierende Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die auf den Zielreplikationsserver repliziert werden sollten.

Zu replizierende Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die auf den Zielreplikationsserver repliziert werden sollten.

Zu replizierende speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die auf den Zielreplikationsserver repliziert werden sollten.

Replizierte Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die auf den Zielreplikationsserver repliziert wurden.

Replizierte Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die auf den Zielreplikationsserver repliziert wurden.

Replizierte speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Zu löschende Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die auf dem Zielreplikationsserver gelöscht werden sollten.

Zu löschende Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die auf dem Zielreplikationsserver gelöscht werden sollten.

Zu löschende speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die auf dem Zielreplikationsserver gelöscht werden sollten.

Gelöschte Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die auf dem Zielreplikationsserver gelöscht wurden.

Gelöschte Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die auf dem Zielreplikationsserver gelöscht wurden.

Gelöschte speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die auf dem Zielreplikationsserver gelöscht wurden.

Aufgrund von Fehlern nicht gelöschte Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver gelöscht wurden.

Aufgrund von Fehlern nicht gelöschte Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver gelöscht wurden.

Aufgrund von Fehlern nicht gelöschte speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver gelöscht wurden.

Zu aktualisierende Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die auf dem Zielreplikationsserver aktualisiert werden sollten. Wenn die Metadaten einer Datei geändert werden, werden die geänderten Felder an den Zielreplikationsserver gesendet.

Zu aktualisierende Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die auf dem Zielreplikationsserver aktualisiert werden sollten. Wenn die Metadaten einer Datei geändert werden, werden die geänderten Felder an den Zielreplikationsserver gesendet.

Zu aktualisierende speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die auf dem Zielreplikationsserver aktualisiert werden sollten. Wenn die Metadaten einer Datei geändert werden, werden die geänderten Felder an den Zielreplikationsserver gesendet.

Aktualisierte Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die auf dem Zielreplikationsserver aktualisiert wurden.

Aktualisierte Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die auf dem Zielreplikationsserver aktualisiert wurden.

Aktualisierte speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die auf dem Zielreplikationsserver aktualisiert wurden.

Aufgrund von Fehlern nicht aktualisierte Sicherungsdateien
: Die Anzahl der Sicherungsdateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver aktualisiert wurden.

Aufgrund von Fehlern nicht aktualisierte Archivierungsdateien
: Die Anzahl der Archivierungsdateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver aktualisiert wurden.

Aufgrund von Fehlern nicht aktualisierte speicherverwaltete Dateien
: Die Anzahl der speicherverwalteten Dateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver aktualisiert wurden.

Zu replizierende Byte für Sicherungsdateien (MB)
: Die Anzahl der Byte für Sicherungsdateien, die auf den Zielreplikationsserver repliziert werden sollten.

Zu replizierende Byte für Archivierungsdateien (MB)
: Die Anzahl der Byte für Archivierungsdateien, die auf den Zielreplikationsserver repliziert werden sollten.

Zu replizierende Byte für speicherverwaltete Dateien (MB)
: Die Anzahl der Byte für speicherverwaltete Dateien, die auf den Zielreplikationsserver repliziert werden sollten.

Replizierte Byte für Sicherungsdateien (MB)
: Die Anzahl der Byte für Sicherungsdateien, die auf den Zielreplikationsserver repliziert wurden.

  Wenn eine Datei in einem deduplizierten Speicherpool gespeichert wurde, kann die Anzahl der Byte in der gespeicherten Datei kleiner als die Anzahl der Byte in der ursprünglichen Datei sein. Dieses Feld stellt die Anzahl der physischen Byte in der ursprünglichen Datei dar.

Replizierte Byte für Archivierungsdateien (MB)
: Die Anzahl der Byte für Archivierungsdateien, die auf den Zielreplikationsserver repliziert wurden.

  Wenn eine Datei in einem deduplizierten Speicherpool gespeichert wurde, kann die Anzahl der Byte in der gespeicherten Datei kleiner als die Anzahl der Byte in der ursprünglichen Datei sein. Dieses Feld stellt die Anzahl der physischen Byte in der ursprünglichen Datei dar.

Replizierte Byte für speicherverwaltete Dateien (MB)
: Die Anzahl der Byte für speicherverwaltete Dateien, die auf den Zielreplikationsserver repliziert wurden.

  Wenn eine Datei in einem deduplizierten Speicherpool gespeichert wurde, kann die Anzahl der Byte in der gespeicherten Datei kleiner als die Anzahl der Byte in der ursprünglichen Datei sein. Dieses Feld stellt die Anzahl der physischen Byte in der ursprünglichen Datei dar.

Übertragene Byte für Sicherungsdateien (MB)
: Die Anzahl der Byte für Sicherungsdateien, die an den Zielreplikationsserver gesendet wurden.

  Der Wert in diesem Feld stellt die tatsächliche Anzahl der Dateibyte dar, die an den Zielreplikationsserver gesendet wurden. Dieser Wert wird berechnet, indem die Anzahl der Byte, die aufgrund der Deduplizierung nicht gesendet wurden, von der Anzahl der zu replizierenden Byte subtrahiert wird.

Übertragene Byte für Archivierungsdateien (MB)
: Die Anzahl der Byte für Archivierungsdateien, die an den Zielreplikationsserver gesendet wurden.

  Der Wert in diesem Feld stellt die tatsächliche Anzahl der Dateibyte dar, die an den Zielreplikationsserver gesendet wurden. Dieser Wert wird berechnet, indem die Anzahl der Byte, die aufgrund der Deduplizierung nicht gesendet wurden, von der Anzahl der zu replizierenden Byte subtrahiert wird.

Übertragene Byte für speicherverwaltete Dateien (MB)
: Die Anzahl der Byte für speicherverwaltete Dateien, die an den Zielreplikationsserver gesendet wurden.

  Der Wert in diesem Feld stellt die tatsächliche Anzahl der Dateibyte dar, die an den Zielreplikationsserver gesendet wurden. Dieser Wert wird berechnet, indem die Anzahl der Byte, die aufgrund der Deduplizierung nicht gesendet wurden, von der Anzahl der zu replizierenden Byte subtrahiert wird.

Aufgrund von Fehlern nicht replizierte Byte für Sicherungsdateien (MB)
: Die Anzahl der Byte für Sicherungsdateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte Byte für Archivierungsdateien (MB)
: Die Anzahl der Byte für Archivierungsdateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Aufgrund von Fehlern nicht replizierte Byte für speicherverwaltete Dateien (MB)
: Die Anzahl der Byte für speicherverwaltete Dateien, die aufgrund von Fehlern nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Byte für Sicherungsdateien (MB)
: Die Anzahl der Byte für Sicherungsdateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Byte für Archivierungsdateien (MB)
: Die Anzahl der Byte für Archivierungsdateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Noch nicht replizierte Byte für speicherverwaltete Dateien (MB)
: Die Anzahl der Byte für speicherverwaltete Dateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Gesamtzahl der Dateien, die keine Aktion erfordert haben
: Die Gesamtzahl der Dateien in dem Dateibereich, die nicht repliziert, aktualisiert oder gelöscht werden mussten.

Gesamtzahl der zu replizierenden Dateien
: Die Gesamtzahl der Dateien, die auf den Zielreplikationsserver repliziert werden sollten.

Gesamtzahl der replizierten Dateien
: Die Gesamtzahl der Dateien, die auf den Zielreplikationsserver repliziert wurden.

Gesamtzahl der aufgrund von Fehlern nicht replizierten Dateien
: Die Gesamtzahl der Dateien, die aufgrund von Fehlern nicht repliziert wurden.

Gesamtzahl der noch nicht replizierten Dateien
: Die Gesamtzahl der Dateien, die noch nicht auf den Zielreplikationsserver repliziert wurden.

Gesamtzahl der zu löschenden Dateien
: Die Gesamtzahl der Dateien, die auf dem Zielreplikationsserver gelöscht werden sollten.

Gesamtzahl der gelöschten Dateien
: Die Gesamtzahl der Dateien, die auf dem Zielreplikationsserver gelöscht wurden.

Gesamtzahl der aufgrund von Fehlern nicht gelöschten Dateien
: Die Gesamtzahl der Sicherungsdateien, Archivierungsdateien und speicherverwalteten Dateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver gelöscht wurden.

Gesamtzahl der zu aktualisierenden Dateien
: Die Gesamtzahl der Dateien, die auf dem Zielreplikationsserver aktualisiert werden sollten. Wenn die Metadaten einer Datei geändert werden, werden die geänderten Felder an den Zielreplikationsserver gesendet.

Gesamtzahl der aktualisierten Dateien
: Die Gesamtzahl der Dateien, die auf dem Zielreplikationsserver aktualisiert wurden.

Gesamtzahl der aufgrund von Fehlern nicht aktualisierten Dateien
: Die Gesamtzahl der Sicherungsdateien, Archivierungsdateien und speicherverwalteten Dateien, die aufgrund von Fehlern nicht auf dem Zielreplikationsserver aktualisiert wurden.

Summe der zu replizierenden Byte (MB)
: Die Gesamtzahl der Byte, die auf den Zielreplikationsserver repliziert werden sollten.

Summe der replizierten Byte (MB)
: Die Gesamtzahl der Byte, die auf den Zielserver repliziert wurden.

  Wenn eine Datei in einem deduplizierten Speicherpool gespeichert wurde, kann die Anzahl der Byte in der gespeicherten Datei kleiner als die Anzahl der Byte in der ursprünglichen Datei sein. Dieses Feld stellt die Anzahl der physischen Byte in der ursprünglichen Datei dar.

Summe übertragener Byte (MB)
: Die Gesamtzahl der Byte, die an den Zielreplikationsserver übertragen wurden.

  Für Dateien, die in einem deduplizierten Speicherpool gespeichert wurden, schließt der Wert in diesem Feld die Anzahl der Byte in der ursprünglichen Datei ein, bevor doppelte Bereiche entfernt wurden. Waren doppelte Bereiche bereits auf dem Zielreplikationsserver vorhanden, ist die Anzahl der Byte in der ursprünglichen Datei größer als die Anzahl der übertragenen Byte.

Summe der aufgrund von Fehlern nicht replizierten Byte (MB)
: Die Gesamtzahl der Byte, die übersprungen wurden, da sie vom Quellenreplikationsserver nicht an den Zielreplikationsserver übertragen werden konnten.

Summe der noch nicht replizierten Byte (MB)
: Die Gesamtzahl der Byte, die noch nicht an den Zielreplikationsserver übertragen wurden.

Geschätzte Fertigstellung in Prozent
: Die geschätzte Fertigstellung in Prozent auf der Basis der Anzahl der Byte.

Geschätzte verbleibende Zeit
: Die geschätzte verbleibende Zeit bis zum Abschluss des Knotenreplikationsprozesses.

Geschätzte Zeit der Fertigstellung
: Die geschätzte Zeit, zu der der Knotenreplikationsprozess beendet sein wird.

Tabelle 1. Zugehörige Befehle für QUERY REPLICATION

Befehl	**Beschreibung**
CANCEL REPLICATION	Bricht Knotenreplikationsprozesse ab.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY REPLNODE	Zeigt Informationen zum Replikationsstatus eines Clientknotens an.
QUERY REPLRULE	Zeigt Informationen zu Knotenreplikationsregeln an.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
SET REPLRETENTION	Gibt den Aufbewahrungszeitraum für Replikationsprotokollsätze an.

QUERY REPLNODE (Informationen zum Replikationsstatus für einen Clientknoten anzeigen)

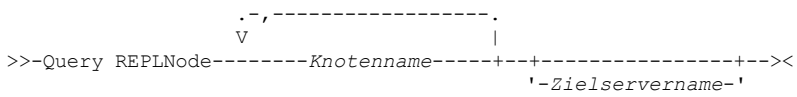
Verwenden Sie diesen Befehl, um die Anzahl der Dateien anzuzeigen, die für jeden replizierten Dateibereich gespeichert werden. Informationen werden zu Dateibereichen für jeden Clientknoten angezeigt, der für die Replikation konfiguriert ist.

Ein Clientknoten ist für die Replikation konfiguriert, wenn er aktiviert oder inaktiviert ist.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Knotenname (Erforderlich)

Gibt den Clientknoten an, der der Eigner der Dateien ist, zu denen Informationen angezeigt werden sollen. Sie können einen oder mehrere Namen angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen. Verwenden Sie zwischen den Namen keine Leerzeichen. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben.

Informationen zu Clientknoten, die den Dateikriterien entsprechen, aber nicht für die Replikation konfiguriert sind, werden nicht angezeigt.

Zielservername

Gibt den Namen des Replikationsservers an, der nach Replikationsinformationen abgefragt werden soll. Dieser Parameter ist wahlfrei. Wenn Sie keinen Wert für diesen Parameter angeben, wird der Server, der das Standardziel für replizierte Daten ist, abgefragt.

Als Wert für diesen Parameter können Sie auch einen Server angeben, der früher ein Ziel für replizierte Daten war.

Die Clientknoten, die für einen Replikationsserver definiert sind, können die Quelle oder das Ziel der replizierten Daten sein. Um zu bestimmen, ob ein bestimmter Clientknoten Daten sendet oder empfängt, geben Sie den Befehl QUERY NODE aus. Suchen Sie im Feld 'Replikationsmodus' der Ausgabe nach dem Wert *Send* oder *Receive*.

Um den Namen des aktiven Zielreplikationsservers anzuzeigen, geben Sie den Befehl QUERY STATUS aus und suchen Sie den Namen im Feld 'Zielreplikationsserver'.

Beispiel: Clientknotendateien auf einem Quellen- und einem Zielreplikationsserver auflisten

Der Name des Clientknotens ist NODE1.

```
query replnode *

Knoten- Typ    Dateiber.- FSID  Dateien    Replikations- Dateien
name           Name             auf Server server (1)    auf Server (1)
-------------------------------------------------------------------------
NODE1  SpMg    /hmsmfs    1      1
NODE1  Bkup    /lspace2   2      27
NODE1  Arch    /lspace2   2      22        TGTSRV        22
NODE1  Bkup    /lspace    3      18.096
NODE1  Arch    /lspace    3      61.150    TGTSRV        61.150
NODE2
```

Die Anzahl der Dateien, die für die Replikationsserver angezeigt werden, kann aus folgenden Gründen abweichen:

- Die Ausgabe des Befehls QUERY REPLNODE zeigt die Anzahl der Dateien an, die aus der Belegungstabelle abgerufen wurden. Die Belegungstabelle enthält nur Dateien, die eine Länge größer als Null haben. Dateien, die die Länge 0 haben und repliziert wurden, werden in dieser Ausgabe nicht wiedergespiegelt.
- Wenn nur aktive Daten auf den Zielserver repliziert werden, ist die Anzahl der Dateien, die für den Quelllenserver angezeigt werden, größer als die Anzahl der Dateien, die auf dem Zielserver angezeigt werden. Die Ursache für die Abweichung liegt darin, dass der Quellenreplikationsserver sowohl über aktive als auch über inaktive Daten und der Zielserver nur über aktive Daten verfügt.
- Ein Clientknoten kann über Daten verfügen, die vom Quellenreplikationsserver exportiert und auf den Zielreplikationsserver importiert wurden. Wenn diese Daten synchronisiert wurden und wenn der Clientknoten auch Daten auf dem Zielreplikationsserver gespeichert hat, ist die Anzahl der Dateien auf dem Zielreplikationsserver größer als die Anzahl der Dateien, die infolge von Export- und Importoperationen und der Replikation gespeichert wurden.

- Wenn Sie Knotendaten von einem Quellenserver mit einer Version vor Version 7.1 auf einen Zielserver mit Version 7.1 oder höher replizieren, werden Dateien mit mehr als 10 GB in kleinere Dateien aufgeteilt, wenn der Parameter SPLITLARGEOBJECTS für die Knotendefinition auf `Yes` gesetzt ist. Alle diese Teildateien werden auf dem Zielserver gezählt.

Feldbeschreibungen

Knotenname
: Der Name des Clientknotens, der der Eigner der Dateien ist.

Typ
: Der Datentyp. Ist dieses Feld leer, ist der Clientknoten für die Replikation konfiguriert, aber er verfügt über keine Daten auf dem Replikationsserver. In der Beispielausgabe ist NODE2 für die Replikation konfiguriert, aber der Knoten verfügt über keine Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten.

  Die folgenden Werte sind gültig:

  Arch
  : Archivierungsdaten

  Bkup
  : Sicherungsdaten

  SpMg
  : Daten, die von IBM Spectrum Protect for Space Management-Clients umgelagert wurden

Dateibereichsname
: Der Name des Dateibereichs, der zu dem Knoten gehört.

  Ist dieses Feld leer, ist der Clientknoten für die Replikation konfiguriert, aber er verfügt über keine Daten auf dem Replikationsserver.

  Dateibereichsnamen können eine andere Zeichenumsetztabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

  Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

FSID
: Die Dateibereichs-ID des Dateibereichs. Der Server ordnet eine eindeutige FSID zu, wenn ein Dateibereich zum ersten Mal auf dem Server gespeichert wird. Ist dieses Feld leer, ist der Clientknoten für die Replikation konfiguriert, aber er verfügt über keine Daten auf dem Replikationsserver.

Dateien auf Server
: Die Anzahl der Sicherungsdateien, Archivierungsdateien und speicherverwalteten Dateien auf dem Server, auf dem dieser Befehl ausgegeben wird. Ist dieses Feld leer, ist der Clientknoten für die Replikation konfiguriert, aber er verfügt über keine Daten auf dem Replikationsserver.

Replikationsserver (1)
: Der Name des Replikationsservers, der nach Informationen abgefragt wird. Ist dieses Feld leer, können eine oder mehrere der folgenden Bedingungen vorhanden sein:

  - Der Dateibereich des Knotens auf dem Replikationsserver, auf dem der Befehl ausgegeben wurde, verfügt über keine Daten.
  - Der Clientknoten ist nicht auf dem Replikationsserver (1) definiert.
  - Der Clientknoten ist auf dem Replikationsserver (1) definiert, aber der Knoten ist nicht für die Replikation konfiguriert.
  - Der entsprechende Dateibereich auf dem Replikationsserver (1) verfügt über keine Daten oder der Dateibereich ist nicht definiert.

Dateien auf Server (1)
: Die Anzahl der Dateien für den Datentyp, die auf dem Zielreplikationsserver gespeichert sind. Dieses Feld kann leer sein. Ist dies der Fall, können eine oder mehrere der folgenden Bedingungen vorhanden sein:

  - Der Replikationsserver (1) verfügt über keine Daten.
  - Der Clientknoten ist nicht auf dem Replikationsserver (1) definiert.
  - Der Clientknoten ist auf dem Replikationsserver (1) definiert, aber der Knoten ist nicht für die Replikation konfiguriert.
  - Der entsprechende Dateibereich auf dem Replikationsserver (1) verfügt über keine Daten oder der Dateibereich ist nicht definiert.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REPLNODE

Befehl	Beschreibung

Befehl	Beschreibung
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY REPLRULE	Zeigt Informationen zu Knotenreplikationsregeln an.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
UPDATE REPLRULE	Aktiviert oder inaktiviert Replikationsregeln.

QUERY REPLRULE (Replikationsregeln abfragen)

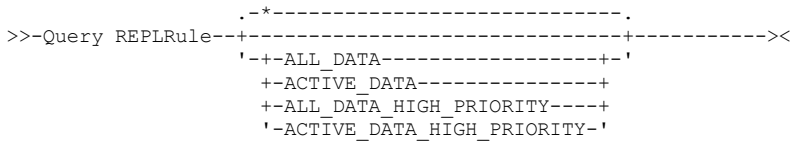
Verwenden Sie diesen Befehl, um Informationen zu Replikationsregeln anzuzeigen.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Parameter

Regelname
: Gibt den Namen der Replikationsregel an, zu der Informationen angezeigt werden sollen. Dieser Parameter ist wahlfrei. Sie können Platzhalterzeichen verwenden, um eine oder mehrere Regeln anzugeben. Wenn Sie diesen Parameter nicht angeben, werden Informationen zu allen Regeln in der Ausgabe der Abfrage angezeigt. Sie können die folgenden Werte angeben:

  ALL_DATA
  : Zeigt Informationen zu der Replikationsregel ALL_DATA an. Mit dieser Regel werden Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten repliziert. Die Daten werden mit einer normalen Priorität repliziert.

  ACTIVE_DATA
  : Zeigt Informationen zu der Replikationsregel ACTIVE_DATA an. Mit dieser Regel werden nur aktive Sicherungsdaten repliziert. Die Daten werden mit einer normalen Priorität repliziert. Diese Regel ist für Archivierungsdaten oder speicherverwaltete Daten nicht gültig.
    Achtung: Wenn Sie ACTIVE_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

    - Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
    - Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
    - Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

    Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

  ALL_DATA_HIGH_PRIORITY
  : Zeigt Informationen zu der Regel ALL_DATA_HIGH_PRIORITY an. Mit dieser Regel werden Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten repliziert. Die Daten werden mit einer normalen Priorität repliziert. In einem Replikationsprozess werden Daten mit hoher Priorität vor Daten mit normaler Priorität repliziert.

  ACTIVE_DATA_HIGH_PRIORITY

Zeigt Informationen zu der Regel ACTIVE_DATA_HIGH_PRIORITY an.

Diese Regel entspricht der Replikationsregel ACTIVE_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

Beispiel: Informationen zu einer Serverreplikationsregel anzeigen

Der Name der Regel lautet ALL_DATA_HIGH_PRIORITY.

```
query replrule all_data_high_priority

Name der Replikationsregel: ALL_DATA_HIGH_PRIORITY
                       Zielreplikationsserver:
                                   Nur aktive: No
Aktiviert: Ja
```

Feldbeschreibungen

Name der Replikationsregel
: Gibt den Namen der Regel an, die abgefragt wurde.

Zielreplikationsserver
: Gibt den Namen des Zielreplikationsservers an.

Nur aktive
: Gibt an, ob die Regel nur für aktive Sicherungsdaten gilt. Die folgenden Werte sind gültig:

  Yes
  : Gibt an, dass nur aktive Sicherungsdaten für Dateibereiche repliziert werden, denen diese Regel zugeordnet ist.

  No
  : Gibt an, dass alle Sicherungsdaten für Dateibereiche repliziert werden, denen diese Regel zugeordnet ist.

Aktiviert
: Gibt an, ob die Regel aktiviert oder inaktiviert ist. Die folgenden Werte sind gültig:

  Yes
  : Gibt an, dass die Regel für die Replikation aktiviert ist. Daten in Dateibereichen, denen die Regel zugeordnet ist, werden repliziert.

  No
  : Gibt an, dass die Regel nicht für die Replikation aktiviert ist. Daten in Dateibereichen, denen die Regel zugeordnet ist, werden nicht repliziert.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REPLRULE

Befehl	Beschreibung
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY REPLNODE	Zeigt Informationen zum Replikationsstatus eines Clientknotens an.
UPDATE REPLRULE	Aktiviert oder inaktiviert Replikationsregeln.

QUERY REPLSERVER (Replikationsserver abfragen)

Verwenden Sie diesen Befehl, um Informationen zu allen Replikationsservern anzuzeigen, die dem Server bekannt sind. Die Ausgabe dieses Befehls schließt Serverinformationen für den Server ein, auf dem der Befehl ausgegeben wurde. Der Befehl gibt an, ob eine Replikationsserverdefinition als Ergebnis eines Befehls REMOVE REPLSERVER gelöscht wird.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                    .-*----------.
>>-Query REPLServer--+------------+---------------------------><
                    '-Servername-'
```

Beispiel: Übersichtsstatistik zu allen Replikationsservern anzeigen

Informationen zum Replikationsserver anzeigen. Den Befehl entweder auf dem Quellen- oder dem Zielreplikationsserver ausgeben:

```
query replserver *

Global eindeutige Replikations-ID: 4d.83.fc.30.67.c1.11.e1.b8.
                                   40.f0.de.f1.5e.f1.89
                               Servername: Server1
                        Letzte Replikation:
                        Überwachungssignal:
      Adresse höherer Ebene für Übernahme: server1.example.com
        TCP-Anschlussnummer für Übernahme: 1500
        SSL-Anschlussnummer für Übernahme: 1542
                              Löschen aktiv: No
                     Ungleiche Maßnahmen:

        Global eindeutige Replikations-ID: 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.27.00.58.dc
                               Servername: DRServer1
                        Letzte Replikation: 06/30/2012 08:16:30 PM
                        Überwachungssignal: 07/09/2012 22:15:22 PM
      Adresse höherer Ebene für Übernahme: drserver1.example.com
        TCP-Anschlussnummer für Übernahme: 1500
        SSL-Anschlussnummer für Übernahme: 1542
                              Löschen aktiv: No
                     Ungleiche Maßnahmen: On
        Global eindeutige Replikations-ID: 90.4f.53.b0.8e.cb.11.e3.a8.
                                           2f.00.14.5e.55.b3.67
                                     Servername: DRSERVER2
                                                Letzte Replikation: 04/01/14   12:38:28
                                Überwachungssignal: 05/29/14   11:15:44
        Adresse höherer Ebene für Übernahme: drserver2.example.com
        TCP-Anschlussnummer für Übernahme: 1500
                SSL-Anschlussnummer für Übernahme:
                              Löschen aktiv: No
                                           Ungleiche Maßnahmen: Off
```

Beispiel: Übersichtsstatistik zu einem bestimmten Replikationsserver anzeigen

Informationen zum Replikationsserver DRServer1 anzeigen. Den Befehl entweder auf dem Quellen- oder dem Zielreplikationsserver ausgeben:

```
query replserver drserver1

Global eindeutige Replikations-ID: 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.27.00.58.dc
                               Servername: DRServer1
                        Letzte Replikation: 06/30/2012 08:16:30 PM
                        Überwachungssignal: 07/09/2012 22:15:22 PM
      Adresse höherer Ebene für Übernahme: drserver1.example.com
        TCP-Anschlussnummer für Übernahme: 1500
        SSL-Anschlussnummer für Übernahme: 1542
                              Löschen aktiv: No
                     Ungleiche Maßnahmen: On
```

Parameter

Servername
: Gibt den Namen des Replikationsservers an, der abgefragt werden soll. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Alle übereinstimmenden Server werden abgefragt. Wird kein Wert für diesen Parameter angegeben, werden alle Server abgefragt. Der Parameter ist wahlfrei.

Feldbeschreibungen

Global eindeutige Replikations-ID
: Die eindeutige ID für den IBM Spectrum Protect-Server. Die Werte für die global eindeutige Replikations-ID werden erstellt, wenn ein Server zum ersten Mal in einem Replikationsprozess verwendet wird.
Tipp: Die im Feld 'Global eindeutige Replikations-ID' aufgelistete ID ist nicht mit dem Wert für die ID im Feld 'Maschinen-GUID' identisch, das im Befehl QUERY STATUS angezeigt wird.

Servername
: Der Name des Replikationsservers.

Letzte Replikation
: Das Datum des letzten Replikationsprozesses, in dem der Server verwendet wurde.

Überwachungssignal
: Das letzte Mal, dass der Server eine erfolgreiche Testkommunikationssitzung beendet hat.

TCP-Anschlussnummer für Übernahme
: Der aktive TCP-Clientanschluss (TCP = Transmission Control Protocol) auf dem Replikationsserver, der für Clientverbindungen verwendet wird. Wenn der Client für TCP konfiguriert ist, wird der Anschluss verwendet, um die Verbindung zum Übernahmeserver herzustellen.

SSL-Anschlussnummer für Übernahme
: Der aktive SSL-Anschluss (SSL = Secure Sockets Layer) auf dem Replikationsserver, der für Clientverbindungen verwendet wird. Wenn der Client für SSL konfiguriert ist, wird der Anschluss verwendet, um die Verbindung zum Übernahmeserver herzustellen.

Adresse höherer Ebene für Übernahme

Die Adresse der höheren Ebene, die der Client verwendet, um während einer Übernahme die Verbindung zum Replikationsserver herzustellen.

Löschen aktiv
: Gibt an, ob ein Befehl REMOVE REPLSERVER für diesen Replikationsserver ausgegeben wurde und der Befehl noch ausgeführt wird. Die folgenden Werte sind gültig:

  Yes
  : Das Löschen des Replikationsservers ist aktiv.

  No
  : Das Löschen des Replikationsservers ist nicht aktiv.

Ungleiche Maßnahmen
: Gibt an, ob die Maßnahmen, die auf dem Zielreplikationsserver definiert sind, aktiviert sind. Die folgenden Werte sind gültig:

  On
  : Die Maßnahmen auf dem Zielreplikationsserver verwalten replizierte Clientknotendaten.

  Off
  : Die Maßnahmen auf dem Quellenreplikationsserver verwalten replizierte Clientknotendaten.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REPLSERVER

Befehl	Beschreibung
REMOVE REPLNODE (Clientknoten aus Replikation entfernen)	Entfernt einen Knoten aus der Replikation.
REMOVE REPLSERVER (Replikationsserver entfernen)	Entfernt einen Server aus der Replikation.

QUERY REQUEST (Anstehende Ladeanforderungen abfragen)

Verwenden Sie den Befehl QUERY REQUEST, um Informationen über eine oder mehrere anstehende Ladeanforderungen anzuzeigen. Der Server gibt Anforderungen an den Administrator zum Ausführen einer Aktion aus, wie beispielsweise zum Einlegen eines Banddatenträgers in ein Kassettenarchiv, nachdem ein Befehl CHECKIN LIBVOL ausgegeben wurde.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query REQuest--+--------------------+-----------------------><
                  '-Anforderungsnummer-'
```

Parameter

Anforderungsnummer
: Gibt die Identifikationsnummer der anstehenden Ladeanforderung an. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle anstehenden Ladeanforderungen.

Beispiel: Alle anstehenden Ladeanforderungen auflisten

Informationen zu allen anstehenden Ladeanforderungen anzeigen, nachdem ein Befehl CHECKIN LIBVOL ausgegeben wurde.

```
query request
```

Ausgabe für ein manuelles Kassettenarchiv

AIX-Betriebssysteme

```
ANR8352I Ausstehende Anforderungen:
ANR8326I 001: 8MM Datenträger EXP001 R/W
in Laufwerk 8MM.1 (/dev/mt0) des Kassettenarchivs
MANUALLIB innerhalb von 60 Minuten laden.
```

Linux-Betriebssysteme

```
ANR8352I Ausstehende Anforderungen:
ANR8326I 001: 8MM Datenträger EXP001 R/W
```

```
in Laufwerk 8MM.1 (/dev/mt0) des Kassettenarchivs
MANUALLIB innerhalb von 60 Minuten laden.
```

Windows-Betriebssysteme

```
ANR8352I Ausstehende Anforderungen:
ANR8326I 001: GENERICTAPE Datenträger EXP001 R/W
in Laufwerk 8MM.1 (mt3.0.0.0) des Kassettenarchivs
MANUALLIB innerhalb von 60 Minuten laden.
```

Ausgabe für ein automatisiertes Kassettenarchiv

AIX-Betriebssysteme Windows-Betriebssysteme

```
ANR8352I Ausstehende Anforderungen:
ANR8306I 001: LTO-Datenträger 133540L5 R/W in den Schacht mit Elementnummer
 31 des Kassettenarchivs LTOLIB innerhalb von 60 Minuten einlegen; wenn bereit, 'REPLY'
 mit der Anforderungs-ID ausgeben.
```

Linux-Betriebssysteme

```
ANR8352I Ausstehende Anforderungen:
ANR8306I 001: 3590 Datenträger 133540 R/W in den Schacht mit Elementnummer
 31 des Kassettenarchivs 3590LIB innerhalb von 60 Minuten einlegen; wenn bereit, 'REPLY'
 mit der Anforderungs-ID ausgeben.
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REQUEST

Befehl	Beschreibung
CANCEL REQUEST	Bricht anstehende Datenträgerladeanforderungen ab.
REPLY	Erlaubt einer Anforderung, die Verarbeitung fortzusetzen.

QUERY RESTORE (Wiederanlauffähige Zurückschreibungssitzungen abfragen)

Mit diesem Befehl können Informationen über die wiederanlauffähigen Zurückschreibungssitzungen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query--RESTore--+------------+--+-------------------+-------->
                   '-Knotenname-'  '-Dateibereichsname-'

   .-Format--=--Standard-----.  .-NAMEType--=--SERVER------.
>--+-------------------------+--+--------------------------+--><
   '-Format--=--+-Standard-+-'  '-NAMEType--=--+-SERVER--+-'
                '-Detailed-'                   +-UNIcode-+
                                               '-FSID----'
```

Parameter

Knotenname
: Gibt den Clientknoten an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden alle Clientknoten mit wiederanlauffähigen Zurückschreibungssitzungen angezeigt. Für diesen Parameter muss ein Wert angegeben werden, wenn ein Dateibereichsname angegeben wird.

Dateibereichsname
: Gibt den Dateibereich an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden alle Dateibereiche für den angegebenen Knoten abgeglichen.

  Ein Server, der über Clients mit Unterstützung für Unicode verfügt, muss möglicherweise den Dateibereichsnamen, den Sie eingeben, konvertieren. Beispielsweise muss der Server gegebenenfalls den Namen, den Sie eingeben, aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich unter dem Parameter NAMETYPE.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard

Gibt an, dass Teilinformationen angezeigt werden.

Detailed
: Gibt an, dass die gesamten Informationen angezeigt werden.

NAMEType
: Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode verfügt. Sie können diesen Parameter für IBM Spectrum Protect-Clients mit Unicode-Unterstützung angeben, die die Betriebssysteme Windows, Macintosh OS 9, Macintosh OS X und NetWare verwenden.

  Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Gültige Werte:

  SERVER
  : Der Server verwendet die Zeichenumsetztabelle des Servers, um die Dateibereichsnamen zu interpretieren.

  UNIcode
  : Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server Probleme beim Zugriff auf die Systemkonvertierungsroutinen hat.

  FSID
  : Der Server interpretiert die Dateibereichsnamen als ihre Dateibereichs-IDs (FSIDs).

Beispiel: Eine wiederanlauffähige Zurückschreibungssitzung für einen bestimmten Clientknoten anzeigen

Zeigen Sie ausführliche Informationen zum Clientknoten JAMES an, der dem Dateibereich DRIVE_F_R zugeordnet ist. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query restore james drive_f_r format=detailed

    Sitzungsnummer: -1
  Zurückschreibungsstatus: Wiederanlauffähig
      Abgelaufene Minuten: 2
               Knotenname: JAMES
                     FSID: 1
       Dateibereichsname: DRIVE_F_R:
      Dateispezifikation: /RESTORE/TESTDIRF\\
```

Feldbeschreibungen

Sitzungsnummer
: Gibt die Sitzungsnummer für die wiederanlauffähige Zurückschreibungssitzung an. Die Nummer für aktive Zurückschreibungssitzungen entspricht der im Befehl QUERY SESSION angezeigten Nummer. Bei Zurückschreibungssitzungen im wiederanlauffähigen Status wird eine negative Zahl als Sitzungsnummer angezeigt. Alle in der Ausgabe des Befehls QUERY RESTORE angezeigten Sitzungsnummern können von der Ausgabe des Befehls QUERY RESTORE angegeben werden.

Zurückschreibungsstatus
: - Aktiv: Gibt an, dass die Zurückschreibungssitzung Dateien aktiv in den Client zurückschreibt.
  - Wiederanlauffähig: Gibt an, dass die Zurückschreibungssitzung fehlgeschlagen ist und an dem Unterbrechungspunkt erneut gestartet werden kann.

Abgelaufene Minuten
: Gibt die Anzahl Minuten seit dem Start der Zurückschreibungssitzung an. Alle wiederanlauffähigen Zurückschreibungssitzungen, deren abgelaufene Zeit größer als die Serveroption RESTOREINTERVAL ist, können bei Bedarf oder während der Verfallsverarbeitung automatisch aus der Datenbank gelöscht werden. Ist die abgelaufene Zeit kürzer als RESTOREINTERVAL, kann dieser Eintrag nur gelöscht werden (und der Dateibereich freigegeben werden), indem der Befehl CANCEL RESTORE ausgegeben und der Wert für RESTOREINTERVAL herabgesetzt wird.

Knotenname
: Gibt den Knoten an, der der wiederanlauffähigen Zurückschreibungssitzung zugeordnet ist.

FSID
: Gibt die Dateibereichs-ID des Dateibereichs an.

Dateibereichsname
: Gibt den Dateibereich an, der der wiederanlauffähigen Zurückschreibungssitzung zugeordnet ist.

  Dateibereichsnamen können eine andere Zeichenumsetztabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

  Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann

unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

Dateispezifikation
Gibt die Dateispezifikation an, die in der Operation zum Zurückschreiben verwendet wird. Dieselbe Dateispezifikation muss angegeben werden, wenn eine fehlgeschlagene Operation zum Zurückschreiben an ihrem Unterbrechungspunkt erneut gestartet werden soll.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY RESTORE

Befehl	Beschreibung
CANCEL RESTORE	Bricht eine wiederanlauffähige Zurückschreibungssitzung ab.

QUERY RPFCONTENT (Inhalt der auf Zielserver gespeicherten Plandatei abfragen)

Verwenden Sie diesen Befehl, um den Inhalt einer Wiederherstellungsplandatei anzuzeigen, die auf einem Zielserver gespeichert ist (d. h., wenn der Parameter DEVCLASS im Befehl PREPARE angegeben wurde). Dieser Befehl kann entweder von dem Server, der die Datei erstellt hat (Quellen-Server), oder von dem Server, auf dem die Wiederherstellungsplandatei gespeichert ist (Ziel-Server), ausgegeben werden. Dieser Befehl kann nicht über die Server-Konsole ausgegeben werden.

Die Ausgabe kann sich verzögern, wenn sich die Datei auf Band befindet.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Query RPFContent--Plandateiname------------------------------>

>--+-DEVclass----Einheitenklassenname-+---------------------><
   '-NODEName---=--Knotenname-----------'
```

Parameter

Plandateiname (Erforderlich)
Gibt den Namen der Wiederherstellungsplandatei an, die abgefragt werden soll. Das Format des Dateinamens lautet servername.yyyymmdd.hhmmss. Sollen die Namen von vorhandenen Dateien angezeigt werden, den Befehl QUERY RPFILE ausgeben.

DEVclass
Gibt den Namen der Einheitenklasse an, die zum Erstellen der Wiederherstellungsplandatei verwendet wurde. Platzhalterzeichen sind nicht zulässig.
Diesen Parameter angeben, wenn

- der Inhalt der Wiederherstellungsplandatei angezeigt werden soll, die für diesen Server erstellt wurde.
- Dieser Befehl wird für denselben Server ausgegeben, auf dem der Befehl PREPARE ausgegeben wurde (Quellenserver).
- Der angegebene Einheitenklassenname wurde in dem Befehl PREPARE verwendet, mit dem die Wiederherstellungsplandatei erstellt wurde.

NODEName
Gibt den auf dem Ziel-Server registrierten Knotennamen des Quellen-Servers an, der die Wiederherstellungsplandatei erstellt hat. Platzhalterzeichen sind nicht zulässig.
Diesen Parameter angeben, wenn

- der Inhalt der Wiederherstellungsplandatei angezeigt werden soll, die auf diesem Server gespeichert war.
- dieser Befehl für den Server ausgegeben wird, der das Ziel des Befehls PREPARE war, der die Wiederherstellungsplandatei erstellt hat.
- der angegebene Knotenname auf diesem Server mit der Knotenart SERVER registriert ist.
- der IBM Spectrum Protect-Server, der die Wiederherstellungsplandatei erstellt hat, nicht verfügbar ist.

Beispiel: Den Wiederherstellungsplan für den Quellenserver anzeigen

Auf dem Quellenserver den Inhalt einer Wiederherstellungsplandatei anzeigen, die für diesen Server am 19. März 1998 um 6:10 Uhr erstellt wurde. Der Befehl PREPARE gibt die Einheitenklasse REMOTE an. Die Ausgabe dieses Befehls ist der gesamte Inhalt der Wiederherstellungsplandatei.

```
query rpfcontent branch1.19980319.061000 devclass=remote
```

Beispiel: Den Wiederherstellungsplan für den Zielserver anzeigen

Auf dem Zielserver den Inhalt einer Wiederherstellungsplandatei anzeigen, die auf diesem Server am 19. März 1998 um 6:10 Uhr gespeichert wurde. Der Server, der die Datei erstellt hat, ist auf dem Zielserver als Knoten POLARIS mit der Knotenart SERVER registriert. Die Ausgabe dieses Befehls ist der gesamte Inhalt der Wiederherstellungsplandatei.

```
query rpfcontent branch1.19980319.061000 nodename=polaris
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY RPFCONTENT

Befehl	Beschreibung
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY RPFILE	Zeigt Informationen über Wiederherstellungsplandateien an.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.

Zugehörige Informationen:

Wiederherstellungsplandatei

QUERY RPFILE (Auf Zielserver gespeicherte Infos über Plandateien abfragen)

Mit diesem Befehl können Informationen über Wiederherstellungsplandateien angezeigt werden, die auf einem Ziel-Server gespeichert sind. Dieser Befehl kann entweder von dem Server, der die Datei erstellt hat (Quellen-Server), oder von dem Server, auf dem die Wiederherstellungsplandatei gespeichert ist (Ziel-Server), ausgegeben werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query RPFile--+-DEVclass----Einheitenklassenname-+---------->
                 '-NODEName----Knotenname-----------'

   .-Source--=--DBBackup-------.  .-Format--=--Standard-----.
>--+---------------------------+--+-------------------------+-->
   '-Source--=--+-DBBackup---+-'  '-Format--=--+-Standard-+-'
                '-DBSnapshot-'                 '-Detailed-'
```

Parameter

DEVclass
: Gibt den Namen der Einheitenklasse an, die zum Erstellen der Wiederherstellungsplandateien verwendet wurde. Diesen Parameter verwenden, wenn die Anmeldung an dem Server erfolgte, der die Wiederherstellungsplandatei erstellt hat. Es können Platzhalterzeichen in dem Namen der Einheitenklasse verwendet werden. Alle Wiederherstellungsplandateien, die mit der angegebenen Einheitenklasse erstellt werden, werden in der Abfrage berücksichtigt.

NODEName
: Gibt den auf dem Ziel-Server registrierten Knotennamen des Quellen-Servers an, der die Wiederherstellungsplandateien erstellt hat. Diesen Parameter verwenden, wenn die Anmeldung an dem Ziel-Server erfolgte. Dieser Parameter kann verwendet werden, wenn der Quellen-Server nicht verfügbar ist. Es können Platzhalterzeichen verwendet werden, um den Knotennamen anzugeben. Alle Dateiobjekte, die mit dem angegebenen Knotennamen gespeichert sind, werden in dieser Abfrage berücksichtigt.

Source
: Gibt die Art der Datenbanksicherung an, die bei der Vorbereitung der Wiederherstellungsplandatei angegeben wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBACKUP. Gültige Werte:

  DBBackup
  : Die Wiederherstellungsplandatei wurde mit angegebenen Gesamtsicherungen und Teilsicherungen der Datenbank vorbereitet.

  DBSnapshot
  : Die Wiederherstellungsplandatei wurde mit angegebenen Datenbankmomentaufnahmesicherungen vorbereitet.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard

Zeigt Teilinformationen für die Wiederherstellungsplandatei an.

Detailed
: Zeigt alle Informationen für die Wiederherstellungsplandatei an.

Beispiel: Ausführliche Informationen zu den Wiederherstellungsplänen anzeigen

Wiederherstellungsplandateien anzeigen, die für diesen Server unter Verwendung der angegebenen Einheitenklasse erstellt wurden. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query rpfile devclass=* format=detailed


     Name der Wiederherstellungsplandatei: ALASKA.20000406.170423
                                Knotenname: BRANCH1
                    Einheitenklassenname: REMOTE
      Art der Wiederherstellungsplandatei: RPFILE
                  Verwaltungsklassenname: STANDARD
    Größe der Wiederherstellungsplandatei: 16,255 Bytes
                    Zum Löschen markiert: Yes
                                Löschdatum: 06/12/2000 13:05:31

     Name der Wiederherstellungsplandatei: ALASKA.20000407.170845
                                Knotenname: BRANCH1
                    Einheitenklassenname: REMOTE
      Art der Wiederherstellungsplandatei: RPFSNAPSHOT
                  Verwaltungsklassenname: STANDARD
    Größe der Wiederherstellungsplandatei: 16.425 Byte
                    Zum Löschen markiert: No
                                Löschdatum:
```

Beispiel: Eine Liste der Wiederherstellungspläne für einen bestimmten Knotennamen anzeigen

Eine Liste aller Wiederherstellungsplandateiobjekte anzeigen, die mit dem angegebenen Knotennamen (TYPE=SERVER) gespeichert sind. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query rpfile nodename=branch1

    Wiederherstellungsplandatei   Knotenname      Einheitenklassenname
    ----------------------------  ---------       ------------------
     ALASKA.19980406.170423         BRANCH1         REMOTE
     ALASKA.19980407.170845         BRANCH1         REMOTE
```

Feldbeschreibungen

Name der Wiederherstellungsplandatei
: Der Name der Wiederherstellungsplandatei.

Knotenname
: Der Knotenname, der mit dem Zielserver registriert ist und zum Speichern der Wiederherstellungsplandateiobjekte verwendet wird.

Einheitenklassenname
: Der Einheitenklassenname, der im Quellenserver definiert ist und zum Erstellen der Wiederherstellungsplandateien verwendet wird.

Art der Wiederherstellungsplandatei
: Die Art der Wiederherstellungsplandatei:

  RPFILE
  : Der Plan nimmt Gesamt- und Teilsicherungen der Datenbank an.

  RPFSNAPSHOT
  : Der Plan nimmt Datenbankmomentaufnahmesicherungen an.

Verwaltungsklassenname
: Der Name der Verwaltungsklasse, der die Wiederherstellungsplandatei auf dem Ziel-Server zugeordnet ist.

Größe der Wiederherstellungsplandatei
: Die geschätzte Größe des Wiederherstellungsplandateiobjekts auf dem Ziel-Server.

Zum Löschen markiert
: Die Angabe, ob das Objekt, das die Wiederherstellungsplandatei enthält, auf dem Quellen-Server gelöscht und auf dem Ziel-Server zum Löschen markiert wurde, wenn der Aufbewahrungszeitraum noch nicht abgelaufen ist. Gültige Werte:

  Yes
  : Das Objekt ist zum Löschen markiert.

  No
  : Das Objekt ist nicht zum Löschen markiert.

Löschdatum
: Das Datum, an dem das Objekt auf dem Quellen-Server gelöscht und auf dem Ziel-Server zum Löschen markiert wurde. Dieses Feld bleibt leer, wenn das Objekt nicht zum Löschen markiert wurde.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY RPFILE

Befehl	Beschreibung
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.
QUERY RPFCONTENT	Zeigt den Inhalt einer Wiederherstellungsplandatei an.

QUERY SAN (Einheiten in dem SAN abfragen)

Verwenden Sie diesen Befehl, um Informationen zu Einheiten abzurufen, die in einem SAN (Storage Area Network - Speicherbereichsnetz) erkannt werden können, so dass Sie IBM Spectrum Protect für die LAN-unabhängige Datenversetzung konfigurieren können.

 AIX-BetriebssystemeDer Befehl QUERY SAN erfordert die libhbaapi.a, die die allgemeine SNIA Host Bus Adapter (HBA) API unterstützt. Mit diesem Bibliotheksobjekt kann IBM Spectrum Protect die hbaapi-Funktionen aufrufen, die im allgemeinen SNIA HBAAPI-Standard angegeben sind.
 Windows-BetriebssystemeDer Befehl QUERY SAN erfordert die hbaapi.dll, die die allgemeine SNIA Host Bus Adapter (HBA) API unterstützt. Mit diesem Bibliotheksobjekt kann IBM Spectrum Protect die hbaapi-Funktionen aufrufen, die im allgemeinen SNIA HBAAPI-Standard angegeben sind.
 Linux-BetriebssystemeDer Befehl QUERY SAN erfordert die libhaapi.so, die die allgemeine SNIA Host Bus Adapter (HBA) API unterstützt. Mit diesem Bibliotheksobjekt kann IBM Spectrum Protect die hbaapi-Funktionen aufrufen, die im allgemeinen SNIA HBAAPI-Standard angegeben sind.
Mit dem Befehl QUERY SAN werden möglicherweise nicht alle Einheiten angezeigt, wenn die Serveroption SANDISCOVERY nicht auf ON gesetzt ist.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
              .-Type--=--Any---------.
>>-Query SAN--+----------------------+-------------------------->
              '-Type--=--+-Any-----+-'
                         +-DRive---+
                         '-LIBRary-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Type
: Gibt den Typ der Einheit an, die angezeigt wird. Dieser Parameter ist wahlfrei. Der Standardwert ist Any. Gültige Werte:

  Any
  : Gibt an, dass alle in dem SAN erkannten Einheiten angezeigt werden.

  DRive
  : Gibt an, dass nur Laufwerkeinheiten angezeigt werden.

  LIBRary
  : Gibt an, dass nur Kassettenarchiveinheiten angezeigt werden.

Format
: Gibt die Art der Informationen an, die angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist Standard. Gültige Werte:

  Standard
  : Gibt an, dass die angezeigten Informationen zusammengefasst werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

  Tipp: Die Ausgabe zeigt möglicherweise nicht die Seriennummer der Einheit an. Ist dies der Fall, suchen Sie die Seriennummer auf der Rückseite der Einheit oder fragen Sie den Hersteller der Einheit.

Beispiel: Laufwerkeinheiten auflisten

Übersichtsdaten für Laufwerkeinheiten in einem SAN anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query san type=drive
```

```
Einheitentyp     Lieferant     Produkt     Seriennummer     Einheit
-------------    ----------    ---------   ---------        ----------
LIBRARY     STK           L180          MPC01000128      /dev/smc1
DRIVE       STK           9840D       331001017229     /dev/rmt3
DRIVE            Quantum       DLT4000     JF62806275       /dev/rmt4
DRIVE            Quantum       DLT4000     JP73213185       /dev/rmt5
DRIVE       STK           9840D       331000028779     /dev/rmt6
```

Beispiel: Informationen zu Laufwerkeinheiten anzeigen

Ausführliche Informationen zu allen Laufwerkeinheiten in einem SAN anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query san type=drive format=detailed
```

```
                    Einheitentyp:   DRIVE
                                        Lieferant: IBM
                                          Produkt: 03570B02
                                     Seriennummer:
                                          Einheit: mt10.2.0.3
                  Einheit zum Versetzen von Daten: No
                                     Knoten-WWN: 5005076206039E05
                                  Anschluss-WWN: 5005076206439E05
                                            LUN: 0
                                 SCSI-Anschluss: 3
                                       SCSI-Bus: 0
                                      SCSI-Ziel: 10
```

Feldbeschreibungen

Einheitentyp
: Der Typ der Einheit, die angezeigt wird.

Lieferant
: Der Name des Lieferanten der Einheit.

Produkt
: Der Name des Produkts, der vom Lieferanten zugeordnet wird.

Seriennummer
: Die Seriennummer der Einheit.

Einheit
: Der Gerätedateiname der Einheit.

Einheit zum Versetzen von Daten
: Gibt an, ob die Einheit eine Einheit zum Versetzen von Daten ist.

Knoten-WWN
: Der weltweit verwendete Name (World Wide Name) der Einheit.

Anschluss-WWN
: Der weltweit verwendete Name (World Wide Name) der Einheit, der für den Anschluss spezifisch ist, mit dem die Einheit verbunden ist.

LUN
: Die Nummer der logischen Einheit (Logical Unit Number) der Einheit.

SCSI-Anschluss
: Der Anschluss des Fibre Channel (oder SCSI) Host Bus Adapter.

SCSI-Bus
: Der Bus der Host Bus Adapter-Karte.

SCSI-Ziel
: Die Zielnummer der Einheit.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SAN

Befehl	Beschreibung
DEFINE DATAMOVER	Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.

QUERY SCHEDULE (Zeitpläne abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Zeitpläne angezeigt werden.

Für den Befehl QUERY SCHEDULE sind zwei Formate möglich, abhängig davon, ob der Zeitplan für Clientoperationen oder für Verwaltungsbefehle gilt. Syntax und Parameter für jede Operation werden separat definiert. Abhängig davon, ob der Zeitplan eine klassische oder erweiterte Darstellung verwendet, können einige Optionen in der Abfrageanzeige leer sein.

Tabelle 1. Zugehörige Befehle für QUERY SCHEDULE

Befehl	Beschreibung
COPY SCHEDULE	Erstellt eine Kopie eines Zeitplans.
DEFINE SCHEDULE	Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.
UPDATE SCHEDULE	Ändert die Attribute eines Zeitplans.

- QUERY SCHEDULE (Clientzeitpläne abfragen)
  Mit diesem Befehl können Informationen über einen oder mehrere Clientzeitpläne angezeigt werden.
- QUERY SCHEDULE (Verwaltungszeitplan abfragen)
  Mit diesem Befehl können Informationen über einen oder mehrere Verwaltungszeitpläne angezeigt werden.

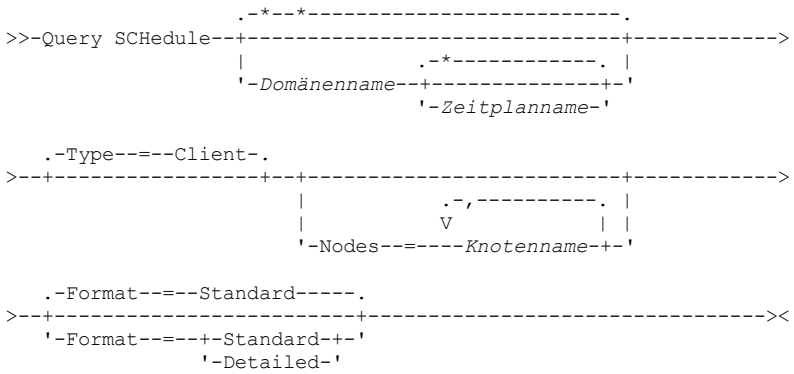
QUERY SCHEDULE (Clientzeitpläne abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Clientzeitpläne angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Domänenname
: Gibt den Namen der Maßnahmendomäne an, zu der der Zeitplan gehört. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.Wird ein Domänenname angegeben, ist kein Zeitplanname erforderlich.

Zeitplanname
: Gibt den Namen des Zeitplans an, der zur angegebenen Maßnahmendomäne gehört. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.Wird ein Zeitplanname angegeben, ist gleichzeitig auch ein Domänenname erforderlich.

Type=Client
: Gibt an, daß die Abfrage Client-Zeitpläne anzeigt. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT.

Nodes
: Gibt den Namen eines oder mehrerer Client-Knoten an, die den Zeitplänen zugeordnet sind, die angezeigt werden sollen. Dieser Parameter ist wahlfrei. Es kann ein Platzhalterzeichen verwendet werden, um Client-Knoten anzugeben. Wird kein Clientname angegeben, werden alle Zeitpläne, die mit den Parametern DOMAINNAME und SCHEDULENAME übereinstimmen, angezeigt. Es können mehrere Client-Knoten angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, daß Teilinformationen für die Zeitpläne angezeigt werden.

  Detailed

Gibt an, daß ausführliche Informationen für die Zeitpläne angezeigt werden.

Für erweiterte Zeitpläne zeigt das Standardformat ein Leerzeichen in der Spalte "Intervall" und einen Stern in der Spalte "Tag" an. Geben Sie FORMAT=DETAILED aus, um vollständige Informationen zu einem erweiterten Zeitplan anzuzeigen.

Beispiel: Zeitpläne für eine bestimmte Maßnahmendomäne auflisten

Alle Zeitpläne anzeigen, die zur Maßnahmendomäne EMPLOYEE_RECORDS gehören. Für Feldbeschreibungen siehe Feldbeschreibungen: Zeitpläne für eine bestimmte Maßnahmendomäne.

```
query schedule employee_records
```

Für erweiterte Zeitpläne zeigt das Standardformat ein Leerzeichen in der Spalte "Intervall" und einen Stern in der Spalte "Tag" an. Geben Sie FORMAT=DETAILED aus, um vollständige Informationen zu einem erweiterten Zeitplan anzuzeigen.

```
Domäne  * Zeitplanname    Aktion Start-      Dauer   Interv. Tag
                                 datum/-zeit
------- - --------------  ------ ----------  -------- ------ ---
EMPLOY    WEEKLY_BACKUP   Inc Bk 2004.06.04  1 H      1 D    Any
EE_RE-                           17.04.20
CORDS
EMPLOY-   EMPLOYEE_BACKUP Inc Bk 2004.06.04  1 H             (*)
EE_RE-                           17.04.20
CORDS
```

Feldbeschreibungen: Zeitpläne für eine bestimmte Maßnahmendomäne

Domäne
: Gibt den Namen der Maßnahmendomäne an, zu der der angegebene Zeitplan gehört.

* (Stern)
: Gibt an, ob ein Zeitplan abgelaufen ist. Steht in dieser Spalte ein Stern, ist der betreffende Zeitplan abgelaufen.

Zeitplanname
: Gibt den Namen des Zeitplans an.

Aktion
: Gibt die Aktion an, die bei der Verarbeitung dieses Zeitplans ausgeführt wird.

Startdatum/-zeit
: Gibt das/die anfängliche Startdatum/Uhrzeit für diesen Zeitplan an.

Dauer
: Gibt die Länge des Startfensters für diesen Zeitplan an.

Intervall
: Gibt die Zeit zwischen den Startfenstern an (bei DAYOFWEEK=ANY). Für erweiterte Zeitpläne ist die Spalte leer.

Tag
: Gibt den Wochentag an, an dem die Startfenster für den Zeitplan beginnen. Für erweiterte Zeitpläne enthält die Spalte einen Stern.

Beispiel: Ausführliche Clientzeitpläne anzeigen

Von einem verwalteten Server ausführliche Informationen über Clientzeitpläne anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen: Ausführliche Clientzeitpläne.

```
query schedule * type=client format=detailed
```

```
                     Name der Maßnahmendomäne: ADMIN_RECORDS
                        Zeitplanname: ADMIN_BACKUP
                                     Beschreibung:
                                   Aktion: Backup
                                Subaktion: vApp
                                 Optionen:
                                  Objekte:
                                Priorität: 5
                             Startdatum/-zeit: 04/06/2013 17.04.20
                                       Dauer: 1 Stunde
    Maximale Ausführungszeit (Minuten): 0
                   Zeitplandarstellung: Klassisch
                                      Intervall: 1 Tag(e)
                                Wochentag: Any
                                            Monat:
                          Tag des Monats:
                         Woche des Monats:
                                           Verfall:
              Letzte Aktualisierung durch
                              (Administrator): $$CONFIG_MANAGER$$
         Datum/Zeit der letzten Aktualisierung: 04/06/2013 17.51.49
                   Verwaltendes Profil: ADMIN_INFO

                        Name der Maßnahmendomäne: EMPLOYEE_RECORDS
                          Zeitplanname: EMPLOYEE_BACKUP
```

```
                                Beschreibung:
                              Aktion: Incremental
                                   Subaktion:
                             Optionen:
                              Objekte:
                             Priorität: 5
                       Startdatum/-zeit: 2004.06.04 17.04.33
                                 Dauer: 1 Stunde
    Maximale Ausführungszeit (Minuten): 0
                  Zeitplandarstellung: Erweitert
                                Intervall:
                             Wochentag: Any
                                 Monat: Mär,Jun,Nov
                       Tag des Monats: -14,14,22
                     Woche des Monats: Last
                                  Verfall:
            Letzte Aktualisierung durch
                          (Administrator): $$CONFIG_MANAGER$$
         Datum/Zeit der letzten Aktualisierung: 2004.06.04 17.18.30
                  Verwaltendes Profil: EMPLOYEE
```

Feldbeschreibungen: Ausführliche Clientzeitpläne

Name der Maßnahmendomäne
: Gibt den Namen der Maßnahmendomäne an.

Zeitplanname
: Gibt den Namen des Zeitplans an.

Beschreibung
: Beschreibung des Zeitplans.

Aktion
: Gibt die Art der Aktion an, die bei der Verarbeitung dieses Zeitplans ausgeführt wird. Eine Liste der Aktionen befindet sich unter dem Befehl DEFINE SCHEDULE.

Subaktion
: Gibt an, dass der Typ der Operation, der mit dem Parameter ACTION angegeben wird, geplant werden soll. Eine Liste der Subaktionen befindet sich unter dem Befehl DEFINE SCHEDULE.

Optionen
: Gibt die Optionen an, die dem Befehl DSMC geliefert werden, wenn der Zeitplan ausgeführt wird.

Objekte
: Gibt die Objekte an, für die die angegebene Aktion ausgeführt wird.

Priorität
: Gibt den Prioritätswert für den Zeitplan an.

Startdatum/-zeit
: Gibt das/die anfängliche Startdatum/Uhrzeit für den Zeitplan an.

Dauer
: Gibt die Länge des Startfensters für den Zeitplan an.

Maximale Ausführungszeit (Minuten)
: Gibt die Anzahl Minuten an, in denen alle Clientsitzungen, die von der geplanten Operation gestartet werden, abgeschlossen werden sollten. Sind Sitzungen nach Ablauf der maximalen Ausführungszeit noch aktiv, gibt der Server eine Warnung aus, aber die Ausführung der Sitzungen wird fortgesetzt.

Zeitplandarstellung
: Gibt an, ob klassische oder erweiterte Zeitplanregeln verwendet werden.

Intervall
: Gibt die Zeit zwischen den Startfenstern an (bei DAYOFWEEK=ANY). Diese Angabe wird für Zeitpläne mit erweiterter Syntax nicht angezeigt.

Wochentag
: Gibt den Wochentag an, an dem die Startfenster für den Zeitplan beginnen. Bei Verwendung eines Standardformats wird für erweiterte Zeitpläne im Feld 'Wochentag' ein Stern angezeigt.

Monat
: Gibt die Monate an, in denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.

Tag des Monats
: Gibt die Tage des Monats an, an denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.

Woche des Monats
: Gibt die Wochen (erste, zweite, dritte, vierte oder letzte) des Monats an, in denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.

Verfall
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der dieser Zeitplan abläuft. Ist diese Spalte leer, läuft der Zeitplan nicht ab.

Letzte Aktualisierung durch (Administrator)
: Gibt den Namen des Administrators an, der den Zeitplan zuletzt aktualisiert hat. Enthält dieses Feld $$CONFIG_MANAGER$$, ist der Zeitplan einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.

Datum/Zeit der letzten Aktualisierung
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Zeitplan zuletzt aktualisiert wurde.

Verwaltendes Profil
Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition dieses Zeitplans zu erhalten.

QUERY SCHEDULE (Verwaltungszeitplan abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Verwaltungszeitpläne angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                  .-*------------.
>>-Query SCHedule--+--------------+--Type--=--Administrative---->
                   '-Zeitplanname-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Zeitplanname
Gibt den Namen des Zeitplans an, der abgefragt werden soll. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.

Type=Administrative (Erforderlich)
Gibt an, daß die Abfrage Verwaltungszeitpläne anzeigt.

Format
Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard
Gibt an, daß Teilinformationen für die Zeitpläne angezeigt werden.

Detailed
Gibt an, daß ausführliche Informationen für die Zeitpläne angezeigt werden.

Für erweiterte Zeitpläne zeigt das Standardformat ein Leerzeichen in der Spalte "Intervall" und einen Stern in der Spalte "Tag" an. Geben Sie FORMAT=DETAILED aus, um vollständige Informationen zu einem erweiterten Zeitplan anzuzeigen.

Beispiel: Ausführliche Informationen zu Zeitplänen für Verwaltungsbefehle anzeigen

Von einem verwalteten Server ausführliche Informationen über Verwaltungszeitpläne anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query schedule * type=administrative
format=detailed
```

```
                                Zeitplanname: BACKUP_ARCHIVEPOOL
                                Beschreibung:
                                     Befehl: backup db
                                  Priorität: 5
                            Startdatum/-zeit: 2004.06.04 16.57.15
                                      Dauer: 1 Stunde
          Maximale Ausführungszeit (Minuten): 0
                        Zeitplandarstellung: Klassisch
                                  Intervall: 1 Tag(e)
                                  Wochentag: Any
                                      Monat:
                             Tag des Monats:
                           Woche des Monats:
                                    Verfall:
                                     Aktiv: No
    Letzte Aktualisierung durch Administrator: $$CONFIG MANAGER$$
        Datum/Zeit der letzten Aktualisierung: 2004.06.04 17.51.49
                        Verwaltendes Profil: ADMIN_INFO

                                Zeitplanname: MONTHLY_BACKUP
                                Beschreibung:
                                     Befehl: q status
                                  Priorität: 5
```

```
                          Startdatum/-zeit: 2004.06.04 16.57.14
                                    Dauer: 1 Stunde
        Maximale Ausführungszeit (Minuten): 0
                       Zeitplandarstellung: Erweitert
                                 Intervall:
                                 Wochentag: Die,Do,Fre
                                     Monat: Aug,Nov
                               Tag des Monats:
                              Woche des Monats: Second,Third
                                   Verfall:
                                     Aktiv: No
    Letzte Aktualisierung durch Administrator: $$CONFIG MANAGER$$
        Datum/Zeit der letzten Aktualisierung: 2004.06.04 17.51.49
                       Verwaltendes Profil: ADMIN_INFO
```

Feldbeschreibungen

Zeitplanname
: Gibt den Namen des Zeitplans an.

Beschreibung
: Beschreibung des Zeitplans.

Befehl
: Gibt den geplanten Befehl an.

Priorität
: Gibt den Prioritätswert für diesen Zeitplan an.

Startdatum/-zeit
: Gibt das/die anfängliche Startdatum/Uhrzeit für diesen Zeitplan an.

Dauer
: Gibt die Länge des Startfensters an.

Maximale Ausführungszeit (Minuten)
: Gibt die Anzahl Minuten an, in denen Serverprozesse, die von geplanten Befehlen gestartet werden, abgeschlossen werden müssen. Sind Prozesse nach Ablauf der maximalen Ausführungszeit noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.
  Tipps:

  - Dieser Parameter gilt nicht für einige Prozesse, wie z. B. Prozesse zum Identifizieren doppelter Daten, deren Ausführung nach Ablauf der maximalen Ausführungszeit fortgesetzt werden kann.
  - Einigen Befehlen kann eine andere Abbruchzeit zugeordnet werden. Beispielsweise kann der Befehl MIGRATE STGPOOL einen Parameter einschließen, der die Länge der Zeit angibt, die die Speicherpoolumlagerung ausgeführt wird, bevor die Umlagerung automatisch abgebrochen wird. Wenn Sie einen Befehl planen, für den eine Abbruchzeit definiert ist, und Sie außerdem eine maximale Ausführungszeit für den Zeitplan definieren, werden die Prozesse zu der Abbruchzeit abgebrochen, die zuerst erreicht wird.

Zeitplandarstellung
: Gibt an, ob klassische oder erweiterte Zeitplanregeln verwendet werden.

Intervall
: Gibt die Zeit zwischen den Startfenstern an (bei DAYOFWEEK=ANY). Diese Angabe wird für Zeitpläne mit erweiterter Syntax nicht angezeigt.

Wochentag
: Gibt den Wochentag an, an dem die Startfenster beginnen.

Monat
: Gibt die Monate an, in denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.

Tag des Monats
: Gibt die Tage des Monats an, an denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.

Woche des Monats
: Gibt die Wochen (erste, zweite, dritte, vierte oder letzte) des Monats an, in denen der Zeitplan ausgeführt wird. Diese Angabe wird für Zeitpläne mit klassischer Syntax nicht angezeigt.

Verfall
: Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Ist diese Spalte leer, läuft der Zeitplan nicht ab.

Aktiv?
: Gibt an, ob der Zeitplan termingerecht ausgeführt wurde.

Letzte Aktualisierung durch (Administrator)
: Gibt den Namen des Administrators an, der den Zeitplan zuletzt aktualisiert hat. Enthält dieses Feld $$CONFIG_MANAGER$$, ist der Zeitplan einer Domäne zugeordnet, die von dem Konfigurationsmanager verwaltet wird.

Datum/Zeit der letzten Aktualisierung
: Gibt an, wann der Zeitplan zuletzt geändert wurde (Datum und Uhrzeit).

Verwaltendes Profil
: Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition dieses Zeitplans zu erhalten.

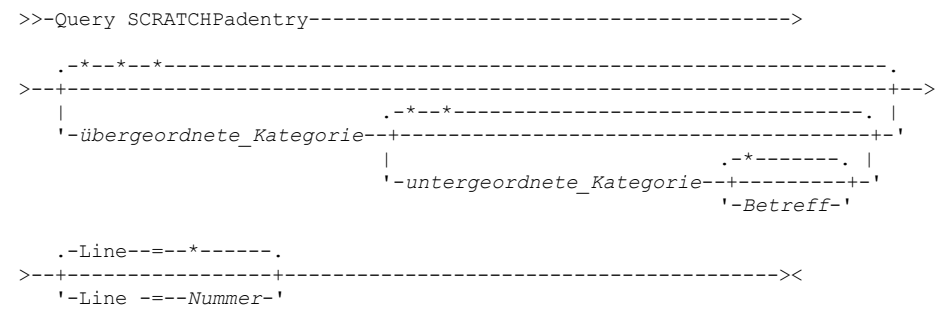
QUERY SCRATCHPADENTRY (Scratchpadeintrag abfragen)

Mit diesem Befehl können Sie Daten anzeigen, die im Scratchpad enthalten sind.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

übergeordnete_Kategorie
: Gibt die übergeordnete Kategorie an, die abgefragt werden soll. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden. Sie können alle übergeordneten Kategorien abfragen, indem Sie diesen Parameter übergehen.

untergeordnete_Kategorie
: Gibt die untergeordnete Kategorie an, die abgefragt werden soll. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden. Sie können alle untergeordneten Kategorien in der übergeordneten Kategorie abfragen, indem Sie diesen Parameter übergehen.

Betreff
: Gibt den Betreff an, der abgefragt werden soll. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden. Sie können alle Betreffs in der untergeordneten Kategorie abfragen, indem Sie diesen Parameter übergehen.

Line
: Gibt die Nummer der Zeile an, die abgefragt werden soll. Geben Sie für *Nummer* eine ganze Zahl im Bereich von 1 bis 1000 ein. Sie können alle Zeilen mit Daten im Betreff abfragen, indem Sie diesen Parameter übergehen.

Beispiel: Scratchpadeinträge abfragen

Fragen Sie eine Datenbank ab, in der Informationen zu den Standorten aller Administratoren gespeichert sind.

```
query scratchpadentry admin_info location

          Übergeordnete Scratchpadkategorie: admin_info
              Untergeordnete Scratchpadkategorie: location
                                    Scratchpadbetreff: codjo
                          Zeilennummer im Scratchpad: 1
                                         Scratchpaddaten: Toronto 5A24
                            Datum/Zeit der Erstellung: 2013-09-10, 10:15:50
                 Datum/Zeit der letzten Aktualisierung: 2013-09-10, 10:15:50
Letzte Aktualisierung durch (Administrator): CODJO

                 Übergeordnete Scratchpadkategorie: admin_info
                Untergeordnete Scratchpadkategorie: location
                                    Scratchpadbetreff: jane
                          Zeilennummer im Scratchpad: 1
                                         Scratchpaddaten: Raleigh GF85
                            Datum/Zeit der Erstellung: 2013-09-09, 14:29:40
                 Datum/Zeit der letzten Aktualisierung: 2013-09-09, 14:29:40
Letzte Aktualisierung durch (Administrator): JANE_W

                 Übergeordnete Scratchpadkategorie: admin_info
                Untergeordnete Scratchpadkategorie: location
                                    Scratchpadbetreff: jane
                          Zeilennummer im Scratchpad: 2
                                         Scratchpaddaten: Nicht im Büro 1.-15.11.
                            Datum/Zeit der Erstellung: 2013-09-09, 14:30:05
                 Datum/Zeit der letzten Aktualisierung: 2013-10-31, 16:55:52
Letzte Aktualisierung durch (Administrator): JANE_W

                 Übergeordnete Scratchpadkategorie: admin_info
                Untergeordnete Scratchpadkategorie: location
                                    Scratchpadbetreff: montse
                          Zeilennummer im Scratchpad: 1
                                         Scratchpaddaten: Barcelona B19
```

```
                          Datum/Zeit der Erstellung: 2013-09-10, 04:34:37
                  Datum/Zeit der letzten Aktualisierung: 2013-09-10, 04:34:37
Letzte Aktualisierung durch (Administrator): MONTSERRAT
```

Feldbeschreibungen

Scratchpaddaten
: Die Daten, die in dem Scratchpadeintrag gespeichert sind.

Datum/Zeit der Erstellung
: Das Datum und die Uhrzeit, an dem bzw. zu der der Scratchpadeintrag erstellt wurde.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der der Scratchpadeintrag zuletzt aktualisiert wurde.

Letzte Aktualisierung durch (Administrator)
: Der Administrator, der den Scratchpadeintrag zuletzt aktualisiert hat.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SCRATCHPADENTRY

Befehl	Beschreibung
DEFINE SCRATCHPADENTRY	Erstellt eine Zeile mit Daten im Scratchpad.
DELETE SCRATCHPADENTRY	Löscht eine Zeile mit Daten aus dem Scratchpad.
SET SCRATCHPADRETENTION	Gibt den Zeitraum an, den Scratchpadeinträge aufbewahrt werden.
UPDATE SCRATCHPADENTRY	Aktualisiert Daten in einer Zeile im Scratchpad.

QUERY SCRIPT (IBM Spectrum Protect-Prozeduren abfragen)

Mit diesem Befehl können Informationen über Prozeduren angezeigt werden.

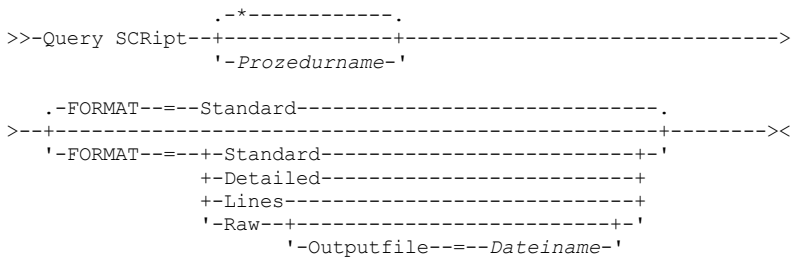
Dieser Befehl kann mit dem Befehl DEFINE SCRIPT verwendet werden, um eine neue Prozedur unter Verwendung des Inhalts aus einer anderen Prozedur zu erstellen.

Berechtigungsklasse

Die für diesen Befehl erforderliche Berechtigungsklasse hängt davon ab, ob der Parameter Outputfile im Befehl angegeben ist.

- Ist der Parameter Outputfile nicht angegeben, kann jeder Administrator diesen Befehl ausgeben.
- Ist der Parameter Outputfile angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf YES gesetzt, muss der Administrator die Systemberechtigung haben.
- Ist der Parameter Outputfile angegeben und ist die Serveroption REQSYSAUTHOUTFILE auf NO gesetzt, muss der Administrator die Bedienerberechtigung, die Maßnahmenberechtigung, die Speicherberechtigung oder die Systemberechtigung haben.

Syntax



Parameter

Prozedurname
: Gibt den Namen der Prozedur an, für die Informationen angezeigt werden sollen. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben.
  Wichtig: Wird keine Prozedur angegeben, zeigt die Abfrage Informationen über alle Prozeduren an. Die zur Verarbeitung dieses Befehls erforderliche Zeit und der Umfang der angezeigten Informationen kann sehr umfangreich sein.

Format
: Gibt das Ausgabeformat für die Anzeige der Prozedurinformationen an. Der Standardwert ist STANDARD. Gültige Werte:

  Standard

Gibt an, daß nur der Prozedurname und die Beschreibung in einer Prozedur angezeigt werden.

Detailed
: Gibt an, daß ausführliche Informationen über die Prozedur angezeigt werden. Diese Informationen enthalten die Befehle in der Prozedur und ihre Zeilennummern, das Datum der letzten Aktualisierung und den Administrator, der die Aktualisierungen ausgeführt hat.

Lines
: Gibt an, daß der Prozedurname, die Zeilennummer der Befehle, die Kommentarzeilen und die Befehle in der Prozedur angezeigt werden.

Raw
: Gibt an, dass die in der Prozedur enthaltenen Befehle in eine Datei geschrieben werden, die mit dem Parameter Outputfile angegeben wird. Dieses Format bietet die Möglichkeit, die Ausgabe aus einer Prozedur in eine Datei umzuleiten, die dann mithilfe des Befehls DEFINE SCRIPT in eine andere Prozedur kopiert werden kann.

  Wird keine Ausgabedatei angegeben, gibt der IBM Spectrum Protect-Server "query script" mit "format=raw" an der Konsole aus.

Outputfile
: Gibt den Namen der Datei an, in die die Ausgabe umgeleitet wird, wenn FORMAT=Raw angegeben wird. Die angegebene Datei muss sich auf dem Server befinden, der diesen Befehl ausführt. Ist die Datei vorhanden, wird die Abfrageausgabe an das Ende der Datei angehängt.

Beispiel: Die Prozedurbeschreibungen auflisten

Die Standardinformationen über Prozeduren anzeigen.

```
query script *

Name             Beschreibung
---------------  ----------------------------------------------------
QCOLS            Spalten für angegebene SQL-Tabelle anzeigen
QSAMPLE          Beispiel-SQL-Abfrage
EXAMPLE          Speicherpools und Datenbank sichern, wenn keine Sitzungen
```

Beispiel: Den Inhalt einer Prozedur mit Zeilennummern anzeigen

Die Zeilen mit Informationen für die Prozedur Q_AUTHORITY anzeigen.

```
query script q_authority format=lines

Name         Zeilen- Befehl
             Anzahl
----------   ------  ------------------------------------------------
Q_AUTHORITY  1       /* ---------------------------------------*/
             5       /* Prozedurname: Q_AUTHORITY               */
             10      /* Beschreibung: Administratoren mit der   */
             15      /*               Berechtigung für Befehle, */
             20      /*               die eine bestimmte Berech-*/
             25      /*               tigung erfordern, anzeigen.*/
                         30      /* Parameter 1: Berechtigungsname in der Form*/
             35      /*              x_priv - EX. policy_priv   */
             40      /* Beispiel:  run q_authority storage_priv */
             45      /* ---------------------------------------*/
             50      select admin_name from admins where -
             55        upper(system_priv) <> 'NO' or -
             60        upper($1) <> 'NO'
```

Beispiel: Eine Prozedur aus einer vorhandenen Prozedur erstellen

Die Prozedur ENGDEV abfragen und die Ausgabe in die Datei MY.SCRIPT umleiten.

```
query script engdev format=raw outputfile=my.script
```

Beispiel: Ausführliche Informationen zur Prozedur anzeigen

Ausführliche Informationen zu Prozeduren anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query script * format=detailed

                                     Name: QCOLS
                             Zeilennummer: DESCRIPTION
                                  Befehl: Spalten für eine angegebene
                                          SQL-Tabelle anzeigen
   Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
         Datum/Zeit der letzten Aktualisierung: 12/02/1997 16:05:29

                                     Name: QCOLS
                             Zeilennummer: 1
                                  Befehl: Spaltenname aus Spalten auswählen;
```

```
                                                dabei ist tabname='$1'
   Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
         Datum/Zeit der letzten Aktualisierung: 12/02/1997 16:05:29
```

Feldbeschreibungen

Name
: Der Name der Prozedur.

Zeilennummer
: Die Zeilennummer der Prozedur oder die Zeichenfolge DESCRIPTION.

Befehl
: Der Befehl in der Zeile, die im vorherigen Feld angezeigt wurde.

Letzte Aktualisierung durch (Administrator)
: Der Name des Administrators, der die Prozedur definiert oder zuletzt aktualisiert hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der der Administrator die Prozedur definiert oder aktualisiert hat.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SCRIPT

Befehl	Beschreibung
COPY SCRIPT	Erstellt eine Kopie einer Prozedur.
DEFINE SCRIPT	Definiert eine Prozedur für den IBM Spectrum Protect-Server.
DELETE SCRIPT	Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur.
RENAME SCRIPT	Vergibt einen neuen Namen für eine Prozedur.
RUN	Führt ein Script aus.
UPDATE SCRIPT	Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.

Zugehörige Konzepte:
Server-Scripts

QUERY SERVER (Server abfragen)

Mit diesem Befehl können Informationen über eine Server-Definition angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                .-*----------.  .-Format--=--Standard-----.
>>-Query SERver--+------------+--+-------------------------+--><
                 '-Servername-'  '-Format--=--+-Standard-+-'
                                              '-Detailed-'
```

Parameter

Servername
: Gibt den Namen des Servers an, der abgefragt werden soll. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden.Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Server-Namen.

Format
: Gibt an, wie die Informationen angezeigt werden. Der Parameter ist wahlfrei. Der Standardwert ist STANDARD.

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Alle Server auflisten

Informationen im Standardformat über alle Server anzeigen.Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query server *
```

```
Server-  Übertr.  Adresse d.  Adresse d.  Tage  Server-  Kennwort-  Ersetzen
Name     Methode  höh. Ebene  unt. Ebene  seit  kenn-    vergabe    möglich
                                          ltzt. wort-    virtueller
                                          Zugr. vergabe  Bereich
-------- ------ ----------- --------  ------ ------- -------- --------
SERVER_A TCPIP  9.115.35.6  1501         11     Yes      No       No
SERVER_B TCPIP  9.115.45.24 1500         <1     Yes      No       No
ASTRO    TCPIP  9.115.32.21 1500         24     Yes      No       No
```

Beispiel: Ausführliche Informationen zu einem bestimmten Server anzeigen

Von einem verwalteten Server ausführliche Informationen zu SERVER_A anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query server server_a format=detailed
```

```
Servername: SERVER_A
                                      Übertragungsmethode: TCPIP
                                      Übertragungsmethode: TCPIP
                                Adresse der höheren Ebene: 9.115.4.15
                                Adresse der unteren Ebene: 1500
                                            Beschreibung:
                                   Ersetzen möglich: No
                                         Knotenname:
                              Datum/Zeit des letzten Zugriffs: 07/09/2013 09:00:00
                                    Tage seit letztem Zugriff: <1
                                        Komprimierung: Vom Client definiert
                                Archivierung löschen?: No
                                                  URL:
                                Registrierung (Datum/Uhrzeit): 07/08/2013 09:15:09
                                        Registriert durch: $$CONFIG_MANAGER$$
                              Byte empfangen (letzte Sitzung): 362
                               Byte gesendet (letzte Sitzung): 507
                                    Dauer der letzten Sitzung: 0,00
                 Inaktiver Wartestatus in % (letzte Sitzung): 0,00
               Auf Übertragung warten in % (letzte Sitzung): 0,00
               Auf Datenträger warten in % (letzte Sitzung): 0,00
                                 Verweildauer vor Löschen: 5
                                      Verwaltendes Profil:
                                 Serverkennwort definiert: Yes
                    Serverkennwort definiert (Datum/Uhrzeit): 07/08/2013 09:15:09
                                    Tage seit Kennwortvergabe: 1
                        Ungültige Anmeldeversuche für Server: 0
                      Kennwortvergabe für virtuellen Bereich: No
        Datum/Zeit der Kennwortvergabe für virtuellen Bereich:(?)
             Tage seit Kennwortvergabe für virtuellen Bereich:(?)
      Ungültige Anmeldeversuche für virtuellen Bereichsknoten: 0
                                    Protokoll auswerten: No
                                                Version: 7
                                                Release: 1
                                                  Stufe: 0.0
                                               Rolle(n): Replikation
                                                    SSL: No
          Sitzungssicherheit: Strict
                                   Transportmethode: TLS 1.2
```

Feldbeschreibungen

Servername
: Der Name des Servers.

Übertragungsmethode
: Die Übertragungsmethode, mit der die Verbindung zum Server hergestellt wird.

Übertragungsmethode
: Die Methode, die für die Datenübertragung zwischen Servern verwendet wird.

Adresse der höheren Ebene
: Die IP-Adresse des Servers (in Schreibweise mit Trennzeichen).

Adresse der unteren Ebene
: Die Anschlußnummer des Servers.

Beschreibung
: Die Server-Beschreibung.

Ersetzen möglich
: Gibt an, ob eine Serverdefinition auf einem verwalteten Server durch eine Definition von einem Konfigurationsmanager ersetzt werden kann.

Knotenname
: Der Name des Clientknotens.

Datum/Zeit des letzten Zugriffs

Das Datum und die Uhrzeit, an dem bzw. zu der der Clientknoten zuletzt auf den Server zugegriffen hat.

Tage seit letztem Zugriff
Die Anzahl der Tage seit dem Zugriff des Client-Knotens auf den Server.

Komprimierung
Die Art der Komprimierung, die von IBM Spectrum Protect für Clientdateien ausgeführt wird.

Archivierung löschen?
Gibt an, ob der Clientknoten seine eigenen Archivierungsdateien löschen kann. Der Wert (?) gibt an, dass dieses Feld nicht definiert ist und für diese Definition nicht gilt.

URL
Der URL für den Zugriff auf diesen Server von einer browserbasierten Schnittstelle aus.

Registrierung (Datum/Uhrzeit)
Das Datum und die Uhrzeit, an dem bzw. zu der der Clientknoten registriert wurde.

Registriert durch
Der Name des Administrators, der den Clientknoten registriert hat.

Byte empfangen (letzte Sitzung)
Die Anzahl der Byte, die während der letzten Sitzung des Clientknotens vom Server empfangen wurden.

Byte gesendet (letzte Sitzung)
Die Anzahl Byte, die an den Clientknoten gesendet wurden.

Dauer der letzten Sitzung
Die Dauer der letzten Sitzung des Client-Knotens in Sekunden.

Inaktiver Wartestatus in % (letzte Sitzung)
Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client keine Funktionen ausgeführt hat.

Auf Übertragung warten in % (letzte Sitzung)
Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client auf eine Antwort von dem Server gewartet hat.

Auf Datenträger warten in % (letzte Sitzung)
Der Prozentsatz der gesamten Sitzungszeit, zu dem der Client auf das Laden eines austauschbaren Datenträgers gewartet hat.

Verweildauer vor Löschen
Die Anzahl der Tage, die ein Objekt auf dem Zielserver verbleibt, nachdem es zum Löschen markiert wurde.

Verwaltendes Profil
Das Profil, aus dem der verwaltete Server die Definition dieses Servers erhalten hat.

Serverkennwort definiert
Gibt an, ob das Kennwort für den Server definiert wird.

Serverkennwort definiert (Datum/Uhrzeit)
Gibt an, wann das Kennwort für den Server definiert wurde.

Tage seit Kennwortvergabe
Die Anzahl der Tage seit der Definition des Server-Kennworts.

Ungültige Anmeldeversuche für Server
Die maximale Anzahl ungültiger Anmeldeversuche, die der Server akzeptieren kann.

Kennwortvergabe für virtuellen Bereich
Gibt an, ob das Kennwort für die Anmeldung beim Zielserver definiert wird.

Datum/Zeit der Kennwortvergabe für virtuellen Bereich
Gibt an, wann das Kennwort für die Unterstützung virtueller Bereiche definiert wurde.

Tage seit Kennwortvergabe für virtuellen Bereich
Die Anzahl der Tage seit der Definition des Kennworts für die Unterstützung virtueller Bereiche.

Ungültige Anmeldeversuche für virtuellen Bereichsknoten
Die maximale Anzahl ungültiger Anmeldeversuche, die auf dem Ziel-Server akzeptiert werden.

Protokoll auswerten (veraltet)

Gibt an, ob für den Speicheragenten die Funktion für die Datenprüfung aktiviert ist. Dieses Feld wird nicht mehr verwendet.

Version
Die Softwareversion des IBM Spectrum Protect-Servers.

Release
Das Software-Release des IBM Spectrum Protect-Servers.

Stufe
Die Softwarestufe des IBM Spectrum Protect-Servers.

Rolle(n)
Die Rolle des Servers. Eine der Rollen, für die der Server verwendet wird, ist z. B. die Replikation.

SSL
Gibt an, ob die SSL-Kommunikation (SSL = Secure Sockets Layer) verwendet wird.

Sitzungssicherheit
Gibt die Stufe der Sitzungssicherheit an, die für den Server durchgesetzt wird. Die gültigen Werte sind STRICT und TRANSITIONAL.

Transportmethode
Gibt die Transportmethode an, die zuletzt für den angegebenen Server verwendet wurde. Die gültigen Werte sind TLS 1.2, TLS 1.1 und NONE. Ein Fragezeichen (?) wird angezeigt, bis eine erfolgreiche Authentifizierung ausgeführt wird.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SERVER

Befehl	Beschreibung
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DELETE DEVCLASS	Löscht eine Einheitenklasse.
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
DELETE SERVER	Löscht die Definition eines Servers.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemePROTECT STGPOOL	AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeSchützt einen Verzeichniscontainerspeicherpool.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
RECONCILE VOLUMES	Stimmt Definitionen von virtuellen Datenträgern auf dem Quellenserver mit Archivierungsobjekten des Zielservers ab.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
SET REPLSERVER	Gibt einen Zielreplikationsserver an.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.
UPDATE SERVER	Aktualisiert Informationen über einen Server.

QUERY SERVERGROUP (Servergruppe abfragen)

Mit diesem Befehl können Informationen über Server-Gruppen und Gruppenteile angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                      .-*-----------.
>>-QUERY SERVERGroup--+-------------+--------------------------><
                      '-Gruppenname-'
```

Parameter

Gruppenname
: Gibt die Server-Gruppe an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden.

Beispiel: Servergruppen auflisten

Von einem verwalteten Server alle Servergruppen abfragen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query servergroup *

Servergruppe    Mitglieder      Beschreibung         Verwaltendes Profil
------------    ------------    -----------------    ----------------
ADMIN_GROUP     SERVER_A        Headquarters             ADMIN_INFO
                                 SERVER_B
                                 SERVER_C
                                 SERVER_D
```

Feldbeschreibungen

Servergruppe
: Der Name der Server-Gruppe.

Mitglieder
: Die Gruppenteile.

Beschreibung
: Die Beschreibung der Server-Gruppe.

Verwaltendes Profil
: Das Profil oder die Profile, für die der verwaltete Server subskribiert hat, um die Definition der Servergruppen zu erhalten.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SERVERGROUP

Befehl	Beschreibung
COPY SERVERGROUP	Erstellt eine Kopie einer Servergruppe.
DEFINE SERVERGROUP	Definiert eine neue Servergruppe.
DELETE SERVERGROUP	Löscht eine Servergruppe.
QUERY SERVER	Zeigt Informationen über Server an.
RENAME SERVERGROUP	Benennt eine Servergruppe um.
UPDATE SERVERGROUP	Aktualisiert eine Servergruppe.

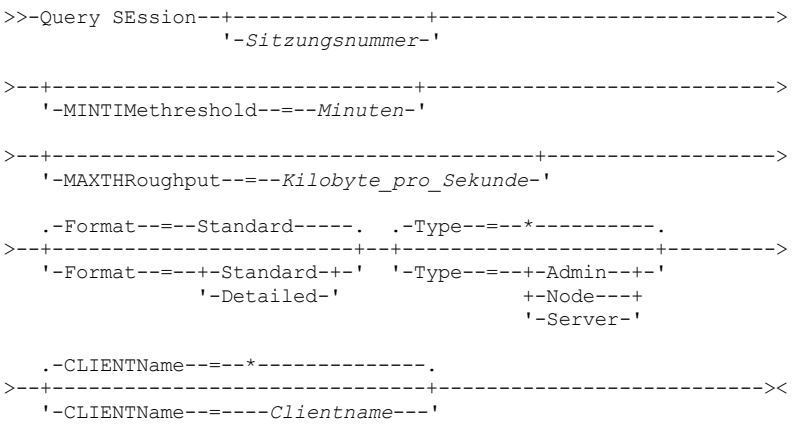
QUERY SESSION (Clientsitzungen abfragen)

Mit diesem Befehl können Informationen zu Verwaltungs-, Knoten- und Serversitzungen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Sitzungsnummer
: Gibt die Nummer der Verwaltungssitzung oder Client-Knotensitzung an, die abgefragt werden soll. Dieser Parameter ist wahlfrei. Wird kein Wert für diesen Parameter angegeben, werden alle Sitzungen angezeigt.

MINTIMethreshold
: Gibt an, dass Sitzungen angezeigt werden sollen, für die mindestens diese Anzahl Minuten ab dem Zeitpunkt verstrichen sind, zu dem der Client Daten zum Speichern an den Server gesendet hat. Dieser Parameter ist wahlfrei. Die Mindestanzahl Minuten ist 1. Die maximale Anzahl Minuten beträgt 99999999.

MAXTHRoughput
: Gibt an, daß Sitzungen angezeigt werden sollen, in denen Daten mit einer geringeren Übertragungsgeschwindigkeit als dieser Anzahl Kilobyte pro Sekunde übertragen werden. Dieser Parameter ist wahlfrei. Die Mindestanzahl Kilobyte pro Sekunde beträgt 0. Die maximale Anzahl Kilobyte pro Sekunde beträgt 99999999.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Die folgenden Werte sind gültig:

Standard
: Gibt an, daß Teilinformationen für die Sitzung angezeigt werden.

Detailed
: Gibt an, daß die gesamten Informationen für die Sitzung angezeigt werden.

Type
: Gibt den Typ der Sitzungen an, der in den Abfrageergebnissen berücksichtigt werden soll. Wird kein Wert für diesen Parameter angegeben, werden alle Typen von Sitzungen abgefragt. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  Admin
  : Gibt an, dass Verwaltungssitzungen angezeigt werden.

  Node
  : Gibt an, dass Knotensitzungen angezeigt werden.

  Server
  : Gibt an, dass Serversitzungen angezeigt werden.

CLIENTName
: Gibt den Namen eines Administrators, Clientknotens oder Servers an, der abgefragt werden soll. Sie können einen oder mehrere Namen angeben. Sie können auch Knotengruppen und Proxy-Knoten angeben. Werden mehrere Namen angegeben, sind die Namen durch Kommas voneinander zu trennen; verwenden Sie zwischen den Namen keine Leerzeichen. Sie können Platzhalterzeichen für Knotennamen, aber nicht für Knotengruppennamen verwenden. Der Parameter ist wahlfrei.

  Während der Knotenreplikation wird der Clientname auf dem Zielserver als *Knotenname (Servername)* angezeigt. Dabei ist *Knotenname* der Knoten, dessen Daten repliziert werden, und *Servername* der Name des Quellenservers. Sie können entweder den Knotennamen oder den Servernamen im Parameter CLIENTName angeben, um die Replikationssitzungen anzuzeigen.

Beispiel: Aktive Clientknotensitzungen auflisten

Informationen zu allen Verwaltungs- und Clientknotensitzungen, die mit dem Server kommunizieren, anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query session
```

```
Sitz.  Über.  Sitz.    Warte- Byte  Byte    Sitz. Platt-   Client-
nummer meth.  status   zeit gesend. empf.   typ   form     Name
------ ------ ------ ------ ------- ------- ----- -------- ------
     4  TCP/IP  Run    0 S    1.4 K    162   Admin  WinNT   ADMIN
```

Beispiel: Ausführliche Informationen zu aktiven Clientknotensitzungen anzeigen

Ausführliche Informationen zu allen Verwaltungs- und Clientknotensitzungen, die mit dem Server kommunizieren, anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query session format=detailed
```

```
             Sitzungsnummer: 4
            Übertragungsmethode: Tcp/Ip
                 Sitzungsstatus: Run
                      Wartezeit: 0 S
                  Byte gesendet: 1,4 K
                 Byte empfangen: 162
                    Sitzungstyp: Admin
                                Plattform: WinNT
                     Clientname: ADMIN
    Datenträgerzugriffsstatus:
                   Benutzername:
  Ersten Daten gesendet am/um:
    Proxy durch Speicheragent:
                      Aktionen:
                 Übernahmemodus: No
```

Feldbeschreibungen

Sitzungsnummer
: Gibt eine eindeutige Sitzungsidentifikationsnummer an, die vom Server zugeordnet wird.

Übertragungsmethode
: Gibt die Methode an, die vom Client für die Kommunikation mit dem Server verwendet wird.

Sitzungsstatus
: Gibt den aktuellen Übertragungsstatus des Servers an. Die folgenden Status sind gültig:

End
Die Sitzung wird beendet (Sitzungsressourcen werden freigegeben).
IdleW
Es wird auf die nächste Anforderung des Clients gewartet (Sitzung ist inaktiv).
MediaW
Die Sitzung wartet darauf, auf einen Datenträger mit sequenziellem Zugriff zugreifen zu können.
RecvW
Der Server wartet darauf, eine unerwartete Nachricht vom Client zu empfangen.
Run
Der Server führt gerade eine Clientanforderung aus (und wartet nicht auf das Senden von Daten).
SendW
Der Server wartet darauf, Daten an den Client zu senden (wartet auf bereits gesendete Daten, die an den Clientknoten weitergegeben werden sollen).
SSLiW
Die Sitzung wartet auf die Beendigung der SSL-Initialisierung (SSL = Secure Sockets Layer).
Start
Die Sitzung wird gestartet (Identifikationsüberprüfung läuft).

Wartezeit
Gibt die Zeit an (Sekunden, Minuten oder Stunden), die sich der Server im angezeigten aktuellen Status befindet.
Byte gesendet
Gibt die Anzahl der Datenbyte an, die an den Clientknoten gesendet wurden, seit die Sitzung eingeleitet wurde.
Byte empfangen
Gibt die Anzahl der Datenbyte an, die vom Clientknoten empfangen wurden, seit die Sitzung eingeleitet wurde.
Sitzungstyp
Gibt die Art der Sitzung an, die gerade läuft: ADMIN bei einer Verwaltungssitzung, NODE bei einer Clientknotensitzung oder SERVER. SERVER gibt an, dass der Server eine Sitzung startet und serverübergreifende Operationen einleitet, wie beispielsweise Sitzungen für zentrale Konfiguration, gemeinsame Nutzung von Speicherarchiven und Speicheragenten.
Plattform
Gibt den Typ des Betriebssystems an, das dem Client zugeordnet ist.
Clientname
Gibt den Namen des Client-Knoten bzw. Administrators an.

Für Knotenreplikationssitzungen wird der Clientname nach dem Start der Datenübertragung auf dem Zielserver in *Knotenname* (*Servername*) aktualisiert.

Datenträgerzugriffsstatus
Gibt den Statustyp "Auf Datenträger warten" an. Befindet sich eine Sitzung in einem Datenträgerwartestatus, zeigt dieses Feld eine Liste aller Mountpunkte und aller sequenziellen Datenträger für die Sitzung an. Die Liste der Mountpunkte gibt die Einheitenklasse und den zugeordneten Speicherpool an. Die Liste der Datenträger gibt die Datenträger des primären Speicherpools sowie die Datenträger aller Kopienspeicherpools und Pools für aktive Daten zusammen mit den zugeordneten Speicherpools an.

Der Server erlaubt es mehreren Sitzungen, einen Datenträger in einem Speicherpool, dem der Einheitentyp FILE oder CENTERA zugeordnet ist, gleichzeitig zu lesen, und einer Sitzung, auf den Datenträger zu schreiben. Daher kann ein Datenträger in einem Speicherpool mit einem Einheitentyp FILE oder CENTERA für mehrere Sitzungen als aktueller Datenträger erscheinen.

Proxy durch Speicheragent
Gibt den Speicheragenten an, der der Proxy für die LAN-unabhängige Datenversetzung für den Knoten ist.
Benutzername
Gibt die Benutzer-ID des Knotens auf einem Mehrbenutzersystem an, mit der die Verbindung zum Server hergestellt wird, wenn es sich nicht um denselben Systembenutzer handelt, der ursprünglich mit dem Server verbunden war.
Ersten Daten gesendet am/um
Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Client zum ersten Mal Daten zum Speichern an den Server gesendet hat.
Aktionen
Zeigt eine Liste der Aktionen an, die während der Sitzung ausgeführt wurden. Eine Aktion wird nur ein Mal aufgelistet, auch wenn die Aktion während einer Sitzung mehrmals ausgeführt wurde. Die folgenden Aktionen sind gültig:

BkIns
Ein oder mehrere Sicherungsobjekte wurden auf dem Server gespeichert. Die Operation kann eine Teilsicherung oder eine selektive Sicherung gewesen sein.
BkUpd
Ein oder mehrere Attribute wurden für ein Sicherungsobjekt aktualisiert, das auf dem Server gespeichert ist.
BkDel
Ein oder mehrere Sicherungsobjekte, die auf dem Server gespeichert waren, wurden gelöscht.
BkRebind
Ein oder mehrere Sicherungsobjekte, die auf dem Server gespeichert sind, wurden an eine andere Verwaltungsklasse gebunden.
NoQueryRestore
Eine Zurückschreibungsoperation ohne Abfrage wurde von dem Client eingeleitet, um gesicherte Dateien vom Server in das Clientsystem zurückzuschreiben.
ArIns

Ein oder mehrere Archivierungsobjekte wurden auf dem Server gespeichert.

ObjRtrv
: Eine oder mehrere Dateien wurden von dem Server abgerufen. Möglicherweise sollten Archivierungsdateien abgerufen oder Sicherungsdaten (außer Sicherungsdaten aus einer Zurückschreibungsoperation ohne Abfrage) zurückgeschrieben werden.

MigIns
: Eine oder mehrere Dateien wurden von IBM Spectrum Protect for Space Management (HSM-Client) umgelagert und auf dem Server gespeichert.

MigDel
: Eine oder mehrere speicherverwaltete Dateien, die auf dem Server gespeichert waren, wurden gelöscht.

MigRebind
: Eine oder mehrere speicherverwaltete Dateien, die auf dem Server gespeichert sind, wurden an eine andere Verwaltungsklasse gebunden.

MigRecall
: Eine oder mehrere speicherverwaltete Dateien, die auf dem Server gespeichert sind, wurden zurückgerufen.

MigUpd
: Die Attribute für eine oder mehrere speicherverwaltete Dateien, die auf dem Server gespeichert sind, wurden aktualisiert.

FSAdd
: Der Clientknoten hat einen oder mehrere neue Dateibereiche zum Serverspeicher hinzugefügt.

FSUpd
: Der Clientknoten hat Attribute für einen oder mehrere Dateibereiche aktualisiert, die für den Server definiert sind.

DefAuth
: Ein Befehl SET ACCESS wurde von dem Clientknoten verarbeitet, der zur Folge hatte, dass eine Berechtigungsregel für den Zugriff auf die Daten des Clientknotens hinzugefügt wurde.

Übernahmemodus
: Gibt an, ob die Clientsitzung im Übernahmemodus gestartet wurde. Die folgenden Werte sind gültig:

  Force
  : Das Flag FORCEFAILOVER ist auf dem Client angegeben und der Übernahmemodus wird für die Sitzung erzwungen.

  Yes
  : Die Clientsitzung wurde im Übernahmemodus gestartet.

  No
  : Die Clientsitzung wurde nicht im Übernahmemodus gestartet.

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für QUERY SESSION

Befehl	Beschreibung
CANCEL SESSION	Bricht aktive Sitzungen mit dem Server ab.

QUERY SHREDSTATUS (Status für Schreddern abfragen)

Verwenden Sie diesen Befehl, um Informationen zu Daten anzuzeigen, die geschreddert werden sollen.

Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie über die Administratorberechtigung verfügen.

Syntax

```
                        .-Format--=--Standard-----.
>>-QUERY SHREDstatus--+-------------------------+--------------><
                      '-Format--=--+-Standard-+-'
                                   '-Detailed-'
```

Parameter

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.Dies ist der Standardwert.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Übersichtsdaten zum Schreddern anzeigen

Teilinformationen zum Schreddern von Daten auf dem Server anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query shredstatus

Schreddern  Objekte, die auf
  aktiv       Schreddern
                  warten
 -------      --------
      NO           4
```

Beispiel: Ausführliche Informationen zum Schreddern anzeigen

Ausführliche Informationen zum Schreddern von Daten auf dem Server anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query shredstatus format=detailed

Schreddern Objekte, die   Belegter      Noch zu
  aktiv    auf Schreddern Speicherber.  schreddernde
            warten        (MB)          Daten (MB)
--------- --------  --------  ----------
    NO        4              182           364
```

Feldbeschreibungen

Schreddern aktiv
: Gibt an, ob der Server zu diesem Zeitpunkt aktiv Daten schreddert.

Objekte, die auf Schreddern warten
: Die Anzahl der Objekte, die gegenwärtig auf das Schreddern warten.

Belegter Speicherbereich (MB)
: Der Serverspeicherbereich (in MB), der durch die Objekte belegt ist, die gegenwärtig auf das Schreddern warten. Dies ist der Speicherbereich, der verfügbar wird, wenn die Objekte geschreddert wurden.

Noch zu schreddernde Daten (MB)
: Das Datenvolumen, das noch geschreddert werden muss.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SHREDSTATUS

Befehl	Beschreibung
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
GENERATE BACKUPSETTOC	Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.
MOVE DATA	Versetzt Daten aus einem angegebenen Speicherpooldatenträger in einen anderen Speicherpooldatenträger.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
SETOPT	Aktualisiert eine Serveroption, ohne den Server zu stoppen und erneut zu starten.
SHRED DATA	Startet manuell den Prozess zum Schreddern gelöschter Daten.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

QUERY SPACETRIGGER (Speicherbereichsauslöser abfragen)

Verwenden Sie diesen Befehl, um die Einstellungen der Speicherbereichsauslöser für den Speicherpool anzuzeigen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query SPACETrigger--STG--+-------------------------+-------->
```

```
                          '-STGPOOL--=--Speicherpool-'

   .-Format--=--Standard-----.
>--+-------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

STG
: Gibt einen Speicherbereichsauslöser für den Speicherpool an.

STGPOOL
: Gibt einen oder mehrere Speicherpools an (unter Verwendung eines Platzhalterzeichens), für die Informationen zum Speicherpoolauslöser angezeigt werden. Wird STG angegeben, aber STGPOOL nicht angegeben, wird der standardmäßige Speicherbereichsauslöser für den Speicherpool (sofern vorhanden) angezeigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Die ausführlichen Einstellungen des Speicherbereichsauslösers für einen Speicherpool anzeigen

Diesen Befehl ausgeben:

```
query spacetrigger stg stgpool=archivepool format=detailed
```

 AIX-Betriebssysteme

```
         Speicherpool Prozent belegt:   50
         Prozentsatz für Speicherpoolerweiterung:   20
              Präfix für Speicherpoolerweiterung:   /usr/tivoli/tsm/server/filevol/
                                 SPEICHERPOOL:   ARCHIVEPOOL
     Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
           Datum/Zeit der letzten Aktualisierung:   05/10/2004 11:59:59
```

 Linux-Betriebssysteme

```
         Speicherpool Prozent belegt:   50
         Prozentsatz für Speicherpoolerweiterung:   20
              Präfix für Speicherpoolerweiterung:   /opt/tivoli/tsm/server/filevol/
                                 SPEICHERPOOL:   ARCHIVEPOOL
     Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
           Datum/Zeit der letzten Aktualisierung:   05/10/2004 11:59:59
```

 Windows-Betriebssysteme

```
         Speicherpool Prozent belegt:   50
         Prozentsatz für Speicherpoolerweiterung:   20
              Präfix für Speicherpoolerweiterung:   c:\Programmdateien\tivoli\filevol\
                                 SPEICHERPOOL:   ARCHIVEPOOL
     Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
           Datum/Zeit der letzten Aktualisierung:   05/10/2004 11:59:59
```

Feldbeschreibungen

Speicherpool Prozent belegt
: Der Auslöserauslastungsprozentsatz, bei dem IBM Spectrum Protect mehr Speicherbereich für den Speicherpool zuordnet.

Prozentsatz für Speicherpoolerweiterung
: Der Prozentsatz des Speicherbereichs, um den der Speicherpool erweitert werden soll.

Präfix für Speicherpoolerweiterung
: Das Präfix, das dem Speicherbereichsauslöser zugeordnet ist.

STGPOOL
: Der in der Abfrage verwendete Speicherpoolname.

Letzte Aktualisierung durch (Administrator)
: Der Administrator, der den Speicherbereichsauslöser für den Speicherpool zuletzt aktualisiert hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der der Administrator den Speicherbereichsauslöser für den Speicherpool zuletzt aktualisiert hat.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SPACETRIGGER

Befehl	Beschreibung
DEFINE SPACETRIGGER	Definiert einen Speicherbereichsauslöser zum Erweitern des Speicherbereichs für einen Speicherpool.
DELETE SPACETRIGGER	Löscht den Speicherbereichsauslöser für den Speicherpool.
UPDATE SPACETRIGGER	Ändert Attribute des Speicherbereichsauslösers für den Speicherpool.

QUERY STATUS (Systemparameter abfragen)

Mit dem Befehl QUERY STATUS können Informationen zu Systemparametern angezeigt werden.

Diesen Befehl verwenden, um

- die Servicestufe für den Server anzuzeigen.
- Informationen zu allgemeinen Serverparametern anzuzeigen, zum Beispiel zu den mit den SET-Befehlen definierten Parametern.
- Informationen zu Clientsitzungen anzufordern, beispielsweise die Verfügbarkeit des Servers, Kennwortauthentifizierung, Einstellungen für die Abrechnung oder die Aufbewahrungsdauer der Informationen, die im Aktivitätenprotokoll aufbewahrt werden.
- Informationen über den zentralen Scheduler anzuzeigen, beispielsweise den zentralen Planungsmodus des Servers.
- die maximale Anzahl der Wiederholungen anzuzeigen, die nach der fehlgeschlagenen Ausführung eines geplanten Befehls zulässig sind.
- anzuzeigen, ob Subdateien auf diesem Server gesichert werden können, wie durch den Befehl SET SUBFILE angegeben ist.
- Informationen zu einem Zielreplikationsserver anzuzeigen.
- Lizenzinformationen anzuzeigen.

Tipp: Um Informationen zu einem Zielreplikationsserver anzuzeigen, müssen Sie den Befehl auf dem Zielreplikationsserver ausgeben.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query STatus-------------------------------------------------><
```

Parameter

Keine.

Beispiel: Den Status eines Konfigurationsmanagers abfragen

Allgemeine Informationen zu Serverparametern anzeigen. Der Befehl wird von einem Konfigurationsmanager ausgeführt. Beschreibungen der angezeigten Felder befinden sich in Feldbeschreibungen.

```
query status
```

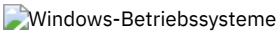
AIX-Betriebssysteme

```
                                 Servername: SETSHOT
          Server-Host-Name oder IP-Adresse: setshot
             Server-TCP/IP-Anschlussnummer: 1500
                       Überkreuzdefinition: On
                 Serverkennwort definiert: Yes
        Datum/Zeit der Serverinstallation: 2016-07-08, 09:45:53
           Datum/Zeit des Serverneustarts: 2016-10-10, 05:38:49
                        Authentifizierung: Off
                     Kennwortablaufdauer: 9.999 Tag(e)
Grenzwert für ungültige Anmeldeversuche: 0
                Mindestlänge für Kennwort: 0
                            Registrierung: Geschlossen
                      Subdateisicherung: Client
                          Verfügbarkeit: Aktiviert
        Inaktivierte eingehende Sitzungen:
         Inaktivierte abgehende Sitzungen:
                                Abrechnung: Off
Aufbewahrungsdauer für Aktivitätenprotokoll: 30 Tag(e)
       Anzahl Sätze im Aktivitätenprotokoll: 222919
            Größe des Aktivitätenprotokolls: 6 M
 Aufbewahrungszeitraum für Aktivitätsübers.: 30 Tag(e)
```

```
                                  Intervall für Lizenzprüfung: 30 Tag(e)
                                        Letzte Lizenzprüfung: 2016-10-21, 07:40:20
                                   Server-Lizenzbestimmungen: Gültig
                                         Zentraler Scheduler: Aktiv
                                  Maximale Anzahl Sitzungen: 300
                              Maximale Anzahl geplanter Sitzungen: 75
                           Aufbewahrungszeitraum für Ereignissätze: 14 Tag(e)
                                    Dauer von Clientaktionen: 5 Tage(e)
                             Zeitplanzufallsgenerierung (Prozent): 25
                                   Intervall für Zeitplanabfragen: Client
                            Maximale Anzahl Befehlswiederholungen: Client
                                  Wiederholungszeitlimit: Client
                        Prüfstufe für clientseitige Deduplizierung: 0%
                                               Planungsmodi: Beliebig
                                          Aktive Empfänger: CONSOLE ACTLOG
                                     Konfigurationsmanager?: Off
                                   Aktualisierungsintervall: 60
                              Datum/Zeit der letzten Aktualisierung:
                                   Anzeigen von Nachrichtenkontext: On
          Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis: 120 Minute(n)
                                            Maschinen-GUID:
d4.cg.f6.ae.04.6e.11.e3.80.1f.00.21.5e.18.df.01
                                Aufbewahrungsschutz für Archivierung: Off
                                    Datenbankverzeichnisse: /TSMserver/DB1,/TSMserver/DB2
                      Gesamtspeicherbereich des Dateisystems (MB): 222.720,00
                 Verwendeter Speicherbereich im Dateisystem (MB): 47.780,74
                         Freier verfügbarer Speicherbereich (MB): 174.939,26
                                      Verschlüsselungsstufe: AES
           Aktualisierungsintervall für Client-CPU-Informationen: 180
                                    Abgehende Replikation: Enabled
                                   Zielreplikationsserver: POWER
        Standardreplikationsregel für Archivierungsdaten: ALL_DATA
           Standardreplikationsregel für Sicherungsdaten: ALL_DATA
      Standardreplikationsregel für speicherverwaltete Daten: ALL_DATA
            Aufbewahrungszeitraum für Replikationsdatensätze: 30 Tag(e)
                                          LDAP-Benutzer:
                                  LDAP-Kennwort definiert: No
                                 Standardauthentifizierung: Local
                          Adresse höherer Ebene für Übernahme:
                             Aufbewahrungszeit für Scratchpad: 365 Tag(e)
       Replikationswiederherstellung beschädigter Dateien: On
                                       SUR-Belegung (TB): 5,66
                                  SUR-Belegung (Datum/Zeit): 2016-10-10, 05:39:33
                                   Front-End-Kapazität (MB): 226.331
                                   Anzahl Front-End-Clients: 6
                               Datum für Front-End-Kapazität: 2016-10-13, 09:20:02
                                        Produktangebot: IBM Spectrum Protect
```

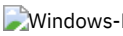

```
                                           Servername: GOBI
                                Server-Host-Name oder IP-Adresse:
                                   Server-TCP/IP-Anschlussnummer: 1500
                                             Überkreuzdefinition: On
                                      Serverkennwort definiert: Yes
                                  Datum/Zeit der Serverinstallation: 2016-07-08, 11:29:03
                                     Datum/Zeit des Serverneustarts: 2016-11-10, 14:25:03
                                           Authentifizierung: On
                                         Kennwortablaufdauer: 90 Tag(e)
                           Grenzwert für ungültige Anmeldeversuche: 0
                                 Mindestlänge für Kennwort: 0
                                              Registrierung: Geschlossen
                                        Subdateisicherung: No
                                           Verfügbarkeit: Aktiviert
                                Inaktivierte eingehende Sitzungen:
                                 Inaktivierte abgehende Sitzungen:
                                              Abrechnung: Off
                           Aufbewahrungsdauer für Aktivitätenprotokoll: 30 Tag(e)
                                 Anzahl Sätze im Aktivitätenprotokoll: 21346
                                      Größe des Aktivitätenprotokolls: <1 M
                           Aufbewahrungszeitraum für Aktivitätsübers.: 30 Tag(e)
                                  Intervall für Lizenzprüfung: 30 Tag(e)
                                        Letzte Lizenzprüfung: 2016-10-21, 23:27:23
                                   Server-Lizenzbestimmungen: Gültig
                                         Zentraler Scheduler: Aktiv
                                  Maximale Anzahl Sitzungen: 500
                              Maximale Anzahl geplanter Sitzungen: 250
                           Aufbewahrungszeitraum für Ereignissätze: 14 Tag(e)
                                    Dauer von Clientaktionen: 5 Tage(e)
                             Zeitplanzufallsgenerierung (Prozent): 25
                                   Intervall für Zeitplanabfragen: Client
                            Maximale Anzahl Befehlswiederholungen: Client
```

```
                                  Wiederholungszeitlimit: Client
                Prüfstufe für clientseitige Deduplizierung: 0%
                                       Planungsmodi: Beliebig
                                  Aktive Empfänger: CONSOLE ACTLOG
                                Konfigurationsmanager?: Off
                               Aktualisierungsintervall: 60
                    Datum/Zeit der letzten Aktualisierung:
                           Anzeigen von Nachrichtenkontext: Off
      Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis: 120 Minute(n)
                                       Maschinen-GUID:
fc.e7.be.58.4a.a7.11.e0.8a.c8.e4.1f.13.34.11.e0
                     Aufbewahrungsschutz für Archivierung: Off
                                  Datenbankverzeichnisse:
/TSMdbspace1/gpcinst1,/TSMdbspace2/gpcinst1,/TSMdbspace3/gpcinst1
            Gesamtspeicherbereich des Dateisystems (MB): 302.379,84
          Verwendeter Speicherbereich im Dateisystem (MB): 106.793,65
                Freier verfügbarer Speicherbereich (MB): 195.586,20
                                Verschlüsselungsstufe: AES
       Aktualisierungsintervall für Client-CPU-Informationen: 180
                                  Abgehende Replikation: Enabled
                                  Zielreplikationsserver:
      Standardreplikationsregel für Archivierungsdaten: ALL_DATA
         Standardreplikationsregel für Sicherungsdaten: ALL_DATA
    Standardreplikationsregel für speicherverwaltete Daten: ALL_DATA
      Aufbewahrungszeitraum für Replikationsdatensätze: 30 Tag(e)
                                       LDAP-Benutzer:
                               LDAP-Kennwort definiert: No
                              Standardauthentifizierung: Local
                 Adresse höherer Ebene für Übernahme:
                    Aufbewahrungszeit für Scratchpad: 365 Tag(e)
  Replikationswiederherstellung beschädigter Dateien: Off
                                   SUR-Belegung (TB): 0,00
                              SUR-Belegung (Datum/Zeit): 2016-10-10, 14:25:35
                               Front-End-Kapazität (MB): 226.331
                              Anzahl Front-End-Clients: 6
                          Datum für Front-End-Kapazität: 2016-10-13, 09:20:02
                                       Produktangebot: IBM Spectrum Protect
```




```
                                       Servername: EXCELSIOR
                    Server-Host-Name oder IP-Adresse: excelsior.storage.
                                                      newyork.example.com
                       Server-TCP/IP-Anschlussnummer: 1500
                                 Überkreuzdefinition: On
                              Serverkennwort definiert: Yes
                    Datum/Zeit der Serverinstallation: 2016-07-08, 18:02:50
                       Datum/Zeit des Serverneustarts: 2016-11-10, 11:48:32
                                    Authentifizierung: On
                                 Kennwortablaufdauer: 90 Tag(e)
      Grenzwert für ungültige Anmeldeversuche: 0
                           Mindestlänge für Kennwort: 0
                                    Registrierung: Geschlossen
                                 Subdateisicherung: No
                                     Verfügbarkeit: Aktiviert
                    Inaktivierte eingehende Sitzungen:
                     Inaktivierte abgehende Sitzungen:
                                       Abrechnung: On
  Aufbewahrungsdauer für Aktivitätenprotokoll: 30 Tag(e)
         Anzahl Sätze im Aktivitätenprotokoll: 1346376
              Größe des Aktivitätenprotokolls: 37 M
   Aufbewahrungszeitraum für Aktivitätsübers.: 30 Tag(e)
                  Intervall für Lizenzprüfung: 30 Tag(e)
                        Letzte Lizenzprüfung: 2016-10-21, 17:05:16
                    Server-Lizenzbestimmungen: Gültig
                          Zentraler Scheduler: Aktiv
                    Maximale Anzahl Sitzungen: 25
             Maximale Anzahl geplanter Sitzungen: 12
      Aufbewahrungszeitraum für Ereignissätze: 14 Tag(e)
                     Dauer von Clientaktionen: 5 Tage(e)
        Zeitplanzufallsgenerierung (Prozent): 25
              Intervall für Zeitplanabfragen: Client
       Maximale Anzahl Befehlswiederholungen: Client
                          Wiederholungszeitlimit: Client
      Prüfstufe für clientseitige Deduplizierung: 0%
                                       Planungsmodi: Beliebig
                                  Aktive Empfänger: CONSOLE ACTLOG
                                                    NTEVENTLOG
                                Konfigurationsmanager?: Off
                               Aktualisierungsintervall: 60
                    Datum/Zeit der letzten Aktualisierung:
```

```
                                Anzeigen von Nachrichtenkontext: Off
            Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis: 120 Minute(n)
                                                Maschinen-GUID:
e9.3e.f1.70.ff.c5.11.e2.a5.67.5c.f3.fc.0c.5e.60
                              Aufbewahrungsschutz für Archivierung: Off
                                       Datenbankverzeichnisse: e:\Server1\TSMDBdir
                    Gesamtspeicherbereich des Dateisystems (MB): 102.270,00
                 Verwendeter Speicherbereich im Dateisystem (MB): 22.032,79
                         Freier verfügbarer Speicherbereich (MB): 80.237,20
                                         Verschlüsselungsstufe: AES
 Aktualisierungsintervall für Client-CPU-Informationen: 180
                                      Abgehende Replikation: Enabled
                                    Zielreplikationsserver: EXPLORER
          Standardreplikationsregel für Archivierungsdaten: ALL_DATA
             Standardreplikationsregel für Sicherungsdaten: ALL_DATA
Standardreplikationsregel für speicherverwaltete Daten: ALL_DATA
       Aufbewahrungszeitraum für Replikationsdatensätze: 30 Tag(e)
                                           LDAP-Benutzer: cn=excelsior_ldapadmin,ou=excelsior,
                                                          ou=John Doe,dc=tsmadldap,dc=storage,
                                                          dc=newyork, dc=example,dc=com
                                    LDAP-Kennwort definiert: Yes
                                  Standardauthentifizierung: LDAP
                       Adresse höherer Ebene für Übernahme:
                          Aufbewahrungszeit für Scratchpad: 365 Tag(e)
    Replikationswiederherstellung beschädigter Dateien: On
                                        SUR-Belegung (TB): 8,98
                                  SUR-Belegung (Datum/Zeit): 2016-10-10, 11:49:27
                                   Front-End-Kapazität (MB): 226.331
                                   Anzahl Front-End-Clients: 6
```




```
                                Datum für Front-End-Kapazität: 2016-10-13, 09:20:02
                                                Produktangebot: IBM Spectrum Protect
```

Feldbeschreibungen

Servername
: Gibt den Namen des Servers an.

Server-Host-Name oder IP-Adresse
: Gibt die Server-TCP/IP-Adresse an.

Server-TCP/IP-Anschlussnummer
: Gibt die Serveranschlussadresse an.

Überkreuzdefinition
: Gibt an, ob ein anderer Server, der den Befehl DEFINE SERVER ausführt, sich automatisch selbst für diesen Server definiert. Siehe Befehl SET CROSSDEFINE.

Server-Kennwort definiert
: Gibt an, ob das Kennwort für den Server definiert wurde.

Datum/Zeit der Serverinstallation
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Server installiert wurde.

Datum/Zeit des Serverneustarts
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der der Server zuletzt gestartet wurde.

Authentifizierung
: Gibt an, ob die Kennwortauthentifizierung aktiviert oder inaktiviert ist.

Kennwortablaufdauer
: Gibt die Anzahl Tage an, nach deren Ablauf das Kennwort für den Administrator oder den Clientknoten seine Gültigkeit verliert.

Grenzwert für ungültige Anmeldeversuche
: Gibt die Anzahl der ungültigen Anmeldeversuche an, die zulässig sind, bevor der Knoten gesperrt wird.

Mindestlänge für Kennwort
: Gibt die Mindestanzahl Zeichen für das Kennwort an.

Registrierung
: Gibt an, ob die Registrierung für den Clientknoten geöffnet oder geschlossen ist.

Subdateisicherung
: Gibt an, ob Subdateien auf diesem Server gesichert werden können, wie durch den Befehl SET SUBFILE angegeben ist.

Verfügbarkeit
: Gibt an, ob der Server aktiviert oder inaktiviert ist.

Inaktivierte eingehende Sitzungen
: Gibt die Namen der Server an, von denen eine Übertragung zwischen Servern nicht zulässig ist. Um eingehende Serversitzungen zu aktivieren, verwenden Sie den Befehl ENABLE SESSIONS.

Inaktivierte abgehende Sitzungen
: Gibt die Namen der Server an, zu denen eine Übertragung zwischen Servern nicht zulässig ist. Um abgehende Serversitzungen zu aktivieren, verwenden Sie den Befehl ENABLE SESSIONS.

Abrechnung
: Gibt an, ob am Ende jeder Sitzung des Clientknotens ein Abrechnungssatz generiert wird.

Aufbewahrungsdauer für Aktivitätenprotokoll
: Gibt die Anzahl der Tage, die Informationen im Aktivitätenprotokoll aufbewahrt werden, oder die Größe des Protokolls an.

Anzahl Sätze im Aktivitätenprotokoll
: Gibt die Anzahl der Sätze im Aktivitätenprotokoll an.

Größe des Aktivitätenprotokolls
: Gibt die Größe des Aktivitätenprotokolls an.

Aufbewahrungszeitraum für Aktivitätsübersicht
: Gibt die Anzahl der Tage an, die Informationen in der SQL-Aktivitätsübersichtstabelle aufbewahrt werden sollen.

Intervall für Lizenzprüfung
: Gibt den Zeitraum an (in Tagen), nach dessen Ablauf der Lizenzmanager automatisch die IBM Spectrum Protect-Lizenz prüft. Zusätzliche Lizenzinformationen sind verfügbar, wenn der Befehl QUERY LICENSE verwendet wird.

Letzte Lizenzprüfung
: Gibt an, wann die Lizenzprüfung zuletzt durchgeführt wurde (Datum und Uhrzeit). Zusätzliche Lizenzinformationen sind verfügbar, wenn der Befehl QUERY LICENSE verwendet wird.

Server-Lizenzbestimmungen
: Gibt an, ob sich der Server an die Lizenzbedingungen hält (Gültig) oder nicht (Fehlgeschlagen). Mit dem Befehl QUERY LICENSE kann abgefragt werden, aufgrund welcher Faktoren der Server nicht die Lizenzbedingungen einhält.

Zentraler Scheduler
: Gibt an, ob die zentrale Zeitplanung aktiv oder inaktiv ist.

Maximale Anzahl Sitzungen
: Gibt die maximale Anzahl Client-/Serversitzungen an.

Maximale Anzahl geplante Sitzungen
: Gibt die maximale Anzahl Client-/Serversitzungen an, die bei der Arbeit mit einem Verarbeitungszeitplan verfügbar sind.

Aufbewahrungszeitraum für Ereignissätze
: Gibt an, wie lange Scheduler-Ereignissätze beibehalten werden (Anzahl Tage).

Dauer von Clientaktionen
: Gibt den Zeitraum an, in dem der Client den mit dem Befehl DEFINE CLIENTACTION definierten Zeitplan verarbeitet.

Zeitplanzufallsgenerierung (Prozent)
: Gibt an, welcher Anteil des Startfensters für die Ausführung von geplanten Ereignissen im Clientabfragemodus verwendet wird.

Intervall für Zeitplanabfragen
: Gibt die Häufigkeit an, mit der Clients den Server nach geplanter Arbeit abfragen, und zwar im Clientabfragemodus. Lautet der Wert in diesem Feld 'Client', wird die Abfragehäufigkeit vom Clientknoten bestimmt.

Maximale Anzahl Befehlswiederholungen
: Gibt an, wie oft ein Client-Scheduler maximal versucht, einen geplanten Befehl auszuführen, nachdem ein Versuch fehlgeschlagen ist. Lautet der Wert in diesem Feld 'Client', wird die maximale Anzahl vom Clientknoten bestimmt.

Wiederholungszeitlimit
: Gibt die Anzahl Minuten zwischen fehlgeschlagenen Versuchen des Client-Schedulers an, den Server anzusprechen oder einen geplanten Befehl auszuführen. Lautet der Wert in diesem Feld 'Client', bestimmt der Clientknoten die Anzahl der Minuten.

Prüfstufe für clientseitige Deduplizierung
: Gibt einen Prozentsatz der Bereiche an, die vom IBM Spectrum Protect-Server geprüft werden sollen. Die Bereiche werden während der clientseitigen Datendeduplizierung erstellt.

Planungsmodi
: Gibt die vom Server unterstützten Modi für die zentrale Zeitplanung an.

Aktive Empfänger
: Gibt die Empfänger an, für die das Protokollieren von Ereignissen begonnen hat.

Konfigurationsmanager?
: Gibt an, ob der Server ein Konfigurationsmanager ist.

Aktualisierungsintervall
: Gibt das Intervall an, nach dem der verwaltete Server eine Aktualisierung aller Änderungen von einem Konfigurationsmanager anfordert.

Datum/Zeit der letzten Aktualisierung
: Wenn der Server ein verwalteter Server ist, werden das Datum und die Uhrzeit der letzten erfolgreichen Aktualisierung der Konfigurationsdaten vom Konfigurationsmanager angegeben.

Anzeigen von Nachrichtenkontext
: Gibt an, ob das Anzeigen von Nachrichtenkontext aktiviert oder inaktiviert ist.

Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis
: Gibt die ungefähre Anzahl der Minuten an, die Inhaltsverzeichnisdaten, auf die nicht verwiesen wird, in der Datenbank aufbewahrt werden.

Maschinen-GUID
: Die global eindeutige ID (Globally Unique Identifer = GUID) zu dem Zeitpunkt, als der Server das letzte Mal gestartet wurde. Diese GUID identifiziert das Hostsystem, zu dem der aktuelle Server gehört.

Aufbewahrungsschutz für Archivierung
: Gibt an, ob der Aufbewahrungsschutz für Archivierungsdaten aktiviert oder inaktiviert ist.

Datenbankverzeichnisse
: Gibt die Positionen der Datenbankverzeichnisse an.

Gesamtspeicherbereich des Dateisystems (MB)
: Gibt die Gesamtgröße des Dateisystems an.

Verwendeter Speicherbereich im Dateisystem (MB)
: Gibt den Speicherbereich an, der in dem Dateisystem verwendet wird.

Freier verfügbarer Speicherbereich (MB)

Gibt den Speicherbereich an, der verfügbar ist.

Verschlüsselungsstufe
: Gibt die Datenverschlüsselungsstufe an: AES oder DES.

Aktualisierungsintervall für Client-CPU-Informationen
: Gibt die Anzahl der Tage an, die zwischen Clientsuchläufen nach CPU-Informationen vergehen, die für PVU-Schätzungen verwendet werden.

Abgehende Replikation
: Gibt an, ob die Replikationsverarbeitung aktiviert oder inaktiviert ist. Ist die abgehende Replikation inaktiviert, können keine neuen Replikationsprozesse auf dem Server gestartet werden.

Zielreplikationsserver
: Gibt den Namen des Servers an, der das Ziel für Knotenreplikationsoperationen ist. Ist kein Zielreplikationsserver vorhanden, ist dieses Feld leer.

Standardreplikationsregel für Archivierungsdaten
: Gibt die Serverreplikationsregel an, die für Archivierungsdaten gilt. Die folgenden Werte sind gültig:

  ALL_DATA
  : Repliziert Archivierungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

  ALL_DATA_HIGH_PRIORITY
  : Repliziert Archivierungsdaten. Die Daten werden mit einer hohen Priorität repliziert.

  NONE
  : Die Archivierungsdaten werden nicht repliziert.

Standardreplikationsregel für Sicherungsdaten
: Gibt die Serverreplikationsregel an, die für Sicherungsdaten gilt. Die folgenden Werte sind gültig:

  ALL_DATA
  : Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert.

  ACTIVE_DATA
  : Repliziert nur aktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert.
    Achtung: Wenn Sie ACTIVE_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

    - Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
    - Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
    - Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

    Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

  ALL_DATA_HIGH_PRIORITY
  : Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit einer hohen Priorität repliziert.

  ACTIVE_DATA_HIGH_PRIORITY

    Diese Regel entspricht der Replikationsregel ACTIVE_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

  NONE
  : Die Sicherungsdaten werden nicht repliziert.

Standardreplikationsregel für speicherverwaltete Daten
: Gibt die Serverreplikationsregel an, die für speicherverwaltete Daten gilt. Die folgenden Werte sind gültig:

  ALL_DATA
  : Repliziert speicherverwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.

  ALL_DATA_HIGH_PRIORITY
  : Repliziert speicherverwaltete Daten. Die Daten werden mit einer hohen Priorität repliziert.

  NONE
  : Speicherverwaltete Daten werden nicht repliziert.

Aufbewahrungszeitraum für Replikationsdatensätze
: Gibt die Anzahl der Tage an, die Replikationsprotokolldatensätze in der Datenbank des Quellenreplikationsservers aufbewahrt werden.

LDAP-Benutzer
: Gibt die Benutzer-ID an, die im Befehl SET LDAPUSER angegeben wurde. Diese Benutzer-ID kann Verwaltungsbefehle für den Namensbereich ausgeben, der für IBM Spectrum Protect auf dem LDAP-Verzeichnisserver reserviert ist.

LDAP-Kennwort definiert
: Dieses Ausgabefeld zeigt an, ob ein Kennwort für die Benutzer-ID definiert ist, die im Befehl SET LDAPUSER angegeben wurde. Die Werte lauten YES und NO. Lautet der Wert YES, kann die im Befehl SET LDAPUSER angegebene Benutzer-ID Verwaltungsbefehle für den LDAP-Namensbereich ausgeben, der für IBM Spectrum Protect reserviert ist. Lautet der Wert NO, geben Sie den Befehl SET LDAPPASSWORD aus, um das Kennwort für die Benutzer-ID festzulegen, die im Befehl SET LDAPUSER angegeben wurde.

Standardauthentifizierung
: Gibt die Standardkennwortauthentifizierungsmethode an: LOCAL oder LDAP.

Authentifizierungsziel	Authentifizierungsmethode
IBM Spectrum Protect-Server	LOCAL
LDAP-Verzeichnisserver	LDAP

: Wenn Sie den Befehl SET DEFAULTAUTHENTICATION ausgeben, definieren Sie die resultierende Authentifizierungsmethode für alle Befehle REGISTER ADMIN und REGISTER NODE. Der Standardwert ist LOCAL.

Adresse höherer Ebene für Übernahme
: Gibt die Adresse höherer Ebene für den Übernahmeserver an, der vom Client verwendet wird. Clientzurückschreibungsoperationen werden durch Übernahme an diese Adresse der höheren Ebene übertragen, wenn die vom Client verwendete Schnittstelle von der Schnittstelle abweicht, die von der Replikation verwendet wird.

Aufbewahrungszeit für Scratchpad
: Gibt die Anzahl Tage an, die Scratchpadeinträge nach ihrer letzten Aktualisierung aufbewahrt werden.

Replikationswiederherstellung beschädigter Dateien
: Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen. Dies ist eine systemseitige Einstellung. Ist ON angegeben, kann der Knotenreplikationsprozess so konfiguriert werden, dass beschädigte Dateien auf einem Quellenreplikationsserver erkannt und durch unbeschädigte Dateien von einem Zielreplikationsserver ersetzt werden. Ist OFF angegeben, werden beschädigte Dateien nicht durch einen Zielreplikationsserver wiederhergestellt.

SUR-Belegung (TB)
: Wenn Sie über eine Lizenz für IBM Spectrum Protect Suite (SUR) verfügen, gibt dieses Feld die SUR-Belegung auf dem Server an. Die *SUR-Belegung* ist die Größe des Speicherbereichs, die zum Speichern der Daten verwendet wird, die von den IBM Spectrum Protect-Produkten im SUR-Produktpaket verwaltet werden.

SUR-Belegung (Datum/Zeit)
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die SUR-Belegung zuletzt erfasst wurde.

Front-End-Kapazität (MB)
: Gibt den Umfang der primären Daten an, die von Clients gesichert werden. Clients umfassen Anwendungen, virtuelle Maschinen und Systeme. Dieser Wert wird für das Front-End-Lizenzierungsmodell verwendet.

Anzahl Front-End-Clients
: Gibt die Anzahl der Clients an, die eine Kapazitätsnutzung auf der Basis des Front-End-Lizenzierungsmodells zurückgemeldet haben.

Datum für Front-End-Kapazität
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der Front-End-Kapazitätsdaten zuletzt erfasst wurden.

Produktangebot
: Gibt ein Produktangebot an.

Mit dem Befehl SET PRODUCTOFFERING angegebener Wert	In der Befehlsausgabe für QUERY STATUS angezeigter Wert
ENTry	IBM Spectrum Protect Entry
DATARet	IBM Spectrum Protect for Data Retention
BASIC	IBM Spectrum Protect
EE	IBM Spectrum Protect Extended Edition
SUIte	IBM Spectrum Protect Suite
SUITEEntry	IBM Spectrum Protect Suite Entry
SUITEArchive	IBM Spectrum Protect Suite - Archive
SUITEProtectier	IBM Spectrum Protect Suite - ProtecTier
SUITEFrontend	IBM Spectrum Protect Suite - FrontEnd
SUITEENTRYFrontend	IBM Spectrum Protect Suite Entry - FrontEnd
CLEAR	NULL

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY STATUS

Befehl	Beschreibung
BEGIN EVENTLOGGING	Startet das Ereignisprotokoll für einen bestimmten Empfänger.
DISABLE REPLICATION	Verhindert die Verarbeitung abgehender Replikation auf einem Server.
DISABLE SESSIONS	Verhindert, dass neue Sitzungen auf IBM Spectrum Protect zugreifen, lässt jedoch zu, dass bestehende Sitzungen fortgesetzt werden.
ENABLE REPLICATION	Ermöglicht die Verarbeitung abgehender Replikation auf einem Server.
ENABLE SESSIONS	Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.

Befehl	Beschreibung
END EVENTLOGGING	Beendet das Ereignisprotokoll für einen bestimmten Empfänger.
QUERY LICENSE	Zeigt Informationen über Lizenzen und Prüfvorgänge an.
SET ACCOUNTING	Gibt an, ob am Ende jeder Clientsitzung Abrechnungssätze erstellt werden.
SET ACTLOGRETENTION	Gibt die Anzahl Tage an, die Protokollsätze im Aktivitätenprotokoll aufbewahrt werden sollen.
SET CONTEXTMESSAGING	Gibt an, dass das Anzeigen von Nachrichtenkontext für eine Nachricht ANR9999D aktiviert werden soll.
SET CPUINFOREFRESH	Gibt die Anzahl der Tage zwischen Clientsuchläufen nach Workstationinformationen an, die für PVU-Schätzungen verwendet werden.
SET CROSSDEFINE	Gibt an, ob Server überkreuz definiert werden sollen.
SET DEDUPVERIFICATIONLEVEL	Gibt den Prozentsatz der Bereiche an, die vom Server während der clientseitigen Deduplizierung geprüft werden sollen.
SET DEFAULTAUTHENTICATION	Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an.
SET EVENTRETENTION	Gibt die Anzahl Tage für die Aufbewahrung von Sätzen geplanter Operationen an.
SET LDAPPASSWORD	Legt das Kennwort für den LDAPUSER fest.
SET LDAPUSER	Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht.
SET MAXCMDRETRIES	Gibt die maximale Anzahl Wiederholungen nach der fehlgeschlagenen Ausführung eines geplanten Befehls an.
SET MAXSCHEDSESSIONS	Gibt die maximale Anzahl Client-/Serversitzungen an, die bei der Arbeit mit einem Verarbeitungszeitplan verfügbar sind.
SET PASSEXP	Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.
SET PRODUCTOFFERING	Definiert das für Ihr Unternehmen lizenzierte Produktangebot.
SET QUERYSCHEDPERIOD	Gibt die Häufigkeit an, mit der Clients geplante Arbeit im Clientsendeaufrufmodus abrufen.
SET RANDOMIZE	Gibt die Zufallsgenerierung von Startzeiten innerhalb eines Fensters für Zeitpläne im Clientsendeaufrufmodus an.
SET REPLRECOVERDAMAGED	Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.
SET RETRYPERIOD	Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.
SET SCHEDMODES	Gibt den zentralen Planungsmodus für den Server an.
SET SERVERHLADDRESS	Gibt die Adresse der höheren Ebene eines Servers an.
SET SERVERLLADDRESS	Gibt die Adresse der unteren Ebene eines Servers an.
SET SERVERNAME	Gibt den Namen an, unter dem der Server registriert ist.
SET SERVERPASSWORD	Gibt das Serverkennwort an.
SET SUMMARYRETENTION	Gibt die Anzahl Tage an, die Informationen in der Aktivitätsübersichtstabelle aufbewahrt werden sollen.
SET TOCLOADRETENTION	Gibt die Anzahl Minuten an, die Informationen für Inhaltsverzeichnisgruppen, auf die nicht verwiesen wird, aufbewahrt werden sollen.

QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)

Mit diesem Befehl können Sie Informationen zu Schwellenwerten für die Statusüberwachung anzeigen.

Mit Statusüberwachungsschwellenwerten werden die definierten Bedingungen mit den Serverabfragen für die Statusüberwachung verglichen und die Ergebnisse in die Statusüberwachungstabelle eingefügt.

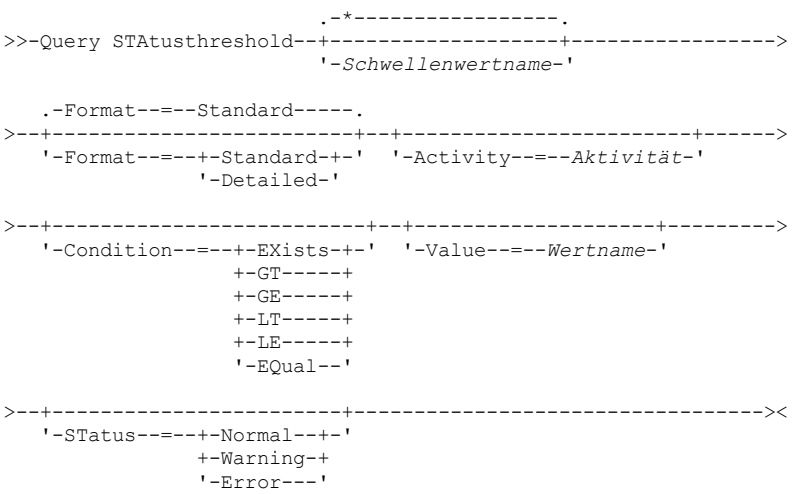
Es können mehrere Schwellenwerte für eine Aktivität definiert werden. Sie können beispielsweise einen Schwellenwert erstellen, der einen Warnstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 80 % ist. Sie können dann einen anderen Schwellenwert erstellen, der einen Fehlerstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 90 % ist.

Anmerkung: Wenn bereits ein Schwellenwert für eine Bedingung EXISTS definiert ist, können Sie keinen anderen Schwellenwert mit einem der anderen Bedingungstypen definieren.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Schwellenwertname
: Gibt den Schwellenwertnamen an. Der Name darf 48 Zeichen nicht überschreiten.

Format
: Gibt an, wie die Informationen angezeigt werden. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen für die angegebenen Statusschwellenwerte angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen für die angegebenen Statusschwellenwerte angezeigt werden.

Activity
: Gibt die Aktivität an, für die Statusanzeiger angezeigt werden sollen. Wird kein Wert angegeben, werden Informationen für alle Aktivitäten angezeigt. Eine Liste der Aktivitäten befindet sich in der Beschreibung des Befehls DEFINE STATUSTHRESHOLD.

Condition
: Begrenzt die Ausgabe auf die Schwellenwerte, die mit dem angegebenen Wert übereinstimmen. Gültige Werte:

  EXists
  : Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich EXISTS ist.

  GT
  : Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich GT ist.

  GE
  : Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich GE ist.

  LT
  : Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich LT ist.

  LE
  : Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich LE ist.

  EQual
  : Zeigt Statusschwellenwerte an, bei denen die Bedingung gleich EQUAL ist.

Value
: Zeigt Schwellenwerte an, die den angegebenen Wert haben. Wird kein Wert angegeben, werden Informationen für alle Werte angezeigt. Sie können eine ganze Zahl von 0 bis 9223372036854775807 angeben.

STatus

Zeigt Statusschwellenwerte an, die den angegebenen Statuswert haben. Wird kein Wert angegeben, werden Informationen für alle Werte angezeigt. Gültige Werte:

Normal
: Zeigt die Statusschwellenwerte an, die einen normalen Statuswert haben.

Warnung
: Zeigt die Statusschwellenwerte an, die einen Warnstatuswert haben.

Fehler
: Zeigt die Statusschwellenwerte an, die einen Fehlerstatuswert haben.

Statusschwellenwert abfragen

Mit dem folgenden Befehl alle Statusschwellenwerte abfragen:

```
query statusthreshold
```

```
Schwellenwert-    Name der          Bedingungs- Wert      Berichts-
name              Aktivität         name                status
---------------   ---------------   ---------   -------   -------
ACTIVELOGCHECK    AUSLASTUNG DER    >           90        ERROR
                   AKTIVEN
                   PROTOKOLLDATEI
                   (%)
AVGSTGPLW         DURCHSCHNITTL.    >           85        WARNING
                   SPEICHERPOOL-
                   AUSLASTUNG
                   (%)
AVGSTGPLE         DURCHSCHNITTL.    >           90        ERROR
                   SPEICHERPOOL-
                   AUSLASTUNG
                   (%)
```

Statusschwellenwerte abfragen und Detailformat anzeigen

Mit dem folgenden Befehl Statusschwellenwerte abfragen und die Ausgabe im Detailformat anzeigen:

```
query statusthreshold f=d
```

```
Schwellenwertname: ACTIVELOGCHECK
 Name der Aktivität: AUSLASTUNG DER AKTIVEN PROTOKOLLDATEI (%)
Bedingungsname: >
               Wert: 90
     Berichtsstatus: ERROR
         Servername: TSMAWP24

  Schwellenwertname: AVGSTGPLW
 Name der Aktivität: DURCHSCHNITTLICHE SPEICHERPOOLAUSLASTUNG (%)
Bedingungsname: >
               Wert: 85
     Berichtsstatus: WARNING
         Servername: TSMAWP24

  Schwellenwertname: AVGSTGPLE
 Name der Aktivität: DURCHSCHNITTLICHE SPEICHERPOOLAUSLASTUNG (%)
Bedingungsname: >
               Wert: 95
     Berichtsstatus: ERROR
         Servername: TSMAWP24
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY STATUSTHRESHOLD

Befehl	Beschreibung
DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)	Definiert einen Schwellenwert für die Statusüberwachung.
DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)	Löscht einen Schwellenwert für die Statusüberwachung.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.

Befehl	Beschreibung
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.
UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)	Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.

QUERY STGPOOL (Speicherpools abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Speicherpools angezeigt werden. Mit diesem Befehl können auch Umlagerungsprozesse für Speicherpools überwacht werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                  .-*--------.  .-Format--=--Standard-----.
>>-Query STGpool--+----------+--+-------------------------+----->
                  '-Poolname-'  '-Format--=--+-Standard-+-'
                                             '-Detailed-'

   .-POoltype--=--ANY---------------.
>--+--------------------------------+-------------------------><
   '-POoltype--=--+-ANY-----------+-'
                  +-PRimary-------+
                  +-COpy----------+
                  +-COPYCONtainer-+
                  '-ACTIVEdata----'
```

Parameter

Poolname
: Gibt den Speicherpool an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherpools angezeigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Geben Sie einen der folgenden Werte an:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

POoltype
: Gibt den Typ des Speicherpools an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist ANY. Geben Sie einen der folgenden Werte an:

  ANY
  : Primäre Speicherpools, Kopienspeicherpools und Pools für aktive Daten abfragen.

  PRimary
  : Nur primäre Speicherpools abfragen.

  COpy
  : Nur Kopienspeicherpools abfragen.

  COPYCONtainer
  : Nur Containerkopienspeicherpools abfragen.

  ACTIVEdata

Nur Speicherpools für aktive Daten abfragen.

Beispiel: Ausführliche Informationen zu Plattenspeicherpools mit wahlfreiem Zugriff anzeigen

Tipp: In den Beispielen für die detaillierte Ausgabe sind einige Felder leer, da sie für die angegebene Umgebung nicht gelten.
Ausführliche Informationen zu einem Speicherpool mit dem Namen DISKPOOL anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool diskpool format=detailed
```

```
                     Speicherpoolname: DISKPOOL
                                         Speicherpooltyp: Primary
                                    Einheitenklassenname: DISK
                                              Speichertyp: DEVCLASS
                                                 Cloudtyp:
                                                Cloud-URL:
                                                 Cloud-ID:
                                           Cloudposition:
                                  Geschätzte Kapazität: 66 G
                           Speicherbereichsauslöser Ausl.: 0.0
                                  Auslastung in %: 0,0
                                  Umlagerung in %: 3.1
                        Prozent logische Belegung: 100.0
                      Obere Umlagerungsschwelle in %: 90
                     Untere Umlagerungsschwelle in %: 70
                              Umlagerungsverzögerung: 0
                               Umlagerung fortsetzen: Yes
                                 Umlagerungsprozesse: 1
                            Wiederherstellungsprozesse: 1
                                 Nächster Speicherpool:
                          Speicherpool wiederherstellen:
                            Schwelle für maximale Größe: No Limit
                                           Zugriff: Read/Write
                                      Beschreibung:
                                    Überlaufstandort:
                  Umgelagerte Dateien zwischenspeichern?:
                                    Zusammenfassen?: Group
                               Wiederherstellungsschwelle: 60
          Grenzwert für Wiederh. ausgelag. Datenträger:
                     Maximale Anzahl Arbeitsdatenträger: 32
                   Anzahl verwendeter Arbeitsdatenträger: 1
Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
                            Wird Umlagerung ausgeführt?: No
                            Umgelagerte Datenmenge (MB): 0.00
                        Abgelaufene Umlagerungszeit (Sek): 0
                       Wird Wiederherstellung ausgeführt?: No

    Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
                 Datum/Zeit der letzten Aktualisierung: 01/03/2014 13:57:16
                                Speicherpooldatenformat: Native
                                  Kopienspeicherpool(s):
                               Pool(s) für aktive Daten:
                          Kopieren bei Fehler fortsetzen?: No
                                               CRC-Daten: Yes
                                Wiederherstellungstyp: Threshold
                        Daten nach Löschen überschreiben: 2 Mal
                                   Daten deduplizieren?: No
          Prozesse zum Identifizieren doppelter Daten:
                                          Komprimiert:
                             Deduplizierungseinsparungen:
                              Komprimierungseinsparungen:
                       Eingesparter Gesamtspeicherbereich:
                         Modus für automatisches Kopieren: Client
                   Enthält vom Client deduplizierte Daten?: No
                         Maximale Anzahl simultaner Writer:
                                       Schutzprozesse:
                                    Schutzspeicherpool:
                          Lokale Speicherpools schützen:
                   Grenzwert für Datenträgerwiederherstellung:
                    Datum des letzten Schutzes in fernem Pool:
                   Datum des letzten Schutzes in lokalem Pool:
                          Deduplizierung erfordert Sicherung?:
                                       Verschlüsselt:
                                Prozent verschlüsselt:
                        Belegter Cloudspeicherbereich (MB):
                                          Bucketname:
                               Lokale geschätzte Kapazität:
                                   Lokale proz. Auslastung:
                          Lokale logische Belegung in Prozent:
```

Beispiel: Ausführliche Informationen zu Plattenspeicherpools mit sequenziellem Zugriff anzeigen

Ausführliche Informationen zu einem Speicherpool mit dem Namen FILEPOOL anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool filepool format=detailed
```

```
                                  Speicherpoolname: FILEPOOL
                                       Speicherpooltyp: Primary
                                  Einheitenklassenname: FILEC
                                            Speichertyp: DEVCLASS
                                               Cloudtyp:
                                             Cloud-URL:
                                               Cloud-ID:
                                           Cloudposition:
                                  Geschätzte Kapazität: 66 G
                           Speicherbereichsauslöser Ausl.: 0.0
                                         Auslastung in %: 0,0
                                         Umlagerung in %: 3.1
                               Prozent logische Belegung: 100.0
                           Obere Umlagerungsschwelle in %: 90
                          Untere Umlagerungsschwelle in %: 70
                                   Umlagerungsverzögerung: 0
                                    Umlagerung fortsetzen: Yes
                                      Umlagerungsprozesse: 1
                                Wiederherstellungsprozesse: 1
                                     Nächster Speicherpool:
                               Speicherpool wiederherstellen:
                                 Schwelle für maximale Größe: No Limit
                                                 Zugriff: Read/Write
                                            Beschreibung:
                                          Überlaufstandort:
                    Umgelagerte Dateien zwischenspeichern?:
                                          Zusammenfassen?: Group
                                Wiederherstellungsschwelle: 60
              Grenzwert für Wiederh. ausgelag. Datenträger:
                         Maximale Anzahl Arbeitsdatenträger: 32
                   Anzahl verwendeter Arbeitsdatenträger: 1
Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
                           Wird Umlagerung ausgeführt?: No
                           Umgelagerte Datenmenge (MB): 0.00

                Abgelaufene Umlagerungszeit (Sek): 0
                     Wird Wiederherstellung ausgeführt?: No
               Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
                     Datum/Zeit der letzten Aktualisierung: 01/02/2014 13:57:16
                                Speicherpooldatenformat: Native
                                  Kopienspeicherpool(s):
                               Pool(s) für aktive Daten:
                           Kopieren bei Fehler fortsetzen?: No
                                             CRC-Daten: Yes
                                    Wiederherstellungstyp: Threshold
                         Daten nach Löschen überschreiben:
                                     Daten deduplizieren?: Yes
               Prozesse zum Identifizieren doppelter Daten: 1
                                           Komprimiert:
                           Deduplizierungseinsparungen: 65.396 K (49,99 %)
                            Komprimierungseinsparungen:
                        Eingesparter Gesamtspeicherbereich: 65.396 K (49,99 %)
                          Modus für automatisches Kopieren: Client
                   Enthält vom Client deduplizierte Daten?: Yes
                         Maximale Anzahl simultaner Writer:
                                        Schutzprozesse:
                                    Schutzspeicherpool:
                            Lokale Speicherpools schützen:
                 Grenzwert für Datenträgerwiederherstellung:
                  Datum des letzten Schutzes in fernem Pool:
                 Datum des letzten Schutzes in lokalem Pool:
                        Deduplizierung erfordert Sicherung?:
                                        Verschlüsselt:
                                 Prozent verschlüsselt:
                          Belegter Cloudspeicherbereich (MB):
                                           Bucketname:
                                 Lokale geschätzte Kapazität:
                                    Lokale proz. Auslastung:
                          Lokale logische Belegung in Prozent:
```

Beispiel: Ausführliche Informationen zu sequenziellen Speicherpools anzeigen

Ausführliche Informationen zu einem sequenziellen Speicherpool für aktive Daten mit dem Namen FILEPOOL anzeigen, der eine Einheitenklasse FILE verwendet. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool filepool format=detailed
```

```
                                Speicherpoolname: FILEPOOL
                                     Speicherpooltyp: Active-data
                                Einheitenklassenname: FILEC
                                         Speichertyp: DEVCLASS
                                            Cloudtyp:
                                           Cloud-URL:
                                            Cloud-ID:
                                       Cloudposition:
                                Geschätzte Kapazität: 0.0 M
                           Speicherbereichsauslöser Ausl.: 0.0
                                        Auslastung in %: 0,0
                                        Umlagerung in %: 0.0
                             Prozent logische Belegung: 0.0
                          Obere Umlagerungsschwelle in %: 90
                        Untere Umlagerungsschwelle in %: 70
                                 Umlagerungsverzögerung: 0
                                  Umlagerung fortsetzen: Yes
                                    Umlagerungsprozesse: 1
                               Wiederherstellungsprozesse: 1
                                     Nächster Speicherpool:
                              Speicherpool wiederherstellen:
                                Schwelle für maximale Größe: No Limit
                                                Zugriff: Read/Write
                                           Beschreibung:
                                       Überlaufstandort:
                     Umgelagerte Dateien zwischenspeichern?:
                                       Zusammenfassen?: Group
                                Wiederherstellungsschwelle: 60
           Grenzwert für Wiederh. ausgelag. Datenträger:
                     Maximale Anzahl Arbeitsdatenträger: 99
                   Anzahl verwendeter Arbeitsdatenträger: 0
Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
                                Wird Umlagerung ausgeführt?: No
                                Umgelagerte Datenmenge (MB): 0.00

                    Abgelaufene Umlagerungszeit (Sek): 0
                         Wird Wiederherstellung ausgeführt?: No
               Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
                     Datum/Zeit der letzten Aktualisierung: 01/02/2014 11:37:57
                                  Speicherpooldatenformat: Native
                                    Kopienspeicherpool(s):
                                Pool(s) für aktive Daten:
                           Kopieren bei Fehler fortsetzen?:
                                                CRC-Daten: Yes
                                  Wiederherstellungstyp: Threshold
                         Daten nach Löschen überschreiben:
                                     Daten deduplizieren?: Yes
               Prozesse zum Identifizieren doppelter Daten: 1
                                               Komprimiert:
                           Deduplizierungseinsparungen: 65.396 K (49,99 %)
                            Komprimierungseinsparungen:
                        Eingesparter Gesamtspeicherbereich: 65.396 K (49,99 %)
                          Modus für automatisches Kopieren:
                     Enthält vom Client deduplizierte Daten?: No
                           Maximale Anzahl simultaner Writer:
                                            Schutzprozesse:
                                       Schutzspeicherpool:
                              Lokale Speicherpools schützen:
                       Grenzwert für Datenträgerwiederherstellung:
                        Datum des letzten Schutzes in fernem Pool:
                       Datum des letzten Schutzes in lokalem Pool:
                              Deduplizierung erfordert Sicherung?:
                                           Verschlüsselt:
                                  Prozent verschlüsselt:
                         Belegter Cloudspeicherbereich (MB):
                                               Bucketname:
                                Lokale geschätzte Kapazität:
                                    Lokale proz. Auslastung:
                        Lokale logische Belegung in Prozent:
```

Beispiel: Übersichtsdaten zu einem bestimmten Speicherpool anzeigen

Informationen zu einem Speicherpool mit dem Namen POOL1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool pool1
```

```
Speicher-   Einheiten-   Geschätzte  %    %    Ob.   Unt.  Nächster
poolname    klassenname  Kapazität  Ausl Uml.  Uml.  Uml.  Speicher-
                                               %     %     pool
----------  ----------   --------- ----- ----- ----  ---- --------
POOL1       DISK         58.5 M     0.8  0.7    90    70   POOL2
```

Beispiel: Ausführliche Informationen zu einem 8-mm-Bandspeicherpool anzeigen

Ausführliche Informationen über den Speicherpool 8MMPOOL anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool 8mmpool format=detailed
```

```
                              Speicherpoolname: 8MMPOOL
                                  Speicherpooltyp: Primary
                             Einheitenklassenname: 8MMTAPE
                                      Speichertyp: DEVCLASS
                                         Cloudtyp:
                                        Cloud-URL:
                                         Cloud-ID:
                                    Cloudposition:
                                Geschätzte Kapazität: 0.0 M
                          Speicherbereichsauslöser Ausl.: 0.0
                                  Auslastung in %: 0,0
                                  Umlagerung in %:
                               Prozent logische Belegung: 0.0
                          Obere Umlagerungsschwelle in %: 90
                         Untere Umlagerungsschwelle in %: 70
                                  Umlagerungsverzögerung: 0
                                   Umlagerung fortsetzen: Yes
                                     Umlagerungsprozesse: 1
                               Wiederherstellungsprozesse: 1
                                    Nächster Speicherpool:
                             Speicherpool wiederherstellen:
                               Schwelle für maximale Größe: 5 M
                                                Zugriff: Read/Write
                                           Beschreibung: Hauptspeicherpool
                                       Überlaufstandort: Room1234/Bldg31
                    Umgelagerte Dateien zwischenspeichern?:
                                       Zusammenfassen?: No
                                Wiederherstellungsschwelle: 60
          Grenzwert für Wiederh. ausgelag. Datenträger:
                     Maximale Anzahl Arbeitsdatenträger: 5
                   Anzahl verwendeter Arbeitsdatenträger: 3
Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
                                Wird Umlagerung ausgeführt?: No
                                Umgelagerte Datenmenge (MB): 0.00

                        Abgelaufene Umlagerungszeit (Sek): 0
                        Wird Wiederherstellung ausgeführt?: No
              Letzte Aktualisierung durch (Administrator): ADMIN
                    Datum/Zeit der letzten Aktualisierung: 01/08/2014 06:55:45
                                 Speicherpooldatenformat: Native
                                   Kopienspeicherpool(s): COPYPOOL1
                               Pool(s) für aktive Daten: ACTIVEPOOL1 ACTIVEPOOL2
                          Kopieren bei Fehler fortsetzen?: Yes
                                            CRC-Daten: Yes
                                     Wiederherstellungstyp: Threshold
                           Daten nach Löschen überschreiben:
                                       Daten deduplizieren?: No
              Prozesse zum Identifizieren doppelter Daten:
                                          Komprimiert:
                               Deduplizierungseinsparungen:
                                Komprimierungseinsparungen:
                         Eingesparter Gesamtspeicherbereich:
                                          Komprimiert: No
                               Deduplizierungseinsparungen:
                                Komprimierungseinsparungen:
                         Eingesparter Gesamtspeicherbereich:
                           Modus für automatisches Kopieren: Client
                      Enthält vom Client deduplizierte Daten?: No
                            Maximale Anzahl simultaner Writer:
                                       Schutzprozesse:
                                    Schutzspeicherpool:
                           Lokale Speicherpools schützen:
                Grenzwert für Datenträgerwiederherstellung:
            Datum des letzten Schutzes in fernem Pool:
                Datum des letzten Schutzes in lokalem Pool:
                       Deduplizierung erfordert Sicherung?:
                                       Verschlüsselt:
                                Prozent verschlüsselt:
                         Belegter Cloudspeicherbereich (MB):
                                          Bucketname:
                                Lokale geschätzte Kapazität:
                                    Lokale proz. Auslastung:
                           Lokale logische Belegung in Prozent:
```

Beispiel: Ausführliche Informationen zum Speicherpool NAS2CLASS anzeigen

Ausführliche Informationen zum Speicherpool NAS2LIBPOOL anzeigen. Bei der Definition dieses Speicherpools wird das Datenformat auf NETAPPDUMP gesetzt. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool nas2libpool format=detailed
```

```
                     Speicherpoolname: NAS2
                                          Speicherpoolname: NAS2LIBPOOL
                                           Speicherpooltyp: Primary
                                       Einheitenklassenname: NAS2CLASS
                                                 Speichertyp: DEVCLASS
                                                    Cloudtyp:
                                                  Cloud-URL:
                                                    Cloud-ID:
                                               Cloudposition:
                                        Geschätzte Kapazität: 0.0 M
                                 Speicherbereichsauslöser Ausl.:
                                               Auslastung in %: 0,0
                                               Umlagerung in %:
                                     Prozent logische Belegung: 0.0
                                 Obere Umlagerungsschwelle in %:
                                Untere Umlagerungsschwelle in %:
                                         Umlagerungsverzögerung:
                                          Umlagerung fortsetzen:
                                            Umlagerungsprozesse:
                                    Wiederherstellungsprozesse:
                                         Nächster Speicherpool:
                                  Speicherpool wiederherstellen:
                                    Schwelle für maximale Größe:
                                                       Zugriff: Read/Write
                                                  Beschreibung:
                                                Überlaufstandort:
                        Umgelagerte Dateien zwischenspeichern?:
                                                Zusammenfassen?: Group
                                     Wiederherstellungsschwelle:
                    Grenzwert für Wiederh. ausgelag. Datenträger:
                               Maximale Anzahl Arbeitsdatenträger: 50
                             Anzahl verwendeter Arbeitsdatenträger: 0
               Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
                                    Wird Umlagerung ausgeführt?:
                                    Umgelagerte Datenmenge (MB):

Abgelaufene Umlagerungszeit (Sek):
         Wird Wiederherstellung ausgeführt?:
Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
      Datum/Zeit der letzten Aktualisierung: 01/02/2014 16:24:43
                        Speicherpooldatenformat: NetApp Dump
                          Kopienspeicherpool(s):
                       Pool(s) für aktive Daten:
             Kopieren bei Fehler fortsetzen?: No
                                     CRC-Daten: No
                           Wiederherstellungstyp:
            Daten nach Löschen überschreiben:
                            Daten deduplizieren?: No
Prozesse zum Identifizieren doppelter Daten:
                                    Komprimiert:
                  Deduplizierungseinsparungen:
                   Komprimierungseinsparungen:
          Eingesparter Gesamtspeicherbereich:
            Modus für automatisches Kopieren: Client
    Enthält vom Client deduplizierte Daten?: No
          Maximale Anzahl simultaner Writer:
                                Schutzprozesse:
                           Schutzspeicherpool:
              Lokale Speicherpools schützen:
 Grenzwert für Datenträgerwiederherstellung:

  Datum des letzten Schutzes in fernem Pool:
 Datum des letzten Schutzes in lokalem Pool:
        Deduplizierung erfordert Sicherung?:
                                Verschlüsselt:
                        Prozent verschlüsselt:
         Belegter Cloudspeicherbereich (MB):
                                  Bucketname:
                 Lokale geschätzte Kapazität:
                     Lokale proz. Auslastung:
         Lokale logische Belegung in Prozent:
```

Beispiel: Ausführliche Informationen zu einem Verzeichniscontainerspeicherpool anzeigen, der für die Datendeduplizierung verwendet wird

Zeigen Sie ausführliche Informationen zum Verzeichniscontainerspeicherpool DPOOL1 an. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool dpool1 format=detailed

                                  Speicherpoolname: DPOOL1
                                       Speicherpooltyp: Primary
                                  Einheitenklassenname:
                                            Speichertyp: Verzeichnis
                                               Cloudtyp:
                                             Cloud-URL:
                                               Cloud-ID:
                                          Cloudposition:
                                  Geschätzte Kapazität: 798 G
                           Speicherbereichsauslöser Ausl.:
                                         Auslastung in %: 3,4
                                         Umlagerung in %:
                               Prozent logische Belegung: 100.0
                          Obere Umlagerungsschwelle in %:
                        Untere Umlagerungsschwelle in %:
                                  Umlagerungsverzögerung:
                                   Umlagerung fortsetzen:
                                     Umlagerungsprozesse:
                                Wiederherstellungsprozesse:
                                     Nächster Speicherpool:
                              Speicherpool wiederherstellen:
                                Schwelle für maximale Größe: No Limit
                                                Zugriff: Read/Write
                                           Beschreibung:
                                        Überlaufstandort:
                      Umgelagerte Dateien zwischenspeichern?:
                                        Zusammenfassen?:
                               Wiederherstellungsschwelle:
             Grenzwert für Wiederh. ausgelag. Datenträger:
                        Maximale Anzahl Arbeitsdatenträger:
                      Anzahl verwendeter Arbeitsdatenträger:
Verzögerungszeitraum für Containerwiederverwendung: 1 Tag(e)
                                Wird Umlagerung ausgeführt?:
                                Umgelagerte Datenmenge (MB):


                    Abgelaufene Umlagerungszeit (Sek):
                         Wird Wiederherstellung ausgeführt?:
               Letzte Aktualisierung durch (Administrator): SERVER_CONSOLE
                     Datum/Zeit der letzten Aktualisierung: 01/02/2014 16:24:43
                                  Speicherpooldatenformat: Native
                                    Kopienspeicherpool(s):
                                 Pool(s) für aktive Daten:
                           Kopieren bei Fehler fortsetzen?:
                                                CRC-Daten: No
                                    Wiederherstellungstyp:
                           Daten nach Löschen überschreiben:
                                     Daten deduplizieren?: Yes
                Prozesse zum Identifizieren doppelter Daten:
                                               Komprimiert: Yes
Belegter Speicherbereich für geschützte Daten: 1.599 M
                    Anstehender Speicherbereich insgesamt: 100 M
                              Deduplizierungseinsparungen: 1.331 M (67,56 %)
                               Komprimierungseinsparungen: 194.805 K (29,82 %)
                  Eingesparter Gesamtspeicherbereich: 1.521 M (77,22 %)
                            Modus für automatisches Kopieren:
                    Enthält vom Client deduplizierte Daten?:
                          Maximale Anzahl simultaner Writer: No Limit
                                              Schutzprozesse:
                                        Schutzspeicherpool: DPOOL2
                               Lokale Speicherpools schützen:
                 Grenzwert für Datenträgerwiederherstellung:
                               Datum des letzten Schutzes:
                  Datum des letzten Schutzes in fernem Pool:
                 Datum des letzten Schutzes in lokalem Pool:
                        Deduplizierung erfordert Sicherung?:
                                               Verschlüsselt:
                                  Prozent verschlüsselt: 34,56 %
                           Belegter Cloudspeicherbereich (MB):
                                                Bucketname:
                                  Lokale geschätzte Kapazität:
                                      Lokale proz. Auslastung:
                           Lokale logische Belegung in Prozent:
```

Beispiel: Ausführliche Informationen zu einem Cloud-Containerspeicherpool anzeigen, der für die Datendeduplizierung verwendet wird

Zeigen Sie ausführliche Informationen zum Cloud-Containerspeicherpool CPOOL1 an. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpool cpool1 format=detailed

                                    Speicherpoolname: CPOOL1
                                         Speicherpooltyp: Primary
                                    Einheitenklassenname:
                                             Speichertyp: CLOUD
                                                Cloudtyp: SWIFT
                                              Cloud-URL: http://localhost.local
                                                Cloud-ID: Bailey
                                           Cloudposition: ONPREMISE
                                    Geschätzte Kapazität:
                               Speicherbereichsauslöser Ausl.:
                                           Auslastung in %:
                                           Umlagerung in %:
                                 Prozent logische Belegung: 0.0
                               Obere Umlagerungsschwelle in %:
                              Untere Umlagerungsschwelle in %:
                                        Umlagerungsverzögerung:
                                         Umlagerung fortsetzen:
                                           Umlagerungsprozesse:
                                Wiederherstellungsprozesse:
                                        Nächster Speicherpool:
                             Speicherpool wiederherstellen:
                               Schwelle für maximale Größe: No Limit
                                                   Zugriff: Read/Write
                                            Beschreibung:
                                          Überlaufstandort:
                         Umgelagerte Dateien zwischenspeichern?:
                                          Zusammenfassen?:
                                 Wiederherstellungsschwelle:
                      Grenzwert für Wiederh. ausgelag. Datenträger:
                                Maximale Anzahl Arbeitsdatenträger:
                              Anzahl verwendeter Arbeitsdatenträger:
Verzögerungszeitraum für die Wiederverwendung des Datenträgers: 1
                                    Wird Umlagerung ausgeführt?:
                                    Umgelagerte Datenmenge (MB):

                                Abgelaufene Umlagerungszeit (Sek):
                               Wird Wiederherstellung ausgeführt?:
                        Letzte Aktualisierung durch (Administrator): CODY
                              Datum/Zeit der letzten Aktualisierung: 2015-05-28, 10:47:52
                                       Speicherpooldatenformat: Native
                                         Kopienspeicherpool(s):
                                      Pool(s) für aktive Daten:
                                 Kopieren bei Fehler fortsetzen?:
                                                   CRC-Daten: No
                                        Wiederherstellungstyp:
                                 Daten nach Löschen überschreiben:
                                          Daten deduplizieren?: Yes
                        Prozesse zum Identifizieren doppelter Daten:
                                                  Komprimiert: Yes
                                Deduplizierungseinsparungen: 9.241 K (89,76 %)
                                 Komprimierungseinsparungen: 1.033 K (98,81 %)
                           Eingesparter Gesamtspeicherbereich: 10.274 K (99,79 %)
                             Modus für automatisches Kopieren:
                        Enthält vom Client deduplizierte Daten?:
                              Maximale Anzahl simultaner Writer: No Limit
                                           Schutzprozesse:
                                        Schutzspeicherpool:
                                Lokale Speicherpools schützen:
                         Grenzwert für Datenträgerwiederherstellung:
                          Datum des letzten Schutzes in fernem Pool:
                         Datum des letzten Schutzes in lokalem Pool:
                                Deduplizierung erfordert Sicherung?:
                                           Verschlüsselt: Yes
                                  Prozent verschlüsselt: 34,56 %
                           Belegter Cloudspeicherbereich (MB): 4.231
                                           Bucketname: ibmsp.
                                                      8ae4ec058cf11e680fe0a270000000
                                  Lokale geschätzte Kapazität: 168 G
                                      Lokale proz. Auslastung: 0,1
                             Lokale logische Belegung in Prozent: 100,0
```

Feldbeschreibungen

Speicherpoolname
: Der Name des Speicherpools.

Speicherpooltyp
: Der Typ des Speicherpools.

Einheitenklassenname
: Der Name der Einheitenklasse, die dem Speicherpool zugeordnet ist.

Speichertyp
Der Typ des Speichers, der für den Speicherpool definiert ist. Die folgenden Speichertypen können angezeigt werden:

DEVCLASS
Der Speicherpool gibt eine Einheitenklasse an, die den Typ der Einheit bestimmt, auf der Daten gespeichert werden.
DIRECTORY
Der Speicherpool erstellt logische Container für Daten in Dateisystemverzeichnissen.
CLOUD
Der Speicherpool erstellt logische Container für Daten in einer Cloudumgebung.

Cloudtyp
Für Cloudspeicherpools der Typ der Cloudplattform.
Cloud-URL
Für Cloudspeicherpools die URL für den Zugriff auf die private On-Premises-Cloud oder die öffentliche Off-Premises-Cloud.
Cloud-ID
Für Cloudspeicherpools die Benutzer-ID für den Zugriff auf die private On-Premises-Cloud oder die öffentliche Off-Premises-Cloud.
Cloudposition
Gibt für Cloudspeicherpools an, ob die Cloud eine private On-Premises-Cloud oder eine öffentliche Off-Premises-Cloud ist.

Geschätzte Kapazität
Die geschätzte Kapazität des Speicherpools in Megabyte (M) oder Gigabyte (G).

Bei Platteneinheiten (DISK) ist die geschätzte Kapazität die Kapazität aller Datenträger im Speicherpool, einschließlich der Datenträger, die abgehängt sind.

Für Speicherpools mit sequenziellem Zugriff ist die geschätzte Kapazität die Summe des geschätzten Speicherbereichs aller Datenträger mit sequenziellem Zugriff in dem Speicherpool, unabhängig von ihrem Zugriffsmodus. Mindestens ein Datenträger muss in einem Speicherpool mit sequenziellem Zugriff verwendet werden (entweder ein Arbeitsdatenträger oder ein privater Datenträger), um die geschätzte Kapazität zu berechnen.

Für Bandeinheiten und FILE-Einheiten schließt die geschätzte Kapazität für den Speicherpool die folgenden Faktoren ein:

- Die Kapazität aller Arbeitsdatenträger, die der Speicherpool bereits angefordert hat oder anfordern kann. Die Anzahl der Arbeitsdatenträger wird mit dem Parameter MAXSCRATCH im Befehl DEFINE STGPOOL oder UPDATE STGPOOL definiert.
- Die Gesamtzahl der verfügbaren Arbeitsdatenträger im Bandarchiv.
- Die geschätzte Kapazität ist der Wert von MAXSCRATCH bzw. die Gesamtzahl der verfügbaren Arbeitsdatenträger im Bandarchiv, je nachdem, welcher Wert kleiner ist.

Die Berechnungen der geschätzten Kapazität hängen von dem verfügbaren Speicherbereich für die Einheit ab, die dem Speicherpool zugeordnet ist. Für FILE-Speicherpools wird die Kapazität für den Speicherpool reduziert, wenn der verfügbare Speicher kleiner als der gesamte geschätzte Speicherbereich aller FILE-Datenträger in dem Speicherpool ist. Der für die Kapazität angezeigte Wert wird schrittweise um die Größe eines FILE-Datenträgers reduziert, während der verfügbare Speicherbereich weiter zurückgeht.

Für Centera stellt der Wert die Gesamtkapazität der Centera-Speichereinheit dar, die gerade abgefragt wird.

Speicherbereichsauslöser Ausl.
Die Auslastung des Speicherpools, die vom Speicherbereichsauslöser (sofern vorhanden) für diesen Speicherpool berechnet wurde. Speicherbereichsauslöser können nur für Speicherpools definiert werden, die dem Einheitentyp DISK oder FILE zugeordnet sind.

Bei Einheiten mit sequenziellem Zugriff wird die Auslastung des Speicherbereichsauslösers als Prozentsatz der Anzahl der verwendeten Byte auf jedem Datenträger mit sequenziellem Zugriff in Relation zur Größe des Datenträgers und der geschätzten Kapazität aller vorhandenen Datenträger im Speicherpool ausgedrückt. Sie schließt keine potenziellen Arbeitsdatenträger ein. Im Gegensatz zur Berechnung der prozentualen Auslastung legt die Berechnung der Auslastung des Speicherbereichsauslösers den Schwerpunkt auf die Erstellung neuer privater Dateidatenträger durch den Speicherbereichsauslöser über die Verwendung weiterer Arbeitsdatenträger.

Bei Platteneinheiten wird die Auslastung des Speicherbereichsauslösers als Prozentsatz der geschätzten Kapazität einschließlich Cachedaten ausgedrückt. Daten, die sich auf abgehängten Datenträgern befinden, werden jedoch ausgeschlossen. Der Wert für die Auslastung des Speicherbereichsauslösers kann höher als der Wert für die prozentuale Umlagerung sein, wenn Sie den Befehl QUERY STGPOOL ausgeben, während eine Dateierstellung ausgeführt wird. Der Wert für die Auslastung des Speicherbereichsauslösers wird durch den Umfang des Speicherbereichs bestimmt, der zugeordnet ist, während die Transaktion ausgeführt wird. Der Wert für die prozentuale Umlagerung stellt nur den Speicherbereich dar, der von festgeschriebenen Dateien belegt ist. Am Ende der Transaktion werden diese Werte synchronisiert.

Der Wert für die Auslastung des Speicherbereichsauslösers schließt Cachedaten auf Plattendatenträgern ein. Ist Caching aktiviert und findet eine Umlagerung statt, bleibt daher der Wert unverändert, da die umgelagerten Daten als Cachedaten auf dem Datenträger verbleiben. Der Wert verringert sich nur dann, wenn die Cachedaten verfallen oder wenn der Speicherbereich, der von Cachedateien belegt ist, für Dateien ohne Cachenutzung verwendet werden muss.

Auslastung in %
Die geschätzte Auslastung des Speicherpools als Prozentsatz.

Bei Einheiten mit sequenziellem Zugriff ist dieser Wert ein Prozentsatz der Anzahl der aktiven Byte auf jedem Datenträger mit sequenziellem Zugriff und der geschätzten Kapazität aller Datenträger im Speicherpool. Der Prozentsatz schließt die Anzahl potenzieller Arbeitsdatenträger ein, die möglicherweise zugeordnet sind.

Bei Platteneinheiten ist dieser Wert ein Prozentsatz der geschätzten Kapazität, einschließlich Cachedaten und Daten, die sich auf abgehängten Datenträgern befinden. Der Wert für Auslastung in % kann höher sein als der Wert für Umlagerung in %, wenn dieser Befehl ausgegeben wird, während eine Dateierstellungstransaktion ausgeführt wird. Der Wert für Auslastung in % wird durch den Umfang des zugeordneten Speicherbereichs bestimmt, während die Transaktion ausgeführt wird. Der Wert für Umlagerung in % stellt nur den Speicherbereich dar, der von festgeschriebenen Dateien belegt ist. Am Ende der Transaktion werden diese Werte synchronisiert.

Der Wert für Auslastung in % schließt Cachedaten auf Plattendatenträgern ein. Ist Caching aktiviert und findet eine Umlagerung statt, bleibt daher der Wert für Auslastung in % unverändert, da die umgelagerten Daten als Cachedaten auf dem Datenträger verbleiben. Der Wert für Auslastung in % verringert sich nur dann, wenn die Cachedaten verfallen oder wenn der Speicherbereich, der von Cachedateien belegt ist, für Nicht-Cachedateien verwendet werden muss.

Für Centera ist dies eine Schätzung der Auslastung der gesamten Centera-Speichereinheit, nicht des gerade abgefragten Speicherpools.

Umlagerung in % (nur primäre Speicherpools)
Der geschätzte Prozentsatz der Daten im Speicherpool, die umgelagert werden können. Der Server verwendet diesen Wert sowie die obere und die untere Umlagerungsschwelle, um zu bestimmen, wann die Umlagerung gestartet und gestoppt werden soll.

Bei Platteneinheiten mit wahlfreiem Zugriff wird dieser Wert als Prozentsatz des Werts für die geschätzte Kapazität angegeben, einschließlich der Daten, die sich auf abgehängten Datenträgern befinden, jedoch ohne Cachedaten.

Bei Platteneinheiten mit sequenziellem Zugriff wird dieser Wert als Prozentsatz des Werts für die geschätzte Kapazität angegeben. Der Wert schließt die Kapazität aller für den Pool angegebenen Arbeitsdatenträger ein. Für andere Typen von Einheiten mit sequenziellem Zugriff ist dieser Wert der Prozentsatz der Gesamtzahl der Datenträger in dem Pool, die mindestens ein Byte aktiver Daten enthalten. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein.

Der Wert für Auslastung in % schließt Cachedaten auf einem Datenträger ein; der Wert für Umlagerung in % schließt Cachedaten aus. Ist Caching aktiviert und findet eine Umlagerung statt, verringert sich daher der Wert für Umlagerung in %, der Wert für Auslastung in % bleibt jedoch unverändert, da die umgelagerten Daten als Cachedaten auf dem Datenträger verbleiben. Der Wert für Auslastung in % verringert sich nur dann, wenn die Cachedaten verfallen oder wenn der Speicherbereich, der von Cachedateien belegt ist, für Nicht-Cachedateien verwendet werden muss.

Prozent logische Belegung
Die logische Belegung des Speicherpools als Prozentsatz der Gesamtbelegung. Die logische Belegung ist der Speicherbereich, der von Clientdateien belegt ist, die Teil oder kein Teil eines Aggregats sein können. Ein Wert für Prozent logische Belegung, der kleiner als 100 % ist, gibt an, dass innerhalb von Aggregaten in dem Speicherpool freier Speicherbereich verfügbar ist.

Obere Umlagerungsschwelle in % (nur primäre Speicherpools)
Die obere Umlagerungsschwelle, die angibt, wann der Server mit der Umlagerung für den Speicherpool beginnen kann. Der Server startet Umlagerungsprozesse, wenn die Kapazitätsnutzung diesen Schwellenwert erreicht.

Untere Umlagerungsschwelle in % (nur primäre Speicherpools)
Die untere Umlagerungsschwelle, die angibt, wann der Server die Umlagerung für den Speicherpool stoppen kann. Der Server stoppt Umlagerungsprozesse, wenn die Kapazitätsnutzung diesen Schwellenwert erreicht.

Umlagerungsverzögerung (nur primäre Speicherpools)
Die Mindestanzahl Tage, die eine Datei in einem Speicherpool verbleiben muß, bevor der Server die Datei in den nächsten Speicherpool umlagern kann. Bei einem Plattenspeicherpool werden die Tage ab dem Zeitpunkt gezählt, zu dem die Datei in dem Speicherpool gespeichert oder von einem Client zuletzt abgerufen wurde. Bei einem Speicherpool mit sequenziellem Zugriff werden die Tage ab dem Zeitpunkt gezählt, zu dem die Datei in dem Speicherpool gespeichert wurde.

Umlagerung fortsetzen (nur primäre Speicherpools)
Angabe, ob der Server die Umlagerung von Dateien in den nächsten Speicherpool auch dann fortsetzt, wenn die Dateien für die Anzahl der Tage, die durch die Umlagerungsverzögerung angegeben werden, nicht in dem Pool waren.

Umlagerungsprozesse
Die Anzahl paralleler Prozesse, die zum Umlagern von Dateien aus einem primären Speicherpool mit wahlfreiem oder sequenziellem Zugriff verwendet werden.

Wiederherstellungsprozesse
Die Anzahl paralleler Prozesse, die zum Wiederherstellen der Datenträger in einem primären Speicherpool mit sequenziellem Zugriff oder Kopienspeicherpool verwendet werden.

Nächster Speicherpool (nur primäre Speicherpools)
Der Speicherpool, der der Zielort für Daten ist, die aus diesem Speicherpool umgelagert werden.

Speicherpool wiederherstellen (nur primäre Speicherpools mit sequenziellem Zugriff)
Falls angegeben, der Speicherpool, der der Zielort für Daten ist, die von Datenträgern während der Wiederherstellungsverarbeitung versetzt werden. Wird kein Pool angegeben, werden bei der Wiederherstellungsverarbeitung standardmäßig Daten nur zwischen Datenträgern innerhalb desselben Speicherpools versetzt.

Schwelle für maximale Größe (nur primäre Speicherpools)
Die maximale Größe von Dateien, die in dem Speicherpool gespeichert werden kann.

Zugriff
Der Zugriffsmodus für Daten in dem Speicherpool. Die folgenden Zugriffsmodi sind gültig:

Lesen/Schreiben

Auf die Daten kann im Modus 'Schreib-/Lesezugriff' zugegriffen werden.

Schreibgeschützt
: Auf die Daten kann im Lesezugriffsmodus zugegriffen werden.

Wird konvertiert
: Der Speicherpool wird gerade in einen Verzeichniscontainerspeicherpool konvertiert.

Konvertierung gestoppt
: Der Prozess der Konvertierung des Speicherpools in einen Verzeichniscontainerspeicherpool wurde gestoppt.

Bereinigung für Konvertierung erforderlich
: Um den Speicherpool erfolgreich zu konvertieren, müssen Sie den Speicherpool bereinigen. Die Konvertierung wurde aufgrund von beschädigten Daten nicht abgeschlossen. Geben Sie den Befehl QUERY CLEANUP aus, um beschädigte Dateien zu identifizieren.

Konvertiert
: Der Speicherpool wurde in einen Verzeichniscontainerspeicherpool konvertiert.

Beschreibung
: Die Beschreibung des Speicherpools.

Überlaufstandort (nur Speicherpools mit sequenziellem Zugriff)
: Der Standort, an dem Datenträger in dem Speicherpool gespeichert werden, wenn sie mit dem Befehl MOVE MEDIA aus einem automatisierten Speicherarchiv ausgegeben werden.

Umgelagerte Dateien zwischenspeichern? (nur Speicherpools mit wahlfreiem Zugriff)
: Angabe, ob Caching für Dateien aktiviert ist, die in den nächsten Speicherpool umgelagert werden.

Zusammenfassen? (nur Speicherpools mit sequenziellem Zugriff)
: Angabe, ob die Kollokation inaktiviert oder aktiviert ist. Ist die Kollokation inaktiviert, lautet der Wert dieses Felds No. Ist die Kollokation aktiviert, lauten die gültigen Werte Group, Node und File space.

Wiederherstellungsschwelle (nur Speicherpools mit sequenziellem Zugriff)
: Die Schwelle, die bestimmt, wann Datenträger in einem Speicherpool wiederhergestellt werden. Der Server vergleicht den Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger mit diesem Wert, um festzustellen, ob eine Wiederherstellung erforderlich ist.

Grenzwert für Wiederh. ausgelag. Datenträger
: Die Anzahl der ausgelagerten Datenträger, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool wiederhergestellt wird. Dieses Feld gilt nur bei POOLTYPE=COPY.

Maximale Anzahl Arbeitsdatenträger (nur Speicherpools mit sequenziellem Zugriff)
: Die maximale Anzahl der Arbeitsdatenträger, die der Server für den Speicherpool anfordern kann.

Anzahl verwendeter Arbeitsdatenträger (nur Speicherpools mit sequenziellem Zugriff)
: Die Anzahl der Arbeitsdatenträger, die in dem Speicherpool verwendet werden.

Verzögerungszeitraum für Containerwiederverwendung (nur Containerspeicherpools)
: Die Anzahl Tage, die nach dem Löschen aller Dateien aus dem Container verstreichen müssen, bevor der Container vom Server wiederverwendet wird.

Wird Umlagerung ausgeführt? (nur primäre Speicherpools)
: Angabe, ob mindestens ein Umlagerungsprozess für den Speicherpool aktiv ist.

Umgelagerte Datenmenge (MB) (nur primäre Speicherpools)
: Das Datenvolumen in Megabyte, das umgelagert wird, wenn die Umlagerung aktiv ist. Ist die Umlagerung nicht aktiv, gibt dieser Wert die bei der letzten Umlagerung umgelagerte Datenmenge an. Werden für den Speicherpool mehrere gleichzeitig stattfindende Umlagerungsprozesse verwendet, gibt dieser Wert das von allen Prozessen umgelagerte Gesamtvolumen der Daten an.

Abgelaufene Umlagerungszeit (Sekunden) (nur primäre Speicherpools)
: Die Zeit, die seit Beginn der Umlagerung vergangen ist, wenn die Umlagerung aktiv ist. Ist die Umlagerung nicht aktiv, gibt dieser Wert die Zeit an, die für die Ausführung der letzten Umlagerung erforderlich ist. Werden für den Speicherpool mehrere gleichzeitig stattfindende Umlagerungsprozesse verwendet, gibt dieser Wert den von allen Prozessen benötigten Gesamtzeitaufwand an (vom Anfang des ersten bis zum Abschluß des letzten Prozesses).

Wird Wiederherstellung ausgeführt? (nur Speicherpools mit sequenziellem Zugriff)
: Angabe, ob für den Speicherpool ein Wiederherstellungsprozess aktiv ist.

Letzte Aktualisierung durch (Administrator)
: Der Name des Administrators, der den Speicherpool definiert bzw. zuletzt aktualisiert hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der ein Administrator den Speicherpool definiert oder zuletzt aktualisiert hat.

Speicherpooldatenformat
: Der Typ des Datenformats, der zum Schreiben von Daten in diesen Speicherpool verwendet wird (beispielsweise NATIVE, NETAPPDUMP, CELERRADUMP oder NDMPDUMP).

Kopienspeicherpool(s)
: In die aufgelisteten Kopienspeicherpools werden zu demselben Zeitpunkt Daten geschrieben, zu dem Daten in dem primären Speicherpool gesichert oder archiviert werden, der mit diesem Befehl abgefragt wird.

Pool(s) für aktive Daten
: In die hier aufgelisteten Pools für aktive Daten werden zu demselben Zeitpunkt Daten geschrieben, zu dem Daten in dem primären Speicherpool gesichert werden, der mit diesem Befehl abgefragt wird.

Kopieren bei Fehler fortsetzen?
: Gibt an, ob ein Server das Schreiben von Daten in andere Kopienspeicherpools in der Liste fortsetzt oder die gesamte Transaktion beendet, wenn bei einem der Kopienpools in der Liste ein Schreibfehler auftritt. Dieses Feld gilt nur für primäre Speicherpools mit wahlfreiem Zugriff und für primäre Speicherpools mit sequenziellem Zugriff.

CRC-Daten

Gibt an, ob Daten durch eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) ausgewertet werden, wenn Daten während des Speicherns und Abrufens auf einer Einheit übertragen werden.

Wiederherstellungstyp
Gibt an, ob Datenträger in diesem Speicherpool nach Schwellenwert (threshold) oder nach SnapLock-Aufbewahrungsdauer wiederhergestellt werden.

Daten nach Löschen überschreiben
Gibt an, wie oft Daten physisch überschrieben werden, nachdem sie aus der Datenbank gelöscht wurden.

Daten deduplizieren?
Angabe, ob Daten in dem Speicherpool dedupliziert werden.

Prozesse zum Identifizieren doppelter Daten
Die Anzahl der Prozesse zum Identifizieren doppelter Daten, die als Standardwert für den Speicherpool angegeben wurde. Die in diesem Feld angegebene Anzahl der Prozesse zum Identifizieren doppelter Daten ist möglicherweise nicht gleich der Anzahl der Prozesse zum Identifizieren doppelter Daten, die ausgeführt werden.

Komprimiert
Angabe, ob der Speicherpool komprimiert ist.

Zusätzlicher Speicherbereich für geschützte Daten

Der Umfang des Speicherbereichs in MB, der zum Schützen von Daten ferner Server verwendet wird. Dies ist der Gesamtumfang des Speicherbereichs, der für Daten verwendet wird, die von anderen Servern als Ergebnis der Ausführung des Befehls PROTECT STGPOOL empfangen werden.

Nicht belegter anstehender Speicherbereich insgesamt
Der Umfang des Speicherbereichs, der zu einem geplanten Zeitpunkt in einem Verzeichniscontainerspeicherpool verfügbar wird. Der Speicherbereich wird von deduplizierten Datenbereichen belegt, die aus dem Speicherpool entfernt werden, wenn der über den Parameter REUSEDELAY im Befehl DEFINE STGPOOL festgelegte Zeitraum abläuft.

Deduplizierungseinsparungen
Der Umfang und Prozentsatz der Daten, der im Speicherpool mithilfe der Datendeduplizierung eingespart wird.

Komprimierungseinsparungen
Das Datenvolumen, das im Speicherpool durch die Komprimierung eingespart wird.

Eingesparter Gesamtspeicherbereich
Das Gesamtdatenvolumen, das im Speicherpool eingespart wurde.

Modus für automatisches Kopieren
Gibt an, ob Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen, Serverdatenumlagerungsprozessen oder aller drei Operationen gleichzeitig in Kopienspeicherpools oder Pools für aktive Daten geschrieben werden. Der Wert CLIENT gibt entweder Clientspeicheroperationen oder Serverimportoperationen an. Der Wert ALL gibt an, dass Operationen mit simultanem Schreiben immer dann ausgeführt werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

Ist der Speicherpool ein Kopienspeicherpool oder ein Pool für aktive Daten oder ist die Funktion für simultanes Schreiben inaktiviert, ist dieses Feld leer.

Enthält vom Client deduplizierte Daten?
Gibt an, ob der Speicherpool Daten enthält, die von Clients dedupliziert wurden. Auf Speicherpools, die von Clients deduplizierte Daten enthalten, kann von Speicheragenten mit Version 6.1 oder einer früheren Version nicht für die LAN-unabhängige Datenversetzung zugegriffen werden.
Tipp: Dieses Feld ist für Containerspeicherpools leer. Sie können keine Containerspeicherpools für die LAN-unabhängige Datenversetzung verwenden.

Maximale Anzahl simultaner Writer
Die maximale Anzahl der Ein-/Ausgaben, die gleichzeitig für den Speicherpool ausgeführt werden können.

Schutzprozesse
Die Anzahl der Schutzprozesse.

Schutzspeicherpool
Der Name des Containerspeicherpools, in dem die Daten auf dem Zielreplikationsserver geschützt werden.

Lokale Speicherpools schützen
Gibt an, ob lokale Speicherpools geschützt werden.

Grenzwert für Datenträgerwiederherstellung
Gibt bei Containerkopienspeicherpools die maximale Anzahl der Datenträger an, die der Server während des Speicherpoolschutzes wiederherstellt.

Datum des letzten Schutzes in fernem Pool
Das Datum, an dem der Speicherpool zuletzt in einem Speicherpool auf einem fernen Server geschützt wurde.

Datum des letzten Schutzes in lokalem Pool
Das Datum, an dem der Speicherpool zuletzt in einem Speicherpool auf dem lokalen Server geschützt wurde.

Deduplizierung erfordert Sicherung?
Gibt an, ob der sequenzielle Speicherpool gesichert werden muss, wenn der Speicherpool deduplizierte Daten enthält.

Verschlüsselt
: Gibt für Verzeichniscontainerspeicherpools oder Cloud-Containerspeicherpools an, ob Clientdaten verschlüsselt werden, bevor sie in den Speicherpool geschrieben werden.

Prozent verschlüsselt
: Der Prozentsatz der deduplizierten Clientdaten, die im Verzeichniscontainerspeicherpool oder Cloud-Containerspeicherpool verschlüsselt sind.

Belegter Cloudspeicherbereich (MB)
: Bei Cloudspeicherpools der Speicherbereich, der vom Cloudspeicher belegt wird, angegeben in Megabyte.

Bucketname
: Bei Cloudspeicherpools, die Simple Storage Service (S3) verwenden, der Name, den IBM Spectrum Protect dem S3-Bucket oder der IBM® Cloud Object Storage-Vault zuordnet. Dieser Wert kann auch der Name sein, den Sie dem Bucket mit dem Parameter BUCKETNAME im Befehl DEFINE STGPOOL oder UPDATE STGPOOL zugeordnet haben.

Lokale geschätzte Kapazität
: Bei Cloudspeicherpools, die lokalen Speicher verwenden, die geschätzte Kapazität des lokalen Speichers in Megabyte (M) oder Gigabyte (G).

Lokale proz. Auslastung
: Bei Cloudspeicherpools, die lokalen Speicher verwenden, die geschätzte Auslastung der lokalen Speicherkomponente des Cloudspeicherpools als Prozentsatz.

Lokale logische Belegung in Prozent
: Bei Cloudspeicherpools, die lokalen Speicher verwenden, die logische Belegung des Cloudspeicherpools als Prozentsatz der Gesamtbelegung. Die logische Belegung ist der Speicherbereich, der von Clientdateien belegt ist, die Teil oder kein Teil eines Aggregats sein können. Ein Wert für Lokale logische Belegung in Prozent, der kleiner als 100 % ist, gibt an, dass innerhalb von Aggregaten in dem Cloudspeicherpool freier Speicherbereich verfügbar ist.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY STGPOOL

Befehl	Beschreibung
CONVERT STGPOOL	Konvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE STGPOOL	Löscht einen Speicherpool aus dem Serverspeicher.
QUERY STGPOOLDIRECTORY	Zeigt Informationen zu Speicherpoolverzeichnissen an.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

QUERY STGPOOLDIRECTORY (Speicherpoolverzeichnis abfragen)

Mit diesem Befehl können Informationen zu einem oder zu mehreren Speicherpoolverzeichnissen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                          .-*-----------.
>>-Query STGPOOLDIRectory--+-------------+---------------------->
                          '-Verzeichnis-'

                            .-ACCess--=--Any-------------.
>--+----------------------+--+---------------------------+----->
   '-STGpool--=--Poolname-'  '-ACCess--=--+-READWrite---+-'
                                          +-READOnly----+
                                          +-DEStroyed---+
                                          +-Any---------+
                                          '-UNAVailable-'

   .-Format--=--Standard-----.
```

```
>--+------------------------+--------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Verzeichnis
: Gibt das Speicherpoolverzeichnis an, das abgefragt werden soll. Dieser Parameter ist wahlfrei.

  *
  : Gibt an, dass ein Stern (*) ein Platzhalterzeichen darstellt. Verwenden Sie Platzhalterzeichen, wie z. B. einen Stern, für die Übereinstimmung mit beliebigen Zeichen. Alternativ können Sie ein Fragezeichen (?) oder ein Prozentzeichen (%) verwenden, die exakt einem Zeichen entsprechen. Dies ist der Standardwert.

  Verzeichnis
  : Gibt das Speicherpoolverzeichnis an. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherpoolverzeichnisse angezeigt. Die maximale Länge des Speicherpoolverzeichnisses beträgt 1024 Zeichen.

STGpool
: Gibt den Namen des Speicherpools an, der abgefragt werden soll. Wird kein Wert für diesen Parameter angegeben, werden alle Speicherpoolverzeichnisse angezeigt. Die maximale Länge des Speicherpoolnamens beträgt 30 Zeichen. Dieser Parameter ist wahlfrei.

ACCess
: Gibt an, dass die Ausgabe durch den Verzeichniszugriffsmodus eingeschränkt wird. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

  READWrite
  : Alle Speicherpoolverzeichnisse mit dem Zugriffsmodus `READWRITE` anzeigen.

  READOnly
  : Alle Speicherpoolverzeichnisse mit dem Zugriffsmodus `READONLY` anzeigen.

  DEStroyed
  : Alle Speicherpoolverzeichnisse mit dem Zugriffsmodus `DESTROYED` anzeigen. Die Verzeichnisse sind im Speicherpoolverzeichnis als dauerhaft beschädigt gekennzeichnet.

  Any
  : Alle Speicherpoolverzeichnisse anzeigen. Dies ist der Standardwert.

  UNAVailable
  : Verzeichnisse mit dem Zugriffsmodus `UNAVAILABLE` anzeigen.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Sie können einen der folgenden Werte angeben:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

Beispiel: Übersichtsdaten zu einem bestimmten Speicherpoolverzeichnis anzeigen

Informationen zu dem Speicherpoolverzeichnis mit dem Namen DPOOL anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query stgpooldirectory C:\data
```

```
Speicher-   Verzeichnis   Zugriff
poolname
----------  ----------   ---------
DPOOL       C:\data       Read/Write
```

Beispiel: Ausführliche Informationen zum Speicherpoolverzeichnis anzeigen

Ausführliche Informationen zu dem Speicherpoolverzeichnis mit dem Namen DPOOL anzeigen.

```
query stgpooldirectory stgpool=dpool format=detailed
```


```
                Speicherpoolname: DPOOL
                                 Verzeichnis: /storage/sampleDir
                                     Zugriff: Read/Write
                   Freier Speicherbereich (MB): 323.170
                    Gesamtspeicherbereich (MB): 476.938
                                 Dateisystem: /storage
                             Absoluter Pfad: /storage/data
```

Windows-Betriebssysteme

```
Speicherpoolname: DPOOL
                  Verzeichnis: /storage2/sampleDir
                      Zugriff: Read/Write
   Freier Speicherbereich (MB): 323.170
    Gesamtspeicherbereich (MB): 476.938
                  Dateisystem: /storage
              Absoluter Pfad: /storage2/sampleDir
```

Feldbeschreibungen

Speicherpoolname
: Der Name des Speicherpools.

Verzeichnis
: Der Name des Speicherpoolverzeichnisses.

Zugriff
: Der Zugriffsmodus der Daten in dem Speicherpoolverzeichnis.

Freier Speicherbereich (MB)
: Der Speicherbereich im Speicherpoolverzeichnis in Megabyte, der nicht verwendet wird.

Gesamtspeicherbereich (MB)
: Der Gesamtspeicherbereich im Speicherpoolverzeichnis in Megabyte.

Dateisystem
: Der Name des Dateisystems, in dem sich das Speicherpoolverzeichnis befindet.

Absoluter Pfad
: Der Name des absoluten Pfads, in dem sich das Speicherpoolverzeichnis befindet. Der absolute Pfadname enthält den Namen des Stammverzeichnisses und alle Unterverzeichnisse im Pfadnamen. Alle symbolischen Verbindungen werden in den absoluten Pfadnamen aufgelöst.

Tabelle 1. Zugehörige Befehle für QUERY STGPOOLDIRECTORY

Befehl	Beschreibung
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeDEFINE STGPOOLDIRECTORY	Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeDELETE STGPOOLDIRECTORY	Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeUPDATE STGPOOLDIRECTORY	Ändert die Attribute eines Speicherpoolverzeichnisses.

QUERY SUBSCRIBER (Informationen zu Subskribenten anzeigen)

Mit diesem Befehl können auf einem Konfigurationsmanager Informationen über Subskribenten und ihre Profilsubskriptionen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                    .-*----------.
>>-Query SUBSCRIBer--+------------+----------------------------->
                     '-Servername-'

   .-PROFIle----*----------.
>--+-----------------------+-----------------------------------><
   '-PROFIle----Profilname-'
```

Parameter

Servername

Gibt den Namen eines verwalteten Servers an, für den Subskriptionsinformationen angezeigt werden sollen. Es können Platzhalterzeichen verwendet werden, um mehrere Server-Namen anzugeben. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle verwalteten Server.

PROFIle
: Gibt einen Profilnamen an, für den Informationen angezeigt werden sollen. Es können Platzhalterzeichen verwendet werden, um mehrere Profilnamen anzugeben. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Profile.

Beispiel: Die Profilsubskriptionen eines Konfigurationsmanagers auflisten

Subskribenteninformationen für alle Profilsubskriptionen für diesen Konfigurationsmanager anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query subscriber

Subskribent       Profilname         Aktuell?       Datum/Zeit der
                                                    letzten Aktualisierung
---------------   ---------------    ------------   -----------------
SERVER2           DEFAULT_PROFILE    Yes            Thu, May 14, 1998
                                                    01:14:42 PM
SERVER2           SETUP              Yes            Thu, May 14, 1998
                                                    01:14:42 PM
```

Feldbeschreibungen

Subskribent
: Der Name des Subskribenten (verwalteter Server).

Profilname
: Der Name des Profils.

Aktuell?
: Angabe, ob die Subskription mit den aktuellen Informationen, die dem Profil zugeordnet sind, aktualisiert wurde. Gültige Werte:

  Yes
  : Der verwaltete Server ist auf dem aktuellen Stand.

  No
  : Der verwaltete Server ist nicht auf dem aktuellen Stand. Enthält dieses Feld den Wert NO, nachdem das Profil aktualisiert wurde, die Servernachrichten auf Fehlerbedingungen überprüfen, die möglicherweise das Fehlschlagen der Aktualisierung verursacht haben.

  Unknown
  : Entweder verfügt der verwaltete Server über eine neuere Version des Profils als der Konfigurationsmanager oder das Profil ist nicht mehr auf dem Konfigurationsmanager vorhanden, die Subskription ist jedoch noch dem Profil zugeordnet.

Datum/Zeit der letzten Aktualisierung
: Gibt das Datum und die Uhrzeit an, an dem bzw. zu der die Konfigurationsdaten für die Subskription erfolgreich an den Subskribenten verteilt wurden.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SUBSCRIBER

Befehl	Beschreibung
DEFINE SUBSCRIPTION	Subskribiert einen verwalteten Server für ein Profil.
DELETE SUBSCRIBER	Löscht veraltete Subskriptionen verwalteter Server.
DELETE SUBSCRIPTION	Löscht eine angegebene Profilsubskription.
NOTIFY SUBSCRIBERS	Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
QUERY SUBSCRIPTION	Zeigt Informationen über Profilsubskriptionen an.

QUERY SUBSCRIPTION (Subskriptionsinformationen anzeigen)

Mit diesem Befehl können auf einem verwalteten Server Profilsubskriptionsinformationen angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                        .-*----------.
>>-Query SUBSCRIPtion--+------------+-------------------------><
                        '-Profilname-'
```

Parameter

Profilname
: Gibt den Namen des Profils an, für das Subskriptionsinformationen angezeigt werden. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben. Dieser Parameter ist wahlfrei. Der Standardwert lautet alle Profile.

Beispiel: Subskriptionsinformationen anzeigen

Subskriptionsinformationen für alle Profile anzeigen.

```
query subscription

Konfigurations-     Profilname           Datum/Zeit der
manager                                  letzten Aktualisierung
---------------     ---------------      ---------
SERVER1             ADMIN_INFO           Thu, May 14, 1998
                                         01:35:13
SERVER1             DEFAULT_PROFILE      Thu, May 14, 1998
                                         01:35:13
SERVER1             EMPLOYEE             Thu, May 14, 1998
                                         01:35:13 PM
```

Feldbeschreibungen

Konfigurationsmanager
: Der Name des Konfigurationsmanagers.

Profilname
: Der Name des Profils.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der die neuesten Konfigurationsdaten erfolgreich an den Subskribenten verteilt wurden.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SUBSCRIPTION

Befehl	Beschreibung
DEFINE SUBSCRIPTION	Subskribiert einen verwalteten Server für ein Profil.
DELETE SUBSCRIBER	Löscht veraltete Subskriptionen verwalteter Server.
DELETE SUBSCRIPTION	Löscht eine angegebene Profilsubskription.
NOTIFY SUBSCRIBERS	Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.
QUERY SUBSCRIBER	Zeigt Informationen über Subskribenten und ihre Subskriptionen für Profile an.

QUERY SYSTEM (Systemkonfiguration und Kapazität abfragen)

Mit diesem Befehl können konsolidierte Informationen zur Konfiguration und Kapazität des Servers abgerufen werden.

Dieser Befehl konsolidiert die Ausgabe aus Anweisungen SELECT, Befehlen SHOW und anderen IBM Spectrum Protect-Befehlen. Die Ausgabe wird von mehreren IBM Spectrum Protect-Befehlen generiert, wie z. B.:

- QUERY ASSOCIATION
- QUERY COPYGROUP
- QUERY DATAMOVER
- QUERY DB
- QUERY DBSPACE
- QUERY DEVCLASS
- QUERY DIRSPACE
- QUERY DOMAIN
- QUERY LIBRARY
- QUERY LOG
- QUERY MGMTCLASS
- QUERY OPTION

- QUERY PROCESS
- QUERY REPLRULE
- QUERY SCHEDULE
- QUERY SERVER
- QUERY SESSION
- QUERY STATUS
- QUERY STGPOOL
- QUERY VOLHISTORY
- QUERY VOLUME

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-Query SYStem-------------------------------------------------><
```

Beispiel: Konsolidierte Systeminformationen anzeigen

Den Befehl QUERY SYSTEM ausgeben, um konsolidierte Systeminformationen abzurufen. Beispielausgabedaten für diese Abfragebefehle befinden sich in den Erläuterungen zum jeweiligen Befehl.

```
query system
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY SYSTEM

Befehl	Beschreibung
QUERY ASSOCIATION	Zeigt die Clients an, die einem oder mehreren Zeitplänen zugeordnet sind.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY DB	Zeigt Zuordnungsinformationen zu der Datenbank an.
QUERY DBSPACE	Zeigt Informationen zum Speicherplatz an, der für die Datenbank definiert ist.
QUERY DEVCLASS	Zeigt Informationen zu Einheitenklassen an.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
QUERY LOG	Zeigt Informationen zum Wiederherstellungsprotokoll an.
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.
QUERY OPTION	Zeigt Informationen über Serveroptionen an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY SCHEDULE	Zeigt Informationen über Zeitpläne an.
QUERY SESSION	Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.
QUERY VOLUME	Zeigt Informationen über Speicherpooldatenträger an.

QUERY TAPEALERTMSG (Status des Befehls SET TAPEALERTMSG anzeigen)

Mit diesem Befehl kann der Status des Befehls SET TAPEALERTMSG angezeigt werden. Sie können Bandalerts aktivieren oder inaktivieren. Bei einer Aktivierung kann IBM Spectrum Protect Diagnoseinformationen aus einer Band- oder Kassettenarchiveinheit abrufen und mit Hilfe von ANR-Nachrichten anzeigen. Bei einer Inaktivierung fragt IBM Spectrum Protect diese Informationen nicht ab.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-Query TAPEAlertmsg----------------------------------------><
```

Beispiel: Den Status des Befehls QUERY TAPEALERTMSG anzeigen

Stellen Sie mit dem Befehl QUERY TAPEALERTMSG fest, ob Bandalerts aus Einheiten abgerufen und in Form von ANR-Nachrichten angezeigt werden sollen.

```
query tapealertmsg
```

```
ANR2017I Administrator SERVER_CONSOLE hat folgenden Befehl ausgegeben:
         QUERY TAPEALERTMSG
ANR8960I QUERY TAPEALERTMSG: Die Anzeige von Bandalerts von SCSI-Einheiten
         ist aktiviert.
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY TAPEALERTMSG

Befehl	Beschreibung
SET TAPEALERTMSG	Gibt an, ob Band- und Kassettenarchiveinheiten Diagnoseinformationen an den Server melden.

QUERY TOC (Inhaltsverzeichnis für ein Sicherungsimage anzeigen)

Mit diesem Befehl können Verzeichnis- und Dateiangaben im Inhaltsverzeichnis (TOC) für ein angegebenes Sicherungsimage angezeigt werden. Mit diesem Befehl werden keine Inhaltsverzeichnisinformationen in die IBM Spectrum Protect-Datenbank geladen. Das angegebene Inhaltsverzeichnis wird aus einem Speicherpool gelesen, wenn der Befehl QUERY TOC ausgegeben wird.

Dieser Befehl kann nicht von der Serverkonsole ausgegeben werden. Ist das Inhaltsverzeichnis auf einem austauschbaren Datenträger gespeichert, ist ein Mountpunkt erforderlich und die Ausgabe wird verzögert, während der Speicherpooldatenträger geladen wird.

Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie entweder System- oder Maßnahmenberechtigung für die Domäne, der der Knoten zugeordnet ist, oder Clienteignerberechtigung für den Knoten haben.

Syntax

```
>>-Query TOC--Knotenname--Dateibereichsname--------------------->

>--+-----------------------------------------------+------------>
   '-CREATIONDate--=--Datum--CREATIONTime--=--Zeit-'

   .-Format--=--Standard-----.
>--+-------------------------+---------------------------------><
   '-Format--=--+-Standard-+-'
                '-Detailed-'
```

Parameter

Knotenname (Erforderlich)
: Gibt den Namen des NAS-Knotens an, zu dem das Inhaltsverzeichnis gehört. Sie können zur Angabe dieses Namens keine Platzhalterzeichen verwenden.

Dateibereichsname (Erforderlich)
: Gibt den Namen des Dateibereichs an, zu dem das Inhaltsverzeichnis gehört. Der angegebene Dateibereichsname darf keine Platzhalterzeichen enthalten.

CREATIONDate
: Gibt das Erstellungsdatum des Sicherungsimages an, für das das Inhaltsverzeichnis angezeigt werden soll. Dieser Parameter ist wahlfrei. Wird CREATIONDATE angegeben, muss auch CREATIONTIME angegeben werden. Werden diese Parameter nicht angegeben, wird der Inhalt des letzten Sicherungsimages für den angegebenen Knoten und Dateibereich angezeigt, vorausgesetzt, dieses Image hat ein Inhaltsverzeichnis. Das Erstellungsdatum kann nur wie folgt angegeben werden:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	05/15/2002

Gibt an, dass der Inhalt des Sicherungsimages angezeigt werden soll, das an diesem Datum erstellt wurde. Sie können dieses Datum der Ausgabe des Befehls QUERY NASBACKUP entnehmen.

CREATIONTime

Gibt die Erstellungszeit des Sicherungsimages an, für das das Inhaltsverzeichnis angezeigt werden soll. Dieser Parameter ist wahlfrei. Wird CREATIONTIME angegeben, muss auch CREATIONDATE angegeben werden. Werden diese Parameter nicht angegeben, wird der Inhalt des letzten Sicherungsimages für den angegebenen Knoten und Dateibereich angezeigt, vorausgesetzt, dieses Image hat ein Inhaltsverzeichnis. Die Erstellungszeit kann nur wie folgt angegeben werden:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Erstellungsdatum.	10:30:08

Gibt an, dass der Inhalt des Sicherungsimages angezeigt werden soll, das zu dieser Uhrzeit am angegebenen Datum erstellt wurde. Sie können diese Uhrzeit der Ausgabe des Befehls QUERY NASBACKUP entnehmen.

Format

Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

Standard

Gibt an, dass Teilinformationen für die Dateien angezeigt werden.

Detailed

Gibt an, dass die vollständigen Informationen für die Dateien angezeigt werden, einschließlich der hexadezimalen Darstellung jedes Datei- oder Verzeichnisnamens.

Beispiel: Ausführliche Informationen zum Inhaltsverzeichnis für einen bestimmten Knoten anzeigen

Mit dem Befehl QUERY TOC Informationen in dem Inhaltsverzeichnis anzeigen, das zum NAS-Knoten NETAPP im Dateibereich /vol/vol1 gehört, der am 12/06/2002 um 11:22:46 Uhr erstellt wurde. Ein detailliertes Format angeben.

```
query toc netapp /vol/vol1 creationdate=12/06/2002 creationtime=11:22:46
    format=detailed

Objekte im Image, die am 12/06/2002 um 11:22:46 Uhr
für Dateibereich /vol/vol1 in Knoten NETAPP gesichert wurden:


                              Objektname: /.etc
                  Hexadezimaler Objektname: 2f657463
                               Objekttyp: Verzeichnis
                             Objektgröße: 4.096
          Datum/Zeit der letzten Datenänderung: 07/31/2002 14:21:19

                              Objektname: /.etc/oldmaps/ndmp
                  Hexadezimaler Objektname: 2f6574632f6f6c646d6170
                                            732f6e646d70
                               Objekttyp: Verzeichnis
                             Objektgröße: 4.096
          Datum/Zeit der letzten Datenänderung: 07/31/2002 14:21:19

                              Objektname: /.etc/oldmaps/ndmp/TSM
                                            /vol/vol1/3df0e8fd
                  Hexadezimaler Objektname: 2f6574632f6f6c646d6170
                                            732f6e646d702f54534d2
                                            02f766f6c2f766f6c312f3
                                            364663065386664
                               Objekttyp: Datei
                             Objektgröße: 36,864
          Datum/Zeit der letzten Datenänderung: 12/06/2002 11:14:22
```

Feldbeschreibungen

Objektname

Der Name des Objekts.

Hexadezimaler Objektname

Der Name des Objekts im Hexadezimalformat.

Objekttyp

Der Typ des Objekts.

Objektgröße

Die Größe des Objekts.

Datum/Zeit der letzten Datenänderung

Der Zeitpunkt (Datum und Uhrzeit), an dem das Objekt zuletzt geändert wurde.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY TOC

Befehl	Beschreibung
BACKUP NODE	Sichert einen NAS-Knoten (NAS = Network Attached Storage).
QUERY NASBACKUP	Zeigt Informationen zu NAS-Sicherungsimages an.
RESTORE NODE	Schreibt einen NAS-Knoten (NAS = Network Attached Storage) zurück.

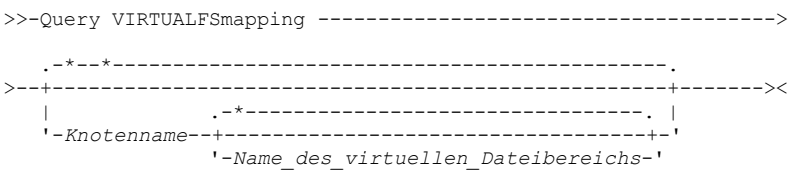
QUERY VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs abfragen)

Verwenden Sie diesen Befehl, um eine Definition für die Zuordnung des virtuellen Dateibereichs abzufragen.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Knotenname
: Gibt den Clientknoten an, zu dem der virtuelle Dateibereich gehört. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Der Standardwert ist alle Clientknotennamen. Für diesen Parameter muss ein Wert angegeben werden, wenn der Name eines virtuellen Dateibereichs angegeben wird.

Name_des_virtuellen_Dateibereichs
: Gibt den Namen der abzufragenden Zuordnung des virtuellen Dateibereichs an. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Dieser Parameter ist wahlfrei. Wird kein Wert angegeben, werden alle Zuordnungen des virtuellen Dateibereichs abgefragt. Bei den Zuordnungsnamen des virtuellen Dateibereichs muss die Groß-/Kleinschreibung berücksichtigt werden. Mit dem Befehl QUERY VIRTUALFSMAPPING kann die korrekte Schreibweise für die abzufragende Zuordnung des virtuellen Dateibereichs bestimmt werden.

Beispiel: Virtuelle Dateibereiche für einen bestimmten Knoten anzeigen

Die gegenwärtig definierten virtuellen Dateibereiche für Knoten NAS1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query virtualfsmapping nas1

Knoten- Name d. Zuordnung  Dateiber.-  Pfad              Hexadezimaler
name    d. virt. Dateiber. Name                         Pfad?
------  -----------------  ----------  ----------------- -----------
NAS1    /mikesdir          /vol/vol2   /mikes            No
NAS1    /tmpdir            /vol/vol1   /tmp              No
NAS1    /nonASCIIDir       /vol/vol3   2f73657276657231  Yes
```

Feldbeschreibungen

Knotenname
: Gibt den Namen des Clientknotens an.

Name der Zuordnung des virtuellen Dateibereichs
: Gibt den Namen der Zuordnung des virtuellen Dateibereichs an.

Dateibereichsname

: Der Name des Dateibereichs, der zu dem Knoten gehört.

: Dateibereichsnamen können eine andere Zeichenumsetztabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal

gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

Pfad
: Gibt den Pfad zum Clientknoten an.

Hexadezimaler Pfad
: Gibt an, ob der Pfad ein hexadezimaler Pfad ist.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY VIRTUALFSMAPPING

Befehl	Beschreibung
DEFINE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs definieren.
DELETE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs löschen.
UPDATE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs aktualisieren.

QUERY VOLHISTORY (History-Daten für sequentielle Datenträger anzeigen)

Mit diesem Befehl können History-Daten von sequenziellen Datenträgern angezeigt werden. Um Protokolldaten sequenzieller Datenträger in einer oder mehreren Dateien zu speichern, verwenden Sie den Befehl BACKUP VOLHISTORY.

Verwenden Sie die Serveroption VOLUMEHISTORY, um eine oder mehrere Protokolldateien für Datenträger anzugeben. Nachdem der Server erneut gestartet wurde, aktualisiert IBM Spectrum Protect die Datenträgerinformationen in der Datenbank und in den Dateien.

Mit dem Befehl QUERY BACKUPSET können Informationen zur angegebenen Sicherungsgruppe abgefragt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                    .-BEGINDate--=--frühestes_Datum-.
>>-Query VOLHistory--+-------------------------------+---------->
                     '-BEGINDate--=--Datum-----------'

   .-ENDDate--=--aktuelles_Datum-.
>--+-----------------------------+----------------------------->
   '-ENDDate--=--Datum-----------'

   .-BEGINTime--=--00:00:00-.
>--+------------------------+---------------------------------->
   '-BEGINTime--=--Zeit-----'

   .-ENDTime--=--aktuelle_Uhrzeit-.
>--+-------------------------------+---------------------------->
   '-ENDTime--=--Zeit-------------'

   .-Type--=--All-------------.
>--+--------------------------+------------------------------><
   '-Type--=--+-All---------+-'
              +-BACKUPSET---+
              +-DBBackup----+
              +-DBRpf-------+
              +-DBSnapshot--+
              +-EXPort------+
              |        (1)  |
              +-REMote------+
              +-RPFile------+
              +-RPFSnapshot-+
              +-STGDelete---+
              +-STGNew------+
              '-STGReuse----'
```

Anmerkungen:

1. Dieser Parameter ist nur für die Betriebssysteme AIX, HP-UX, Linux, Solaris und Windows verfügbar.

Parameter

BEGINDate

Gibt an, dass Informationen beginnend mit den Sätzen angezeigt werden sollen, die an einem angegebenen Datum erstellt wurden. Dieser Parameter ist wahlfrei. Standardwert ist das früheste Datum, ab dem History-Daten vorliegen.
Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage	TODAY–7 **oder** –7. Sollen Informationen beginnend mit den Sätzen, die vor einer Woche erstellt wurden, angezeigt werden, BEGINDATE=TODAY-7 oder BEGINDATE=-7 angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDDate

Gibt an, dass Informationen bis zu den Sätzen angezeigt werden sollen, die an dem angegebenen Datum erstellt wurden. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum.
Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage beträgt 9999.	TODAY–1 **oder** –1. Sollen Sätze angezeigt werden, die bis gestern erstellt wurden, ENDDATE=TODAY-1 oder ENDDATE=-1 angeben.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt an, dass Informationen beginnend mit den Sätzen angezeigt werden sollen, die zu der angegebenen Uhrzeit erstellt wurden. Dieser Parameter ist wahlfrei. Der Standardwert ist Mitternacht (00:00:00).
Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Anfangsdatum	12:33:28
NOW	Die aktuelle Uhrzeit am angegebenen Anfangsdatum	NOW

Wert	Beschreibung	Beispiel
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Anfangsdatum	NOW+03:00 **oder** +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW+03:00 oder BEGINTIME=+03:00 ausgegeben, zeigt IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 Uhr oder später am Anfangsdatum an.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum	NOW-03:30 **oder** -03:30. Wird dieser Befehl um 9:00 Uhr mit der Angabe BEGINTIME=NOW-03:30 oder BEGINTIME=-03:30 ausgegeben, zeigt IBM Spectrum Protect Sätze mit der Uhrzeit 5:30 Uhr oder später am Anfangsdatum an.

ENDTime

Gibt an, dass Informationen bis zu den Sätzen angezeigt werden sollen, die zu der angegebenen Uhrzeit am Enddatum erstellt wurden. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit.
Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Enddatum	10:30:08
NOW	Die aktuelle Uhrzeit am angegebenen Enddatum	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum	NOW+03:00 **oder** +03:00. Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW+03:00 oder ENDTIME=+03:00 ausgegeben, zeigt IBM Spectrum Protect Sätze mit der Uhrzeit 12:00 Uhr oder später am Enddatum an.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum	NOW-03:30 **oder** -03:30 Wird dieser Befehl um 9:00 Uhr mit der Angabe ENDTIME=NOW-3:30 oder ENDTIME=-3:30 ausgegeben, zeigt IBM Spectrum Protect Sätze mit der Uhrzeit 5:30 Uhr oder früher am Enddatum an.

Type

Gibt die Art der Sätze an, die aus der Datenträger-History-Datei angezeigt werden sollen. Dieser Parameter ist wahlfrei. Standardwert ist ALL. Gültige Werte:

Alle
: Gibt alle Sätze an.

BACKUPSET
: Gibt an, dass nur Informationen über Datenträger mit Sicherungsgruppen angezeigt werden.

DBBackup
: Gibt an, dass nur Sätze angezeigt werden, die Informationen über Datenträger mit Gesamt- und Teilsicherungen der Datenbank enthalten (Datenträgertypen BACKUPFULL und BACKUPINCR).

DBRpf
: Gibt an, dass nur Sätze angezeigt werden, die Informationen über Datenträger mit Gesamt- und Teilsicherungen der Datenbank und über Datenträger mit Wiederherstellungsplandateiobjekten enthalten (Datenträgertypen BACKUPFULL, BACKUPINCR und RPFILE).

DBSnapshot
: Gibt an, dass nur Sätze angezeigt werden sollen, die Informationen über Datenträger enthalten, die für Datenbankmomentaufnahmesicherungen verwendet werden.

EXPort
: Gibt nur Sätze an, die Informationen über Exportdatenträger enthalten.

REMote
: Gibt an, dass nur Sätze angezeigt werden sollen, die Informationen zu Datenträgern enthalten, die von Kassettenarchivclients verwendet werden.

RPFile
: Gibt an, dass nur Sätze angezeigt werden sollen, die Informationen zu Dateiobjekten eines Wiederherstellungsplans enthalten, die auf einem Zielserver gespeichert sind und unter der Annahme von Datenbankgesamtsicherungen und Teilsicherungen erstellt wurden. Mit dem Parameter werden nur Sätze zu Wiederherstellungsplandateien angezeigt, die unter Verwendung der IBM Spectrum Protect-Funktion für virtuelle Datenträger für die Übertragung zwischen Servern auf einem anderen IBM Spectrum Protect-Server gespeichert werden.

RPFSnapshot
: Gibt an, dass nur Sätze angezeigt werden sollen, die Informationen zu Dateiobjekten eines Wiederherstellungsplans enthalten, die auf einem Zielserver gespeichert sind und unter der Annahme von Datenbankmomentaufnahmesicherungen erstellt wurden. Mit RPFSnapshot werden nur Sätze zu Wiederherstellungsplandateien angezeigt, die unter Verwendung der IBM Spectrum Protect-

Funktion für virtuelle Datenträger für die Übertragung zwischen Servern auf einem anderen IBM Spectrum Protect-Server gespeichert werden.

STGDelete
: Gibt nur Sätze an, die Informationen über gelöschte sequenzielle Datenträger aus dem Speicherpool enthalten.

STGNew
: Gibt nur Sätze an, die Informationen über neue Speicherdatenträger mit sequenziellem Zugriff enthalten.

STGReuse
: Gibt nur Sätze an, die Informationen über wiederverwendete sequenzielle Datenträger aus dem Speicherpool enthalten.

Beispiel: Datenträgerprotokolldaten für einen Speicherpooldatenträger anzeigen

Zeigen Sie Datenträgerprotokolldaten für einen Speicherpooldatenträger an, der in der Datenbank gespeichert ist. Für Feldbeschreibungen siehe Feldbeschreibungen. Den folgenden Befehl ausgeben:

```
query volhistory type=stgnew
```

```
                                                Datum/Uhrzeit: 02/25/2011 18:28:06
                                              Datenträgertyp: STGNEW
                                              Sicherungsserie:
                                            Sicherungsoperation:
                                               Datenträgerfolge:
                                              Einheitenklasse: FILE
                                              Datenträgername: /adsmfct/server/prvol1
                                            Datenträgerstandort:
                                                        Befehl:
                                    Obere Datenbanksicherungs-ID:
                                   Untere Datenbanksicherungs-ID:
                         Ausgangsposition für Datenbanksicherung:
                 Adresse der höheren Ebene für Datenbanksicherung:
                 Adresse der unteren Ebene für Datenbanksicherung:
                  Summe der Datenbyte für Datenbanksicherung (MB):
               Summe der Protokollbyte für Datenbanksicherung (MB):
                           Obere Blocknummer für Datenbanksicherung:
                          Untere Blocknummer für Datenbanksicherung:
                                 Datenbanksicherungsdatenstrom-ID:
      Folgenummer des Datenbanksicherungsdatenträgers für Datenstrom:
```

Anmerkung: Die Datenträgerhistorydatei enthält zusätzliche Felder, die in der Ausgabe der Abfrage nicht angezeigt werden. Diese Felder beziehen sich speziell auf die Unterstützung der Datenbanksicherung und -zurückschreibung. Sie sind nicht für die Verwendung oder Änderung durch IBM Spectrum Protect-Administratoren bestimmt. Die Felder sind mit einer Nachricht in Klammern versehen, die angibt, dass die Felder nur für die interne IBM Spectrum Protect-Verwendung und nicht für die Änderung bestimmt sind.

Beispiel: Datenträgerprotokolldaten für einen Datenbanksicherungsdatenträger anzeigen

Zeigen Sie Datenträgerprotokolldaten für einen Datenbanksicherungsdatenträger an, der in der Datenbank gespeichert ist. Für Feldbeschreibungen siehe Feldbeschreibungen. Den folgenden Befehl ausgeben:

```
query volhistory type=dbb
```

```
                                          Datum/Uhrzeit: 02/25/2011 18:28:06
                                        Datenträgertyp: BACKUPFULL
                                        Sicherungsserie: 176
                                      Sicherungsoperation: 0
                                         Datenträgerfolge: 0
                                        Einheitenklasse: FILE
                                        Datenträgername: /adsmfct/server/prvol1
                                      Datenträgerstandort:
                                                  Befehl:
                              Obere Datenbanksicherungs-ID: 0
                             Untere Datenbanksicherungs-ID: 0
                   Ausgangsposition für Datenbanksicherung: 0
           Adresse der höheren Ebene für Datenbanksicherung:
           Adresse der unteren Ebene für Datenbanksicherung:
            Summe der Datenbyte für Datenbanksicherung (MB): 0
         Summe der Protokollbyte für Datenbanksicherung (MB): 0
                     Obere Blocknummer für Datenbanksicherung: 0
                    Untere Blocknummer für Datenbanksicherung: 0
                           Datenbanksicherungsdatenstrom-ID: 1
  Folgenummer des Datenbanksicherungsdatenträgers für Datenstrom: 10.001
```

Anmerkung: Die Datenträgerhistorydatei enthält zusätzliche Felder, die in der Ausgabe der Abfrage nicht angezeigt werden. Diese Felder beziehen sich speziell auf die Unterstützung der Datenbanksicherung und -zurückschreibung. Sie sind nicht für die Verwendung oder Änderung durch IBM Spectrum Protect-Administratoren bestimmt. Die Felder sind mit einer Nachricht in Klammern versehen, die angibt, dass die Felder nur für die interne IBM Spectrum Protect-Verwendung und nicht für die Änderung bestimmt sind.

Feldbeschreibungen

Datum/Uhrzeit
: Das Datum und die Uhrzeit, an dem bzw. zu der der Datenträger erstellt wurde.

Datenträgertyp
: Der Typ des Datenträgers:

  BACKUPFULL
  : Datenträger mit Gesamtsicherung der Datenbank.

  BACKUPINCR
  : Datenträger mit Teilsicherung der Datenbank.

  BACKUPSET
  : Datenträger mit Clientsicherungsgruppe.

  DBSNAPSHOT
  : Datenträger mit Datenbankmomentaufnahmesicherung.

  EXPORT
  : Exportdatenträger.

  REMOTE
  : Ein Datenträger, der auf dem Kassettenarchivclient verwendet wird, der der im Feld für den Datenträgerstandort angegebene IBM Spectrum Protect-Server ist. Die Datenträger-History auf dem Server, der der Kassettenarchivclient ist, enthält ausführliche Informationen zur Verwendung des Datenträgers.

  RPFILE
  : Datenträger mit Wiederherstellungsplandateiobjekt, der unter der Annahme von Gesamt- und Teilsicherungen der Datenbank erstellt wurde.

  RPFSnapshot
  : Datenträger mit Wiederherstellungsplandateiobjekt, der unter der Annahme von Datenbankmomentaufnahmesicherungen erstellt wurde.

  STGDELETE
  : Gelöschter Datenträger aus dem Speicherpool mit sequenziellem Zugriff.

  STGNEW
  : Hinzugefügter Datenträger aus dem Speicherpool mit sequenziellem Zugriff.

  STGREUSE
  : Wiederverwendeter Datenträger aus dem Speicherpool mit sequenziellem Zugriff.

Sicherungsserie
: Der Wert dieses Felds hängt vom Datenträgertyp ab:

  - Für den Datenträgertyp BACKUPFULL oder BACKUPINCR: Die Kennung der Sicherungsserie.
  - Für den Datenträgertyp DBSNAPSHOT: Die Kennung der Sicherungsserie, die dem Eintrag DBSNAPSHOT zugeordnet ist.
  - Für den Datenträgertyp RPFILE: Die Kennung der Sicherungsserie, die dem Eintrag RPFILE zugeordnet ist.
  - Für den Datenträgertyp RPFSNAPSHOT: Die Kennung der Sicherungsserie, die dem Eintrag RPFSNAPSHOT zugeordnet ist.
  - Für den Datenträgertyp BACKUPSET: Dieses Feld ist leer.
  - Für alle anderen Datenträgertypen: Immer 0.

  Eine Sicherungsserie besteht aus einer Gesamtsicherung und aus allen Teilsicherungen, die zu dieser Gesamtsicherung gehören. Eine neue Sicherungsserie beginnt bei der nächsten Gesamtsicherung der Datenbank.

Sicherungsoperation
: Für den Datenträgertyp BACKUPFULL oder BACKUPINCR: Die Operationsnummer dieses Sicherungsdatenträgers innerhalb der Sicherungsserie. Eine Gesamtsicherung innerhalb einer Sicherungsserie wird als Operation 0 angegeben. Die erste Teilsicherung für diese Gesamtsicherung wird als Operation 1 bezeichnet, die zweite Teilsicherung als Operation 2 usw.

  Für Datenträgertypen DBSNAPSHOT: Die Operationsnummer dieses DBSNAPSHOT-Datenträgers innerhalb der DBSNAPSHOT-Serie.

  Für alle anderen Datenträgertypen: Immer 0.

  Dieses Feld ist leer, wenn der Datenträgertyp BACKUPSET lautet.

Datenträgerfolge
: Die Folge oder Position des Datenträgers innerhalb der Sicherungsserie.

  - Für den Datenträgertyp BACKUPFULL oder BACKUPINCR: Die Folge oder Position des Datenträgers innerhalb der Sicherungsserie. Die Datenträgerfolge 1 kennzeichnet den für die erste Operation (eine Gesamtsicherung) verwendeten ersten Datenträger usw. Belegt die Gesamtsicherung beispielsweise drei Datenträger, werden diese Datenträger als Datenträgerfolge 1, 2 und 3 gekennzeichnet. Der erste Datenträger der nächsten Operation (die erste Teilsicherung) wird demnach als Datenträgerfolge 4 bezeichnet.
  - Für Datenträgertypen BACKUPSET: Die Folge oder Position des Datenträgers innerhalb der BACKUPSET-Serie.
  - Für Datenträgertypen DBSNAPSHOT: Die Folge oder Position des Datenträgers innerhalb der DBSNAPSHOT-Serie. Die Datenträgerfolge 1 gibt den ersten Datenträger für die erste DBSNAPSHOT-Operation an, usw.
  - Für den Datenträgertyp EXPORT: Die Folgenummer des Datenträgers, wenn er zum Exportieren von Daten verwendet wurde.
  - Für den Datenträgertyp RPFILE: Der Wert dieses Feldes ist immer 1.

- Für alle anderen Datenträgertypen: Immer 0.

Einheitenklasse
: Der Name der Einheitenklasse, die diesem Datenträger zugeordnet ist.

Datenträgername
: Der Name des Datenträgers.

Datenträgerstandort
: Der Standort des Datenträgers. Diese Informationen sind nur für die folgenden Datenträgertypen verfügbar:

  - BACKUPFULL
  - BACKUPINCR
  - EXPORT
  - REMOTE
  - RPFILE

  Für den Datenträgertyp REMOTE ist dieses Feld für den Standort der Servername des Kassettenarchivclients, der Eigner dieses Datenträgers ist.

  Für den Datenträgertyp RPFILE ist dieses Feld für den Standort der Servername, der in der Einheitenklassendefinition definiert ist, die von dem Befehl PREPARE verwendet wird, wenn der Parameter DEVCLASS angegeben ist.

Befehl
: Lautet der Datenträgertyp EXPORT oder BACKUPSET und lautet die Datenträgerfolge 1 (der erste Datenträger), zeigt dieses Feld den Befehl, der zum Generieren des Datenträgers verwendet wurde. Befindet sich EXPORT oder BACKUPSET auf mehreren Datenträgern, wird der Befehl mit dem ersten Datenträger, aber nicht mit allen anderen Datenträgern angezeigt.

  Bei einem anderen Datenträgertyp als EXPORT oder BACKUPSET ist dieses Feld leer.

Tipp: Die folgenden Felder werden von IBM Spectrum Protect-Servern mit Version 6.3 oder höher nicht verwendet. Die Felder werden jedoch für die Kompatibilität mit früheren Releases angezeigt.

- Obere Datenbanksicherungs-ID
- Untere Datenbanksicherungs-ID
- Ausgangsposition für Datenbanksicherung
- Adresse der höheren Ebene für Datenbanksicherung
- Adresse der unteren Ebene für Datenbanksicherung
- Summe der Datenbyte für Datenbanksicherung (MB)
- Summe der Protokollbyte für Datenbanksicherung (MB)
- Obere Blocknummer für Datenbanksicherung
- Untere Blocknummer für Datenbanksicherung

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY VOLHISTORY

Befehl	Beschreibung
BACKUP VOLHISTORY	Zeichnet Datenträger-History-Daten in externen Dateien auf.
DELETE VOLHISTORY	Löscht History-Daten sequenzieller Datenträger aus der Datenträger-History-Datei.
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY RPFILE	Zeigt Informationen über Wiederherstellungsplandateien an.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
UPDATE VOLHISTORY	Ändert Standortinformationen für einen Datenträger in der Datenträger-History-Datei oder fügt Informationen hinzu.

QUERY VOLUME (Speicherpooldatenträger abfragen)

Mit diesem Befehl können Informationen über einen oder mehrere Speicherpooldatenträger angezeigt werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                .-*---------------.
```

Parameter

Datenträgername
: Gibt den Datenträger an, der abgefragt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Name angegeben, werden alle Speicherpooldatenträger in der Abfrage berücksichtigt.

ACCess
: Gibt an, daß die Ausgabe auf bestimmte Datenträgerzugriffsmodi beschränkt ist. Dieser Parameter ist wahlfrei. Es können mehrere Zugriffsmodi angegeben werden, indem die Modi ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, wird die Ausgabe nicht auf bestimmte Zugriffsmodi beschränkt. Gültige Werte:

  READWrite
  : Datenträger mit dem Zugriffsmodus READWRITE anzeigen.Client-Knoten und Server-Prozesse haben Lese- und Schreibzugriff auf Dateien, die auf den Datenträgern gespeichert sind.

  READOnly
  : Datenträger mit dem Zugriffsmodus READONLY anzeigen.Clientknoten und Serverprozesse haben nur Lesezugriff auf Dateien, die auf den Datenträgern gespeichert sind.

  UNAVailable
  : Datenträger mit dem Zugriffsmodus UNAVAILABLE anzeigen.Clientknoten und Serverprozesse können nicht auf Dateien zugreifen, die auf den Datenträgern gespeichert sind.

  OFFsite
  : Kopienspeicherpooldatenträger mit dem Zugriffsmodus OFFSITE anzeigen. Die Datenträger befinden sich an ausgelagerten Standorten, von denen aus sie nicht geladen werden können.

  DEStroyed
  : Datenträger für primären Speicherpool mit dem Zugriffsmodus DESTROYED anzeigen. Die Datenträger sind als permanent beschädigt gekennzeichnet.

STatus
: Gibt an, daß die Ausgabe auf bestimmte Datenträgerstatus beschränkt ist. Dieser Parameter ist wahlfrei. Es können mehrere Statuswerte angegeben werden, indem die Werte ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, wird die Ausgabe auf keinen bestimmte Status beschränkt. Gültige Werte:

  ONline
  : Datenträger mit wahlfreiem Zugriff anzeigen, die für den Server verfügbar sind.

  OFfline
  : Datenträger mit wahlfreiem Zugriff anzeigen, die für den Server nicht verfügbar sind.

  EMPty
  : Datenträger mit sequentiellem Zugriff anzeigen, die keine Daten enthalten.

  PENding
  : Datenträger mit dem Status PENDING anzeigen. Diese Datenträger können Datenträger mit sequenziellem Zugriff sein, auf denen alle Dateien gelöscht wurden, aber für die die mit dem Parameter REUSEDELAY im Befehl DEFINE STGPOOL angegebene Zeit noch nicht abgelaufen ist. Bei diesen Datenträgern kann es sich auch um Plattendatenträger mit wahlfreiem Zugriff handeln, die gelöscht

wurden, aber noch gelöschte Daten enthalten, die auf das Schreddern warten. Nach dem Schreddern der Daten wird der Datenträger physisch gelöscht.

FILling
: Datenträger mit sequentiellem Zugriff anzeigen, auf die der Server geschrieben hat, die aber noch nicht vollständig beschrieben sind.

FULl
: Datenträger mit sequenziellem Zugriff anzeigen, die vom Server gefüllt wurden.

STGPool
: Gibt den Speicherpool an, der in der Abfrage berücksichtigt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Speicherpoolname angegeben, werden alle Speicherpools in der Abfrage berücksichtigt.

DEVclass
: Gibt die Einheitenklasse an, die in der Abfrage berücksichtigt werden soll. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Einheitenklassenname angegeben, werden alle Einheiten in der Abfrage berücksichtigt.

Format
: Gibt an, wie die Informationen angezeigt werden. Dieser Parameter ist wahlfrei. Der Standardwert ist STANDARD. Gültige Werte:

  Standard
  : Gibt an, dass Teilinformationen angezeigt werden.

  Detailed
  : Gibt an, dass die gesamten Informationen angezeigt werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme

Beispiel: Alle Dateispeicherpooldatenträger auflisten

Informationen zu allen Speicherpooldatenträgern mit dem Einheitenklassenname FILE anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query volume devclass=file
```

```
Datenträger-            Speicher-   Einheiten- Gesch.     %     Datentr.-
name                    poolname    klassen-   Kapazit.  Ausl.  status
----------------------- ----------- ---------- --------- ----- -------
/FCT/SERVER/COVOl1      COPYSTG      FILE         0,0 M    0,0 Pending
/FCT/SERVER/COVOl2      COPYSTG      FILE         0,0 M    0,0 Empty
/FCT/SERVER/COVOl3      COPYSTG      FILE         0,0 M    0,0 Empty
/FCT/SERVER/PRVOl1      PRIMESTG     FILE         0,0 M    0,0 Empty
/FCT/SERVER/PRVOl2      PRIMESTG     FILE         0,0 M    0,0 Empty
```

 Windows-Betriebssysteme

Beispiel: Alle Speicherpooldatenträger mit demselben Präfix auflisten

Informationen zu allen Speicherpooldatenträgern, deren Name mit dem Präfix ATF beginnt, anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query volume atf*
```

```
Datenträger-            Speicher-   Einheiten- Gesch.     %     Datentr.-
name                    poolname    klassen-   Kapazit.  Ausl.  status
----------------------- ----------- ---------- --------- ----- -------
ATF001                  8MMPOOL     8MMTAPE       4,8 G   18,2 Filling
ATF002                  8MMPOOL     8MMTAPE       4,8 G   18,2 Filling
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

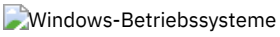
Beispiel: Ausführliche Informationen zu einem bestimmten Speicherpooldatenträger anzeigen

Ausführliche Informationen über den Speicherpooldatenträger /fct/server/covol1 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query volume covol1 format=detailed
```

```
                  Datenträgername: /FCT/SERVER/COVOl1
                            Speicherpoolname: COPYSTG
                       Einheitenklassenname: DISK
                       Geschätzte Kapazität: 10,0 M
                 Skalierte Kapazität angewendet:
                              Auslastung in %: 6,7
                             Datenträgerstatus: On-line
                                       Zugriff: Read/Write
           Wiederherstellbarer Speicher in %: 3,2
                        Arbeitsdatenträger?: Yes
                           Im Fehlerstatus?: No
               Anzahl beschreibbarer Seiten: 1
                              Anzahl Mounts: 11
```

```
                  Anzahl Schreibarbeitsgänge: 1
       Ungefähres Datum des letzten Schreibens: 04/14/1998 16:17:26
           Ungefähres Datum des letzten Lesens: 04/01/1998 13:26:18
                               Anstehend seit:
                           Anzahl Schreibfehler: 0
                              Anzahl Lesefehler: 0
                            Datenträgerstandort:
         Datenträger kann in MVS LAN-frei sein: No
   Letzte Aktualisierung durch (Administrator): COLLIN
         Datum/Zeit der letzten Aktualisierung: 05/01/1998 14:07:27
          Anfang der Wiederherstellungsperiode:
            Ende der Wiederherstellungsperiode:
                   Geschützter logischer Block:
  Manager für Laufwerkverschlüsselungsschlüssel:
```



Beispiel: Ausführliche Informationen zu einem bestimmten Speicherpooldatenträger anzeigen

Ausführliche Informationen über den Speicherpooldatenträger WPDV00 anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query volume wpdv00 format=detailed
```

```
                    Datenträgername: WPDV00
                               Speicherpoolname: TAPEPOOL
                           Einheitenklassenname: TAPE
                           Geschätzte Kapazität: 5,8 M
                 Skalierte Kapazität angewendet:
                               Auslastung in %: 0,1
                             Datenträgerstatus: On-line
                                       Zugriff: Read/Write
            Wiederherstellbarer Speicher in %: 3,2
                          Arbeitsdatenträger?: Yes
                             Im Fehlerstatus?: No
                  Anzahl beschreibbarer Seiten: 1
                               Anzahl Mounts: 11
                    Anzahl Schreibarbeitsgänge: 1
       Ungefähres Datum des letzten Schreibens: 04/14/1998 16:17:26
           Ungefähres Datum des letzten Lesens: 04/01/1998 13:26:18
                               Anstehend seit:
                           Anzahl Schreibfehler: 0
                              Anzahl Lesefehler: 0
                            Datenträgerstandort:
         Datenträger kann in MVS LAN-frei sein: No
   Letzte Aktualisierung durch (Administrator): COLLIN
         Datum/Zeit der letzten Aktualisierung: 05/01/1998 14:07:27
          Anfang der Wiederherstellungsperiode:
            Ende der Wiederherstellungsperiode:
                   Geschützter logischer Block:
  Manager für Laufwerkverschlüsselungsschlüssel:
```

Beispiel: Ausführliche Informationen zu einem Speicherpooldatenträger mit einer bestimmten Einheitenklasse anzeigen

Ausführliche Informationen zu einem Datenträger in einem Speicherpool mit dem Einheitenklassennamen FILECLASS anzeigen. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query volume devclass=fileclass format=detailed
```


```
Datenträgername: Z:\WORM_CFS\0000000E.BFS
                    Datenträgername: /WORM_FILESYS/0000000E.BFS
                               Speicherpoolname: FILEPOOL
                           Einheitenklassenname: FILECLASS
                           Geschätzte Kapazität: 2,0 G
                 Skalierte Kapazität angewendet:
                               Auslastung in %: 0,0
                             Datenträgerstatus: Filling
                                       Zugriff: Read/Write
            Wiederherstellbarer Speicher in %: 0,0
                          Arbeitsdatenträger?: Yes
                             Im Fehlerstatus?: No
                  Anzahl beschreibbarer Seiten: 1
                               Anzahl Mounts: 1
                    Anzahl Schreibarbeitsgänge: 1
       Ungefähres Datum des letzten Schreibens: 03/22/2004 15:23:46
           Ungefähres Datum des letzten Lesens: 03/22/2004 15:23:46
                               Anstehend seit:
                           Anzahl Schreibfehler: 0
                              Anzahl Lesefehler: 0
                            Datenträgerstandort:
```

```
        Datenträger kann in MVS LAN-frei sein: No
   Letzte Aktualisierung durch (Administrator):
        Datum/Zeit der letzten Aktualisierung: 03/22/2004 15:23:46
         Anfang der Wiederherstellungsperiode: 03/22/2005
           Ende der Wiederherstellungsperiode: 04/22/2005
                  Geschützter logischer Block:
  Manager für Laufwerkverschlüsselungsschlüssel:
```

Beispiel: Ausführliche Informationen zu einem bestimmten Speicherpooldatenträger anzeigen

Ausführliche Informationen zu dem Speicherpooldatenträger 000642 anzeigen. Der Datenträger befindet sich in einem Speicherpool, dem die Einheitenklasse 3592 zugeordnet ist. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
query volume 000642 format=detailed
```

```
                    Datenträgername: 000642
                              Speicherpoolname: 3592POOL
                            Einheitenklassenname: 3592CLASS
                            Geschätzte Kapazität: 2,0 G
                  Skalierte Kapazität angewendet:
                                 Auslastung in %: 0,0
                               Datenträgerstatus: Filling
                                         Zugriff: Read/Write
              Wiederherstellbarer Speicher in %: 0,0
                           Arbeitsdatenträger?: Yes
                              Im Fehlerstatus?: No
                  Anzahl beschreibbarer Seiten: 1
                                  Anzahl Mounts: 1
                    Anzahl Schreibarbeitsgänge: 1
        Ungefähres Datum des letzten Schreibens: 03/22/2004 15:23:46
            Ungefähres Datum des letzten Lesens: 03/22/2004 15:23:46
                                  Anstehend seit:
                            Anzahl Schreibfehler: 0
                               Anzahl Lesefehler: 0
                             Datenträgerstandort:
          Datenträger kann in MVS LAN-frei sein: No
     Letzte Aktualisierung durch (Administrator):
          Datum/Zeit der letzten Aktualisierung: 03/22/2004 15:23:46
           Anfang der Wiederherstellungsperiode: 03/22/2005
             Ende der Wiederherstellungsperiode: 04/22/2005
                    Geschützter logischer Block: Yes
    Manager für Laufwerkverschlüsselungsschlüssel: IBM Spectrum Protect
```

Feldbeschreibungen

Datenträgername
: Der Name des Speicherpooldatenträgers.

Speicherpoolname
: Der Speicherpool, für den der Datenträger definiert ist.

Einheitenklassenname
: Die Einheitenklasse, die dem Speicherpool zugeordnet ist.

Geschätzte Kapazität
: Die geschätzte Kapazität des Datenträgers in Megabyte (M), Gigabyte (G) oder Terabyte (T).

  Bei Platteneinheiten ist dies die Kapazität des Datenträgers.

  Bei Einheiten mit sequenziellem Zugriff ist dieser Wert der geschätzte Gesamtspeicherbereich, der auf dem Datenträger verfügbar ist (auf der Basis der Einheitenklasse).

Skalierte Kapazität angewendet
: Der Prozentsatz der Kapazität, der als Maßstabsfaktor für einen Datenträger dient. Beispiel: Der Wert 20 für einen Datenträger, dessen maximale Kapazität 300 GB beträgt, gibt an, dass der Datenträger nur 20 Prozent von 300 GB oder 60 GB speichern kann. Dieses Attribut gilt nur für Einheiten IBM® 3592.

Auslastung in %
: Die geschätzte Auslastung des Datenträgers. Die Auslastung umfasst den gesamten Speicherbereich, der sowohl von Dateien als auch von Aggregaten belegt ist, einschließlich des leeren Speicherbereichs innerhalb der Aggregate.

  Bei Plattendatenträgern umfasst die Auslastung auch den Speicherbereich, der von zwischengespeicherten Daten belegt wird.

Datenträgerstatus
: Der Status des Datenträgers.

Zugriff
: Angabe, ob der Datenträger für den Server verfügbar ist.

Wiederherstellbarer Speicher in % (nur Datenträger mit sequenziellem Zugriff)
: Der Speicherbereich auf diesem Datenträger, der zurückgefordert werden kann, da Daten verfallen sind oder gelöscht wurden. Dieser Wert wird mit der Wiederherstellungsschwelle für den Speicherpool verglichen, um zu bestimmen, ob eine Wiederherstellung erforderlich ist.

Wiederherstellbarer Speicherbereich schließt leeren Speicherbereich innerhalb von Aggregaten ein.

Bei der Bestimmung der wiederherzustellenden Datenträger in einem Speicherpool bestimmt der Server zuerst den Wiederherstellungsschwellenwert. Der Wiederherstellungsschwellenwert wird durch den Wert des Parameters THRESHOLD im Befehl RECLAIM STGPOOL oder, wenn dieser Wert nicht angegeben wurde, durch den Wert des Parameters RECLAIM in einer Speicherpooldefinition angegeben. Der Server überprüft dann den Prozentsatz des wiederherstellbaren Speicherbereichs für jeden Datenträger in dem Speicherpool. Ist der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools, ist der Datenträger ein Kandidat für die Wiederherstellung.

Beispiel: Angenommen, der Speicherpool FILEPOOL hat einen Wiederherstellungsschwellenwert von 70 Prozent. Dieser Wert gibt an, dass der Server jeden Datenträger in dem Speicherpool wiederherstellen kann, der einen höheren Prozentsatz des wiederherstellbaren Speicherbereichs als 70 Prozent hat. Der Speicherpool verfügt über drei Datenträger:

- FILEVOL1 hat 65 Prozent wiederherstellbaren Speicherbereich
- FILEVOL2 hat 80 Prozent wiederherstellbaren Speicherbereich
- FILEVOL3 hat 95 Prozent wiederherstellbaren Speicherbereich

Wenn die Wiederherstellung beginnt, vergleicht der Server den Prozentsatz des wiederherstellbaren Speicherbereichs für jeden Datenträger mit dem Wiederherstellungsschwellenwert von 70 Prozent. In diesem Beispiel sind FILEVOL2 und FILEVOL3 Kandidaten für die Wiederherstellung, da ihr Prozentsatz des wiederherstellbaren Speicherbereichs größer als 70 Prozent ist.

Für Datenträger, die zu einem SnapLock-Speicherpool gehören, wird der Wert angezeigt, aber nicht verwendet.

Arbeitsdatenträger? (nur Datenträger mit sequenziellem Zugriff)
: Angabe, ob dieser Datenträger wieder als Arbeitsdatenträger verwendet wird, wenn er leer wird.

Im Fehlerstatus?
: Angabe, ob ein Fehler beim Datenträger vorliegt. Der Server kann nicht auf Datenträger schreiben, die sich im Fehlerstatus befinden.

Anzahl beschreibbarer Seiten
: Diese Informationen sind für IBM Spectrum Protect reserviert.

Anzahl Mounts
: Die Häufigkeit, mit der der Server den Datenträger für die Verwendung geöffnet hat. Die Häufigkeit, mit der der Server den Datenträger geöffnet hat, ist nicht immer mit der Häufigkeit identisch, mit der der Datenträger physisch in ein Laufwerk geladen wurde. Nachdem ein Datenträger physisch geladen wurde, kann der Server denselben Datenträger mehrere Male für verschiedene Operationen öffnen, beispielsweise für verschiedene Clientsicherungssitzungen.

Anzahl Schreibarbeitsgänge (nur Datenträger mit sequenziellem Zugriff)
: Angabe, wie oft der Datenträger von Anfang bis Ende beschrieben wurde.

Ungefähres Datum des letzten Schreibens
: Das ungefähre Datum, an dem der Datenträger zuletzt beschrieben wurde.

Ungefähres Datum des letzten Lesens
: Das ungefähre Datum, an dem der Datenträger zuletzt gelesen wurde.

Anstehend seit
: Das Datum, an dem der Status des Datenträgers in 'Anstehend' geändert wurde.

Anzahl Schreibfehler
: Die Anzahl Schreibfehler, die auf dem Datenträger aufgetreten sind.

Anzahl Lesefehler
: Die Anzahl Lesefehler, die auf dem Datenträger aufgetreten sind.

Datenträgerstandort
: Der Standort des Datenträgers.

Datenträger kann in MVS LAN-frei sein
: Gibt an, ob der Datenträger LAN-unabhängig ist. Ein LAN-unabhängiger Datenträger ist ein Datenträger, der definiert und (mindestens einmal) von dem IBM Spectrum Protect z/OS-Datenmanagerserver verwendet wurde.

Letzte Aktualisierung durch (Administrator)
: Der Administrator, der den Datenträger definiert oder zuletzt aktualisiert hat.

Datum/Zeit der letzten Aktualisierung
: Das Datum und die Uhrzeit, an dem bzw. zu der der Datenträger definiert oder zuletzt aktualisiert wurde.

Anfang der Wiederherstellungsperiode
: Stellt das Datum dar, nach dem der Server mit der Wiederherstellung dieses Datenträgers beginnt. Dieses Datum darf nicht nach dem Datum liegen, das durch das Ende der Wiederherstellungsperiode dargestellt ist. Befinden sich bei Beginn der Wiederherstellungsperiode Dateien auf dem Datenträger, die nicht verfallen sind, werden sie während der Wiederherstellungsverarbeitung auf einen neuen WORM-Datenträger versetzt. Dieses Feld zeigt nur dann ein Datum an, wenn sich dieser Datenträger in einem Speicherpool befindet, für den der Wert des Parameters RECLAMATIONTYPE SNAPLOCK lautet.

  Sind mehrere Archivierungen auf demselben Datenträger gespeichert, basiert der Anfang der Wiederherstellungsperiode des Datenträgers auf dem Datum der neuesten Archivierung. Für SnapLock-Datenträger bestimmt der Parameter RETVer des Befehls DEFINE COPYGROUP, wie lange eine Archivierung gespeichert wird. Ist RETVer auf 100 Tage gesetzt, beginnt die Wiederherstellungsperiode des Datenträgers 100 Tage nach dem Speichern der ersten Archivierung auf dem Datenträger. Wird eine zweite Archivierung auf demselben Datenträger gespeichert, wird das Anfangsdatum der Wiederherstellung auf 100 Tage nach dem Speichern der neuen Archivierung angepasst. Wird der Wert für RETVer geändert, nachdem die erste Archivierung gespeichert wurde, gilt das älteste Wiederherstellungsdatum für alle Archivierungen auf dem Datenträger. Beispiel: Angenommen, RETVer ist für eine anfängliche Archivierung auf 100 gesetzt, aber wird dann

in 50 geändert. Wird eine zweite Archivierung auf dem Datenträger drei Tage nach der ersten Archivierung gespeichert, beginnt die Wiederherstellungsperiode erst 100 Tage nach dem Speichern der ersten Archivierung.

Ende der Wiederherstellungsperiode
: Stellt das Datum dar, bis zu dem der IBM Spectrum Protect-Server die Wiederherstellungsverarbeitung auf diesem Datenträger beenden muss, um den ununterbrochenen Schutz der Daten sicherzustellen. Es stellt außerdem das Attribut der physischen Datei für das Datum des letzten Zugriffs im NetApp-Dateiserver dar, mit dem verhindert wird, dass die Datei vor diesem Datum gelöscht wird. Dieses Feld zeigt nur dann ein Datum an, wenn sich dieser Datenträger in einem Speicherpool befindet, für den der Wert des Parameters RECLAMATIONTYPE SNAPLOCK lautet.

Manager für Laufwerkverschlüsselungsschlüssel
: Der Manager für Laufwerkverschlüsselungsschlüssel. Dieses Feld gilt nur für Datenträger in einem Speicherpool, dem der Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet ist.

Geschützter logischer Block
: Gibt an, ob der Schutz logischer Blöcke für den Datenträger aktiviert ist. Sie können den Schutz logischer Blöcke nur mit den folgenden Typen von Laufwerken und Datenträgern verwenden:

  - IBM LTO5 und höher
  - IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
  - Oracle StorageTek T10000C- und T10000D-Laufwerke

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY VOLUME

Befehl	Beschreibung
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
DELETE VOLUME	Löscht einen Datenträger aus einem Speicherpool.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.
UPDATE VOLUME	Aktualisiert die Attribute der Speicherpooldatenträger.
VARY	Gibt an, ob ein Plattendatenträger für die Verwendung durch den Server verfügbar ist.

QUIT (Interaktiven Modus des Verwaltungsclient verlassen)

Mit diesem Befehl kann eine Verwaltungs-Client-Sitzung im interaktiven Modus beendet werden.

Der Befehl QUIT kann nicht von der Verwaltungs-ID SERVER_CONSOLE oder im Konsolenmodus, Stapelbetrieb oder Mountmodus des Verwaltungsclients verwendet werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-QUIT-----------------------------------------------------------><
```

Parameter

Keine.

Beispiel: Eine interaktive Verwaltungsclientsitzung beenden

Eine im interaktiven Modus befindliche Verwaltungssitzung des Clients verlassen.

```
quit
```

Zugehörige Befehle

Keine.

RECLAIM STGPOOL (Datenträger im Speicherpool mit sequenziellem Zugriff wiederherstellen)

Verwenden Sie diesen Befehl, um Datenträger in einem Speicherpool mit sequenziellem Zugriff wiederherzustellen. Bei der Wiederherstellung werden keine inaktiven Versionen von Sicherungsdaten von Datenträgern in Pools für aktive Daten versetzt.

Dieser Befehl kann für die folgenden Typen von Speicherpools nicht verwendet werden:

- Containerkopienspeicherpools. Speicherbereich in diesen Speicherpools wird im Rahmen der Verarbeitung wiederhergestellt, die durch die Befehle PROTECT STGPOOL erfolgt.
- Speicherpools mit einem der folgenden Datenformate:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
- Speicherpools, die eine Einheitenklasse CENTERA verwenden.
- Speicherpools, die eine Einheitenklasse WORM (Write Once Read Many) verwenden. Die Wiederherstellung ist nicht erforderlich, da WORM-Datenträger nicht wiederverwendbar sind. Sie können jedoch eine Wiederherstellung ausführen, um Daten auf weniger Datenträgern zusammenzufassen.

Verwenden Sie diesen Befehl nur, wenn die automatische Wiederherstellung für den Speicherpool nicht verwendet wird. Dieser Befehl akzeptiert die Werte der Attribute RECLAIMPROCESS und RECLAIMSTGPOOL der Speicherpooldefinition. Dieser Befehl akzeptiert auch die Werte der Parameter OFFSITERECLAIMLIMIT und RECLAIM der Speicherpooldefinition, sofern sie nicht durch die Befehlsparameter OFFSITERECLAIMLIMIT und THRESHOLD überschrieben werden.

Tipps:

- Wird dieser Befehl ausgegeben, werden doppelte Daten in einem primären Speicherpool, Kopienspeicherpool oder Pool für aktive Daten entfernt, der für die Deduplizierung von Daten definiert ist.
- Wenn Sie diesen Befehl verwenden, um deduplizierte Objekte in denselben Speicherpool zurückzuschreiben, werden alle doppelten Datenblöcke durch Referenzen auf deduplizierte Speicherbereiche ersetzt.

Für Speicherpools, die mit RECLAMATIONTYPE=SNAPLOCK definiert sind, löscht dieser Befehl auch leere WORM-FILE-Datenträger, die ihren Wiederherstellungszeitraum überschritten haben.

Berechtigungsklasse

Um diesen Befehl auszugeben, benötigen Sie die Systemberechtigung, die uneingeschränkte Speicherberechtigung oder die eingeschränkte Speicherberechtigung für den Speicherpool, der wiederhergestellt wird, und den Wiederherstellungsspeicherpool, sofern zutreffend.

Syntax

```
>>-RECLaim STGpool--Poolname--+--------------------+------------>
                              '-THreshold--=--Zahl-'

                             .-Wait--=--No------.
>--+----------------------+--+------------------+--------------->
   '-DUration--=--Minuten-'  '-Wait--=--+-No--+-'
                                        '-Yes-'

>--+-----------------------------------------------+-------------><
   '-OFFSITERECLAIMLimit--=--Anzahl_Datenträger-'
```

Parameter

Poolname (Erforderlich)
: Gibt den Speicherpool an, in dem Datenträger wiederhergestellt werden sollen.

DUration
: Gibt die maximale Anzahl Minuten an, die die Wiederherstellung ausgeführt wird, bevor sie automatisch abgebrochen wird. Sie können eine Zahl von 1 bis 9999 angeben. Dieser Parameter ist wahlfrei.

  Nachdem die angegebene Anzahl Minuten verstrichen ist, stoppt der Server den Wiederherstellungsprozess, wenn er den Prozess das nächste Mal überprüft. Der Server überprüft den Wiederherstellungsprozess, wenn er einen anderen auswählbaren Datenträger aus dem Speicherpool lädt, der wiederhergestellt wird. Außerdem überprüft der Server den Wiederherstellungsprozess, wenn er mit der Wiederherstellung eines neuen Stapels Dateien auf dem gegenwärtig geladenen Datenträger beginnt. Aus diesem Grund kann die Wiederherstellung länger dauern als mit dem Wert für diesen Parameter angegeben ist.

  Bis zur Überprüfung des Wiederherstellungsprozesses durch den Server gibt es keinen Hinweis darüber, dass die Dauer abgelaufen ist. Wenn der Server den Wiederherstellungsprozess stoppt, gibt er die Nachricht ANR4927W aus: `Wiederherstellung für Datenträger xxx beendet - Dauer überschritten.`

Wenn Sie diesen Parameter nicht angeben, wird der Prozess nur gestoppt, wenn keine weiteren Datenträger dem Schwellenwert entsprechen.

Wird ein Wert für die Dauer der Wiederherstellung eines Kopienspeicherpools mit ausgelagerten Datenträgern angegeben, kann die Wiederherstellung beendet werden, bevor Datenträger wiederhergestellt werden. In den meisten Fällen sollte beim Einleiten der Wiederherstellung für einen Kopienspeicherpool mit ausgelagerten Datenträgern die Anzahl der ausgelagerten Datenträger, die wiederhergestellt werden sollen, und nicht die Dauer begrenzt werden. Ausführliche Informationen befinden sich in der Beschreibung des Parameters OFFSITERECLAIMLIMIT.

THreshold
Gibt den Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger an, mit dem der Datenträger für die Wiederherstellung auswählbar ist. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der Serverdatenbank gelöscht wurden. Der wiederherstellbare Speicherbereich schließt auch freien Speicherbereich ein.

Sie können eine Zahl von 1 bis 99 angeben. Dieser Parameter ist wahlfrei. Falls nicht angegeben, wird das Attribut RECLAIM der Speicherpooldefinition verwendet.

Um den Prozentsatz des wiederherstellbaren Speicherbereichs für einen Datenträger zu bestimmen, geben Sie den Befehl QUERY VOLUME aus und geben Sie FORMAT=DETAILED an. Der Wert im Feld 'Wiederherstellbarer Speicher in %' ist der Prozentsatz des wiederherstellbaren Speicherbereichs für den Datenträger.

Geben Sie einen Wert von 50 Prozent oder höher für diesen Parameter an, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Zieldatenträger gespeichert werden können.

OFFSITERECLAIMLimit
Gibt die maximale Anzahl ausgelagerter Speicherpooldatenträger an, die der Server wiederherzustellen versucht. Dieser Parameter ist nur für Kopienspeicherpools gültig. Sie können eine Zahl von 0 bis 99999 angeben. Dieser Parameter ist wahlfrei. Falls nicht angegeben, wird das Attribut OFFSITERECLAIMLIMIT der Speicherpooldefinition verwendet.

Wait
Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die von dem Hintergrundprozess erstellt werden, werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Wird dieser Prozess abgebrochen, wurden möglicherweise bereits einige Dateien vor dem Abbruch auf neue Datenträger versetzt.

Yes
Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Ausgabenachrichten werden dem Verwaltungsclient angezeigt, wenn die Operation beendet ist. Nachrichten werden auch im Aktivitätenprotokoll und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.
Einschränkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

Beispiel: Datenträger in einem Speicherpool mit sequenziellem Zugriff wiederherstellen

Datenträger in dem Speicherpool TAPEPOOL wiederherstellen. Angeben, dass die Wiederherstellung so schnell wie möglich nach 60 Minuten beendet werden soll.

```
reclaim stgpool tapepool duration=60
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RECLAIM STGPOOL

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
MIGRATE STGPOOL	Lagert Dateien aus einem primären Speicherpool in den nächsten Speicherpool in der Hierarchie um.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.

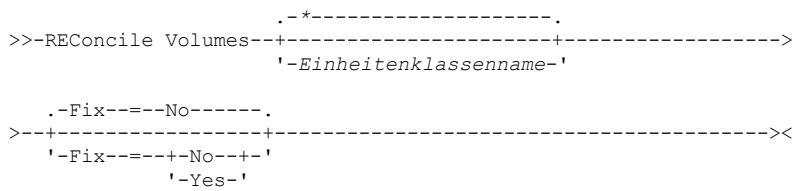
RECONCILE VOLUMES (Unterschiede abstimmen)

Diesen Befehl vom Quellen-Server ausgeben, um Unterschiede zwischen den Definitionen der virtuellen Datenträger auf dem Quellen-Server und den Archivierungsdateien auf dem Ziel-Server abzustimmen. IBM Spectrum Protect sucht alle Datenträger mit der angegebenen Einheitenklasse auf dem Quellen-Server und alle entsprechenden Archivierungsdateien auf dem Ziel-Server. Der Datenträgerbestand auf dem Ziel-Server wird auch mit der lokalen Definition für virtuelle Datenträger verglichen, um festzustellen, ob Inkonsistenzen vorhanden sind.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Einheitenklassenname
: Gibt den Einheitenklassennamen der virtuellen Datenträger an. Wird kein Name angegeben, werden alle virtuellen Datenträger von IBM Spectrum Protect abgestimmt. Dieser Parameter ist wahlfrei.

FIX
: Gibt an, ob IBM Spectrum Protect versucht, die gefundenen Inkonsistenzen zu korrigieren. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, daß IBM Spectrum Protect keine Inkonsistenzen korrigiert.

  Yes
  : Gibt an, daß IBM Spectrum Protect die folgenden Korrekturen vornimmt:

    - Speicherpooldatenträger auf dem Quellen-Server, die auf dem Ziel-Server nicht gefunden werden, werden von IBM Spectrum Protect als nicht verfügbar markiert. Datenträger, die nur in der Datenträger-History gefunden werden, wie beispielsweise Datenbanksicherungen und Import- und Exportdatenträger, werden als inkonsistent gemeldet.
    - Archivierungsdateien auf dem Ziel-Server, die nicht mit virtuellen Datenträgern auf dem Quellen-Server übereinstimmen, werden zum Löschen vom Ziel-Server markiert.

    Die folgende Tabelle zeigt Details zu den Aktionen:

FIX=	Auf dem Quellen-Server	Auf dem Ziel-Server	Aktion
NO	Datenträger vorhanden	Keine Dateien vorhanden	Fehler berichten
		Dateien vorhanden, aber zum Löschen markiert	
		Aktive Dateien vorhanden, aber Attribute stimmen nicht überein	
	Datenträger nicht vorhanden	Aktive Dateien vorhanden	Fehler berichten
		Dateien vorhanden, aber zum Löschen markiert	Keine.
YES	Datenträger vorhanden	Keine Dateien vorhanden	Fehler berichten **Speicherpooldatenträger:** Als nicht verfügbar markiert

FIX=	Auf dem Quellen-Server	Auf dem Ziel-Server	Aktion
		Dateien vorhanden, aber zum Löschen markiert	Fehler berichten **Speicherpooldatenträger:** Stimmen die Attribute überein, sind die Dateien auf dem Ziel-Server erneut als aktiv zu markieren; die Datenträger auf dem Quellen-Server sind als nicht verfügbar zu markieren und es empfiehlt sich, ein AUDIT VOLUME durchzuführen, um die Daten zu prüfen. Stimmen die Attribute nicht überein, sind die Datenträger als nicht verfügbar zu markieren.
		Aktive Dateien vorhanden, aber Attribute stimmen nicht überein	Fehler berichten **Speicherpooldatenträger:** Als nicht verfügbar markieren und empfehlen, daß ein AUDIT VOLUME durchgeführt wird, um die Daten zu prüfen.
	Datenträger nicht vorhanden	Aktive Dateien vorhanden	Dateien zum Löschen auf dem Ziel-Server markieren.
		Dateien vorhanden, aber zum Löschen markiert	Keine.

Beispiel: Abweichungen zwischen den Definitionen der virtuellen Datenträger abstimmen

Die Unterschiede zwischen allen Definitionen der virtuellen Datenträger auf dem Quellen-Server und den Archivierungsdateien auf dem Ziel-Server abstimmen, um alle Inkonsistenzen zu korrigieren.

```
reconcile volumes remote1 fix=yes
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RECONCILE VOLUMES

Befehl	Beschreibung
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DELETE SERVER	Löscht die Definition eines Servers.
QUERY SERVER	Zeigt Informationen über Server an.
UPDATE SERVER	Aktualisiert Informationen über einen Server.

REGISTER-Befehle

Mit den REGISTER-Befehlen können Objekte in IBM Spectrum Protect definiert oder hinzugefügt werden.

- REGISTER ADMIN (Administrator-ID registrieren)
- REGISTER LICENSE (Neue Lizenz registrieren)
- REGISTER NODE (Knoten registrieren)

REGISTER ADMIN (Administrator-ID registrieren)

Verwenden Sie diesen Befehl, um dem Server einen Administrator hinzuzufügen. Nach der Registrierung kann der Administrator eine begrenzte Gruppe von Befehlen, einschließlich aller Abfragebefehle, ausgeben. Sollen weitere Berechtigungen zur Verfügung gestellt werden, verwenden Sie den Befehl GRANT AUTHORITY.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

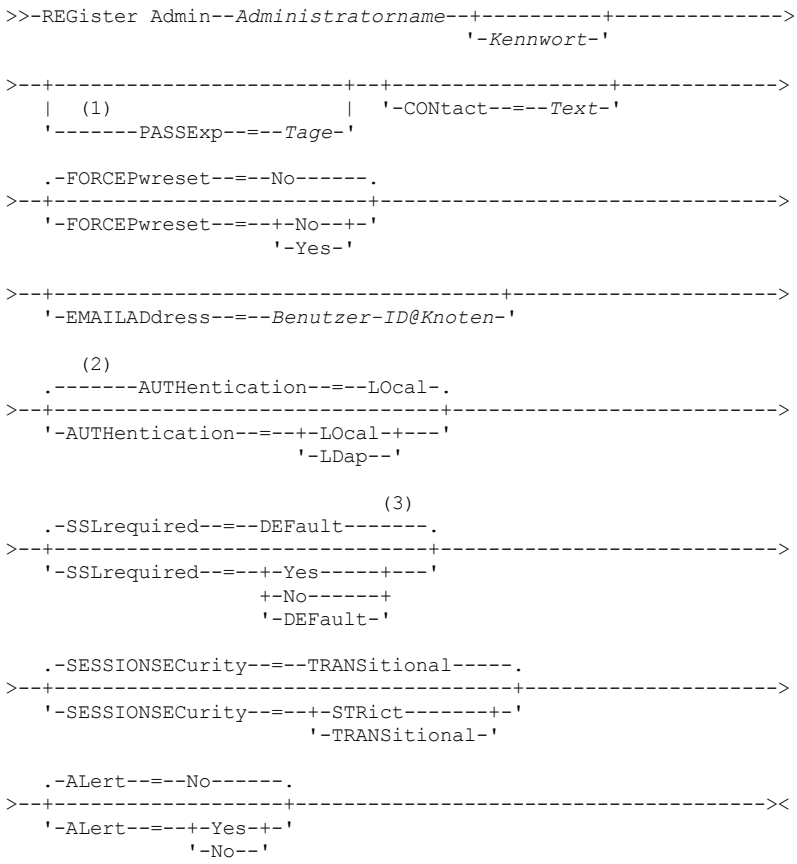
Wenn Sie einen Administrator mit dem Namen eines vorhandenen Knotens registrieren, beachten Sie die Authentifizierungsmethode des Administrators und die Einstellung für SSLREQUIRED. Jeder Knoten, der denselben Namen wie der Administrator hat, der registriert wird, übernimmt diese Einstellungen.
Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in

Kennwörter und Anmeldeverfahren verwalten.

- Geben Sie keine Benutzer-ID mit Administratorberechtigung an, die mit einem Knotennamen identisch ist. Wenn die Benutzer-ID mit Administratorberechtigung mit dem Knotennamen übereinstimmt, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierungsoperation fehlschlägt.

Syntax



Anmerkungen:

1. Der Befehl PASSEXP gilt nicht für Administratoren, die sich mit einem LDAP-Verzeichnisserver authentifizieren.
2. Der Standardwert kann sich ändern, wenn Sie den Befehl SET DEFAULTAUTHENTICATION ausgegeben und LDAP angegeben haben.
3. Der Parameter SSLREQUIRED ist veraltet.

Parameter

Administratorname (Erforderlich)
Gibt den Namen des zu registrierenden Administrators an. Die maximale Länge des Namens beträgt 64 Zeichen.

Der Administratorname NONE darf nicht angegeben werden.

Soll die Administrator-ID mit einem LDAP-Server authentifiziert werden, stellen Sie sicher, dass die Administrator-ID nicht mit dem Namen eines Knotens übereinstimmt, der sich mit einem LDAP-Server authentifiziert.

Kennwort
Gibt das Kennwort des zu registrierenden Administrators an. Das Kennwort darf maximal 64 Zeichen lang sein.
Wenn Sie Kennwörter lokal mit dem IBM Spectrum Protect-Server authentifizieren, müssen Sie ein Kennwort angeben. Bei dem Kennwort muss die Groß-/Kleinschreibung nicht beachtet werden.
Wenn Sie Kennwörter mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifizieren, geben Sie kein Kennwort im Befehl REGISTER ADMIN an.

PASSExp
Gibt die Anzahl der Tage an, die das Kennwort gültig ist. Für die Kennwortablaufdauer kann ein Wert von 0 bis 9999 Tage definiert werden. Der Wert 0 bedeutet, dass das Kennwort niemals abläuft. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird das Kennwort mit der globalen Verfallsperiode von 90 Tagen definiert. Dieser Parameter hat keine Auswirkungen auf Kennwörter, die sich mit einem LDAP-Verzeichnisserver authentifizieren.

CONtact

Liefert Informationen zum Administrator, der registriert wird. Dieser Parameter ist wahlfrei. Diese Zeichenfolge kann maximal 255 Zeichen lang sein. Die Kontaktinformationen müssen in Anführungszeichen eingeschlossen sein, falls Leerzeichen enthalten sind.

FORCEPwreset

Gibt an, ob der Administrator das Kennwort ändern oder zurücksetzen muss. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass der Administrator bei dem Versuch, sich beim Server anzumelden, das Kennwort nicht ändern bzw. zurücksetzen muss.

Yes

Gibt an, dass das Kennwort des Administrators bei der nächsten Anmeldung abläuft. Der Client bzw. Administrator muss das Kennwort dann ändern oder zurücksetzen. Wird kein Kennwort angegeben, wird eine Fehlernachricht empfangen.
Einschränkung: Für Benutzer-IDs mit Administratorberechtigung, die mit einem LDAP-Server authentifiziert werden, wird der Kennwortablauf mithilfe von LDAP-Serverdienstprogrammen definiert. Geben Sie daher nicht FORCEPWRESET=YES an, wenn Sie AUTHENTICATION=LDAP angeben.

EMAILADdress

Gibt die E-Mail-Adresse für diesen Administrator an.

AUTHentication

Dieser Parameter gibt die Authentifizierungsmethode für die Administrator-ID an. Geben Sie einen der folgenden Werte an: LDAP oder LOCAL. Der Parameter ist wahlfrei und nimmt standardmäßig den Wert LOCAL an. Der Standardwert kann sich in LDAP ändern, wenn Sie den Befehl SET DEFAULTAUTHENTICATION verwenden und LDAP angeben.

LOcal

Gibt an, dass die lokale IBM Spectrum Protect-Serverdatenbank verwendet wird.

LDap

Gibt an, dass die Administrator-ID Kennwörter mit einem LDAP-Verzeichnisserver authentifiziert. Bei Kennwörtern, die mit einem LDAP-Verzeichnisserver authentifiziert werden, muss die Groß-/Kleinschreibung beachtet werden.
Tipp: Ein Kennwort ist nicht erforderlich, wenn Sie einen Administrator registrieren und `AUTHENTICATION=LDAP` auswählen. Bei der Anmeldung werden Sie zur Eingabe eines Kennworts aufgefordert.

SSLrequired (veraltet)

Gibt an, ob die Administrator-ID das Protokoll Secure Sockets Layer (SSL) für die Kommunikation zwischen dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren verwenden muss. Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, müssen Sie die Sitzungen mit SSL oder einer anderen Netzsicherheitsmethode schützen.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter SSLREQUIRED wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

SESSIONSECurity

Gibt an, ob der Administrator die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

STRict

Gibt an, dass die striktesten Sicherheitseinstellungen für den Administrator durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem Server und dem Administrator verwendet. Um anzugeben, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, lesen Sie die Informationen zur Clientoption SSL.
Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der Administrator mit dem Server authentifizieren kann:

- Der Administrator und der Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Administrator muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen dem Server und dem Administrator konfiguriert werden.

Administratoren, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem Server authentifizieren.

TRANSitional

Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Administrator durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Administrator nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Administrator weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Administrator jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Administrator kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Administrator erfolgreich mit einem

Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Administrator nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Administrator, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Administrator nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. Befehlsweiterleitung oder Export zwischen Servern, wenn sich der Administrator beim IBM Spectrum Protect-Server als Administrator von einem anderen Server authentifiziert.

ALert
Gibt an, ob Alerts an die E-Mail-Adresse eines Administrators gesendet werden.

Yes
Gibt an, dass Alerts an die E-Mail-Adresse des angegebenen Administrators gesendet werden.

No
Gibt an, dass Alerts nicht an die E-Mail-Adresse des angegebenen Administrators gesendet werden. Dies ist der Standardwert.

Tipp: Die Alertüberwachung muss aktiviert sein und die E-Mail-Einstellungen müssen korrekt definiert sein, damit Alerts erfolgreich als E-Mail empfangen werden können. Um die aktuellen Einstellungen anzuzeigen, geben Sie den Befehl QUERY MONITORSETTINGS aus.

Beispiel: Einen Administrator registrieren

Den Administrator LARRY mit dem Kennwort PASSONE definieren. LARRY kann als Mitarbeiter der zweiten Schicht gekennzeichnet werden, indem diese Information im Parameter CONTACT angegeben wird. Den folgenden Befehl ausgeben:

```
register admin larry passone contact='zweite schicht'
```

Beispiel: Eine Administrator-ID registrieren und die Authentifizierungsmethode definieren

Eine Administrator-ID für Harry definieren, damit sich Harry mit einem LDAP-Server authentifizieren kann. Den folgenden Befehl ausgeben:

```
register admin harry authentication=ldap
```

Beispiel: Einen Administrator registrieren und die Sitzungssicherheit 'strict' durchsetzen

Einen Administrator mit dem Namen Harry registrieren und von Harry verlangen, dass er die striktesten Sicherheitseinstellungen verwendet, um sich mit dem Server zu authentifizieren. Den folgenden Befehl ausgeben:

```
register admin harry sessionsecurity=strict
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REGISTER ADMIN

Befehl	Beschreibung
GRANT AUTHORITY	Ordnet einem Administrator Berechtigungsklassen zu.
LOCK ADMIN	Verweigert einem Administrator den Zugriff auf IBM Spectrum Protect.
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REMOVE ADMIN	Löscht einen Administrator aus der Liste der registrierten Administratoren.
RENAME ADMIN	Ändert den Namen eines IBM Spectrum Protect-Administrators.
SET DEFAULTAUTHENTICATION	Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an.
SET PASSEXP	Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.
UNLOCK ADMIN	Ermöglicht einem gesperrten Administrator den Zugriff auf IBM Spectrum Protect.
UPDATE ADMIN	Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

Zugehörige Tasks:

Tivoli Storage Manager-Objekte benennen
Zugehörige Informationen:
Ssl (Clientoption)

REGISTER LICENSE (Neue Lizenz registrieren)

Verwenden Sie diesen Befehl, um neue Lizenzen für Serverkomponenten zu registrieren, einschließlich IBM Spectrum Protect (Basis), IBM Spectrum Protect Extended Edition und IBM Spectrum Protect for Data Retention.

Lizenzen werden in Registrierungszertifikatsdateien gespeichert. Die Registrierungszertifikatsdateien enthalten Lizenzinformationen für das Serverprodukt. In der NODELOCK-Datei werden die Lizenzinformationen für Ihre Installation aufbewahrt. Ihre Lizenzvereinbarung bestimmt, welche Komponenten Sie verwenden dürfen, auch wenn Sie den Befehl REGISTER LICENSE nicht verwenden können, um alle Komponenten zu registrieren. Es wird erwartet, dass Sie die Lizenzvereinbarung einhalten und nur die Komponenten verwenden, die Sie gekauft haben. Die Verwendung des Befehls REGISTER LICENSE impliziert, dass Sie den Lizenzbedingungen zustimmen und Sie die Lizenzbedingungen akzeptieren, die in Ihrer Lizenzvereinbarung angegeben sind.

Wichtig:

- Bevor Sie ein Upgrade von einer vorherigen Version von IBM Spectrum Protect durchführen, müssen Sie die NODELOCK-Datei löschen oder umbenennen.
- Um die Registrierung von Lizenzen zurückzunehmen, müssen Sie die NODELOCK-Datei im Serverinstanzverzeichnis Ihrer Installation löschen und alle zuvor registrierten Lizenzen erneut registrieren.
- Sie können keine Lizenzen für IBM Spectrum Protect for Mail, IBM Spectrum Protect for Databases, IBM Spectrum Protect for ERP und IBM Spectrum Protect for Space Management registrieren.

Um einen Bericht zu erstellen, der Ihnen hilft, die Lizenzvoraussetzungen für Ihr System zu bestimmen, führen Sie den Befehl QUERY PVUESTIMATE aus. Der Bericht enthält Schätzungen der Anzahl von Clienteinheiten und PVU-Summen für Servereinheiten. Die Schätzungen sind rechtlich nicht bindend.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-REGister LICense--FILE--=--+-tsmbasic.lic-+-----------------><
                              +-tsmee.lic-----+
                              +-dataret.lic--+
                              '-*.lic--------'
```

Parameter

FILE
: Gibt den Namen der Registrierungszertifikatsdatei an, die die zu registrierende Lizenz enthält. Die Angabe kann ein Platzhalterzeichen (*) enthalten. Geben Sie den vollständigen Dateinamen oder anstelle des Dateinamens ein Platzhalterzeichen ein. Bei den Dateinamen muß die Groß-/Kleinschreibung berücksichtigt werden. Die folgenden Werte können verwendet werden:

  tsmbasic.lic
  : Zum Lizenzieren von IBM Spectrum Protect (Basis).

  tsmee.lic
  : Zum Lizenzieren von IBM Spectrum Protect Extended Edition. Dazu gehören Disaster Recovery Manager, große Kassettenarchive und NDMP.

  dataret.lic
  : Zum Lizenzieren von IBM Spectrum Protect for Data Retention. Diese Lizenz ist erforderlich, um den Aufbewahrungsschutz für Daten (Data Retention Protection) sowie die Aussetzung der Verfallsverarbeitung und des Löschens (Status "Löschen unzulässig") zu aktivieren.

  *.lic
  : Zum Lizenzieren aller IBM Spectrum Protect-Lizenzen für Serverkomponenten.

Beispiel: Eine Lizenz registrieren

Die IBM Spectrum Protect-Basislizenz registrieren.

```
register license file=tsmbasic.lic
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REGISTER LICENSE

Befehl	Beschreibung
AUDIT LICENSES	Prüft die Einhaltung der definierten Lizenzen.
QUERY LICENSE	Zeigt Informationen über Lizenzen und Prüfvorgänge an.
QUERY PVUESTIMATE	Zeigt Prozessor-Value-Unit-Schätzungen an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET LICENSEAUDITPERIOD	Gibt die Anzahl Tage zwischen den automatischen Lizenzprüfungen an.

REGISTER NODE (Knoten registrieren)

Verwenden Sie diesen Befehl, um einen Knoten für den Server zu registrieren.

Dieser Befehl kann eine Benutzer-ID mit Administratorberechtigung erstelllen, die über Clienteignerberechtigung für den Knoten verfügt. Mit dieser Benutzer-ID mit Administratorberechtigung kann von fernen Standorten über einen Web-Browser auf den Web-Client für Sichern/Archivieren zugegriffen werden.
Tipp:

- In früheren Produktreleases erstellte der Befehl REGISTER NODE automatisch eine Benutzer-ID mit Administratorberechtigung, deren Name mit dem Knotennamen übereinstimmte. Ab IBM Spectrum Protect Version 8.1 erstellt der Befehl REGISTER NODE nicht automatisch eine Benutzer-ID mit Administratorberechtigung, deren Name mit dem Knotennamen übereinstimmt.
- Wenn Sie die Verwendung der LAN-unabhängigen Option mit diesem Knoten planen, müssen Sie eine Administrator-ID registrieren, die mit dem Knotennamen übereinstimmt. Um die Administrator-ID zu registrieren, verwenden Sie den Parameter USERID oder registrieren Sie manuell den Administrator und erteilen Sie dem Knoten die Eignerberechtigung.

Benötigt ein Client eine andere als die Maßnahmendomäne STANDARD, muss der Clientknoten mit diesem Befehl registriert oder der registrierte Knoten aktualisiert werden.

Voraussetzung: Wenn Sie `sslrequired=serveronly` in einem Befehl REGISTER NODE definieren, wird die Einstellung für SSLREQUIRED für den Administrator auf YES zurückgesetzt. Soll eine Nicht-SSL-Sitzung mit einem Speicheragenten verwendet werden, benennen Sie den Administrator mit dem identischen Namen um, indem Sie den Befehl RENAME ADMIN ausgeben.
Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol): Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
Wenn Sie einen Knoten registrieren oder aktualisieren, können Sie angeben, ob beschädigte Dateien auf dem Knoten von einem Replikationsserver wiederhergestellt werden können. Dateien können nur wiederhergestellt werden, wenn alle folgenden Bedingungen erfüllt sind:

- Version 7.1.1 oder höher ist auf dem Quellen- und Zielreplikationsserver installiert.
- Der Systemparameter REPLRECOVERDAMAGED ist auf ON gesetzt. Der Systemparameter kann mit dem Befehl SET REPLRECOVERDAMAGED definiert werden.
- Der Quellenserver schließt mindestens eine Datei ein, die auf dem Knoten, der repliziert wird, als beschädigt markiert ist.
- Die Knotendaten wurden repliziert, bevor die Beschädigung aufgetreten ist.

In der folgenden Tabelle wird beschrieben, wie sich Parametereinstellungen auf die Wiederherstellung beschädigter, replizierter Dateien auswirken.

Tabelle 1. Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken

Einstellung für den Systemparameter REPLRECOVERDAMAGED	Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE	Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE	Ergebnis
OFF	YES, NO oder nicht angegeben	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.
OFF	ONLY	YES oder NO	Eine Fehlernachricht wird angezeigt, weil Dateien nicht wiederhergestellt werden können, wenn der Systemparameter REPLRECOVERDAMAGED auf OFF gesetzt ist.
ON	YES	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.

Einstellung für den Systemparameter REPLRECOVERDAMAGED	Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE	Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE	Ergebnis
ON	NO	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.
ON	ONLY	YES oder NO	Beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt, aber es findet keine Standardknotenreplikation statt.
ON	Nicht angegeben	YES	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.
ON	Nicht angegeben	NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

Syntax

```
>>-REGister Node--Knotenname--+----------+---------------------->
                              '-Kennwort-'

                               .-USerid--=--NONE------------.
>--+-------------------------+--+----------------------------+--->
   |  (1)                    |  '-USerid--=--+-NONE--------+-'
   '-------PASSExp--=--Tage-'               '-Benutzer-ID-'

                         .-DOmain--=--STANDARD--------.
>--+------------------+--+----------------------------+--------->
   '-CONtact--=--Text-'  '-DOmain--=----Domänenname---'

   .-COMPression--=--Client-----.  .-ARCHDELete--=--Yes-----.
>--+----------------------------+--+-------------------------+--->
   '-COMPression--=--+-Client-+-'  '-ARCHDELete--=--+-Yes-+-'
                     +-Yes----+                     '-No--'
                     '-No-----'

   .-BACKDELete--=--No------.
>--+------------------------+---------------------------------->
   '-BACKDELete--=--+-No--+-'
                    '-Yes-'

>--+--------------------------------+------------------------->
   '-CLOptset--=--Optionsgruppenname-'

   .-FORCEPwreset--=--No------.  .-Type--=--Client------.
>--+--------------------------+--+---------------------+------->
   '-FORCEPwreset--=--+-No--+-'  '-Type--=--+-Client--+-'
                      '-Yes-'               |     (2) |
                                            +-NAS-----+
                                            '-Server--'

>--+-------------+--+-----------------------------------+------->
   '-URL--=--URL-'  '-UTILITYUrl--=--Dienstprogramm-URL-'

   .-MAXNUMMP--=--1------.  .-AUTOFSRename--=--No---------.
>--+---------------------+--+----------------------------+----->
   '-MAXNUMMP--=--Anzahl-'  '-AUTOFSRename--=--+-Yes----+-'
                                               +-No-----+
                                               '-Client-'

   .-KEEPMP--=--No------. (3)
>--+--------------------+---------------------------------------->
   '-KEEPMP--=--+-No--+-'
                '-Yes-'
```


.-VALIdateprotocol--=--No-----------.
>--+-----------------------------------+----------------------->
'-VALIdateprotocol--=--+-No-------+-'
+-Dataonly-+
'-All------'
.-TXNGroupmax--=--0----------.
>--+----------------------------+------------------------------->
'-TXNGroupmax--=--+-0------+-'
'-Anzahl-'
.-DATAWritepath--=--ANY---------.
>--+-------------------------------+----------------------------->
'-DATAWritepath--=--+-ANY-----+-'
+-LAN-----+
'-LANFree-'
.-DATAReadpath--=--ANY---------.
>--+-------------------------------+----------------------------->
'-DATAReadpath--=--+-ANY-----+-'
+-LAN-----+
'-LANFree-'
>--+-------------------------+---------------------------------->
'-TARGETLevel--=--V.R.M.F-'
.-SESSIONINITiation--=--Clientorserver---.
>--+---+-->
'-SESSIONINITiation--=--+-Clientorserver---+-'
'-SERVEROnly--HLAddress--=--IP-Adresse--LLAddress--=--TCP-Anschluss-'
>--+---+---->
'-HLAddress--=--IP-Adresse--LLAddress--=--TCP-Anschluss-'
>--+-------------------------------------+---------------------->
'-EMAILADdress--=--Benutzer-ID@Knoten-'
.-DEDUPlication--=--Clientorserver-----.
>--+-------------------------------------+---------------------->
'-DEDUPlication--=--+-Clientorserver-+-'
'-SERVEROnly-----'
.-BACKUPINITiation--=--All----------.
>--+-----------------------------------+------------------------>
| (4) |
'-BACKUPINITiation--=--+-All--+-----'
'-ROOT-'
>--+----------------------------+------------------------------->
'-REPLState--=--+-ENabled--+-'
'-DISabled-'
.-BKREPLRuledefault--=--DEFAULT-----------------------------.
>--+---+-->
| (5) |
'-------BKREPLRuledefault--=--+-ALL_DATA------------------+-'
+-ACTIVE_DATA----------------+
+-ALL_DATA_HIGH_PRIORITY----+
+-ACTIVE_DATA_HIGH_PRIORITY-+
+-DEFAULT--------------------+
'-NONE----------------------'
.-ARREPLRuledefault--=--DEFAULT--------------------------.
>--+---+--->
| (5) |
'-------ARREPLRuledefault--=--+-ALL_DATA---------------+-'
+-ALL_DATA_HIGH_PRIORITY-+
+-DEFAULT----------------+
'-NONE------------------'
.-SPREPLRuledefault--=--DEFAULT--------------------------.
>--+---+--->
| (5) |
'-------SPREPLRuledefault--=--+-ALL_DATA---------------+-'
+-ALL_DATA_HIGH_PRIORITY-+
+-DEFAULT----------------+
'-NONE------------------'
.-RECOVERDamaged--=--Yes-----.
>--+-------------------------------+----------------------------->
'-RECOVERDamaged--=--+-Yes-+-'
'-No--'

```
   .-ROLEOVERRIDE--=--Usereported-----.
>--+--------------------------------+------------------------>
   '-ROLEOVERRIDE--=--+-Client------+-'
                      +-Server------+
                      +-Other-------+
                      '-Usereported-'

      (6)
   .-------AUTHentication--=--LOcal-.
>--+-------------------------------+------------------------->
   '-AUTHentication--=--+-LOcal-+---'
                        '-LDap--'

                                (7)
   .-SSLrequired--=--DEFault--------.
>--+-------------------------------+------------------------->
   '-SSLrequired--=--+-Yes---------+-'
                     +-No----------+
                     +-DEFault-----+
                     '-SERVERonly-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+-------------------------------------+--------------------->
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'

   .-SPLITLARGEObjects--=--Yes-----.
>--+-----------------------------+--------------------------><
   '-SPLITLARGEObjects--=--+-Yes-+-'
                           '-No--'
```

Anmerkungen:

1. Der Befehl PASSEXP gilt nicht für Administratoren, die sich mit einem LDAP-Verzeichnisserver (LDAP = Lightweight Directory Access Protocol) authentifizieren.
2. Dieser Parameter ist nur für die Betriebssysteme AIX, Linux, Solaris und Windows verfügbar.
3. Der Parameter VALIDATEPROTOCOL ist veraltet.
4. Der Parameter BACKUPINITIATION wird ignoriert, wenn das Betriebssystem des Clientknotens nicht unterstützt wird.
5. Der Parameter BKREPLRULEDEFAULT, ARREPLRULEDEFAULT oder SPREPLRULEDEFAULT kann nur angegeben werden, wenn Sie den Parameter REPLSTATE angeben.
6. Der Standardwert kann sich ändern, wenn Sie den Befehl SET DEFAULTAUTHENTICATION ausgegeben und LDAP angegeben haben.
7. Der Parameter SSLREQUIRED ist veraltet.

Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, der registriert werden soll. Die maximale Länge des Namens beträgt 64 Zeichen.

  Der Knotenname NONE kann nicht angegeben werden.

Kennwort
: Gibt das Clientknotenkennwort an, das eine maximale Länge von 64 Zeichen hat.

  Wenn Sie Kennwörter lokal mit dem IBM Spectrum Protect-Server authentifizieren, müssen Sie ein Kennwort angeben. Bei dem Kennwort muss die Groß-/Kleinschreibung nicht beachtet werden.

  Wenn Sie Kennwörter mit einem LDAP-Server authentifizieren, geben Sie kein Kennwort im Befehl REGISTER NODE an.

PASSExp
: Gibt die Anzahl der Tage an, die das Kennwort gültig ist. Für die Kennwortablaufdauer kann ein Wert von 0 bis 9999 Tage definiert werden. Der Wert 0 bedeutet, dass das Kennwort niemals abläuft. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird die allgemeine Kennwortablaufdauer des Servers verwendet. Die allgemeine Kennwortablaufdauer beträgt 90 Tage, sofern sie nicht mit dem Befehl SET PASSEXP geändert wird.

  Sie können die Kennwortablaufdauer mit dem Befehl UPDATE NODE oder SET PASSEXP ändern. Sie können den Befehl SET PASSEXP ausgeben, um einen allgemeinen Ablaufzeitraum für alle Administratoren und Clientknoten zu definieren. Sie können den Befehl auch verwenden, um die Kennwortablaufdauer selektiv zu definieren. Wenn Sie eine Kennwortablaufdauer selektiv mit dem Befehl REGISTER NODE, UPDATE NODE oder SET PASSEXP festlegen, wird die Ablaufdauer von der jeweiligen allgemeinen Kennwortablaufdauer ausgeschlossen, die mit dem Befehl SET PASSEXP erstellt wurde.

  Sie können den Befehl RESET PASSEXP verwenden, um die Kennwortablaufdauer auf die allgemeine Kennwortablaufdauer zurückzusetzen. Der Befehl PASSEXP gilt nicht für Knoten, die sich mit einem LDAP-Server authentifizieren.

USerid

Gibt die Benutzer-ID mit Administratorberechtigung an, die über Clienteignerberechtigung verfügt. Dieser Parameter ist wahlfrei. Wird vom Client PASSWORDACCESS=GENERATE verwendet, um das Kennwort zu ändern, kann die gleichnamige Benutzer-ID mit Administratorberechtigung verwendet werden, um von einem fernen Standort auf den Web-Client für Sichern/Archivieren zuzugreifen. Sie können einen der folgenden Werte angeben:

NONE
: Gibt an, dass keine Benutzer-ID mit Administratorberechtigung erstellt wird. Dies ist der Standardwert.

Benutzer-ID
: Gibt an, dass eine Benutzer-ID mit Administratorberechtigung mit dem angegebenen Namen erstellt wird. Mit diesem Parameter kann einer vorhandenen Benutzer-ID mit Administratorberechtigung die Clienteignerberechtigung erteilt werden.

Wenn Sie einen Knoten registrieren, der denselben Namen wie ein Administrator hat, ändern sich die Authentifizierungsmethode des Administrators und die Einstellung für SSLREQUIRED, damit sie mit der Authentifizierungsmethode des Knotens übereinstimmen. Kennwörter, die von Knoten und Administratoren mit denselben Namen gemeinsam genutzt werden, bleiben bei einer Authentifizierungsänderung synchronisiert.

Wenn Sie die Verwendung der LAN-unabhängigen Option mit diesem Knoten planen, verwenden Sie den Parameter USERID, um eine Administrator-ID zu registrieren, die mit dem Knotennamen übereinstimmt.

Für Benutzer von LDAP-Servern: Soll der Knoten mit einem LDAP-Server authentifiziert werden, behalten Sie die Standardeinstellung (USERID=NONE) bei oder geben Sie eine Benutzer-ID mit Administratorberechtigung an, die sich vom Knotennamen unterscheidet. Wenn die Benutzer-ID mit Administratorberechtigung mit dem Knotennamen übereinstimmt, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierungsoperation fehlschlägt.

CONtact
: Gibt eine Informationszeichenfolge an, die den Knoten identifiziert. Der Parameter ist wahlfrei.Die maximale Länge der Zeichenfolge beträgt 255 Zeichen. Die Kontaktinformationen müssen in Anführungszeichen eingeschlossen sein, falls Leerzeichen enthalten sind.

DOmain
: Gibt den Namen der Maßnahmendomäne an, der der Knoten zugeordnet ist. Der Parameter ist wahlfrei.Wird kein Maßnahmendomänenname angegeben, wird der Knoten der Standardmaßnahmendomäne (STANDARD) zugeordnet.

  Wenn ein Quellenserver als Knoten registriert wird, wird er einer Maßnahmendomäne zugeordnet. Daten vom Quellenserver werden in dem Speicherpool gespeichert, der in der Archivierungskopiengruppe der Standardverwaltungsklasse dieser Domäne angegeben ist.

COMPression
: Gibt an, ob der Clientknoten seine Dateien komprimiert, bevor diese Dateien zum Sichern und Archivieren an den Server gesendet werden. Der Parameter ist wahlfrei.Der Standardwert ist CLIENT.
  Einschränkung: Dieser Parameter gilt nicht für Knoten mit dem Typ NAS oder SERVER.

  Sie können einen der folgenden Werte angeben:

  Client
  : Gibt an, dass der Client festlegt, ob Dateien komprimiert werden.

  Yes
  : Gibt an, dass der Clientknoten seine Dateien komprimiert, bevor diese Dateien zum Sichern und Archivieren an den Server gesendet werden.

  No
  : Gibt an, dass der Clientknoten seine Dateien nicht komprimiert, bevor diese Dateien zum Sichern und Archivieren an den Server gesendet werden.

ARCHDELete
: Gibt an, ob der Clientknoten seine eigenen Archivierungsdateien aus dem Server löschen darf. Der Parameter ist wahlfrei.Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

  Yes
  : Gibt an, dass der Clientknoten seine eigenen Archivierungsdateien aus dem Server löschen darf.

  No
  : Gibt an, dass der Clientknoten seine eigenen Archivierungsdateien nicht aus dem Server löschen darf.

BACKDELete
: Gibt an, ob der Clientknoten seine eigenen Sicherungsdateien aus dem Server löschen darf. Der Parameter ist wahlfrei.Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

  No
  : Gibt an, dass der Clientknoten seine eigenen Sicherungsdateien nicht aus dem Server löschen darf.

  Yes
  : Gibt an, dass der Clientknoten seine eigenen Sicherungsdateien aus dem Server löschen darf.

CLOptset
: Gibt den Namen der Optionsgruppe an, die der Client verwenden soll. Der Parameter ist wahlfrei.

FORCEPwreset

Gibt an, ob ein Client zum Ändern oder Zurücksetzen des Kennworts gezwungen werden soll. Der Parameter ist wahlfrei.Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No
: Gibt an, dass die Kennwortablaufdauer über den Befehl SET PASSEXP definiert wird. Der Client muss das Kennwort nicht ändern oder zurücksetzen, während er sich beim Server anmeldet.

Yes
: Gibt an, dass das Kennwort des Clientknotens bei der nächsten Anmeldung abläuft. Der Client muss das Kennwort dann ändern oder zurücksetzen. Wird kein Kennwort angegeben, wird eine Fehlernachricht empfangen.
Einschränkung: Für Knoten, die mit einem LDAP-Server authentifiziert werden, wird der Kennwortablauf mithilfe von LDAP-Serverdienstprogrammen definiert. Geben Sie daher nicht FORCEPWRESET=YES an, wenn Sie AUTHENTICATION=LDAP angeben.

Type
: Gibt den Typ des Knotens an, der registriert wird. Der Parameter ist wahlfrei. Der Standardwert ist CLIENT. Sie können einen der folgenden Werte angeben:

Client
: Gibt an, dass der Clientknoten ein Client für Sichern/Archivieren, ein IBM Spectrum Protect for Space Management-Client oder ein Anwendungsclient ist.

NAS
: Gibt an, dass der Knoten ein NAS-Dateiserver ist, dessen Daten durch NDMP-Operationen geschützt werden. Der Knotenname darf nicht SERVER lauten.
Anmerkung: Der Name des NAS-Knotens muss mit dem Namen der Einheit zum Versetzen von Daten übereinstimmen. Aus diesem Grund kann der Name nicht geändert werden, nachdem eine entsprechende Einheit zum Versetzen von Daten definiert wurde.

Server
: Gibt an, dass der Clientknoten ein Quellenserver ist, der auf dem Zielserver registriert wird.

URL
: Gibt die URL des IBM Spectrum Protect-Web-Clients an, die auf dem Clientsystem konfiguriert ist. Sie können die URL in einem Web-Browser und im Operations Center verwenden, um den Clientknoten über Fernzugriff zu verwalten.

Dieser Parameter ist wahlfrei. Die URL muss den DNS-Namen oder die IP-Adresse des Clientsystems und die Anschlussnummer enthalten, die auf dem Clientsystem für den IBM Spectrum Protect-Web-Client definiert ist. Beispiel: `http://client.mycorp.com:1581`

UTILITYUrl
: Gibt die Adresse der IBM Spectrum Protect-Clientverwaltungsservices an, die auf dem Clientsystem konfiguriert sind. Diese URL wird vom Operations Center verwendet, um auf Clientprotokolldateien zuzugreifen, sodass Sie im Operations Center Clientprobleme über Fernzugriff diagnostizieren können.

Dieser Parameter ist wahlfrei. Sie können eine URL mit maximal 200 Zeichen angeben. Die URL muss mit `https` beginnen. Sie enthält den DNS-Namen oder die IP-Adresse des Clientsystems und die Anschlussnummer, die auf dem Clientsystem für die IBM Spectrum Protect-Clientverwaltungsservices definiert ist. Beispiel: `https://client.mycorp.com:9028`

Wird keine Anschlussnummer angegeben, verwendet das Operations Center die Anschlussnummer 9028. Dies ist die Standardanschlussnummer, wenn Sie die Clientverwaltungsservices auf dem Clientsystem installieren.

MAXNUMMP
: Gibt die maximale Anzahl der Mountpunkte an, die ein Knoten nur für Operationen, wie beispielsweise Sicherung, Archivierung und IBM Spectrum Protect for Space Management-Umlagerung, auf dem Server oder dem Speicheragenten verwenden darf. Der Parameter ist optional und gilt nicht für Knoten mit dem Typ NAS oder SERVER. Der Standardwert ist 1. Sie können eine ganze Zahl im Bereich von 0 bis 999 angeben. Der Wert 0 gibt an, dass ein Knoten keinen Mountpunkt für eine Operation zum Speichern von Clientdaten anfordern kann. Der MAXNUMMP-Wert wird während der Operationen zum Lesen von Clientdaten, wie beispielsweise Zurückschreiben, Abrufen und Zurückrufen durch IBM Spectrum Protect for Space Management, nicht ausgewertet oder umgesetzt. Mountpunkte, die für Operationen zum Lesen von Daten verwendet werden, werden jedoch in Bezug auf versuchte gleichzeitig ablaufende Datenspeicherungsoperationen für denselben Clientknoten ausgewertet und können verhindern, dass die Datenspeicherungsoperationen Mountpunkte anfordern können.

Für Datenträger in einem Speicherpool, dem der Einheitentyp FILE oder CENTERA zugeordnet ist, kann der Server über mehrere Sitzungen verfügen, um gleichzeitig denselben Datenträger zu lesen, und über eine Sitzung verfügen, um auf diesen Datenträger zu schreiben. Um den gemeinsamen Zugriff zu erweitern und einen effizienten Zugriff für Knoten mit Daten in Speicherpools des Typs FILE oder CENTERA zur Verfügung zu stellen, erhöhen Sie den Wert des Parameters MAXNUMMP.

Für Knoten, die mit aktivierter Funktion für simultanes Schreiben Daten in primären Speicherpools speichern, müssen Sie den Wert des Parameters MAXNUMMP anpassen, um die korrekte Anzahl der Mountpunkte für jede Clientsitzung anzugeben. Eine Clientsitzung erfordert einen Mountpunkt für den primären Speicherpool und einen Mountpunkt für jeden Kopienspeicherpool und jeden Pool für aktive Daten.

Hat ein Server bei der serverübergreifenden Sicherung eine andere Version als der andere Server, setzen Sie die Anzahl der Mountpunkte auf dem Zielserver auf einen höheren Wert als 1. Andernfalls wird eine Fehlernachricht ausgegeben.

Ein Speicheragent verfolgt unabhängig die Anzahl der Mountpunkte, die während einer Clientsitzung verwendet werden. Ist auf einem Knoten ein Speicheragent installiert, kann der Wert für MAXNUMMP überschritten werden. Der Wert für MAXNUMMP kann auch unter Bedingungen überschritten werden, bei denen der Knoten nicht auf einen Mountpunkt warten muss.

Anmerkung: Der Server kann der Operation eines Clients eine Operation mit höherer Priorität vorziehen, und der Client kann einen Mountpunkt verlieren, wenn keine anderen Mountpunkte verfügbar sind.

KEEPMP

Gibt an, ob der Clientknoten den Mountpunkt für die gesamte Sitzung beibehält. Der Parameter ist wahlfrei.Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

Yes

Gibt an, dass der Clientknoten den Mountpunkt während der gesamten Sitzung beibehalten muss. Haben Maßnahmendefinitionen zur Folge, dass Daten in einem Plattenspeicherpool gespeichert werden, nachdem die Daten in einem Speicherpool mit sequenziellem Zugriff gespeichert wurden, werden alle von der Sitzung belegten Mountpunkte nicht freigegeben.

No

Gibt an, dass der Clientknoten den Mountpunkt während der Sitzung freigibt. Haben Maßnahmendefinitionen zur Folge, dass Daten in einem Plattenspeicherpool gespeichert werden, nachdem die Daten in einem Speicherpool mit sequenziellem Zugriff gespeichert wurden, werden alle von der Sitzung belegten Mountpunkte freigegeben.

AUTOFSRename

Geben Sie an, ob Dateibereiche automatisch umbenannt werden, wenn ein Upgrade des Clientsystems zur Unterstützung von Unicode durchgeführt wird, oder geben Sie an, ob Dateibereiche bei Bedarf vom Client umbenannt werden. Der Parameter ist wahlfrei. Der Standardwert ist NO. Wird der Parameter auf YES gesetzt, wird das automatische Umbenennen aktiviert. Das automatische Umbenennen findet statt, wenn der Client eine der folgenden Operationen ausführt: Archivierung, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung. Beim automatischen Umbenennen werden die Namen von bestehenden gesicherten Dateibereichen, die nicht in Unicode sind, im Serverspeicher geändert. Anschließend werden die Dateibereiche in Unicode gesichert. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients mit den Betriebssystemen Windows, Macintosh OS X und NetWare verwenden.

Nachdem der Client mit Unterstützung für Unicode installiert wurde, werden alle neuen Dateibereiche, die der Client sichert, im Serverspeicher mit der Zeichenumsetztabelle UTF-8 gespeichert. UTF-8 ist eine byte-orientierte Verschlüsselungsform, die durch den Unicode Standard angegeben wird.

Sie können einen der folgenden Werte angeben:

Yes

Vorhandene Dateibereiche werden automatisch umbenannt, wenn ein Upgrade auf einen Client durchgeführt wird, der Unicode unterstützt, und der Client eine der folgenden Operationen ausführt: Archivierung, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung. Das Umbenennen findet statt, wenn der Client die grafische Benutzerschnittstelle, die Befehlszeile oder den Client-Scheduler verwendet.
Beispielsweise wird ein Laufwerk vom Server wie folgt umbenannt:

```
Ursprünglicher Name: D_DRIVE
Neuer Name: D_DRIVE_OLD
```

Der neue Name gibt an, dass der Dateibereich auf dem Server in einem Format gespeichert wird, das kein Unicode ist.

No

Vorhandene Dateibereiche werden nicht automatisch umbenannt, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine der folgenden Operationen ausführt: Archivieren, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung.

Client

Die Option AUTOFSRENAME in der Optionsdatei des Clients bestimmt, ob Dateibereiche umbenannt werden.

Standardmäßig ist die Clientoption auf PROMPT gesetzt. Wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine IBM Spectrum Protect-Operation mit der grafischen Benutzerschnittstelle oder der Befehlszeile ausführt, zeigt das Programm dem Benutzer einmalig eine Bedienerführung an und fordert den Benutzer zur Angabe auf, ob Dateibereiche umbenannt werden sollen.

Wenn der Client-Scheduler eine Operation ausführt, fordert das Programm nicht zur Angabe einer Auswahl für das Umbenennen auf, und es werden keine Dateibereiche umbenannt. Sicherungen von vorhandenen Dateibereichen werden wie zuvor gesendet (nicht in Unicode).

VALIdateprotocol (veraltet)

Gibt an, ob IBM Spectrum Protect eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) ausführt, um die Daten zu validieren, die zwischen dem Client und dem Server gesendet werden. Der Parameter ist wahlfrei. Der Standardwert ist NO.
Wichtig: Ab Version 8.1.2 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter VALIDATEPROTOCOL wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

TXNGroupmax

Gibt die Anzahl der Dateien pro Transaktions-COMMIT an, die zwischen einem Client und einem Server übertragen werden. Der Parameter ist wahlfrei. Die Clientleistung kann verbessert werden, indem ein höherer Wert für diese Option verwendet wird.

Der Standardwert ist 0. Der Wert 0 gibt an, dass der Knoten den globalen Serverwert verwendet, der in der Serveroptionsdatei definiert ist. Soll ein anderer Wert als der globale Serverwert verwendet werden, geben Sie einen Wert von 4 bis 65.000 für diesen Parameter an. Der Knotenwert hat Vorrang vor dem Serverwert.

Achtung: Die Vergrößerung des Werts für TXNGROUPMAX führt zu einer Erhöhung der Auslastung des Wiederherstellungsprotokolls. Eine höhere Auslastung des Wiederherstellungsprotokolls kann das Risiko erhöhen, dass der Protokollspeicherbereich nicht mehr ausreicht. Werten Sie die Leistung jedes Knotens aus, bevor Sie den Parameter ändern.

DATAWritepath

Gibt den Übertragungspfad an, der verwendet wird, wenn der Client während Speicheroperationen (Sicherung oder Archivierung) Daten an den Server und/oder den Speicheragenten sendet. Der Parameter ist wahlfrei.Der Standardwert ist ANY.
Anmerkung: Ist kein Pfad verfügbar, kann der Knoten keine Daten senden. Wenn Sie z. B. die LAN-unabhängige Option auswählen, aber kein LAN-unabhängiger Pfad definiert ist, schlägt die Operation fehl.

Sie können einen der folgenden Werte angeben:

ANY
: Gibt an, dass Daten über einen beliebigen verfügbaren Pfad an den Server und/oder Speicheragenten gesendet werden. Ein LAN-unabhängiger Pfad wird verwendet, wenn einer verfügbar ist. Ist kein LAN-unabhängiger Pfad verfügbar, werden die Daten über das LAN übertragen.

LAN
: Gibt an, dass Daten über das LAN gesendet werden.

LANFree
: Gibt an, dass Daten über einen LAN-unabhängigen Pfad gesendet werden.

DATAReadpath

Gibt den Übertragungspfad an, der verwendet wird, wenn der Server und/oder Speicheragent während Operationen wie Zurückschreiben oder Abrufen Daten für einen Client lesen. Der Parameter ist wahlfrei.Der Standardwert ist ANY.
Anmerkung: Ist kein Pfad verfügbar, können keine Daten gelesen werden. Wenn Sie z. B. die LAN-unabhängige Option auswählen, aber kein LAN-unabhängiger Pfad definiert ist, schlägt die Operation fehl. Der Wert für den Übertragungspfad gilt auch für Übernahmeverbindungen. Wird der Wert auf LANFree gesetzt, kann für den Knoten auf dem sekundären Server keine Übernahme erfolgen.

Sie können einen der folgenden Werte angeben:

ANY
: Gibt an, dass der Server und/oder Speicheragent einen beliebigen verfügbaren Pfad verwenden, um Daten zu lesen. Ein LAN-unabhängiger Pfad wird verwendet, wenn einer verfügbar ist. Ist kein LAN-unabhängiger Pfad verfügbar, werden die Daten über das LAN gelesen.

LAN
: Gibt an, dass Daten über das LAN gelesen werden.

LANFree
: Gibt an, dass Daten über einen LAN-unabhängigen Pfad gelesen werden.

TARGETLevel

Gibt das Clientimplementierungspaket für diesen Knoten an. Für V.R.M.F (Version.Release.Modifikation.Fix-Level) kann ein gültiges Releasepaket angegeben werden. Beispiel: `TARGETLevel=6.2.0.0`.

Sie müssen jedes Segment mit einer Zahl angeben, die für ein Implementierungspaket zutreffend ist. Sie können keinen Stern in einem Feld als Ersetzung für eine gültige Zahl verwenden. Der Parameter ist wahlfrei.
Einschränkung: Der Parameter TARGETLEVEL gilt nicht für Knoten mit dem Typ NAS oder SERVER.

SESSIONINITiation

Steuert, ob der Server oder der Client Sitzungen einleitet. Der Standardwert gibt an, dass der Client Sitzungen einleitet. Der Parameter ist wahlfrei.

Clientorserver
: Gibt an, dass der Client Sitzungen mit dem Server einleiten kann, indem über den TCP/IP-Anschluss kommuniziert wird, der mit der Serveroption TCPPORT definiert wird. Die Zeitplanung über Serversystemanfrage kann ebenfalls verwendet werden, um den Client aufzufordern, eine Verbindung zum Server herzustellen.

SERVEROnly
: Gibt an, dass der Server keine Clientanforderungen für Sitzungen akzeptiert. Alle Sitzungen müssen durch die Zeitplanung über Serversystemanfrage an dem Anschluss eingeleitet werden, der mit dem Befehl REGISTER oder UPDATE NODE für den Client definiert wird. Sie können den Clientakzeptor (dsmcad) nicht verwenden, um den Scheduler zu starten, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist.

HLAddress
: Gibt die Client-IP-Adresse an, die der Server anspricht, um geplante Ereignisse einzuleiten. Dieser Parameter muss verwendet werden, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server anzusprechen.

  Die Adresse kann entweder im numerischen Format oder im Hostnamenformat angegeben werden. Wird eine numerische Adresse verwendet, wird sie ohne Prüfung durch einen Domänennamensserver gesichert. Ist die Adresse nicht korrekt, kann dies zu Fehlern führen, wenn der Server versucht, den Client anzusprechen. Adressen im Hostnamensformat werden mit einem Domänennamensserver geprüft. Geprüfte Namen werden mit Domänennamenservices (Domain Name Services) gesichert und aufgelöst, wenn der Server den Client anspricht.

LLAddress

Gibt die Clientanschlussnummer an, an der der Client für Sitzungen von dem Server empfangsbereit ist. Dieser Parameter muss verwendet werden, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server anzusprechen.

Der Wert für diesen Parameter muss mit dem Wert der Clientoption TCPCLIENTPORT übereinstimmen. Der Standardwert ist 1501.

EMAILADdress

Dieser Parameter wird für weitere Kontaktinformationen verwendet. Der Parameter ist wahlfrei. Die mit diesem Parameter angegebenen Informationen werden von IBM Spectrum Protect nicht verwendet.

DEDUPlication

Gibt an, wo die Datendeduplizierung für diesen Knoten stattfinden kann. Der Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Clientorserver

Gibt an, dass von diesem Knoten gespeicherte Daten entweder auf dem Client oder auf dem Server dedupliziert werden können. Dieser Wert ist der Standardwert. Um die Datendeduplizierung auf dem Client auszuführen, müssen Sie auch den Wert YES für die Clientoption DEDUPLICATION angeben. Sie können diese Option in der Clientoptionsdatei oder in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server angeben.

SERVEROnly

Gibt an, dass von diesem Knoten gespeicherte Daten nur auf dem Server dedupliziert werden können.

BACKUPINITiation

Gibt an, ob die ID eines Benutzers ohne Rootberechtigung auf dem Clientknoten Dateien auf dem Server sichern kann. Der Parameter ist wahlfrei.Der Standardwert ALL gibt an, dass IDs der Benutzer ohne Rootberechtigung Daten auf dem Server sichern können. Sie können einen der folgenden Werte auswählen:

All

Gibt an, dass die IDs der Benutzer ohne Rootberechtigung Dateien auf dem Server sichern können. ALL ist der Standardwert, wenn BACKUPINITIATION nicht angegeben wird.

ROOT

Gibt an, dass die Rootbenutzer-ID Dateien auf dem Server sichern kann. Wenn Sie den Client für Sichern/Archivieren der Version 6.4 oder höher verwenden, haben berechtigte Benutzer dieselben Berechtigungen wie die Rootbenutzer-ID.
Einschränkung: Das Attribut wird vom Server ignoriert, wenn der Client für Sichern/Archivieren eine Verbindung von einem anderen Betriebssystem als AIX, Linux, Solaris oder Mac OS herstellt.
Hinweis: Die Anwendungsprogrammierschnittstelle (API) ist von dem Parameter BACKUPINITIATION auf dem Server betroffen. Standardmäßig dürfen alle API-Benutzer Daten sichern. Es wird nicht empfohlen, den Parameter auf einem API-Knoten auf `ROOT` zu setzen.

REPLState

Gibt an, ob Daten, die zu dem Clientknoten gehören, für die Replikation bereit sind. Dieser Parameter ist wahlfrei. Geben Sie diesen Parameter nur an, wenn Sie den Befehl REGISTER NODE auf einem Server ausgeben, der für die Replikation von Daten auf einen Zielreplikationsserver konfiguriert ist. Wenn Sie einen Clientknoten auf einem Quellenreplikationsserver registrieren und die Replikation für den Knoten definieren, registrieren Sie den Knoten nicht auf dem Zielreplikationsserver. Der Clientknoten wird automatisch auf dem Zielserver erstellt, wenn zum ersten Mal die Replikation erfolgt.
Sie können einen der folgenden Werte auswählen:

ENabled

Gibt an, dass der Clientknoten für die Replikation konfiguriert und für die Replikation bereit ist. Wenn Sie diesen Parameter angeben, wird der Replikationsmodus in der Clientknotendefinition auf dem Quellenreplikationsserver automatisch auf SEND gesetzt. Diese Einstellung gibt an, dass Daten, die zu dem Clientknoten gehören, während der Replikation an einen Zielserver gesendet werden.

Wenn die Replikation zum ersten Mal für den Clientknoten erfolgt, wird der Replikationsstatus des Knotens auf dem Zielreplikationsserver automatisch auf ENABLED gesetzt. Der Replikationsmodus auf dem Zielreplikationsserver wird auf RECEIVE gesetzt. Diese Einstellung gibt an, dass Daten, die zu dem Clientknoten gehören, von einem Quellenreplikationsserver empfangen werden. Um den Replikationsstatus und -modus zu bestimmen, geben Sie den Befehl QUERY NODE auf einem Quellen- oder Zielreplikationsserver aus.

DISabled

Gibt an, dass der Knoten für die Replikation konfiguriert ist, aber die Replikation erst erfolgt, wenn sie aktiviert wurde.

BKREPLRuledefault, ARREPLRuledefault und SPREPLRuledefault

Gibt die Replikationsregel an, die für einen Datentyp gilt, wenn die Dateibereichsregeln für den Datentyp auf DEFAULT gesetzt sind.
Einschränkung: Der Parameter BKREPLRULEDEFAULT, ARREPLRULEDEFAULT oder SPREPLRULEDEFAULT kann nur angegeben werden, wenn Sie den Parameter REPLSTATE angeben.

BKREPLRuledefault

Gibt die Replikationsregel für Sicherungsdaten an.

ARREPLRuledefault

Gibt die Replikationsregel für Archivierungsdaten an.

SPREPLRuledefault
: Gibt die Replikationsregel für speicherverwaltete Daten an.

Sind die Dateibereichsregeln für den Datentyp auf DEFAULT gesetzt und geben Sie keine Regel für den Parameter BKREPLRULEDEFAULT, ARREPLRULEDEFAULT oder SPREPLRULEDEFAULT an, werden Daten gemäß der Serverregel für den Datentyp repliziert.

Sie können Replikationsregeln für normale Priorität oder Replikationsregeln für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Sie können die folgenden Regeln angeben:

ALL_DATA
: Repliziert aktive und inaktive Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.

ACTIVE_DATA
: Repliziert nur aktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert. Diese Regel ist nur für BKREPLRULEDEFAULT gültig.
Achtung:

  Wenn Sie ACTIVE_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

  - Wenn eine Releaseversion vor Version 7.1.1 entweder auf dem Quellenreplikationsserver oder auf dem Zielreplikationsserver installiert ist.
  - Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
  - Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Releaseversion vor Version 7.1.1 ausführen.

  Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

ALL_DATA_HIGH_PRIORITY
: Repliziert aktive und inaktive Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Daten werden mit einer hohen Priorität repliziert.

ACTIVE_DATA_HIGH_PRIORITY
: Diese Regel entspricht der Replikationsregel ACTIVE_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden. Diese Regel ist nur für BKREPLRULEDEFAULT gültig.

DEFAULT
: Repliziert Daten gemäß der Serverreplikationsregel für Sicherungsdaten.

  Beispiel: Angenommen, Sie möchten die Archivierungsdaten in allen Dateibereichen replizieren, die zu einem Clientknoten gehören. Die Replikation der Archivierungsdaten hat eine hohe Priorität. Eine Methode zur Ausführung dieser Task ist die Angabe von `ARREPLRULEDEFAULT=DEFAULT`. Stellen Sie sicher, dass die Dateibereichsregeln für Archivierungsdaten ebenfalls auf DEFAULT gesetzt sind und die Serverregel für Archivierungsdaten auf ALL_DATA_HIGH_PRIORITY gesetzt ist.

  Einschränkung: Wenn ein Knoten für die Replikation konfiguriert ist, werden die Dateibereichsregeln auf DEFAULT gesetzt, nachdem der Knoten Daten auf dem Quellenreplikationsserver gespeichert hat.

NONE
: Daten des angegebenen Typs werden nicht repliziert.

  Sollen beispielsweise speicherverwaltete Daten, die zu einem Clientknoten gehören, nicht repliziert werden, geben Sie `SPREPLRULEDEFAULT=NONE` an.

RECOVERDamaged
: Gibt an, ob beschädigte Dateien für diesen Knoten von einem Zielreplikationsserver wiederhergestellt werden können. Der Parameter ist wahlfrei.Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

  Yes
  : Gibt an, dass die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver für diesen Knoten aktiviert ist.

  No
  : Gibt an, dass die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver für diesen Knoten nicht aktiviert ist. Tipp: Der Wert des Parameters RECOVERDAMAGED ist nur eine von mehreren Einstellungen, die bestimmen, ob beschädigte Dateien wiederhergestellt werden. Informationen zur Angabe der Einstellungen finden Sie in Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken.

ROLEOVERRIDE

Gibt an, ob die zurückgemeldete Rolle des Clients für die Zurückmeldung der PVU-Schätzung (PVU - Prozessor-Value-Unit) überschrieben werden soll. Der Standardwert ist USEREPORTED. Der Parameter ist wahlfrei.

Die vom Client zurückgemeldete Rolle ist entweder 'Clienteinheit' (z. B. eine Workstation) oder 'Servereinheit' (z. B. Datei-/Druckserver, Anwendungsserver, Datenbank). Standardmäßig meldet der Client seine Rolle auf der Basis des Clienttyps und des Betriebssystems zurück. Alle Clients melden anfänglich ihre Rolle als 'Servereinheit' zurück, mit Ausnahme von Clients für Sichern/Archivieren, auf denen Microsoft Windows-Workstationverteilungen (Windows Vista) und Macintosh OS X ausgeführt werden.

Geben Sie einen der folgenden Werte an:

Client
: Gibt eine Clienteinheit an.

Server
: Gibt eine Servereinheit an.

Other
: Gibt an, dass dieser Knoten nicht für die Zurückmeldung der PVU-Schätzung verwendet werden soll. Dieser Wert kann nützlich sein, wenn mehrere Knoten für ein physisches System implementiert sind (z. B. virtuelle Umgebungen, Testknoten, Knoten im Ruhezustand und Knoten, die nicht in der Produktion oder im Clustering sind).

Usereported
: Die zurückgemeldete Rolle verwenden, die vom Client bereitgestellt wird.

AUTHentication
: Dieser Parameter gibt die Kennwortauthentifizierungsmethode für den Knoten an. Geben Sie einen der folgenden Werte an: LDAP oder LOCAL. Der Parameter ist wahlfrei und nimmt standardmäßig den Wert LOCAL an. Der Standardwert kann sich in LDAP ändern, wenn Sie den Befehl SET DEFAULTAUTHENTICATION verwenden und LDAP angeben.

LOcal
: Gibt an, dass die lokale IBM Spectrum Protect-Serverdatenbank verwendet wird.

LDap
: Gibt an, dass der Knoten einen LDAP-Server für die Kennwortauthentifizierung verwendet.

SSLrequired (veraltet)

: Gibt an, ob der Knoten das Protokoll Secure Sockets Layer (SSL) für die Kommunikation mit dem IBM Spectrum Protect-Server verwenden muss. Der Parameter ist wahlfrei.Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, müssen Sie die Sitzungen mit SSL oder einer anderen Netzsicherheitsmethode schützen.

Wichtig: Ab Version 8.1.2 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter SSLREQUIRED wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

SESSIONSECurity
: Gibt an, ob der Knoten die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

STRict
: Gibt an, dass die striktesten Sicherheitseinstellungen für den Knoten durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem Server und dem Knoten verwendet. Um anzugeben, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, lesen Sie die Informationen zur Clientoption SSL.
Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der Knoten mit dem Server authentifizieren kann:

- Der Knoten und der Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Knoten muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen dem Server und dem Knoten konfiguriert werden.

Knoten, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem Server authentifizieren.

TRANSitional
: Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Knoten durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Knoten nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Knoten weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Knoten jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Knoten kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Knoten erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Knoten nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Knoten, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Knoten nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von

Funktionen wie z. B. virtuelle Datenträger, wenn sich der Knoten beim IBM Spectrum Protect-Server als Knoten von einem anderen Server authentifiziert.

SPLITLARGEObjects
Gibt an, ob große Objekte, die von diesem Knoten gespeichert werden, automatisch vom Server in kleinere Teile aufgeteilt werden, um die Serververarbeitung zu optimieren. Der Parameter ist wahlfrei.Die Angabe von 'Yes' hat zur Folge, dass der Server große Objekte (über 10 GB) in kleinere Teile aufteilt, wenn sie von einem Clientknoten gespeichert werden. Bei Angabe von 'No' wird dieser Prozess übergangen. Geben Sie 'No' nur an, wenn Ihr primäres Ziel die Maximierung des Durchsatzes von Sicherungen direkt auf Band ist. Der Standardwert ist 'Yes'.

Beispiel: Einen Clientknoten registrieren, der nur vom Rootbenutzer gesichert werden kann

Den Clientknoten `mete0rite` mit dem Kennwort *KingK0ng* registrieren, um nur dem Rootbenutzer das Sichern von Dateien auf dem Server zu erlauben.

```
register node mete0rite KingK0ng
backupinit=root
```

Beispiel: Einen Clientknoten und ein Kennwort registrieren und die Komprimierung aktivieren

Den Clientknoten `JOEOS2` mit dem Kennwort *SECRETCODE* registrieren und diesen Knoten der Maßnahmendomäne `DOM1` zuordnen. Dieser Knoten kann seine eigenen Sicherungs- und Archivierungsdateien aus dem Server löschen. Der Clientknoten komprimiert alle Dateien, bevor sie an den Server gesendet werden. Dieser Befehl erstellt automatisch die Benutzer-ID mit Administratorberechtigung `JOEOS2` mit dem Kennwort *SECRETCODE*. Außerdem verfügt der Administrator jetzt über die Clienteignerberechtigung für den Knoten `JOEOS2`.

```
register node joeos2 secretcode domain=dom1
 archdelete=yes backdelete=yes
 compression=yes
```

Beispiel: Einem vorhandenen Benutzer mit Verwaltungsaufgaben die Clienteignerberechtigung erteilen

Der vorhandenen Benutzer-ID mit Administratorberechtigung *HELPADMIN* die Clienteignerberechtigung erteilen, wenn der Clientknoten `JAN` registriert wird. Dieser Schritt würde nicht automatisch die Administrator-ID `JAN` erstellen, sondern dem Administrator *HELPADMIN* die Clienteignerberechtigung für diesen Knoten erteilen.

```
register node jan pwdsafe userid=helpadmin
```

Beispiel: Einen NAS-Dateiserverknoten registrieren, der NDMP-Operationen verwendet

Den Knotennamen `NAS1` für einen NAS-Dateiserver registrieren, der NDMP-Operationen verwendet. Diesen Knoten einer speziellen NAS-Domäne zuordnen.

```
register node nas1 pw4pw domain=nasdom type=nas
```

Beispiel: Einen Knoten registrieren und die maximale Anzahl der Dateien pro Transaktionsfestschreibung angeben

Einen Knoten mit dem Namen `ED` registrieren und TXNGroupmax auf 1.000 setzen.

```
register node ed pw45twx txngroupmax=1000
```

Beispiel: Einen Knoten registrieren und die Datendeduplizierung auf dem Clientsystem zulassen

Einen Knoten mit dem Namen `JIM` registrieren und die Datendeduplizierung auf dem Clientsystem zulassen.

```
register node jim jim deduplication=clientorserver
```

Beispiel: Den Knoten mit dem Namen ED registrieren und die Rolle als 'Servereinheit' für die Zurückmeldung der PVU-Schätzung definieren

Den Knoten mit dem Namen `ED` registrieren und die Rolle als 'Servereinheit' für die Zurückmeldung der PVU-Schätzung definieren.

```
register node ed pw45twx roleoverride=server
```

Beispiel: Einen Knoten auf einem Quellenreplikationsserver registrieren

NODE1 für einen Quellenreplikationsserver definieren. Eine Replikationsregel für die Sicherungsdaten angeben, die zu NODE1 gehören, sodass aktive Sicherungsdaten mit einer hohen Priorität repliziert werden. Die Replikation für den Knoten aktivieren.

```
register node node1 bkreplruledefault=active_data_high_priority replstate=enabled
```

Beispiel: Einen Knoten registrieren, der mit einem LDAP-Server authentifiziert wird

Registrieren Sie einen Knoten mit dem Namen NODE17, der sich mit einem LDAP-Server authentifizieren muss.

```
register node node17 authentication=ldap
```

Tipp: Wenn Sie einen Knoten auf diese Weise registrieren, wird keine Benutzer-ID mit Administratorberechtigung erstellt.

Beispiel: Knoten für die Kommunikation mit einem Server unter Verwendung der Sitzungssicherheit 'strict' registrieren

Einen Knoten mit dem Namen NODE4 registrieren, um die striktesten Sicherheitseinstellungen für die Authentifizierung mit dem Server zu verwenden.

```
register node node4 sessionsecurity=strict
```

Beispiel: Einen Knoten registrieren und die Wiederherstellung beschädigter Dateien aktivieren

Den Knotennamen PAYROLL registrieren. Für den Knoten PAYROLL die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver aktivieren.

```
register node payroll recoverdamaged=yes
```

Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für REGISTER NODE

Befehl	Beschreibung
DEFINE ASSOCIATION	Ordnet Clients einem Zeitplan zu.
DEFINE DATAMOVER	Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.
DEFINE MACHNODEASSOCIATION	Ordnet einen IBM Spectrum Protect-Knoten einer Maschine zu.
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
LOCK NODE	Verhindert, dass ein Client auf den Server zugreift.
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY PVUESTIMATE	Zeigt eine Schätzung der Clienteinheiten und Servereinheiten an, die verwaltet werden.
QUERY REPLNODE	Zeigt Informationen zum Replikationsstatus eines Clientknotens an.
REGISTER ADMIN	Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
REMOVE REPLNODE	Entfernt einen Knoten aus der Replikation.
RENAME NODE	Ändert den Namen eines Clientknotens.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
RESET PASSEXP	Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.
SET DEFAULTAUTHENTICATION	Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an.
SET PASSEXP	Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.
SET CPUINFOREFRESH	Gibt die Anzahl der Tage zwischen Clientsuchläufen nach Workstationinformationen an, die für PVU-Schätzungen verwendet werden.

Befehl	Beschreibung
SET DEDUPVERIFICATIONLEVEL	Gibt den Prozentsatz der Bereiche an, die vom Server während der clientseitigen Deduplizierung geprüft werden sollen.
SET REPLRECOVERDAMAGED	Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.
UNLOCK NODE	Ermöglicht einem gesperrten Benutzer in einer bestimmten Maßnahmendomäne wieder den Zugriff auf den Server.
UPDATE ADMIN	Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.
UPDATE FILESPACE	Ändert Knotenreplikationsregeln für Dateibereiche.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

Zugehörige Konzepte:
Tasks für Rootbenutzer und berechtigte Benutzer des UNIX- und Linux-Clients
Zugehörige Informationen:
Ssl (Clientoption)

REMOVE-Befehle

Mit den REMOVE-Befehlen kann ein Objekt aus IBM Spectrum Protect entfernt werden.

- REMOVE ADMIN (Benutzer-ID mit Administratorberechtigung löschen)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeREMOVE DAMAGED (Beschädigte Daten aus einem Quellenspeicherpool entfernen)
- REMOVE NODE (Knoten oder zugehörigen Maschinenknoten löschen)
- REMOVE REPLNODE (Clientknoten aus Replikation entfernen)
- REMOVE REPLSERVER (Replikationsserver entfernen)

REMOVE ADMIN (Benutzer-ID mit Administratorberechtigung löschen)

Verwenden Sie diesen Befehl, um eine Benutzer-ID mit Administratorberechtigung aus dem System zu entfernen.

Die letzte Benutzer-ID mit Systemadministratorberechtigung oder die Verwaltungs-ID SERVER_CONSOLE kann nicht aus dem System entfernt werden.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol): Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-REMove Admin--Administratorname------------------------------>

   .-SYNCldapdelete----No------.
>--+---------------------------+------------------------------><
   '-SYNCldapdelete----+-No--+-'
                       '-Yes-'
```

Parameter

Administratorname (Erforderlich)
Gibt die Benutzer-ID mit Administratorberechtigung, die entfernt werden soll.
SYNCldapdelete
Gibt an, ob die Administrator-ID auf dem LDAP-Server (LDAP = Lightweight Directory Access Protocol) gelöscht werden soll.

Yes
Die Administrator-ID wird auf dem LDAP-Server gelöscht.
Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwalten beschrieben wird.)
No

Die Administrator-ID wird auf dem LDAP-Server nicht gelöscht. Dies ist der Standardwert.

Beispiel: Eine Benutzer-ID mit Administratorberechtigung entfernen

Entfernen Sie die Benutzer-ID larry mit Administratorberechtigung, die nicht auf einem LDAP-Server definiert ist. Geben Sie den folgenden Befehl aus:

```
remove admin larry
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REMOVE ADMIN

Befehl	Beschreibung
LOCK ADMIN	Verweigert einem Administrator den Zugriff auf IBM Spectrum Protect.
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.
REGISTER ADMIN	Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.
RENAME ADMIN	Ändert den Namen eines IBM Spectrum Protect-Administrators.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

REMOVE DAMAGED (Beschädigte Daten aus einem Quellenspeicherpool entfernen)

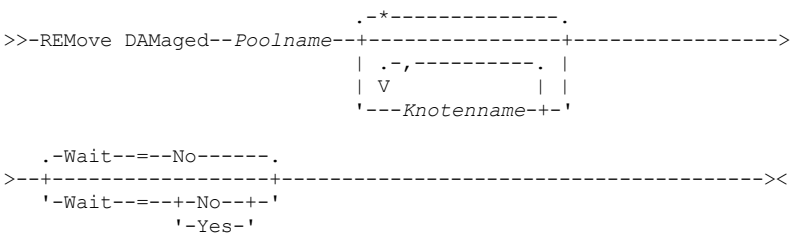
Mit diesem Befehl können Sie nach der Speicherpoolkonvertierung beschädigte Daten aus einem Speicherpool entfernen, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet.

Mit dem Befehl REMOVE DAMAGED werden beschädigte Daten permanent aus dem Speicherpool entfernt.
Tipp: Bevor Sie beschädigte Daten aus dem Speicherpool entfernen, versuchen Sie, eine unbeschädigte Version der Daten aus einem Kopienspeicherpool oder Speicherpool für aktive Daten wiederherzustellen, indem Sie den Befehl RESTORE STGPOOL ausgeben. Sie können eine unbeschädigte Version der Daten von einem Zielreplikationsserver wiederherstellen, indem Sie den Befehl REPLICATE NODE ausgeben und den Parameter RECOVERDAMAGED=YES angeben.

Berechtigungsklasse

Für diesen Befehl ist die eingeschränkte Speicherberechtigung erforderlich.

Syntax



Parameter

Poolname (Erforderlich)
: Geben Sie einen primären Speicherpool an, der eine Einheitenklasse FILE, eine Bandeinheitenklasse oder ein virtuelles Bandarchiv (VTL = Virtual Tape Library) verwendet. Der Speicherpool enthält die beschädigten Daten. Dieser Parameter ist erforderlich.

Knotenname
: Gibt den Namen des Clientknotens an. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Sie können ein Platzhalterzeichen anstelle eines Knotennamens verwenden, wenn beschädigte Daten auf allen Knoten in dem Speicherpool entfernt werden sollen.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server beschädigte Daten aus dem Speicherpool entfernt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können diesen Parameter nur in einer Verwaltungsbefehlszeile angeben. Sie können einen der folgenden Werte angeben:

  No

Gibt an, dass die Befehlsprozesse im Hintergrund ausgeführt werden.

Yes

Gibt an, dass die Befehlsprozesse im Vordergrund ausgeführt werden. Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist.

Beispiel: Beschädigte Daten aus einem Speicherpool entfernen und darauf warten, dass der Server die Verarbeitung beendet

Beschädigte Daten aus einem Speicherpool mit dem Namen POOL1 entfernen und darauf warten, dass der Server die Verarbeitung im Vordergrund beendet.

```
remove damaged pool1 wait=yes
```

Tabelle 1. Zugehörige Befehle für REMOVE DAMAGED

Befehl	Beschreibung
CONVERT STGPOOL	Konvertiert einen Speicherpool in einen Verzeichniscontainerspeicherpool.
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.
REPAIR STGPOOL	Repariert einen Verzeichniscontainerspeicherpool.

REMOVE NODE (Knoten oder zugehörigen Maschinenknoten löschen)

Verwenden Sie diesen Befehl, um einen Knoten von dem Server zu entfernen. Wenn Sie Disaster Recovery Manager verwenden und der zu löschende Knoten einer Maschine zugeordnet ist, wird auch die Zuordnung zwischen dem Knoten und der Maschine gelöscht.

Ist ein Knoten Teil einer Kollokationsgruppe und wird der Knoten von dem Server entfernt, wird der Knoten aus der Kollokationsgruppe entfernt. Wird ein Knoten entfernt und enthielt der Knoten Dateibereiche in einer Dateibereichskollokationsgruppe, werden diese Dateibereiche aus der Liste der Gruppenmitglieder entfernt.

Wenn Sie einen Knoten entfernen, der Daten in einem deduplizierten Speicherpool gespeichert hat, wird der Knotenname DELETED in der Ausgabe des Befehls QUERY OCCUPANCY angezeigt, bis alle Datendeduplizierungsabhängigkeiten entfernt wurden.

Wenn ein Knoten entfernt wird, wird die entsprechende Verwaltungs-ID nur entfernt, wenn die folgenden Bedingungen zutreffen:

- Der Administratorname stimmt mit dem Knotennamen überein.
- Der Administrator hat Clienteigner- oder Clientzugriffsberechtigung *nur* für den Knoten, der entfernt wird.
- Der Administrator ist kein verwaltetes Objekt.

Bevor ein Knoten entfernt werden kann, müssen alle zu diesem Knoten gehörigen Bereiche für Archivierungs- und Sicherungsdateien gelöscht werden.
Bevor ein NAS-Knoten entfernt werden kann, der über eine entsprechende Einheit zum Versetzen von Daten verfügt, müssen Sie die folgenden Tasks in dieser Reihenfolge ausführen:

1. Alle Pfade von der Einheit zum Versetzen von Daten löschen
2. Die Einheit zum Versetzen von Daten löschen
3. Alle Definitionen des virtuellen Dateibereichs für den Knoten löschen
4. Den NAS-Knoten entfernen

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol): Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

Syntax

```
                            .-SYNCldapdelete--=--No------.
>>-REMove Node--Knotenname--+----------------------------+-----><
                            '-SYNCldapdelete--=--+-No--+-'
                                                 '-Yes-'
```

Parameter

Knotenname (Erforderlich)
Gibt den Namen des zu löschenden Knotens an.
SYNCldapdelete
Gibt an, ob der Knoten auf dem LDAP-Server (LDAP = Lightweight Directory Access Protocol) entfernt werden soll.

Yes
Gibt an, dass der Knoten entfernt wird.
Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwalten beschrieben wird.)
No
Gibt an, dass der Knoten nicht entfernt wird. Dies ist der Standardwert.

Beispiel: Einen Clientknoten entfernen

Den Clientknoten LARRY entfernen.

```
remove node larry
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REMOVE NODE

Befehl	Beschreibung
AIX-BetriebssystemeWindows-BetriebssystemeDELETE MACHNODEASSOCIATION	AIX-BetriebssystemeWindows-BetriebssystemeLöscht die Zuordnung zwischen einer Maschine und einem Knoten.
DELETE DATAMOVER	Löscht eine Einheit zum Versetzen von Daten.
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
DELETE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs löschen.
LOCK NODE	Verhindert, dass ein Client auf den Server zugreift.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
AIX-BetriebssystemeWindows-BetriebssystemeQUERY MACHINE	AIX-BetriebssystemeWindows-BetriebssystemeZeigt Informationen über Maschinen an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY SESSION	Zeigt Informationen zu allen aktiven Administrator- und Clientsitzungen mit IBM Spectrum Protect an.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
RENAME NODE	Ändert den Namen eines Clientknotens.

REMOVE REPLNODE (Clientknoten aus Replikation entfernen)

Verwenden Sie diesen Befehl, um einen Knoten aus der Replikation zu entfernen, wenn die Daten, die zu dem Knoten gehören, nicht mehr repliziert werden sollen.

Sie können keine Clientknotendaten löschen, indem Sie den Befehl REMOVE REPLNODE ausgeben. Sie können den Befehl auf einem Quellen- oder einem Zielreplikationsserver ausgeben. Sie können diesen Befehl nur über einen Verwaltungsbefehlszeilenclient ausgeben. Dieser Befehl kann nicht über die Server-Konsole ausgegeben werden.

Wird der Befehl REMOVE REPLNODE für einen Clientknoten ausgegeben, dessen Replikationsmodus auf SEND oder RECEIVE gesetzt ist, wird der Modus auf NONE gesetzt. Der Replikationsstatus wird ebenfalls auf NONE gesetzt. Nach dem Entfernen eines Clientknotens aus der Replikation kann der Zielreplikationsserver Sicherungsdaten, Archivierungsdaten und speicherverwaltete Daten direkt vom Knoten akzeptieren.

Wenn ein Clientknoten aus der Replikation entfernt wird, werden Informationen in der Datenbank zur Replikation für den Knoten gelöscht. Wenn der Clientknoten später für die Replikation aktiviert wird, repliziert der Replikationsprozess alle Daten, die durch Replikationsregeln und Einstellungen angegeben sind.

Wenn Sie den Befehl REMOVE REPLNODE ausgeben, werden die Daten, die zu einem Clientknoten gehören, nicht gelöscht. Sollen Dateibereichsdaten gelöscht werden, die zu dem Clientknoten gehören, geben Sie den Befehl DELETE FILESPACE für jeden Dateibereich aus, der zu dem Knoten gehört. Soll die Clientknotendefinition nicht aufbewahrt werden, geben Sie den Befehl REMOVE NODE aus. Sollen

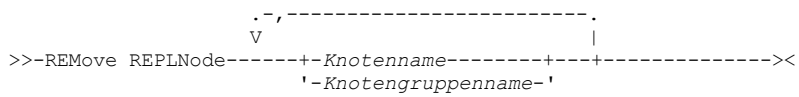
Dateibereichsdaten und die Clientknotendefinition gelöscht werden, geben Sie DELETE FILESPACE und REMOVE NODE auf dem Zielreplikationsserver aus.

Einschränkung: Wenn ein Knotenreplikationsprozess für einen mit diesem Befehl angegebenen Clientknoten aktiv ist, schlägt der Befehl fehl und die Replikationsinformationen für den Knoten werden nicht entfernt.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

Syntax



Parameter

Knotenname oder Knotengruppenname (Erforderlich)
: Gibt den Namen des Clientknotens oder der definierten Gruppe von Clientknoten an, der bzw. die aus der Replikation entfernt werden soll. Sollen mehrere Clientknotennamen und Clientknotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen verwenden, um Clientknotennamen anzugeben, aber Sie können keine Platzhalterzeichen verwenden, um Clientknotengruppennamen anzugeben. Sie können Knoten- oder Knotengruppennamen nicht mit dem Domänennamen kombinieren.

Beispiel: Drei Clientknoten und eine Clientknotengruppe aus der Replikation entfernen

Die Namen der Clientknoten sind NODE1, NODE2 und NODE3. Der Name der Clientknotengruppe lautet PAYROLL. Geben Sie den folgenden Befehl auf dem Quellen- und Zielreplikationsserver aus:

```
remove replnode node*,payroll
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REMOVE REPLNODE

Befehl	Beschreibung
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.

REMOVE REPLSERVER (Replikationsserver entfernen)

Verwenden Sie diesen Befehl, um einen Replikationsserver aus der Liste der Replikationsserver zu entfernen oder zu einem Replikationsserver in der Liste der Replikationsserver zu wechseln. Mit diesem Befehl werden alle Informationen zum Replikationsstatus für alle Knoten gelöscht, die auf diesen Server repliziert wurden.

Sie können den Befehl auf einem Quellen- oder einem Zielreplikationsserver ausgeben.
Einschränkung: Sie können keine Clientknotendaten mit dem Befehl REMOVE REPLSERVER löschen.

Verwenden Sie den Befehl, um zwischen Replikationsservern zu wechseln und Replikationsinformationen für einen alten Server zu entfernen. Der Befehl hat keine Auswirkungen auf den aktuellen Replikationsmodus oder -status von Knotendefinitionen. Geben Sie den Befehl sowohl auf dem Quellenserver als auch auf dem Zielserver aus, damit die Informationen zum Replikationsstatus für beide Server konsistent bleiben.

Einschränkung: Wenn Sie den Standardreplikationsserver für den Befehl REMOVE REPLSERVER angeben und ein Knotenreplikationsprozess aktiv ist, schlägt der Befehl fehl und es werden keine Replikationsinformationen entfernt.

Dieser Befehl wird als Hintergrundoperation ausgeführt und kann nicht abgebrochen werden. IBM Spectrum Protect löscht Replikationsinformationen, die dem angegebenen Server zugeordnet sind, als Serie von Stapeldatenbanktransaktionen. Wenn ein Systemfehler auftritt, kann ein partielles Löschen erfolgen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-REMove REPLServer--GUID-------------------------------------><
```

Parameter

Replikations-GUID (Erforderlich)

Die eindeutige ID für den Replikationsserver, der entfernt wird. Sie können Platzhalterzeichen verwenden, um die global eindeutige ID (GUID) für die Replikation anzugeben, es kann jedoch nur eine einzige GUID mit dem Platzhalterzeichen übereinstimmen. Wenn die Platzhalterzeichenfolge mehreren GUIDs entspricht, schlägt der Befehl fehl. Sie müssen die Platzhalterzeichenfolge qualifizieren, damit nur die zu löschende GUID gefunden wird.

Beispiel: Ein Platzhalterzeichen verwenden, um einen Replikationsserver zu entfernen

Entfernen Sie einen Replikationsserver, indem Sie ein Platzhalterzeichen zur Angabe der GUID verwenden.

```
remove replserver e*
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REMOVE REPLSERVER

Befehl	Beschreibung
REMOVE REPLNODE (Clientknoten aus Replikation entfernen)	Entfernt einen Knoten aus der Replikation.
QUERY REPLSERVER (Replikationsserver abfragen)	Zeigt Informationen zu Replikationsservern an.

RENAME-Befehle

Mit den RENAME-Befehlen kann der Name eines vorhandenen Objekts geändert werden.

- RENAME ADMIN (Administrator umbenennen)
- RENAME FILESPACE (Clientdateibereich auf dem Server umbenennen)
- RENAME NODE (Knoten umbenennen)
- RENAME SCRIPT (IBM Spectrum Protect-Prozedur umbenennen)
- RENAME SERVERGROUP (Servergruppe umbenennen)
- RENAME STGPOOL (Den Namen eines Speicherpools ändern)

RENAME ADMIN (Administrator umbenennen)

Verwenden Sie diesen Befehl, um eine Benutzer-ID mit Administratorberechtigung zu ändern. Bestehende Informationen zu diesem Administrator, zum Beispiel Kennwort, Kontaktinformationen und Berechtigungsklassen, werden nicht geändert.

Wenn Sie eine bestehende Administrator-ID einer anderen Person zuordnen, verwenden Sie den Befehl UPDATE ADMIN, um das Kennwort zu ändern.

Wenn ein Administrator und ein Knoten einen Namen gemeinsam nutzen und die Authentifizierungsmethode des Administrators geändert wird, ändert sich auch die Knotenauthentifizierungsmethode. Wenn Sie einen Administrator in den Namen eines vorhandenen Knotens umbenennen, können sich die Authentifizierungsmethode und die Einstellung für SSLREQUIRED für den Knoten ändern. Sind diese Einstellungen unterschiedlich, haben der Administrator und der Knoten nach dem Umbenennen dieselbe Authentifizierungsmethode und dieselbe Einstellung für SSLREQUIRED.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
- Benennen Sie keine Benutzer-ID mit Administratorberechtigung so um, dass sie mit einem Knotennamen identisch ist. Wenn die Namen übereinstimmen, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierung fehlschlägt.

Die Verwaltungs-ID SERVER_CONSOLE kann nicht umbenannt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-REName Admin--aktueller_Administratorname--neuer_Administratorname-->

   .-SYNCldapdelete--=--No------.
>--+----------------------------+-----------------------------><
   '-SYNCldapdelete--=--+-No--+-'
                        '-Yes-'
```

Parameter

aktueller_Administratorname (Erforderlich)
: Gibt die Benutzer-ID mit Administratorberechtigung, die umbenannt werden soll.

neuer_Administratorname (Erforderlich)
: Gibt die neue Benutzer-ID mit Administratorberechtigung an. Die maximale Länge des Namens beträgt 64 Zeichen.

SYNCldapdelete
: Gibt an, ob die Administrator-ID auf dem LDAP-Server (LDAP = Lightweight Directory Access Protocol) gelöscht und die ID durch eine neue ID ersetzt werden soll.

  Yes
  : Die Administrator-ID wird auf dem LDAP-Server gelöscht und durch eine neue ID ersetzt.
    Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwalten beschrieben wird.)

  No
  : Die Administrator-ID wird auf dem LDAP-Server nicht gelöscht und ersetzt. Dies ist der Standardwert.

Beispiel: Einen Administrator umbenennen

Den IBM Spectrum Protect-Administrator CLAUDIA in BILL umbenennen.

```
rename admin claudia bill
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RENAME ADMIN

Befehl	Beschreibung
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.
UPDATE ADMIN	Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.

RENAME FILESPACE (Clientdateibereich auf dem Server umbenennen)

Mit diesem Befehl können vorhandene Clientdateibereiche auf dem Server oder importierte Dateibereiche umbenannt werden.

Möglicherweise möchten Sie einen Dateibereich umbenennen, der importiert wurde, oder die Erstellung neuer Unicode-fähiger Dateibereiche für Unicode-fähige Clients veranlassen.

Einschränkung: Benennen Sie keine NAS- oder VMware-Dateibereiche um. Wenn Sie einen NAS- oder VMware-Dateibereich umbenennen, ist er nicht mehr sichtbar und kann nicht zurückgeschrieben werden. Um einen umbenannten NAS- oder VMware-Dateibereich zurückzuschreiben, müssen Sie den Dateibereich in seinen ursprünglichen Namen umbenennen und den Parameter 'force' wie folgt definieren: force=yes

Berechtigungsklasse

Jeder Administrator mit uneingeschränkter Maßnahmenberechtigung oder eingeschränkter Maßnahmenberechtigung für die Maßnahmendomäne des Clients kann diesen Befehl ausgeben.

Syntax

```
>>-REName FIlespace--Knotenname---------------------------------->

>--aktueller_Dateibereichsname--neuer_Dateibereichsname--------->

   .-NAMEType--=--SERVER------.
```

```
>--+-------------------------+--------------------------------->
   '-NAMEType--=--+-SERVER--+-'
                  +-UNIcode-+
                  '-FSID----'

   .-NEWNAMEType--=--SERVER----------.
>--+-------------------------------+--+---------------+------><
   |                           (1)   |  '-force--=--yes-'
   '-NEWNAMEType--=--+-UNIcode-----+-'
                     '-HEXadecimal-'
```

Anmerkungen:

1. Dieser Parameter ist der Standardwert, wenn NAMEType=UNIcode angegeben wird.

Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, zu dem der umzubenennende Dateibereich gehört.

aktueller_Dateibereichsname (Erforderlich)
: Gibt den Namen des Dateibereichs an, der umbenannt werden soll. Bei einem Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden, und der Name muss genau so angegeben werden, wie er für den Server definiert ist. Namen für die Zuordnung virtueller Dateibereiche sind zulässig.

neuer_Dateibereichsname (Erforderlich)
: Gibt den neuen Namen für den Dateibereich an. Bei einem Clientdateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden, und der Name muss genau so angegeben werden, wie er für den Server definiert werden soll. Bei diesem Parameter kann es sich nicht um einen vorhandenen Namen für die Zuordnung eines virtuellen Dateibereichs handeln. Ist der aktuelle_Dateibereichsname ein virtueller Dateibereich, muss der neue_Dateibereichsname allen Regeln zum Definieren eines virtuellen Dateibereichsnamens entsprechen. Für weitere Informationen siehe Befehl DEFINE VIRTUALFSMAPPING.
  Wichtig: Ist der Typ des neuen Namens ein hexadezimaler Typ, geben Sie gültige UTF-8-Hexadezimalwerte an, damit die Zeichenumsetztabelle des Servers den Dateibereichsnamen wie gewünscht anzeigt. Geben Sie beispielsweise keinen Wert an, der als Rücksetzzeichen interpretiert werden kann.
  Wenn Sie einen Dateibereich umbenennen, der Teil einer Dateibereichskollokationsgruppe ist, wird die Kollokationsgruppe mit dem neuen Namen aktualisiert.

NAMEType
: Geben Sie an, wie der Server den aktuellen Dateibereichsnamen interpretieren soll, den Sie eingeben. Dieser Parameter ist nützlich, wenn der Server über Clients mit Unterstützung für Unicode verfügt. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients mit den Betriebssystemen Windows, Macintosh OS X und NetWare verwenden.

  Der Standardwert lautet SERVER. Wird ein Name für die Zuordnung eines virtuellen Dateibereichs angegeben, müssen Sie SERVER verwenden. Gültige Werte:

  SERVER
  : Der Server verwendet die Zeichenumsetztabelle des Servers, um den Dateibereichsnamen zu interpretieren.

  UNIcode
  : Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

  FSID
  : Der Server interpretiert den Dateibereichsnamen als Dateibereichs-ID (FSID).

NEWNAMEType
: Angeben, wie der Server den neuen Dateibereichsnamen interpretieren soll, den Sie eingeben. Der Standardwert lautet SERVER, wenn Sie für NAMETYPE SERVER angegeben haben oder wenn der Dateibereich, der umbenannt werden soll, nicht Unicode ist. Der Standardwert lautet UNICODE, wenn Sie für NAMETYPE UNICODE angegeben haben oder wenn der Dateibereich, der umbenannt werden soll, Unicode ist. Wird ein Name für die Zuordnung eines virtuellen Dateibereichs angegeben, müssen Sie SERVER verwenden. Gültige Werte:

  SERVER
  : Der Server verwendet die Zeichenumsetztabelle des Servers, um den Dateibereichsnamen zu interpretieren.

  UNIcode
  : Der Server konvertiert den eingegebenen Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den tatsächlichen Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Ist die Konvertierung nicht erfolgreich, möchten Sie möglicherweise den Parameter HEXADECIMAL angeben.

  HEXadecimal
  : Der Server interpretiert den Dateibereichsnamen, den Sie eingeben, als hexadezimale Darstellung eines Namens in Unicode. Durch die Verwendung der hexadezimalen Darstellung wird sichergestellt, dass der Server den Dateibereich unabhängig von der Zeichenumsetztabelle des Servers korrekt umbenennen kann.
    Soll die hexadezimale Darstellung eines Dateibereichsnamens angezeigt werden, können Sie den Befehl QUERY FILESPACE mit FORMAT=DETAILED verwenden.

Einschränkung: Sie können nicht einen neuen Namen mit einer Art, die von der Art des ursprünglichen Namens abweicht, angeben. Sie können den Namen eines Dateibereichs, der in Unicode ist, in einen anderen Namen in Unicode umbenennen. Sie können einen Dateibereich, der nicht in Unicode ist, umbenennen und einen neuen Namen in der Zeichenumsetztabelle des Servers verwenden. Die beiden Arten können jedoch nicht gemischt werden.

force
Um einen NAS- oder VMware-Dateibereich umzubenennen, müssen Sie diesen Parameter wie folgt definieren: force=yes

Einen importierten Dateibereich umbenennen, um ein Überschreiben zu verhindern

Der AIX-Clientknoten LARRY hat den Dateibereich /r033 auf dem IBM Spectrum Protect-Server gesichert. Der Dateibereich wurde auf Band exportiert und später wieder auf den Server importiert. Beim Importieren dieses Dateibereichs wurde der vom System generierte Name /r031 für den importierten Dateibereich erstellt, da der Name /r033 für den Clientknoten LARRY vorhanden war.

Der Clientknoten LARRY verfügte jedoch bereits über einen Dateibereich mit dem Namen /r031, der nicht gesichert wurde und daher dem Server unbekannt war. Wird der importierte Dateibereich nicht umbenannt, überschreibt er den Dateibereich /r031, da der von der Funktion IMPORT generierte Dateibereichsname mit dem Namen eines Dateibereichs auf Clientknoten LARRY übereinstimmt, der dem Server nicht bekannt ist.

Verwenden Sie den folgenden Befehl, um den importierten Dateibereich /r031 umzubenennen. Der neue Name /imported-r033 gibt an, dass der neue Dateibereich ein importiertes Abbild des Dateibereichs /r033 ist.

```
rename filespace larry /r031 /imported-r033
```

Dateibereich umbenennen, um einen Unicode-fähigen Dateibereich zu erstellen

Client JOE verwendet einen deutschen Unicode-aktivierten IBM Spectrum Protect-Client. JOE hat mehrere große Dateibereiche, die nicht Unicode-fähig sind, im Serverspeicher gesichert. Dateibereich \\joe\c$ enthält einige Dateien mit japanischen Dateinamen, die nicht in einem Dateibereich gesichert werden können, der nicht Unicode-fähig ist. Da die Dateibereiche groß sind, möchte der Administrator jetzt nicht alle Dateibereiche von JOE in Unicode-fähige Dateibereiche konvertieren. Der Administrator möchte nur den Nicht-Unicode-Dateibereich \\joe\c$ umbenennen, so dass bei der nächsten Sicherung des Dateibereichs ein neuer Unicode-fähiger Dateibereich erstellt wird. Der neue Unicode-fähige Dateibereich ermöglicht die erfolgreiche Sicherung der japanischen Dateien.

Verwenden Sie den folgenden Befehl, um \\joe\c$ umzubenennen:

```
rename filespace joe \\joe\c$ \\joe\c$_old
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RENAME FILESPACE

Befehl	Beschreibung
DEFINE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs definieren.
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY OCCUPANCY	Zeigt Dateibereichsdaten anhand des Speicherpools an.

RENAME NODE (Knoten umbenennen)

Verwenden Sie diesen Befehl, um einen Knoten umzubenennen.

Wenn Sie eine bestehende Knoten-ID einer anderen Person zuordnen, verwenden Sie den Befehl UPDATE NODE, um das Kennwort zu ändern.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
- Benennen Sie einen Knoten nicht so um, dass er mit einer vorhandenen Benutzer-ID mit Administratorberechtigung übereinstimmt. Wenn Sie einen Knoten umbenennen und der Knotenname mit einer Benutzer-ID mit Administratorberechtigung übereinstimmt, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierung fehlschlägt.

Einschränkungen:

- Ein NAS-Knoten, für den eine entsprechende Einheit zum Versetzen von Daten definiert ist, kann nicht umbenannt werden. Verfügt die Einheit zum Versetzen von Daten über definierte Pfade, müssen die Pfade zuerst gelöscht werden.
- Wenn ein Knoten für die Replikation konfiguriert ist, kann er nicht umbenannt werden.

Wenn Sie einen Knoten in den Namen eines vorhandenen Administrators umbenennen, werden die Authentifizierungsmethode des Administrators und die Einstellung für SSLREQUIRED aktualisiert, damit sie mit dem Knoten übereinstimmen. Wenn ein Knoten und ein Administrator einen Namen gemeinsam nutzen und die Knotenauthentifizierungsmethode oder die Einstellung für SSLREQUIRED des Knotens geändert wird, werden die Administratoreinstellungen ebenfalls geändert. Sie müssen über die Berechtigung auf Systemebene verfügen, um die Knotenauthentifizierungsmethode oder die Einstellung für SSLREQUIRED des Knotens und einen Administrator mit demselben Namen zu aktualisieren.

Berechtigungsklasse

Sie müssen über Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne verfügen, der der Clientknoten zugeordnet ist.

Syntax

```
>>-REName Node--aktueller_Knotenname--neuer_Knotenname---------->

   .-SYNCldapdelete--=--No------.
>--+----------------------------+------------------------------><
   '-SYNCldapdelete--=--+-No--+-'
                        '-Yes-'
```

Parameter

aktueller_Knotenname (Erforderlich)
: Gibt den Namen des Knotens an, der umbenannt werden soll.

neuer_Knotenname (Erforderlich)
: Gibt den neuen Namen des Knotens an. Die maximale Länge beträgt 64 Zeichen.

SYNCldapdelete
: Gibt an, ob der Knotenname auf dem LDAP-Server (LDAP = Lightweight Directory Access Protocol) gelöscht und ersetzt wird.

  Yes
  : Gibt an, dass der Knotenname gelöscht und ersetzt wird.
    Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwalten beschrieben wird.)

  No
  : Gibt an, dass der Knotenname nicht gelöscht und ersetzt wird. Dies ist der Standardwert.

Beispiel: Einen Knoten umbenennen

Den Knoten JOE in JOYCE umbenennen.

```
rename node joe joyce
```

Beispiel: Einen Knoten umbenennen, der einen Namensbereich mit anderen Servern gemeinsam nutzt

Benennen Sie den Knoten JOYCE in JOE um und löschen Sie den vorherigen Namen auf den entsprechenden LDAP-Servern nicht.

```
rename node joyce joe
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RENAME NODE

Befehl	Beschreibung
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

Zugehörige Tasks:
NAS-Dateiserverknoten verwalten

RENAME SCRIPT (IBM Spectrum Protect-Prozedur umbenennen)

Mit diesem Befehl kann eine IBM Spectrum Protect-Prozedur umbenannt werden.

Berechtigungsklasse

Für diesen Befehl ist die Bediener-, Maßnahmen-, System- oder Speicherberechtigung erforderlich.

Syntax

```
>>-REName SCRipt--aktueller_Prozedurname--neuer_Prozedurname--->><
```

Parameter

aktueller_Prozedurname (Erforderlich)
: Gibt den Namen der Prozedur an, die umbenannt werden soll.

neuer_Prozedurname (Erforderlich)
: Gibt den neuen Namen für die Prozedur an. Der Name kann bis zu 30 Zeichen umfassen.

Beispiel: Ein Script umbenennen

SCRIPT1 in die neue Prozedur SCRIPT2 umbenennen.

```
rename script script1 script2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RENAME SCRIPT

Befehl	Beschreibung
COPY SCRIPT	Erstellt eine Kopie einer Prozedur.
DEFINE SCRIPT	Definiert eine Prozedur für den IBM Spectrum Protect-Server.
DELETE SCRIPT	Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur.
QUERY SCRIPT	Zeigt Informationen über Prozeduren an.
RUN	Führt ein Script aus.
UPDATE SCRIPT	Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.

RENAME SERVERGROUP (Servergruppe umbenennen)

Mit diesem Befehl kann eine Server-Gruppe umbenannt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-REName SERVERGroup--aktueller_Gruppenname--neuer_Gruppenname->><
```

Parameter

aktueller_Gruppenname (Erforderlich)
: Gibt die Server-Gruppe an, die umbenannt werden soll.

neuer_Gruppenname (Erforderlich)
: Gibt den neuen Namen der Server-Gruppe an. Die maximale Länge des Namens beträgt 64 Zeichen.

Beispiel: Eine Servergruppe umbenennen

Die Server-Gruppe WEST_COMPLEX in BIG_WEST umbenennen.

```
rename servergroup west_complex big_west
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RENAME SERVERGROUP

Befehl	Beschreibung
COPY SERVERGROUP	Erstellt eine Kopie einer Servergruppe.
DEFINE SERVERGROUP	Definiert eine neue Servergruppe.
DELETE SERVERGROUP	Löscht eine Servergruppe.
QUERY SERVERGROUP	Zeigt Informationen über Servergruppen an.
UPDATE SERVERGROUP	Aktualisiert eine Servergruppe.

RENAME STGPOOL (Den Namen eines Speicherpools ändern)

Mit diesem Befehl kann der Name eines Speicherpools geändert werden. Sie können Speicherpoolnamen ändern, um dieselben Namen auf einem Konfigurationsmanager und seinen verwalteten Servern zu verwenden.

Wenn Sie einen Speicherpool umbenennen, behalten alle Administratoren mit eingeschränkter Speicherberechtigung für den alten Speicherpool automatisch die eingeschränkte Speicherberechtigung für den umbenannten Speicherpool. Befindet sich der umbenannte Speicherpool in einer Speicherpoolhierarchie, wird die Hierarchie beibehalten. Sie müssen die Verwaltungsklasse oder Kopiengruppe aktualisieren, um den neuen Speicherpoolnamen als Ziel für Dateien anzugeben.

Sind Prozesse aktiv, wenn ein Speicherpool umbenannt wird, wird der alte Name möglicherweise noch in Nachrichten oder Abfragen für diese Prozesse angezeigt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-REName STGpool--aktueller_Poolname--neuer_Poolname---------><
```

Parameter

aktueller_Poolname (Erforderlich)
: Gibt den Speicherpool an, der umbenannt werden soll.

neuer_Poolname (Erforderlich)
: Gibt den neuen Namen des Speicherpools an. Die maximale Länge des Namens beträgt 30 Zeichen.

Beispiel: Den Namen eines Speicherpools ändern

Speicherpool STGPOOLA umbenennen in STGPOOLB:

```
rename stgpool stgpoola stgpoolb
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RENAME STGPOOL

Befehl	Beschreibung
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE STGPOOL	Löscht einen Speicherpool aus dem Serverspeicher.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
RESTORE STGPOOL	Schreibt Dateien aus Kopienspeicherpools in einen primären Speicherpool zurück.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

REPAIR STGPOOL (Verzeichniscontainerspeicherpool reparieren)

Mit diesem Befehl können deduplizierte Speicherbereiche in einem Verzeichniscontainerspeicherpool repariert werden. Beschädigte deduplizierte Speicherbereiche werden mit Bereichen repariert, die auf dem Zielreplikationsserver oder in Containerkopienspeicherpools auf demselben Server gesichert werden.

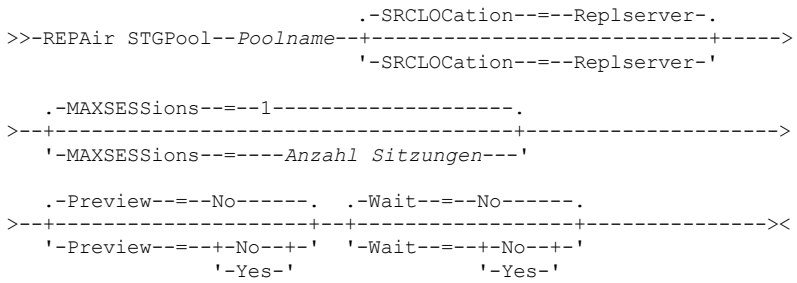
Einschränkungen:

- Sie können den Befehl REPAIR STGPOOL nur ausgeben, wenn Sie bereits den Befehl PROTECT STGPOOL ausgegeben haben, um Daten in einem anderen Speicherpool auf einem Zielreplikationsserver oder auf demselben Server zu sichern.
- Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe des Replikationsservers reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:
  - Der Zielserver ist nicht verfügbar.
  - Der Zielspeicherpool ist beschädigt.
  - Ein Netzausfall tritt auf.
- Wenn Sie einen Verzeichniscontainerspeicherpool mithilfe von Containerkopienpools reparieren, schlägt der Befehl REPAIR STGPOOL fehl, wenn eine der folgenden Bedingungen auftritt:
  - Der Containerkopienspeicherpool ist nicht verfügbar.
  - Der Containerkopienspeicherpool ist beschädigt.

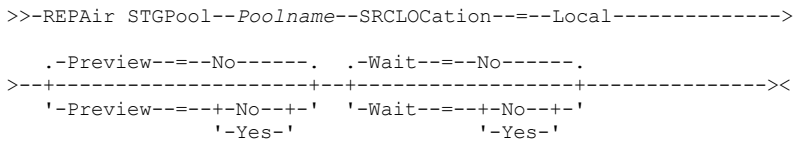
Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax, wenn die Quelle der Replikationsserver ist



Syntax, wenn die Quelle ein Speicherpool auf demselben Server ist



Parameter

Poolname (Erforderlich)
: Gibt den Namen des Verzeichniscontainerspeicherpools an, der die Daten enthält, die repariert werden müssen.

SRCLOCation
: Gibt die Quellenposition an, die verwendet wird, um die Daten zu reparieren. Der Standardwert ist REPLSERVER. Dieser Parameter ist nur erforderlich, wenn sich die Quellenposition auf demselben Server befindet. Sie können einen der folgenden Werte angeben:

  Local
  : Gibt an, dass die Daten mithilfe von Containerkopienspeicherpools auf demselben Server repariert werden.

  Replserver
  : Gibt an, dass die Daten mithilfe eines Verzeichniscontainerspeicherpools auf dem Zielreplikationsserver repariert werden.

MAXSESSions
: Gibt die maximale Anzahl der Datensitzungen an, die Daten an einen Zielserver senden können. Dieser Parameter ist wahlfrei, wenn Sie Daten mithilfe eines Replikationsservers reparieren.
Der angegebene Wert kann im Bereich 1 - 20 liegen. Der Standardwert ist 1. Wenn Sie die Anzahl der Sitzungen erhöhen, können Sie den Speicherpool schneller reparieren.

  Wenn Sie einen Wert für den Parameter MAXSESSIONS definieren, stellen Sie sicher, dass die verfügbare Bandbreite und die Prozessorkapazität des Quellen- und Zielservers ausreichend sind.

  Tipps:

- Wird ein Befehl QUERY SESSION ausgegeben, kann die Gesamtzahl der Sitzungen die Anzahl der Datensitzungen überschreiten.
- Die Anzahl der Sitzungen, die für die Reparatur von Speicherpools verwendet werden, hängt vom Datenvolumen ab, das repariert wird. Wird nur ein geringes Datenvolumen repariert, wird durch die Erhöhung der Anzahl Sitzungen kein Vorteil erzielt.

Preview
: Gibt an, ob eine Voranzeige der Daten aufgerufen werden soll oder ob die Daten repariert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

  No
  : Gibt an, dass die Daten in dem Speicherpool repariert, aber nicht vorangezeigt werden.

  Yes
  : Gibt an, dass die Daten vorangezeigt, aber nicht repariert werden.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Reparaturverarbeitung für den Speicherpool beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können diesen Parameter nur in einer Verwaltungsbefehlszeile angeben. Sie können einen der folgenden Werte angeben:

  No
  : Gibt an, dass die Befehlsprozesse im Hintergrund ausgeführt werden. Um die Hintergrundverarbeitung des Befehls REPAIR STGPOOL zu überwachen, geben Sie den Befehl QUERY PROCESS aus.

  Yes
  : Gibt an, dass die Befehlsprozesse im Vordergrund ausgeführt werden. Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist.

Beispiel: Einen Speicherpool reparieren und die Daten voranzeigen

Einen Speicherpool mit dem Namen POOL1 reparieren und die Daten voranzeigen.

```
repair stgpool pool1 preview=yes
```

Beispiel: Einen Speicherpool reparieren und eine maximale Anzahl Sitzungen angeben

Einen Speicherpool mit dem Namen POOL1 reparieren und ein Maximum von 10 Sitzungen angeben.

```
repair stgpool pool1 maxsessions=10
```

Beispiel: Einen Speicherpool mit Band reparieren

Einen Speicherpool mit dem Namen POOL1 reparieren und 'Local' für die Quellenposition angeben.

```
repair stgpool pool1 SRCLOCation=local
```

Tabelle 1. Zugehörige Befehle für REPAIR STGPOOL

Befehl	Beschreibung
DEFINE STGPOOL (Verzeichniscontainer)	Definiert einen Verzeichniscontainerspeicherpool.
DEFINE STGPOOL (Containerkopie)	Definiert einen Containerkopienspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden.
DEFINE STGPOOLDIRECTORY	Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.

REPLICATE NODE (Daten in Dateibereichen replizieren, die zu einem Clientknoten gehören)

Verwenden Sie diesen Befehl, um Daten in Dateibereichen zu replizieren, die zu einem oder mehreren Clientknoten oder zu definierten Gruppen von Clientknoten gehören.

Wenn Sie diesen Befehl ausgeben, wird ein Prozess gestartet, in dem Daten, die zu den angegebenen Clientknoten gehören, gemäß Replikationsregeln repliziert werden. Dateien, die nicht mehr auf dem Quellenreplikationsserver gespeichert werden, aber auf dem Zielreplikationsserver vorhanden sind, werden während dieses Prozesses gelöscht.

Wenn ein Knotenreplikationsprozess bereits für einen mit diesem Befehl angegebenen Clientknoten ausgeführt wird, wird der Knoten übersprungen und die Replikation für andere Knoten gestartet, die für die Replikation aktiviert sind.

Nach der Beendigung des Knotenreplikationsprozesses kann ein Wiederherstellungsprozess auf dem Zielreplikationsserver gestartet werden. Dateien werden nur wiederhergestellt, wenn alle folgenden Bedingungen erfüllt sind:

- Version 7.1.1 oder höher ist auf dem Quellen- und Zielreplikationsserver installiert.
- Der Systemparameter REPLRECOVERDAMAGED ist auf ON gesetzt. Der Systemparameter kann mit dem Befehl SET REPLRECOVERDAMAGED definiert werden.
- Der Quellenserver schließt mindestens eine Datei ein, die auf dem Knoten, der repliziert wird, als beschädigt markiert ist.
- Die Knotendaten wurden repliziert, bevor die Beschädigung aufgetreten ist.

In der folgenden Tabelle wird beschrieben, wie sich Einstellungen auf die Wiederherstellung beschädigter, replizierter Dateien auswirken. Einschränkung: Sie können den Parameter REPLRECOVERDAMAGED nicht für Verzeichniscontainer- oder Cloudspeicherpools verwenden.

Tabelle 1. Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken

Einstellung für den Systemparameter REPLRECOVERDAMAGED	Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE	Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE	Ergebnis
OFF	YES, NO oder nicht angegeben	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.
OFF	ONLY	YES oder NO	Eine Fehlernachricht wird angezeigt, weil Dateien nicht wiederhergestellt werden können, wenn der Systemparameter REPLRECOVERDAMAGED auf OFF gesetzt ist.
ON	YES	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.
ON	NO	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.
ON	ONLY	YES oder NO	Beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt, aber es findet keine Standardknotenreplikation statt.
ON	Nicht angegeben	YES	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.
ON	Nicht angegeben	NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.

Tipp: Wenn der Befehl QUERY PROCESS während der Knotenreplikation ausgegeben wird, kann die Ausgabe nicht erwartete Ergebnisse für die Anzahl der abgeschlossenen Replikationen anzeigen. Der Grund liegt darin, dass zu Knotenreplikationszwecken für jeden Dateibereich angenommen wird, dass er drei logische Dateibereiche enthält:

- Einen Bereich für Sicherungsobjekte
- Einen Bereich für Archivierungsobjekte
- Einen Bereich für speicherverwaltete Objekte

Standardmäßig generiert der Befehl QUERY PROCESS Ergebnisse für jeden logischen Dateibereich. Andere Faktoren haben ebenfalls Auswirkungen auf die Ausgabe des Befehls QUERY PROCESS:

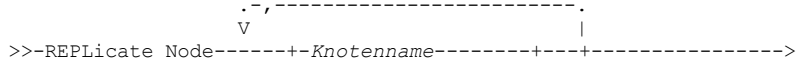
- Verfügt ein Dateibereich über eine Replikationsregel, die auf NONE gesetzt ist, wird der Dateibereich nicht in der Anzahl der Dateibereiche berücksichtigt, die verarbeitet werden.
- Wenn Sie im Befehl REPLICATE NODE Datentypen angeben, werden nur diese Datentypen in der Anzahl der Dateibereiche berücksichtigt, die verarbeitet werden, abzüglich aller Dateibereiche, die ausgeschlossen sind.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



```
                    '-Knotengruppenname-'

   .-*---------------------------------.
>--+-----------------------------------+------------------------>
   |       .-,---------------------.   |
   |  (1)  V                       |   |
   '-----+-----Dateibereichsname---+-+-'
         | .-,------------.          |
         | V        (2)   |          |
         '-----FSID-------+----------'

   .-NAMEType--=--SERVER-------.
>--+---------------------------+-------------------------------->
   '-NAMEType--=--+-SERVER---+-'
                  +-UNIcode--+
                  |      (2) |
                  '-FSID-----'

   .-CODEType--=--BOTH-----------.
>--+-----------------------------+------------------------------>
   '-CODEType--=--+-BOTH-------+-'
                  +-UNIcode----+
                  '-NONUNIcode-'

   .-DATAtype--=--ALl------------------.
>--+-----------------------------------+------------------------>
   |              .-,----------------. |
   |              V                  | |
   '-DATAtype--=----+-ALl----------+-+-'
                    +-BACKUP-------+
                    +-BACKUPActive-+
                    +-ARCHive------+
                    '-SPACEManaged-'

   .-PRIORITY--=--ALL--------.
>--+-------------------------+---------------------------------->
   '-PRIORITY--=--+-ALL----+-'
                  +-HIGH---+
                  '-NORMAL-'

   .-MAXSESSions--=--10-------------------.
>--+-----------------------------------+---------------------->
   '-MAXSESSions--=----Anzahl Sitzungen---'

   .-Preview--=--No---------------------------------.
>--+---------------------------------------------+----------->
   '-Preview--=--+-No-----------------------------+-'
                 |      .-LISTfiles--=--No------. |
                 '-Yes--+-----------------------+-'
                        '-LISTfiles--=--+-No--+-'
                                        '-Yes-'

   .-Wait--=--No------.
>--+------------------+--+-----------------------------+-------->
   '-Wait--=--+-No--+-'  '-RECOVERDamaged--=--+-Yes--+-'
              '-Yes-'                         +-No---+
                                              '-Only-'

   .-FORCEREConcile--=--No------.
>--+---------------------------+------------------------------->
   '-FORCEREConcile--=--+-No--+-'
                        '-Yes-'

   .-TRANSFERMethod--=--Tcpip--------.
>--+-------------------------------+------------------------><
   '-TRANSFERMethod--=--+-Tcpip----+-'
                        |      (3) |
                        '-Fasp-----'
```

Anmerkungen:

1. Mischen Sie nicht Dateibereichs-IDs (FSIDs) und Dateibereichsnamen in demselben Befehl.
2. Geben Sie nicht die FSID an, wenn Sie Platzhalterzeichen für den Clientknotennamen verwenden.
3. Linux-BetriebssystemeDer Parameter TRANSFERMETHOD ist nur auf Betriebssystemen Linux x86_64 verfügbar.

Parameter

Knotenname oder Knotengruppenname (Erforderlich)

Gibt den Namen des Clientknotens oder der definierten Gruppe von Clientknoten an, dessen bzw. deren Daten repliziert werden sollen. Sie können auch eine Kombination von Clientknotennamen und Clientknotengruppennamen angeben. Sollen mehrere Clientknotennamen oder Clientknotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können Platzhalterzeichen für Clientknotennamen, aber nicht für Clientknotengruppennamen verwenden. Die Replikationsregeln für alle Dateibereiche in den angegebenen Clientknoten werden überprüft.

Dateibereichsname oder FSID

Gibt den Namen des Dateibereichs oder die ID des Dateibereichs (FSID) an, der repliziert werden soll. Ein Name oder eine FSID ist optional. Wenn Sie keinen Namen oder keine FSID angeben, können alle Daten in allen Dateibereichen für die angegebenen Clientknoten für die Replikation ausgewählt werden.

Dateibereichsname

Gibt den Namen des Dateibereichs an, der zu replizierende Daten enthält. Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Um die korrekte Schreibweise für den Dateibereich zu bestimmen, geben Sie den Befehl QUERY FILESPACE aus. Mehrere Namen sind ohne Leerzeichen durch Kommas voneinander zu trennen. Wenn Sie einen Namen angeben, können Sie Platzhalterzeichen verwenden.

Ein Server, der über Clients mit Dateibereichen verfügt, die für Unicode aktiviert sind, muss möglicherweise den Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls einen Namen aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich in der Beschreibung des Parameters NAMETYPE. Geben Sie keinen Dateibereichsnamen an oder geben Sie ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

FSID

Gibt die Dateibereichs-ID für den zu replizierenden Dateibereich an. Der Server verwendet FSIDs zum Lokalisieren der Dateibereiche, die repliziert werden sollen. Um die FSID für einen Dateibereich zu bestimmen, geben Sie den Befehl QUERY FILESPACE aus. Mehrere FSIDs sind ohne Leerzeichen durch Kommas voneinander zu trennen. Wenn Sie eine FSID angeben, muss der Wert des Parameters NAMETYPE FSID lauten.

NAMEType

Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Sie können diesen Parameter für IBM Spectrum Protect-Clients verwenden, die für Unicode aktiviert sind und die über die Betriebssysteme Windows, Macintosh OS X und NetWare verfügen.
Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

SERVER

Der Server verwendet die Zeichenumsetztabelle des Servers, um Dateibereichsnamen zu interpretieren.

UNIcode

Der Server konvertiert Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von den Zeichen in dem Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann.

FSID

Der Server interpretiert Dateibereichsnamen unter Verwendung ihrer Dateibereichs-IDs.

CODEType

Gibt den Typ der Dateibereiche an, die bei der Knotenreplikationsverarbeitung berücksichtigt werden sollen. Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Der Standardwert lautet BOTH. Dieser Standardwert gibt an, dass Dateibereiche unabhängig vom Typ der Codepage eingeschlossen werden. Sie können einen der folgenden Werte angeben:

UNIcode

Gibt Dateibereiche an, die nur in Unicode sind.

NONUNIcode

Gibt Dateibereiche an, die nicht in Unicode sind.

BOTH

Gibt alle Dateibereiche unabhängig von der Art der Zeichenumsetztabelle an.

DATAtype

Gibt den Typ der Daten an, die repliziert werden sollen. Daten werden gemäß der Replikationsregel repliziert, die für den Datentyp gilt. Dieser Parameter ist wahlfrei. Sie können einen oder mehrere Datentypen angeben. Wenn Sie keinen Datentyp angeben, werden alle Sicherungsdaten, Archivierungsdaten und speicherverwaltete Daten repliziert. Mehrere Datentypen sind ohne Leerzeichen durch Kommas voneinander zu trennen. Sie können keine Platzhalterzeichen verwenden. Sie können einen der folgenden Werte angeben:

ALl

Repliziert alle Sicherungsdaten, Archivierungsdaten und speicherverwaltete Daten in einem Dateibereich gemäß der Regel, die dem Datentyp zugeordnet ist. Beispiel: Angenommen, NODE1 hat einen einzelnen Dateibereich. Es gelten die folgenden Replikationsregeln:

- Die Dateibereichsregeln für Sicherungs- und Archivierungsdaten in dem Dateibereich sind auf ALL_DATA gesetzt.

- Die Dateibereichsregel für speicherverwaltete Daten ist auf DEFAULT gesetzt.
- Die Clientknotenregel für speicherverwaltete Daten ist auf NONE gesetzt.

Wenn Sie den Befehl `REPLICATE NODE NODE1 DATATYPE=ALL` ausgeben, werden nur Sicherungs- und Archivierungsdaten repliziert.

BACKUP
: Repliziert aktive und inaktive Sicherungsdaten in einem Dateibereich, wenn die steuernde Replikationsregel ALL_DATA, ACTIVE_DATA, ALL_DATA_HIGH_PRIORITY oder ACTIVE_DATA_HIGH_PRIORITY lautet.

BACKUPActive
: Repliziert nur aktive Sicherungsdaten in einem Dateibereich, wenn die steuernde Replikationsregel ACTIVE_DATA oder ACTIVE_DATA_HIGH_PRIORITY lautet.

ARCHive
: Repliziert nur Archivierungsdaten in einem Dateibereich, wenn die steuernde Replikationsregel ALL_DATA oder ALL_DATA_HIGH_PRIORITY lautet.

SPACEManaged
: Repliziert nur speicherverwaltete Daten in einem Dateibereich, wenn die steuernde Replikationsregel ALL_DATA oder ALL_DATA_HIGH_PRIORITY lautet.

PRIority
: Gibt die zu replizierenden Daten auf der Basis der Priorität der Replikationsregel an. Sie können einen der folgenden Werte angeben:

All
: Repliziert alle Daten in einem Dateibereich, wenn die steuernde Replikationsregel ALL_DATA, ACTIVE_DATA, ALL_DATA_HIGH_PRIORITY oder ACTIVE_DATA_HIGH_PRIORITY lautet.

High
: Repliziert nur Daten in einem Dateibereich, die die steuernde Replikationsregel ALL_DATA_HIGH_PRIORITY oder ACTIVE_DATA_HIGH_PRIORITY haben.

Normal
: Repliziert nur Daten in einem Dateibereich, die die steuernde Replikationsregel ALL_DATA oder ACTIVE_DATA haben.

MAXSESSions
: Gibt die maximal zulässige Anzahl der Datensitzungen an, die zum Senden von Daten an einen Zielreplikationsserver verwendet werden sollen. Dieser Parameter ist wahlfrei. Der Wert kann zwischen 1 und 99 liegen. Der Standardwert ist 10.

Wird die Anzahl der Sitzungen erhöht, kann der Durchsatz bei der Knotenreplikation verbessert werden.

Berücksichtigen Sie bei der Festlegung dieses Werts die Anzahl der logischen und physischen Laufwerke, die dem Replikationsprozess zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke hängt von den folgenden Faktoren ab:

- Andere IBM Spectrum Protect-Aktivitäten und Systemaktivitäten
- Die Grenzwerte für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff, die betroffen sind

Stellen Sie sicher, dass genügend Mountpunkte und Laufwerke verfügbar sind, damit die Knotenreplikationsprozesse ausgeführt werden können. Jede Replikationssitzung benötigt möglicherweise für Speicherpooldatenträger einen Mountpunkt auf dem Quellen- und Zielreplikationsserver. Lautet der Einheitentyp nicht FILE, benötigt jede Sitzung möglicherweise auch ein Laufwerk auf dem Quellen- und Zielreplikationsserver.

Berücksichtigen Sie bei der Festlegung eines Werts für MAXSESSIONS auch die verfügbare Bandbreite und die Prozessorkapazität des Quellen- und Zielreplikationsservers.

Tipp:

- Der vom Parameter MAXSESSIONS angegebene Wert gilt nur für Datensitzungen. Datensitzungen sind Sitzungen, in denen Daten an einen Zielreplikationsserver gesendet werden. Wird jedoch ein Befehl QUERY SESSION ausgegeben, kann die Gesamtzahl der Sitzungen die Anzahl der Datensitzungen überschreiten. Die Differenz resultiert aus kurzen Steuersitzungen, die zum Abfragen und Definieren von Replikationsoperationen verwendet werden.
- Der Wert des Parameters MAXSESSIONS stellt die maximal zulässige Anzahl Sitzungen dar. Die Anzahl der Sitzungen, die für die Replikation verwendet werden, hängt vom Datenvolumen ab, das repliziert werden soll. Wird nur ein geringes Datenvolumen repliziert, wird durch die Erhöhung der Anzahl Sitzungen kein Vorteil erzielt. Die Gesamtzahl der Sitzungen kann kleiner als der Wert sein, der mit dem Parameter MAXSESSIONS angegeben wird.

Preview
: Gibt an, ob eine Voranzeige der Daten aufgerufen werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

No
: Gibt an, dass die Daten auf den Zielserver repliziert, aber nicht vorangezeigt werden.

Yes
: Gibt an, dass die Daten vorangezeigt, aber nicht repliziert werden. Wenn Sie PREVIEW=YES angeben, werden nur Datenträger, die physisch geladen werden müssen, wie z. B. Banddatenträger, angezeigt. Datenträger, die Speicherpools zugeordnet sind, die die

Einheitenklasse FILE haben, werden nicht angezeigt.

Die folgenden Informationen werden in der Ausgabe angezeigt:

- Die Namen der Clientknoten, deren Daten repliziert würden.
- Die Anzahl der Dateien, die repliziert oder gelöscht würden.
- Die geschätzte Zeit für die Ausführung des Knotenreplikationsprozesses.
- Eine Liste der Datenträger, die geladen würden.
- Eine Zusammenfassung der Informationen zu replizierten, beschädigten Daten. In der Zusammenfassung werden die Anzahl der Knoten, der Dateibereiche, der Dateien und der Byte aufgelistet, die während eines Replikationswiederherstellungsprozesses wiederhergestellt werden können. Die Zusammenfassung wird nur angezeigt, wenn RECOVERDAMAGED=YES oder RECOVERDAMAGED=ONLY angegeben ist.

Wenn die Daten des mit dem Befehl REPLICATE NODE angegebenen Clientknotens nie repliziert wurden und Sie `PREVIEW=YES` angeben, werden der Knoten und seine Dateibereiche automatisch auf dem Zielreplikationsserver definiert.

LISTfiles

Gibt an, ob die Namen der Dateien aufgelistet werden sollen, die repliziert würden. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Die Angabe dieses Parameters bedeutet, dass der Parameter WAIT auf YES gesetzt ist und Sie den Parameter WAIT nicht an der Serverkonsole ausgeben können.

Sie können einen der folgenden Werte angeben:

No
: Gibt an, dass die Namen der Dateien, die repliziert würden, nicht angezeigt werden.

Yes
: Gibt an, dass die Namen der Dateien, die repliziert würden, angezeigt werden.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

  No
  : Gibt an, dass der Befehl im Hintergrund verarbeitet wird. Um die Hintergrundverarbeitung des Befehls REPLICATE NODE zu überwachen, geben Sie den Befehl QUERY PROCESS aus.

  Yes
  : Gibt an, dass der Befehl im Vordergrund verarbeitet wird. Nachrichten werden erst angezeigt, wenn die Verarbeitung des Befehls beendet ist. Sie können nicht `WAIT=YES` an der Serverkonsole angeben.

RECOVERDamaged
: Gibt an, ob nach der Beendigung des Knotenreplikationsprozesses ein Wiederherstellungsprozess auf einem Zielreplikationsserver gestartet wird. Dieser Parameter ist optional und überschreibt den Wert, den Sie bei der Definition oder Aktualisierung eines Knotens für den Parameter RECOVERDamaged angegeben haben. Sie können einen der folgenden Werte angeben:

  Yes
  : Gibt an, dass ein Replikationsprozess gestartet wird, um beschädigte Dateien wiederherzustellen. Dies gilt jedoch nur, wenn die Einstellung für den Systemparameter REPLRECOVERDAMAGED ON lautet. Lautet die Einstellung OFF, werden beschädigte Dateien nicht wiederhergestellt.

  No
  : Gibt an, dass beschädigte Dateien nicht wiederhergestellt werden.

  Only
  : Gibt an, dass ein Replikationsprozess nur zum Zweck der Wiederherstellung beschädigter Dateien gestartet wird. Dies gilt jedoch nur, wenn die Einstellung für den Systemparameter REPLRECOVERDAMAGED ON lautet. Lautet die Einstellung OFF, werden beschädigte Dateien nicht wiederhergestellt, und Sie erhalten eine Benachrichtigung, dass die Wiederherstellung nicht gestartet wurde.
  Einschränkung: Wenn Sie eine ungültige Kombination von Werten und Einstellungen für die Dateiwiederherstellung angeben, wird die Replikation gestoppt und eine Fehlernachricht angezeigt.

FORCEREConcile
: Gibt an, ob alle Dateien auf dem Quellenreplikationsserver mit den Dateien auf dem Zielreplikationsserver verglichen und die Unterschiede zwischen ihnen synchronisiert werden sollen. Vor Version 7.1.1 war dieses Verhalten der Standardwert für die Replikationsverarbeitung. Wenn IBM® Tivoli Storage Manager Version 7.1.1 oder höher auf dem Quellen- und Zielreplikationsserver installiert ist, wird während der Erstreplikation automatisch ein Abgleich ausgeführt. Nach der Erstreplikation können Sie diesen Parameter aus folgenden Gründen verwenden:

  - Um Dateien auf dem Quellen- und dem Zielreplikationsserver zu synchronisieren, wenn sie unterschiedlich sind.
  - Um inaktive Dateien, die übersprungen wurden, zu replizieren, wenn die Replikationsregeln von ACTIVE_DATA in ALL_DATA geändert werden.
  - Um inaktive Dateien auf dem Zielreplikationsserver zu löschen, wenn die Replikationsregeln von ALL_DATA in ACTIVE_DATA geändert werden.

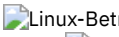
- Um sicherzustellen, dass nur aktive Daten repliziert werden, wenn Sie die Replikationsregel ACTIVE_DATA verwenden, sodass der Zielreplikationsserver nur über aktive Dateien verfügt.
- Um die Dateien zu resynchronisieren, damit der Zielreplikationsserver dieselben Dateien wie der Quellenreplikationsserver hat, wenn Sie zuvor oder derzeit die Maßnahmen auf dem Zielreplikationsserver zum Verwalten replizierter Dateien verwendet haben bzw. verwenden.
- Um die Dateien auf dem Quellen- und dem Zielreplikationsserver zu resynchronisieren, wenn die Datenbank mit einer anderen Methode als dem Befehl DSMSERV RESTORE DB auf einen früheren Zeitpunkt zurückgesetzt wird.
- Um Dateien an die neue Verwaltungsklasse auf dem Zielreplikationsserver erneut zu binden, wenn diese Verwaltungsklasse nicht vorhanden war, als die Dateien repliziert wurden. Sie müssen die Maßnahmen verwenden, die auf dem Zielreplikationsserver definiert sind, um replizierte Dateien zu verwalten.

Hinweis: Wenn die Regel ACTIVE_DATA zugeordnet ist, wird ein Abgleich nur für aktive Dateien auf dem Quellenreplikationsserver ausgeführt.

Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No
: Gibt an, dass die Replikationsverarbeitung keinen Abgleich erzwingt, um alle Dateien auf dem Quellenreplikationsserver mit Dateien auf dem Zielreplikationsserver zu vergleichen. Stattdessen verfolgt die Replikationsverarbeitung Dateiänderungen auf dem Quellenreplikationsserver seit der letzten Replikation und synchronisiert diese Änderungen auf dem Zielreplikationsserver. NO ist der Standardwert.

Yes
: Gibt an, dass die Replikationsverarbeitung einen Abgleich erzwingt, um alle Dateien auf dem Quellenreplikationsserver mit Dateien auf dem Zielreplikationsserver zu vergleichen, und die Dateien auf dem Zielreplikationsserver mit den Dateien auf dem Quellenreplikationsserver synchronisiert.


TRANSFERMethod


Gibt die Methode an, die für die Datenübertragung zwischen Servern verwendet wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Tcpip
: Gibt an, dass TCP/IP für die Übertragung von Daten verwendet wird. Dieser Wert ist der Standardwert.

Fasp
: Gibt an, dass die Aspera FASP-Technologie (Fast Adaptive Secure Protocol) für die Übertragung von Daten verwendet wird. Mit der Aspera FASP-Technologie kann die Datenübertragung in einem Weitverkehrsnetz (WAN) optimiert werden. Wenn Sie TRANSFERMETHOD=FASP angeben, werden alle Parameter TRANSFERMETHOD überschrieben, die Sie im Befehl DEFINE SERVER oder UPDATE SERVER angegeben haben.
  Einschränkungen:

  - Mit der Aspera FASP-Technologie können nur Daten übertragen werden, die in einem Verzeichniscontainerspeicherpool gespeichert sind. Zur Übertragung von Daten, die nicht in einem Verzeichniscontainerspeicherpool gespeichert sind, wird TCP/IP verwendet.
  - Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie bestimmen, ob die Technologie für Ihre Systemumgebung geeignet ist, und die entsprechenden Lizenzen installieren. Anweisungen finden Sie unter Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann. Wenn die Lizenzen fehlen oder abgelaufen sind, schlägt die Knotenreplikation fehl.
  - Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.

Beispiel: Daten nach Datentyp und Priorität replizieren

Aktive Sicherungsdaten und Archivierungsdaten mit hoher Priorität replizieren, die zu allen Clientknoten in der Gruppe PAYROLL gehören.

```
replicate node payroll datatype=backupactive,archive priority=high
```

Beispiel: Alle Daten, die zu einem Knoten gehören, gemäß den zugeordneten Replikationsregeln replizieren

NODE1 hat einen einzelnen Dateibereich. Es gelten die folgenden Replikationsregeln:

- Dateibereichsregeln:
  - Sicherungsdaten: ACTIVE_DATA
  - Archivierungsdaten: DEFAULT
  - Speicherverwaltete Daten: DEFAULT
- Clientknotenregeln:
  - Sicherungsdaten: DEFAULT
  - Archivierungsdaten: ALL_DATA_HIGH_PRIORITY
  - Speicherverwaltete Daten: DEFAULT
- Serverregeln:
  - Sicherungsdaten: ALL_DATA
  - Archivierungsdaten: ALL_DATA

- Speicherverwaltete Daten: NONE

```
replicate node node1 priority=all
```

Aktive Sicherungsdaten in dem Dateibereich werden mit normaler Priorität repliziert. Archivierungsdaten werden mit hoher Priorität repliziert. Speicherverwaltete Daten werden nicht repliziert.

Beispiel: Beschädigte Dateien ohne Starten des vollständigen Replikationsprozesses wiederherstellen

Alle beschädigten Dateien auf den Clientknoten der Group PAYROLL wiederherstellen, ohne den vollständigen Replikationsprozess zu starten. Sicherstellen, dass die Einstellung für den Systemparameter REPLRECOVERDAMAGED ON lautet. Anschließend den folgenden Befehl ausgeben:

```
replicate node payroll recoverdamaged=only
```

Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für REPLICATE NODE

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
CANCEL REPLICATION	Bricht Knotenreplikationsprozesse ab.
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY REPLNODE	Zeigt Informationen zum Replikationsstatus eines Clientknotens an.
QUERY REPLRULE	Zeigt Informationen zu Knotenreplikationsregeln an.
QUERY SERVER	Zeigt Informationen über Server an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REMOVE REPLNODE	Entfernt einen Knoten aus der Replikation.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemePROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.
SET REPLRECOVERDAMAGED	Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.
UPDATE FILESPACE	Ändert Knotenreplikationsregeln für Dateibereiche.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.
UPDATE REPLRULE	Aktiviert oder inaktiviert Replikationsregeln.
VALIDATE REPLICATION	Überprüft die Replikation für Dateibereiche und Datentypen.

REPLY (Verarbeitung einer Anforderung fortsetzen)

Mit Hilfe dieses Befehls und einer Identifikationsnummer kann der Server darüber informiert werden, dass eine angeforderte Operation beendet wurde. Nicht alle Serveranforderungen erfordern eine Antwort. Dieser Befehl ist nur erforderlich, wenn die Anforderungsnachricht ausdrücklich angibt, dass eine Antwort benötigt wird.

Berechtigungsklasse

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

Syntax

```
>>-REPly--Anforderungsnummer----------------------------------->

>--+-------------------------------+--------------------------><
   '-LABEL--=--Datenträgerkennsatz-'
```

Parameter

Anforderungsnummer **(Erforderlich)**
: Gibt die Identifikationsnummer der Anforderung an.

LABEL
: Gibt den Kennsatz an, der auf einen Datenträger geschrieben werden soll, wenn Sie auf eine Nachricht von einem Prozess des Befehls LABEL LIBVOLUME antworten. Dieser Parameter ist wahlfrei.

Beispiel: Auf eine Anforderung antworten

Eine Antwortanforderung mit 3 als Anforderungsnummer beantworten.

```
reply 3
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REPLY

Befehl	Beschreibung
CANCEL REQUEST	Bricht anstehende Datenträgerladeanforderungen ab.
QUERY REQUEST	Zeigt Informationen über alle anstehenden Ladeanforderungen an.

RESET PASSEXP (Kennwortablaufdauer zurücksetzen)

Verwenden Sie den Befehl RESET PASSEXP, um die Kennwortablaufdauer für Kennwörter von Administratoren und Clientknoten auf die allgemeine Kennwortablaufdauer zurückzusetzen. Der Befehl RESET PASSEXP gilt nicht für Kennwörter, die auf einem LDAP-Verzeichnisserver gespeichert werden.

Einschränkung: Sie können die Kennwortablaufdauer nicht mit dem Befehl SET PASSEXP auf eine allgemeine Kennwortablaufdauer zurücksetzen.

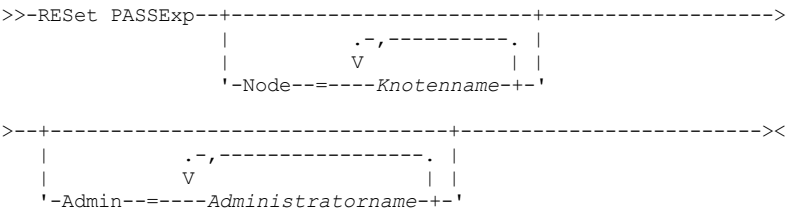
Verwenden Sie den Befehl QUERY STATUS, um die allgemeine Kennwortablaufdauer anzuzeigen.

Einschränkung: Wird der Parameter NODE oder ADMIN nicht angegeben, wird die Kennwortablaufdauer für alle Clientknoten und Administratoren zurückgesetzt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Node
: Gibt den Namen des Knotens an, dessen Kennwortablaufdauer zurückgesetzt werden soll. Soll eine Liste mit Knoten angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

Admin
: Gibt den Namen des Administrators an, dessen Kennwortablaufdauer zurückgesetzt werden soll. Soll eine Liste mit Administratoren angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

Beispiel: Die Kennwortablaufdauer für bestimmte Clientknoten zurücksetzen

Die Kennwortablaufdauer für die Clientknoten bj und katie zurücksetzen.

```
reset passexp node=bj,katie
```

Beispiel: Die Kennwortablaufdauer für alle Benutzer zurücksetzen

Die Kennwortablaufdauer für alle Benutzer auf die allgemeine Kennwortablaufdauer zurücksetzen.

```
reset passexp
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESET PASSEXP

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET PASSEXP	Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.
UPDATE ADMIN	Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

RESTART EXPORT (Ausgesetzte Exportoperation erneut starten)

Mit diesem Befehl kann eine ausgesetzte Exportoperation erneut gestartet werden.

Eine Exportoperation wird ausgesetzt, wenn eine der folgenden Bedingungen festgestellt wird:

- Ein Befehl SUSPEND EXPORT wird für die aktive Exportoperation ausgegeben
- Segmentvorableerung - die Datei, die für den Export gelesen wird, wird von einem anderen Prozess gelöscht
- Übertragungsfehler bei einem Export zwischen Servern
- Keine verfügbaren Mountpunkte
- Erforderliche Datenträger sind nicht verfügbar
- E/A-Fehler wurden festgestellt

Wichtig: Knoten oder Dateibereiche (auf dem exportierenden Server) in der ursprünglichen Exportoperation, die später umbenannt werden, werden bei der wieder aufgenommenen Operation nicht berücksichtigt. Alle verbleibenden Daten für Knoten oder Dateibereiche auf dem Zielserver, die vor der Wiederaufnahme gelöscht werden, werden verworfen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung erforderlich.

Syntax

```
                    .-*-------------.
>>-RESTART EXPORT -+---------------+---------------------------><
                    '---Export-ID---'
```

Parameter

Export-ID
: Dieser optionale Parameter ist die eindeutige ID für die ausgesetzte Exportoperation zwischen Servern. Es kann ein Platzhalterzeichen verwendet werden, um diesen Namen anzugeben. Der Name der Export-ID kann mit dem Befehl QUERY EXPORT ermittelt werden, der alle momentan ausgesetzten Exportoperationen zwischen Servern auflistet.

Beispiel: Einen ausgesetzten Export erneut starten

Die ausgesetzte Exportoperation erneut starten, die durch die Export-ID EXPORTALLACCTNODES angegeben ist.

```
restart export exportallacctnodes
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESTART EXPORT

Befehl	Beschreibung
CANCEL EXPORT	Löscht eine ausgesetzte Exportoperation.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.

Befehl	Beschreibung
EXPORT SERVER	Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server.
QUERY EXPORT	Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.
SUSPEND EXPORT	Setzt eine aktive Exportoperation aus.

RESTORE-Befehle

Mit den RESTORE-Befehlen können IBM Spectrum Protect-Speicherpools oder -Datenträger zurückgeschrieben werden.

- RESTORE NODE (NAS-Knoten zurückschreiben)
- RESTORE STGPOOL (Speicherpooldaten aus einem Kopienpool oder einem Pool für aktive Daten zurückschreiben)
- RESTORE VOLUME (Daten primärer Datenträger aus Kopienpool oder Pool für aktive Daten zurückschreiben)

RESTORE NODE (NAS-Knoten zurückschreiben)

Verwenden Sie diesen Befehl, um eine Zurückschreibungsoperation für einen NAS-Knoten (NAS = Network Attached Storage) einzuleiten.

Sie können den Befehl RESTORE NODE verwenden, um Sicherungen zurückzuschreiben, die entweder mit dem Clientbefehl BACKUP NAS oder mit dem Serverbefehl BACKUP NODE erstellt wurden. NAS-Daten können aus nativen primären IBM Spectrum Protect-Pools oder nativen IBM Spectrum Protect-Kopienpools, aus primären NAS-Pools oder NAS-Kopienpools oder aus einer beliebigen Kombination, die für die Zurückschreibung erforderlich ist, zurückgeschrieben werden.

Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie die Systemberechtigung, die Maßnahmenberechtigung für die Domäne, der der Knoten zugeordnet ist, oder die Clienteignerberechtigung für den Knoten haben.

Syntax

```
>>-RESTORE Node--Knotenname--Quellendateisystem----------------->

   .-Quellendateisystem-.
>--+--------------------+---------------------------------------->
   '-Zieldateisystem----'

>--+-------------------------------------+----------------------->
   |                .-,---------.        |
   |                V           |        |
   '-FILELIST--=--+---Dateiname-+-----+-'
                  '-FILE:--Dateiliste-'

   .-NAMEType--=--SERVER----------.
>--+-----------------------------+---------------------------->
   '-NAMEType--=--+-SERVER------+-'
                  +-HEXadecimal-+
                  '-UNIcode-----'

   .-PITDate--=--TODAY-------------.
>--+-------------------------------+---------------------------->
   '-PITDate--=--+-mm/dd/yyyy----+-'
                 +-TODAY---------+
                 +-TODAY-AnzTage-+
                 '- -AnzTage-----'

   .-PITTime--=--NOW-----------.  .-Wait--=--No------.
>--+-------------------------+--+-------------------+---------->
   '-PITTime--=--+-hh:mm:ss--+-'  '-Wait--=--+-No--+-'
                 +-NOW-------+               '-Yes-'
                 +-NOW-hh:mm-+
                 '- -hh:mm---'

   .-TYPE--=--BACKUPImage-----.
>--+--------------------------+------------------------------><
   '-TYPE--=--+-BACKUPImage-+-'
              '-SNAPMirror--'
```

Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Knotens an, der zurückgeschrieben werden soll. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

Quellendateisystem (Erforderlich)
: Gibt den Namen des Dateisystems an, das zurückgeschrieben werden soll. Für diesen Namen können keine Platzhalterzeichen verwendet werden. Es kann nur ein Dateisystem zum Zurückschreiben angegeben werden. Namen virtueller Dateibereiche sind zulässig.

Zieldateisystem
: Gibt an, dass der Dateiserver die Daten in ein vorhandenes angehängtes Dateisystem auf dem Dateiserver zurückschreibt. Dieser Parameter ist wahlfrei. Der Standardwert ist die ursprüngliche Position des Dateisystems auf dem Dateiserver. Namen virtueller Dateibereiche sind zulässig.

FILELIST
: Gibt die Liste der Dateien oder Verzeichnisse an, die zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass das gesamte Dateisystem zurückgeschrieben werden soll. Wird dieser Wert angegeben, versucht der Server, die Objekte aus dem entsprechenden Image zurückzuschreiben. Werden die Parameter PITDATE und PITTIME angegeben, wird die Datei aus dem letzten Sicherungsimage vor der angegebenen Zeit zurückgeschrieben. Werden die Parameter PITDATE und PITTIME nicht angegeben, wird die Datei aus dem letzten Sicherungsimage des Dateisystems zurückgeschrieben.

  Ist das Image eine Differenzsicherung, werden Objekte zuerst aus der entsprechenden Gesamtsicherung und dann aus der Differenzsicherung zurückgeschrieben. Die Zurückschreibung wird ausgeführt, indem die entsprechenden Images nach den angegebenen Objekten durchsucht werden und alle gefundenen Objekte zurückgeschrieben werden. Auf die Inhaltsverzeichnisse für diese Images wird nicht zugegriffen, so dass der Server nicht überprüft, ob die Objekte tatsächlich in den Images enthalten sind.

  Der Ordnerpfad und Dateiname müssen unter Verwendung von Schrägstrichsymbolen (/) eingegeben werden. Es ist kein abschließender Schrägstrich (/) am Ende des Dateinamens erforderlich. Alle Argumente, die ein Leerzeichen enthalten, müssen über Anführungszeichen verfügen ("Argument mit Leerzeichen"), die das gesamte Argument einschließen.

  ```
  FILELIST="/path/to/filename1 with blanks",/path/to/filename2_no_blanks
  ```

  Alle Dateinamen, die Kommas enthalten, müssen Anführungszeichen haben, die das gesamte Argument einschließen, und müssen in Hochkommas eingeschlossen sein ('"Argument mit Kommas"').

  ```
  FILELIST='"/Pfad/zu/Dateiname1,mit,Kommas"',/Pfad/zu/Dateiname2_ohne_Kommas
  ```

  Um ein vollständiges Verzeichnis zurückzuschreiben, geben Sie anstelle eines Dateinamens einen Verzeichnisnamen an. Alle Dateien in dem Verzeichnis und in seinen Unterverzeichnissen werden zurückgeschrieben. Es ist kein abschließender Schrägstrich (/) am Ende des Verzeichnisnamens erforderlich:

  ```
  FILELIST=/path/to/mydir
  ```

  Dateiname
  : Gibt einen oder mehrere Datei- oder Verzeichnisnamen an, die zurückgeschrieben werden sollen. Die angegebenen Namen dürfen keine Platzhalterzeichen enthalten. Mehrere Namen müssen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Bei Dateinamen muss die Groß-/Kleinschreibung berücksichtigt werden.

  FILE:Dateiliste
  : Gibt den Namen einer Datei an, die eine Liste der Datei- oder Verzeichnisnamen enthält, die zurückgeschrieben werden sollen. In der angegebenen Datei muss jeder Datei- oder Verzeichnisname in einer separaten Zeile stehen. Leerzeilen und Kommentarzeilen, die mit einem Stern beginnen, werden ignoriert. Beispiel:
    Um die Dateien FILE01, FILE02 und FILE03 zurückzuschreiben, erstellen Sie eine Datei mit dem Namen RESTORELIST, die eine Zeile für jede Datei enthält:

    ```
    FILE01
    FILE02
    FILE03
    ```

    Sie können die Dateien, die zurückgeschrieben werden sollen, mit dem folgenden Befehl angeben:

    ```
    FILELIST=FILE:RESTORELIST
    ```

NAMEType
: Gibt an, wie der Server die Namen, die als FILELIST=Dateiname angegeben werden, oder die Namen, die in der mit FILELIST=Dateiliste angegebenen Datei aufgelistet sind, interpretieren soll. Dieser Parameter ist nützlich, wenn die Namen Unicode-Zeichen enthalten. Er hat keine Auswirkungen, wenn der Parameter FILELIST nicht angegeben wird. Der Standardwert lautet SERVER. Gültige Werte:

  SERVER
  : Der Server verwendet die Codepage des Servers, um die Namen zu interpretieren.

  HEXadecimal
  : Der Server interpretiert die eingegebenen Namen als hexadezimale Darstellung eines Namens in Unicode. Soll die hexadezimale Darstellung eines Datei- oder Verzeichnisnamens angezeigt werden, können Sie den Befehl QUERY TOC mit FORMAT=DETAILED verwenden.

  UNIcode
  : Der Server interpretiert die Namen als UTF-8-verschlüsselt. Diese Option ist nur gültig, wenn Sie eine Liste mit FILELIST=FILE:Dateiliste angegeben haben.

Einschränkung: Network Data Management Protocol (NDMP) verfügt über Einschränkungen, die verhindern, dass IBM Spectrum Protect das erfolgreiche Zurückschreiben einzelner Dateien und Verzeichnisse melden kann.

PITDate

Gibt das Datum des Zeitpunkts an. Bei Verwendung mit dem Parameter PITTIME gibt PITDATE den Zeitpunkt an, ab dem Daten zum Zurückschreiben ausgewählt werden sollen. Die letzten Daten, die an oder vor dem angegebenen Datum und der angegebenen Uhrzeit gesichert wurden, werden zurückgeschrieben. Dieser Parameter ist wahlfrei. Der Standardwert ist TODAY.
Sie können das Datum mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	06/25/2001
TODAY	Das aktuelle Datum	TODAY
TODAY-Tage *oder* -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage	TODAY–7 *oder* –7. Um Daten zurückzuschreiben, die vor einer Woche gesichert wurden, geben Sie PITDATE=TODAY-7 oder PITDATE=-7 an.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

PITTime

Gibt die Uhrzeit des Zeitpunkts an. Bei Verwendung mit dem Parameter PITDATE gibt PITTIME den Zeitpunkt an, ab dem Daten zum Zurückschreiben ausgewählt werden sollen. Die letzten Daten, die an oder vor dem angegebenen Datum und der angegebenen Uhrzeit gesichert wurden, werden zurückgeschrieben. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit.
Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit am angegebenen Datum	12:33:28
NOW	Die aktuelle Uhrzeit am angegebenen Datum	NOW
NOW-HH:MM *oder* -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Anfangsdatum	NOW-03:30 *oder* -03:30. Wird dieser Befehl um 9:00 Uhr mit der Angabe PITTIME=NOW-03:30 oder PITTIME=-03:30 ausgegeben, schreibt der Server Sicherungssätze mit der Uhrzeit 5:30 Uhr oder später am Datum des Zeitpunkts zurück.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist NO. Gültige Werte:

No
: Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Mit dem Befehl QUERY PROCESS kann die Hintergrundverarbeitung dieses Befehls überwacht werden.

Yes
: Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Der Befehl muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist. Einschränkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

TYPE

Gibt den Typ des Images an, das zurückgeschrieben werden soll. Der Standardwert für diesen Parameter ist BACKUPIMAGE, und er wird verwendet, um Daten aus standardmäßigen NDMP-Basis- oder -Differenzsicherungen zurückzuschreiben. Andere Imagetypen stellen Sicherungsmethoden dar, die für einen bestimmten Dateiserver spezifisch sein können. Gültige Werte:

BACKUPImage
: Gibt an, dass das Dateisystem aus den entsprechenden standardmäßigen NDMP-Sicherungsimages zurückgeschrieben werden soll. Dies ist die Standardmethode für die Ausführung einer NDMP-Zurückschreibungsoperation. Mit dem Typ BACKUPIMAGE können Sie Daten aus Basis- und Differenzsicherungen sowie Daten auf Dateiebene zurückschreiben.

SNAPMirror
: Gibt an, dass das Dateisystem aus einem NetApp SnapMirror-Image abgerufen werden soll. SnapMirror-Images sind Gesamtsicherungsimages auf Blockebene eines NetApp-Dateisystems. Ein SnapMirror-Image kann nur in ein Dateisystem

zurückgeschrieben werden, das als SnapMirror-Zieldatenträger vorbereitet wurde. Ausführliche Informationen enthält die Dokumentation zu Ihrem NetApp-Dateiserver.

Nachdem ein SnapMirror-Image abgerufen und in ein Zieldateisystem kopiert wurde, unterbricht IBM Spectrum Protect die SnapMirror-Beziehung, die von dem Dateiserver während der Operation erstellt wurde. Nach Abschluss der Zurückschreibung kehrt das Zieldateisystem in denselben Status wie das ursprüngliche Dateisystem zum Zeitpunkt der Sicherung zurück.

Beachten Sie die folgenden Einschränkungen, wenn der Parameter TYPE auf SNAPMIRROR gesetzt wird:

Einschränkungen:

- Sie können nicht den Parameter FILELIST angeben.
- Weder der *Quellendateisystemname* noch der *Zieldateisystemname* kann der Name eines virtuellen Dateibereichs sein.
- Dieser Parameter ist nur für NetApp- und IBM® N-Series-Dateiserver gültig.

Beispiel: Ein vollständiges Verzeichnis zurückschreiben

Alle Dateien und Unterverzeichnisse in dem Verzeichnis `/mydir` zurückschreiben.

```
restore node nasnode /myfs /dest filelist=/path/to/mydir
```

Beispiel: Daten aus einem Dateisystem zurückschreiben

Die Daten aus dem Dateisystem `/vol/vol10` auf NAS-Knoten `NAS1` zurückschreiben.

```
restore node nas1 /vol/vol10
```

Beispiel: Eine Sicherung auf Verzeichnisebene an dieselbe Position zurückschreiben

Die Sicherung auf Verzeichnisebene an die ursprüngliche Position zurückschreiben. Die Quelle ist der virtuelle Dateibereich `/MIKESDIR`, und es ist kein Zielort angegeben.

```
restore node nas1 /mikesdir
```

Für dieses und das nächste Beispiel wird angenommen, dass die folgenden Definitionen für virtuelle Dateibereiche auf dem Server für den Knoten `NAS1` vorhanden sind.

```
VFS-Name             Dateisystem     Pfad
/mikesdir            /vol/vol2       /mikes
/TargetDirVol2       /vol/vol2       /tmp
/TargetDirVol1       /vol/vol1       /tmp
```

Beispiel: Eine Sicherung auf Verzeichnisebene in ein anderes Dateisystem zurückschreiben

Die Sicherung auf Verzeichnisebene in ein anderes Dateisystem zurückschreiben, aber den Pfad beibehalten.

```
restore node nas1 /mikesdir /vol/vol0
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESTORE NODE

Befehl	Beschreibung
BACKUP NODE	Sichert einen NAS-Knoten (NAS = Network Attached Storage).
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
DEFINE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs definieren.
QUERY NASBACKUP	Zeigt Informationen zu NAS-Sicherungsimages an.
QUERY TOC	Zeigt Details zum Inhaltsverzeichnis für ein angegebenes Sicherungsimage an.

RESTORE STGPOOL (Speicherpooldaten aus einem Kopienpool oder einem Pool für aktive Daten zurückschreiben)

Mit diesem Befehl können Dateien aus einem oder mehreren Kopienspeicherpools oder Pools für aktive Daten in einen primären Speicherpool zurückgeschrieben werden.

Von IBM Spectrum Protect werden alle Dateien im primären Speicherpool zurückgeschrieben, die

- als fehlerhaft identifiziert wurden.

- sich auf einem Datenträger mit dem Zugriffsmodus DESTROYED befinden.

Einschränkung: Sie können diesen Befehl nicht für Containerspeicherpools verwenden. Verwenden Sie den Befehl REPLICATE STGPOOL, um Daten für Containerspeicherpools zu schützen.

Mit diesem Befehl können auch Datenträger identifiziert werden, die zerstörte Primärdateien enthalten. Während der Zurückschreibungsverarbeitung wird für jeden Datenträger (im zurückgeschriebenen Speicherpool), der zerstörte, nicht zwischengespeicherte Dateien enthält, eine Nachricht ausgegeben. Mit dem Befehl QUERY CONTENT können zerstörte Primärdateien auf einem bestimmten Datenträger abgefragt werden.

Sie können keinen Speicherpool zurückschreiben, der mit der Einheitenklasse CENTERA definiert ist.

Neben dem Zurückschreiben von Daten in primäre Speicherpools mit dem Datenformat NATIVE oder NONBLOCK können Sie mit diesem Befehl auch Daten in primäre Speicherpools zurückschreiben, die NDMP-Datenformate haben (NETAPPDUMP, CELERRADUMP oder NDMPDUMP). Der primäre Speicherpool muss dasselbe Datenformat wie der Kopienspeicherpool haben, aus dem Daten zurückgeschrieben werden sollen. IBM Spectrum Protect unterstützt die Back-End-Datenversetzung für NDMP-Images.

Tipp: Um NAS-Clientknotendaten in NAS-Speicherpools zurückzuschreiben, müssen Sie manuell den Zugriffsmodus der Datenträger mit dem Befehl UPDATE VOLUME in DESTROYED ändern. Verwenden Sie jedoch Disaster Recovery Manager, enthält die Plandatei die Informationen, die der Server benötigt, um die Datenträger automatisch als DESTROYED zu markieren.
Die Zurückschreibung von Dateien kann unvollständig sein, wenn Sicherungsdateikopien in Kopienspeicherpools oder Pools für aktive Daten von anderen IBM Spectrum Protect-Prozessen während der Zurückschreibungsverarbeitung versetzt oder gelöscht wurden. Um diesen Fehler zu verhindern, geben Sie nicht die folgenden Befehle für Datenträger in Kopienspeicherpools oder Pools für aktive Daten aus, während die Zurückschreibungsverarbeitung läuft:

- MOVE DATA
- DELETE VOLUME (DISCARDDATA=YES)
- AUDIT VOLUME (FIX=YES)

Die Wiederherstellungsverarbeitung für Kopienspeicherpools kann verhindert werden, indem der Prozentsatz für RECLAIM im Befehl UPDATE STGPOOL auf 100 gesetzt wird.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den primären Speicherpool, für den Dateien zurückgeschrieben werden sollen, erforderlich. Wenn ein Administrator mit eingeschränkter Speicherberechtigung Dateien in einem neuen primären Speicherpool zurückschreiben möchte, muss er auch über die Berechtigung für diesen neuen Speicherpool verfügen.

Syntax

```
>>-RESTORE STGpool--Name_des_primären_Pools---------------------->

>--+---------------------------------+--------------------------->
   '-COPYstgpool--=--Kopienpoolname-'

   .-ACTIVEDATAOnly--=--No-------------.
>--+-----------------------------------+------------------------->
   '-ACTIVEDATAOnly--=--+-No---------+-'
                        '-Yes--| A |-'

>--+-----------------------------------------------+------------->
   '-NEWstgpool--=--Name_des_neuen_primären_Pools-'

   .-MAXPRocess--=--1------.  .-Preview--=--No------.
>--+----------------------+--+--------------------+----------->
   '-MAXPRocess--=--Anzahl-'  '-Preview--=--+-No--+-'
                                            '-Yes-'

   .-Wait--=--No------.
>--+------------------+---------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'

A (Yes)

|--ACTIVEDATAPool--=--Name_des_Pools_für_aktive_Daten-----------|
```

Parameter

Name_des_primären_Pools (Erforderlich)
: Gibt den Namen des primären Speicherpools an, der zurückgeschrieben wird.

COPYstgpool

Gibt den Namen des Kopienspeicherpools an, aus dem die Dateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien aus jedem Kopienspeicherpool, in dem Kopien gefunden werden, zurückgeschrieben. Verwenden Sie diesen Parameter nicht mit den Parametern ACTIVEDATAONLY oder ACTIVEDATAPOOL.

ACTIVEDATAOnly
: Gibt an, dass aktive Versionen von Sicherungsdateien nur aus Pools für aktive Daten zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird dieser Parameter nicht angegeben, werden Dateien aus Kopienspeicherpools zurückgeschrieben. Verwenden Sie diesen Parameter nicht mit dem Parameter COPYSTGPOOL. Gültige Werte:

  No
  : Gibt an, dass der Speicherpool nicht aus Pools für aktive Daten zurückgeschrieben wird.

  Yes
  : Gibt an, dass der Speicherpool aus Pools für aktive Daten zurückgeschrieben wird, die mit dem Parameter ACTIVEDATAPOOL angegeben werden. Wird YES als Wert für ACTIVEDATAONLY angegeben, aber wird kein Wert für ACTIVEDATAPOOL angegeben, werden Dateien aus jedem Pool für aktive Daten zurückgeschrieben, in dem aktive Versionen von Sicherungsdateien lokalisiert werden können.

  Achtung: Das Zurückschreiben eines primären Speicherpools aus einem Pool für aktive Daten kann zur Folge haben, dass einige oder alle inaktiven Dateien aus der Datenbank gelöscht werden, wenn der Server bestimmt, dass eine inaktive Datei ersetzt werden muss, aber der Server die Datei im Pool für aktive Daten nicht finden kann.

ACTIVEDATAPool
: Gibt den Namen des Pools für aktive Daten an, aus dem die aktiven Versionen von Sicherungsdateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien aus jedem Pool für aktive Daten zurückgeschrieben, in dem aktive Versionen von Sicherungsdateien lokalisiert werden können.

NEWstgpool
: Gibt den Namen des neuen Speicherpools an, in den die Dateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien in den ursprünglichen primären Speicherpool (den Pool, der wiederhergestellt wird) zurückgeschrieben.

MAXPRocess
: Gibt die maximale Anzahl paralleler Prozesse an, die für das Zurückschreiben von Dateien verwendet werden. Die Verwendung mehrerer paralleler Prozesse kann den Durchsatz der Zurückschreibung verbessern. Dieser Parameter ist wahlfrei. Es kann ein Wert von 1 bis 999 angegeben werden. Der Standardwert ist 1.

  Bei der Bestimmung dieses Werts ist die Anzahl Mountpunkte (logische Laufwerke) und physischer Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Aktivitäten und Systemaktivitäten sowie von den Mountlimits der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Zurückschreibung betroffen sind.

  Jeder Prozess benötigt einen Mountpunkt für Datenträger aus dem Kopienspeicherpool und, falls der Einheitentyp nicht FILE lautet, außerdem ein Laufwerk. Werden Dateien in einen Speicherpool mit sequenziellem Zugriff zurückgeschrieben, benötigt jeder Prozess einen zusätzlichen Mountpunkt für Datenträger für primäre Speicherpools und, falls die Einheitenklasse nicht FILE lautet, ein zusätzliches Laufwerk. Beispiel: Angenommen, es werden maximal 3 Prozesse für die Zurückschreibung eines primären sequenziellen Speicherpools aus einem Kopienspeicherpool mit derselben Einheitenklasse angegeben. Jeder Prozess benötigt zwei Mountpunkte und zwei Laufwerke. Um alle drei Prozesse ausführen zu können, muss das Mountlimit für die Einheitenklasse mindestens 6 betragen und es müssen mindestens 6 Mountpunkte und 6 Laufwerke verfügbar sein.

  Für die Voranzeige einer Zurückschreibung wird nur ein einziger Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

Preview
: Gibt an, ob eine Voranzeige der Zurückschreibung, nicht aber ihre Ausführung gewünscht wird. Anhand der Voranzeige können die Datenträger identifiziert werden, die zum Zurückschreiben des Speicherpools erforderlich sind. Die Voranzeige zeigt Folgendes an:

  - Eine Liste der Datenträger des primären Speicherpools, die beschädigte Dateien enthalten.
  - Die Anzahl Dateien und die Anzahl Byte, die zurückgeschrieben werden sollen, wobei davon ausgegangen wird, daß der Zugriffsmodus der erforderlichen Datenträger aus dem Kopienspeicherpool READWRITE oder READONLY lautet, wenn die Operation zum Zurückschreiben ausgeführt wird.
  - Eine Liste der Datenträger aus dem Kopienspeicherpool, die Dateien enthalten, die zurückgeschrieben werden sollen. Diese Datenträger müssen geladen werden, wenn die Zurückschreibung ausgeführt wird.
  - Eine Liste aller Datenträger mit Dateien, die nicht zurückgeschrieben werden können.

  Anmerkung: Soll nur eine Liste mit ausgelagerten Kopienspeicherpooldatenträgern angezeigt werden, die während einer Zurückschreibung geladen werden sollen, den Zugriffsmodus der Kopienpooldatenträger in UNAVAILABLE ändern. Damit wird die Wiederherstellungs- und Datenversetzungsverarbeitung der Datenträger verhindert, bis sie für die Zurückschreibung vor Ort versetzt werden.
  Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, daß die Zurückschreibung ausgeführt wird.

  Yes
  : Gibt an, daß eine Voranzeige der Zurückschreibung, aber nicht die Ausführung der Zurückschreibung gewünscht wird.

Wait

Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

No

Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden.

Bei dem Hintergrundprozess erstellte Nachrichten werden im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden. Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise einige Dateien bereits vor dem Abbruch zurückgeschrieben.

Yes

Gibt an, dass der Server diese Operation im Vordergrund ausführt. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Der Server zeigt dann die Ausgabenachrichten dem Verwaltungsclient an, wenn die Operation beendet ist.
Anmerkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

Beispiel: Dateien aus einem Kopienspeicherpool in den primären Speicherpool zurückschreiben

Dateien aus allen Kopienspeicherpools sollen in den primären Speicherpool PRIMARY_POOL zurückgeschrieben werden.

```
restore stgpool primary_pool
```

Beispiel: Dateien aus einem bestimmten Pool für aktive Daten in den primären Speicherpool zurückschreiben

Dateien aus dem Pool für aktive Daten ADP1 in den primären Speicherpool PRIMARY_POOL zurückschreiben.

```
restore stgpool primary_pool activedataonly=yes activedatapool=adp1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESTORE STGPOOL

Befehl	Beschreibung
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
QUERY CONTENT	Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
RESTORE VOLUME	Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopienspeicherpools zurück.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.
UPDATE VOLUME	Aktualisiert die Attribute der Speicherpooldatenträger.

RESTORE VOLUME (Daten primärer Datenträger aus Kopienpool oder Pool für aktive Daten zurückschreiben)

Mit diesem Befehl können alle Dateien auf beschädigten Datenträgern in einen primären Speicherpool zurückgeschrieben werden, der in einem Kopienspeicherpool gesichert oder in einen Pool für aktive Daten kopiert wurde. IBM Spectrum Protect schreibt keine Cache-Kopien von Dateien zurück, und entfernt diese Cache-Dateien während der Zurückschreibungsverarbeitung aus der Datenbank.

Neben dem Zurückschreiben von Daten auf Datenträger in Speicherpools mit dem Datenformat NATIVE oder NONBLOCK können Sie mit diesem Befehl auch Daten auf Datenträger in Speicherpools zurückschreiben, die NDMP-Datenformate haben (NETAPPDUMP, CELERRADUMP oder NDMPDUMP). Die Datenträger, die zurückgeschrieben werden sollen, müssen dasselbe Datenformat wie die Datenträger in dem Kopienspeicherpool haben. IBM Spectrum Protect unterstützt die Back-End-Datenversetzung für NDMP-Images.

Dieser Befehl ändert den Zugriffsmodus der angegebenen Datenträger in DESTROYED. Nachdem alle Dateien auf einem Datenträger in andere Standorte zurückgeschrieben wurden, wird der leere zerstörte Datenträger aus der Datenbank gelöscht.

Das Zurückschreiben kann aus folgenden Gründen unvollständig sein:

- Dateien wurden entweder nie gesichert oder die Sicherungskopien wurden als beschädigt markiert. Mit dem Befehl QUERY CONTENT können weitere Informationen zu den auf dem Datenträger verbleibenden Dateien abgerufen werden.
- Im Befehl RESTORE wurde zwar ein Kopienspeicherpool angegeben, aber die Dateien wurden in einem anderen Kopienspeicherpool gesichert. Wird der Befehl RESTORE nochmals ausgegeben, sollte der Parameter PREVIEW angegeben werden, um zu sehen, ob dies der Fall ist.
- Datenträger im Kopienspeicherpool, die für das Zurückschreiben benötigt werden, sind ausgelagert oder nicht verfügbar. Das Aktivitätenprotokoll auf Nachrichten prüfen, die während der Zurückschreibungsverarbeitung aufgetreten sind.
- Sicherungsdateikopien in Kopienspeicherpools wurden von anderen Prozessen während der Zurückschreibung versetzt oder gelöscht. Siehe 3.
- Ein Pool für aktive Daten wurde für die Zurückschreibung angegeben, und es waren keine inaktiven Dateien zum Kopieren verfügbar.

Wichtig:

1. Sie können keine Datenträger in Speicherpools zurückschreiben, die mit der Einheitenklasse CENTERA definiert sind.
2. Vor dem Zurückschreiben eines Datenträgers mit wahlfreiem Zugriff den Befehl VARY ausgeben, um den Datenträger abzuhängen.
3. Um zu verhindern, dass Kopienspeicherpooldateien von anderen Prozessen versetzt oder gelöscht werden, dürfen die folgenden Befehle während einer Zurückschreibung nicht für Kopienspeicherpooldatenträger ausgegeben werden:
   - MOVE DATA
   - DELETE VOLUME (DISCARDDATA=YES)
   - AUDIT VOLUME (FIX=YES)

   Um die Wiederherstellungsverarbeitung von Kopienspeicherpools zu verhindern, den Befehl UPDATE STGPOOL ausgeben und den Parameter RECLAIM in diesem Befehl auf 100 setzen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den primären Speicherpool erforderlich. Wenn ein Administrator mit eingeschränkter Berechtigung Dateien in einen neuen primären Speicherpool zurückschreiben möchte, muss er auch über die Berechtigung für den neuen Speicherpool verfügen.

Syntax

Parameter

Datenträgername (Erforderlich)
: Gibt den Namen des zurückzuschreibenden Datenträgers des primären Speicherpools an. Soll eine Liste mit Datenträgern angegeben werden, die zu demselben primären Speicherpool gehören, die Namen ohne Leerzeichen durch Kommas voneinander trennen.

COPYstgpool
: Gibt den Namen des Kopienspeicherpools an, aus dem die Dateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien aus jedem Kopienspeicherpool, in dem Kopien gefunden werden, zurückgeschrieben. Verwenden Sie diesen Parameter nicht mit den Parametern ACTIVEDATAONLY oder ACTIVEDATAPOOL.

ACTIVEDATAOnly
: Gibt an, dass aktive Versionen von Sicherungsdateien nur aus Pools für aktive Daten zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird dieser Parameter nicht angegeben, werden Dateien aus Kopienspeicherpools

zurückgeschrieben. Verwenden Sie diesen Parameter nicht mit dem Parameter COPYSTGPOOL. Gültige Werte:

No
: Gibt an, dass der Speicherpool nicht aus Pools für aktive Daten zurückgeschrieben wird.

Yes
: Gibt an, dass der Speicherpool aus Pools für aktive Daten zurückgeschrieben wird, die mit dem Parameter ACTIVEDATAPOOL angegeben werden. Wird YES als Wert für ACTIVEDATAONLY angegeben, aber wird kein Wert für ACTIVEDATAPOOL angegeben, werden Dateien aus jedem Pool für aktive Daten zurückgeschrieben, in dem aktive Versionen von Sicherungsdateien lokalisiert werden können.

Achtung: Das Zurückschreiben eines Datenträgers aus einem Pool für aktive Daten kann zur Folge haben, dass einige oder alle inaktiven Dateien aus der Datenbank gelöscht werden, wenn der Server bestimmt, dass eine inaktive Datei ersetzt werden muss, aber der Server die Datei im Pool für aktive Daten nicht finden kann.

ACTIVEDATAPool
: Gibt den Namen des Pools für aktive Daten an, aus dem die aktiven Versionen von Sicherungsdateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien aus jedem Pool für aktive Daten zurückgeschrieben, in dem aktive Versionen von Sicherungsdateien lokalisiert werden können.

NEWstgpool
: Gibt den Namen des neuen Speicherpools an, in den die Dateien zurückgeschrieben werden sollen. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, werden Dateien in den ursprünglichen primären Speicherpool zurückgeschrieben.

MAXPRocess
: Gibt die maximale Anzahl paralleler Prozesse für das Zurückschreiben von Dateien an. Mit Hilfe von parallelen Prozessen kann der Durchsatz verbessert werden. Dieser Parameter ist wahlfrei. Es kann ein Wert von 1 bis 999 angegeben werden. Der Standardwert ist 1.

  Bei der Bestimmung dieses Werts ist die Anzahl Mountpunkte (logische Laufwerke) und physischer Laufwerke zu berücksichtigen, die dieser Operation zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl verfügbarer Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect-Aktivitäten und Systemaktivitäten sowie von den Mountlimits der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Zurückschreibung betroffen sind.

  Jeder Prozess benötigt einen Mountpunkt für Datenträger aus dem Kopienspeicherpool. Lautet der Einheitentyp nicht FILE, benötigt jeder Prozess außerdem ein Laufwerk. Wird ein sequentieller Speicherpool zurückgeschrieben, benötigt jeder Prozess einen zusätzlichen Mountpunkt für Datenträger des primären Speicherpools und, falls der Einheitentyp nicht FILE lautet, ein zusätzliches Laufwerk. Beispiel: Angenommen, es werden maximal drei Prozesse für die Zurückschreibung eines primären sequentiellen Speicherpools aus einem Kopienspeicherpool mit derselben Einheitenklasse angegeben. Jeder Prozess benötigt zwei Mountpunkte und zwei Laufwerke. Um alle drei Prozesse ausführen zu können, muss das Mountlimit für die Einheitenklasse mindestens 6 betragen und es müssen mindestens 6 Mountpunkte und 6 Laufwerke verfügbar sein.

  Für die Voranzeige einer Zurückschreibung wird nur ein einziger Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

Preview
: Gibt an, ob eine Voranzeige der Zurückschreibung, nicht aber ihre Ausführung gewünscht wird. Mit dieser Option können die ausgelagerten Datenträger identifiziert werden, die zum Zurückschreiben eines Speicherpools erforderlich sind. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, dass die Operation zum Zurückschreiben ausgeführt werden soll.

  Yes
  : Gibt an, daß die Operation zum Zurückschreiben vorab angezeigt werden soll, ohne die Daten zurückzuschreiben.
    Tipp: Wird eine Zurückschreibung vorab angezeigt, um eine Liste der ausgelagerten Kopienpooldatenträger anzuzeigen, die geladen werden müssen, sollte der Zugriffsmodus der identifizierten Datenträger in UNAVAILABLE geändert werden. Dies verhindert so lange die Wiederherstellungs- und Datenversetzungsverarbeitung (MOVE DATA) für diese Datenträger, bis sie zur Verwendung bei der Zurückschreibungsverarbeitung zum Standort vor Ort transportiert werden.
    Die Voranzeige zeigt folgendes an:

    - Die Anzahl Dateien und Byte, die zurückgeschrieben werden sollen, wenn der Zugriffsmodus der Datenträger aus dem Kopienspeicherpool READWRITE oder READONLY lautet, wenn die Zurückschreibung ausgeführt wird.
    - Eine Liste der Datenträger aus dem Kopienspeicherpool, die Dateien enthalten, die zurückgeschrieben werden sollen. Diese Datenträger müssen geladen werden, wenn die Zurückschreibung ausgeführt wird.
    - Eine Liste der Datenträger mit Dateien, die nicht zurückgeschrieben werden können.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet.

    Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Bei dem Hintergrundprozess erstellte Nachrichten werden entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise einige Dateien bereits vor dem Abbruch gesichert.

Yes

Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Die Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungsclient an, wenn der Befehl beendet ist. Hinweis: Sie können nicht WAIT=YES an der Serverkonsole angeben.

Beispiel: Datendateien auf einem Primärdatenträger zurückschreiben

Dateien auf dem Datenträger PVOL2 im primären Speicherpool PRIMARY_POOL sollen zurückgeschrieben werden.

```
restore volume pvol2
```

Beispiel: Datendateien auf einem Primärdatenträger aus einem Pool für aktive Daten zurückschreiben

Dateien auf dem Datenträger VOL001 im primären Pool PRIMARY_POOL aus dem Pool für aktive Daten ADP1 zurückschreiben.

```
restore volume vol001 activedataonly=yes activedatapool=adp1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RESTORE VOLUME

Befehl	Beschreibung
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
RESTORE STGPOOL	Schreibt Dateien aus Kopienspeicherpools in einen primären Speicherpool zurück.

REVOKE-Befehle

Mit den REVOKE-Befehlen können Sie Berechtigungen oder den Zugriff widerrufen.

- REVOKE AUTHORITY (Administratorberechtigung entziehen)
- REVOKE PROXYNODE (Proxyberechtigung für einen Clientknoten entziehen)

REVOKE AUTHORITY (Administratorberechtigung entziehen)

Mit diesem Befehl können einem Administrator eine oder mehrere Berechtigungsklassen entzogen werden.

Sie können diesen Befehl auch verwenden, um die Anzahl der Maßnahmendomänen zu reduzieren, für die ein Administrator mit eingeschränkter Maßnahmenberechtigung berechtigt ist, und die Anzahl der Speicherpools zu reduzieren, für die ein Administrator mit eingeschränkter Speicherberechtigung berechtigt ist.

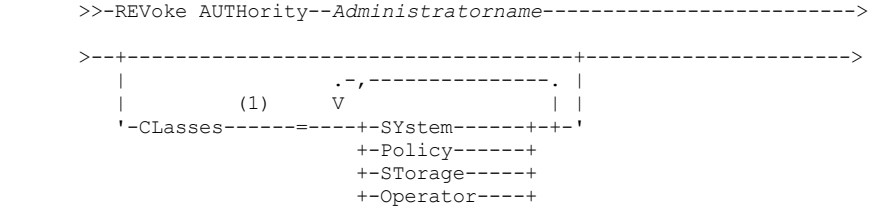
Wird der Befehl REVOKE AUTHORITY ohne die Parameter CLASSES, DOMAINS und STGPOOLS verwendet, werden dem angegebenen Administrator sämtliche Berechtigungen entzogen.

Mindestens ein Administrator muss über Systemberechtigung verfügen; diesem kann deshalb die Berechtigung nicht entzogen werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



```
                      '-Node--| A |-'

>--+-----------------------------+----------------------------->
   |             .-,-----------. |
   |             V             | |
   '-DOmains--=----Domänenname-+-'

>--+-------------------------------+--------------------------><
   |                   .-,--------. |
   |          (1)      V          | |
   '-STGpools------=----Poolname-+-'

A

   .-AUTHority--=--Access-----.
|--+--------------------------+--+-DOmains--=--Domänenname-+----|
   '-AUTHority--=--+-Access-+-'  '-NOde--=--Knotenname-----'
                   '-Owner--'
```

Anmerkungen:

1. Werden alle diese Parameter ausgelassen, werden diesem Administrator sämtliche Berechtigungen entzogen.

Parameter

Administratorname (Erforderlich)
Gibt den Namen des Administrators an, dessen Administratorberechtigung entzogen oder reduziert werden soll.

CLasses
Gibt eine oder mehrere Administratorberechtigungsklassen an, die entzogen werden sollen. Es können mehrere Klassen angegeben werden, indem die Klassen durch ein Komma voneinander getrennt werden.

SYstem
Gibt an, dass diesem Administrator die Systemberechtigung entzogen werden soll. Bei Angabe von CLASSES=SYSTEM können keine anderen Klassen angegeben werden und auch die Parameter DOMAINS und STGPOOLS können nicht angegeben werden.

Policy
Gibt an, dass diesem Administrator die Maßnahmenberechtigung entzogen werden soll. Sollen alle Maßnahmenberechtigungen entzogen werden, ist CLASSES=POLICY anzugeben. Der Parameter DOMAINS darf dann nicht angegeben werden.

STorage
Gibt an, dass diesem Administrator die Speicherberechtigung entzogen werden soll. Sollen alle Speicherberechtigungen entzogen werden, ist CLASSES=STORAGE anzugeben. Der Parameter STGPOOLS darf dann nicht angegeben werden.

Operator
Gibt an, dass diesem Administrator die Bedienerberechtigung entzogen werden soll.

Node
Gibt an, dass die Knotenberechtigung für diesen Benutzer entzogen werden soll.

AUTHority
Gibt die Berechtigungsstufe an, die für einen Benutzer mit Knotenberechtigung entzogen werden soll. Dieser Parameter ist wahlfrei.

Hat ein Administrator bereits die System- oder Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Knoten gehört, wird mit diesem Befehl die Berechtigung des Administrators nicht geändert.

Gültige Berechtigungsstufen sind:

Access
Gibt an, dass die Clientzugriffsberechtigung entzogen wird. Dies ist der Standardwert, wenn CLASSES=NODE angegeben wird.
Anmerkung: Ein Clientknoten kann die Option REVOKEREMOTEACCESS definieren, um den Zugriff eines Benutzers mit Knotenberechtigung und Clientzugriffsberechtigung zu verhindern. Hat ein Benutzer mit Knotenberechtigung die Client-Eignerberechtigung oder hat er die System- oder Maßnahmenberechtigung für die Maßnahmendomäne, zu der der Knoten gehört, kann dieser Administrator dennoch auf den Web-Client für Sichern/Archivieren zugreifen.

Owner
Gibt an, dass die Clienteignerberechtigung entzogen wird.

DOmains
Gibt an, dass die Clientzugriffsberechtigung oder Clienteignerberechtigung eines Administrators für alle Clients in der angegebenen Maßnahmendomäne entzogen werden soll. Dieser Parameter kann nicht zusammen mit dem Parameter NODE verwendet werden.

NOde
Gibt an, dass die Clientzugriffsberechtigung oder Clienteignerberechtigung eines Administrators für den Knoten entzogen werden soll. Dieser Parameter kann nicht zusammen mit dem Parameter DOMAIN verwendet werden.

DOmains

Gibt bei Verwendung mit CLASSES=POLICY eine Liste mit Maßnahmendomänen an, die von einem Administrator mit eingeschränkter Maßnahmenberechtigung nicht mehr verwaltet werden dürfen. (Der Administrator hatte die Berechtigung zum Verwalten dieser Domänen, bis der Befehl REVOKE ausgegeben wurde.) Dieser Parameter ist wahlfrei. Die Listeneinträge werden durch Kommas ohne Leerzeichen voneinander getrennt. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.Für alle übereinstimmenden Domänen wird die Berechtigung entzogen. Bei Angabe von DOMAINS ist der Parameter CLASSES=POLICY wahlfrei.

STGpools

Gibt eine Liste mit Speicherpools an, die von einem Administrator mit eingeschränkter Speicherberechtigung nicht mehr verwaltet werden dürfen. (Der Administrator hatte die Berechtigung zum Verwalten dieser Speicherpools, bis der Befehl REVOKE ausgegeben wurde.) Dieser Parameter ist wahlfrei. Die Listeneinträge werden durch Kommas ohne Leerzeichen voneinander getrennt. Es können Platzhalterzeichen verwendet werden, um einen Namen anzugeben.Für alle übereinstimmenden Speicherpools wird die Berechtigung entzogen. Bei Angabe von STGPOOLS ist der Parameter CLASSES=STORAGE wahlfrei.

Hinweise

1. Soll die uneingeschränkte Speicherberechtigung für eine Administrator in die eingeschränkte Speicherberechtigung geändert werden, muss mit diesem Befehl zunächst die uneingeschränkte Berechtigung entzogen werden. Danach ist es möglich, dem Administrator mit dem Befehl GRANT AUTHORITY eingeschränkte Speicherberechtigung zu erteilen und die Speicherpools anzugeben, für die der Administrator berechtigt sein soll.

   Soll einem Administrator die uneingeschränkte Speicherberechtigung entzogen werden, den Parameter CLASSES=STORAGE angeben. Der Parameter STGPOOLS kann nicht dazu verwendet werden, einem Administrator mit uneingeschränkter Speicherberechtigung die Berechtigung für ausgewählte Speicherpools zu entziehen.

2. Soll die uneingeschränkte Maßnahmenberechtigung für eine Administrator in die eingeschränkte Maßnahmenberechtigung geändert werden, muss mit diesem Befehl zunächst die uneingeschränkte Berechtigung entzogen werden. Danach ist es möglich, dem Administrator mit dem Befehl GRANT AUTHORITY eingeschränkte Maßnahmenberechtigung zu erteilen und die Maßnahmendomänen anzugeben, für die der Administrator berechtigt sein soll.

   Soll einem Administrator die uneingeschränkte Maßnahmenberechtigung entzogen werden, den Parameter CLASSES=POLICY angeben. Der Parameter DOMAINS kann nicht verwendet werden, um einem Administrator mit uneingeschränkter Berechtigung die Berechtigung für ausgewählte Domänen zu entziehen.

Beispiel: Bestimmte Administratorberechtigungen entziehen

Der Administratorin CLAUDIA soll ein Teil ihrer Berechtigungen entzogen werden. CLAUDIA hat eingeschränkte Maßnahmenberechtigung für die Maßnahmendomänen EMPLOYEE_RECORDS und PROG1. Ihre Maßnahmenberechtigung soll nun auf die Maßnahmendomäne EMPLOYEE_RECORDS beschränkt werden.

```
revoke authority claudia classes=policy
domains=employee_records
```

Beispiel: Alle Administratorberechtigungen entziehen

Der Administrator LARRY verfügt derzeit über Bedienerberechtigung und eingeschränkte Maßnahmenberechtigung. Ihm sollen jedoch alle Administratorberechtigungen entzogen werden. Um alle Berechtigungen zu entziehen, muss der Name des Administrators angegeben werden; es darf jedoch weder CLASSES noch DOMAINS noch STGPOOLS angegeben werden. LARRY bleibt dann zwar Administrator, aber er kann nur solche Befehle ausführen, die jeder andere Administrator auch ausführen kann.

```
revoke authority larry
```

Beispiel: Knotenberechtigung entziehen

Die Benutzerin CONNIE im Help Desk-Personal verfügt gegenwärtig über die Knotenberechtigung mit Client-Eignerberechtigung für den Client-Knoten WARD3. Ihr soll die Knotenberechtigung mit Client-Eignerberechtigung entzogen werden.

```
revoke authority connie classes=node
authority=owner node=ward3
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REVOKE AUTHORITY

Befehl	Beschreibung
GRANT AUTHORITY	Ordnet einem Administrator Berechtigungsklassen zu.
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.

REVOKE PROXYNODE (Proxyberechtigung für einen Clientknoten entziehen)

Verwenden Sie diesen Befehl, um die Berechtigung für einen Agentenclientknoten zur Ausführung von Sicherungs- und Zurückschreibungsoperationen für einen Zielknoten auf dem IBM Spectrum Protect-Server zu entziehen.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung

Syntax

```
>>-REVoke PROXynode TArget--=--Zielknotenname------------------>

>--AGent--=--Agentenknotenname--------------------------------><
```

Parameter

TArget (Erforderlich)
: Gibt den Zielknoten an, für den einem Agentenknoten die Proxyberechtigung erteilt wurde. Platzhalterzeichen und durch Kommas getrennte Listen mit Knotennamen sind zulässig.

AGent (Erforderlich)
: Gibt den Knoten an, der die Berechtigung als Proxy für den Zielknoten hat. Platzhalterzeichen und durch Kommas getrennte Listen mit Knotennamen sind zulässig.

Beispiel: Die Proxy-Berechtigung eines Knotens widerrufen

Um dem Zielknoten NASCLUSTER die Berechtigung als Proxy für alle Knoten zu entziehen, die mit dem Buchstaben M beginnen, geben Sie den folgenden Befehl aus.

```
revoke proxynode target=nascluster agent=m*
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für REVOKE PROXYNODE

Befehl	Beschreibung
GRANT PROXYNODE	Erteilt einem Agentenknoten die Proxyberechtigung.
QUERY PROXYNODE	Zeigt die Knoten an, die die Berechtigung als Proxyknoten haben.

ROLLBACK (Nicht festgeschriebene Änderungen in einem Makro rückgängig machen)

Mit diesem Befehl können innerhalb eines Makros Änderungen rückgängig gemacht werden, die von Befehlen, die vom Server ausgeführt wurden, vorgenommen, jedoch noch nicht in der Datenbank festgeschrieben wurden. Eine festgeschriebene Änderung ist permanent und kann nicht rückgängig gemacht werden. Der Befehl ROLLBACK ist für das Testen von Makros nützlich.

Bei Verwendung dieses Befehls muß sichergestellt werden, daß die Verwaltungs-Client-Sitzung nicht mit der Option ITEMCOMMIT ausgeführt wird.

Wichtig: SETOPT-Befehle innerhalb eines Makros können nicht rückgängig gemacht werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-ROLLBACK-------------------------------------------------><
```

Parameter

Keine.

Beispiel: Änderungen in einem Makro rückgängig machen

Für das Makro REGN soll der Befehl ROLLBACK ausgeführt werden, um zu bestätigen, dass das Makro keine Änderungen festschreibt. Der Makroinhalt lautet:

```
/* Mit dem Makro werden Maßnahmen-
administratoren registriert und Berechtigungen erteilt */
REGister Admin sara hobby
GRant AUTHority sara CLasses=Policy
REGister Admin ken plane
GRant AUTHority ken CLasses=Policy
ROLLBACK      /* verhindert, daß Änderungen festgeschrieben werden */
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für ROLLBACK

Befehl	Beschreibung
COMMIT	Schreibt Änderungen in der Datenbank fest.
MACRO	Führt eine angegebene Makrodatei aus.

Zugehörige Konzepte:
Makros des Verwaltungsclients

RUN (IBM Spectrum Protect-Prozedur ausführen)

Mit diesem Befehl kann eine IBM Spectrum Protect-Prozedur ausgeführt werden. Soll dieser Befehl auf einem anderen Server ausgegeben werden, muß die Prozedur, die ausgeführt wird, auf diesem Server definiert sein.

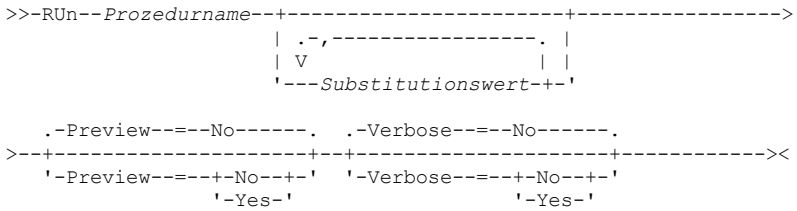
RUN-Befehle können in Prozeduren eingeschlossen werden, solange sie keine Schleifen erstellen. Beispielsweise sollten RUN-Befehle nicht eingeschlossen werden, wenn die Prozedur SCRIPT_A die Prozedur SCRIPT_B und die Prozedur SCRIPT_B die Prozedur SCRIPT_A ausführt.

Wichtig: IBM Spectrum Protect verfügt über keinen Befehl, mit dem ein Script nach dem Starten abgebrochen werden kann. Um ein Script zu stoppen, muss der Server angehalten werden.

Berechtigungsklasse

Für diesen Befehl ist die Bediener-, Maßnahmen-, System- oder Speicherberechtigung erforderlich.

Syntax



Parameter

Prozedurname (Erforderlich)
: Gibt den Namen der Prozedur an, die verarbeitet werden soll. Der angegebene Name darf keine Substitutionsvariable wie beispielsweise $1 sein.

Substitutionswert
: Gibt einen oder mehrere Substitutionswerte für Variablen an, wenn die Prozedur ausgeführt wird. In einer Prozedur besteht eine Substitutionsvariable aus dem Zeichen '$' gefolgt von einer Zahl. Bei der Ausführung der Prozedur ersetzt IBM Spectrum Protect die in einer Prozedur definierten Substitutionsvariablen durch die Werte, die mit diesem Befehl angegeben werden. Für jede in der Prozedur definierte Substitutionsvariable müssen Werte angegeben werden. Andernfalls schlägt die Prozedur fehl. Dieser Parameter ist wahlfrei.

Preview
: Gibt an, ob die Befehlszeilen einer Prozedur vorab angezeigt werden sollen, ohne die Prozedur tatsächlich zu verarbeiten. Der Standardwert ist NO.
Gültige Werte:

  Yes
  : Gibt an, daß die in einer Prozedur enthaltenen Befehlszeilen angezeigt werden, die Prozedur jedoch nicht verarbeitet wird.

  No

Gibt an, daß die in einer Prozedur enthaltenen Befehlszeilen angezeigt werden und die Prozedur verarbeitet wird.

Verbose
: Gibt an, ob die Befehlszeilen, die Variablensubstitution und die Tests der bedingten Logik, die in einer Prozedur verwendet werden, angezeigt werden, wenn die Prozedur verarbeitet wird. Dieser Parameter wird ignoriert, wenn PREVIEW=YES angegeben wird. Der Standardwert ist NO.
Gültige Werte:

  Yes
  : Gibt an, daß die Befehlszeilen, die Variablensubstitution und die Tests der bedingten Logik angezeigt werden, wenn die Prozedur verarbeitet wird.

  No
  : Gibt an, daß die Befehlszeilen, die Variablensubstitution und die Tests der bedingten Logik nicht angezeigt werden, wenn die Prozedur verarbeitet wird.

Beispiel: Die Befehle anzeigen, die von einem Script mit einer Substitutionsvariablen für den Tabellennamen generiert werden

Um das folgende Beispielscript mit dem Namen QSAMPLE auszuführen, geben Sie einen Befehl RUN aus, der den Tabellennamen ACTLOG als Wert für die Substitutionsvariable $1 angibt. Verwenden Sie die Ausgabe, um die Befehle voranzuzeigen, die von dem Script generiert werden, bevor die Befehle ausgeführt werden.

```
001  /* SQL-Beispielabfrage im breiten Format*/
005  SET SQLDISPLAYMODE WIDE
010  SELECT colname FROM -
015  COLUMNS WHERE TABNAME='$1'
```

```
run qsample actlog preview=yes
```

```
ANR1461I RUN: Befehlsprozedur QSAMPLE wird ausgeführt.
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 5 :
              set sqldisplaymode wide.
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 15 :
              select colname from columns where tabname='ACTLOG'.
ANR1470I RUN: Befehlsprozedur QSAMPLE erfolgreich ausgeführt
              (Modus PREVIEW)
```

Beispiel: Ein Script ausführen, um die Befehle anzuzeigen und auszuführen, die von dem Script generiert werden

Führen Sie dasselbe Script wie im vorherigen Beispiel aus, um sowohl die generierten Befehle als auch die Ergebnisse der Befehle anzuzeigen.

```
run qsample actlog verbose=yes
```

```
ANR1461I RUN: Befehlsprozedur QSAMPLE wird ausgeführt.
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 5 :
              set sqldisplaymode wide.
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 5 : RC=RC_OK
ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 15 :
              select colname from columns where tabname='ACTLOG'.

COLNAME
------------------
DATE_TIME
MSGNO
SEVERITYMESSAGE
ORIGINATOR
NODENAME
OWNERNAME
SCHEDNAME
DOMAINNAME
SESSID

ANR1466I RUN: Befehlsprozedur QSAMPLE, Zeile 15 : RC=RC_OK
ANR1462I RUN: Befehlsprozedur QSAMPLE erfolgreich ausgeführt.
```

Beispiel: Ein Script ausführen, um nur die Ergebnisse der Befehle in dem Script anzuzeigen

Führen Sie das vorherige Beispielscript aus, um nur die Ergebnisse der generierten Befehle in dem Script anzuzeigen.

```
run qsample actlog verbose=no
```

```
COLNAME
------------------
DATE_TIME
MSGNO
```

```
SEVERITYMESSAGE
ORIGINATOR
NODENAME
OWNERNAME
SCHEDNAME
DOMAINNAME
SESSID

ANR1462I RUN: Befehlsprozedur QSAMPLE erfolgreich ausgeführt.
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für RUN

Befehl	Beschreibung
COPY SCRIPT	Erstellt eine Kopie einer Prozedur.
DEFINE SCRIPT	Definiert eine Prozedur für den IBM Spectrum Protect-Server.
DELETE SCRIPT	Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur.
QUERY SCRIPT	Zeigt Informationen über Prozeduren an.
RENAME SCRIPT	Vergibt einen neuen Namen für eine Prozedur.
UPDATE SCRIPT	Ändert Zeilen oder fügt Zeilen in einer Prozedur hinzu.

Zugehörige Tasks:
Server-Script ausführen

SELECT (SQL-Abfrage für die IBM Spectrum Protect-Datenbank ausführen)

Verwenden Sie den Befehl SELECT, um eine angepasste Abfrage der IBM Spectrum Protect-Datenbank zu erstellen und zu formatieren.

IBM Spectrum Protect stellt eine SQL-Schnittstelle zu einem DB2-Programm zur Verfügung. Einschränkungen und Richtlinien für die Handhabung von SQL-Abfragen werden direkt von DB2 gesteuert.

Als Hilfestellung für das Auffinden der verfügbaren Informationen stellt IBM Spectrum Protect drei Systemkatalogtabellen zur Verfügung:

SYSCAT.TABLES
: Enthält Informationen zu allen Tabellen, die mit dem Befehl SELECT abgefragt werden können.

SYSCAT.COLUMNS
: Beschreibt die Spalten in jeder Tabelle.

Diese Tabellen können mit dem Befehl SELECT abgefragt werden, um die Position von gewünschten Informationen zu ermitteln.

Hinweise

Der Befehl SELECT kann nicht von einer Serverkonsole ausgegeben werden.

Da der Befehl SELECT keine Sätze sperrt und entsperrt, kann ein Konflikt bei einem Satz dazu führen, dass der Server fälschlicherweise die Nachricht ANR2034E ausgibt: `SELECT: Keine Übereinstimmung mit diesen Kriterien gefunden.` Überprüfen Sie Ihre Auswahlkriterien und wiederholen Sie den Befehl, wenn sie korrekt sind.

Um die Verarbeitung eines Befehls SELECT nach dem Start zu stoppen, brechen Sie die Verwaltungssitzung ab, in der der Befehl ausgegeben wurde. Die Sitzung entweder von der Server-Konsole oder einer anderen Verwaltungssitzung abbrechen.

Temporäre Tabellenbereiche werden verwendet, um SQL-Abfragen innerhalb von DB2 zu verarbeiten. Unzureichender temporärer Speicherbereich kann zur Folge haben, dass SQL-Abfragen fehlschlagen.

Um die Ausgabe in eine durch Kommas getrennte Datei für den Import in ein Spreadsheet zu exportieren, verwenden Sie die Befehlszeilenoptionen -comma und > im Befehl dsmadmc.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

Informationen zur Syntax und zu Richtlinien für die Anweisung SELECT finden Sie in der Produktinformation zu DB2.

Wichtig: Die gültige Syntax für die mit Zeitmarke versehene Anweisung SELECT lautet:

```
SELECT * FROM SUMMARY WHERE ACTIVTY='EXPIRATION' AND START_TIME >'2009-05-10 00:00:00' AND START_TIME <'2009-
05-11 23:23:23'
```

Liste der Beispiele

Mit dem Befehl SELECT kann eine Vielzahl von Abfragen angepasst werden. Die nachfolgend gezeigten Beispiele lassen die Vielseitigkeit dieses Befehls ahnen. Er bietet jedoch noch wesentlich mehr Möglichkeiten. Lediglich für die komplexeren Befehle werden die Ausgabedaten aus der Abfrage gezeigt, um das Ausgabeformat zu illustrieren.

In der folgenden Liste sind die SELECT-Beispielbefehle zusammengefasst:

- Kennwörter für Administrator-IDs auflisten, die mit einem externen LDAP-Verzeichnisserver authentifiziert werden
- Verfügbare Tabellen auflisten
- Clientknoten und Verwaltungsclients auflisten, die gegenwärtig für den Serverzugriff gesperrt sind
- Clientknoten und Verwaltungsclients auflisten, die in jüngster Zeit nicht das korrekte Kennwort angegeben haben
- Knoten in der Maßnahmendomäne STANDARD auflisten, die nicht dem täglichen Sicherungszeitplan DAILYBACKUP zugeordnet sind
- Die Administratoren auflisten, die über Maßnahmenberechtigung verfügen
- Nachrichten des Typs E (FEHLER) oder W (WARNUNG) auflisten, die in dem Zeitraum ausgegeben wurden, für den Aktivitätenprotokollsätze aufbewahrt wurden
- Die Verwaltungszeitpläne auflisten, die vom Administrator JAKE definiert oder geändert wurden
- Die relativen Prioritäten der Verwaltungszeitpläne auflisten
- Die Verwaltungsklassen auflisten, die eine Archivierungskopiengruppe mit einem Aufbewahrungszeitraum von mehr als 365 Tagen haben
- Die Clientknoten auflisten, die sich in jeder Maßnahmendomäne befinden
- Die Anzahl der Dateien bestimmen, die von jedem Knoten archiviert wurden
- Die Clients auflisten, die die Speicherverwaltung verwenden
- Bestimmen, wie viele Datenträger wiederhergestellt würden, wenn der Wiederherstellungsschwellenwert für Speicherpool TAPE in 50 Prozent geändert wird
- Bestimmen, wie viele Sicherungsdateien für jeden Knoten betroffen wären, wenn die Verwaltungsklasse DAILY in der Maßnahmendomäne STANDARD geändert oder gelöscht würde
- Für alle aktiven Clientsitzungen bestimmen, wie lange sie verbunden waren und wie hoch ihr effektiver Durchsatz in Byte pro Sekunde war
- Bestimmen, wie lange die aktuellen Hintergrundprozesse ausgeführt wurden und wie hoch ihr effektiver Durchsatz in Zeit und Dateien pro Sekunde war
- Die Anzahl der Clientknoten für jeden Plattformtyp bestimmen
- Die Anzahl der Dateibereiche bestimmen, die jeder Clientknoten hat, und die Clientknoten in aufsteigender Reihenfolge auflisten
- Statistische Informationen zur Berechnung der Anzahl ausgelagerter Datenträger abrufen, deren Speicherbereich während der Wiederherstellung eines Speicherpools wiederhergestellt wird
- Detailsätze zur PVU-Schätzung abrufen
- Informationen zu den Knotenrollen abrufen
- Informationen zum Status abrufen

Beispiel: Administrator-IDs auflisten, die sich mit dem IBM Spectrum Protect-Server authentifizieren

Alle Administrator-IDs auflisten, deren Kennwörter mit dem IBM Spectrum Protect-Server authentifiziert werden:

```
select admin_name from admins where
authentication=local
```

Beispiel: Verfügbare Tabellen auflisten

Alle Tabellen auflisten, die für das Abfragen der IBM Spectrum Protect-Datenbank verfügbar sind.

```
select * from syscat.tables

      ABSCHEMA: SERVER1
       TABNAME: ACTLOG
   CREATE_TIME: 1999-05-01 07:39:06
      COLCOUNT: 10
INDEX_COLCOUNT: 1
  UNIQUE_INDEX: FALSE
       REMARKS: Server-Aktivitätenprotokoll

     TABSCHEMA: SERVER1
       TABNAME: ADMIN_SCHEDULES
   CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 14
INDEX_COLCOUNT: 1
  UNIQUE_INDEX: TRUE
       REMARKS: Verwaltungsbefehlzeitpläne

     TABSCHEMA: SERVER1
       TABNAME: ADMINS
   CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 15
INDEX_COLCOUNT: 1
  UNIQUE_INDEX: TRUE
       REMARKS: Server-Administratoren
```

```
     TABSCHEMA: SERVER1
       TABNAME: ARCHIVES
   CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 10
INDEX_COLCOUNT: 5
  UNIQUE_INDEX: FALSE
       REMARKS: Client-Archivierungsdateien
```

Beispiel: Clientknoten und Verwaltungsclients auflisten, die gegenwärtig für den Serverzugriff gesperrt sind

```
select node_name from nodes where locked='YES'

select admin_name from admins where locked='YES'
```

Beispiel: Clientknoten, Verwaltungsclients und Server auflisten, die die Sitzungssicherheit 'Transitional' (Vorübergehend) verwenden

```
select node_name from nodes where session_security='Transitional'

select admin_name from admins where session_security='Transitional'

select server_name from servers where session_security='Transitional'
```

Beispiel: Clientknoten und Verwaltungsclients auflisten, die in jüngster Zeit nicht das korrekte Kennwort angegeben haben

```
select node_name from nodes where invalid_pw_count <>0

select admin_name from admins where invalid_pw_count <>0
```

Beispiel: Knoten in der Maßnahmendomäne STANDARD auflisten, die nicht dem täglichen Sicherungszeitplan DAILYBACKUP zugeordnet sind

```
select node_name from nodes where domain_name='STANDARD' and
node_name not in (select node_name from associations
where domain_name='STANDARD' and
schedule_name='DAILYBACKUP')
```

Beispiel: Die Administratoren auflisten, die über Maßnahmenberechtigung verfügen

```
select admin_name from admins where
upper(system_priv) <>'NO'
or upper(policy_priv) <>'NO'
```

Beispiel: Nachrichten des Typs E (FEHLER) oder W (WARNUNG) auflisten, die in dem Zeitraum ausgegeben wurden, für den Aktivitätenprotokollsätze aufbewahrt wurden

```
select date_time,msgno,message from actlog
where severity='E' or severity='W'
```

Beispiel: Die Verwaltungszeitpläne auflisten, die vom Administrator JAKE definiert oder geändert wurden

```
select schedule_name from admin_schedules
where chg_admin='JAKE'
```

Beispiel: Die relativen Prioritäten der Verwaltungszeitpläne auflisten

```
select schedule_name,priority from admin_schedules order
by priority
```

Beispiel: Die Verwaltungsklassen auflisten, die eine Archivierungskopiengruppe mit einem Aufbewahrungszeitraum von mehr als 365 Tagen haben

```
select domain_name,set_name,class_name from ar_copygroups
where retver='NOLIMIT' or cast(retver as integer) >365
```

Beispiel: Die Verwaltungsklassen auflisten, die mehr als fünf Sicherungsversionen angeben

```
select domain_name,set_name,class_name from bu_copygroups
where verexists = 'NOLIMIT' or
cast(verexists as integer)>5
```

Beispiel: Die Clientknoten auflisten, die die Clientoptionsgruppe SECURE verwenden

```
select node_name from nodes where option_set='SECURE'
```

Beispiel: Die Clientknoten auflisten, die sich in jeder Maßnahmendomäne befinden

```
select domain_name,num_nodes from domains
```

Beispiel: Die Anzahl der Dateien bestimmen, die von jedem Knoten archiviert wurden

Achtung: Die Ausführung dieses Befehls nimmt unter Umständen viel Zeit in Anspruch.

```
select node_name,count(*) from archives
group by node_name
```

Beispiel: Die Clients auflisten, die die Speicherverwaltung verwenden

```
select node_name from auditocc where spacemg_mb <>0
```

Beispiel: Bestimmen, wie viele Datenträger wiederhergestellt würden, wenn der Wiederherstellungsschwellenwert für Speicherpool TAPE in 50 Prozent geändert wird

```
select count(*) from volumes where stgpool_name='TAPE'
and upper(status)='FULL' and pct_utilized < 50
```

Beispiel: Bestimmen, wie viele Sicherungsdateien für jeden Knoten betroffen wären, wenn die Verwaltungsklasse DAILY in der Maßnahmendomäne STANDARD geändert oder gelöscht würde

Anmerkung: Die Ausführung dieses Befehls nimmt viel Zeit und viele Ressourcen in Anspruch.

```
select node_name, count(*) as "Files" from backups
where class_name='DAILY' and node_name in
(select node_name from nodes where domain_name='STANDARD')
group by node_name
```

Beispiel: Für alle aktiven Clientsitzungen bestimmen, wie lange sie verbunden waren und wie hoch ihr effektiver Durchsatz in Byte pro Sekunde war

```
select session_id as "Session",
client_name as "Client",
state as "State",
current_timestamp-start_time as "Elapsed Time",
(cast(bytes_sent as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes sent/second",
(cast(bytes_received as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes received/second"
from sessions
```

```
                Sitzung: 24
                    Client: ALBERT
                    Status: Run
               Antwortzeit: 0 01:14:05.000000
        Byte gesendet (Sek): 564321.9302768451
      Byte empfangen (Sek): 0.0026748857944

                Sitzung: 26
                 Client: MILTON
                 Status: Run
            Antwortzeit: 0 00:06:13.000000
     Byte gesendet (Sek): 1638.5284210992221
   Byte empfangen (Sek): 675821.6888561849
```

Beispiel: Bestimmen, wie lange die aktuellen Hintergrundprozesse ausgeführt wurden und wie hoch ihr effektiver Durchsatz in Zeit und Dateien pro Sekunde war

Anmerkung: Beim Verfall wird die Anzahl der verarbeiteten Byte nicht angegeben.

```
select process_num as "Number",
   process,
current_timestamp-start_time as "Elapsed Time",
   (cast(files_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
   as "Files/second",
   (cast(bytes_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
   as "Bytes/second"
   from processes

          Nummer: 1
             PROCESS: Expiration
         Antwortzeit: 0 00:24:36.000000
     Dateien/Sekunde: 6.3216755870092
        Byte/Sekunde: 0.0000000000000
```

Beispiel: Die Anzahl der Clientknoten für jeden Plattformtyp bestimmen

```
select platform_name,count(*) as "Number of Nodes"
from nodes group by platform_name

PLATFORM_NAME     Anzahl Knoten
-------------     ---------------

  AIX                      6
  SunOS                   27
  Win32                   14
  Linux                   20
```

Beispiel: Die Anzahl der Dateibereiche bestimmen, die jeder Clientknoten hat, und die Clientknoten in aufsteigender Reihenfolge auflisten

```
select node_name, count(*) as "number of filespaces"
from filespaces group by node_name order by 2

NODE_NAME              Anzahl Dateibereiche
------------------     --------------------
    ALBERT                    2
    MILTON                    2
    BARNEY                    3
    SEBASTIAN                 3
    MAILHOST                  4
    FALCON                    4
    WILBER                    4
    NEWTON                    4
    JEREMY                    4
    WATSON                    5
        RUSSELL                                5
```

Beispiel: Statistische Informationen zur Berechnung der Anzahl ausgelagerter Datenträger abrufen, deren Speicherbereich während der Wiederherstellung eines Speicherpools wiederhergestellt wird

```
select * from summary where activity='OFFSITE RECLAMATION'

           START_TIME: 2004-06-16 13:47:31.000000
                       END_TIME: 2004-06-16 13:47:34.000000
                       ACTIVITY: OFFSITE RECLAMATION
                         NUMBER: 4
                         ENTITY: COPYPOOL
                       COMMMETH:
                        ADDRESS:
                 SCHEDULE_NAME:
                       EXAMINED: 170
                       AFFECTED: 170
                      FAILED: 0
                            BYTES: 17821251
                             IDLE: 0
                            MEDIAW: 0
                          PROCESSES: 2
                    SUCCESSFUL: YES
                   VOLUME_NAME:
                    DRIVE_NAME:
                  LIBRARY_NAME:
                      LAST_USE:
                          COMM_WAIT:
                   NUM_OFFSITE_VOLS: 2
```

Beispiel: Die Speicherpools identifizieren, die von Clients deduplizierte Daten enthalten

```
select stgpool_name,has_client_dedup_data from stgpools

Speicherpoolname            hat vom Client deduplizierte Daten
--------------------        --------------------
ADPOOL                      NO
ARCHIVEPOOL                 NO
BACKUPPOOL                  NO
COPYDEDUP                   NO
COPYNODEDUP                 NO
FILEPOOL                    YES
FILEPOOL2                   NO
LANFREEFILEPOOL             YES
SPACEMGPOOL                 NO
```

Beispiel: Informationen zur Datenbank abrufen

```
select * from db

       DATABASE_NAME: TSMDB1
  TOT_FILE_SYSTEM_MB: 2048000
    USED_DB_SPACE_MB: 12576
       FREE_SPACE_MB: 1576871
         TOTAL_PAGES: 983044
        USABLE_PAGES: 982908
          USED_PAGES: 977736
          FREE_PAGES: 5172
      BUFF_HIT_RATIO: 96.2
      TOTAL_BUFF_REQ: 53967
       SORT_OVERFLOW: 0
     LOCK_ESCALATION: 0
       PKG_HIT_RATIO: 70.0
          LAST_REORG: 2010-07-15 17:32:55.000000
      FULL_DEV_CLASS: OUTFILE
     NUM_BACKUP_INCR: 0
    LAST_BACKUP_DATE: 2010-01-21 10:37:59.000000
    PHYSICAL_VOLUMES: 0
           PAGE_SIZE:
  NUM_BACKUP_STREAMS: 4
```

Beispiel: Detailsätze zur Prozessor-Value-Unit-Schätzung abrufen

Die PVU-Schätzung für den Knoten ACCTSRECSRV generieren, der von dem Produkt IBM Spectrum Protect Extended Edition verwendet wird.

```
select * from pvuestimate_details where node_name='ACCTSRECSRV'

           PRODUCT: PRODEE
      LICENSE_NAME: MGSYSLAN
         NODE_NAME: ACCTSRECSRV
         LAST_USED: 2008-01-20 16:12:24.000000
            TRYBUY: FALSE
       PROC_VENDOR: IBM
        PROC_BRAND: POWER5+ QCM
         PROC_TYPE: 4
        PROC_MODEL:
        PROC_COUNT: 2
              ROLE: SERVER
     ROLE_OVERRIDE: USEREPORTED
    ROLE_EFFECTIVE: SERVER
       VALUE_UNITS: 50
  VALUE_FROM_TABLE: YES
               PVU: 100
      SCAN_ERROR : NO
       API_CLIENT: NO
     PVU_AGNOSTIC: NO
       HYPERVISOR: VMWARE
             GUID: 01.2e.1c.80.e5.04-
                    .11.da.aa.ab.00.-
                    15.58.0b.d9.47
          VERSION: 6
          RELEASE: 3
            LEVEL: 1
         VENDOR_D: IBM(R)
          BRAND_D: POWER5(TM) QCM
           TYPE_D: Quad-core Module
          MODEL_D: All Existing
        PRODUCT_D: IBM Spectrum Protect Extended Edition
```

Feldbeschreibungen

PRODUCT
: Rollup der Lizenztypen nach Produkten auf der im Befehl QUERY PVUESTIMATE angegebenen Ebene. Gültige Werte sind PRODEE, PRODBASIC, PRODDATARET, PRODMAIL, PRODDB, PRODSYSB, PRODSPACE, PRODSAN, PRODERP oder leer.

LICENSE_NAME
: Die Lizenz, die diesem Knoten zugeordnet ist.

NODE_NAME
: Der Knotenname.

LAST_USED
: Datum und Uhrzeit, an dem bzw. zu der der angegebene Knoten zum letzten Mal unter dieser Lizenz die Verbindung zum System hergestellt hat.

TRYBUY
: Gibt an, ob die Lizenz eine Probelizenz ist. Gültige Werte sind TRUE oder FALSE.

PROC_VENDOR
: Der Name des vom Client zurückgemeldeten Prozessorherstellers.

PROC_BRAND
: Der Name der vom Client zurückgemeldeten Prozessormarke.

PROC_TYPE
: Der vom Client zurückgemeldete Prozessortyp. Dieser Wert spiegelt auch die Anzahl der Kerne wieder. Beispielwerte sind 1=SINGLE CORE, 2=DUO CORE und 4=QUAD CORE.

PROC_MODEL
: Das vom Client zurückgemeldete Prozessormodell.

PROC_COUNT
: Die Anzahl der Prozessoren.

ROLE
: Die Knotenrolle. Gültige Werte sind CLIENT, SERVER oder OTHER.

ROLE_OVERRIDE
: Der im Befehl UPDATE NODE angegebene Überschreibungswert.

ROLE_EFFECTIVE
: Tatsächliche Rolle auf der Basis der Werte in den Feldern ROLE und ROLE_OVERRIDE.

VALUE_UNITS
: Die zugeordnete Prozessor-Value-Unit (PVU) für den Prozessor.

PVU
: Der berechnete PVU-Wert.

  ```
  PVU pro Knoten = Anzahl Prozessoren pro Knoten * Prozessortyp * PVU-Wert
  ```

  Dabei stellt der `Prozessortyp` die Anzahl der Kerne dar, und der `PVU-Wert` ist der Wert, der für den Prozessortyp in der IBM® PVU-Tabelle definiert ist.

VALUE_FROM_TABLE
: Markierung, die angibt, ob die Prozessor-Value-Unit auf der Basis der IBM PVU-Tabelle berechnet wurde. Gültige Werte sind YES oder NO. Bei NO wird ein Wert von 100 für jeden Knoten angewendet, der als Server definiert ist. Ist keine Rolle für einen Knoten definiert, wird die Rolle 'Server' zum Zweck der PVU-Berechnung angenommen.

SCAN_ERROR
: Markierung, die angibt, ob Lizenzinformationen vom Client zurückgemeldet wurden. Gültige Werte sind YES oder NO.

API_CLIENT
: Markierung, die eine API-Anwendung angibt. Gültige Werte sind YES oder NO.

PVU_AGNOSTIC
: Markierung, die angibt, dass der Release-Level der Clientversion vor IBM Spectrum Protect Version 6.3 liegt. Liegt die Version vor Version 6.3, werden keine gültigen PVU-Messwerte erwartet. Gültige Werte sind YES oder NO.

HYPERVISOR
: Der Name der vom Client zurückgemeldeten VM-Software.

GUID
: Global eindeutige ID (GUID) des Computers, auf dem sich der Knoten befindet. Die GUID wird aus der Knotentabelle abgerufen.

VERSION
: Die Version des Clients.

RELEASE
: Das Release des Clients.

LEVEL
: Die Stufe des Clients.

VENDOR_D
: Der Anzeigewert für den Prozessorhersteller aus der PVU-Tabelle.

BRAND_D
: Der Anzeigewert für die Prozessormarke aus der PVU-Tabelle.

TYPE_D
: Der Anzeigewert für den Prozessortyp aus der PVU-Tabelle.

MODEL_D
: Der Anzeigewert für das Prozessormodell aus der PVU-Tabelle.

PRODUCT_D
: Der Anzeigewert für das Produkt aus der PVU-Tabelle. Die folgenden Werte sind gültig:

- IBM Spectrum Protect
- IBM Spectrum Protect Extended Edition
- IBM Spectrum Protect for Data Retention
- IBM Spectrum Protect for SAN
- IBM Spectrum Protect for Space Management
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for System Backup and Recovery
- Leer

Beispiel: Informationen zur Rolle und PVU-bezogene Informationen anfordern

Das folgende Beispiel zeigt Teilergebnisse für einen ausgewählten Knoten, einschließlich PVU-bezogene Informationen und Rolleninformationen. Gültige Rollen sind CLIENT, SERVER oder OTHER. Die Prozessor-Value-Unit wird nur für Knoten berechnet, die als Server definiert sind.

```
select * from nodes

  ROLE: CLIENT
     ROLE_O: USEREPORTED
    PVENDOR: INTEL
     PBRAND: INTEL
      PTYPE: 4
     PMODEL:
     PCOUNT: 1
 HYPERVISOR:
       PAPI: NO
 SCANERROR: NO
```

SET-Befehle

Mit den SET-Befehlen können Sie Werte angeben, die viele verschiedene IBM Spectrum Protect-Operationen betreffen.

- SET ACCOUNTING (Abrechnungssätze aktivieren/inaktivieren)
- SET ACTLOGRETENTION (Aufbewahrungsdauer für das Aktivitätenprotokoll definieren)
- SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)
- SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)
- SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)
- SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)
- SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)
- SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)
- SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)
- SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)
- SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)
- SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)
- SET ARCHIVERETENTIONPROTECTION (Aufbewahrungsschutz für Daten aktivieren)
- SET ARREPLRULEDEFAULT (Serverreplikationsregel für Archivierungsdaten definieren)
- SET BKREPLRULEDEFAULT (Serverreplikationsregel für Sicherungsdaten definieren)
- SET CLIENTACTDURATION (Verweildauer für Clientaktion definieren)
- SET CONFIGMANAGER (Konfigurationsmanager angeben)
- SET CONFIGREFRESH (Aktualisierung der Konfiguration verwalteter Server definieren)
- SET CONTEXTMESSAGING (Anzeigen von Nachrichtenkontext aktivieren oder inaktivieren)
- SET CPUINFOREFRESH (Aktualisierungsintervall für Informationssuche auf Client-Workstation)
- SET CROSSDEFINE (Querdefinition von Servern angeben)
- SET DBRECOVERY (Einheitenklasse für automatische Sicherungen definieren)
- SET DEDUPVERIFICATIONLEVEL (Prozentsatz der zu prüfenden Bereiche definieren)
- SET DEFAULTAUTHENTICATION (Standardauthentifizierungsmethode für Befehle REGISTER NODE und REGISTER ADMIN definieren)
- SET DISSIMILARPOLICIES (Die Maßnahmen auf dem Zielreplikationsserver für die Verwaltung replizierter Daten aktivieren)
- SET DRMACTIVEDATASTGPOOL (Von DRM zu verwaltende Pools für aktive Daten angeben)
- SET DRMCHECKLABEL (Kennsatzprüfung angeben)
- SET DRMCMDFILENAME (Namen einer Datei angeben, die Befehle enthalten soll)
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeSET DRMCOPYCONTAINERSTGPOOL (Containerkopienspeicherpools angeben, die von DRM-Befehlen verarbeitet werden sollen)
- SET DRMCOPYSTGPOOL (Von DRM zu verwaltende Kopienspeicherpools angeben)
- SET DRMCOURIERNAME (Kuriernamen angeben)
- SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsserie angeben)
- SET DRMFILEPROCESS (Dateiverarbeitung angeben)
- SET DRMINSTRPREFIX (Präfix für Wiederherstellungsanweisungsdateinamen angeben)
- SET DRMNOTMOUNTABLENAME (Nicht mountfähigen Standort angeben)
- SET DRMPLANPREFIX (Präfix für Wiederherstellungsplandateinamen angeben)

- SET DRMPLANVPOSTFIX (Namen für Ersatzdatenträger angeben)
- SET DRMPRIMSTGPOOL (Von DRM zu verwaltende primäre Speicherpools angeben)
- SET DRMRPFEXPIREDAYS (Kriterien für Verfall von Wiederherstellungsplandateien definieren)
- SET DRMVAULTNAME (Aufbewahrungsort angeben)
- SET EVENTRETENTION (Aufbewahrungszeitraum für Ereignissätze definieren)
- SET FAILOVERHLADDRESS (Adresse höherer Ebene für Übernahme definieren)
- SET INVALIDPWLIMIT (Anzahl der ungültigen Anmeldeversuche definieren)
- SET LDAPPASSWORD (LDAP-Kennwort für den Server definieren)
- SET LDAPUSER (ID für einen LDAP-Verzeichnisserver angeben)
- SET LICENSEAUDITPERIOD (Dauer für Lizenzprüfung definieren)
- SET MAXCMDRETRIES (Maximale Anzahl Befehlswiederholungen definieren)
- SET MAXSCHEDSESSIONS (Maximale Anzahl geplanter Sitzungen definieren)
- SET MINPWLENGTH (Mindestlänge für Kennwort definieren)
- SET MONITORINGADMIN (Name des Überwachungsadministrators definieren)
- SET MONITOREDSERVERGROUP (Gruppe überwachter Server definieren)
- SET NODEATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen Knoten an)
- SET PASSEXP (Ablaufdatum für Kennwort definieren)
- SET PRODUCTOFFERING (Produktangebot definieren, das für Ihr Unternehmen lizenziert ist)
- SET QUERYSCHEDPERIOD (Zeitraum für Abfrage von Clientknoten definieren)
- SET RANDOMIZE (Zufallsgenerierung von geplanten Startzeiten definieren)
- SET REPLRECOVERDAMAGED (Angeben, ob beschädigte Dateien von einem Replikationsserver wiederhergestellt werden)
- SET REPLRETENTION (Aufbewahrungszeitraum für Replikationsdatensätze definieren)
- SET REPLSERVER (Zielreplikationsserver definieren)
- SET RETRYPERIOD (Zeitintervall zwischen Wiederholungsversuchen definieren)
- SET SCHEDMODES (Modus für zentrale Zeitplanung auswählen)
- SET SERVERHLADDRESS (Serveradresse der höheren Ebene definieren)
- SET SERVERLLADDRESS (Serveradresse der unteren Ebene definieren)
- SET SERVERNAME (Servernamen angeben)
- SET SERVERPASSWORD (Kennwort für Server definieren)
- SET SPREPLRULEDEFAULT (Serverreplikationsregel für speicherverwaltete Daten definieren)
- SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)
- SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)
- SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)
- SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)
- SET SUBFILE (Subdateisicherung für Clientknoten definieren)
- SET SUMMARYRETENTION (Anzahl Tage für Aufbewahren in Aktivitätsübersichtstabelle definieren)
- SET TAPEALERTMSG (Bandalerts aktivieren oder inaktivieren)
- SET TOCLOADRETENTION (Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis definieren)
- SET VMATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen VM-Dateibereich an)

SET ACCOUNTING (Abrechnungssätze aktivieren/inaktivieren)

Mit diesem Befehl kann festgelegt werden, ob am Ende jeder Client-Knotensitzung ein Abrechnungssatz erstellt werden soll. Ein Abrechnungssatz protokolliert den von einer Client-Knotensitzung benötigten Speicherbereich.

Mit dem Befehl QUERY STATUS kann geprüft werden, ob Abrechnungssätze generiert werden. Bei der Installation wird dieser Wert auf OFF gesetzt.

Die Abrechnungssätze werden in einer Abrechnungsdatei mit dem Namen dsmaccnt.log gespeichert.

 AIX-Betriebssysteme  Linux-BetriebssystemeDie Umgebungsvariable DSMSERV_ACCOUNTING_DIR gibt das Verzeichnis an, in dem sich die Abrechnungsdatei befindet.

 Windows-BetriebssystemeEin Registryeintrag steuert die Position des Abrechnungsprotokolls.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ACCounting--+-ON--+-------------------------------------><
                   '-OFf-'
```

Parameter

ON
: Gibt an, dass der Server am Ende jeder Clientknotensitzung einen Abrechnungssatz erstellen soll.

OFf
: Gibt an, dass der Server keine Abrechnungssätze erstellen soll.

Beispiel: Abrechnungssätze erstellen

Geben Sie den folgenden Befehl aus, um am Ende jeder Clientknotensitzung einen Abrechnungssatz zu erstellen:

```
set accounting on
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ACCOUNTING

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET ACTLOGRETENTION (Aufbewahrungsdauer für das Aktivitätenprotokoll definieren)

Verwenden Sie diesen Befehl, um die Sätze des Aktivitätenprotokolls nach Datum oder Größe zu verwalten. Das Aktivitätenprotokoll enthält normale Aktivitätsnachrichten, die vom Server generiert werden. Diese Nachrichten enthalten Informationen zu Server- und Clientoperationen, wie die Startzeit der Sitzungen oder E/A-Fehler von Einheiten.

Unter anderem sind folgende Nachrichten im Aktivitätenprotokoll enthalten:

- Anfang und Ende von Client-Sitzungen.
- Anfang und Ende von Umlagerungen.
- Diagnosefehlernachrichten
- Ausgabedaten geplanter Verwaltungsbefehle

Bei der Serverinstallation basiert die Verwaltung des Aktivitätenprotokolls auf dem Aufbewahrungszeitraum. Der Aufbewahrungszeitraum wird auf 30 Tage gesetzt.

Sie können den Zeitraum anpassen, für den das Aktivitätenprotokoll Nachrichten aufbewahrt, um unzureichende oder veraltete Daten zu vermeiden. Nach Ablauf des Aufbewahrungszeitraums entfernt der Server automatisch die Nachrichten aus dem Aktivitätenprotokoll.

Alternativ können Sie die Gesamtgröße des Aktivitätenprotokolls begrenzen, um den Speicherbereich zu steuern, der von dem Aktivitätenprotokoll belegt wird. Der Server entfernt regelmäßig die ältesten Sätze im Aktivitätenprotokoll, bis die Größe des Aktivitätenprotokolls nicht mehr die konfigurierte maximal zulässige Größe überschreitet.

Mit dem Befehl QUERY STATUS können Sie die aktuelle Anzahl der Sätze im Aktivitätenprotokoll und die Größe (in Megabyte) anzeigen, die das Aktivitätenprotokoll gegenwärtig belegt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                              .-Mgmtstyle--=--Date-----.
>>-Set ACTlogretention--Anzahl--+------------------------+-----><
                              '-Mgmtstyle--=--+-Date-+-'
                                              '-Size-'
```

Parameter

Anzahl (Erforderlich)
: Gibt die Anzahl der Tage an, die Nachrichten im Aktivitätenprotokoll aufbewahrt werden sollen, wenn das Protokoll nach Datum verwaltet wird, oder gibt die maximale Größe des Aktivitätenprotokolls an, wenn das Protokoll nach Größe verwaltet wird. Bei der Verwaltung auf der Basis des Aufbewahrungszeitraums gibt der Wert 1 an, dass die Sätze im Aktivitätenprotokoll nur für den aktuellen Tag aufbewahrt werden sollen. Bei der Verwaltung auf der Basis der Größe gibt der Wert 1 eine maximale Größe von 1 MB für das Aktivitätenprotokoll an. Es kann eine Zahl von 0 bis 9999 angegeben werden. Der Wert 0 inaktiviert die Aufbewahrungsdauer für das Aktivitätenprotokoll.

Mgmtstyle

Gibt an, ob die Verwaltung des Aktivitätenprotokolls auf dem Aufbewahrungszeitraum oder der Größe basiert. Dieser Parameter ist wahlfrei. Der Standardwert ist DATE. Gültige Werte:

Date
: Gibt an, dass die Verwaltung des Aktivitätenprotokolls auf dem Aufbewahrungszeitraum basiert.

Size
: Gibt an, dass die Verwaltung des Aktivitätenprotokolls auf der Größe basiert.

Beispiel: Aufbewahrungsdauer für das Aktivitätenprotokoll definieren

Der Server soll die Sätze im Aktivitätenprotokoll 60 Tage lang aufbewahren. Den folgenden Befehl ausgeben:

```
set actlogretention 60
```

Beispiel: Die Größe des Aktivitätenprotokolls definieren

Den Server so definieren, dass die Größe des Aktivitätenprotokolls auf 300 MB begrenzt wird. Den folgenden Befehl ausgeben:

```
set actlogretention 300 mgmtstyle=size
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET ACTLOGRETENTION

Befehl	Beschreibung
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)

Verwenden Sie diesen Befehl, um die Dauer anzugeben, die ein Alert aktiv bleibt, bevor er inaktiv wird. Wenn ein aktiver Alert erneut ausgelöst wird, wird die Dauer erneut gestartet.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ALERTACtiveduration -Anzahl Minuten---------------------><
```

Parameter

Anzahl Minuten (Erforderlich)
: Gibt die Anzahl Minuten an, die ein Alert aktiv bleibt, bevor er inaktiv wird. Geben Sie einen Wert von 1 bis 20160 an. Der anfängliche Serverstandardwert ist 480 Minuten.

Die Dauer eines aktiven Alert auf einen Tag setzen

Mit dem folgenden Befehl angeben, dass Alerts 1440 Minuten aktiv bleiben, bevor sich ihr Status in 'inaktiv' ändert:

```
set alertactiveduration 1440
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTACTIVEDURATION

Befehl	Beschreibung
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)	Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.
SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)	Gibt an, wie lange ein Alert geschlossen bleibt, bevor er gelöscht wird.

Befehl	Beschreibung
SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)	Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.
SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)	Gibt an, wie oft der Alertmonitor Alerts in der Datenbank aktualisiert und bereinigt.

SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)

Verwenden Sie diesen Befehl, um die Dauer anzugeben, die ein Alert geschlossen bleibt, bevor er gelöscht wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ALERTCLosedduration -Anzahl Minuten--------------------><
```

Parameter

Anzahl Minuten (Erforderlich)
: Gibt die Anzahl Minuten an, die ein Alert geschlossen bleibt, bevor er gelöscht wird. Wird der Wert 0 angegeben, werden Alerts unverzüglich gelöscht, nachdem sie geschlossen wurden. Geben Sie einen Wert von 0 bis 99999 an. Der Standardwert wird auf 60 Minuten gesetzt, wenn die IBM Spectrum Protect-Serverdatenbank anfänglich formatiert wird.

Alerts zwei Stunden nach dem Schließen löschen

Angeben, dass Alerts 120 Minuten geschlossen bleiben, bevor sie gelöscht werden:

```
set alertclosedduration 120
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTCLOSEDDURATION

Befehl	Beschreibung
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)	Gibt an, wie lange ein Alert aktiv bleibt, bevor er in den Status 'inaktiv' versetzt wird.
SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)	Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.
SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)	Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.
SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)	Gibt an, wie oft der Alertmonitor Alerts in der Datenbank aktualisiert und bereinigt.

SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)

Verwenden Sie diesen Befehl, um das Senden von Alerts als E-Mail an angegebene Administratoren zu ermöglichen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ALERTEMail--+-ON--+-------------------------------------><
                   '-OFf-'
```

Parameter

ON
: Gibt an, dass Alerts als E-Mail an angegebene Administratoren gesendet werden können.

OFf
: Gibt an, dass Alerts nicht als E-Mail an angegebene Administratoren gesendet werden können. Wenn die Serverdatenbank anfänglich formatiert wird, wird die Einstellung für ALERTEMAIL auf OFF gesetzt.

Das Senden von Alerts bei ihrem Auftreten an den Administrator ermöglichen

Den folgenden Befehl ausgeben, um das Senden von Alerts als E-Mail zu ermöglichen:

```
SET ALERTEMAIL ON
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTEMAIL

Befehl	Beschreibung
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)	Gibt die E-Mail-Adresse des Absenders des Alerts an.
SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)	Gibt den Hostnamen des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.
SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)	Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.
SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)	Gibt die Administratoren an, die Alertzusammenfassungen als E-Mail empfangen möchten.

SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)

Verwenden Sie diesen Befehl, um die E-Mail-Adresse des Absenders des Alert anzugeben.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ALERTEMAILFRomaddr -E-Mail-Adresse---------------------><
```

Parameter

E-Mail-Adresse (Erforderlich)
: Gibt die E-Mail-Adresse des Absenders an. E-Mail-Adressen haben das Format *Name@Domäne*. E-Mail-Namen, einschließlich der Adresse, dürfen 64 Zeichen nicht überschreiten, und der Domänenname darf 255 Zeichen nicht überschreiten.

Die E-Mail-Adresse des Absenders des Alert angeben

Den folgenden Befehl ausgeben, um die E-Mail-Adresse des Absenders anzugeben:

```
set alertemailfromaddr djadmin@mydomain.com
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTEMAILFROMADDR

Befehl	Beschreibung
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)	Ermöglicht das Senden von Alerts als E-Mail an angegebene Administratoren.

Befehl	Beschreibung
SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)	Gibt den Hostnamen des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.
SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)	Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.
SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)	Gibt die Administratoren an, die Alertzusammenfassungen als E-Mail empfangen möchten.

SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)

Verwenden Sie diesen Befehl, um den Hostnamen des SMTP-Mail-Servers (SMTP = Simple Mail Transfer Protocol) anzugeben, der zum Senden der Alert-E-Mail verwendet wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ALERTEMAILSMTPHost--Hostname---------------------------><
```

Parameter

Hostname (Erforderlich)
: Gibt den Hostnamen des SMTP-Mail-Servers an.

Den Hostnamen des SMTP-Mail-Servers als mail.domain.com angeben

Den folgenden Befehl ausgeben, um `mail.domain.com` als SMTP-Mail-Server anzugeben:

```
set alertemailsmtphost mail.domain.com
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTEMAILSMTPHOST

Befehl	Beschreibung
SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)	Ermöglicht das Senden von Alerts als E-Mail an angegebene Administratoren.
SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)	Gibt die E-Mail-Adresse des Absenders des Alerts an.
SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)	Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.
SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)	Gibt die Administratoren an, die Alertzusammenfassungen als E-Mail empfangen möchten.

SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)

Verwenden Sie diesen Befehl, um die Anschlussnummer des SMTP-Mail-Servers anzugeben. Dieser E-Mail-Server wird zum Senden der Alerts als E-Mail verwendet.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ALERTEMAILSMTPPort--TCP-Anschluss----------------------><
```

Parameter

TCP-Anschluss (Erforderlich)
Gibt die Anschlussnummer des SMTP-Mail-Servers an. Geben Sie einen Wert von 1 bis 32767 an. Die Standardanschlussnummer ist 25.

Die Anschlussnummer des SMTP-Mail-Servers angeben

Den folgenden Befehl ausgeben, um die Anschlussnummer 450 für den SMTP-Mail-Server anzugeben:

```
set alertemailsmtpport 450
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTEMAILSMTPPORT

Befehl	Beschreibung
SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)	Ermöglicht das Senden von Alerts als E-Mail an angegebene Administratoren.
SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)	Gibt die E-Mail-Adresse des Absenders des Alerts an.
SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)	Gibt den Hostnamen des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.
SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)	Gibt die Administratoren an, die Alertzusammenfassungen als E-Mail empfangen möchten.

SET ALERTSUMMARYTOADMINS (Liste der Administratoren für den Empfang von Alertzusammenfassungen als E-Mail definieren)

Verwenden Sie diesen Befehl, um die Administratoren anzugeben, die jede Stunde Alertzusammenfassungen als E-Mail empfangen möchten.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ALERTSUMMARYToadmins--+-Administratorname-+------------><
                             '-,-----------------'
```

Parameter

Administratorname (Erforderlich)
Gibt den Namen des Administrators an, der Alertzusammenfassungen als E-Mail empfangen möchte. Es können maximal drei Administratornamen angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden.

Zwei Administratoren für den Empfang von Alertzusammenfassungen angeben

Mit dem folgenden Befehl angeben, dass die Administratoren HARRY und COLIN Alertzusammenfassungen empfangen möchten:

```
set alertsummarytoadmins HARRY,COLIN
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTSUMMARYTOADMINS

Befehl	Beschreibung
SET ALERTEMAIL (Alertmonitor für das Senden von Alerts als E-Mail an Administratoren definieren)	Ermöglicht das Senden von Alerts als E-Mail an angegebene Administratoren.
SET ALERTEMAILFROMADDR (E-Mail-Adresse des Absenders definieren)	Gibt die E-Mail-Adresse des Absenders des Alerts an.
SET ALERTEMAILSMTPHOST (Hostname des SMTP-Mail-Servers definieren)	Gibt den Hostnamen des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.
SET ALERTEMAILSMTPPORT (Hostanschluss des SMTP-Mail-Servers definieren)	Gibt den Anschluss des SMTP-Mail-Servers an, der zum Senden von Alerts in einer E-Mail verwendet wird.

SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)

Verwenden Sie diesen Befehl, um die Dauer anzugeben, die ein Alert inaktiv bleibt. Nach Ablauf dieses Zeitraums wird der Alert geschlossen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ALERTINactiveduration -Anzahl Minuten------------------><
```

Parameter

Anzahl Minuten (Erforderlich)
: Gibt die Anzahl Minuten an, die ein Alert inaktiv bleibt, bevor er geschlossen wird. Sie können einen Wert im Bereich von 1 bis 20160 angeben. Der anfängliche Serverstandardwert ist 480 Minuten.

Den Alertstatus nach 60 Minuten von 'inaktiv' in 'geschlossen' ändern

Mit dem folgenden Befehl angeben, dass ein Alert 60 Minuten im Status 'inaktiv' verbleibt, bevor sein Status in 'geschlossen' geändert wird:

```
set alertinactiveduration 60
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTINACTIVEDURATION

Befehl	Beschreibung
SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)	Gibt an, wie lange ein Alert aktiv bleibt, bevor er in den Status 'inaktiv' versetzt wird.
SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)	Gibt an, wie lange ein Alert geschlossen bleibt, bevor er gelöscht wird.
SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)	Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.
SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)	Gibt an, wie oft der Alertmonitor Alerts in der Datenbank aktualisiert und bereinigt.

SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)

Verwenden Sie diesen Befehl, um den Alertmonitor zu aktivieren oder zu inaktivieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                    .-OFf-.
>>-Set ALERTMONITOR -+-ON--+-----------------------------------><
```

Parameter

ON
: Gibt an, dass der IBM Spectrum Protect-Server Alerts überwacht.

OFf
: Gibt an, dass der IBM Spectrum Protect-Server Alerts nicht überwacht. Wenn die IBM Spectrum Protect-Serverdatenbank anfänglich formatiert wird, wird die Einstellung für die Alertüberwachung auf OFF gesetzt.

Alertüberwachung aktivieren

Den folgenden Befehl ausgeben, um die Alertüberwachung zu aktivieren:

```
set alertmonitor on
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTMONITOR

Befehl	Beschreibung
SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)	Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.
SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)	Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.
SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)	Gibt an, wie lange ein Alert geschlossen bleibt, bevor er gelöscht wird.
SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)	Gibt an, wie oft der Alertmonitor Alerts in der Datenbank aktualisiert und bereinigt.

SET ALERTUPDATEINTERVAL (Häufigkeit definieren, mit der der Alertmonitor Alerts aktualisiert und bereinigt)

Mit diesem Befehl können Sie angeben, wie oft der Alertmonitor Alerts aktualisiert und bereinigt, die in der IBM Spectrum Protect-Serverdatenbank gespeichert sind.

Während dieses Prüfintervalls werden vom Alertmonitor alle Alerts auf dem Server untersucht und die folgenden Aktionen ausgeführt:

- Der Alertmonitor bestimmt, ob der Zeitraum für den aktiven oder inaktiven Status abgelaufen ist. Läuft der angegebene Zeitraum ab, wird der Alertstatus in den nächsten Status aktualisiert. Beispiel:
  - 'Aktiv' in 'inaktiv'
  - 'Inaktiv' in 'geschlossen'
- Ist ein Alert für die mit dem Befehl SET ALERTCLOSEDDURATION angegebene Dauer geschlossen, wird der Alert gelöscht.

Sie können mit dem Befehl QUERY MONITORSETTINGS bestimmen, ob die Alertüberwachung aktiviert ist. Verwenden Sie den Befehl SET ALERTMONITOR, um die Alertüberwachung zu aktivieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ALERTUPDateinterval -Anzahl Minuten---------------------><
```

Parameter

Anzahl Minuten (Erforderlich)
: Gibt die Zeit in Minuten an, die der Monitor wartet, bevor Alerts auf dem Server aktualisiert und bereinigt werden. Geben Sie einen Wert von 1 bis 9999 an. Der Server hat einen ursprünglichen Standardwert von 10 Minuten.

Das Alertaktualisierungsintervall auf 60 Minuten setzen

Mit dem folgenden Befehl angeben, dass Alerts jede Stunde aktualisiert werden:

```
set alertupdateinterval  60
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ALERTUPDATEINTERVAL

Befehl	Beschreibung
SET ALERTACTIVEDURATION (Dauer eines aktiven Alert definieren)	Gibt an, wie lange ein Alert aktiv bleibt, bevor er in den Status 'inaktiv' versetzt wird.
SET ALERTINACTIVEDURATION (Dauer eines inaktiven Alert definieren)	Gibt an, wie lange ein Alert inaktiv bleibt, bevor er geschlossen wird.
SET ALERTCLOSEDDURATION (Dauer eines geschlossenen Alert definieren)	Gibt an, wie lange ein Alert geschlossen bleibt, bevor er gelöscht wird.

Befehl	Beschreibung
SET ALERTMONITOR (Alertmonitor aktivieren oder inaktivieren)	Gibt an, ob die Alertüberwachung aktiviert oder inaktiviert ist.

SET ARCHIVERETENTIONPROTECTION (Aufbewahrungsschutz für Daten aktivieren)

Mit diesem Befehl können Sie den Aufbewahrungsschutz für Archivierungsdaten aktivieren und inaktivieren. Der Server darf keine Daten enthalten, damit dieser Befehl arbeitet. Bei der Installation wird dieser Wert auf OFF gesetzt.

Ist der Aufbewahrungsschutz für Archivierungsdaten aktiv, gilt Folgendes:

- Es können nur Archivierungskopien auf dem Server gespeichert werden.
- Eine Archivierungskopie kann erst gelöscht werden, wenn der Parameter RETVER im Befehl DEFINE COPYGROUP (Archivierung) erfüllt wurde.

Das Definieren von Speicherpools mit dem Typ RECLAMATIONTYPE=SNAPLOCK wird nur auf Servern mit aktiviertem Aufbewahrungsschutz für Daten unterstützt.

Verwenden Sie den Befehl QUERY STATUS, um den Status des Aufbewahrungsschutzes für Archivierungsdaten anzuzeigen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-Set ARCHIVERETENTIONPROTECTion -+-OFf-+--------------------><
                                   '-ON--'
```

Parameter

OFf
: Gibt an, dass der Aufbewahrungsschutz für Archivierungsdaten nicht aktiv ist.

ON
: Gibt an, dass der Aufbewahrungsschutz für Archivierungsdaten aktiv ist.

Beispiel: Aufbewahrungsschutz für Daten aktivieren

Den Aufbewahrungsschutz für Archivierungsdaten durch Ausgabe des folgenden Befehls aktivieren:

```
set archiveretentionprotection on
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ARCHIVERETENTIONPROTECTION

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
AUDIT VOLUME	Vergleicht Datenbank- und Speicherpooldaten und (wahlfrei) beseitigt Inkonsistenzen.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

Befehl	Beschreibung
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.

SET ARREPLRULEDEFAULT (Serverreplikationsregel für Archivierungsdaten definieren)

Mit diesem Befehl können Sie die Serverreplikationsregel für Archivierungsdaten definieren.

Einschränkung: Die Replikationsregel, die Sie mit diesem Befehl definieren, wird nur angewendet, wenn Dateibereichsregeln und Clientknotenregeln für Archivierungsdaten auf DEFAULT gesetzt sind.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Sie können eine Replikationsregel für normale Priorität oder eine Replikationsregel für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Beispiel: Angenommen, Ihre Clientknoten enthalten Archivierungsdaten und Sicherungsdaten. Die Replikation der Archivierungsdaten hat eine höhere Priorität als die der Sicherungsdaten. Um die Archivierungsdaten zu priorisieren, geben Sie den Befehl SET ARREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL_DATA_HIGH_PRIORITY an. Um die Sicherungsdaten zu priorisieren, geben Sie den Befehl SET BKREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL_DATA für Sicherungsdaten an. Die Regel ALL_DATA für Sicherungsdaten repliziert Sicherungsdaten mit einer normalen Priorität.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set ARREPLRuledefault--+-ALL_DATA---------------+----------><
                          +-ALL_DATA_HIGH_PRIORITY-+
                          '-NONE--------------------'
```

Parameter

ALL_DATA
: Repliziert Archivierungsdaten mit einer normalen Priorität.

ALL_DATA_HIGH_PRIORITY
: Repliziert Archivierungsdaten mit einer hohen Priorität.

NONE
: Die Archivierungsdaten werden nicht repliziert.

Beispiel: Die Serverreplikationsregel für Archivierungsdaten definieren

Die Standardregel für Archivierungsdaten so definieren, dass die Replikation mit einer hohen Priorität erfolgt.

```
set arreplruledefault all_data_high_priority
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET ARREPLRULEDEFAULT

Befehl	Beschreibung
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY REPLRULE	Zeigt Informationen zu Knotenreplikationsregeln an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.

Befehl	Beschreibung
SET BKREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für Sicherungsdaten an.
SET SPREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für speicherverwaltete Daten an.
UPDATE FILESPACE	Ändert Knotenreplikationsregeln für Dateibereiche.
UPDATE REPLRULE	Aktiviert oder inaktiviert Replikationsregeln.
VALIDATE REPLICATION	Überprüft die Replikation für Dateibereiche und Datentypen.

SET BKREPLRULEDEFAULT (Serverreplikationsregel für Sicherungsdaten definieren)

Mit diesem Befehl können Sie die Serverreplikationsregel für Sicherungsdaten definieren.

Einschränkung: Die Replikationsregel, die Sie mit diesem Befehl definieren, wird nur angewendet, wenn Dateibereichsregeln und Clientknotenregeln für Sicherungsdaten auf DEFAULT gesetzt sind.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Sie können Replikationsregeln für normale Priorität oder Replikationsregeln für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Beispiel: Angenommen, Ihre Clientknoten enthalten Archivierungsdaten und aktive Sicherungsdaten. Die Replikation der aktiven Sicherungsdaten hat eine höhere Priorität als die der Archivierungsdaten. Um die Sicherungsdaten zu priorisieren, geben Sie den Befehl SET BKREPLRULEDEFAULT aus und geben Sie die Replikationsregel ACTIVE_DATA_HIGH_PRIORITY an. Um die Archivierungsdaten zu priorisieren, geben Sie den Befehl SET ARREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL_DATA für Archivierungsdaten an. Die Regel ALL_DATA für Archivierungsdaten repliziert Archivierungsdaten mit einer normalen Priorität.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set BKREPLRuledefault--+-ALL_DATA------------------+-------><
                          +-ACTIVE_DATA---------------+
                          +-ALL_DATA_HIGH_PRIORITY----+
                          +-ACTIVE_DATA_HIGH_PRIORITY-+
                          '-NONE--------------------'
```

Parameter

ALL_DATA
: Repliziert aktive und inaktive Sicherungsdaten. Die Daten werden mit normaler Priorität repliziert.

ACTIVE_DATA
: Repliziert aktive Sicherungsdaten. Die Daten werden mit normaler Priorität repliziert.
Achtung: Wenn Sie ACTIVE_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

  - Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
  - Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
  - Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

  Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

ALL_DATA_HIGH_PRIORITY
: Repliziert aktive und inaktive Sicherungsdaten. Daten werden mit einer hohen Priorität repliziert.

ACTIVE_DATA_HIGH_PRIORITY

  Diese Regel entspricht der Replikationsregel ACTIVE_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

NONE
: Die Sicherungsdaten werden nicht repliziert.

Beispiel: Die Serverreplikationsregel für Sicherungsdaten definieren

Die Standardregel für Sicherungsdaten so definieren, dass nur aktive Daten und die Daten mit einer hohen Priorität repliziert werden.

```
set bkreplruledefault active_data_high_priority
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET BKREPLRULEDEFAULT

Befehl	Beschreibung
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY REPLRULE	Zeigt Informationen zu Knotenreplikationsregeln an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
SET ARREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für Archivierungsdaten an.
SET REPLRETENTION	Gibt den Aufbewahrungszeitraum für Replikationsprotokollsätze an.
SET SPREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für speicherverwaltete Daten an.
UPDATE FILESPACE	Ändert Knotenreplikationsregeln für Dateibereiche.
UPDATE REPLRULE	Aktiviert oder inaktiviert Replikationsregeln.
VALIDATE REPLICATION	Überprüft die Replikation für Dateibereiche und Datentypen.

SET CLIENTACTDURATION (Verweildauer für Clientaktion definieren)

Mit diesem Befehl kann die Dauer des Zeitplans angegeben werden, der mit dem Befehl DEFINE CLIENTACTION definiert wurde. Eine Clientaktion definiert einen Zeitplan, der einmal auf einem Client ausgeführt wird.

Das Programm löscht diese Ereignissätze, unabhängig davon, ob der Client den Zeitplan verarbeitet hat oder nicht. Die Zeitpläne werden jedoch erst gelöscht, nachdem die ersten Ereignissätze gelöscht wurden. Der Aufbewahrungszeitraum für Ereignisse wird bei der Installation standardmäßig auf 10 Tage gesetzt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-SET CLIENTACTDuration--Tage---------------------------------><
```

Parameter

Tage (Erforderlich)
Gibt die Anzahl der Tage an, die der Zeitplan für die Client-Aktion aktiv ist. Zulässige Werte sind ganze Zahlen von 0 bis 999. Der Standardwert lautet 5 Tage.

Die angegebene Anzahl der Tage bestimmt, wie lange der Zeitplan in der Datenbank aufbewahrt wird, bevor er gelöscht wird. Der Wert 0 gibt an, dass die Dauer des Zeitplans unbegrenzt ist, und der Zeitplan und die Zuordnungen werden nicht aus der Datenbank gelöscht.

Beispiel: Eine Verweildauer von 15 Tagen für die Clientaktion definieren

Um anzugeben, dass der Zeitplan für die Clientaktion 15 Tage aktiv sein soll, den folgenden Befehl ausgeben:

```
set clientactduration 15
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET CLIENTACTDURATION

Befehl	Beschreibung
DEFINE CLIENTACTION	Definiert einen Befehl, der bei einem Clientknoten ausgeführt werden soll.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET CONFIGMANAGER (Konfigurationsmanager angeben)

Mit diesem Befehl kann angegeben werden, ob es sich bei einem Server um einen Konfigurationsmanager handelt. Auf einem Konfigurationsmanager können Konfigurationsprofile definiert werden, für die andere Server subskribieren können.

Ein Server kann nicht als Konfigurationsmanager bestimmt werden, wenn der Server für ein oder mehrere Profile auf einem anderen Konfigurationsmanager subskribiert.

Ist ein Server ein Konfigurationsmanager, kann diese Definition erst geändert werden, wenn alle Profile einschließlich des Standardprofils gelöscht werden.

Mit dem Befehl QUERY STATUS kann bestimmt werden, ob ein Server ein Konfigurationsmanager ist. Wenn ein Server installiert wird, wird er nicht als Konfigurationsmanager bestimmt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                        .-OFf-.
>>-Set CONFIGManager--+-----+-----------------------------------><
                      '-ON--'
```

Parameter

ON
: Gibt an, dass der Server ein Konfigurationsmanager ist.

  Wenn ein Server als Konfigurationsmanager bestimmt wird, erstellt IBM Spectrum Protect ein Standardprofil mit dem Namen DEFAULT_PROFILE und ordnet dem Profil alle auf dem Konfigurationsmanager definierten Server und Servergruppen zu. Das Standardprofil kann geändert oder gelöscht werden.

OFf
: Gibt an, dass der Server kein Konfigurationsmanager ist.

Beispiel: Einen Konfigurationsmanager angeben

Einen Server als Konfigurationsmanager bestimmen.

```
set configmanager on
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET CONFIGMANAGER

Befehl	Beschreibung
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET CONFIGREFRESH	Gibt das Zeitintervall an, in dem verwaltete Server die Konfigurationsmanager ansprechen sollen.

SET CONFIGREFRESH (Aktualisierung der Konfiguration verwalteter Server definieren)

Mit diesem Befehl kann auf einem verwalteten Server angegeben werden, wie oft dieser Server bei seinem Konfigurationsmanager nach aktualisierten Konfigurationsdaten nachfragen soll.

Soll die aktuelle Einstellung angezeigt werden, den Befehl QUERY STATUS ausgeben. Bei der Installation wird das Intervall auf 60 Minuten gesetzt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set CONFIGRefresh--Minuten---------------------------------><
```

Parameter

Minuten (Erforderlich)
Gibt das Intervall in Minuten an, in dem ein verwalteter Server aktualisierte Konfigurationsdaten von seinem Konfigurationsmanager anfordern soll. Eine ganze Zahl von 0 bis 10000 angeben.

- Ist der Wert größer als 0, nimmt der verwaltete Server sofort Verbindung mit dem Konfigurationsmanager auf. Die nächste Verbindung wird hergestellt, wenn das angegebene Intervall erreicht ist.
- Ist der Wert 0, nimmt der verwaltete Server keine Verbindung mit dem Konfigurationsmanager auf.

Dieser Wert wird ignoriert, wenn der Server nicht für mindestens ein Profil auf einem Konfigurationsmanager subskribiert.

Beispiel: Ein Aktualisierungsintervall von 45 Minuten definieren

Angeben, dass ein verwalteter Server alle 45 Minuten Verbindung mit seinem Konfigurationsmanager aufnehmen soll.

```
set configrefresh 45
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET CONFIGREFRESH

Befehl	Beschreibung
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DELETE PROFASSOCIATION	Löscht die Zuordnung zwischen einem Objekt und einem Profil.
NOTIFY SUBSCRIBERS	Weist Server auf die erforderliche Aktualisierung ihrer Konfigurationsdaten hin.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

SET CONTEXTMESSAGING (Anzeigen von Nachrichtenkontext aktivieren oder inaktivieren)

Verwenden Sie diesen Befehl, um zusätzliche Informationen abzurufen, wenn Nachrichten ANR9999D auftreten. IBM Spectrum Protect fragt die Serverkomponenten nach Informationen ab, die den Prozessnamen, den Threadnamen, die Sitzungs-ID, die Transaktionsdaten, die aktivierten Sperren und die verwendeten Datenbanktabellen umfassen.

Anmerkung: Werden nachfolgende Nachrichten aus demselben Codebereich von demselben Thread ausgegeben, enthält nur die erste dieser Nachrichten die Kontextinformationen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set CONTEXTmessaging--+-ON--+-------------------------------><
```

```
'-OFf-'
```

Parameter

ON
: Gibt an, dass das Anzeigen von Nachrichtenkontext aktiviert werden soll.

OFf
: Gibt an, dass das Anzeigen von Nachrichtenkontext inaktiviert werden soll.

Beispiel: Anzeigen von Nachrichtenkontext aktivieren oder inaktivieren

Das Anzeigen von Nachrichtenkontext aktivieren, um zusätzliche Informationen zu empfangen, die bei der Bestimmung der Ursache der Nachrichten ANR9999D helfen können.

```
set contextmessaging on
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET CONTEXTMESSAGING

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET CPUINFOREFRESH (Aktualisierungsintervall für Informationssuche auf Client-Workstation)

Mit diesem Befehl können Sie die Anzahl der Tage zwischen Suchläufen nach Client-Workstation-Informationen angeben, die verwendet werden, um die Prozessor-Value-Unit (PVU) zu schätzen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set CPUINFOREFRESH--Tage-----------------------------------><
```

Parameter

Tage (Erforderlich)
: Gibt die Anzahl der Tage zwischen Suchläufen nach Clienteinheiten an. Soll die aktuelle Einstellung abgerufen werden, geben Sie den Befehl QUERY STATUS aus. Die gültigen Werte sind 1 - 9999. Der Standardwert ist 180.

Beispiel: Die Zeit vor der nächsten Aktualisierung auf 90 Tage setzen

```
SET CPUINFOREFRESH 90
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET CPUINFOREFRESH

Befehl	Beschreibung
QUERY PVUESTIMATE	Zeigt eine Schätzung der Clienteinheiten und Servereinheiten an, die verwaltet werden.

SET CROSSDEFINE (Querdefinition von Servern angeben)

Mit diesem Befehl kann angegeben werden, ob ein Server automatisch für einen anderen Server definiert wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set CROSSDefine--+-ON--+-----------------------------------><
                    '-OFf-'
```

Parameter

ON
: Gibt an, daß ein Server für einen anderen Server definiert werden kann. Soll ein Server automatisch für einen anderen Server definiert werden, muß diese Querdefinition auch in der Server-Definition zugelassen werden.

OFf
: Gibt an, daß ein Server nicht für einen anderen Server definiert werden kann.

Beispiel: Querdefinition von Servern angeben

Angeben, dass ein Server für einen anderen Server definiert werden kann.

```
set crossdefine on
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET CROSSDEFINE

Befehl	Beschreibung
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
SET SERVERHLADDRESS	Gibt die Adresse der höheren Ebene eines Servers an.
SET SERVERLLADDRESS	Gibt die Adresse der unteren Ebene eines Servers an.
SET SERVERPASSWORD	Gibt das Serverkennwort an.

SET DBRECOVERY (Einheitenklasse für automatische Sicherungen definieren)

Verwenden Sie diesen Befehl, um die Einheitenklasse und die Anzahl der Datenströme anzugeben, die für automatische Datenbanksicherungen verwendet werden sollen. Mit diesem Befehl können Sie auch den Befehl BACKUP DB zum automatischen Sichern des Masterverschlüsselungsschlüssels für den Server konfigurieren.

Der Masterverschlüsselungsschlüssel wird verwendet, um Daten in Verzeichniscontainer- und Cloud-Containerspeicherpools sowie sensible Informationen in der Serverdatenbank zu verschlüsseln. Wird der Masterverschlüsselungsschlüssel nicht gesichert, können Sie möglicherweise nicht auf diese verschlüsselten Elemente zugreifen, wenn ein Katastrophenfall eintritt.

Wenn Sie den Befehl BACKUP DB ausführen und die Einheitenklasse nicht die im Befehl SET DBRECOVERY angegebene Einheitenklasse ist, wird eine Warnung zurückgegeben. Die Sicherungsoperation wird jedoch fortgesetzt und ist nicht betroffen.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-SET DBRECOVery--Einheitenklassenname-------------------------->

   .-NUMStreams--=--1------.  .-COMPress--=--No------.
>--+----------------------+--+---------------------+---------->
   '-NUMStreams--=--Anzahl-'  '-COMPress--=--+-No--+-'
                                             '-Yes-'

   .-PROTECTKeys--=--Yes-----.
>--+------------------------+--+---------------------------+--><
   '-PROTECTKeys--=--+-No--+-'  '-PASSword--=--Kennwortname-'
                     '-Yes-'
```

Parameter

Einheitenklassenname **(Erforderlich)**
: Gibt die Einheitenklasse an, die für Datenbanksicherungen verwendet werden soll.

NUMStreams

Gibt die Anzahl der parallelen Datenversetzungsdatenströme an, die beim Sichern der Datenbank verwendet werden sollen. Der Standardwert ist 1 und die maximale Anzahl ist 32. Die Erhöhung dieses Werts hat eine entsprechende Erhöhung der Anzahl der zu verwendenden Datenbanksicherungssitzungen und der Anzahl von Laufwerken zur Folge, die für die Einheitenklasse verwendet werden müssen. Ein Wert für NUMSTREAMS, der im Befehl BACKUP DB angegeben wird, überschreibt den Wert, der in dem Befehl SET DBRECOVERY definiert ist. Der Wert für NUMSTREAMS wird für alle Typen der Datenbanksicherung verwendet.
Wird ein Wert angegeben, der größer als die Anzahl der für die Einheitenklasse verfügbaren Laufwerke ist, wird die Anzahl der verfügbaren Laufwerke verwendet. Die verfügbaren Laufwerke werden für die Einheitenklasse durch den Parameter MOUNTLIMIT oder durch die Anzahl der Onlinelaufwerke für die angegebene Einheitenklasse definiert. Die Sitzung wird in der Ausgabe von QUERY SESSION angezeigt. Wenn Sie die Anzahl der Datenströme erhöhen, werden mehr Datenträger aus der entsprechenden Einheitenklasse für diese Operation verwendet. Mit einer größeren Anzahl von Datenträgern kann die Geschwindigkeit von Datenbanksicherungen erhöht werden, jedoch auf Kosten einer größeren Anzahl von Datenträgern, die nicht vollständig belegt sind.

COMPress
Gibt an, ob Datenträger während der Datenbanksicherungsverarbeitung komprimiert werden. Dieser Parameter ist wahlfrei. Der Standardwert ist No. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass die Datenträger, die mit dem Befehl BACKUP DB erstellt werden, nicht komprimiert werden.

Yes
Gibt an, dass die Datenträger, die mit dem Befehl BACKUP DB erstellt werden, komprimiert werden.

Wird der Parameter COMPRESS im Befehl BACKUP DB angegeben, überschreibt er den Wert, der im Befehl SET DBRECOVERY definiert ist. Andernfalls wird der im Befehl SET DBRECOVERY definierte Wert verwendet.
Einschränkungen:

- Gehen Sie mit Vorsicht vor, wenn Sie den Parameter COMPRESS angeben. Bei Verwendung der Komprimierung während Datenbanksicherungen kann die Größe der Sicherungsdateien verringert werden. Die Komprimierung kann jedoch die Zeit für die Ausführung der Datenbanksicherungsverarbeitung verlängern.
- Sichern Sie keine komprimierten Daten auf Band. Wenn in Ihrer Systemumgebung Datenbanksicherungen auf Band gespeichert werden, setzen Sie den Parameter COMPRESS in den Befehlen SET DBRECOVERY und BACKUP DB auf No.

PROTECTKeys
Gibt an, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels für den Server enthalten, der zum Verschlüsseln von Speicherpooldaten verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist 'Yes'. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass Datenbanksicherungen keine Kopie des Masterverschlüsselungsschlüssels für den Server enthalten.
Achtung: Wenn Sie PROTECTKEYS=NO angeben, müssen Sie den Masterverschlüsselungsschlüssel für den Server manuell sichern und den Schlüssel verfügbar machen, wenn Sie die Wiederherstellung nach einem Katastrophenfall (Disaster Recovery) implementieren.

Yes
Gibt an, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels für den Server enthalten.
Achtung: Wenn Sie PROTECTKEYS=YES angeben, müssen Sie auch den Parameter PASSWORD angeben.

PASSword
Gibt das Kennwort an, das zum Schützen der Datenbanksicherungen verwendet wird. Standardmäßig werden Datenbanksicherungen geschützt.
Wichtig: Sie müssen sich dieses Kennwort merken. Wenn Sie ein Kennwort für die Datenbanksicherung angeben, müssen Sie dasselbe Kennwort im Befehl RESTORE DB zum Zurückschreiben der Datenbank angeben.

Beispiel: Eine Einheitenklasse für Datenbanksicherungen angeben

Die Einheitenklasse DBBACK für Datenbanksicherungen angeben. Den folgenden Befehl ausgeben:

```
set dbrecovery dbback
```

Beispiel: Eine Einheitenklasse und die Anzahl von Datenströmen für Datenbanksicherungen angeben

Die Einheitenklasse DBBACK für Datenbanksicherungen angeben und angeben, dass die Sicherung zwei Datenversetzungsdatenströme verwenden soll. Den folgenden Befehl ausgeben:

```
set dbrecovery dbback numstreams=2
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

Beispiel: Verschlüsselungsschlüssel des Speicherpools in Datenbanksicherungen schützen

Speicherpooldaten verschlüsseln, indem angegeben wird, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels für den Server enthalten. Den folgenden Befehl ausgeben:

```
set dbrecovery dbback protectkeys=yes password=Kennwortname
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DBRECOVERY

Befehl	Beschreibung
BACKUP DB	Sichert die IBM Spectrum Protect-Datenbank auf Datenträgern mit sequenziellem Zugriff.
QUERY DB	Zeigt Zuordnungsinformationen zu der Datenbank an.
QUERY DBSPACE	Zeigt Informationen zum Speicherplatz an, der für die Datenbank definiert ist.

SET DEDUPVERIFICATIONLEVEL (Prozentsatz der zu prüfenden Bereiche definieren)

Verwenden Sie diesen Befehl, um die Bereiche zu überprüfen, die während der clientseitigen Deduplizierung von Daten an den Server gesendet wurden.

Eine außer Kontrolle geratene Anwendung, die sich auf einem Clientsystem befindet und die Client-, API- oder GUI-Anwendung imitiert, kann eine Attacke auf den Server auslösen. Um die Anfälligkeit des Servers für diese Attacken zu verringern, können Sie einen Prozentsatz der Clientbereiche angeben, die vom Server geprüft werden sollen.

Wenn der Server erkennt, dass gerade eine Sicherheitsattacke ausgeführt wird, wird die aktuelle Sitzung abgebrochen. Außerdem wird die Einstellung des Parameters DEDUPLICATION im Befehl REGISTER NODE geändert. Die Einstellung wird von CLIENTORSERVER in SERVERONLY geändert. Mit der Einstellung SERVERONLY wird die clientseitige Deduplizierung von Daten für diesen Knoten inaktiviert.

Der Server gibt auch in einer Nachricht an, dass eine mögliche Sicherheitsattacke festgestellt und die clientseitige Deduplizierung von Daten für den Knoten inaktiviert wurde. Wird die clientseitige Deduplizierung von Daten inaktiviert, werden alle anderen Clientoperationen (z. B. Sicherungsoperationen) fortgesetzt. Es wird nur die clientseitige Deduplizierung von Daten inaktiviert. Wird die clientseitige Deduplizierung von Daten für einen Knoten inaktiviert, da eine mögliche Attacke festgestellt wurde, dedupliziert der Server die Daten, die für die clientseitige Datendeduplizierung ausgewählt werden können.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                              .-0-----------.
>>-Set DEDUPVERificationlevel--+-------------+-----------------><
                              '-Prozentwert-'
```

Parameter

Prozentwert (Erforderlich)
: Geben Sie einen ganzzahligen Wert zwischen 0 - 100 an, um den Prozentsatz der zu prüfenden Clientbereiche anzugeben. Der Wert 0 gibt an, dass keine Clientbereiche geprüft werden. Der Standardwert für diesen Befehl ist 0.
Tipps:

- Die Prüfung der Bereiche beansprucht Verarbeitungskapazität und hat negative Auswirkungen auf die Serverleistung. Geben Sie für eine optimale Leistung keine Werte größer als 10 für diesen Befehl an.
- Um den aktuellen Wert für SET DEDUPVERIFICATIONLEVEL anzuzeigen, geben Sie den Befehl QUERY STATUS aus.

Beispiel: Eine Mindeststufe für die Datendeduplizierungsprüfung angeben

Um anzugeben, dass 1 % der während der clientseitigen Datendeduplizierung erstellten Bereiche geprüft werden soll, geben Sie den folgenden Befehl aus:

```
set dedupverificationlevel 1
```

Beispiel: Die Datendeduplizierungsprüfung inaktivieren

Um anzugeben, dass keine der während der clientseitigen Datendeduplizierung erstellten Bereiche geprüft werden sollen, geben Sie den folgenden Befehl aus:

```
set dedupverificationlevel 0
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DEDUPVERIFICATIONLEVEL

Befehl	Beschreibung
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
QUERY CONTENT	Zeigt Informationen über Dateien in einem Speicherpooldatenträger an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

SET DEFAULTAUTHENTICATION (Standardauthentifizierungsmethode für Befehle REGISTER NODE und REGISTER ADMIN definieren)

Verwenden Sie diesen Befehl, um die Standardkennwortauthentifizierungsmethode für Knoten und Administratoren zu definieren, die das Ergebnis der Befehle REGISTER NODE und REGISTER ADMIN sind.

Wenn Sie LDAP angeben, definieren Sie den Standardwert für die Authentifizierung mit einem externen Verzeichnis für alle neuen Befehle REGISTER NODE oder REGISTER ADMIN. Dieser Befehl erleichtert die Registrierung von Knoten oder Administratoren, wenn Sie einen LDAP-Verzeichnisserver verwenden.
Tipp: Die Standardauthentifizierungseinstellung kann überschrieben werden, wenn die Authentifizierungsmethode in einem Befehl REGISTER NODE oder REGISTER ADMIN angegeben wird.

Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie über die Systemberechtigung verfügen.

Syntax

```
>>-SET DEFAULTAUTHentication--+-LOcal-+------------------------><
                              '-LDap--'
```

Parameter

LOcal
: Gibt an, dass alle zukünftigen Befehle REGISTER NODE und REGISTER ADMIN, die Sie ausgeben, LOCAL als Parameterwert für die Standardauthentifizierung verwenden. Lokal authentifizierte Kennwörter sind die Kennwörter, die auf dem IBM Spectrum Protect-Server gespeichert werden. Bei den lokal authentifizierten Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

LDap
: Gibt an, dass alle zukünftigen Befehle REGISTER NODE und REGISTER ADMIN, die Sie ausgeben, LDAP als Parameterwert für die Standardauthentifizierung verwenden. LDAP-authentifizierte Kennwörter sind die Kennwörter, die auf einem LDAP-Verzeichnisserver gespeichert werden. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung beachtet werden.

Beispiel: Den Wert für die Standardkennwortauthentifizierung auf LDAP setzen

Angeben, dass alle ausgegebenen Befehle REGISTER NODE oder REGISTER ADMIN Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren sollen.

```
set defaultauthentication ldap
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DEFAULTAUTHENTICATION

Befehl	Beschreibung
SET LDAPPASSWORD	Legt das Kennwort für den LDAPUSER fest.

Befehl	Beschreibung
SET LDAPUSER	Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht.
SET LDAPUSER	Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht.
REGISTER ADMIN	Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.

SET DISSIMILARPOLICIES (Die Maßnahmen auf dem Zielreplikationsserver für die Verwaltung replizierter Daten aktivieren)

Verwenden Sie den Befehl SET DISSIMILARPOLICIES, um die Maßnahmen, die auf dem Zielreplikationsserver definiert sind, für die Verwaltung von replizierten Clientknotendaten zu aktivieren. Wenn Sie die Maßnahmen auf dem Zielreplikationsserver nicht verwenden, werden replizierte Clientknotendaten von Maßnahmen auf dem Quellenreplikationsserver verwaltet.

Stellen Sie sicher, dass IBM Spectrum Protect Version 7.1.1 oder höher auf dem Quellen- und Zielreplikationsserver installiert ist, bevor Sie diesen Befehl ausgeben. Geben Sie diesen Befehl auf dem Quellenreplikationsserver aus.

Bevor Sie die Maßnahmen verwenden, die auf einem Zielreplikationsserver definiert sind, müssen Sie den Befehl VALIDATE REPLPOLICY für diesen Zielreplikationsserver ausgeben. Dieser Befehl zeigt die Unterschiede zwischen den Maßnahmen für die Clientknoten auf dem Quellenreplikationsserver und den Maßnahmen auf dem Zielreplikationsserver an. Sie können die Maßnahmen auf dem Zielreplikationsserver ändern, bevor Sie diese Maßnahmen für die Verwaltung von replizierten Clientknotendaten aktivieren.

Um den Namen des Zielreplikationsservers abzurufen, für den Daten verwaltet werden sollen, und zu überprüfen, ob die Maßnahmen auf dem Zielreplikationsserver auf ON gesetzt sind, verwenden Sie den Befehl QUERY REPLSERVER. Bei der Installation wird dieser Wert auf OFF gesetzt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                                          .-OFf-.
>>-Set DISSIMILARPolicies--Zielservername--+-----+------------><
                                          +-OFf-+
                                          '-ON--'
```

Parameter

Zielservername (Erforderlich)
: Gibt den Namen des Zielreplikationsservers an, für den die Maßnahmen aktiviert werden sollen.

ON
: Gibt an, dass die replizierten Clientknotendaten von den Maßnahmen verwaltet werden, die auf dem Zielreplikationsserver definiert sind.

OFf
: Gibt an, dass die replizierten Clientknotendaten von den Maßnahmen verwaltet werden, die auf dem Quellenreplikationsserver definiert sind. Off ist der Standardwert.

Beispiel: Die Maßnahmen auf einem Zielreplikationsserver verwenden

Um replizierte Clientknotendaten auf dem Zielreplikationsserver CVTCVS_LXS_SRV2 zu verwalten, geben Sie den folgenden Befehl auf dem Quellenreplikationsserver aus:

```
set dissimilarpolicies CVTCVS_LXS_SRV2 on
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DISSIMILARPOLICIES

Befehl	Beschreibung
QUERY REPLSERVER	Zeigt Informationen zu Replikationsservern an.
VALIDATE REPLPOLICY	Prüft die Maßnahmen auf dem Zielreplikationsserver.

SET DRMACTIVEDATASTGPOOL (Von DRM zu verwaltende Pools für aktive Daten angeben)

Mit diesem Befehl können Namen von Pools für aktive Daten angegeben werden, die nach einem Katastrophenfall wiederhergestellt werden sollen. IBM Spectrum Protect verwendet diese Namen, wenn der Befehl PREPARE, MOVE DRMEDIA oder QUERY DRMEDIA nicht den Parameter ACTIVEDATASTGPOOL enthält.

Standardmäßig sind Datenträger in Pools für aktive Daten nicht für die Verarbeitung durch Disaster Recovery Manager auswählbar. Um Datenträger im Pool für aktive Daten zu verarbeiten, müssen Sie den Befehl SET DRMACTIVEDATASTGPOOL ausgeben oder Sie müssen den Befehlszeilenparameter ACTIVEDATASTGPOOL im Befehl MOVE DRMEDIA, QUERY DRMEDIA oder PREPARE verwenden.

Mit dem Befehl QUERY DRMSTATUS können die aktuellen Einstellungen angezeigt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set DRMACTIVEDatastgpool-----------------------------------><

   .-,--------------------------------.
   V                                  |
>----Name_des_Pools_für_aktive_Daten-+-------------------------><
```

Parameter

Name_des_Pools_für_aktive_Daten (Erforderlich)
: Gibt die Namen der Pools für aktive Daten an. Mehrere Namen sind ohne Leerzeichen durch Kommas voneinander zu trennen. Es können Platzhalterzeichen verwendet werden. Die angegebenen Namen überschreiben die vorherigen Einstellungen. Wird eine Nullzeichenfolge ("") eingegeben, werden alle aktuellen Namen entfernt, und es werden keine Datenträger im Pool für aktive Daten im Status MOUNTABLE verarbeitet, wenn sie nicht explizit als MOVE DRMEDIA-, QUERY DRMEDIA- oder PREPARE-Befehlsparameter eingegeben wurden.

Beispiel: Einen auswählbaren Pool für aktive Daten definieren

ACTIVEDATAPOOL1 als auswählbaren Pool für aktive Daten definieren.

```
set drmactivedatapool activedatastgpool1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMACTIVEDATASTGPOOL

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.
SET DRMCOPYSTGPOOL	Gibt an, dass Kopienspeicherpools von DRM verwaltet werden.
SET DRMPRIMSTGPOOL	Gibt an, dass primäre Speicherpools von DRM verwaltet werden.

SET DRMCHECKLABEL (Kennsatzprüfung angeben)

Mit diesem Befehl kann angegeben werden, ob IBM Spectrum Protect die Kennsätze von sequenziellen Datenträgern liest, die mit dem Befehl MOVE DRMEDIA entnommen wurden. Bei der Installation wird der Wert für DRMCHECKLABEL auf YES gesetzt.

Mit dem Befehl QUERY DRMSTATUS kann die aktuelle Einstellung überprüft werden.

 AIX-Betriebssysteme  Linux-BetriebssystemeDieser Befehl gilt nicht für Einheitentypen 349X.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                       .-Yes-.
>>-Set DRMCHECKLabel--+-----+---------------------------------><
                      +-Yes-+
                      '-No--'
```

Parameter

Yes
: Gibt an, dass IBM Spectrum Protect die Kennsätze sequenzieller Datenträgern liest, die mit dem Befehl MOVE DRMEDIA entnommen wurden.

No
: Gibt an, dass IBM Spectrum Protect die Kennsätze sequenzieller Datenträger, die mit dem Befehl MOVE DRMEDIA entnommen wurden, nicht liest.

Beispiel: Angeben, dass keine Kennsatzprüfung durchgeführt werden soll

Geben Sie an, dass keine Kennsatzprüfung ausgeführt wird.

```
set drmchecklabel no
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCHECKLABEL

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

SET DRMCMDFILENAME (Namen einer Datei angeben, die Befehle enthalten soll)

Mit diesem Befehl kann eine Datei angegeben werden, die die Befehle enthalten kann, die bei der Ausgabe der Befehle MOVE DRMEDIA und QUERY DRMEDIA erstellt werden. Wird der Befehl SET DRMCMDFILENAME nicht ausgegeben, generiert der Befehl MOVE DRMEDIA oder QUERY DRMEDIA einen Dateinamen.

Mit dem Befehl QUERY DRMSTATUS kann der aktuelle Name der Befehlsdatei angezeigt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set DRMCMDFilename--Dateiname------------------------------><
```

Parameter

Dateiname (Erforderlich)

AIX-BetriebssystemeLinux-BetriebssystemeGibt einen vollständigen Pfadnamen für eine Datei an, die die von dem Befehl MOVE DRMEDIA oder QUERY DRMEDIA erstellten Befehle enthalten soll.

Windows-BetriebssystemeGibt einen vollständigen Pfadnamen für eine Datei an, die die von dem Befehl MOVE DRMEDIA oder QUERY DRMEDIA erstellten Befehle enthalten soll. Der Dateiname kann bis zu 259 Zeichen umfassen.

Achtung: Ist eine Datei mit demselben Namen bereits vorhanden, versucht der Befehl MOVE DRMEDIA oder QUERY DRMEDIA, die Datei zu verwenden. Die vorhandenen Daten werden dann überschrieben.

Beispiel: Den Namen einer Datei angeben, die DRMEDIA-Befehle enthalten soll

AIX-BetriebssystemeLinux-BetriebssystemeDen Dateinamen /adsm/drm/orm/exec.cmds angeben.

```
set drmcmdfilename /adsm/drm/orm/exec.cmds
```

Windows-BetriebssystemeDen Dateinamen c:\drm\orm\exec.cmd angeben.

```
set drmcmdfilename c:\drm\orm\exec.cmd
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCMDFILENAME

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

SET DRMCOPYCONTAINERSTGPOOL (Containerkopienspeicherpools angeben, die von DRM-Befehlen verarbeitet werden sollen)

Verwenden Sie diesen Befehl, um die Containerkopienspeicherpools anzugeben, die vom Befehl MOVE DRMEDIA oder QUERY DRMEDIA verarbeitet werden sollen, wenn dieser Befehl nicht den Parameter COPYCONTAINERSTGPOOL enthält.

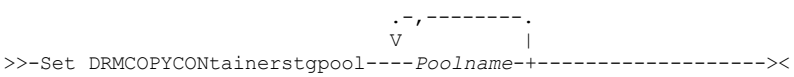
Standardmäßig werden Datenträger in Containerkopienspeicherpools von den Befehlen MOVE DRMEDIA und QUERY DRMEDIA nicht verarbeitet. Um die Datenträger zu verarbeiten, müssen Sie den Befehl SET DRMCOPYCONTAINERSTGPOOL ausgeben oder den Parameter COPYCONTAINERSTGPOOL im Befehl MOVE DRMEDIA oder QUERY DRMEDIA verwenden.

Tipp: Um die aktuellen Einstellungen anzuzeigen, verwenden Sie den Befehl QUERY DRMSTATUS.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Poolname (Erforderlich)
: Gibt die Namen der Containerkopienspeicherpools an. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden. Die angegebenen Namen ersetzen die vorherigen Einstellungen. Wird eine Nullzeichenfolge ("") eingegeben, werden alle aktuellen Namen entfernt.

Beispiel: Speicherpools angeben, die von den Befehlen MOVE DRMEDIA und QUERY DRMEDIA verarbeitet werden sollen

CONTCOPY1 und CONTCOPY2 als Containerkopienspeicherpools definieren, die verarbeitet werden sollen.

```
set drmcopycontainerstgpool contcopy1,contcopy2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCOPYCONTAINERSTGPOOL

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

SET DRMCOPYSTGPOOL (Von DRM zu verwaltende Kopienspeicherpools angeben)

Mit diesem Befehl können Namen von Kopienspeicherpools angegeben werden, die nach einem Unglück wiederhergestellt werden sollen. IBM Spectrum Protect verwendet diese Namen, wenn der Befehl PREPARE nicht den Parameter COPYSTGPOOL enthält.

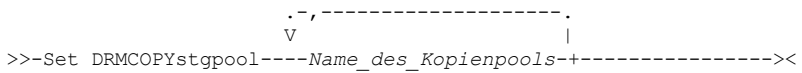
Wenn der Befehl MOVE DRMEDIA oder QUERY DRMEDIA nicht den Parameter COPYSTGPOOL enthält, werden mit dem Befehl die Datenträger im Status MOUNTABLE verarbeitet, die sich in dem im Befehl SET DRMCOPYSTGPOOL angegebenen Kopienspeicherpool befinden. Bei der Installation sind alle Kopienspeicherpools für die DRM-Verarbeitung auswählbar.

Mit dem Befehl QUERY DRMSTATUS können die aktuellen Einstellungen angezeigt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Name_des_Kopienpools (Erforderlich)
: Gibt die Namen der Kopienspeicherpools an. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Es können Platzhalterzeichen verwendet werden. Die angegebenen Namen ersetzen die vorherigen Einstellungen. Wird eine Nullzeichenfolge ("") eingegeben, werden alle aktuellen Namen entfernt, und alle Kopienspeicherpools sind für die Verarbeitung auswählbar.

Beispiel: Einen auswählbaren Kopienspeicherpool definieren

COPYSTGPOOL1 als auswählbaren Kopienspeicherpool definieren.

```
set drmcopystgpool copystgpool1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCOPYSTGPOOL

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.
SET DRMPRIMSTGPOOL	Gibt an, dass primäre Speicherpools von DRM verwaltet werden.

SET DRMCOURIERNAME (Kuriernamen angeben)

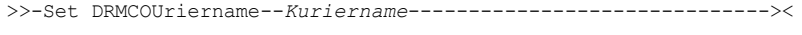
Mit diesem Befehl kann der Name des Kuriers angegeben werden. Bei der Installation wird dieser Name auf COURIER gesetzt. Der Befehl MOVE DRMEDIA verwendet den Kuriernamen, um den Standort von Datenträgern anzugeben, die in den Status COURIER übergehen.

Mit dem Befehl QUERY DRMSTATUS kann der Kuriername abgefragt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Kuriername (Erforderlich)
: Gibt den Namen des Kuriers an. Der Name kann bis zu 255 Zeichen umfassen. Den Namen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Beispiel: Den Kuriernamen definieren

Den Namen des Kuriers als Joe's Courier Service definieren.

```
set drmcouriername "Joe's Courier Service"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMCOURIERNAME

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsserie angeben)

Mit diesem Befehl kann angegeben werden, wann eine Datenbanksicherungsserie für die Verfallsverarbeitung ausgewählt werden kann.

Der mit diesem Befehl definierte Wert gilt sowohl für eine Sicherungsserie mit Datenbankmomentaufnahmen als auch für eine Gesamt- und Teilsicherungsserie der Datenbank. Jede Art von Datenbanksicherungsserie kann für die Verfallsverarbeitung ausgewählt werden, wenn alle folgenden Bedingungen zutreffen:

- Das Alter des letzten Datenträgers der Serie überschreitet den mit dem Befehl SET DRMDBBACKUPEXPIREDAYS definierten Verfallswert und den für den Parameter DELgraceperiod im Befehl DEFINE SERVER angegebenen Wert. Der Parameter DELgraceperiod gilt nur für ferne Datenbanksicherungen. Der Standardwert für den Parameter DELgraceperiod sind 5 Tage. Wenn Sie beispielsweise den Wert für den Befehl SET DRMDBBACKUPEXPIREDAYS auf 7 Tage und den Wert für den Parameter DELgraceperiod auf 6 Tage setzen, verfällt die Serie ferner Datenbanksicherungen erst nach 13 Tagen.
- Bei Datenträgern, die keine virtuellen Datenträger sind, befinden sich alle Datenträger in der Serie im Status VAULT.
- Der Datenträger ist nicht Teil der letzten Datenbanksicherungsserie.

Hinweis: Die letzte Sicherungsserie jeder Art wird nicht gelöscht.
Weitere Informationen zum Verfall von Datenbanksicherungsdatenträgern, die keine virtuellen Datenträger sind, befinden sich in der Beschreibung des Befehls MOVE DRMEDIA. Weitere Informationen zum Verfall von Datenbanksicherungsdatenträgern, die virtuelle Datenträger sind, befinden sich in der Beschreibung des Befehls EXPIRE INVENTORY.

Mit dem Befehl QUERY DRMSTATUS kann die angegebene Anzahl der Tage angezeigt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set DRMDBBackupexpiredays--Tage-----------------------------><
```

Parameter

Tage (Erforderlich)
: Gibt die Anzahl Tage an, die seit der Erstellung einer Datenbankserie vergangen sein müssen, bevor sie für die Verfallsverarbeitung ausgewählt werden kann. Die Anzahl der Tage muss mit dem Verzögerungszeitraum für die Wiederverwendung von Datenträgern für Kopienspeicherpools übereinstimmen, die von Disaster Recovery Manager verwaltet werden. Geben Sie einen ganzzahligen Wert zwischen 0 und 9999 an.

Beispiel: Den Verfall der Datenbanksicherungsserie definieren

Der Verfallswert für die Datenbanksicherungsserie soll auf 60 gesetzt werden.

```
set drmdbbackupexpiredays 60
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMDBBACKUPEXPIREDAYS

Befehl	Beschreibung
DSMSERV RESTORE DB	Schreibt eine IBM Spectrum Protect-Datenbank zurück.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.

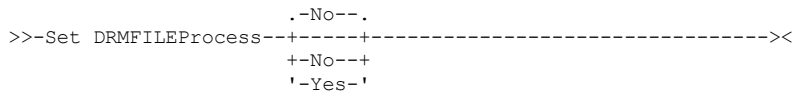
SET DRMFILEPROCESS (Dateiverarbeitung angeben)

Mit diesem Befehl kann angegeben werden, ob der Befehl MOVE DRMEDIA oder QUERY DRMEDIA Datenbanksicherungsdatenträger und Kopienspeicherpooldatenträger verarbeiten soll, die der Einheitenklasse FILE zugeordnet sind. Bei der Installation wird der Wert auf NO gesetzt. Mit dem Befehl QUERY DRMSTATUS kann die aktuelle Einstellung angezeigt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

No
: Gibt an, dass die Befehle MOVE DRMEDIA und QUERY DRMEDIA keine Datenbanksicherungs- und Kopienspeicherpooldatenträger verarbeiten, die der Einheitenklasse FILE zugeordnet sind. Dies ist der Standardwert.

Yes
: Gibt an, dass die Befehle MOVE DRMEDIA und QUERY DRMEDIA Datenbanksicherungs- und Kopienspeicherpooldatenträger verarbeiten, die der Einheitenklasse FILE zugeordnet sind.

Beispiel: Angeben, dass die DRMEDIA-Befehle keine Einheitenklassen des Typs FILE einschließen

Der Dateiverarbeitungswert soll auf 'No' gesetzt werden.

```
set drmfileprocess no
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMFILEPROCESS

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

SET DRMINSTRPREFIX (Präfix für Wiederherstellungsanweisungsdateinamen angeben)

Mit diesem Befehl kann ein Präfix für den Namen der Wiederherstellungsanweisungsdatei angegeben werden. Wenn dieser Befehl ausgegeben wird, verwendet IBM Spectrum Protect das angegebene Präfix, wenn der Befehl PREPARE ohne den Parameter INSTRPREFIX ausgegeben wird.

Mit dem Befehl QUERY DRMSTATUS kann der aktuelle Wert für das Präfix angezeigt werden.

AIX-BetriebssystemeLinux-BetriebssystemeDas Präfix ist das aktuelle Arbeitsverzeichnis des IBM Spectrum Protect-Servers.

Windows-BetriebssystemeWird kein Präfix definiert, wird das Präfix auf das Verzeichnis gesetzt, das dieses Exemplar des Servers darstellt (normalerweise das Verzeichnis, aus dem der Server ursprünglich installiert wurde).

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set DRMINSTRPrefix--Präfix---------------------------------><
```

Parameter

AIX-BetriebssystemeLinux-BetriebssystemePräfix (Erforderlich)
AIX-BetriebssystemeLinux-Betriebssysteme

Gibt ein Pfadnamenpräfix für die Dateien an, die die Wiederherstellungsanweisungen enthalten. Bei der Verarbeitung des Befehls PREPARE hängt IBM Spectrum Protect den Namen der entsprechenden Zeilengruppe für die Wiederherstellungsplandatei an, um die Datei zu lokalisieren. Die maximale Länge beträgt 250 Zeichen.

Das Präfix kann Folgendes sein:

- **Verzeichnispfad:** Das Präfix mit einem Schrägstrich (/) beenden. Beispiel:

  ```
  /adsmsrv/recinstr/
  ```

  Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt lauten:

  ```
  /adsmsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
  ```

- **Verzeichnispfad gefolgt von einer Zeichenfolge:** IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

  ```
  /adsmsrv/recinstr/accounts
  ```

  Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt lauten:

  ```
  /adsmsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
  ```

- **Nur Zeichenfolge:** IBM Spectrum Protect gibt den Verzeichnispfad an und hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an.
  - IBM Spectrum Protect verwendet den Namen des aktuellen Arbeitsverzeichnisses. Das aktuelle Arbeitsverzeichnis lautet beispielsweise /opt/tivoli/tsm/server/bin. Sie geben Folgendes an:

    ```
    shipping
    ```

    Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt aussehen:

    ```
    /opt/tivoli/tsm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
    ```

Windows-BetriebssystemePräfix (Erforderlich)
Windows-Betriebssysteme

Gibt ein Pfadnamenpräfix für die Dateien an, die die Wiederherstellungsanweisungen enthalten. Bei der Verarbeitung des Befehls PREPARE hängt IBM Spectrum Protect den Namen der entsprechenden Zeilengruppe für die Wiederherstellungsplandatei an, um die Datei zu lokalisieren. Die maximale Länge beträgt 200 Zeichen.

Das Präfix kann Folgendes sein:

- **Verzeichnispfad:** Das Präfix mit einem umgekehrten Schrägstrich (\) beenden. Beispiel:

  ```
  c:\adsmsrv\recinstr\
  ```

  Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt lauten:

  ```
  c:\adsmsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
  ```

- **Verzeichnispfad gefolgt von einer Zeichenfolge:** IBM Spectrum Protect behandelt die Zeichenfolge als Teil des Dateinamens. Beispiel:

  ```
  c:\adsmsrv\recinstr\accounts
  ```

Für die Datei RECOVERY.INSTRUCTIONS.GENERAL würde der daraus resultierende Dateiname wie folgt lauten:

```
c:\adsmsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

- **Nur Zeichenfolge:** IBM Spectrum Protect gibt den Verzeichnispfad an und hängt den entsprechenden Namen der Zeilengruppe für die Wiederherstellungsplandatei an. Der Verzeichnispfad ist das Verzeichnis, das dieses Exemplar des IBM Spectrum Protect-Servers darstellt (normalerweise das ursprüngliche Installationsverzeichnis des IBM Spectrum Protect-Servers). Beispielsweise lautet das Verzeichnis, das dieses Exemplar des Servers darstellt, c:\Programme\Tivoli\TSM;\server2, und das folgende Präfix wird angegeben:

  ```
  shipping
  ```

  Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

  ```
  c:\Programme\Tivoli\TSM;\server2\shipping.19971115.051421
  ```

Beispiel: Das Präfix für den Wiederherstellungsplan angeben

 AIX-Betriebssysteme  Linux-BetriebssystemeAngeben, dass die Wiederherstellungsplananweisungen aus dem Verzeichnis /drmplan/primesrv gelesen werden sollen.

```
set drminstrprefix /drmplan/primesrv/
```

 Windows-BetriebssystemeAngeben, dass die Wiederherstellungsplananweisungen aus dem Verzeichnis c:\win32app\ibm\adsm\server2\ gelesen werden sollen.

```
set drminstrprefix c:\win32app\ibm\adsm\server2\
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMINSTRPREFIX

Befehl	Beschreibung
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

SET DRMNOTMOUNTABLENAME (Nicht mountfähigen Standort angeben)

Mit diesem Befehl kann der Name des Standorts vor Ort zum Speichern der Datenträger angegeben werden. Bei der Installation wird der Name auf NOTMOUNTABLE gesetzt. Mit dem Befehl QUERY DRMSTATUS kann der Standortname angezeigt werden.

Der Standortname wird vom Befehl MOVE DRMEDIA verwendet, um den Standort von Datenträgern anzugeben, die in den Status NOTMOUNTABLE übergehen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set DRMNOTMOuntablename--Standort---------------------------><
```

Parameter

Standort (Erforderlich)
: Gibt den Namen des Standorts vor Ort zum Speichern der Datenträger an. Der Name kann bis zu 255 Zeichen umfassen. Den Namen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Beispiel: Den Namen des Standorts vor Ort angeben

Den Namen des Standorts auf room 123/31 setzen.

```
set drmnotmountablename "room 123/31"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMNOTMOUNTABLENAME

Befehl	Beschreibung

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

SET DRMPLANPREFIX (Präfix für Wiederherstellungsplandateinamen angeben)

Mit diesem Befehl kann ein Präfix für einen Wiederherstellungsplandateinamen angegeben werden.

Wenn dieser Befehl ausgegeben wird, verwendet IBM Spectrum Protect das angegebene Präfix, wenn der Befehl PREPARE nicht den Parameter PLANPREFIX enthält.

Mit dem Befehl QUERY DRMSTATUS kann der aktuelle Wert für das Wiederherstellungsplanpräfix angezeigt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set DRMPLANPrefix--Präfix----------------------------------><
```

Parameter

AIX-BetriebssystemeLinux-BetriebssystemePräfix (Erforderlich)
AIX-BetriebssystemeLinux-BetriebssystemeGibt das Präfix für den Namen einer Wiederherstellungsplandatei an. Die maximale Länge des Präfix beträgt 250 Zeichen. Wird eine Nullzeichenfolge ("") eingegeben, wird das aktuelle Präfix entfernt, und der Server verwendet den Algorithmus, der im Parameter PLANPREFIX im Befehl PREPARE beschrieben ist.
Für das Präfix kann folgendes angegeben werden:

- **Ein Verzeichnispfad gefolgt von einem Schrägstrich (/):** IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `jjjjmmtt.hhmmss` an. Beispielsweise wird SET DRMPLANPREFIX auf folgenden Wert gesetzt:

  ```
  /adsmsrv/recplans/
  ```

  Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

  ```
  /adsmsrv/recplans/19971115.051421
  ```

- **Ein Verzeichnispfad gefolgt von einer Zeichenfolge:** IBM Spectrum Protect verwendet die Zeichenfolge als Teil des Dateinamens. IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `.jjjjmmtt.hhmmss` an (den Punkt am Anfang beachten). Beispielsweise wird SET DRMPLANPREFIX auf folgenden Wert gesetzt:

  ```
  /adsmsrv/recplans/accounting
  ```

  Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

  ```
  /adsmsrv/recplans/accounting.19971115.051421
  ```

- **Eine Zeichenfolge, der kein Verzeichnispfad vorausgeht:** IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `.jjjjmmtt.hhmmss` an (den Punkt am Anfang beachten). IBM Spectrum Protect bestimmt den Verzeichnispfad wie folgt:
  - IBM Spectrum Protect verwendet den Verzeichnispfadnamen des aktuellen Arbeitsverzeichnisses des IBM Spectrum Protect-Servers. Beispielsweise lautet das aktuelle IBM Spectrum Protect-Arbeitsverzeichnis /opt/tivoli/tsm/server/bin. Der Befehl SET DRMPLANPREFIX ist auf folgenden Wert gesetzt:

    ```
    shipping
    ```

    Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

    ```
    /opt/tivoli/tsm/server/bin/shipping.19971115.051421
    ```

Windows-BetriebssystemePräfix (Erforderlich)
Windows-BetriebssystemeGibt ein Präfix für den Pfadnamen an, das zum Generieren des Wiederherstellungsplandateinamens verwendet wird. Das Präfix kann bis zu 200 Zeichen umfassen. IBM Spectrum Protect verwendet das Präfix, wenn der Befehl PREPARE ohne den Parameter PLANPREFIX ausgegeben wird. IBM Spectrum Protect erstellt einen eindeutigen Wiederherstellungsplandateinamen, indem an das Präfix das Datum und die Uhrzeit im Format `jjjjmmtt.hhmmss` angehängt wird (zum Beispiel 19951115.051421). Wenn Sie eine Nullzeichenfolge ("") eingeben, wird das aktuelle Präfix entfernt und der Server verwendet den Algorithmus, der im Parameter PLANPREFIX im Befehl PREPARE beschrieben ist.

Für das Präfix kann folgendes angegeben werden:

1. Ein Verzeichnispfad
2. Ein Verzeichnispfad, gefolgt von einer Zeichenfolge
3. Eine Zeichenfolge

Nachfolgend sind die Regeln für die Angabe von möglichen Präfixen beschrieben:

1. Soll ein Verzeichnispfad für das Präfix angegeben werden, muss das Präfix mit einem umgekehrten Schrägstrich (\) beendet werden. IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `jjjjmmtt.hhmmss` an. Beispielsweise ist SET DRMPLANPREFIX auf den folgenden Wert gesetzt:

   ```
   c:\adsmsrv\recplans\
   ```

   Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

   ```
   c:\adsmsrv\recplans\19951115.051421
   ```

   Wichtig: Wird der Befehl SET DRMPLANPREFIX von einem Befehlszeilenclient ausgegeben und ist das letzte Zeichen in der Befehlszeile ein umgekehrter Schrägstrich, interpretiert IBM Spectrum Protect das Zeichen als Fortsetzungszeichen. Um dies zu vermeiden, das Präfix in Anführungszeichen einschließen. Beispiel: `"c:\adsmsrv\recplans\"`
2. Ist das Präfix ein Verzeichnispfad gefolgt von einer Zeichenfolge, verwendet IBM Spectrum Protect die Zeichenfolge als Teil des Dateinamens. IBM Spectrum Protect hängt an das Präfix das Datum und die Uhrzeit im Format `.jjjjmmtt.hhmmss` an (den Punkt am Anfang beachten). Beispielsweise ist SET DRMPLANPREFIX auf den folgenden Wert gesetzt:

   ```
   c:\adsmsrv\recplans\accounting
   ```

   Der hierdurch erstellte Name der Wiederherstellungsplandatei würde wie folgt lauten:

   ```
   c:\adsmsrv\recplans\accounting.19951115.051421
   ```

3. Ist das Präfix eine Zeichenfolge, der kein Verzeichnispfad vorausgeht, hängt IBM Spectrum Protect an das Präfix das Datum und die Uhrzeit im Format `.jjjjmmtt.hhmmss` an (den Punkt am Anfang beachten). Der Verzeichnispfad, der von IBM Spectrum Protect verwendet wird, ist der Verzeichnispfad, der dieses Exemplar des IBM Spectrum Protect-Servers darstellt (normalerweise das Verzeichnis, aus dem der IBM Spectrum Protect-Server ursprünglich installiert wurde). Beispielsweise lautet das Verzeichnis, das dieses Exemplar des Servers darstellt, c:\Programme\Tivoli\TSM;\server2, und das Präfix wird auf folgenden Wert gesetzt:

   ```
   shipping
   ```

   Der daraus resultierende Name der Wiederherstellungsplandatei lautet:

   ```
   c:\Programme\Tivoli\TSM;\server2\shipping.19951115.051421
   ```

Beispiel: Ein Präfix für Wiederherstellungsplandateinamen angeben

Ein Präfix angeben, so dass die generierten Wiederherstellungsplandateien in dem folgenden Verzeichnis gespeichert werden:

- AIX-BetriebssystemeLinux-Betriebssysteme/drmplan/primsrv
- Windows-Betriebssystemec:\drmtest\prepare\

Den folgenden Befehl ausgeben: AIX-BetriebssystemeLinux-Betriebssysteme

```
set drmplanprefix /drmplan/primsrv/
```

Windows-Betriebssysteme

```
set drmplanprefix c:\drmtest\prepare\
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMPLANPREFIX

Befehl	Beschreibung
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

SET DRMPLANVPOSTFIX (Namen für Ersatzdatenträger angeben)

Mit diesem Befehl kann das Zeichen angegeben werden, das an Ersatzdatenträgernamen in der Wiederherstellungsplandatei angehängt werden soll. Das Zeichen kann Ihnen beim Suchen oder Generieren von Ersatzdatenträgernamen helfen, wenn Sie die Wiederherstellungsplandatei verwenden.

Bei der Installation wird das Zeichen auf @ gesetzt. IBM Spectrum Protect generiert Ersatznamen für Datenträger im primären Speicherpool, die mit dem Befehl DEFINE VOLUME hinzugefügt wurden. Das angehängte Zeichen verwenden, um

- Ersatzdatenträgernamen in den Zeilengruppen des Wiederherstellungsplans zu suchen, so daß die Namen zum Zeitpunkt der Wiederherstellung geändert werden können. Beispielsweise sind unter Umständen die Namen der verfügbaren Banddatenträger am Wiederherstellungsort nicht bekannt.
- Ersatzdatenträgernamen zu generieren. Es wird eine Namenskonvention benötigt, die sich auf alle Einheitentypen in den primären Speicherpools anwenden läßt. Folgendes beachten:
  - Die generierte Länge des Ersatzdatenträgernamens
  - Welche Zeichen dürfen für den Namen von Ersatzdatenträgern verwendet werden?
  - Wie ist bei Konflikten mit bestehenden Datenträgernamen vorzugehen?
  - Ein Ersatzdatenträgername darf nicht mit dem Namen eines zerstörten, vorhandenen oder neuen Datenträgers übereinstimmen.

Mit dem Befehl QUERY DRMSTATUS kann das Zeichen angezeigt werden, das an das Ende der Ersatzdatenträgernamen hinzugefügt wurde.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set DRMPLANVpostfix--Zeichen--------------------------------><
```

Parameter

Zeichen (Erforderlich)
Gibt das Zeichen an, das an die Ersatzdatenträgernamen in der Wiederherstellungsplandatei angehängt werden soll. Ein alphanumerisches Zeichen oder Sonderzeichen angeben.
 AIX-BetriebssystemeAchtung: Ein Sonderzeichen kann zu unvorhersehbaren Ergebnissen in der AIX-Shell oder Befehlszeilenumgebung führen.
 Windows-BetriebssystemeAchtung: Ein Sonderzeichen kann zu unvorhersehbaren Ergebnissen in der Windows-Stapel-/-Befehlszeilenumgebung führen.

Beispiel: Das angehängte Zeichen für Ersatzdatenträgernamen angeben

Für das Zeichen, das an die Ersatzdatenträgernamen angehängt wird, soll R definiert werden.

```
set drmplanvpostfix R
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMPLANVPOSTFIX

Befehl	Beschreibung
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

SET DRMPRIMSTGPOOL (Von DRM zu verwaltende primäre Speicherpools angeben)

Mit diesem Befehl können die Namen von primären Speicherpools angegeben werden, die wiederhergestellt werden sollen. Enthält der Befehl PREPARE nicht den Parameter PRIMSTGPOOL, verarbeitet DRM die in diesem Befehl angegebenen Namen.

Mit dem Befehl QUERY DRMSTATUS können die aktuellen Einstellungen angezeigt werden. Bei der Installation sind alle für den Server definierten primären Speicherpools für die DRM-Verarbeitung auswählbar.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                .-,----------------------.
                V                        |
```

```
>>-Set DRMPRIMstgpool----Name_des_primären_Pools-+------------><
```

Parameter

Name_des_primären_Pools (Erforderlich)
Gibt die Namen der primären Speicherpools an, die wiederhergestellt werden sollen. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Die angegebenen Namen ersetzen die vorherigen Einstellungen. Wird eine Nullzeichenfolge ("") eingegeben, werden alle aktuellen Namen entfernt, und alle primären Speicherpools sind für die DRM-Verarbeitung auswählbar.

Beispiel: Einen primären Speicherpool definieren, der von DRM verwaltet werden soll

Den primären Speicherpool, der von DRM verwaltet werden soll, auf PRIMSTGPOOL1 setzen.

```
set drmprimstgpool primstgpool1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMPRIMSTGPOOL

Befehl	Beschreibung
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.
SET DRMCOPYSTGPOOL	Gibt an, dass Kopienspeicherpools von DRM verwaltet werden.

SET DRMRPFEXPIREDAYS (Kriterien für Verfall von Wiederherstellungsplandateien definieren)

Mit diesem Befehl kann angegeben werden, wann Wiederherstellungsplandateien für die Verfallsverarbeitung ausgewählt werden können. Dieser Befehl und die Verfallsverarbeitung gelten nur für Wiederherstellungsplandateien, die mit dem Parameter DEVCLASS erstellt wurden, der im Befehl PREPARE angegeben wurde (d. h. virtuelle Datenträger des Typs RPFILE und RPSNAPSHOT). Mit der Verfallsverarbeitung auf dem Quellenserver werden Plandateien, die auf dem Zielserver gespeichert sind, als verfallen gekennzeichnet. Lokal erstellte Wiederherstellungsplandateien verfallen nicht.

Eine RPFILE-Datei ist einer Gesamt- und Teilsicherungsserie der Datenbank zugeordnet. Eine RPFSNAPSHOT-Datei ist einer Sicherungsserie mit Datenbankmomentaufnahmen zugeordnet.

Achtung: Die neuesten RPFILE- und RPFSNAPSHOT-Dateien werden nie gelöscht.
Eine Wiederherstellungsplandatei kann für die Verfallsverarbeitung ausgewählt werden, wenn die beiden folgenden Bedingungen zutreffen:

- Die letzte Wiederherstellungsplandatei der Serie überschreitet den im Befehl SET DRMRPFEXPIREDAYS angegebenen Verfallswert und den für den Parameter DELgraceperiod im Befehl DEFINE SERVER angegebenen Wert. Der Standardwert für den Parameter DELgraceperiod sind 5 Tage. Wenn Sie beispielsweise den Wert für den Befehl SET DRMRPFEXPIREDAYS auf 80 Tage und den Wert für den Parameter DELgraceperiod auf 6 Tage setzen, verfällt die Wiederherstellungsplandatei erst nach 86 Tagen.
- Die letzte Wiederherstellungsplandatei ist nicht der neuesten Datenbanksicherungsserie zugeordnet.

Weitere Informationen zur Verfallsverarbeitung befinden sich in der Beschreibung des Befehls EXPIRE INVENTORY.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set DRMRPFEXpiredays--Tage---------------------------------><
```

Parameter

Tage (Erforderlich)
Gibt die Anzahl Tage an, die verstreichen müssen, bevor eine Wiederherstellungsplandatei verfällt. Sie können eine Zahl von 0 bis 9999 angeben. Bei der Installation wird dieser Wert auf 60 gesetzt.

Beispiel: Den Verfall des Wiederherstellungsplans definieren

Der Verfallswert für die Wiederherstellungsplandatei soll auf 30 gesetzt werden.

```
set drmrpfexpiredays 30
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMRPFEXPIREDAYS

Befehl	Beschreibung
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.
QUERY RPFCONTENT	Zeigt den Inhalt einer Wiederherstellungsplandatei an.
QUERY RPFILE	Zeigt Informationen über Wiederherstellungsplandateien an.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.
SET DRMDBBACKUPEXPIREDAYS	Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.

SET DRMVAULTNAME (Aufbewahrungsort angeben)

Mit diesem Befehl kann der Name des Aufbewahrungsorts angegeben werden. Bei der Installation wird der Name auf VAULT gesetzt. Mit dem Befehl QUERY DRMSTATUS kann der Name des Aufbewahrungsorts angezeigt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-SET DRMVAultname--Name_des_Aufbewahrungsorts----------------><
```

Parameter

Name_des_Aufbewahrungsorts (Erforderlich)
: Gibt den Namen des Aufbewahrungsorts an. Der Name kann bis zu 255 Zeichen umfassen. Den Namen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Beispiel: Den Namen eines Aufbewahrungsorts angeben

`ironmountain` als Namen des Aufbewahrungsorts angeben.

```
set drmvaultname ironmountain
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET DRMVAULTNAME

Befehl	Beschreibung
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY DRMSTATUS	Zeigt DRM-Systemparameter an.

SET EVENTRETENTION (Aufbewahrungszeitraum für Ereignissätze definieren)

Mit diesem Befehl kann der Aufbewahrungszeitraum für Ereignissätze in der Server-Datenbank definiert werden, mit dem abgeschlossene Zeitpläne überwacht werden können. Ein Ereignissatz wird erstellt, wenn die Verarbeitung eines geplanten Befehls gestartet wird oder fehlschlägt.

Der Aufbewahrungszeitraum für Ereignisdaten kann so angepaßt werden, dass unzureichende oder veraltete Daten vermieden werden. Der Server entfernt die Ereignissätze automatisch aus der Datenbank, wenn das Ende des Aufbewahrungszeitraums erreicht und das Startfenster für das Ereignis abgelaufen ist.

Mit dem Befehl QUERY EVENT können Informationen zu geplanten und abgeschlossenen Ereignissen angezeigt werden.

Mit dem Befehl DELETE EVENT können Ereignissätze gelöscht werden, und zwar unabhängig davon, ob der Aufbewahrungszeitraum abgelaufen ist.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Wert für den Aufbewahrungszeitraum anzuzeigen. Bei der Installation wird dieser Wert auf 10 Tage gesetzt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set EVentretention--Tage-----------------------------------><
```

Parameter

Tage (Erforderlich)
: Die Anzahl der Tage, die Ereignissätze in der Datenbank aufbewahrt werden. Zulässige Werte sind ganze Zahlen von 0 bis 9999. Der Wert 0 gibt an, dass nur Ereignissätze für den aktuellen Tag aufbewahrt werden.

Beispiel: Den Aufbewahrungszeitraum für Ereignissätze definieren

Den Aufbewahrungszeitraum auf 15 Tage setzen.

```
set eventretention 15
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET EVENTRETENTION

Befehl	Beschreibung
DELETE EVENT	Löscht Ereignissätze, die vor einem bestimmten Zeitpunkt erstellt wurden.
QUERY EVENT	Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET FAILOVERHLADDRESS (Adresse höherer Ebene für Übernahme definieren)

Verwenden Sie diesen Befehl, um die IP-Adresse anzugeben, die ein Client während der Übernahme (Failover) für die Herstellung der Verbindung zu diesem Server als sekundärer Replikationsserver verwendet, wenn die Adresse von der IP-Adresse abweicht, die für den Replikationsprozess angegeben ist.

Sie müssen die Adresse des Servers angeben, die verwendet wird, wenn die Adresse der höheren Ebene abweicht. Dieser Befehl ist nur erforderlich, wenn Sie separate dedizierte Netze für die Übertragung zwischen Servern und den Clientzugriff verwenden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-SET FAILOVERHladdress--Adresse der höheren Ebene------------><
```

Parameter

Adresse der höheren Ebene (Erforderlich)

Gibt die Adresse der höheren Ebene eines Servers als numerischen Namen in Schreibweise mit Trennzeichen oder als Hostnamen für die Verwendung während der Übernahme an. Wenn Sie einen Hostnamen angeben, muss ein Server verfügbar sein, der den Namen in das Format in Schreibweise mit Trennzeichen auflösen kann.

Um die IP-Übernahmeadresse zu entfernen, geben Sie den Befehl ohne Angabe eines Werts aus.

Beispiel: Adresse der höheren Ebene für die Übernahme definieren

Der Name der Adresse der höheren Ebene, der für Übernahmeoperationen auf diesem Server definiert werden soll.

```
set failoverhladdress server1
```

Beispiel: Adresse der höheren Ebene entfernen

Um eine Adresse der höheren Ebene für einen Übernahmeserver zu entfernen, geben Sie den folgenden Befehl aus:

```
set failoverhladdress
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für QUERY REPLSERVER

Befehl	Beschreibung
QUERY REPLSERVER (Replikationsserver abfragen)	Zeigt Informationen zu Replikationsservern an.
REMOVE REPLSERVER (Replikationsserver entfernen)	Entfernt einen Server aus der Replikation.

SET INVALIDPWLIMIT (Anzahl der ungültigen Anmeldeversuche definieren)

Mit diesem Befehl kann die Anzahl der zulässigen ungültigen Anmeldeversuche angegeben werden, bevor ein Knoten gesperrt wird.

Der Befehl SET INVALIDPWLIMIT gilt auch für LDAP-Verzeichnisserver, die komplexe Knotenkennwörter speichern. LDAP-Verzeichnisserver können die Anzahl der Anmeldeversuche mit ungültigen Kennwörtern unabhängig vom IBM Spectrum Protect-Server begrenzen. Möglicherweise soll der LDAP-Verzeichnisserver nicht für ungültige Anmeldeversuche für den IBM Spectrum Protect-Namensbereich konfiguriert werden, wenn Sie den Befehl SET INVALIDPWLIMIT verwenden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set--INVALIDPwlimit--Anzahl---------------------------------><
```

Parameter

Anzahl (Erforderlich)
Gibt an, wie viele ungültige Anmeldeversuche zulässig sind, bevor ein Knoten gesperrt wird.

Zulässige Werte sind ganze Zahlen von 0 bis 9999. Der Wert 0 bedeutet, dass nicht geprüft wird, ob ungültige Anmeldeversuche vorliegen. Der Wert 1 bedeutet, dass der Knoten vom Server gesperrt wird, wenn ein Benutzer einmal ein ungültiges Kennwort eingibt. Der Standardwert ist 0.

Wichtig: Wenn Ihr Kennwort mit einem LDAP-Verzeichnisserver authentifiziert wird, kann es vom LDAP-Server und vom IBM Spectrum Protect-Server verwaltet werden. Nicht alle IBM Spectrum Protect-Serverbefehle betreffen Kennwörter, die mit einem LDAP-Server authentifiziert werden. Beispielsweise haben die Befehle SET PASSEXP und RESET PASSEXP keine Auswirkungen auf Kennwörter, die mit einem LDAP-Verzeichnisserver authentifiziert werden. Sie können Ihre Kennwortfunktionen über den IBM Spectrum Protect-Server verwalten. Wenn Sie den Befehl SET INVALIDPWLIMIT ausgegeben haben, werden alle IBM Spectrum Protect-Kennwörter durch den Grenzwert gesteuert, den Sie definiert haben. Wird der LDAP-Verzeichnisserver zur Begrenzung der Anzahl der Anmeldeversuche mit ungültigen Kennwörtern konfiguriert, kann ein Konflikt auftreten.

Beispiel: Die Anzahl zulässiger ungültiger Anmeldeversuche definieren

Für die zulässige Anzahl ungültiger Anmeldeversuche soll der Wert 6 definiert werden.

```
set invalidpwlimit 6
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET INVALIDPWLIMIT

Befehl	Beschreibung

Befehl	Beschreibung
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET MINPWLENGTH	Legt die Mindestlänge für Clientkennwörter fest.

SET LDAPPASSWORD (LDAP-Kennwort für den Server definieren)

Verwenden Sie diesen Befehl, um ein Kennwort für die Benutzer-ID oder Konto-ID zu definieren, die mithilfe des Befehls SET LDAPUSER angegeben wurde.

Voraussetzung: Sie müssen die Option LDAPURL definieren und den Befehl SET LDAPUSER ausgeben, bevor Sie den Befehl SET LDAPPASSWORD ausgeben. Wenn die Option LDAPURL nicht definiert ist, wenn Sie das Benutzerkennwort für den Lightweight Directory Access Protocol-Server (LDAP-Server) festlegen, müssen Sie den IBM Spectrum Protect-Server nach dem Definieren der Option LDAPURL erneut starten.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set LDAPPassword--LDAP-Benutzerkennwort---------------------><
```

Parameter

LDAP-Benutzerkennwort
: Gibt das Kennwort an, das der IBM Spectrum Protect-Server verwendet, wenn er sich mit dem LDAP-Server authentifiziert. Das Kennwort darf maximal 64 Zeichen lang sein. Wenn Ihr Kennwort Gleichheitszeichen enthält, muss das vollständige Kennwort in Anführungszeichen eingeschlossen werden. Sie können die folgenden Zeichen verwenden:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Beispiel: LDAP-Kennwort festlegen

```
set ldappassword LdAp20&12PaSsWoRd
```

Beispiel: Ein LDAP-Kennwort definieren, das Gleichheitszeichen enthält

```
set ldappassword "LdAp=LastWoRd"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET LDAPPASSWORD

Befehl	Beschreibung
AUDIT LDAPDIRECTORY	Prüft einen von IBM Spectrum Protect gesteuerten Namensbereich auf einem LDAP-Verzeichnisserver.
SET DEFAULTAUTHENTICATION	Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an.
SET LDAPUSER	Definiert den Benutzer, der die Kennwörter und Administratoren auf dem LDAP-Verzeichnisserver überwacht.

SET LDAPUSER (ID für einen LDAP-Verzeichnisserver angeben)

Verwenden Sie diesen Befehl, um die ID eines Benutzers oder Kontos anzugeben, mit der auf einen LDAP-Server (LDAP = Lightweight Directory Access Protocol) zugegriffen werden kann.

Die angegebene ID muss über Lesezugriff auf die Konten auf dem LDAP-Server verfügen, die für die Authentifizierung verwendet werden. Um LDAP-IDs zu ändern oder Kennwörter für LDAP-IDs zurückzusetzen, muss die angegebene ID über Schreibberechtigung für die Konten auf dem LDAP-Server verfügen.

Tipp: Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set LDAPUser--LDAP-Benutzer-DN----------------------------><
```

Parameter

LDAP-Benutzer-DN
: Gibt die ID eines Benutzers oder Kontos an, mit der auf einen LDAP-Server zugegriffen werden kann.

Beispiel: Benutzer-ID mit Administratorberechtigung für die Durchführung von Operationen auf einem LDAP-Server angeben

Um einen Administrator mit der Benutzer-ID JACKSPRATT für ein US-Unternehmen mit dem Namen EXAMPLE anzugeben, geben Sie den folgenden Befehl aus:

```
set ldapuser JackSpratt@us.example.com
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET LDAPUSER

Befehl	Beschreibung
AUDIT LDAPDIRECTORY	Prüft einen von IBM Spectrum Protect gesteuerten Namensbereich auf einem LDAP-Verzeichnisserver.
SET DEFAULTAUTHENTICATION	Gibt die Standardkennwortauthentifizierungsmethode für alle Befehle REGISTER NODE oder REGISTER ADMIN an.
SET LDAPPASSWORD	Legt das Kennwort für den LDAPUSER fest.

SET LICENSEAUDITPERIOD (Dauer für Lizenzprüfung definieren)

Mit diesem Befehl kann das Zeitintervall in Tagen angegeben werden, in dem automatisch Lizenzprüfungen von IBM Spectrum Protect durchgeführt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                            .-30---.
>>-Set--LICenseauditperiod--+------+--------------------------><
                            '-Tage-'
```

Parameter

Tage
: Gibt die Anzahl Tage zwischen den automatischen Server-Lizenzprüfungen an. Dieser Parameter ist wahlfrei. Der Standardwert ist 30. Es kann eine ganze Zahl von 1 bis einschließlich 30 angegeben werden.

Beispiel: Eine 14-tägige Serverlizenzprüfung angeben

Angeben, dass der Server alle 14 Tage Lizenzen prüft.

```
set licenseauditperiod 14
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET LICENSEAUDITPERIOD

Befehl	Beschreibung
AUDIT LICENSES	Prüft die Einhaltung der definierten Lizenzen.
QUERY AUDITOCCUPANCY	Zeigt die Serverspeicherauslastung für einen Clientknoten an.
QUERY LICENSE	Zeigt Informationen über Lizenzen und Prüfvorgänge an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER LICENSE	Registriert eine Lizenz für den IBM Spectrum Protect-Server.

SET MAXCMDRETRIES (Maximale Anzahl Befehlswiederholungen definieren)

Mit diesem Befehl kann angegeben werden, wie oft ein Scheduler auf einem Client-Knoten maximal versuchen darf, einen geplanten Befehl, der fehlgeschlagen ist, zu wiederholen.

Der Befehl kann verwendet werden, um die maximale Anzahl Wiederholungen zu überschreiben, die von dem Client-Knoten angegeben wird. Der Wert eines Clients wird nur dann überschrieben, wenn der Client den Server ansprechen kann.

Dieser Befehl wird zusammen mit dem Befehl SET RETRYPERIOD verwendet, um die Zeit und die Anzahl Wiederholungen für die erneute Ausführung eines fehlgeschlagenen Befehls zu steuern.

Der Befehl QUERY STATUS kann ausgegeben werden, um die aktuelle Anzahl Wiederholungen anzuzeigen. Bei der Installation wird IBM Spectrum Protect so konfiguriert, daß jeder Client seine eigene Anzahl Wiederholungen festlegt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set MAXCMDRetries--+--------+-------------------------------><
                      '-Anzahl-'
```

Parameter

Zahl

Gibt an, wie oft der Scheduler auf einem Client-Knoten maximal versuchen darf, einen geplanten Befehl, der fehlgeschlagen ist, zu wiederholen. Dieser Parameter ist wahlfrei.

Standardmäßig bestimmt jeder Client seinen eigenen Wert für diesen Parameter. Zulässige Werte sind ganze Zahlen von 0 bis 9999. Näheres zum Definieren der maximalen Anzahl Befehlswiederholungen auf dem Client steht in der entsprechenden Client-Dokumentation.

Beispiel: Die maximale Anzahl der Befehlswiederholungen auf 2 setzen

Den fehlgeschlagenen Versuch, einen geplanten Befehl zu verarbeiten, nur zweimal wiederholen.

```
set maxcmdretries 2
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET MAXCMDRETRIES

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET RETRYPERIOD	Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.

SET MAXSCHEDSESSIONS (Maximale Anzahl geplanter Sitzungen definieren)

Mit diesem Befehl kann die Anzahl der Sitzungen definiert werden, die der Server für die Verarbeitung geplanter Operationen verwenden kann. Dieser Befehl gibt die maximal zulässige Anzahl geplanter Sitzungen als Prozentsatz aller verfügbaren Serversitzungen an.

Mit der Begrenzung der Anzahl der Sitzungen wird sichergestellt, dass einige Sitzungen für nicht geplante Operationen, wie Sichern oder Archivieren, verfügbar sind. Es kann entweder die Gesamtzahl der Sitzungen (mit dem Parameter MAXSESSIONS) oder der maximale Prozentsatz geplanter Sitzungen erhöht werden. Wird die Gesamtzahl der verfügbaren Sitzungen erhöht, kann dies jedoch negative Auswirkungen auf die Serverleistung haben. Wird der maximale Prozentsatz geplanter Sitzungen erhöht, kann dies die verfügbaren Sitzungen für nicht geplante Operationen verringern.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set MAXSCHedsessions--Prozent------------------------------><
```

Parameter

Prozent (Erforderlich)
Gibt den Prozentsatz der gesamten Server-Sitzungen an, die für geplante Operationen verwendet werden können. Zulässige Werte sind ganze Zahlen von 0 bis 100. Der Parameter MAXSESSIONS in der Serveroptionsdatei bestimmt die maximale Anzahl der insgesamt zur Verfügung stehenden Serversitzungen.

Wird der maximale Prozentsatz geplanter Sitzungen auf 0 gesetzt, können keine geplanten Ereignisse beginnen. Wird der maximale Prozentsatz geplanter Sitzungen auf 100 gesetzt, entspricht die maximale Anzahl geplanter Sitzungen dem Wert der Option MAXSESSIONS.

Tipp: Wenn die maximale Anzahl geplanter Sitzungen nicht mit dem Prozentsatz übereinstimmt, der im Befehl SET MAXSCHEDSESSIONS definiert wurde, führen Sie den Befehl SET MAXSCHEDSESSIONS erneut aus. Bestimmen Sie die Anzahl, die in der Option MAXSESSIONS angegeben ist. Wenn die Anzahl in der Option MAXSESSIONS geändert und der Befehl SET MAXSCHEDSESSIONS seit der Änderung nicht ausgegeben wurde, kann sich die maximale Anzahl geplanter Sitzungen ändern.

Maximal 20 Sitzungen für geplante Aktivitäten definieren

Die Option MAXSESSIONS hat den Wert 80. Sollen nicht mehr als 20 Sitzungen für geplante Aktivitäten verfügbar sein, setzen Sie den Prozentsatz auf 25.

```
set maxschedsessions 25
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET MAXSCHEDSESSIONS

Befehl	Beschreibung
QUERY OPTION	Zeigt Informationen über Serveroptionen an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET MINPWLENGTH (Mindestlänge für Kennwort definieren)

Mit diesem Befehl kann die Mindestlänge eines Kennworts definiert werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set--MINPwlength--Länge-----------------------------------><
```

Parameter

Länge (Erforderlich)
: Gibt die Mindestlänge eines Kennworts an. Zulässige Werte sind ganze Zahlen von 0 bis 64. Der Wert 0 bedeutet, daß die Kennwortlänge nicht geprüft wird. Der Standardwert für die Mindestlänge des Kennworts wird auf 0 gesetzt.

Beispiel: Die Mindestkennwortlänge definieren

Die Mindestlänge für Kennwörter auf 5 Zeichen setzen.

```
set minpwlength 5
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET MINPWLENGTH

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET INVALIDPWLIMIT	Definiert die Anzahl ungültiger Anmeldeversuche, die zulässig sind, bevor ein Knoten gesperrt wird.

SET MONITOREDSERVERGROUP (Gruppe überwachter Server definieren)

Verwenden Sie diesen Befehl, um die Gruppe der Server zu definieren, die hinsichtlich Alerts und Status überwacht werden. Sie können diesen Befehl auch verwenden, um die Gruppe der überwachten Server zu ändern oder zu entfernen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set MONITOREDSERVERGroup--+-------------+------------------><
                             '-Gruppenname-'
```

Parameter

Gruppenname
: Gibt den Namen der IBM Spectrum Protect-Servergruppe an, die alle überwachten Server enthält. Sie können den Namen einer überwachten Servergruppe entfernen, indem Sie den Befehl ohne Angabe eines Werts oder unter Angabe eines leeren Werts ("") ausgeben. Jede Überwachung hinsichtlich Alerts und Status von fernen Servern wird beendet.

Den Namen einer überwachten Servergruppe definieren

Den folgenden Befehl ausgeben, um den Namen SUBS einer überwachten Servergruppe zu definieren:

```
set monitoredservergroup subs
```

Den Namen einer überwachten Servergruppe entfernen

Den folgenden Befehl ausgeben, um die überwachte Servergruppe zu entfernen:

```
set monitoredservergroup
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET MONITOREDSERVERGROUP

Befehl	Beschreibung
DEFINE SERVERGROUP (Server-Gruppe definieren)	Definiert eine neue Servergruppe.
DEFINE GRPMEMBER (Server zu einer Servergruppe hinzufügen)	Definiert einen Server als Teil einer Servergruppe.
DELETE GRPMEMBER (Server aus einer Servergruppe löschen)	Löscht einen Server aus einer Servergruppe.
QUERY SERVERGROUP (Servergruppe abfragen)	Zeigt Informationen über Servergruppen an.

Befehl	Beschreibung
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
SET MONITORINGADMIN (Name des Überwachungsadministrators definieren)	Definiert den Namen des Überwachungsadministrators.

SET MONITORINGADMIN (Name des Überwachungsadministrators definieren)

Verwenden Sie diesen Befehl, um den Namen des Überwachungsadministrators zu definieren, der verwendet wird, um die Verbindung zu den Servern in der überwachten Servergruppe herzustellen.

Um den Namen der überwachten Servergruppe anzuzeigen, geben Sie den Befehl QUERY MONITORSETTINGS aus.

Der angegebene Administratorname muss mit dem Namen eines vorhandenen Administrators übereinstimmen, andernfalls schlägt der Befehl fehl.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set MONITORINGADMIN--+------------------+-----------------><
                        '-Administratorname-'
```

Parameter

Administratorname
: Gibt Administratornamen an. Sie können Namen entfernen, indem Sie den Befehl ohne Angabe eines Werts oder unter Angabe eines leeren Werts ("") ausgeben.

Den Namen des Überwachungsadministrators definieren

Den folgenden Befehl ausgeben, um den Namen MONADMIN für den Überwachungsadministrator zu definieren:

```
set monitoringadmin monadmin
```

Den Namen des Überwachungsadministrators entfernen

Den folgenden Befehl ausgeben, um den Überwachungsadministrator zu entfernen:

```
set monitoringadmin ""
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET MONITORINGADMIN

Befehl	Beschreibung
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
SET MONITOREDSERVERGROUP (Gruppe überwachter Server definieren)	Definiert die Gruppe der überwachten Server.

SET NODEATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen Knoten an)

Verwenden Sie diesen Befehl, um den Auswertungsmodus für Gefährdung für einen einzelnen Knoten anzupassen.

Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie die Systemberechtigung, die Maßnahmenberechtigung für die Domäne, der der Knoten zugeordnet ist, oder die Clienteignerberechtigung für den Knoten haben.

Syntax

```
>>---Set NODEATRISKINTERVAL--Knotenname-------------------------->

>--TYPE--=--+-DEFAULT-------------------+----------------------><
            +-BYPASSED------------------+
            '-CUSTOM--Interval--=--Wert-'
```

Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, der aktualisiert werden soll.

TYPE (Erforderlich)
: Gibt den Auswertungstyp für Gefährdung an. Geben Sie einen der folgenden Werte an:

  DEFAULT
  : Gibt an, dass der Knoten mit demselben Intervall ausgewertet wird, das für die Knotenklassifizierung mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde. Der Wert lautet entweder 'System' oder 'Anwendungen' oder 'VM' und wird vom Statusmonitor bestimmt.

    Sie können beispielsweise `TYPE = DEFAULT` angeben, womit es dem Statusmonitor ermöglicht wird, fortzufahren und den Knoten automatisch zu klassifizieren. Das Intervall, das dann verwendet wird, ist das Intervall, das für diese Klassifizierung mit dem Befehl SET STATUSATRISKINTERVAL definiert wurde.

  BYPASSED
  : Gibt an, dass der Gefährdungsstatus für den Knoten nicht vom Statusmonitor ausgewertet wird. Der Gefährdungsstatus wird auch an das Operations Center als 'Bypassed' (Übergangen) zurückgemeldet.

  CUSTOM
  : Gibt an, dass der Knoten mit dem angegebenen Intervall und nicht mit dem Intervall ausgewertet wird, das mit dem Befehl SET STATUSATRISKINTERVAL angegeben wurde.

Interval
: Gibt die Zeit in Stunden zwischen Clientsicherungsaktivitäten an, bevor der Statusmonitor den Client als gefährdet ansieht. Sie können eine ganze Zahl im Bereich von 6 bis 8808 angeben. Bei `TYPE = CUSTOM` müssen Sie diesen Parameter angeben. Bei `TYPE = BYPASSED` oder `TYPE = DEFAULT` wird dieser Parameter nicht angegeben. Der Intervallwert für alle Clienttypen wird bei der Serverinstallation auf 24 gesetzt.

Für einen Knotennamen ein angepasstes Gefährdungsintervall von 90 Tagen definieren

Das Gefährdungsintervall für einen Knoten mit dem Namen *fred* auf 90 Tage setzen.

```
set nodeatriskinterval fred type=custom interval=2160
```

Die Auswertung für das Gefährdungsintervall übergehen

Die Überprüfung des Gefährdungsintervalls für einen Knoten mit dem Namen *bob* übergehen.

```
set nodeatriskinterval bob type=bypassed
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für set nodeatriskinterval

Befehl	Beschreibung
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET VMATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen VM-Dateibereich an)	Definiert den Gefährdungsmodus für einen VM-Dateibereich.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.

Befehl	Beschreibung
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.
QUERY NODE (Knoten abfragen)	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY FILESPACE (Dateibereiche abfragen)	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.

SET PASSEXP (Ablaufdatum für Kennwort definieren)

Mit diesem Befehl kann die Kennwortablaufdauer für Kennwörter von Administratoren und Clientknoten angegeben werden. Sie können entweder eine allgemeine Kennwortablaufdauer für die Kennwörter aller Administratoren und Clientknoten definieren oder die Kennwortablaufdauer jeweils selektiv festlegen.

Einschränkung: Der Befehl SET PASSEXP gilt nicht für Kennwörter, die sich mit einem LDAP-Verzeichnisserver authentifizieren.

Sie können die Einstellung für SET PASSEXP für einen oder mehrere Knoten überschreiben, indem Sie den Befehl REGISTER NODE oder UPDATE NODE mit dem Parameter PASSEXP verwenden.

Der Parameter NODE oder ADMIN muss angegeben werden, um die Kennwortablaufdauer für Clientknoten oder Administratoren zu ändern, für die Kennwortablaufdauer jeweils selektiv festgelegt wurde. Wird der Parameter NODE oder ADMIN nicht angegeben, verwenden *alle* Clientknoten- und Administratorkennwörter die neue Kennwortablaufdauer. Wenn Sie eine Kennwortablaufdauer für einen Clientknoten oder einen Administrator individuell definieren, der noch nicht über eine definierte Kennwortablaufdauer verfügt, wird sie nicht geändert, wenn Sie später eine Kennwortablaufdauer für alle Benutzer festlegen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set PASSExp--Tage--+-------------------------+--------------->
                      |          .-,----------. |
                      |          V            | |
                      '-Node--=----Knotenname-+-'

>--+---------------------------------+-------------------------><
   |           .-,-----------------. |
   |           V                   | |
   '-Admin--=----Administratorname-+-'
```

Parameter

Tage (Erforderlich)
: Gibt die Anzahl der Tage an, die ein Kennwort gültig ist.

  Sie können einen Wert von 1 bis 9999 angeben, wenn Sie den Parameter NODE oder ADMIN nicht angeben. Wird der Parameter NODE oder ADMIN angegeben, kann ein Wert von 0 bis 9999 angegeben werden. Der Wert 0 bedeutet, dass das Kennwort niemals abläuft. Läuft ein Kennwort ab, fordert der Server zur Eingabe eines neuen Kennworts auf, wenn der Administrator oder der Clientknoten eine Verbindung zum Server herstellt.

Node
: Gibt den Namen des Knotens an, für den die Kennwortablaufdauer definiert wird. Soll eine Liste mit Knoten angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

Admin
: Gibt den Namen des Administrators an, dessen Kennwortablaufdauer definiert werden soll. Soll eine Liste mit Administratoren angegeben werden, die Namen ohne Leerzeichen durch Kommas voneinander trennen. Dieser Parameter ist wahlfrei.

Beispiel: Die Kennwortablaufdauer für das Administrator- und Clientknotenkennwort definieren

Die Kennwortablaufdauer für das Administrator- und Clientknotenkennwort soll auf 45 Tage gesetzt werden.

```
set passexp 45
```

Beispiel: Die Kennwortablaufdauer für einen Administrator definieren

Die Kennwortablaufdauer für den Administrator LARRY auf 120 Tage setzen.

```
set passexp 120 admin=larry
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET PASSEXP

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
RESET PASSEXP	Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.
UPDATE ADMIN	Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

SET PRODUCTOFFERING (Produktangebot definieren, das für Ihr Unternehmen lizenziert ist)

Verwenden Sie den Befehl SET PRODUCTOFFERING, um das IBM Spectrum Protect-Produktangebot zu definieren, das für Ihr Unternehmen lizenziert ist.

Die Definition wird verwendet, um zu bestimmen, ob automatische Berechnungen der Speicherkapazitätsmesswerte erforderlich sind und für die Verwendung durch das IBM® License Metric Tool (ILMT) verfügbar gemacht werden. Führen Sie diesen Befehl nur aus, wenn Sie ILMT verwenden, um die Lizenznutzung zu bestimmen.

Für Produktangebote, bei denen automatische Berechnungen der Speicherkapazitätsmesswerte für die Verwendung durch ILMT verfügbar gemacht werden, definiert der Parameter auch die Methode der Kapazitätsmessung, die für diese Berechnungen verwendet wird.

Die Methode der Kapazitätsmessung wird durch die Lizenzbedingungen Ihres speziellen Produktangebots definiert. Um die derzeit berechnete Speicherkapazität für Ihr Produktangebot zu bestimmen, lesen Sie die Informationen in Lizenzeinhaltung prüfen.

Dieselben Speicherkapazitätsinformationen werden ILMT in einem wöchentlichen Intervall zur Verfügung gestellt. Nachdem ein gültiges Produktangebot mithilfe dieses Befehls definiert wurde, stellt IBM Spectrum Protect die aktuelle Kapazitätsberechnung für dieses Angebot ILMT zur Verfügung. Nachdem die anfängliche Kapazitätsberechnung ILMT zur Verfügung gestellt wurde, wird der Wert wöchentlich von IBM Spectrum Protect aktualisiert.

Berechtigungsklasse

Um diesen Befehl auszuführen, müssen Sie über die Systemberechtigung verfügen.

Syntax

```
>>-SET PRODUCTOFFERING--Produktangebot-------------------------><
```

Parameter

Produktangebot (Erforderlich)
Gibt ein Produktangebot an. Die maximale Länge der Zeichenfolge beträgt 255 Zeichen. Folgende Optionen sind verfügbar:

ENTry
Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Entry ist. Dieses Produktangebot verwendet eine Lizenzmetrik pro verwaltetem Server. Kapazitätsmesswerte für dieses Produktangebot sind nicht zutreffend.

DATARet
Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect for Data Retention ist. Kapazitätsmesswerte für dieses Produktangebot werden nicht automatisch berechnet oder für die Verwendung durch ILMT verfügbar gemacht.

BASIC

Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect ist. Dieses Produktangebot verwendet eine PVU-Lizenzmetrik (PVU = Prozessor-Value-Unit). Kapazitätsmesswerte für dieses Produktangebot sind nicht zutreffend.

EE
: Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Extended Edition ist. Dieses Produktangebot verwendet eine PVU-Lizenzmetrik. Kapazitätsmesswerte für dieses Produktangebot sind nicht zutreffend.

SUIte
: Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

SUITEEntry
: Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite Entry ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

SUITEArchive
: Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite - Archive ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

SUITEProtectier
: Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite - ProtecTier ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

SUITEFrontend
: Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite - FrontEnd ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

SUITEENTRYFrontend
: Gibt an, dass das in Ihrem Unternehmen lizenzierte Produktangebot IBM Spectrum Protect Suite Entry - FrontEnd ist. Kapazitätsmesswerte für dieses Produktangebot werden automatisch berechnet und für die Verwendung durch ILMT verfügbar gemacht.

CLEAR
: Es ist kein Produktangebot angegeben.

Beispiel: Für das Produktangebot IBM Spectrum Protect (BASIC) definieren

```
set productoffering BASIC
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET PRODUCTOFFERING

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET QUERYSCHEDPERIOD (Zeitraum für Abfrage von Clientknoten definieren)

Mit diesem Befehl kann gesteuert werden, wie oft Client-Knoten den Server ansprechen, um geplante Arbeit abzurufen, wenn der Planungsmodus Client-Sendeaufruf lautet.

Jeder Client kann beim Starten seines Schedulers seinen eigenen Wiederholungszeitraum definieren. Mit diesem Befehl kann der Wert überschrieben werden, der von allen Clients angegeben wird, die eine Verbindung zum Server herstellen können.

Wenn Client-Knoten Zeitpläne häufiger abfragen, werden Änderungen an den Zeitplänen von den Knoten schneller empfangen. Häufigere Sendeaufrufe durch die Client-Knoten führen jedoch auch zu vermehrtem Datenaustausch auf dem Netz.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Wert für die Periode zwischen Zeitplanabfragen anzuzeigen. Bei der Installation wird IBM Spectrum Protect so konfiguriert, daß jeder Client-Knoten seinen eigenen Wert für diese Einstellung festlegt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set QUERYSCHedperiod--+---------+---------------------------><
```

```
'-Stunden-'
```

Parameter

Stunden
: Gibt die maximale Anzahl Stunden an, die der Scheduler auf einem Client-Knoten zwischen Versuchen wartet, den Server anzusprechen, um einen Zeitplan abzurufen. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 9999.Wird kein Wert für diesen Parameter angegeben, legt jeder Client seinen eigenen Wert für diesen Parameter fest.

Beispiel: Das Überwachungsintervall für alle Clientknoten definieren

Alle Clients, die den Planungsmodus Sendeaufruf verwenden, sollen den Server alle 24 Stunden ansprechen.

```
set queryschedperiod 24
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET QUERYSCHEDPERIOD

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET SCHEDMODES	Gibt den zentralen Planungsmodus für den Server an.

SET RANDOMIZE (Zufallsgenerierung von geplanten Startzeiten definieren)

Mit diesem Befehl können wahlfreie Startzeiten innerhalb des Startfensters jedes Zeitplans für Clients definiert werden, indem der Planungsmodus Client-Sendeaufruf verwendet wird. Ein Startfenster ist die Startzeit und die Dauer, während der ein Zeitplan eingeleitet werden muß. Der Planungsmodus Client-Sendeaufruf ist eine Client/Server-Übertragungstechnik, bei der der Client den Server nach Arbeit abfragt.

Jeder Zeitplan verfügt über ein Fenster, innerhalb dessen er ausgeführt werden kann. Um einen Ausgleich hinsichtlich der Belastung für Netz und Server zu schaffen, können die Startzeiten für Clients über dieses Fenster gestreut werden. Mit Hilfe dieses Befehls kann der Bruchteil des Fensters angegeben werden, über den die Startzeiten für Clients gestreut werden.

Die Zufallsgenerierung tritt am Anfang des Fensters auf, um Zeit für Wiederholungsversuche zu lassen (falls erforderlich). Ist der Planungsmodus nicht auf 'Sendeaufruf' gesetzt, erfolgt keine Zufallsgenerierung, wenn der erste Kontakt des Clients mit dem Server nach der Startzeit für das Ereignis stattfindet.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Prozentsatz für die Zufallsgenerierung anzuzeigen. Bei der Installation lautet der Wert 25 Prozent.

Der Prozentsatz für die Zufallsgenerierung sollte auf einen Wert größer als 0 gesetzt werden, um Übertragungsfehler zu vermeiden. Übertragungsfehler können auftreten, wenn eine große Gruppe von Clients gleichzeitig die Verbindung zum Server herstellen will. Kommt es zu Übertragungsfehlern, kann der Prozentsatz vergrößert werden, so dass die Kontaktaufnahme vom Client zum Server über einen längeren Zeitraum erfolgen kann. Dadurch wird die Wahrscheinlichkeit von Übertragungsüberlastung und -fehlern verringert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set RANDomize--Prozent-------------------------------------><
```

Parameter

Prozent (Erforderlich)
: Gibt den Prozentsatz des Startfensters an, über den die Startzeiten für einzelne Clients verteilt werden. Zulässige Werte sind ganze Zahlen von 0 bis 50.

  Der Wert 0 gibt an, dass keine Zufallsgenerierung stattfindet und alle Clients Zeitpläne am Anfang der Startfenster ausführen.

  Der Wert 50 gibt an, dass den Clients Startzeiten zugeordnet werden, die willkürlich über die erste Hälfte jedes Startfensters verteilt werden.

Bei der Installation lautet dieser Wert 25 Prozent. Der Wert gibt an, dass die ersten 25 Prozent des Fensters für die Zufallsgenerierung verwendet werden.

Wurde DURUNITS=INDEFINITE im Befehl DEFINE SCHEDULE angegeben, wird der Prozentsatz auf eine 24-Stunden-Periode angewendet. Ein Wert von 25 Prozent hätte beispielsweise ein 6-Stunden-Fenster zur Folge.

Beispiel: Die Zufallsgenerierung von geplanten Startzeiten definieren

Der Wert für die Zufallsgenerierung soll auf 50 Prozent gesetzt werden.

```
set randomize 50
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET RANDOMIZE

Befehl	Beschreibung
DEFINE SCHEDULE	Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET SCHEDMODES	Gibt den zentralen Planungsmodus für den Server an.

SET REPLRECOVERDAMAGED (Angeben, ob beschädigte Dateien von einem Replikationsserver wiederhergestellt werden)

Verwenden Sie diesen Befehl, um die systemweite Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver zu aktivieren. Ist diese Einstellung aktiviert, kann der Knotenreplikationsprozess so konfiguriert werden, dass beschädigte Dateien auf dem Quellenreplikationsserver erkannt und durch unbeschädigte Dateien vom Zielreplikationsserver ersetzt werden.

Der Systemparameter REPLRECOVERDAMAGED betrifft alle Dateiwiederherstellungsprozesse bei allen Replikationsprozessen für alle Knoten und Dateibereiche. Die Dateiwiederherstellung ist nur möglich, wenn die Server-Software der Version 7.1.1 oder höher auf dem Quellen- und Zielreplikationsserver installiert ist und die Knotendaten repliziert wurden, bevor die Dateibeschädigung aufgetreten ist.

Soll die aktuelle Einstellung angezeigt werden, verwenden Sie den Befehl QUERY STATUS.

Wenn Sie den Server installieren, lautet die Standardeinstellung ON.

Wenn ein Upgrade für den Server durchgeführt wird und keine beschädigten Dateien erkannt werden, lautet die Standardeinstellung ON.

Wenn ein Upgrade für den Server durchgeführt wird und beschädigte Dateien erkannt werden, wird der Parameter auf OFF gesetzt und eine Nachricht ausgegeben, die angibt, dass die Wiederherstellung beschädigter Dateien inaktiviert ist. Die Einstellung OFF verhindert, dass der Server Datenbanktabellen nach beschädigten Objekten durchsucht, die wiederhergestellt werden können. Das Verhindern der Suche ist erforderlich, wenn viele beschädigte Dateien erkannt werden. In diesem Fall kann eine Suche sehr viel Zeit in Anspruch nehmen und sollte geplant werden, wenn die Verwendung von Serverressourcen auf ein Minimum beschränkt ist. Wenn die Suche gestartet werden kann und beschädigte Dateien wiederhergestellt werden können, müssen Sie den Befehl SET REPLRECOVERDAMAGED ausgeben und die Einstellung ON angeben. Nachdem der Server die Suche erfolgreich beendet hat, wird der Systemparameter REPLRECOVERDAMAGED auf ON gesetzt.

In der folgenden Tabelle wird beschrieben, wie sich der Systemparameter REPLRECOVERDAMAGED und andere Parameter auf die Wiederherstellung beschädigter, replizierter Dateien auswirken.

Tabelle 1. Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken

Einstellung für den Systemparameter REPLRECOVERDAMAGED	Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE	Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE	Ergebnis
OFF	YES, NO oder nicht angegeben	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.
OFF	ONLY	YES oder NO	Eine Fehlernachricht wird angezeigt, weil Dateien nicht wiederhergestellt werden können, wenn der Systemparameter REPLRECOVERDAMAGED auf OFF gesetzt ist.
ON	YES	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.

Einstellung für den Systemparameter REPLRECOVERDAMAGED	Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE	Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE	Ergebnis
ON	NO	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.
ON	ONLY	YES oder NO	Beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt, aber es findet keine Standardknotenreplikation statt.
ON	Nicht angegeben	YES	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.
ON	Nicht angegeben	NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
   .-Set REPLRECOVERDamaged--+---ON------.
>>-+-------------------------------+-----------------------><
   '-Set REPLRECOVERDamaged--+---+-OFf-+-'
                             '-ON--'
```

Parameter

ON
: Gibt an, dass die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.

OFf
: Gibt an, dass die Knotenreplikation nicht aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.

Beispiel: Wiederherstellung beschädigter Dateien aktivieren

Um eine systemweite Einstellung anzugeben, die es dem Server ermöglicht, beschädigte Dateien von einem Zielreplikationsserver wiederherzustellen, geben Sie den folgenden Befehl aus:

```
set replrecoverdamaged on
```

Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für SET REPLRECOVERDAMAGED

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

SET REPLRETENTION (Aufbewahrungszeitraum für Replikationsdatensätze definieren)

Um geeignete Informationen zu Replikationsprozessen aufzubewahren, können Sie mit diesem Befehl den Zeitraum anpassen, für den der Quellenreplikationsserver Replikationsdatensätze in seiner Datenbank aufbewahren soll. Mit dem Befehl SET REPLRETENTION wird der

Aufbewahrungszeitraum für Replikationsdatensätze für Clientknoten in der Datenbank des Quellenreplikationsservers angegeben. Sie können Replikationsdatensätze für Clientknoten verwenden, um aktive und abgeschlossene Prozesse zu überwachen.

Ein Replikationsdatensatz wird erstellt, wenn die Verarbeitung des Befehls REPLICATE NODE gestartet wird. Standardmäßig werden Replikationsdatensätze für Clientknoten von IBM Spectrum Protect 30 Kalendertage aufbewahrt. Ein Kalendertag besteht aus 24 Stunden, von Mitternacht bis Mitternacht. Beispiel: Angenommen, der Aufbewahrungszeitraum beträgt zwei Kalendertage. Wird ein Replikationsprozess um 23:00 Uhr am Tag *n* abgeschlossen, wird ein Datensatz dieses Prozesses für 25 Stunden bis Mitternacht am Tag *n+1* aufbewahrt. Um den Aufbewahrungszeitraum für Replikationsdatensätze anzuzeigen, geben Sie den Befehl QUERY STATUS auf dem Quellenreplikationsserver aus.

Geben Sie den Befehl SET REPLRETENTION auf dem Server aus, der als Quelle für replizierte Daten agiert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
                      .-30----------.
>>-Set REPLRETention--+-------------+-------------------------><
                      '-Anzahl_Tage-'
```

Parameter

Anzahl_Tage (Erforderlich)

Die Anzahl der Tage, die der Quellenreplikationsserver Replikationsdatensätze aufbewahrt. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert ist 30.

Beispiel: Einen Aufbewahrungszeitraum für Replikationsdatensätze für Clientknoten definieren

Replikationsdatensätze für Clientknoten sollen 10 Tage aufbewahrt werden.

```
set replretention 10
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET REPLRETENTION

Befehl	Beschreibung
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY REPLNODE	Zeigt Informationen zum Replikationsstatus eines Clientknotens an.
QUERY REPLRULE	Zeigt Informationen zu Knotenreplikationsregeln an.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET REPLSERVER (Zielreplikationsserver definieren)

Verwenden Sie diesen Befehl, um den Namen eines Zielreplikationsservers zu definieren. Sie können diesen Befehl auch verwenden, um einen Zielreplikationsserver zu ändern oder zu entfernen.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Um den Namen eines Zielreplikationsservers anzuzeigen, geben Sie auf einem Quellenreplikationsserver den Befehl QUERY STATUS aus.

Wichtig:

- Der Servername, der mit diesem Befehl angegeben wird, muss mit dem Namen einer vorhandenen Serverdefinition übereinstimmen. Er muss auch dem Namen des Servers entsprechen, der als Zielreplikationsserver verwendet werden soll. Wenn der mit diesem Befehl angegebene Servername nicht mit dem Servernamen einer vorhandenen Serverdefinition übereinstimmt, schlägt der Befehl fehl.
- Gehen Sie mit Vorsicht vor, wenn Sie einen Zielreplikationsserver ändern oder entfernen. Wenn Sie einen Zielreplikationsserver ändern, werden replizierte Clientknotendaten an einen anderen Zielreplikationsserver gesendet. Wenn Sie einen Zielreplikationsserver entfernen, werden Clientknotendaten nicht repliziert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set REPLSERVer--+----------------+-------------------------><
                   '-Zielservername-'
```

Parameter

Zielservername

Gibt den Namen des Zielreplikationsservers an. Der angegebene Name muss mit dem Namen eines vorhandenen Servers übereinstimmen. Die maximale Länge eines Namens beträgt 64 Zeichen.

Um einen Zielreplikationsserver zu entfernen, geben Sie den Befehl ohne Angabe eines Werts aus.
Anmerkung: Soll das Replizieren von Daten nicht fortgesetzt werden, können Sie die Knotenreplikationskonfiguration entfernen, nachdem Sie den Zielreplikationsserver entfernt haben.

Beispiel: Einen Zielreplikationsserver definieren

Der Name des Servers, der als Zielreplikationsserver definiert werden soll, lautet SERVER1.

```
set replserver server1
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET REPLSERVER

Befehl	Beschreibung
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
QUERY SERVER	Zeigt Informationen über Server an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
UPDATE SERVER	Aktualisiert Informationen über einen Server.
REMOVE REPLNODE	Entfernt einen Knoten aus der Replikation.
REMOVE REPLSERVER	Entfernt einen Server aus der Replikation.

SET RETRYPERIOD (Zeitintervall zwischen Wiederholungsversuchen definieren)

Mit diesem Befehl kann die Anzahl Minuten angegeben werden, die der Scheduler auf einem Client-Knoten nach einem fehlgeschlagenen Versuch, den Server anzusprechen, bzw. nach Fehlschlagen eines geplanten Befehls wartet, bis er den Versuch wiederholt.

Jeder Client kann beim Starten seines Scheduler-Programms ein eigenes Wiederholungsintervall angeben. Mit diesem Befehl können die Werte überschrieben werden, die von allen Clients angegeben werden, die eine Verbindung mit dem Server herstellen können.

Dieser Befehl wird in Verbindung mit dem Befehl SET MAXCMDRETRIES verwendet, um das Wiederholungsintervall und die Anzahl Wiederholungsversuche bei einem fehlgeschlagenen Befehl zu regulieren.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Wert für die Periode zwischen Wiederholungen anzuzeigen. Bei der Installation erlaubt IBM Spectrum Protect jedem Client, seinen eigenen Wiederholungszeitraum zu bestimmen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set RETRYPeriod--+---------+--------------------------------><
                    '-Minuten-'
```

Parameter

Minuten

Gibt die Anzahl Minuten zwischen den Wiederholungsversuchen an, die der Scheduler auf einem Client-Knoten unternimmt, wenn es ihm nicht gelingt, den Server anzusprechen bzw. einen geplanten Befehl auszuführen. Beim Definieren des Wiederholungszeitraums ist eine Zeitspanne anzugeben, die innerhalb eines typischen Startfensters mehrere Wiederholungsversuche zuläßt. Zulässige Werte sind ganze Zahlen von 1 bis 9999.

Beispiel: Einen Zeitraum von fünfzehn Minuten zwischen Wiederholungsversuchen definieren

Der Client-Scheduler soll die Ausführung alle fünfzehn Minuten wiederholen, wenn es ihm nicht gelingt, den Server anzusprechen bzw. geplante Befehle zu verarbeiten.

```
set retryperiod 15
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET RETRYPERIOD

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET MAXCMDRETRIES	Gibt die maximale Anzahl Wiederholungen nach der fehlgeschlagenen Ausführung eines geplanten Befehls an.

SET SCHEDMODES (Modus für zentrale Zeitplanung auswählen)

Mit diesem Befehl kann bestimmt werden, wie die Clients mit dem Server kommunizieren, um geplante Arbeit zu beginnen. Sie müssen jeden Client so konfigurieren, dass er den gewünschten Planungsmodus auswählt.

Verwenden Sie diesen Befehl mit dem Befehl SET RETRYPERIOD, um die Zeit und die Anzahl Wiederholungen für die Verarbeitung eines fehlgeschlagenen Befehls zu steuern.

Der Befehl QUERY STATUS kann ausgegeben werden, um den Wert für den unterstützten Planungsmodus anzuzeigen. Bei der Installation lautet dieser Wert ANY.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set SCHEDMODes--+-ANY------+--------------------------------><
                   +-POlling--+
                   '-PRompted-'
```

Parameter

ANY
: Gibt an, dass Clients entweder im Planungsmodus Clientsendeaufruf (Polling) oder im Planungsmodus Serversystemanfrage (Prompted) ausgeführt werden können.

POlling
: Gibt an, daß nur der Modus Client-Sendeaufruf (Polling) verwendet werden kann. Client-Knoten fragen den Server in festgelegten Zeitintervallen nach geplanter Arbeit ab.

PRompted
: Gibt an, daß nur der Modus Server-Systemanfrage (Prompted) verwendet werden kann. Dieser Modus steht nur für Clients zur Verfügung, die mit Hilfe von TCP/IP kommunizieren. Client-Knoten warten auf die Kontaktaufnahme durch den Server, wenn geplante Arbeit ausgeführt werden muß und eine Sitzung verfügbar ist.

Beispiel: Geplante Operationen auf Clients beschränken, die den Modus Clientsendeaufruf (Polling) verwenden

Clients können sowohl unter der zentralen Zeitplanung "Serversystemanfrage" als auch "Clientsendeaufruf" ausgeführt werden. Die geplanten Operationen sollen vorübergehend auf Clients beschränkt werden, die den Modus Client-Sendeaufruf (Polling) verwenden. Wenn für den Planungsmodus POLLING festgelegt wird, unterbleibt die Aufforderung des Servers an die Clients, geplante Befehle auszuführen. Das heißt, daß alle Client-Scheduler, die den Modus Server-Systemanfrage (Prompted) verwenden, warten, bis für den Planungsmodus ANY oder PROMPTED angegeben wird.

```
set schedmodes polling
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET SCHEDMODES

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET RETRYPERIOD	Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.

SET SCRATCHPADRETENTION (Aufbewahrungszeitraum für Scratchpad definieren)

Mit diesem Befehl können Sie den Zeitraum definieren, den Scratchpadeinträge aufbewahrt werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-SET SCRATCHPADRETENTION--Tage------------------------------><
```

Parameter

Tage (Erforderlich)
Gibt die Anzahl der Tage an, die ein Scratchpadeintrag nach der letzten Aktualisierung des Scratchpadeintrags aufbewahrt wird. Sie können eine ganze Zahl im Bereich von 1 bis 9999 eingeben.

Beispiel: Scratchpadeinträge für die Dauer von 367 Tagen nach ihrer letzten Aktualisierung aufbewahren

```
set scratchpadretention 367
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET SCRATCHPADRETENTION

Befehl	Beschreibung
DEFINE SCRATCHPADENTRY	Erstellt eine Zeile mit Daten im Scratchpad.
DELETE SCRATCHPADENTRY	Löscht eine Zeile mit Daten aus dem Scratchpad.
QUERY SCRATCHPADENTRY	Zeigt Informationen an, die im Scratchpad enthalten sind.
UPDATE SCRATCHPADENTRY	Aktualisiert Daten in einer Zeile im Scratchpad.

SET SERVERHLADDRESS (Serveradresse der höheren Ebene definieren)

Mit diesem Befehl kann die Adresse der höheren Ebene (IP) eines Servers definiert werden. IBM Spectrum Protect verwendet die Adresse, wenn ein Befehl DEFINE SERVER mit CROSSDEFINE=YES ausgegeben wird. Sie müssen den Befehl SET SERVERHLADDRESS für alle automatischen Clientimplementierungen verwenden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set SERVERHladdress--IP-Adresse----------------------------><
```

Parameter

IP-Adresse (Erforderlich)
: Gibt die Adresse der höheren Ebene eines Servers als numerischen Namen in Schreibweise mit Trennzeichen oder als Host-Namen an. Wird ein Host-Name angegeben, muß ein Server verfügbar sein, der den Namen in das Format in Schreibweise mit Trennzeichen auflösen kann.

Beispiel: Die Adresse der höheren Ebene eines Servers definieren

Die Adresse der höheren Ebene von HQ_SERVER auf 9.230.99.66 setzen.

```
set serverhladdress 9.230.99.66
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET SERVERHLADDRESS

Befehl	Beschreibung
SET CROSSDEFINE	Gibt an, ob Server überkreuz definiert werden sollen.
SET SERVERLLADDRESS	Gibt die Adresse der unteren Ebene eines Servers an.
SET SERVERPASSWORD	Gibt das Serverkennwort an.

SET SERVERLLADDRESS (Serveradresse der unteren Ebene definieren)

Mit diesem Befehl kann die Adresse der unteren Ebene eines Servers definiert werden. IBM Spectrum Protect verwendet die Adresse, wenn ein Befehl DEFINE SERVER mit CROSSDEFINE=YES ausgegeben wird.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set SERVERLladdress--TCP-Anschluss--------------------------><
```

Parameter

TCP-Anschluss (Erforderlich)
: Gibt die Adresse der unteren Ebene des Servers an. Im allgemeinen ist diese Adresse mit der Adresse in der Option TCPPORT in der Server-Optionsdatei des Servers identisch.

Beispiel: Die Adresse der unteren Ebene eines Servers definieren

Die Adresse der unteren Ebene von HQ_SERVER auf 1500 setzen.

```
set serverlladdress 1500
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET SERVERLLADDRESS

Befehl	Beschreibung
SET CROSSDEFINE	Gibt an, ob Server überkreuz definiert werden sollen.
SET SERVERHLADDRESS	Gibt die Adresse der höheren Ebene eines Servers an.
SET SERVERPASSWORD	Gibt das Serverkennwort an.

SET SERVERNAME (Servernamen angeben)

Mit diesem Befehl kann der Server-Name geändert werden. Wenn Sie den IBM Spectrum Protect-Server installieren, wird der Name bei der Installation auf SERVER1 gesetzt.

Mit dem Befehl QUERY STATUS kann der Servername angezeigt werden.

Wird von ADSM nach IBM Spectrum Protect migriert, wird der Name auf ADSM oder auf den Namen gesetzt, der zuletzt mit dem Befehl SET SERVERNAME in ADSM angegeben wurde.

Wichtig:

- Ist dies ein Quellenserver für eine Operation mit virtuellem Datenträger, kann das Ändern des Namens Auswirkungen auf die Fähigkeit des Quellenservers haben, auf die Daten zuzugreifen und die Daten zu verwalten, die er auf dem entsprechenden Zielserver gespeichert hat.
- Um Probleme bezüglich des Eigentumsrechts für Datenträger zu vermeiden, ändern Sie nicht den Namen eines Servers, wenn er ein Kassettenarchivclient ist.

Wenn Sie den Namen eines Servers ändern, beachten Sie die folgenden zusätzlichen Einschränkungen:

- Windows-Clients identifizieren anhand des Servernamens, welche Kennwörter zu welchen Servern gehören. Wird der Servername geändert, nachdem die Clients die Verbindung hergestellt haben, müssen die Clients die Kennwörter erneut eingeben.
- Sie müssen eindeutige Namen auf Servern definieren, die miteinander kommunizieren. In einem Netz, in dem Clients die Verbindung zu mehreren Servern herstellen, wird empfohlen, dass alle Server eindeutige Namen haben.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set SERVername--Servername---------------------------------><
```

Parameter

Servername (Erforderlich)
: Gibt den neuen Server-Namen an. Der Name muss im Servernetz für die unternehmensweite Ereignisprotokollierung, die unternehmensweite Konfiguration die Befehlsweiterleitung oder für virtuelle Datenträger eindeutig sein. Die maximale Länge des Namens beträgt 64 Zeichen.

Beispiel: Den Server benennen

Für den Server soll der Name WELLS_DESIGN_DEPT vergeben werden.

```
set servername wells_design_dept
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET SERVERNAME

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET SERVERPASSWORD (Kennwort für Server definieren)

Mit diesem Befehl kann das Kennwort für die Kommunikation zwischen Servern definiert werden, um die Unternehmensverwaltung sowie die Protokollierung und Überwachung von Unternehmensereignissen zu unterstützen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set SERVERPAssword--Kennwort--------------------------------><
```

Parameter

Kennwort (Erforderlich)
: Gibt ein Kennwort für den Server an. Andere Server müssen dasselbe Kennwort in ihren Definitionen dieses Servers haben.

Beispiel: Ein Serverkennwort definieren

Das Kennwort für HQ_SERVER auf agave setzen.

```
set serverpassword agave
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET SERVERPASSWORD

Befehl	Beschreibung
SET CROSSDEFINE	Gibt an, ob Server überkreuz definiert werden sollen.
SET SERVERHLADDRESS	Gibt die Adresse der höheren Ebene eines Servers an.
SET SERVERLLADDRESS	Gibt die Adresse der unteren Ebene eines Servers an.

SET SPREPLRULEDEFAULT (Serverreplikationsregel für speicherverwaltete Daten definieren)

Mit diesem Befehl können Sie die Serverreplikationsregel für speicherverwaltete Daten definieren.

Einschränkung: Die Replikationsregel, die Sie mit diesem Befehl definieren, wird nur angewendet, wenn Dateibereichsregeln und Clientknotenregeln für speicherverwaltete Daten auf DEFAULT gesetzt sind.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Sie können eine Replikationsregel für normale Priorität oder eine Replikationsregel für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Beispiel: Angenommen, Ihre Clientknoten enthalten speicherverwaltete Daten und Sicherungsdaten. Die Replikation der speicherverwalteten Daten hat eine höhere Priorität als die der Sicherungsdaten. Um die speicherverwalteten Daten zu priorisieren, geben Sie den Befehl SET SPREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL_DATA_HIGH_PRIORITY an. Um die Sicherungsdaten zu priorisieren, geben Sie den Befehl SET BKREPLRULEDEFAULT aus und geben Sie die Replikationsregel ALL_DATA für Sicherungsdaten an. Die Regel ALL_DATA für Sicherungsdaten repliziert Sicherungsdaten mit einer normalen Priorität.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set SPREPLRuledefault--+-ALL_DATA----------------+----------><
                          +-ALL_DATA_HIGH_PRIORITY-+
                          '-NONE--------------------'
```

Parameter

ALL_DATA
: Repliziert speicherverwaltete Daten mit einer normalen Priorität.

ALL_DATA_HIGH_PRIORITY
: Repliziert speicherverwaltete Daten mit einer hohen Priorität.

NONE
: Speicherverwaltete Daten werden nicht repliziert.

Beispiel: Die Serverreplikationsregel für speicherverwaltete Daten definieren

Die Standardregel für speicherverwaltete Daten so definieren, dass die Replikation mit einer hohen Priorität erfolgt.

```
set spreplruledefault all_data_high_priority
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET BKREPLRULEDEFAULT

Befehl	Beschreibung
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.

Befehl	Beschreibung
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY REPLRULE	Zeigt Informationen zu Knotenreplikationsregeln an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
SET ARREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für Archivierungsdaten an.
SET BKREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für Sicherungsdaten an.
UPDATE FILESPACE	Ändert Knotenreplikationsregeln für Dateibereiche.
UPDATE REPLRULE	Aktiviert oder inaktiviert Replikationsregeln.
VALIDATE REPLICATION	Überprüft die Replikation für Dateibereiche und Datentypen.

SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)

Verwenden Sie diesen Befehl, um das Sicherungsaktivitätsintervall anzupassen, das verwendet wird, wenn der Statusmonitor bewertet, ob Clients gefährdet sind.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>---Set STATUSATRISKINTERVAL--TYPE--=----+-ALl----------+------>
                                          +-APplications-+
                                          +-VM-----------+
                                          '-SYstems------'

>----Interval--=--Wert-----------------------------------------><
```

Parameter

TYPE (Erforderlich)
: Gibt den Typ des Clients an, der bewertet werden soll. Geben Sie einen der folgenden Werte an:

  ALl
  : Geben Sie diese Einstellung für alle Clienttypen an.

  APplications
  : Geben Sie diese Einstellung für Anwendungsclients an.

  VM
  : Geben Sie diese Einstellung für VM-Clients an.

  SYstems
  : Geben Sie diese Einstellung für Systemclients an.

Interval (Erforderlich)
: Gibt die Zeit in Stunden zwischen Clientaktivitäten an, bevor der Statusmonitor den Client als gefährdet ansieht. Sie können eine ganze Zahl im Bereich von 6 bis 8808 angeben. Der Intervallwert für alle Clienttypen wird bei der Serverinstallation auf 24 gesetzt.

Für Systemclients ein zweiwöchiges Intervall zur Bestimmung der Gefährdung definieren

Die Intervallprüfung zur Bestimmung der Gefährdung für Systemclients auf 2 Wochen setzen.

```
set statusriskinterval type=systems interval=336
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für

Befehl	Beschreibung

Befehl	Beschreibung
DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)	Definiert einen Schwellenwert für die Statusüberwachung.
DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)	Löscht einen Schwellenwert für die Statusüberwachung.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)	Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.
UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)	Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.

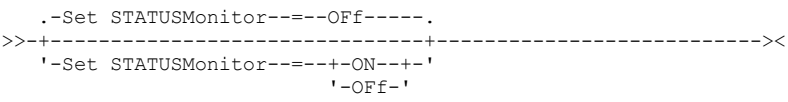
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)

Verwenden Sie diesen Befehl, um die Statusüberwachung zu aktivieren und zu inaktivieren. Wird die Statusüberwachung zum ersten Mal aktiviert, werden auch die Standardschwellenwerte definiert und die Aufbewahrungsdauer für Ereignissätze wird auf mindestens 14 Tage erhöht.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

ON
: Gibt an, dass die Statusüberwachung aktiviert wird. Wenn die Statusüberwachung zum ersten Mal auf ON gesetzt wird, werden alle Standardschwellenwerte definiert, die in den Befehlen DEFINE STATUSTHRESHOLD und UPDATE STATUSTHRESHOLD angegeben sind. Außerdem wird der Wert für den Aufbewahrungszeitraum von Ereignissätzen auf mindestens 14 Tage gesetzt. Wenn Sie die Statusüberwachung aktivieren, werden beispielsweise die Standardwerte für die Auslastung des primären Speicherpools automatisch so definiert, dass eine Warnung angezeigt wird, wenn der Schwellenwert 80 % erreicht, und ein Fehler angezeigt wird, wenn der Schwellenwert eine Auslastung von 90 % erreicht.

OFF
: Gibt an, dass die Statusüberwachung inaktiviert wird. Off ist der Standardwert.

Statusüberwachung aktivieren

Die Statusüberwachung auf 'On' setzen, um die Statusüberwachung zu aktivieren.

```
set statusmonitor on
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET STATUSMONITOR

Befehl	Beschreibung

Befehl	Beschreibung
DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)	Definiert einen Schwellenwert für die Statusüberwachung.
DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)	Löscht einen Schwellenwert für die Statusüberwachung.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)	Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.
UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)	Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.

SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)

Mit diesem Befehl können Sie die Anzahl der Minuten zwischen Serverabfragen für die Statusüberwachung angeben.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set STATUSREFreshinterval--Minuten--------------------------><
```

Parameter

Minuten (Erforderlich)
Gibt die ungefähre Anzahl der Minuten zwischen Serverabfragen für die Statusüberwachung an. Sie können eine ganze Zahl im Bereich von 1 bis 2440 angeben. Der Standardwert ist 5.
Einschränkungen:

- Definieren Sie in einer Speicherumgebung, die vom Operations Center überwacht wird, dasselbe Aktualisierungsintervall auf dem Hub-Server und den Peripherieservern. Werden verschiedene Intervalle verwendet, kann das Operations Center ungenaue Informationen für die Peripherieserver anzeigen.
- Kurze Statusaktualisierungsintervalle verwenden mehr Speicherbereich in der Serverdatenbank und erfordern möglicherweise mehr Prozessor- und Plattenressourcen. Wird beispielsweise das Intervall um die Hälfte verringert, wird der erforderliche Speicherbereich für die Datenbank und das Archivprotokoll verdoppelt. Lange Intervalle verringern die Aktualität von Operations Center-Daten, sind aber für eine Konfiguration mit einem Netz mit langer Latenzzeit besser geeignet.
- Ein Statusaktualisierungsintervall von weniger als 5 Minuten kann die folgenden Probleme verursachen:
  - Operations Center-Daten, von denen angenommen wird, dass sie nach dem definierten Intervall aktualisiert werden, benötigen eine längere Zeit für ihre Aktualisierung.
  - Operations Center-Daten, von denen angenommen wird, dass sie nahezu unverzüglich nach dem Auftreten einer zugehörigen Änderung in der Speicherumgebung aktualisiert werden, benötigen ebenfalls eine längere Zeit für ihre Aktualisierung.

Das Aktualisierungsintervall für die Statusüberwachung definieren

Mit dem folgenden Befehl angeben, dass der Serverstatus alle 6 Minuten abgefragt wird:

```
set statusrefreshinterval 6
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET STATUSREFRESHINTERVAL

Befehl	Beschreibung
DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)	Definiert einen Schwellenwert für die Statusüberwachung.
DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)	Löscht einen Schwellenwert für die Statusüberwachung.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)	Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.
UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)	Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.

SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)

Verwenden Sie diesen Befehl, wenn der Statusmonitor bei der Bewertung des Status für jeden Client Clients als gefährdet ansehen soll.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set STATUSSKIPASFAILURE--+-Yes-+----------------------------->
                            '-No--'

>--TYPE--=--+-ALl----------+----------------------------------><
            +-APplications-+
            +-VM-----------+
            '-SYstems------'
```

Parameter

State (Erforderlich)
: Gibt an, ob die Überprüfung auf Dateien, die während der letzten Sicherung übersprungen wurden, aktiviert werden soll. Diese Überprüfung zeigt an, dass der Client gefährdet ist, wenn Dateien übersprungen wurden. Clientdaten, die übersprungen oder nicht korrekt gesichert werden, werden als gefährdet angesehen.

  Yes
  : Gibt an, dass der Server bewertet, ob ein Client gefährdet ist.

  No
  : Gibt an, dass der Server nicht bewertet, ob ein Client gefährdet ist.

TYPE (Erforderlich)
: Gibt den Typ des Clients an, der bewertet werden soll. Geben Sie einen der folgenden Werte an:

  ALl
  : Geben Sie diese Einstellung für alle Clienttypen an.

APplications
: Geben Sie diese Einstellung für Anwendungsclients an.

VM
: Geben Sie diese Einstellung für VM-Clients an.

SYstems
: Geben Sie diese Einstellung für Systemclients an.

Überprüfung auf Gefährdung für virtuelle Systeme inaktivieren

Die Überprüfung auf Gefährdung für virtuelle Systeme inaktivieren, indem der folgende Befehl ausgegeben wird:

```
set statusskipasfailure off type=vm
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET STATUSSKIPASFAILURE

Befehl	Beschreibung
DEFINE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung definieren)	Definiert einen Schwellenwert für die Statusüberwachung.
DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)	Löscht einen Schwellenwert für die Statusüberwachung.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)	Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)	Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.

SET SUBFILE (Subdateisicherung für Clientknoten definieren)

Mit diesem Befehl kann der Server so definiert werden, dass er Clients das Sichern von Subdateien erlaubt. Auf der Workstation des Clients müssen die Optionen SUBFILECACHEPATH und SUBFILECACHESIZE in der Clientoptionsdatei (dsm.opt) angegeben werden. Wenn Sie einen Windows-Client verwenden, müssen Sie auch die Option SUBFILEBACKUP angeben.

Wurde eine Clientdatei zuvor bereits gesichert, wird mit einer Subdateisicherung normalerweise der Teil (eine Subdatei) der Clientdatei gesichert, der sich geändert hat, und nicht die gesamte Datei.

Mit dem Befehl QUERY STATUS kann bestimmt werden, ob Subdateien auf dem Server gesichert werden können, der diesen Befehl ausführt.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set SUBFILE--+-Client-+-------------------------------------><
                '-No-----'
```

Parameter

Client
: Gibt an, dass der Client-Knoten bestimmen kann, ob eine Subdateisicherung verwendet werden soll.

No

Gibt an, dass die Subdateisicherungen nicht verwendet werden sollen. Bei der Installation wird dieser Wert auf No gesetzt.

Beispiel: Subdateisicherung für Clientknoten definieren

Dem Client-Knoten das Sichern von Subdateien auf dem Server erlauben.

```
set subfile client
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET SUBFILE

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET SUMMARYRETENTION (Anzahl Tage für Aufbewahren in Aktivitätsübersichtstabelle definieren)

Mit diesem Befehl kann die Anzahl der Tage angegeben werden, die Informationen in der SQL-Aktivitätsübersichtstabelle aufbewahrt werden sollen.

Die SQL-Aktivitätsübersichtstabelle enthält Statistiken zu allen Client-Sitzungen und Server-Prozessen. Soll eine Beschreibung der Informationen in der SQL-Aktivitätsübersichtstabelle aufgerufen werden, den folgenden Befehl ausgeben:

```
select colname, remarks from columns where tabname='SUMMARY'
```

Den Befehl QUERY STATUS ausgeben, um die Anzahl der Tage anzuzeigen, die die Informationen aufbewahrt werden. Bei der Installation erlaubt IBM Spectrum Protect jedem Server, seine eigene Anzahl Tage für das Aufbewahren von Informationen in der SQL-Aktivitätsübersichtstabelle zu bestimmen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-Set SUMmaryretention--+------+------------------------------><
                         '-Tage-'
```

Parameter

Tage
: Gibt die Anzahl der Tage an, die Informationen in der Aktivitätsübersichtstabelle aufbewahrt werden sollen. Es kann eine Zahl von 0 bis 9999 angegeben werden. Der Wert 0 gibt an, daß die Informationen in der Aktivitätsübersichtstabelle nicht aufbewahrt werden. Der Wert 1 gibt an, daß die Aktivitätsübersichtstabelle für den aktuellen Tag aufbewahrt wird.

Beispiel: Die Anzahl der Tage angeben, die Informationen in der SQL-Aktivitätsübersichtstabelle aufbewahrt werden sollen

Angeben, daß der Server die Informationen in der Aktivitätsübersichtstabelle 15 Tage aufbewahrt.

```
set summaryretention 15
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET SUMMARYRETENTION

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
SET ACTLOGRETENTION	Gibt die Anzahl Tage an, die Protokollsätze im Aktivitätenprotokoll aufbewahrt werden sollen.
QUERY ACTLOG	Zeigt Nachrichten aus dem Serveraktivitätenprotokoll an.
SELECT	Erlaubt angepasste Abfragen der IBM Spectrum Protect-Datenbank.

SET TAPEALERTMSG (Bandalerts aktivieren oder inaktivieren)

Verwenden Sie diesen Befehl, um es dem IBM Spectrum Protect-Server zu ermöglichen, Hinweise auf Diagnoseinformationen von Kassettenarchiv- und Laufwerkeinheiten zu protokollieren. Bei der Installation wird dieser Wert auf OFF gesetzt. Bei einer Aktivierung kann der Server Diagnoseinformationen aus einer Band- oder Kassettenarchiveinheit abrufen und mit Hilfe von ANR-Nachrichten anzeigen. Bei einer Inaktivierung fragt der Server eine Einheit nicht nach diesen Informationen ab.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-Set TAPEAlertmsg--+-ON--+----------------------------------><
                     '-OFf-'
```

Parameter

ON
: Gibt an, dass Diagnoseinformationen an den Server gemeldet werden.

OFf
: Gibt an, dass Diagnoseinformationen nicht an den Server gemeldet werden.

Beispiel: Das Empfangen von Bandalertnachrichten aktivieren

Dem Server den Empfang von Diagnoseinformationsnachrichten gestatten.

```
set tapealertmsg on
```

Zugehörige Befehle

Tabelle 1. Zugehöriger Befehl für SET TAPEALERTMSG

Befehl	Beschreibung
QUERY TAPEALERTMSG	Zeigt an, ob der Server Hardwarediagnoseinformationen protokolliert.

SET TOCLOADRETENTION (Aufbewahrungszeitraum für Laden für Inhaltsverzeichnis definieren)

Mit diesem Befehl kann die ungefähre Anzahl Minuten angegeben werden, die Inhaltsverzeichnisdaten, auf die nicht verwiesen wird, in der Serverdatenbank geladen bleiben.

Während NDMP-gesteuerter Sicherungsoperationen von NAS-Dateisystemen kann der Server wahlweise Informationen zu Dateien und Verzeichnissen im Image sammeln und diese Informationen in einem Inhaltsverzeichnis innerhalb eines Speicherpools speichern. Mithilfe des Webclients können Dateien und Verzeichnisse in mindestens einem Dateisystemimage untersucht werden. Hierbei werden Einträge aus den Inhaltsverzeichnisdaten angezeigt. Der Server lädt die erforderlichen Inhaltsverzeichnisdaten in eine temporäre Datenbanktabelle.

Nach dem Laden der Daten kann der Benutzer diese Dateien und Verzeichnisse zum Zurückschreiben auswählen. Da diese Datenbanktabelle temporär ist, bleiben die Daten nur über einen bestimmten Zeitraum geladen (gemessen ab dem letzten Verweis auf diese Daten). Bei der Installation wird ein Aufbewahrungszeitraum von 120 Minuten festgelegt. Verwenden Sie den Befehl QUERY STATUS, um den Aufbewahrungszeitraum für das Laden des Inhaltsverzeichnisses anzuzeigen.

Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie über die Systemberechtigung verfügen.

Syntax

```
>>-Set TOCLOADRetention--Minuten-------------------------------><
```

Parameter

Minuten (Erforderlich)
: Gibt die ungefähre Anzahl der Minuten an, die Inhaltsverzeichnisdaten, auf die nicht verwiesen wird, in der Datenbank aufbewahrt werden. Sie können eine ganze Zahl von 30 bis 1000 angeben.

Beispiel: Den Aufbewahrungszeitraum für das Laden des Inhaltsverzeichnisses definieren

Geben Sie mit dem Befehl SET TOCLOADRETENTION an, dass Inhaltsverzeichnisdaten, auf die nicht verwiesen wird, 45 Minuten in der Datenbank aufbewahrt werden sollen.

```
set tocloadretention 45
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SET TOCLOADRETENTION

Befehl	Beschreibung
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.

SET VMATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen VM-Dateibereich an)

Verwenden Sie diesen Befehl, um den Auswertungsmodus für Gefährdung für einen einzelnen VM-Dateibereich anzupassen.

Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie die Systemberechtigung, die Maßnahmenberechtigung für die Domäne, der der Knoten zugeordnet ist, oder die Clienteignerberechtigung für den Knoten haben.

Syntax

```
>>---Set VMATRISKINTERVAL--Knotenname--FSID---------------------->

>--TYPE--=--+-DEFAULT--+--+------------------+----------------><
            +-BYPASSED-+  '-Interval--=--Wert-'
            '-CUSTOM---'
```

Parameter

Knotenname (Erforderlich)
: Gibt den Namen des zu aktualisierenden Clientknotens an, der Eigner des VM-Dateibereichs ist.

FSID (Erforderlich)
: Gibt die Dateibereichs-ID des Clientknotens an, der aktualisiert werden soll.

TYPE (Erforderlich)
: Gibt an, welchen Auswertungsmodus für Gefährdung der Statusmonitor verwenden soll, wenn die Gefährdungsklassifizierung für den VM-Dateibereich des angegebenen Knotens ausgewertet wird. Geben Sie einen der folgenden Werte an:

  DEFAULT
  : Gibt an, dass der VM-Dateibereich mit demselben Intervall ausgewertet wird, das für den Befehl SET STATUSATRISKINTERVAL angegeben wurde.

  BYPASSED
  : Gibt an, dass der Gefährdungsstatus für den VM-Dateibereich nicht vom Statusmonitor ausgewertet wird. Der Gefährdungsstatus wird auch an das Operations Center als 'Bypassed' (Übergangen) zurückgemeldet.

  CUSTOM
  : Gibt an, dass der VM-Dateibereich mit dem angegebenen Intervall und nicht mit dem Intervall ausgewertet wird, das für den Befehl SET STATUSATRISKINTERVAL angegeben wurde.

Interval
: Gibt die Zeit in Stunden zwischen Clientsicherungsaktivitäten an, bevor der Statusmonitor den Client als gefährdet ansieht. Sie können eine ganze Zahl im Bereich von 6 bis 8808 angeben. Bei `TYPE = CUSTOM` müssen Sie diesen Parameter angeben. Bei `TYPE = BYPASSED` oder `TYPE = DEFAULT` wird dieser Parameter nicht angegeben. Der Intervallwert für alle Clienttypen wird bei der Serverinstallation auf 24 gesetzt.

Für einen Knotennamen ein angepasstes Gefährdungsintervall von 90 Tagen definieren

Das Gefährdungsintervall für einen Knoten mit dem Namen *charlievm* (Dateibereichs-ID 50) auf dem Datencenterknoten *alice* auf 90 Tage setzen. Mit dem Befehl QUERY FILESPACE kann die Dateibereichs-ID für die virtuelle Maschine bestimmt werden.

```
set vmatriskinterval alice 50 type=custom interval=2160
```

Die Auswertung für das Gefährdungsintervall übergehen

Die virtuelle Maschine *davevm* (Dateibereichs-ID 213) auf dem Datencenterknoten *erin* von der Überprüfung des Gefährdungsintervalls ausschließen. Mit dem Befehl QUERY FILESPACE kann die Dateibereichs-ID für die virtuelle Maschine *davevm* bestimmt werden. Anschließend die Überprüfung des Gefährdungsintervalls für die virtuelle Maschine auf 'Bypassed' (Übergangen) setzen.

```
set vmatriskinterval erin 213 type=bypassed
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für set vmatriskinterval

Befehl	Beschreibung
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET NODEATRISKINTERVAL (Gibt den Gefährdungsmodus für einen einzelnen Knoten an)	Definiert den Gefährdungsmodus und das Gefährdungsintervall für einen Knoten.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.
QUERY NODE (Knoten abfragen)	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY FILESPACE (Dateibereiche abfragen)	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.

SETOPT (Serveroption für dynamisches Aktualisieren definieren)

Mit dem Befehl SETOPT können Sie die meisten Serveroptionen dynamisch aktualisieren, ohne den Server zu stoppen und erneut zu starten. Für die Option DBDIAGLOGSIZE müssen Sie den Server stoppen und erneut starten. Ein Befehl SETOPT, der in einem Makro oder in einer Prozedur enthalten ist, kann nicht rückgängig gemacht werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-SETOPT--Optionsname--Optionswert---------------------------><
```

Parameter

Optionsname (Erforderlich)
: Gibt eine Zeichenfolge mit Informationen an, die die zu aktualisierende Server-Option identifizieren. Die maximale Länge der Zeichenfolge beträgt 255 Zeichen. Folgende Optionen sind verfügbar:

  - ADMINCOMMTimeout
  - ADMINIDLETIMEOUT
  - ALLOWREORGINDEX
  - ALLOWREORGTABLE

- ARCHLOGCOMPress
- BACKUPINITIATIONROOT
- CHECKTAPEPOS
- CLIENTDEDUPTXNlimit
- COMMTimeout
- Windows-BetriebssystemeDATEFORMAT
- DBDIAGLOGSize
- DBDIAGPATHFSTHreshold
- DEDUPTIER2FILESIZE
- DEDUPTIER3FILESIZE
- DEDUPREQUIRESBACKUP
- DNSLOOKUP
- EXPINterval
- EXPQUiet
- FSUSEDTHreshold
- IDLETimeout
- LDAPCACHEDURATION
- MAXSessions
- MOVEBatchsize
- MOVESizethresh
- NDMPPREFDATAINTERFACE
- Windows-BetriebssystemeNUMBERFORMAT
- NUMOPENVOLSallowed
- RECLAIMDELAY
- RECLAIMPERIOD
- REORGBEGINTime
- REORGDURation
- RESOURCETimeout
- RESTOREINTERVAL
- RETENTIONEXTENSION
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeSANDISCOVERY
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeSANREFRESHTIME
- SERVERDEDUPTXNlimit
- SHREDding
- Windows-BetriebssystemeTCPPORT
- THROUGHPUTDatathreshold
- THROUGHPUTTimethreshold
- Windows-BetriebssystemeTIMEFORMAT
- TXNGroupmax

Optionswert (Erforderlich)
Gibt den Wert für die Server-Option an.

Beispiel: Die maximale Anzahl Clientsitzungen definieren

Die Serveroption für die maximale Anzahl Clientsitzungen mit dem Wert 40 aktualisieren.

```
setopt maxsessions 40
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SETOPT

Befehl	Beschreibung
QUERY OPTION	Zeigt Informationen über Serveroptionen an.
QUERY SYSTEM	Zeigt ausführliche Informationen zum IBM Spectrum Protect-Serversystem an.

SHRED DATA (Daten schreddern)

Verwenden Sie diesen Befehl, um den Prozess zum Schreddern gelöschter sensibler Daten manuell zu starten. Das manuelle Schreddern ist nur möglich, wenn das automatische Schreddern inaktiviert ist.

Der automatische Schredderprozess kann mit der Serveroption SHREDDING gesteuert werden.

Dieser Befehl generiert einen Hintergrundprozess, der mit dem Befehl CANCEL PROCESS abgebrochen werden kann. Um Informationen zu Hintergrundprozessen anzuzeigen, verwenden Sie den Befehl QUERY PROCESS.

Werden Daten aus einem Speicherpool, der das Schreddern erzwingt, gelöscht, während ein manueller Schredderprozess ausgeführt wird, wird die Löschoperation zum aktiven Prozess hinzugefügt.

Berechtigungsklasse

Um diesen Befehl auszugeben, müssen Sie über die Systemberechtigung verfügen.

Syntax

```
                                        .-Wait--=--No------.
>>-SHRED DATA--+----------------------+--+------------------+--->
               '-DUration--=--Minuten-'  '-Wait--=--+-No--+-'
                                                   '-Yes-'

   .-IOERROR--=--SHREDFailure-----.
>--+-----------------------------+----------------------------><
   '-IOERROR--=--+-SHREDFailure-+-'
                 '-SHREDSuccess-'
```

Parameter

DURATION
: Gibt die maximale Anzahl Minuten an, die der Schredderprozess ausgeführt wird, bevor er automatisch abgebrochen wird. Wenn die angegebene Anzahl Minuten verstrichen ist, bricht der Server den Schredderprozess ab. Sobald der Prozess den Abbruch erkennt, wird er beendet. Daher kann der Prozess länger dauern als mit dem Wert für diesen Parameter angegeben ist. Es kann eine Zahl von 1 bis 9999 angegeben werden. Dieser Parameter ist wahlfrei. Falls nicht angegeben, stoppt der Server erst dann, nachdem alle gelöschten sensiblen Daten geschreddert wurden.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

  No
  : Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Bei dem Hintergrundprozess erstellte Nachrichten werden im Aktivitätenprotokoll und/oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden. Ein Hintergrundprozess kann mit dem Befehl CANCEL PROCESS abgebrochen werden. Wird dieser Prozess abgebrochen, wurden möglicherweise einige Dateien bereits vor dem Abbruch geschreddert. Dies ist der Standardwert.

  Yes
  : Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Die Operation muss erst beendet sein, bevor andere Tasks ausgeführt werden können. Der Server zeigt die Ausgabenachrichten dem Verwaltungsclient an, wenn die Operation beendet ist. Nachrichten werden auch im Aktivitätenprotokoll und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.
  AIX-BetriebssystemeLinux-BetriebssystemeAnmerkung: Von der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

IOERROR
: Gibt an, ob beim Auftreten eines E/A-Fehlers während des Schredderns der Daten das Schreddern als erfolgreich betrachtet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist SHREDFAILURE. Gültige Werte:

  SHREDFailure
  : Gibt an, dass die Daten als nicht erfolgreich geschreddert angesehen werden, wenn der Server einen E/A-Fehler während des Schredderns entdeckt, und die Datei, die die Daten enthält, wird als beschädigt markiert. Der Server versucht die Daten bei der nächsten Ausführung des Schredderprozesses erneut zu schreddern. Damit haben Sie die Möglichkeit, den Fehler zu korrigieren und sicherzustellen, dass die Daten ordnungsgemäß geschreddert werden können.

  SHREDSuccess
  : Gibt an, dass die Daten als erfolgreich geschreddert angesehen werden, wenn der Server während des Schredderns einen E/A-Fehler entdeckt und die Datei, die die Daten enthält, zuvor als beschädigt markiert wurde. Sie sollten diese Option nur verwenden, wenn der Server während des Schredderns E/A-Fehler zurückgemeldet hat und Sie den Fehler nicht korrigieren können.

Beispiel: Daten schreddern

Das Schreddern aller gelöschten sensiblen Daten manuell starten. Den Prozess bis zu sechs Stunden ausführen, bevor er automatisch abgebrochen wird.

```
shred data duration=360
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SHRED DATA

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY SHREDSTATUS	Zeigt Informationen zu Daten an, die auf das Schreddern warten.

SUSPEND EXPORT (Momentan aktive Exportoperation aussetzen)

Mit diesem Befehl können Sie eine momentan aktive Exportoperation zwischen Servern aussetzen, die einen anderen FILEDATA-Wert als NONE hat. Die Exportoperation, die ausgesetzt werden soll, muss nach der Initialisierungsphase liegen, um für die Aussetzung ausgewählt werden zu können. Der Status der Exportoperation wird gespeichert. Die Operation kann mit dem Befehl RESTART EXPORT erneut gestartet werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung erforderlich.

Syntax

```
                    .-*-------------.
>>-SUSPend EXPOrt -+---------------+---------------------------><
                   '---Export-ID---'
```

Parameter

EXPORTIDentifier
: Dieser optionale Parameter gibt den Namen der Exportoperation an. Der Name kann mit dem Befehl QUERY EXPORT ermittelt werden, der alle momentan aktiven Exportoperationen zwischen Servern, die ausgesetzt werden können, auflistet. Es kann auch das Platzhalterzeichen verwendet werden, um den Namen anzugeben.

Beispiel: Eine bestimmte Exportoperation aussetzen

Die aktive Exportoperation EXPORTALLACCTNODES aussetzen. Es wird keine Ausgabe generiert, wenn Sie den Befehl SUSPEND EXPORT ausgeben. Sie müssen den Befehl QUERY EXPORT ausgeben, um zu überprüfen, ob die Operation EXPORTALLACCTNODES ausgesetzt ist.

```
suspend export exportallacctnodes
```

Beispiel: Alle aktiven Exportoperationen aussetzen

Alle Exportoperationen mit dem Status AKTIV aussetzen.

```
suspend export *
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SUSPEND EXPORT

Befehl	Beschreibung
CANCEL EXPORT	Löscht eine ausgesetzte Exportoperation.
EXPORT NODE	Kopiert Clientknoteninformationen auf externe Datenträger oder direkt auf einen anderen Server.
EXPORT SERVER	Kopiert den gesamten Server oder einen Teil des Servers auf externe Datenträger oder direkt auf einen anderen Server.
QUERY EXPORT	Zeigt die Exportoperationen an, die gerade aktiv oder ausgesetzt sind.
RESTART EXPORT	Startet eine ausgesetzte Exportoperation erneut.

UNLOCK-Befehle

Verwenden Sie die UNLOCK-Befehle, um den Zugriff erneut einzurichten, nachdem ein Objekt gesperrt wurde.

- UNLOCK ADMIN (Sperre für einen Administrator aufheben)
- UNLOCK NODE (Clientknoten freigeben)
- UNLOCK PROFILE (Profil freigeben)

UNLOCK ADMIN (Sperre für einen Administrator aufheben)

Verwenden Sie den Befehl UNLOCK ADMIN, um es einem gesperrten Administrator zu ermöglichen, wieder auf den Server zuzugreifen. Sie können auch mehrere Administratoren entsperren, die sich mit derselben Methode authentifizieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-UNLOCK Admin--+-*-----------------+--+-----------------------------+-><
                 '-Administratorname-'   '-AUTHentication--=--+-LOcal-+-'
                                                              '-LDap--'
```

Parameter

Administratorname (Erforderlich)
: Gibt den Namen des Administrators an, der entsperrt werden soll. Sie können Platzhalterzeichen verwenden, um den Administratornamen anzugeben. Sie müssen keinen Administratornamen eingeben, wenn alle Administratoren gemäß ihrer Authentifizierungsmethode entsperrt werden sollen. Verwenden Sie das Platzhalterzeichen mit einer Authentifizierungsmethode, um mehrere Administratoren zu entsperren. Der Parameter ist erforderlich (kein Standardplatzhalterzeichen).

AUTHentication
: Gibt die Methode der Kennwortauthentifizierung an, die für einen Administrator zur Anmeldung erforderlich ist.

  LOcal
  : Gibt an, dass Sie Administrator-IDs entsperren möchten, die Kennwörter mit dem IBM Spectrum Protect-Server authentifizieren.

  LDap
  : Gibt an, dass Sie Administrator-IDs entsperren möchten, die Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren.

Beispiel: Eine Administrator-ID entsperren

Der Administrator-ID JOE wird momentan der Zugriff auf IBM Spectrum Protect verweigert. JOE erlauben, auf den Server zuzugreifen. Geben Sie den folgenden Befehl aus:

```
unlock admin joe
```

Beispiel: Alle Administrator-IDs entsperren, die Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren

Die Administrator-IDs, die Kennwörter verwenden, die mit einem LDAP-Verzeichnisserver authentifiziert werden, müssen entsperrt werden, damit die IDs mit dem IBM Spectrum Protect-Server kommunizieren können.

```
unlock admin * authentication=ldap
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UNLOCK ADMIN

Befehl	Beschreibung
LOCK ADMIN	Verweigert einem Administrator den Zugriff auf IBM Spectrum Protect.
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.

UNLOCK NODE (Clientknoten freigeben)

Mit diesem Befehl kann einem gesperrten Clientknoten wieder der Zugriff auf den Server ermöglicht werden. Sie können auch mehrere Knoten entsperren, die dieselbe Methode der Authentifizierung verwenden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

Syntax

```
>>-UNLOCK Node--+-*----------+--+------------------------------+-><
               '-Knotenname-'  '-AUTHentication--=--+-LOcal-+-'
                                                   '-LDap--'
```

Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, der entsperrt werden soll. Es können Platzhalterzeichen verwendet werden, um den Knotennamen anzugeben. Sie müssen keinen Knotennamen eingeben, wenn alle Knoten gemäß ihrer Authentifizierungsmethode entsperrt werden sollen. Verwenden Sie das Platzhalterzeichen mit einer Authentifizierungsmethode, um Gruppen von Knoten zu entsperren. Der Parameter ist erforderlich. Es ist kein Standardplatzhalterzeichen verfügbar.

AUTHentication
: Gibt die Kennwortauthentifizierungsmethode für den Knoten an. Dieser Parameter ist wahlfrei.

  LOcal
  : Gibt an, dass Sie Knoten entsperren möchten, die Kennwörter mit dem IBM Spectrum Protect-Server authentifizieren.

  LDap
  : Gibt an, dass Sie Knoten entsperren möchten, die Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren.

Beispiel: Einen Knoten entsperren

Dem Clientknoten SMITH wird momentan der Zugriff auf IBM Spectrum Protect verweigert. SMITH erlauben, auf den Server zuzugreifen.

```
unlock node smith
```

Beispiel: Alle Knoten entsperren, die sich mit dem IBM Spectrum Protect-Server authentifizieren

Die Knoten, die keine Kennwörter mit LDAP-Verzeichnisservern authentifizieren, müssen entsperrt werden.

```
unlock node * authentication=local
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UNLOCK NODE

Befehl	Beschreibung
LOCK NODE	Verhindert, dass ein Client auf den Server zugreift.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.

UNLOCK PROFILE (Profil freigeben)

Mit diesem Befehl kann auf einem Konfigurationsmanager ein Konfigurationsprofil freigegeben werden, damit es an subskribierende verwaltete Server verteilt werden kann.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-UNLOCK PROFILe--Profilname-----------------------------------><
```

Parameter

Profilname (Erforderlich)
: Gibt das Profil an, das freigegeben werden soll. Es können Platzhalterzeichen verwendet werden, um mehrere Namen anzugeben.

Beispiel: Ein Profil entsperren

Das Profil TOM entsperren.

```
unlock profile tom
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UNLOCK PROFILE

Befehl	Beschreibung
COPY PROFILE	Erstellt eine Kopie eines Profils.
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DELETE PROFASSOCIATION	Löscht die Zuordnung zwischen einem Objekt und einem Profil.
DELETE PROFILE	Löscht ein Profil aus einem Konfigurationsmanager.
LOCK PROFILE	Verhindert die Verteilung eines Konfigurationsprofils.
QUERY PROFILE	Zeigt Informationen über Konfigurationsprofile an.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UPDATE PROFILE	Ändert die Beschreibung eines Profils.

UPDATE-Befehle

Mit den UPDATE-Befehlen können ein oder mehrere Attribute eines vorhandenen IBM Spectrum Protect-Objekts geändert werden.

- UPDATE ADMIN (Administrator aktualisieren)
- UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)
- UPDATE ALERTSTATUS (Status eines Alert aktualisieren)
- UPDATE BACKUPSET (Aufbewahrungszeitraum einer Sicherungsgruppe aktualisieren)
- UPDATE CLIENTOPT (Folgenummer einer Clientoption aktualisieren)
- UPDATE CLOPTSET (Beschreibung einer Clientoptionsgruppe aktualisieren)
- UPDATE COLLOCGROUP (Kollokationsgruppe aktualisieren)
- UPDATE COPYGROUP (Kopiengruppe aktualisieren)
- UPDATE DATAMOVER (Einheit zum Versetzen von Daten aktualisieren)
- UPDATE DEVCLASS (Attribute einer Einheitenklasse aktualisieren)
- UPDATE DOMAIN (Maßnahmendomäne aktualisieren)
- UPDATE DRIVE (Laufwerk aktualisieren)
- UPDATE FILESPACE (Knotenreplikationsregeln für Dateibereich aktualisieren)
- UPDATE LIBRARY (Kassettenarchiv aktualisieren)
- UPDATE LIBVOLUME (Status eines Speicherdatenträgers ändern)
- UPDATE MACHINE (Maschineninformationen aktualisieren)
- UPDATE MGMTCLASS (Verwaltungsklasse aktualisieren)
- UPDATE NODE (Attribute eines Knotens aktualisieren)
- UPDATE NODEGROUP (Knotengruppe aktualisieren)
- UPDATE PATH (Pfad ändern)
- UPDATE POLICYSET (Beschreibung einer Maßnahmengruppe aktualisieren)
- UPDATE PROFILE (Profilbeschreibung aktualisieren)
- UPDATE RECOVERYMEDIA (Wiederherstellungsdatenträger aktualisieren)
- UPDATE REPLRULE (Replikationsregeln aktualisieren)
- UPDATE SCHEDULE (Zeitplan aktualisieren)
- UPDATE SCRIPT (IBM Spectrum Protect-Prozedur aktualisieren)
- UPDATE SERVER (Server aktualisieren, der für die Übertragung zwischen Servern definiert ist)
- UPDATE SERVERGROUP (Beschreibung einer Servergruppe aktualisieren)
- UPDATE SPACETRIGGER (Speicherbereichsauslöser aktualisieren)
- UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)
- UPDATE STGPOOL (Speicherpool aktualisieren)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeUPDATE STGPOOLDIRECTORY (Speicherpoolverzeichnis aktualisieren)
- UPDATE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs aktualisieren)
- UPDATE VOLHISTORY (History-Daten für sequentielle Datenträger aktualisieren)
- UPDATE VOLUME (Speicherpooldatenträger ändern)

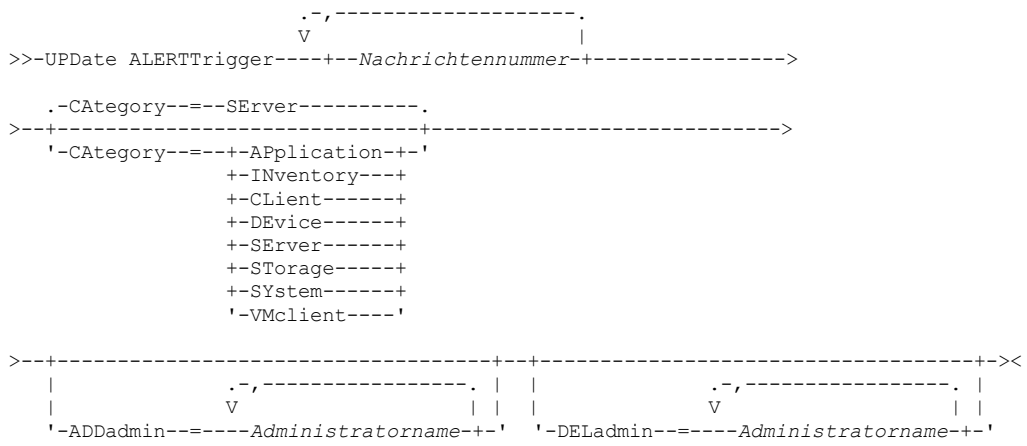
UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)

Verwenden Sie diesen Befehl, um die Attribute eines oder mehrerer Alertauslöser zu aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Nachrichtennummer (Erforderlich)
: Gibt die Nachrichtennummer an, die dem Alertauslöser zugeordnet werden soll. Geben Sie mehrere Nachrichtennummern durch Kommas getrennt und ohne Leerzeichen an. Nachrichtennummern haben eine maximale Länge von acht Zeichen.

CATegory
: Gibt den Kategorietyp für den Alert an, der durch die Nachrichtentypen bestimmt wird. Der Standardwert ist SERVER.
Anmerkung: Wenn Sie die Kategorie eines Alertauslösers ändern, wird die Kategorie von vorhandenen Alerts auf dem Server nicht geändert. Neue Alerts werden mit der neuen Kategorie kategorisiert.
Geben Sie einen der folgenden Werte an:

  APplication
  : Der Alert wird als Anwendungskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Anwendungsclients (TDP) zugeordnet sind.

  INventory
  : Der Alert wird als Bestandskategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die der Datenbank, der aktiven Protokolldatei oder der Archivprotokolldatei zugeordnet sind.

  CLient
  : Der Alert wird als Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Clientaktivitäten zugeordnet sind.

  DEvice
  : Der Alert wird als Einheitenkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Einheitenklassen, Kassettenarchiven, Laufwerken oder Pfaden zugeordnet sind.

  SErver
  : Der Alert wird als allgemeine Serverkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die allgemeinen Serveraktivitäten oder -ereignissen zugeordnet sind.

  STorage
  : Der Alert wird als Speicherkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Speicherpools zugeordnet sind.

  SYstems
  : Der Alert wird als Systemclientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die Systemsicherungs- und -archivierungsclients oder HSM-Clients zugeordnet sind.

  VMclient
  : Der Alert wird als VM-Clientkategorie klassifiziert. Beispielsweise können Sie diese Kategorie für Nachrichten angeben, die VM-Clients zugeordnet sind.

ADmin
: Dieser optionale Parameter gibt den Namen des Administrators an, der eine E-Mail-Benachrichtigung über diesen Alert empfängt. Der Alertauslöser wird erfolgreich definiert, auch wenn keine Administratornamen angegeben werden.

ADDadmin
: Gibt den Namen des Administrators an, der der Liste der Administratoren hinzugefügt werden soll, die E-Mail-Alerts empfangen. Geben Sie mehrere Administratornamen durch Kommas getrennt und ohne Leerzeichen an.

DELadmin
: Gibt den Namen des Administrators an, der aus der Liste der Administratoren gelöscht werden soll, die E-Mail-Alerts empfangen. Geben Sie mehrere Administratornamen durch Kommas getrennt und ohne Leerzeichen an.

Alertauslöser aktualisieren

Mit dem folgenden Befehl die Namen der Administratoren hinzufügen, die beim Auftreten der Alerts ANR1073E und ANR1074E benachrichtigt werden möchten, und den Namen eines Administrators löschen, der nicht mehr benachrichtigt werden möchte:

```
update alerttrigger ANR1073E,ANR1074E ADDadmin=djee,cdawson,mhaye deladmin=harryh
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE ALERTTRIGGER

Befehl	Beschreibung
DEFINE ALERTTRIGGER (Alertauslöser definieren)	Ordnet angegebene Nachrichten einem Alertauslöser zu.
DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)	Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.
QUERY ALERTSTATUS (Status eines Alert abfragen)	Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.
QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)	Zeigt Nachrichtennummern an, die einen Alert auslösen.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
UPDATE ALERTSTATUS (Status eines Alert aktualisieren)	Aktualisiert den Status eines zurückgemeldeten Alert.

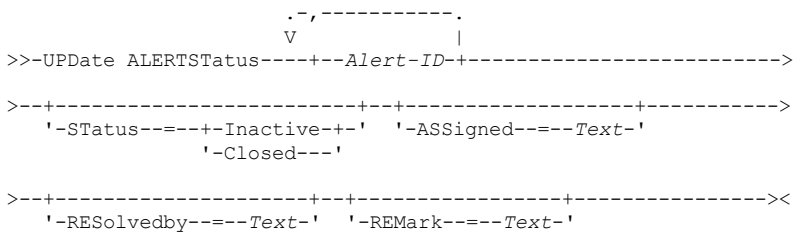
UPDATE ALERTSTATUS (Status eines Alert aktualisieren)

Mit diesem Befehl kann der Status eines zurückgemeldeten Alert aktualisiert werden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax



Parameter

Alert-ID (Erforderlich)
: Gibt den Alert an, der aktualisiert werden soll. Es können mehrere Nachrichtennummern angegeben werden, die ohne Leerzeichen durch Kommas voneinander getrennt werden.

STatus
: Gibt den Statustyp an, der aktualisiert werden soll. Alerts können von 'aktiv' in 'inaktiv' oder 'geschlossen' oder von 'inaktiv' in 'geschlossen' geändert werden. Gültige Werte:

  Inactive
  : Aktive Alerts können in den Status 'inaktiv' geändert werden.

  Closed
  : Aktive und inaktive Alerts können in den Status 'geschlossen' geändert werden.

ASSigned
: Gibt den Namen des Administrators an, dem der Alert zugeordnet ist, der abgefragt werden soll.

RESolvedby
: Gibt den Namen des Administrators an, der den Alert behoben hat, der abgefragt werden soll.

REMark
: Dieser Parameter gibt Begleittext an. Der Begleittext darf 255 Zeichen nicht überschreiten. Enthält die Beschreibung Leerzeichen, schließen Sie den gesamten Text in Anführungszeichen ("") ein. Entfernen Sie zuvor definierten Text, indem Sie eine leere Zeichenfolge ("") für diesen Wert angeben.

Den Begleittext in einem Alert aktualisieren

Den folgenden Befehl ausgeben, um den Begleittext für die Alert-ID-Nummer 25 zu aktualisieren und anzugeben, dass *DJADMIN* den Alert bearbeitet:

```
update alertstatus 25 assigned=DJADMIN
```

Alertstatus aktualisieren

Den folgenden Befehl ausgeben, um die Alert-ID-Nummer 72 in den Status 'geschlossen' zu ändern und einen Kommentar hinzuzufügen, wie der Alert behoben wurde:

```
update alertstatus 72 status=closed remark="Dateisystem für die aktive Protokolldatei
wurde vergrößert"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE ALERTSTATUS

Befehl	Beschreibung
DEFINE ALERTTRIGGER (Alertauslöser definieren)	Ordnet angegebene Nachrichten einem Alertauslöser zu.
DELETE ALERTTRIGGER (Nachricht aus einem Alertauslöser entfernen)	Entfernt eine Nachrichtennummer, die einen Alert auslösen kann.
QUERY ALERTSTATUS (Status eines Alert abfragen)	Zeigt Informationen zu Alerts an, die auf dem Server ausgegeben wurden.
QUERY ALERTTRIGGER (Liste der definierten Alertauslöser abfragen)	Zeigt Nachrichtennummern an, die einen Alert auslösen.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
UPDATE ALERTTRIGGER (Definierten Alertauslöser aktualisieren)	Aktualisiert die Attribute eines oder mehrerer Alertauslöser.

UPDATE ADMIN (Administrator aktualisieren)

Dieser Befehl ermöglicht es, das Kennwort oder Kontaktinformationen für einen Administrator zu ändern. Der Administratorname SERVER_CONSOLE kann jedoch nicht aktualisiert werden.

AIX-BetriebssystemeLinux-BetriebssystemeKennwörter für Administratoren müssen nach gewisser Zeit geändert werden, die durch den Befehl SET PASSEXP festgelegt wird. Der Befehl SET PASSEXP hat keine Auswirkungen auf Kennwörter, die sich mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifizieren.

Einschränkung: Die Authentifizierungsmethode für Ihre eigene Benutzer-ID kann nicht aktualisiert werden. Falls erforderlich, muss ein anderer Administrator diese Änderung vornehmen. Außerdem können Sie bei der Aktualisierung eines Kennworts mit dem Befehl UPDATE ADMIN kein Platzhalterzeichen beim Parameter `Administratorname` verwenden.

Administratoren mit dem Namen eines Knotens können während der Ausführung eines Befehls REGISTER NODE erstellt werden. Damit der Knoten und der Administrator mit demselben Namen synchronisiert bleiben, werden die Authentifizierungsmethode und die Einstellung für SSLREQUIRED für den Knoten aktualisiert, damit sie mit dem Administrator übereinstimmen. Wird die Authentifizierungsmethode des Administrators von LOCAL in LDAP geändert und wird kein Kennwort bereitgestellt, wird der Knoten in den Status "LDAP (künftig)" versetzt. Ein Kennwort wird dann bei der nächsten Anmeldung angefordert. Kennwörter zwischen Knoten und Administratoren mit denselben Namen bleiben bei jeder Authentifizierungsänderung synchron.

Sie müssen den Befehl RENAME ADMIN verwenden, um den Namen eines registrierten Administrators zu ändern.

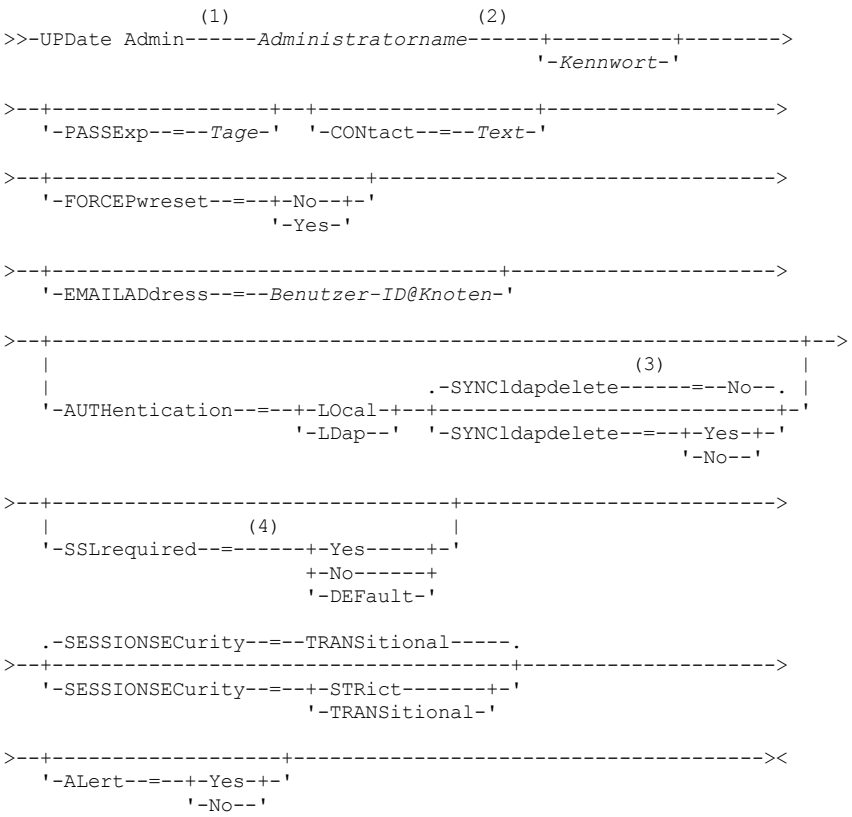
Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
- Falls eine Benutzer-ID mit Administratorberechtigung mit einem Knotennamen übereinstimmt, dürfen Sie die Authentifizierungsmethode nicht in LDAP aktualisieren. Andernfalls stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, weil automatische Kennwortänderungen dasselbe Kennwort zweimal aktualisieren. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierungsoperation fehlschlägt.

Berechtigungsklasse

Zum Ändern des Kennworts oder der Kontaktinformationen eines anderen Administrators ist für diesen Befehl die Systemberechtigung erforderlich. Jeder Administrator kann diesen Befehl ausgeben, um sein Kennwort bzw. seine Kontaktinformationen zu aktualisieren.

Syntax



Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.
2. Kennwörter sind bei diesem Befehl optional, wenn Sie nicht die Authentifizierungsmethode von LDAP in LOCAL ändern möchten.
3. Der Parameter SYNCldapdelete gilt nur, wenn ein Administrator, der sich mit einem LDAP-Verzeichnisserver authentifiziert, zur lokalen Authentifizierung zurückkehrt.
4. Der Parameter SSLREQUIRED ist veraltet.

Parameter

Administratorname (Erforderlich)
Gibt den Namen des Administrators an, der aktualisiert werden soll.

Kennwort
Gibt das Kennwort des Administrators an. Dieser Parameter ist in den meisten Fällen optional. Wenn die Authentifizierungsmethode des Administrators von LDAP in LOCAL geändert wird, ist ein Kennwort erforderlich. Wenn ein LDAP-Server für die Authentifizierung von Administratoren verwendet wird, geben Sie bei Verwendung des Befehls UPDATE ADMIN kein Kennwort an.

PASSExp
Gibt die Anzahl der Tage an, die das Kennwort gültig ist. Für die Kennwortablaufdauer kann ein Wert im Bereich von 0 bis 9999 definiert werden. Der Wert 0 bedeutet, dass das Kennwort niemals abläuft. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird die Kennwortablaufdauer nicht geändert. Dieser Parameter gilt nicht für Kennwörter, die auf einem LDAP-Verzeichnisserver gespeichert werden.

CONtact
Gibt eine Zeichenfolge an, die den Administrator kennzeichnet. Dieser Parameter ist wahlfrei. Die Zeichenfolge in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Sollen zuvor definierte Kontaktinformationen entfernt werden, geben Sie eine Nullzeichenfolge ("") an.

FORCEPwreset
Gibt an, ob der Administrator das Kennwort ändern oder zurücksetzen muss. Dieser Parameter ist wahlfrei. Gültige Werte:

No
Gibt an, dass der Administrator bei dem Versuch, sich beim Server anzumelden, das Kennwort nicht ändern bzw. zurücksetzen muss. Die Kennwortablaufdauer wird mit dem Befehl SET PASSEXP definiert.

Yes
Gibt an, dass das Kennwort des Administrators bei der nächsten Anmeldung abläuft. Der Administrator muss das Kennwort dann ändern oder zurücksetzen. Wenn kein Kennwort angegeben wird, wird ein Syntaxfehler empfangen.
Einschränkungen:

- Für Benutzer-IDs mit Administratorberechtigung, die mit einem LDAP-Server authentifiziert werden, wird der Kennwortablauf mithilfe von LDAP-Serverdienstprogrammen definiert. Geben Sie daher nicht FORCEPWRESET=YES an, wenn

AUTHENTICATION=LDAP angegeben werden soll.
- Soll eine Benutzer-ID mit Administratorberechtigung für die Authentifizierung mit einem LDAP-Server aktualisiert werden, und haben Sie FORCEPWRESET=YES angegeben, müssen Sie das Kennwort ändern, bevor Sie FORCEPWRESET=NO und AUTHENTICATION=LDAP angeben können.

EMAILADdress
Dieser Parameter wird für zusätzliche Kontaktinformationen verwendet. Die mit diesem Parameter angegebenen Informationen werden von IBM Spectrum Protect nicht verwendet.

AUTHentication
Dieser Parameter bestimmt die Kennwortauthentifizierungsmethode, die von der Administrator-ID verwendet wird (LDAP oder LOCAL).

LOcal
Gibt an, dass der Administrator die lokale IBM Spectrum Protect-Serverdatenbank verwendet, um Kennwörter für die Authentifizierung zu speichern.

LDap
Gibt an, dass der Administrator einen LDAP-Verzeichnisserver für die Kennwortauthentifizierung verwendet.

SYNCldapdelete
Dieser Parameter gilt nur, wenn ein Administrator, der sich mit einem LDAP-Server authentifiziert, zur lokalen Authentifizierung zurückkehren möchte.

Yes
Gibt an, dass der Administrator vom LDAP-Server gelöscht wird.
Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwalten beschrieben wird.)

No
Gibt an, dass der Administrator nicht vom LDAP-Server gelöscht wird. Dies ist der Standardwert.

SSLrequired (veraltet)

Gibt an, ob die Administrator-ID das Protokoll Secure Sockets Layer (SSL) für die Kommunikation zwischen dem IBM Spectrum Protect-Server und dem Client für Sichern/Archivieren verwenden muss. Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, müssen Sie die Sitzungen mit SSL oder einer anderen Netzsicherheitsmethode schützen.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter SSLREQUIRED wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

SESSIONSECurity
Gibt an, ob der Administrator die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

STRict
Gibt an, dass die striktesten Sicherheitseinstellungen für den Administrator durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem Server und dem Administrator verwendet. Um anzugeben, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, lesen Sie die Informationen zur Clientoption SSL.
Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der Administrator mit dem Server authentifizieren kann:

- Der Administrator und der Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Administrator muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen dem Server und dem Administrator konfiguriert werden.

Administratoren, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem Server authentifizieren.

TRANSitional
Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Administrator durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Administrator nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Administrator weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Administrator jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Administrator kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Administrator erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Administrator nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Administrator, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Administrator nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. Befehlsweiterleitung oder Export zwischen

Servern, wenn sich der Administrator beim IBM Spectrum Protect-Server als Administrator von einem anderen Server authentifiziert.

ALert
Gibt an, ob Alerts an die E-Mail-Adresse eines Administrators gesendet werden.

Yes
Gibt an, dass Alerts an die E-Mail-Adresse des angegebenen Administrators gesendet werden.

No
Gibt an, dass Alerts nicht an die E-Mail-Adresse des angegebenen Administrators gesendet werden. Dies ist der Standardwert.

Tipp: Die Alertüberwachung muss aktiviert sein und die E-Mail-Einstellungen müssen korrekt definiert sein, damit Alerts erfolgreich als E-Mail empfangen werden können. Um die aktuellen Einstellungen anzuzeigen, geben Sie den Befehl QUERY MONITORSETTINGS aus.

Beispiel: Kennwort und Kennwortablaufdauer aktualisieren

Für den Administrator LARRY soll das neue Kennwort SECRETWORD mit einer Kennwortablaufdauer von 120 Tagen vergeben werden. In diesem Beispiel authentifiziert sich der Administrator mit dem IBM Spectrum Protect-Server.

```
update admin larry secretword passexp=120
```

Beispiel: Alle Administratoren für die Kommunikation mit einem Server unter Verwendung der Sitzungssicherheit 'strict' aktualisieren

Alle Administratoren für die Verwendung der striktesten Sicherheitseinstellungen aktualisieren, um sich mit dem Server zu authentifizieren.

```
update admin * sessionsecurity=strict
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE ADMIN

Befehl	Beschreibung
QUERY ADMIN	Zeigt Informationen zu einem oder zu mehreren IBM Spectrum Protect-Administratoren an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
REGISTER ADMIN	Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
RENAME ADMIN	Ändert den Namen eines IBM Spectrum Protect-Administrators.
SET PASSEXP	Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

Zugehörige Tasks:
Tivoli Storage Manager-Objekte benennen
Zugehörige Informationen:
Ssl (Clientoption)

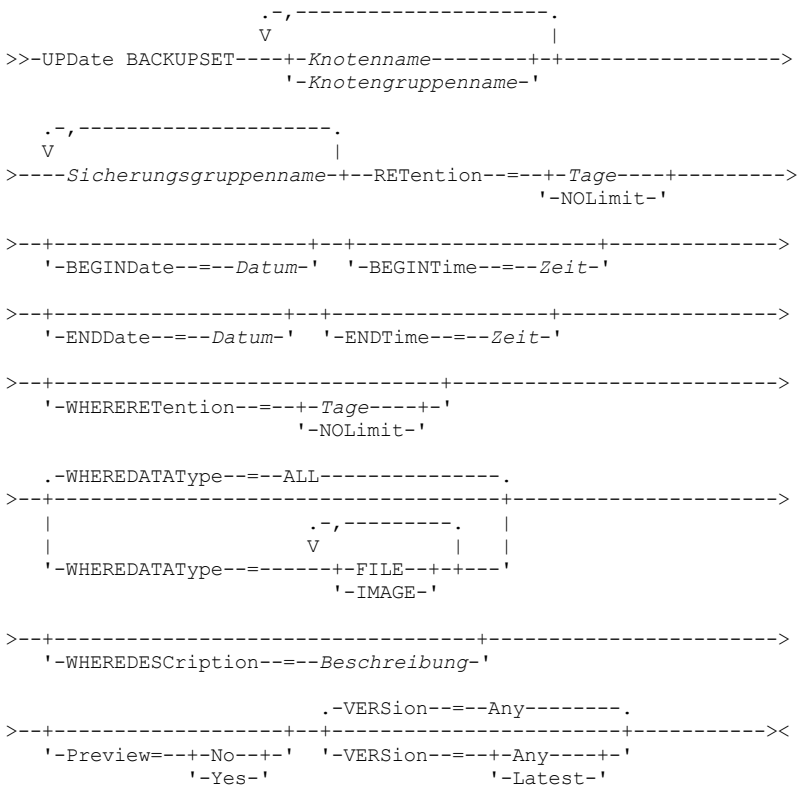
UPDATE BACKUPSET (Aufbewahrungszeitraum einer Sicherungsgruppe aktualisieren)

Mit diesem Befehl kann der Aufbewahrungszeitraum aktualisiert werden, der der Sicherungsgruppe eines Clients zugeordnet ist.

Berechtigungsklasse

Um diesen Befehl ausgeben zu können, müssen Benutzer die Systemberechtigung oder Maßnahmenberechtigung für die Domäne haben, der der Client-Knoten zugeordnet ist.

Syntax



Parameter

Knotenname oder Knotengruppenname (Erforderlich)
: Gibt die Namen der Clientknoten oder Knotengruppen an, deren Daten in der angegebenen Sicherungsgruppe enthalten sind, die aktualisiert werden soll. Sollen mehrere Knoten- und Knotengruppennamen angegeben werden, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Die angegebenen Knotennamen können Platzhalterzeichen enthalten, aber Knotengruppennamen dürfen keine Platzhalterzeichen enthalten.

Sicherungsgruppenname (Erforderlich)
: Gibt den Namen der Sicherungsgruppe an, die aktualisiert werden soll. Der angegebene Sicherungsgruppenname kann Platzhalterzeichen enthalten. Es können mehrere Sicherungsgruppennamen angegeben werden, indem die Namen ohne Leerzeichen durch Kommas voneinander getrennt werden.

RETention (Erforderlich)
: Gibt die aktualisierte Anzahl der Tage an, die die Sicherungsgruppe auf dem Server aufbewahrt werden soll. Sie können eine ganze Zahl von 0 bis 30000 angeben. Gültige Werte:

  Tage
  : Gibt die aktualisierte Anzahl der Tage an, die die Sicherungsgruppe aufbewahrt werden soll.

  NOLimit
  : Gibt an, dass die Sicherungsgruppe auf dem Server unbegrenzt aufbewahrt wird. Wird NOLIMIT angegeben, werden die Datenträger mit der Sicherungsgruppe vom Server unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datenträger aus dem Serverspeicher.
    Achtung: Die Aktualisierung des Aufbewahrungszeitraums einer Sicherungsgruppe kann dazu führen, dass sie zu einem anderen Zeitpunkt als andere Sicherungsgruppen verfällt, die möglicherweise auf demselben Ausgabedatenträger gespeichert sind. Der Datenträger wird in jedem Fall erst dann für andere Verwendungen verfügbar gemacht, wenn alle Sicherungsgruppen verfallen sind.

BEGINDate
: Gibt das Anfangsdatum an, an dem die zu aktualisierende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Dieser Parameter kann mit dem Parameter BEGINTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Anfangsdatum ohne eine Anfangszeit angegeben, lautet die Zeit 24:00 (Mitternacht) an dem angegebenen Datum.
  Sie können das Datum mit einem der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1999
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage *oder* +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage.	TODAY +3 *oder* +3.

Wert	Beschreibung	Beispiel
TODAY-Tage **oder** -Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage.	TODAY-3 *oder* -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

BEGINTime

Gibt die Anfangszeit an, zu der die zu aktualisierende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter kann mit dem Parameter BEGINDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Anfangszeit ohne ein Anfangsdatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Uhrzeit.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den Stunden und Minuten am angegebenen Enddatum	NOW+02:00 *oder* +02:00.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den Stunden und Minuten am angegebenen Enddatum	NOW-02:00 *oder* –02:00.

ENDDate

Gibt das Enddatum an, an dem die zu aktualisierende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDTIME verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird ein Enddatum ohne eine Endzeit angegeben, lautet die Zeit 23:59:59 am angegebenen Enddatum.

Sie können das Datum mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1999
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage *oder* +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage.	TODAY +3 *oder* +3.
TODAY-Tage *oder* — Tage	Das aktuelle Datum minus der Anzahl der angegebenen Tage.	TODAY -3 *oder* -3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

ENDTime

Gibt die Endzeit an, zu der die zu aktualisierende Sicherungsgruppe erstellt wurde. Dieser Parameter ist wahlfrei. Dieser Parameter kann mit dem Parameter ENDDATE verwendet werden, um einen Bereich für das Datum und die Uhrzeit anzugeben. Wird eine Endzeit ohne ein Enddatum angegeben, ist das Datum das aktuelle Datum zu der angegebenen Zeit.

Sie können die Uhrzeit mit einem der folgenden Werte angeben:

Wert	Beschreibung	Beispiel

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM *oder* +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten	NOW+02:00 *oder* +02:00.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW-02:00 *oder* –02:00.

WHERERETention
Gibt den Aufbewahrungszeitraum in Tagen an, der der zu aktualisierenden Sicherungsgruppe zugeordnet ist. Gültige Werte:

Tage
Gibt an, dass die Sicherungsgruppe, die diese Anzahl Tage aufbewahrt wird, aktualisiert wird.
NOLimit
Gibt an, dass die Sicherungsgruppe, die unbegrenzt aufbewahrt wird, aktualisiert wird.

WHEREDESCription
Gibt die Beschreibung an, die der zu aktualisierenden Sicherungsgruppe zugeordnet ist. Dieser Parameter ist wahlfrei. Für die Beschreibung können Platzhalterzeichen angegeben werden. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.
WHEREDATAType
Gibt an, dass die Sicherungsgruppen mit den angegebenen Typen von Daten aktualisiert werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) aktualisiert werden sollen. Bei der Angabe mehrerer Datentypen muss jeder Datentyp durch ein Komma und ohne Leerzeichen voneinander getrennt werden. Gültige Werte:

ALL
Gibt an, dass Sicherungsgruppen für alle Typen von Daten (Dateiebene, Image und Anwendung) aktualisiert werden sollen. Dies ist der Standardwert.
FILE
Gibt an, dass eine Sicherungsgruppe auf Dateiebene aktualisiert werden soll. Sicherungsgruppen auf Dateiebene enthalten Dateien und Verzeichnisse, die vom Client für Sichern/Archivieren gesichert wurden.
IMAGE
Gibt an, dass eine Imagesicherungsgruppe aktualisiert werden soll. Imagesicherungsgruppen enthalten Images, die mit dem Befehl BACKUP IMAGE des Clients für Sichern/Archivieren erstellt wurden.

Preview
Gibt an, ob die Liste der zu aktualisierenden Sicherungsgruppen vorab angezeigt werden soll, ohne die Sicherungsgruppen tatsächlich zu aktualisieren. Dieser Parameter ist wahlfrei. Der Standardwert ist 'No'. Gültige Werte sind:

No
Gibt an, dass die Sicherungsgruppen aktualisiert werden.
Yes
Gibt an, dass der Server die zu aktualisierenden Sicherungsgruppen anzeigt, ohne die Sicherungsgruppen tatsächlich zu aktualisieren.

VERSion
Gibt die Version der Sicherungsgruppe an, die aktualisiert werden soll. Sicherungsgruppen mit demselben Präfixnamen werden als verschiedene Versionen derselben Sicherungsgruppe betrachtet. Dieser Parameter ist wahlfrei. Der Standardwert gibt an, dass alle Versionen aktualisiert werden sollen, die den im Befehl angegebenen Kriterien entsprechen. Gültige Werte:

Any
Gibt an, dass alle Versionen aktualisiert werden sollen, die den im Befehl angegebenen Kriterien entsprechen.
Latest
Gibt an, dass nur die letzte Version der Sicherungsgruppe aktualisiert werden soll. Wenn andere im Befehl angegebene Kriterien (beispielsweise ENDDATE oder WHERERETENTION) die letzte Version der Sicherungsgruppe ausschließen, wird keine Sicherungsgruppe aktualisiert.

Beispiel: Einen Aufbewahrungszeitraum aktualisieren

Den Aufbewahrungszeitraum aktualisieren, wobei die Beschreibung Healthy Computers lautet. Der Aufbewahrungszeitraum ist der Sicherungsgruppe PERS_DATA.3099 zugeordnet, die Daten vom Clientknoten JANE enthält. Den Aufbewahrungszeitraum in 70 Tage ändern.

```
update backupset jane pers_data.3099
retention=70 wheredescription="healthy computers"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE BACKUPSET

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DELETE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.
DELETE NODEGROUP	Löscht eine Knotengruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
GENERATE BACKUPSETTOC	Generiert ein Inhaltsverzeichnis für eine Sicherungsgruppe.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
QUERY BACKUPSETCONTENTS	Zeigt den Inhalt in Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
UPDATE NODEGROUP	Aktualisiert die Beschreibung einer Knotengruppe.

UPDATE CLIENTOPT (Folgenummer einer Clientoption aktualisieren)

Mit diesem Befehl kann die Folgenummer einer Clientoption in einer Clientoptionsgruppe aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

Syntax

```
>>-UPDate CLIENTOpt--Optionsgruppenname--Optionsname------------>

>--aktuelle_Folgenummer--neue_Folgenummer---------------------><
```

Parameter

Optionsgruppenname (Erforderlich)
: Gibt den Namen der Optionsgruppe an.

Optionsname (Erforderlich)
: Gibt eine gültige Client-Option an.

aktuelle_Folgenummer (Erforderlich)
: Gibt die aktuelle Folgenummer der Option an.

neue_Folgenummer (Erforderlich)
: Gibt die neue Folgenummer der Option an.

Beispiel: Folgenummer einer Clientoption aktualisieren

Um die aktuelle Folgenummer der Clientoption zu aktualisieren, den folgenden Befehl ausgeben:

```
update clientopt eng dateformat 0 9
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE CLIENTOPT

Befehl	Beschreibung
COPY CLOPTSET	Kopiert eine Clientoptionsgruppe.
DEFINE CLIENTOPT	Fügt einer Clientoptionsgruppe eine Clientoption hinzu.
DELETE CLIENTOPT	Löscht eine Clientoption aus einer Clientoptionsgruppe.
DELETE CLOPTSET	Löscht eine Clientoptionsgruppe.
QUERY CLOPTSET	Zeigt Informationen über eine Clientoptionsgruppe an.

UPDATE CLOPTSET (Beschreibung einer Clientoptionsgruppe aktualisieren)

Mit diesem Befehl kann die Beschreibung für eine Clientoptionsgruppe aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, der der Clientknoten zugeordnet ist.

Syntax

```
>>-UPDate CLOptset--Optionsgruppenname-------------------------->

>--DESCription--=--Beschreibung-------------------------------><
```

Parameter

Optionsgruppenname (Erforderlich)
: Gibt den Namen der Optionsgruppe an.

DESCription (Erforderlich)
: Gibt eine Beschreibung der Clientoptionsgruppe an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

Beispiel: Beschreibung einer Clientoptionsgruppe aktualisieren

Aktualisieren Sie die Beschreibung für die Clientoptionsgruppe mit dem Namen ENG.

```
update cloptset eng description="unix"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE CLOPTSET

Befehl	Beschreibung
COPY CLOPTSET	Kopiert eine Clientoptionsgruppe.
DEFINE CLIENTOPT	Fügt einer Clientoptionsgruppe eine Clientoption hinzu.
DEFINE CLOPTSET	Definiert eine Clientoptionsgruppe.
DELETE CLIENTOPT	Löscht eine Clientoption aus einer Clientoptionsgruppe.
DELETE CLOPTSET	Löscht eine Clientoptionsgruppe.
QUERY CLOPTSET	Zeigt Informationen über eine Clientoptionsgruppe an.
UPDATE CLIENTOPT	Aktualisiert die Folgenummer einer Clientoption in einer Clientoptionsgruppe.

UPDATE COLLOCGROUP (Kollokationsgruppe aktualisieren)

Verwenden Sie diesen Befehl, um die Beschreibung einer Kollokationsgruppe zu ändern.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate COLLOCGroup--Gruppenname------------------------------>

>--DESCription--=--Beschreibung-------------------------------><
```

Parameter

Gruppenname
: Gibt den Namen der Kollokationsgruppe an, deren Beschreibung aktualisiert werden soll.

DESCription (Erforderlich)
Gibt eine Beschreibung der Kollokationsgruppe an. Dieser Parameter ist erforderlich. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Enthält die Beschreibung Leerzeichen, schließen Sie die gesamte Beschreibung in Anführungszeichen ein.

Beispiel: Eine Kollokationsgruppe aktualisieren

Die Kollokationsgruppe GROUP1 mit einer neuen Beschreibung aktualisieren.

```
update collocgroup group1 "Personalabteilung"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE COLLOCGROUP

Befehl	Beschreibung
DEFINE COLLOCGROUP	Definiert eine Kollokationsgruppe.
DEFINE COLLOCMEMBER	Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE COLLOCGROUP	Löscht eine Kollokationsgruppe.
DELETE COLLOCMEMBER	Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.
MOVE NODEDATA	Versetzt Daten für einen oder mehrere Knoten oder für einen einzelnen Knoten mit ausgewählten Dateibereichen.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
UPDATE STGPOOL	Ändert die Attribute eines Speicherpools.

UPDATE COPYGROUP (Kopiengruppe aktualisieren)

Mit diesem Befehl kann eine Sicherungs- oder Archivierungskopiengruppe aktualisiert werden. Um Clients die Verwendung der aktualisierten Kopiengruppe zu ermöglichen, muss die Maßnahmengruppe aktiviert werden, die die Kopiengruppe enthält.

Tipp: Der Befehl UPDATE COPYGROUP schlägt fehl, wenn ein Kopienspeicherpool als Zielort angegeben wird.

Der Befehl UPDATE COPYGROUP liegt in zwei unterschiedlichen Formaten vor, und zwar abhängig davon, ob eine Sicherungskopiengruppe oder eine Archivierungskopiengruppe aktualisiert werden soll. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für UPDATE COPYGROUP

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
ASSIGN DEFMGMTCLASS	Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu.
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DELETE COPYGROUP	Löscht eine Sicherungs- oder Archivierungskopiengruppe aus einer Maßnahmendomäne und Maßnahmengruppe.
DELETE MGMTCLASS	Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.

Befehl	Beschreibung
EXPIRE INVENTORY	Startet die Verfallsverarbeitung für den Datenträgerbestandsverfall manuell.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.

- UPDATE COPYGROUP (Sicherungskopiengruppe aktualisieren)
  Mit diesem Befehl kann eine definierte Sicherungskopiengruppe aktualisiert werden.
- UPDATE COPYGROUP (Definierte Archivierungskopiengruppe aktualisieren)
  Mit diesem Befehl kann eine definierte Archivierungskopiengruppe aktualisiert werden.

UPDATE COPYGROUP (Sicherungskopiengruppe aktualisieren)

Mit diesem Befehl kann eine definierte Sicherungskopiengruppe aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Kopiengruppe gehört.

Syntax

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Kopiengruppe gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, zu der die Kopiengruppe gehört.Eine Kopiengruppe in der AKTIVEN Maßnahmengruppe kann nicht aktualisiert werden.

Klassenname (Erforderlich)
: Gibt die Verwaltungsklasse an, zu der die Kopiengruppe gehört.

STANDARD
: Gibt die Kopiengruppe an, die STANDARD lauten muss. Dieser Parameter ist wahlfrei.

Type=Backup
: Gibt an, dass eine Sicherungskopiengruppe aktualisiert werden soll. Dieser Parameter ist wahlfrei.

DESTination
Gibt den primären Speicherpool an, in dem der Server anfänglich Sicherungsdaten speichert. Dieser Parameter ist wahlfrei. Ein Kopienspeicherpool kann nicht als Zielort angegeben werden.

FREQuency
Gibt an, wie oft der Server eine Datei sichern kann. Dieser Parameter ist wahlfrei. Der Server sichert eine Datei nur, wenn die angegebene Anzahl Tage seit der letzten Sicherung verstrichen ist. Der Wert für den Parameter FREQUENCY wird nur bei einer vollständigen Teilsicherung verwendet. Dieser Wert wird bei einer selektiven Sicherung oder einer partiellen Teilsicherung ignoriert. Zulässige Werte sind ganze Zahlen von 0 bis 9999. Der Wert 0 bedeutet, daß der Server eine Datei unabhängig vom Datum der letzten Sicherung sichern kann.

VERExists
Gibt die maximale Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die sich momentan im Client-Dateisystem befinden. Dieser Parameter ist wahlfrei.
Wird der Grenzwert durch eine Teilsicherung überschritten, verfällt die älteste Sicherungsversion, die im Serverspeicher vorhanden ist.
Gültige Werte:

Zahl
Gibt die Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die sich momentan im Client-Dateisystem befinden. Zulässige Werte sind ganze Zahlen von 1 bis 9999.

NOLimit
Gibt an, daß der Server alle Sicherungsversionen aufbewahren soll.

Die Anzahl der Sicherungsversionen, die aufbewahrt werden sollen, wird so lange durch diesen Parameter gesteuert, bis Versionen den Aufbewahrungszeitraum überschreiten, der durch den Parameter RETEXTRA angegeben ist.

VERDeleted
Gibt die maximale Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die nach der Sicherung mit dem Server aus dem Client-Dateisystem gelöscht wurden. Dieser Parameter ist wahlfrei.
Löscht ein Benutzer eine Datei aus dem Clientdateisystem, ändert der Server bei der nächsten Teilsicherung die aktive Sicherungsversion der Datei in eine inaktive Version und markiert die ältesten Versionen, die diese Anzahl überschreiten, als verfallen. Das Verfallsdatum der übrigen Versionen wird durch den Aufbewahrungszeitraum bestimmt, der mit dem Parameter RETEXTRA oder RETONLY angegeben wurde.
Gültige Werte:

Anzahl
Gibt die Anzahl Sicherungsversionen an, die für Dateien aufbewahrt werden sollen, die nach der Sicherung aus dem Client-Dateisystem gelöscht werden. Es kann ein Wert von 0 bis 9999 angegeben werden.

NOLimit
Gibt an, dass der Server alle Sicherungsversionen für Dateien, die nach der Sicherung aus dem Clientdateisystem gelöscht werden, aufbewahren soll.

RETExtra
Gibt die Anzahl der Tage an, die der Server eine Sicherungsversion aufbewahrt, nachdem diese Version inaktiv wurde. Die Version einer Datei wird inaktiv, wenn der Client eine aktuellere Sicherungsversion speichert oder wenn der Client die Datei aus der Datenstation löscht und dann eine vollständige Teilsicherung durchführt. Der Server löscht inaktive Versionen auf der Basis des Aufbewahrungszeitraums, auch wenn die Anzahl der inaktiven Versionen die durch den Parameter VEREXISTS oder VERDELETED erlaubte Anzahl nicht überschreitet. Dieser Parameter ist wahlfrei. Gültige Werte:

Tage
Gibt die Anzahl Tage an, die inaktive Sicherungsversionen aufbewahrt werden sollen. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

NOLimit
Gibt an, dass inaktive Sicherungsversionen unbegrenzt aufbewahrt werden sollen.

Wird NOLIMIT angegeben, löscht der Server überzählige Sicherungsversionen auf der Basis des Parameters VEREXISTS (wenn die Datei noch im Client-Dateisystem vorhanden ist) oder auf der Basis des Parameters VERDELETED (wenn die Datei nicht mehr im Client-Dateisystem vorhanden ist).

RETOnly
Gibt die Anzahl Tage an, die die letzte Sicherungsversion einer Datei aufbewahrt werden soll, die aus dem Client-Dateisystem gelöscht wurde. Dieser Parameter ist wahlfrei. Gültige Werte:

Tage
Gibt die Anzahl Tage an, die die letzte verbleibende inaktive Kopie einer Datei aufbewahrt werden soll. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

NOLimit
Gibt an, dass die letzte verbleibende inaktive Version einer Datei unbegrenzt aufbewahrt werden soll.

Wird NOLIMIT angegeben, wird die letzte verbleibende Sicherungsversion unbegrenzt von dem Server aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datei aus dem Server-Speicher.

MODE
Gibt an, ob der Server eine Datei nur sichert, wenn sich die Datei seit der letzten Sicherung geändert hat oder wenn ein Client eine Sicherung anfordert. Dieser Parameter ist wahlfrei. Gültige Werte:

MODified
Gibt an, daß die Datei nur gesichert wird, wenn sie sich seit der letzten Sicherung geändert hat. Eine Datei wird als geändert angesehen, wenn folgende Bedingungen gelten:

- Das Datum der letzten Änderung hat sich geändert.
- Die Dateigröße hat sich geändert.
- Der Dateieigner hat sich geändert.
- Die Dateiberechtigungen haben sich geändert.

ABSolute
Gibt an, daß die Datei unabhängig davon gesichert wird, ob sie geändert wurde.

Der Wert für MODE wird nur für vollständige Teilsicherungen verwendet. Dieser Wert wird bei einer partiellen Teilsicherung oder einer selektiven Sicherung ignoriert.

SERialization
Gibt an, wie der Server Dateien oder Verzeichnisse verarbeitet, wenn sie während der Sicherungsverarbeitung geändert werden. Dieser Parameter ist wahlfrei. Gültige Werte:

SHRSTatic
Gibt an, daß der Server eine Datei oder ein Verzeichnis nur sichert, wenn die Datei oder das Verzeichnis während der Sicherung nicht geändert wird. Der Server versucht bis zu viermal, eine Sicherung durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde. Wird die Datei oder das Verzeichnis während jedes Sicherungsversuchs geändert, sichert der Server die Datei oder das Verzeichnis nicht.

STatic
Gibt an, daß der Server eine Datei oder ein Verzeichnis nur sichert, wenn die Datei oder das Verzeichnis während der Sicherung nicht geändert wird. Der Server versucht nur einmal, die Sicherung durchzuführen.

Plattformen, die die Option STATIC nicht unterstützen, nehmen den Standardwert SHRSTATIC an.

SHRDYnamic
Gibt an, daß der Server die Datei oder das Verzeichnis während des letzten Sicherungsversuchs sichert, auch wenn die Datei oder das Verzeichnis während der Sicherung geändert wird. Der Server versucht bis zu viermal, eine Sicherung durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde.

DYnamic
Gibt an, daß der Server eine Datei oder ein Verzeichnis beim ersten Versuch sichert, auch wenn die Datei oder das Verzeichnis während der Sicherungsverarbeitung geändert wird.

Wichtig: Die Werte SHRDYNAMIC und DYNAMIC sind mit Vorsicht zu verwenden. IBM Spectrum Protect bestimmt anhand dieser Werte, ob eine Datei oder ein Verzeichnis gesichert wird, während Änderungen vorgenommen werden. Aus diesem Grund ist die Sicherungsversion möglicherweise nur eine Sicherung mit grober Übereinstimmung. Eine Sicherung mit grober Übereinstimmung gibt den aktuellen Inhalt der Datei oder des Verzeichnisses nicht korrekt wieder, da sie einige, aber nicht alle Änderungen enthält. Wird eine Datei, die eine Sicherung mit grober Übereinstimmung enthält, zurückgeschrieben, ist die Datei möglicherweise nicht brauchbar. Dies ist von der Anwendung abhängig, die die Datei verwendet. Ist eine Sicherung mit grober Übereinstimmung nicht akzeptabel, definieren Sie für SERIALIZATION den Wert SHRSTATIC oder STATIC, damit IBM Spectrum Protect nur dann eine Sicherungsversion erstellt, wenn die Datei oder das Verzeichnis nicht geändert wird.

TOCDestination

Gibt den primären Speicherpool an, in dem ein Inhaltsverzeichnis für jede NDMP-Sicherungs- oder Sicherungsgruppenoperation anfänglich gespeichert wird, für die ein Inhaltsverzeichnis generiert wird. Dieser Parameter ist wahlfrei. Ein Kopienspeicherpool kann nicht als Zielort angegeben werden. Der als Zielort angegebene Speicherpool muss das Datenformat NATIVE oder NONBLOCK haben. Um Ladeverzögerungen zu vermeiden, wird empfohlen, dass der Speicherpool die Einheitenklasse DISK oder DEVTYPE=FILE hat. Die Generierung eines Inhaltsverzeichnisses ist eine Option für NDMP-Sicherungsoperationen, wird aber nicht für andere Imagesicherungsoperationen unterstützt.

Um einen vorhandenen Zielort für das Inhaltsverzeichnis aus der Kopiengruppe zu entfernen, geben Sie eine leere Zeichenfolge ("") für diesen Wert an.

Wird die Erstellung eines Inhaltsverzeichnisses (TOC) für eine Sicherungsoperation angefordert, die NDMP verwendet, und ist das Image an eine Verwaltungsklasse gebunden, deren Sicherungskopiengruppe keinen Zielort für das Inhaltsverzeichnis angibt, hängt das Ergebnis von dem TOC-Parameter für die Sicherungsoperation ab.

- Bei TOC=PREFERRED (Standardwert) wird die Sicherung ohne Erstellung eines Inhaltsverzeichnisses fortgesetzt.
- Bei TOC=YES schlägt die gesamte Sicherung fehl, da kein Inhaltsverzeichnis erstellt werden kann.

Beispiel: Eine Sicherungskopiengruppe aktualisieren

Die Sicherungskopiengruppe STANDARD in der Maßnahmendomäne EMPLOYEE_RECORDS, Maßnahmengruppe VACATION, Verwaltungsklasse ACTIVEFILES aktualisieren. Den Zielort in DISKPOOL ändern, mit einem Mindestintervall von sieben Tagen zwischen Sicherungen, unabhängig davon, ob die Dateien geändert wurden. Bis zu drei Sicherungsversionen aufbewahren, während eine Datei noch in einem Client-Dateisystem vorhanden ist.

```
update copygroup employee_records vacation
activefiles type=backup destination=diskpool
frequency=7 verexists=3 mode=absolute
```

UPDATE COPYGROUP (Definierte Archivierungskopiengruppe aktualisieren)

Mit diesem Befehl kann eine definierte Archivierungskopiengruppe aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Kopiengruppe gehört.

Syntax

```
>>-UPDate COpygroup---------------------------------------------->

>--Domänenname--Name_der_Maßnahmengruppe--Klassenname----------->

>--+----------+--Type--=--Archive------------------------------->
   '-STANDARD-'

>--+--------------------------+--+------------------+---------->
   '-DESTination--=--Poolname-'  '-FREQuency--=--Cmd-'

>--+------------------------+--+------------------+------------>
   '-RETVer--=--+-Tage----+-'  '-MODE--=--ABSolute-'
                '-NOLimit-'

>--+--------------------+-------------------------------------->
   '-RETMin--=----Tage---'

>--+---------------------------------+------------------------><
   '-SERialization--=--+-SHRSTatic--+-'
                       +-STatic-----+
                       +-SHRDYnamic-+
                       '-DYnamic----'
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Kopiengruppe gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, zu der die Kopiengruppe gehört.Eine Kopiengruppe in der AKTIVEN Maßnahmengruppe kann nicht aktualisiert werden.

Klassenname (Erforderlich)
: Gibt die Verwaltungsklasse an, zu der die Kopiengruppe gehört.

STANDARD
: Gibt die Kopiengruppe an, die STANDARD lauten muss. Dieser Parameter ist wahlfrei.

Type=Archive (Erforderlich)
: Gibt an, dass eine Archivierungskopiengruppe aktualisiert werden soll. Dieser Parameter ist erforderlich.

DESTination
: Gibt den primären Speicherpool an, in dem der Server anfänglich die Archivierungskopie speichert. Dieser Parameter ist wahlfrei. Ein Kopienspeicherpool kann nicht als Zielort angegeben werden.

FREQuency=Cmd
: Gibt die Kopienhäufigkeit an, die CMD lauten muss. Dieser Parameter ist wahlfrei.

RETVer
: Gibt die Anzahl Tage an, die eine Archivierungskopie aufbewahrt werden soll. Dieser Parameter ist wahlfrei. Gültige Werte:

  Tage
  : Gibt die Anzahl Tage an, die eine Archivierungskopie aufbewahrt werden soll. Sie können eine ganze Zahl von 0 bis 30000 angeben.

  NOLimit
  : Gibt an, dass eine Archivierungskopie unbegrenzt aufbewahrt werden soll.

    Wird NOLIMIT angegeben, werden Archivierungskopien von dem Server unbegrenzt aufbewahrt, es sei denn, ein Benutzer oder Administrator löscht die Datei aus dem Serverspeicher.

  Der Wert des Parameters RETVER kann Auswirkungen auf die Verwaltungsklasse haben, mit der der Server ein archiviertes Verzeichnis verbindet. Wenn der Client die Option ARCHMC nicht verwendet, verbindet der Server Verzeichnisse, die archiviert werden, mit der Standardverwaltungsklasse. Verfügt die Standardverwaltungsklasse über keine Archivierungskopiengruppe, verbindet der Server Verzeichnisse, die archiviert werden, mit der Verwaltungsklasse mit dem kürzesten Aufbewahrungszeitraum.

MODE=ABSolute
: Gibt an, dass eine Datei immer archiviert wird, wenn der Client dies anfordert. Der Parameter MODE muss den Wert ABSOLUTE haben. Dieser Parameter ist wahlfrei.

RETMin
: Gibt die Mindestanzahl von Tagen an, die eine Archivierungskopie aufbewahrt werden soll, nachdem sie archiviert wurde. Dieser Parameter ist wahlfrei. Der Standardwert ist 365.

SERialization
: Gibt an, wie der Server Dateien verarbeitet, die während der Archivierung geändert werden. Dieser Parameter ist wahlfrei. Gültige Werte:

  SHRSTatic
  : Gibt an, daß der Server keine Datei archiviert, die gerade geändert wird. Der Server versucht bis zu viermal, eine Archivierung durchzuführen, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde. Wenn die Datei während des Archivierungsversuchs geändert wird, archiviert der Server die Datei nicht.

  STatic
  : Gibt an, daß der Server keine Datei archiviert, die gerade geändert wird. Wenn eine Datei während des Archivierungsversuchs geändert wird, archiviert der Server die Datei nicht.

    Plattformen, die die Option STATIC nicht unterstützen, nehmen den Standardwert SHRSTATIC an.

  SHRDYnamic
  : Gibt an, daß der Server die Datei während des letzten Archivierungsversuchs archiviert, auch wenn die Datei während der Archivierung geändert wird. Der Server versucht bis zu viermal, die Datei zu archivieren, abhängig von dem Wert, der für die Clientoption CHANGINGRETRIES angegeben wurde.

  DYnamic
  : Gibt an, daß der Server eine Datei beim ersten Versuch archiviert, auch wenn sie während der Archivierungsverarbeitung geändert wird.

  Wichtig: Die Werte SHRDYNAMIC und DYNAMIC sind mit Vorsicht zu verwenden. IBM Spectrum Protect bestimmt anhand dieser Werte, ob eine Datei archiviert wird, während Änderungen vorgenommen werden. Aus diesem Grund ist die Archivierungskopie möglicherweise nur eine Sicherung mit grober Übereinstimmung. Eine Sicherung mit grober Übereinstimmung gibt den aktuellen Inhalt der Datei nicht korrekt wieder, da sie einige, aber nicht alle Änderungen enthält. Wird eine Datei, die eine Sicherung mit grober Übereinstimmung enthält, abgerufen, ist die Datei möglicherweise nicht brauchbar. Dies ist von der Anwendung abhängig, die die Datei verwendet. Ist eine Sicherung mit grober Übereinstimmung nicht akzeptabel, definieren Sie für SERIALIZATION den Wert SHRSTATIC oder STATIC, damit IBM Spectrum Protect nur dann eine Archivierungskopie erstellt, wenn die Datei nicht geändert wird.
  Tipp: Gehen Sie bei der Auswahl von Werten für die Aufbewahrungsdauer für primäre Speicherpools, die den Typ RECLAMATIONTYPE=SNAPLOCK haben, mit Vorsicht vor. Datenträger in Speicherpools mit diesem Typ können erst gelöscht werden, wenn die Daten ihrer Aufbewahrungsdauer verstrichen sind.

Beispiel: Mehrere Elemente einer Kopiengruppe aktualisieren

Die Archivierungskopiengruppe STANDARD in der Maßnahmendomäne EMPLOYEE_RECORDS, Maßnahmengruppe VACATION, Verwaltungsklasse ACTIVEFILES aktualisieren. Den Zielort in TAPEPOOL ändern. Archivierungskopien 190 Tage aufbewahren.

```
update copygroup employee_records vacation
activefiles standard type=archive
destination=tapepool retver=190
```

UPDATE DATAMOVER (Einheit zum Versetzen von Daten aktualisieren)

Verwenden Sie diesen Befehl, um die Definition einer Einheit zum Versetzen von Daten zu aktualisieren oder eine Einheit zum Versetzen von Daten abzuhängen, wenn die Hardware gewartet wird.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DATAMover--Name_der_Einheit_zum_Versetzen_von_Daten--->

>--+------------------------+--+----------------------------+--->
   '-HLAddress--=--Adresse-'  '-LLAddress--=--TCP-Anschluss-'

>--+------------------------+--+----------------------+-------->
   '-USERid--=--Benutzer-ID-'  '-PASsword--=--Kennwort-'

>--+--------------------+--------------------------------------><
   '-ONLine--=--+-Yes-+-'
                '-No--'
```

Parameter

Name_der_Einheit_zum_Versetzen_von_Daten (Erforderlich)
Gibt den Namen der Einheit zum Versetzen von Daten an.

HLAddress
Gibt entweder die neue numerische IP-Adresse oder den neuen Domänennamen an, die für den Zugriff auf den NAS-Dateiserver verwendet werden. Dieser Parameter ist wahlfrei.

LLAddress
Gibt die neue TCP-Anschlussnummer für den Zugriff auf den NAS-Dateiserver für NDMP-Sitzungen (NDMP = Network Data Management Protocol) an. Dieser Parameter ist wahlfrei.

USERid
Gibt die Benutzer-ID eines Benutzers an, der berechtigt ist, eine NDMP-Sitzung mit dem NAS-Dateiserver einzuleiten. Geben Sie beispielsweise die Verwaltungs-ID eines NetApp-Dateiservers ein. Dieser Parameter ist wahlfrei.

PASsword
Gibt das neue Kennwort der Benutzer-ID für die Anmeldung beim NAS-Dateiserver an. Dieser Parameter ist wahlfrei.

ONLine
Gibt an, ob die Einheit zum Versetzen von Daten für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei.

Yes
Gibt an, dass die Einheit zum Versetzen von Daten für die Verwendung verfügbar ist.

No
Gibt an, dass die Einheit zum Versetzen von Daten nicht für die Verwendung verfügbar ist.
Achtung: Wird ein Kassettenarchiv durch die Verwendung eines Pfads von einer Einheit zum Versetzen von Daten zu dem Kassettenarchiv gesteuert, und ist die Einheit zum Versetzen von Daten offline, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während die Einheit zum Versetzen von Daten offline ist, wird das Kassettenarchiv nicht initialisiert.

Beispiel: IP-Adresse für eine Einheit zum Versetzen von Daten aktualisieren

Die Einheit zum Versetzen von Daten für den Knoten NAS1 aktualisieren. Die numerische IP-Adresse von 9.67.97.103 in 9.67.97.109 ändern.

```
update datamover nas1 hladdress=9.67.97.109
```

Beispiel: Domänenname für eine Einheit zum Versetzen von Daten aktualisieren

Die Einheit zum Versetzen von Daten für den Knoten NAS1 aktualisieren. Die numerische IP-Adresse von 9.67.97.109 in den Domänennamen NETAPP2.TUCSON.IBM.COM ändern.

```
update datamover nas1 hladdress=netapp2.tucson.ibm.com
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE DATAMOVER

Befehl	Beschreibung
DEFINE DATAMOVER	Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE DATAMOVER	Löscht eine Einheit zum Versetzen von Daten.
QUERY DATAMOVER	Zeigt Definitionen der Einheit zum Versetzen von Daten an.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

UPDATE DEVCLASS (Attribute einer Einheitenklasse aktualisieren)

Mit diesem Befehl kann eine definierte Einheitenklasse aktualisiert werden.

Anmerkung: Die Einheitenklasse DISK wird von IBM Spectrum Protect vordefiniert und kann mit dem Befehl UPDATE DEVCLASS nicht geändert werden.

 AIX-Betriebssysteme  Linux-BetriebssystemeWenn Sie eine Einheitenklasse für Einheiten aktualisieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server aktualisieren).

Die Syntax und Parameterbeschreibungen werden entsprechend des Einheitentyps zur Verfügung gestellt. Die Syntax- und Parameterinformationen sind in der folgenden Reihenfolge aufgeführt.

- UPDATE DEVCLASS (Einheitenklasse 3590 aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse 3592 aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse 4MM aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse 8MM aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse CENTERA aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse DLT aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse FILE aktualisieren)
-  AIX-Betriebssysteme  Windows-BetriebssystemeUPDATE DEVCLASS (Einheitenklasse GENERICTAPE aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse LTO aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse NAS aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse REMOVABLEFILE aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse SERVER aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse VOLSAFE aktualisieren)

Tabelle 1. Zugehörige Befehle für UPDATE DEVCLASS

Befehl	Beschreibung
BACKUP DEVCONFIG	Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DELETE DEVCLASS	Löscht eine Einheitenklasse.
QUERY DEVCLASS	Zeigt Informationen zu Einheitenklassen an.
QUERY DIRSPACE	Zeigt Informationen zu Verzeichnissen FILE an.
UPDATE LIBRARY	Ändert die Attribute eines Kassettenarchivs.

UPDATE DEVCLASS (Einheitenklasse 3590 aktualisieren)

Verwenden Sie die Einheitenklasse 3590, wenn Sie 3590-Bandeinheiten verwenden.

 AIX-Betriebssysteme  Linux-BetriebssystemeWenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server aktualisieren).

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+---------------------------------+-------------------------->
   '-LIBRary---=--Kassettenarchivname-'

>--+-------------------------+--+----------------------+-------->
   '-FORMAT--=--+-DRIVE---+-'  '-ESTCAPacity--=--Größe-'
                +-3590B---+
                +-3590C---+
                +-3590E-B-+
                +-3590E-C-+
                +-3590H-B-+
                '-3590H-C-'

>--+---------------------------------------+---------------------->
   '-PREFIX--=--+-ADSM-------------------+-'
                '-Banddatenträgerpräfix-'

>--+-----------------------------+--+----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

>--+---------------------------+-------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der zu definierenden Einheitenklasse an.

LIBRary

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT
Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

In den folgenden Tabellen sind die Aufzeichnungsformate, die geschätzten Kapazitäten und die Optionen der Aufzeichnungsformate für 3590-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 3590

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
3590B	10,0 GB	Dekomprimiertes (Basis-)Format
3590C	Siehe Anmerkung 20,0 GB	Komprimiertes Format
3590E-B	10,0 GB	Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format
3590E-C	Siehe Anmerkung 20,0 GB	Komprimiertes Format, ähnlich dem 3590C-Format
3590H-B	30,0 GB (J-Kassette - Standardlänge) 60,0 GB (K-Kassette - erweiterte Länge)	Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format
3590H-C	Siehe Anmerkung 60,0 GB (J-Kassette - Standardlänge) 120,0 GB (K-Kassette - erweiterte Länge)	Komprimiertes Format, ähnlich dem 3590C-Format
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein.		

Tabelle 2. Auswahl des Aufzeichnungsformats für 3590-Einheiten

Einheit	Format					
	3590B	3590C	3590E-B	3590E-C	3590H-B	3590H-C
3590	Lesen/ Schreiben	Lesen/ Schreiben	–	–	–	–
Ultra SCSI	Lesen/ Schreiben	Lesen/ Schreiben	–	–	–	–
3590E	Lesen	Lesen	Lesen/ Schreiben	Lesen/ Schreiben	–	–
3590H	Lesen	Lesen	Lesen	Lesen	Lesen/ Schreiben	Lesen/ Schreiben

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die durch diese Einheitenklasse kategorisiert werden. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

PREFIX
Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES
Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl
: Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)
: Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

UPDATE DEVCLASS (Einheitenklasse 3592 aktualisieren)

AIX-Betriebssysteme Linux-BetriebssystemeWenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server aktualisieren).

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+---------------------------------+-------------------------->
   '-LIBRary--=--Kassettenarchivname-'

>--+-----------------------------+----------------------------->
   '-LBProtect--=--+-READWrite-+-'
                   +-WRITEOnly-+
                   '-No--------'

>--+---------------------------+--+-------------------------+---->
   '-SCALECAPacity--=--+-100-+-'  '-FORMAT--=--+-DRIVE---+-'
                       +-90--+                 +-3592----+
                       '-20--'                 +-3592C---+
                                               +-3592-2--+
                                               +-3592-2C-+
                                               +-3592-3--+
                                               +-3592-3C-+
                                               +-3592-4--+
                                               '-3592-4C-'

>--+-----------------------+------------------------------------>
   '-ESTCAPacity--=--Größe-'

>--+-------------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

>--+-----------------------------+--+-----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

>--+-----------------------------+-------------------------------->
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'

>--+-----------------------------------------------+------------><
   |  (1)   (2)                                   |
   '-------------DRIVEEncryption--=--+-ON-------+-'
                                     +-ALLOW----+
                                     +-EXTERNAL-+
                                     '-OFF------'
```

Anmerkungen:

1. Sie können nicht WORM=Yes in Verbindung mit DRIVEENCRYPTION=ON angeben.
2. Laufwerkverschlüsselung wird nur für 3592-Laufwerke der Generation 2 oder höher unterstützt.

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

LBProtect

Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffschutzinformationen, wenn Daten von dem Band gelesen werden.

Die folgenden Werte sind gültig:

READWrite
: Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

  Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

WRITEOnly
: Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

No
: Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur für IBM® 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher unterstützt.

In Technote 1634851, Additional information on the Tivoli Storage Manager LBProtect option, wird erläutert, wann der Parameter LBProtect zu verwenden ist.

SCALECAPacity
: Gibt den Prozentsatz der Datenträgerkapazität an, der zum Speichern von Daten verwendet werden kann. Dieser Parameter ist wahlfrei. Gültige Werte sind 20, 90 oder 100.

  Wird für SCALECAPacity der Wert 100 angegeben, wird die maximale Speicherkapazität zur Verfügung gestellt. Wird der Wert 20 angegeben, wird die schnellste Zugriffszeit zur Verfügung gestellt.

  Anmerkung: Der Wert für SCALECAPacity wird wirksam, wenn Daten zum ersten Mal auf einen Datenträger geschrieben werden. Alle Aktualisierungen an der Einheitenklasse für SCALECAPacity haben erst dann Auswirkungen auf Datenträger, auf die bereits Daten geschrieben wurden, wenn die Datenträger wieder in den Arbeitsdatenträgerstatus versetzt werden.

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

  Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

  In der folgenden Tabelle sind die Aufzeichnungsformate, die geschätzten Kapazitäten und die Optionen der Aufzeichnungsformate für 3592-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 3592

Format	Geschätzte Kapazität	Beschreibung

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
3592	300 GB	Dekomprimiertes (Basis-)Format
3592C	Siehe Anmerkung 900 GB	Komprimiertes Format
3592-2	500 GB 700 GB	JA-Bänder mit dekomprimiertem (Basis-)Format JB-Bänder mit dekomprimiertem (Basis-)Format
3592-2C	1,5 TB 2,1 TB	JA-Bänder mit komprimiertem Format JB-Bänder mit komprimiertem Format
3592–3	640 GB 1 TB	JA-Bänder mit dekomprimiertem (Basis-)Format JB-Bänder mit dekomprimiertem (Basis-)Format
3592–3C	1,9 TB 3 TB	JA-Bänder mit komprimiertem Format JB-Bänder mit komprimiertem Format
3592-4	400 GB 1,5 TB 3,1 TB	JK-Bänder mit dekomprimiertem (Basis-)Format JB-Bänder mit dekomprimiertem (Basis-)Format JC-Band mit dekomprimiertem (Basis-)Format
3592-4C	1,2 TB 4,4 TB 9,4 TB	JK-Bänder mit komprimiertem Format JB-Bänder mit komprimiertem Format JC-Bänder mit komprimiertem Format
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann je nach Effektivität der Komprimierung die tatsächliche Kapazität von dem aufgelisteten Wert abweichen.		

Wichtig: Um eine optimale Leistung zu erzielen, sollte das Mischen von Laufwerken verschiedener Generationen in einem einzelnen SCSI-Kassettenarchiv vermieden werden.

Spezielle Konfigurationen sind auch erforderlich, wenn verschiedene Generationen von 3592-Laufwerken in 349x- und ACSLS-Kassettenarchiven gemischt werden.

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

  Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

  Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DRIVEEncryption
: Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei.

  Die Aktualisierung dieses Parameters wirkt sich nur auf leere Datenträger aus. War ein Datenträger, der gefüllt wurde, zuvor verschlüsselt, oder ist der Datenträger nicht verschlüsselt, und wird der Parameter DRIVEENCRYPTION aktualisiert, behält der Datenträger seinen ursprünglichen verschlüsselten oder nicht verschlüsselten Status. Der Datenträger behält außerdem seinen ursprünglichen Schlüsselverwaltungsstatus.

  ON
  : Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern, wie beispielsweise Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger, werden nicht verschlüsselt.) Wird ON angegeben und entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

  ALLOW

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch erlaubt, wenn entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert ist.

EXTERNAL

Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist.
Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert.
Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

OFF

Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird entweder das Kassettenarchivverfahren oder das Systemverfahren der Verschlüsselung aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

UPDATE DEVCLASS (Einheitenklasse 4MM aktualisieren)

Verwenden Sie die Einheitenklasse 4MM, wenn Sie 4-mm-Bandeinheiten verwenden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+---------------------------------+-------------------------->
   '-LIBRary--=--Kassettenarchivname-'

>--+----------------------+--+----------------------+---------->
   '-FORMAT--=--+-DRIVE-+-'  '-ESTCAPacity--=--Größe-'
                +-DDS1--+
                +-DDS1C-+
                +-DDS2--+
                +-DDS2C-+
                +-DDS3--+
                +-DDS3C-+
                +-DDS4--+
                +-DDS4C-+
                +-DDS5--+
                +-DDS5C-+
                +-DDS6--+
                '-DDS6C-'

>--+--------------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

>--+-----------------------+--+---------------------------+---->
   '-MOUNTWait--=--Minuten-'  '-MOUNTRetention--=--Minuten-'

>--+--------------------------+-------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der zu definierenden Einheitenklasse an.

LIBRary

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten 4-mm-Bandlaufwerke enthält. Dieser Parameter ist wahlfrei. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für 4-mm-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für 4-mm-Bänder

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
DDS1	1,3 GB (60 Meter) 2,0 GB (90 Meter)	Dekomprimiertes Format, gilt nur für 60-Meter-Bänder und 90-Meter-Bänder
DDS1C	Siehe Anmerkung 1,3 GB (60 Meter) 2,0 GB (90 Meter)	Komprimiertes Format, gilt nur für 60-Meter-Bänder und 90-Meter-Bänder
DDS2	4,0 GB	Dekomprimiertes Format, gilt nur für 120-Meter-Bänder
DDS2C	Siehe Anmerkung 8,0 GB	Komprimiertes Format, gilt nur für 120-Meter-Bänder
DDS3	12,0 GB	Dekomprimiertes Format, gilt nur für 125-Meter-Bänder
DDS3C	Siehe Anmerkung 24,0 GB	Komprimiertes Format, gilt nur für 125-Meter-Bänder
DDS4	20,0 GB	Dekomprimiertes Format, gilt nur für 150-Meter-Bänder
DDS4C	Siehe Anmerkung 40,0 GB	Komprimiertes Format, gilt nur für 150-Meter-Bänder
DDS5	36 GB	Dekomprimiertes Format bei Verwendung von DAT 72-Datenträgern
DDS5C	Siehe Anmerkung 72 GB	Komprimiertes Format bei Verwendung von DAT 72-Datenträgern
DDS6	80 GB	Dekomprimiertes Format bei Verwendung von DAT 160-Datenträgern
DDS6C	Siehe Anmerkung 160 GB	Komprimiertes Format bei Verwendung von DAT 160-Datenträgern
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein.		

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die durch diese Einheitenklasse kategorisiert werden. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zur geschätzten Standardkapazität für 4-mm-Bänder siehe Tabelle 1.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

```
AB.CD2.E
```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

  Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

  Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

UPDATE DEVCLASS (Einheitenklasse 8MM aktualisieren)

Verwenden Sie die Einheitenklasse 8MM, wenn Sie 8-mm-Bandeinheiten verwenden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+---------------------------------+------------------------->
   '-LIBRary----Kassettenarchivname-'

>--+----------------------+--+-----------------------+---------->
   '-FORMAT--=--+-DRIVE-+-'  '-ESTCAPacity--=--Größe-'
                +-8200--+
                +-8200C-+
                +-8500--+
                +-8500C-+
                +-8900--+
                +-AIT---+
                +-AITC--+
                +-M2----+
                +-M2C---+
                +-SAIT--+
                +-SAITC-+
                +-VXA2--+
                +-VXA2C-+
                +-VXA3--+
                '-VXA3C-'

>--+--------------------------------------+---------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

>--+-----------------------------+--+-----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

>--+---------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

LIBRary
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die 8-mm-Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können. Weitere Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

  Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

  In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für 8-mm-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformat und geschätzte Standardkapazität für 8-mm-Band

Format **Datenträgertyp**	**Geschätzte Kapazität**	**Beschreibung**
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
8200	2,3 GB	Dekomprimiertes (Standard) Format, verwendet 112-Meter-Standardbandkassetten

Format Datenträgertyp	Geschätzte Kapazität	Beschreibung
8200C	Siehe Anmerkung 3,5 GB 4,6 GB	Komprimiertes Format, verwendet 112-Meter-Standardbandkassetten
8500	Siehe Anmerkung	Laufwerke (Lesen/Schreiben)
15 m	600 MB	Eliant 820 (LS)
15 m	600 MB	Exabyte 8500/8500C (LS)
15 m	600 MB	Exabyte 8505 (LS)
54 m	2,35 GB	Eliant 820 (LS)
54 m	2,35 GB	Exabyte 8500/8500C (LS)
54 m	2,35 GB	Exabyte 8505 (LS)
112 m	5 GB oder 10,0 GB	Eliant 820 (LS)
112 m	5 GB oder 10,0 GB	Exabyte 8500/8500C (LS)
112 m	5 GB oder 10,0 GB	Exabyte 8505 (LS)
160 m XL	7 GB	Eliant 820 (LS)
8500C	Siehe Anmerkung	Laufwerke (Lesen/Schreiben)
15 m	1,2 GB	Eliant 820 (LS)
15 m	1,2 GB	Exabyte 8500/8500C (LS)
15 m	1,2 GB	Exabyte 8505 (LS)
54 m	4,7 GB	Eliant 820 (LS)
54 m	4,7 GB	Exabyte 8500/8500C (LS)
54 m	4,7 GB	Exabyte 8505 (LS)
112 m	5 GB oder 10,0 GB	Eliant 820 (LS)
112 m	5 GB oder 10,0 GB	Exabyte 8500/8500C (LS)
112 m	5 GB oder 10,0 GB	Exabyte 8505 (LS)
160 m XL	7 GB	Eliant 820 (LS)
8900	Siehe Anmerkung	Laufwerk (Lesen/Schreiben)
15 m	–	Mammoth 8900 (L)
54 m	–	Mammoth 8900 (L)
112 m	–	Mammoth 8900 (L)
160 m XL	–	Mammoth 8900 (L)
22 m	2,5 GB	Mammoth 8900 (LS)
125 m	–	Mammoth 8900 (LS mit Upgrade)
170 m	40 GB	Mammoth 8900 (LS)
AIT	Siehe Anmerkung	Laufwerk
SDX1–25C	25 GB	AIT-, AIT2- und AIT3-Laufwerke
SDX1–35C	35 GB	AIT-, AIT2- und AIT3-Laufwerke
SDX2–36C	36 GB	AIT2- und AIT3-Laufwerke
SDX2–50C	50 GB	AIT2- und AIT3-Laufwerke
SDX3–100C	100 GB	AIT3-, AIT4- und AIT5-Laufwerke
SDX3X-150C	150 GB	AIT3-Ex-, AIT4- und AIT5-Laufwerke
SDX4–200C	200 GB	AIT4- und AIT5-Laufwerke
SDX5-400C	400 GB	AIT5-Laufwerk
AITC	Siehe Anmerkung	Laufwerk
SDX1–25C	50 GB	AIT-, AIT2- und AIT3-Laufwerke
SDX1–35C	91 GB	AIT-, AIT2- und AIT3-Laufwerke
SDX2–36C	72 GB	AIT2- und AIT3-Laufwerke
SDX2–50C	130 GB	AIT2- und AIT3-Laufwerke
SDX3–100C	260 GB	AIT3-, AIT4- und AIT5-Laufwerke
SDX3X-150C	390 GB	AIT3-Ex-, AIT4- und AIT5-Laufwerke
SDX4–200C	520 GB	AIT4- und AIT5-Laufwerke
SDX5-400C	1040 GB	AIT5-Laufwerk
M2	Siehe Anmerkung	Laufwerk (Lesen/Schreiben)
75 m	20,0 GB	Mammoth II (LS)
150 m	40,0 GB	Mammoth II (LS)
225 m	60,0 GB	Mammoth II (LS)

Format Datenträgertyp	 Geschätzte Kapazität	Beschreibung
M2C	Siehe Anmerkung	Laufwerk (Lesen/Schreiben)
75 m 150 m 225 m	50,0 GB 100,0 GB 150,0 GB	Mammoth II (LS) Mammoth II (LS) Mammoth II (LS)
SAIT	Siehe Anmerkung 500 GB	Laufwerk (Lesen/Schreiben) Sony SAIT1–500 (LS)
SAITC	Siehe Anmerkung 1300 GB (1,3 TB)	Laufwerk (Lesen/Schreiben) Sony SAIT1–500 (LS)
VXA2 V6 (62 m) V10 (124 m) V17 (170 m)	Siehe Anmerkung 20 GB 40 GB 60 GB	Laufwerk (Lesen/Schreiben) VXA–2
VXA2C V6 (62 m) V10 (124 m) V17 (170 m)	Siehe Anmerkung 40 GB 80 GB 120 GB	Laufwerk (Lesen/Schreiben) VXA–2
VXA3 X6 (62 m) X10 (124 m) X23 (230 m)	Siehe Anmerkung 40 GB 86 GB 160 GB	Laufwerk (Lesen/Schreiben) VXA–3
VXA3C X6 (62 m) X10 (124 m) X23 (230 m)	Siehe Anmerkung 80 GB 172 GB 320 GB	Laufwerk (Lesen/Schreiben) VXA–3
Anmerkung: Die tatsächlichen Kapazitäten können abhängig von den verwendeten Kassetten und Laufwerken variieren. • Für das AITC- und SAITC-Format ist das normale Komprimierungsverhältnis 2,6:1. • Für das M2C-Format ist das normale Komprimierungsverhältnis 2,5:1.		

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zur geschätzten Standardkapazität für 8-mm-Bänder siehe Tabelle 1.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

  Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

  Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

Beispiel: Den Grenzwert für Ladeanforderungen und die Kapazität einer 8-mm-Einheitenklasse aktualisieren

Die Einheitenklasse 8MMTAPE aktualisieren. Den Grenzwert für Ladeanforderungen in 3 und die geschätzte Kapazität in 10 GB ändern.

```
update devclass 8mmtape mountlimit=3 estcapacity=10G
```

Beispiel: Die Ladedauer einer 8-mm-Einheitenklasse aktualisieren

Für die 8-mm-Einheitenklasse 8MMTAPE soll eine Ladedauer von 15 Minuten definiert werden.

```
update devclass 8mmtape mountretention=15
```

UPDATE DEVCLASS (Einheitenklasse CENTERA aktualisieren)

Verwenden Sie die Einheitenklasse CENTERA, wenn Sie EMC Centera-Speichereinheiten verwenden. Der Einheitentyp CENTERA verwendet Dateien als Datenträger zum sequenziellen Speichern von Daten. Er ähnelt der Einheitenklasse FILE.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

                                    (1)
>--HLAddress----IP-Adresse?PEA-Datei--------------------------->

>--+---------------------------+-------------------------------->
   '-MINCAPacity--=----Größe---'

>--+---------------------------+-------------------------------><
   '-MOUNTLimit--=----Anzahl---'
```

Anmerkungen:

1. Für jede Centera-Einheitenklasse müssen Sie eine IP-Adresse angeben. Ein PEA-Dateiname und -Pfad (PEA = Pool Entry Authorization) sind jedoch optional, und die PEA-Dateispezifikation muss auf die IP-Adresse folgen. Verwenden Sie das Zeichen "?", um den PEA-Dateinamen und -Pfad von der IP-Adresse zu trennen.

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

HLAddress
: Gibt eine IP-Adresse für die Centera-Speichereinheit und optional den Namen und Pfad einer PEA-Datei (PEA = Pool Entry Authorization) an. Geben Sie die IP-Adresse in Schreibweise mit Trennzeichen an (beispielsweise 9.10.111.222). Eine Centera-Einheit kann mehrere IP-Adressen haben. Sie müssen jedoch nur eine Adresse als Wert für diesen Parameter angeben.

  AIX-BetriebssystemeBei dem PEA-Dateinamen und -Pfadnamen muss die Groß-/Kleinschreibung beachtet werden.

  Werden Name und Pfad einer PEA-Datei angehängt, stellen Sie sicher, dass die Datei in einem Verzeichnis auf dem System gespeichert wird, auf dem der IBM Spectrum Protect-Server ausgeführt wird. Verwenden Sie das Zeichen "?", um den PEA-Dateinamen und -Pfad von der IP-Adresse oder den IP-Adressen zu trennen. Beispiel: Windows-Betriebssysteme

  ```
  HLADDRESS=9.10.111.222?c:\controlFiles\TSM.PEA
  ```

  AIX-Betriebssysteme

  ```
  HLADDRESS=9.10.111.222?/user/ControlFiles/TSM.PEA
  ```

  Geben Sie nur einen PEA-Dateinamen und Pfad für jede Einheitenklassendefinition an. Geben Sie zwei verschiedene Centera-Einheitenklassen an, die auf dieselbe Centera-Speichereinheit zeigen, und enthalten die Einheitenklassendefinitionen verschiedene PEA-Dateinamen und -Pfade, verwendet der Server die PEA-Datei, die im Einheitenklassenparameter HLADDRESS angegeben ist, der zuerst zum Öffnen der Centera-Speichereinheit verwendet wurde.
  Anmerkung:

  1. Der Server schließt während der Installation keine PEA-Datei ein. Wenn Sie keine PEA-Datei erstellen, verwendet der Server das Centera-Standardprofil, mit dem es Anwendungen erlaubt werden kann, Daten auf einer Centera-Speichereinheit zu lesen, zu schreiben, zu löschen und abzufragen. Um eine genauere Steuerung zu ermöglichen, erstellen Sie eine PEA-Datei mit der Befehlszeilenschnittstelle, die von EMC Centera zur Verfügung gestellt wird. Ausführliche Informationen zur Centera-Authentifizierung und -Berechtigung befinden sich im EMC Centera *Programmer's Guide*.
  2. Sie können den PEA-Dateinamen und -Pfad auch in einer Umgebungsvariablen unter Verwendung der Syntax CENTERA_PEA_LOCATION=*Dateipfad_ Dateiname* angeben. Der mit dieser Umgebungsvariablen angegebene PEA-Dateiname und -Pfad gilt für alle Centera-Cluster. Wird diese Variable verwendet, müssen Sie keinen PEA-Dateinamen und -Pfad mit dem Parameter HLADDRESS angeben.
  3. Die Aktualisierung der Einheitenklasse mit einem neuen oder geänderten PEA-Dateinamen und einer neuen oder geänderten Position kann einen Neustart des Servers erfordern, wenn auf die durch die IP-Adresse identifizierte Centera-Speichereinheit bereits in der aktuellen Instanz des Servers zugegriffen wurde.

MINCAPacity

Gibt die neue Mindestgröße für Centera-Datenträger an, die einem Speicherpool in dieser Einheitenklasse zugeordnet sind. Dieser Wert stellt das Mindestdatenvolumen dar, das auf einem Centera-Datenträger gespeichert wird, bevor der Server den Datenträger als voll kennzeichnet. Centera-Datenträger akzeptieren weiterhin Daten, bis das Mindestdatenvolumen gespeichert wurde. Dieser Parameter ist wahlfrei.

Größe
: Dieser Wert muss als ganze Zahl gefolgt von einem `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte) angegeben werden. Der zulässige Mindestwert ist 1 MB (MINCAPACITY=1M). Der zulässige Maximalwert ist 128 GB (MINCAPacity=128G).

MOUNTLimit
: Gibt die neue maximale Anzahl der Sitzungen an, die auf die Centera-Einheit zugreifen. Dieser Parameter ist wahlfrei. Sie können eine beliebige Zahl von 0 aufwärts angeben; die Summe aller Grenzwerte für Ladeanforderungen für alle Einheitenklassen, die derselben Centera-Einheit zugeordnet sind, darf jedoch die maximale Anzahl der von Centera erlaubten Sitzungen nicht überschreiten.

UPDATE DEVCLASS (Einheitenklasse DLT aktualisieren)

Verwenden Sie die Einheitenklasse DLT, wenn Sie DLT-Bandeinheiten verwenden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+---------------------------------+-------------------------->
   '-LIBRary--=--Kassettenarchivname-'

>--+-------------------------+--+----------------------+------->
   '-FORMAT--=--+-DRIVE----+-'  '-ESTCAPacity--=--Größe-'
                +-DLT1-----+
                +-DLT1C----+
                +-DLT10----+
                +-DLT10C---+
                +-DLT15----+
                +-DLT15C---+
                +-DLT20----+
                +-DLT20C---+
                +-DLT35----+
                +-DLT35C---+
                +-DLT40----+
                +-DLT40C---+
                +-DLT2-----+
                +-DLT2C----+
                +-DLT4-----+
                +-DLT4C----+
                +-SDLT-----+
                +-SDLTC----+
                +-SDLT320--+
                +-SDLT320C-+
                +-SDLT600--+
                +-SDLT600C-+
                +-DLTS4----+
                '-DLTS4C---'

>--+-------------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

>--+---------------------------+--+----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

>--+---------------------------+------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

LIBRary

Gibt den Namen des definierten Kassettenarchivobjekts an, das die DLT-Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für DLT-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformat und geschätzte Standardkapazität für DLT

Format	**Geschätzte Kapazität**	**Beschreibung**
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
DLT1	40,0 GB	Dekomprimiertes Format, verwendet nur CompacTape III- oder CompacTape IV-Kassetten
DLT1C	Siehe 1. 80,0 GB	Komprimiertes Format, verwendet nur CompacTape III- und CompacTape IV-Kassetten
DLT10	10,0 GB	Dekomprimiertes Format, verwendet nur CompacTape III- oder CompacTape IV-Kassetten
DLT10C	Siehe 1. 20,0 GB	Komprimiertes Format, verwendet nur CompacTape III- und CompacTape IV-Kassetten
DLT15	15,0 GB	Dekomprimiertes Format, verwendet nur CompacTape IIIxt- oder CompacTape IV-Kassetten (nicht CompacTape III) Anmerkung: Gültig für DLT2000XT-, DLT4000- und DLT7000-Laufwerke
DLT15C	Siehe 1. 30,0 GB	Komprimiertes Format, verwendet nur CompacTape IIIxt- oder CompacTape IV-Kassetten (nicht CompacTape III) Gültig für DLT2000XT-, DLT4000- und DLT7000-Laufwerke
DLT20	20,0 GB	Dekomprimiertes Format, verwendet nur CompacTape IV-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT20C	Siehe 1. 40,0 GB	Komprimiertes Format, verwendet nur CompacTape IV-Kassetten Gültig für DLT4000-, DLT7000- und DLT8000-Laufwerke
DLT35	35,0 GB	Dekomprimiertes Format, verwendet nur CompacTape IV-Kassetten Gültig für DLT7000- und DLT8000-Laufwerke
DLT35C	Siehe 1. 70,0 GB	Komprimiertes Format, verwendet nur CompacTape IV-Kassetten Gültig für DLT7000- und DLT8000-Laufwerke
DLT40	40,0 GB	Dekomprimiertes Format, verwendet CompacTape IV-Kassetten Gültig für DLT8000-Laufwerk
DLT40C	Siehe 1. 80,0 GB	Komprimiertes Format, verwendet CompacTape IV-Kassetten Gültig für DLT8000-Laufwerk
DLT2	80,0 GB	Dekomprimiertes Format, verwendet Quantum DLT VS1-Banddatenträger
DLT2C	Siehe 1. 160,0 GB	Komprimiertes Format, verwendet Quantum DLT VS1-Banddatenträger
DLT4	160,0 GB	Dekomprimiertes Format, verwendet Quantum DLTtape VS1-Kassetten. Gültig für Quantum DLT-V4-Laufwerk

Format	Geschätzte Kapazität	Beschreibung
DLT4C	Siehe 1. 320,0 GB	Komprimiertes Format, verwendet Quantum DLTtape VS1-Kassetten. Gültig für Quantum DLT-V4-Laufwerk
SDLT Siehe 2.	100,0 GB	Dekomprimiertes Format, verwendet Super DLT Tape 1-Kassetten Gültig für Super DLT-Laufwerk
SDLTC Siehe 2.	Siehe 1. 200,0 GB	Komprimiertes Format, verwendet Super DLT Tape 1-Kassetten Gültig für Super DLT-Laufwerk
SDLT320 Siehe 2.	160,0 GB	Dekomprimiertes Format, verwendet Quantum SDLT I-Datenträger Gültig für Super DLT-Laufwerk
SDLT320C Siehe 2.	Siehe 1. 320,0 GB	Komprimiertes Format, verwendet Quantum SDLT I-Datenträger Gültig für Super DLT-Laufwerk
SDLT600	300,0 GB	Dekomprimiertes Format, verwendet SuperDLTtape-II-Datenträger Gültig für Super DLT-Laufwerk
SDLT600C	Siehe 1. 600,0 GB	Komprimiertes Format, verwendet SuperDLTtape-II-Datenträger Gültig für Super DLT-Laufwerk
DLTS4	800 GB	Dekomprimiertes Format, verwendet Quantum DLT S4-Datenträger. Gültig für ein DLT-S4-Laufwerk
DLTS4C	Siehe 1. 1,6 TB	Komprimiertes Format, verwendet Quantum DLT S4-Datenträger. Gültig für ein DLT-S4-Laufwerk
Anmerkung: 1. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität größer als der aufgeführte Wert sein. 2. IBM Spectrum Protect unterstützt kein Kassettenarchiv, das sowohl Backward Read Compatible (BRC) SDLT- als auch Non-Backward Read Compatible (NBRC) SDLT-Laufwerke enthält.		

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zu geschätzten Kapazitäten siehe Tabelle 1.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

  Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

  Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE aktualisieren)

Verwenden Sie die Einheitenklasse ECARTRIDGE, wenn Sie StorageTek-Laufwerke wie beispielsweise StorageTek T9840 oder T10000 verwenden.

 AIX-Betriebssysteme  Linux-BetriebssystemeWenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server aktualisieren).

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+--------------------------------+-------------------------->
   '-LIBRary--=--Kassettenarchivname-'

>--+------------------------------+------------------------------>
   '-LBProtect--=--+-READWrite-+-'
```

Anmerkungen:

1. Sie können die Laufwerkverschlüsselung nur für Oracle StorageTek T10000B-Laufwerke mit dem Formatwert DRIVE, T10000B oder T10000B-C, für Oracle StorageTek T10000C-Laufwerke mit dem Formatwert DRIVE, T10000C oder T10000C-C und für Oracle StorageTek T10000D-Laufwerke mit dem Formatwert DRIVE, T10000D und T10000D-C verwenden.
2. Sie können nicht WORM=YES in Verbindung mit DRIVEENCRYPTION=ON angeben.

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

LIBRary
Gibt den Namen des definierten Kassettenarchivobjekts mit den ECARTRIDGE-Bandlaufwerken an, die von dieser Einheitenklasse verwendet werden können. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

LBProtect

Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffschutzinformationen, wenn Daten von dem Band gelesen werden.

Die folgenden Werte sind gültig:

READWrite
Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

WRITEOnly
Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für

Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

No

Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur auf Oracle StorageTek T10000C- und Oracle StorageTek T10000D-Laufwerken unterstützt.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

Wichtig: Wird DRIVE für eine Einheitenklasse angegeben, die über inkompatible Einheiten mit sequenziellem Zugriff verfügt, müssen Datenträger in Einheiten geladen werden, die in dem Format lesen oder schreiben können, das beim ersten Laden des Datenträgers eingerichtet wurde. Dies kann zu Verzögerungen führen, wenn die einzige Einheit mit sequenziellem Zugriff, die auf den Datenträger zugreifen kann, bereits im Gebrauch ist.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für ECARTRIDGE-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für ECARTRIDGE-Bänder

Format	**Geschätzte Kapazität**	**Beschreibung**
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
T9840C	40 GB	Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840C-C	80 GB	Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840D	75 GB	Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T9840D-C	150 GB	Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T10000A	500 GB	Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000A-C	1 TB	Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000B	1 TB	Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000B-C	2 TB	Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000C	5 TB	Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000C-C	10 TB	Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D	8 TB	Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D-C	15 TB	Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
Anmerkungen: • Einige Formate verwenden die Datenkomprimierung über Hardware mittels Bandlaufwerk. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität doppelt so groß (oder größer) sein wie der aufgeführte Wert. • T10000A-Laufwerke können nur das T10000A-Format lesen und schreiben. T10000B-Laufwerke können das T10000A-Format lesen, aber nicht schreiben. T10000C-Laufwerke können die T10000A- und T10000B-Formate lesen, aber nicht schreiben. T10000D-Laufwerke können die T10000A-, T10000B- und T10000C-Formate lesen, aber nicht schreiben.		

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zur geschätzten Standardkapazität von Magnetbandkassetten siehe Tabelle 1.

PREFIX
Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention
Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES
Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl
Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)
Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DRIVEEncryption
Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei.
Einschränkung:

1. Sie können die Laufwerkverschlüsselung nur für die folgenden Laufwerke verwenden:
   - Oracle StorageTek T10000B-Laufwerke, die den Formatwert DRIVE, T10000B oder T10000B-C haben
   - Oracle StorageTek T10000C-Laufwerke, die den Formatwert DRIVE, T10000C oder T10000C-C haben
   - Oracle StorageTek T10000D-Laufwerke, die den Formatwert DRIVE, T10000D oder T10000D-C haben
2. Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). (Die Angabe von WORM=YES in Verbindung mit DRIVEENCRYPTION=ON wird nicht unterstützt.)
3. Ist die Verschlüsselung für eine Einheitenklasse aktiviert und ist die Einheitenklasse einem Speicherpool zugeordnet, sollte der Speicherpool nicht einen Arbeitsdatenträgerpool mit anderen Einheitenklassen gemeinsam nutzen, die nicht verschlüsselt werden können. Ist ein Band verschlüsselt und soll das Band in einem Laufwerk verwendet werden, das nicht verschlüsselt werden kann, müssen Sie das Band manuell mit einem neuen Kennsatz versehen, bevor es in diesem Laufwerk verwendet werden kann.

ON
Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern werden nicht verschlüsselt. Beispielsweise werden Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger nicht verschlüsselt.) Wird ON angegeben und ein anderes Verschlüsselungsverfahren aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.

ALLOW
Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

EXTERNAL
Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist. Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert. Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

OFF
Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird ein anderes Verschlüsselungsverfahren aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

UPDATE DEVCLASS (Einheitenklasse FILE aktualisieren)

Verwenden Sie die Einheitenklasse FILE, wenn Dateien im Magnetplattenspeicher als Datenträger verwendet werden, die Daten sequenziell speichern (wie auf Band).

AIX-Betriebssysteme Linux-BetriebssystemeDie Einheitenklasse FILE unterstützt keine Kassettenarchive EXTERNAL.

Windows-BetriebssystemeDie Einheitenklasse FILE unterstützt keine Kassettenarchive EXTERNAL.

AIX-Betriebssysteme Linux-BetriebssystemeWenn Sie eine Einheitenklasse für Einheiten definieren, auf die über einen z/OS Media-Server zugegriffen werden muss, lesen Sie die Informationen in UPDATE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server aktualisieren).

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+-----------------------+--+-----------------------+--------->
   '-MOUNTLimit--=--Anzahl-'  '-MAXCAPacity--=--Größe-'

>--+-----------------------------------+------------------------>
   |               .-,---------------. |
   |               V                 | |
   '-DIRectory--=----Verzeichnisname-+-'

>--+--------------------+-------------------------------------><
   '-SHAREd--=--+-No--+-'
```

```
'-Yes-'
```

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

MOUNTLimit
Gibt die maximale Anzahl von Dateien an, die gleichzeitig für die Ein- und Ausgabe geöffnet sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Wird die Einheitenklasse mit einem Speicheragenten gemeinsam genutzt (durch Angabe des Parameters SHARED=YES), werden Laufwerke definiert oder gelöscht, um eine Übereinstimmung mit dem Wert für MOUNTLIMIT zu erreichen.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

MAXCAPacity
Gibt die maximale Größe einer Datenspeicherdatei an, die durch diese Einheitenklasse kategorisiert wird. Dieser Parameter ist wahlfrei.

Dieser Wert muss als ganze Zahl gefolgt von einem `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte) angegeben werden. Die Mindestgröße ist 1 MB (MAXCAPACITY=1M). Wenn Sie eine Einheitenklasse FILE für Datenbanksicherungsdatenträger definieren, geben Sie einen Wert für MAXCAPACITY an, der für die Größe der Datenbank angemessen ist und der die Anzahl der Datenbankdatenträger minimiert.

MAXCAPACITY=5G gibt beispielsweise an, dass die maximale Kapazität eines Datenträgers in dieser Einheitenklasse 5 Gigabyte beträgt. Der angegebene Wert muss kleiner-gleich der maximal unterstützten Größe einer Datei im Zieldateisystem sein.

AIX-BetriebssystemeLinux-BetriebssystemeKeinen Wert für MAXCAPACITY größer als 640 MB definieren, wenn diese Datei für die REMOVABLEFILE CD-Unterstützung bestimmt ist. Ein Wert, der kleiner als der verwendbare Speicherbereich (650 MB) einer CD ist, ermöglicht eine Eins-zu-Eins-Übereinstimmung zwischen Dateien aus der Einheitenklasse FILE und Kopien, die sich auf CD befinden.

DIRectory
Gibt die Verzeichnisposition(en) der in dieser Einheitenklasse verwendeten Dateien an. Schließen Sie die gesamte Liste der Verzeichnisse in Anführungszeichen ein und verwenden Sie Kommas, um einzelne Verzeichnisnamen voneinander zu trennen. Sonderzeichen (z. B. Leerzeichen) sind in Verzeichnisnamen zulässig. Die Verzeichnisliste "abc def,xyz" enthält beispielsweise zwei Verzeichnisse: abc def und xyz. Dieser Parameter ist wahlfrei.

Durch die Angabe eines oder mehrerer Verzeichnisnamen werden die Positionen angegeben, an denen der Server die Dateien speichert, die Speicherdatenträger für diese Einheitenklasse darstellen.

AIX-BetriebssystemeLinux-BetriebssystemeBei der Verarbeitung des Befehls erweitert der Server den oder die angegebenen Verzeichnisnamen in die vollständig qualifizierte Form (beginnend beim Stammverzeichnis).

Wichtig: Wenn Sie Speicheragenten für den gemeinsamen Zugriff auf FILE-Datenträger verwenden, müssen Sie mit dem Befehl DEFINE PATH einen Pfad für jeden Speicheragenten definieren. Die Pfaddefinition enthält die Verzeichnisnamen, die vom Speicheragenten für den Zugriff auf jedes Verzeichnis verwendet werden.

Wenn der Server später einen Arbeitsdatenträger zuordnen muss, erstellt er eine neue Datei in einem dieser Verzeichnisse. (Der Server kann ein beliebiges der Verzeichnisse auswählen, in dem neue Arbeitsdatenträger erstellt werden sollen.) Bei Arbeitsdatenträgern, die zum Speichern von Clientdaten verwendet werden, hat die durch den Server erstellte Datei die Dateinamenerweiterung .bfs. Bei Arbeitsdatenträgern, auf denen Exportdaten gespeichert werden, wird die Dateinamenerweiterung .exp verwendet.

AIX-BetriebssystemeLinux-BetriebssystemeWenn Sie beispielsweise eine Einheitenklasse mit dem Verzeichnis tsmstor definieren und der Server einen Arbeitsdatenträger in dieser Einheitenklasse benötigt, um Exportdaten zu speichern, könnte der Name der Datei, die der Server erstellt, /tsmstor/00566497.exp lauten.

Windows-BetriebssystemeWenn Sie beispielsweise eine Einheitenklasse mit dem Verzeichnis c:\server definieren und der Server einen Arbeitsdatenträger in dieser Einheitenklasse benötigt, um Exportdaten zu speichern, könnte der Name der Datei, die der Server erstellt, c:\server\00566497.exp lauten.

Tipp: Geben Sie mehrere Verzeichnisse für eine Einheitenklasse an, stellen Sie sicher, dass die Verzeichnisse separaten Dateisystemen zugeordnet sind. Bei Speicherbereichsauslöserfunktionen und Berechnungen des Speicherbereichs im Speicherpool wird der Speicherbereich berücksichtigt, der in jedem Verzeichnis verbleibt. Wenn Sie mehrere Verzeichnisse für eine Einheitenklasse angeben und sich die Verzeichnisse in demselben Dateisystem befinden, berechnet der Server den Speicherbereich durch Hinzufügen von Werten, die den Speicherbereich darstellen, der in jedem Verzeichnis verbleibt. Diese Speicherbereichsberechnungen sind ungenau. Anstatt einen Speicherpool mit ausreichend Speicherbereich für eine Operation auszuwählen, kann der Server den falschen Speicherpool auswählen und frühzeitig über keinen Speicherbereich mehr verfügen. Bei Speicherbereichsauslösern kann eine ungenaue Berechnung zu einem Fehler bei der Erweiterung des Speicherbereichs führen, der in einem Speicherpool verfügbar ist. Ein Fehler bei der Erweiterung des Speicherbereichs in einem Speicherpool ist eine der Bedingungen, die zur Inaktivierung eines Auslösers führen kann. Wird ein Auslöser inaktiviert, da der Speicherbereich in einem Speicherpool nicht erweitert wurde, können Sie den Auslöser erneut aktivieren, indem Sie den

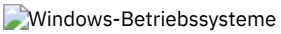
folgenden Befehl ausgeben: `update spacetrigger stg`. Es sind keine weiteren Änderungen an dem Speicherbereichsauslöser erforderlich.
Einschränkung: Soll eine Verzeichnisliste geändert werden, müssen Sie die vollständige Liste ersetzen.

SHAREd
: Gibt an, dass diese Einheitenklasse FILE von dem Server und von einem oder mehreren Speicheragenten gemeinsam genutzt wird. Zur Vorbereitung der gemeinsamen Nutzung wird automatisch ein Kassettenarchiv zusammen mit einer Anzahl von Laufwerken definiert, die dem Wert für MOUNTLIMIT entspricht, der der Einheitenklasse zugeordnet ist. Sind das Kassettenarchiv und die Laufwerke vorhanden und wird der Wert für MOUNTLIMIT geändert, können entweder Laufwerke erstellt werden, um einen neuen höheren Wert für MOUNTLIMIT zu erreichen, oder Laufwerke gelöscht werden, um einen neuen niedrigeren Wert zu erreichen.

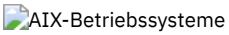
Speicheragenten, die FILE-Datenträger verwenden

Sie müssen sicherstellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können. Für den Zugriff auf FILE-Datenträger ersetzen Speicheragenten Namen aus der Verzeichnisliste in der Einheitenklassendefinition durch die Namen in der Verzeichnisliste für die zugeordnete Pfaddefinition. Der folgende Abschnitt verdeutlicht die Bedeutung übereinstimmender Einheitenklassen und Pfade, um sicherzustellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können.

Beispiel: Sie möchten folgende drei Verzeichnisse für ein FILE-Kassettenarchiv verwenden:


Windows-Betriebssysteme

- c:\server
- d:\server
- e:\server

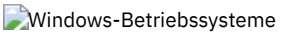

AIX-Betriebssysteme

- /usr/tivoli1
- /usr/tivoli2
- /usr/tivoli3

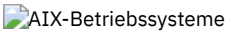

Linux-Betriebssysteme

- /opt/tivoli1
- /opt/tivoli2
- /opt/tivoli3

1. Sie verwenden den folgenden Befehl, um ein FILE-Kassettenarchiv mit dem Namen CLASSA mit einem Laufwerk mit dem Namen CLASSA1 auf SERVER1 zu definieren:

   
   Windows-Betriebssysteme

   ```
   define devclass classa devtype=file
   directory="c:\server,d:\server,e:\server"
   shared=yes mountlimit=1
   ```

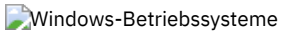
   
   AIX-Betriebssysteme

   ```
   define devclass classa devtype=file
   directory="/usr/tivoli1,/usr/tivoli2,/usr/tivoli3"
   shared=yes mountlimit=1
   ```

   
   Linux-Betriebssysteme

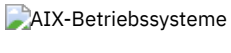
   ```
   define devclass classa devtype=file
   directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
   shared=yes mountlimit=1
   ```

2. Sie wollen, dass der Speicheragent STA1 das FILE-Kassettenarchiv verwenden kann. Daher definieren Sie folgenden Pfad für Speicheragent STA1:

   - 
     Windows-Betriebssysteme

     ```
     define path server1 sta1 srctype=server desttype=drive device=file
     directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
     \\192.168.1.10\e\server" library=classa
     ```

     In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen c:\server durch den Verzeichnisnamen \\192.168.1.10\c\server, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis c:\server auf dem Server befinden.

   - 
     AIX-Betriebssysteme

     ```
     define path server1 sta1 srctype=server desttype=drive device=file
     directory="/usr/ibm1,/usr/ibm2,/usr/ibm3" library=classa
     ```

In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen /usr/tivoli1 durch den Verzeichnisnamen /usr/ibm1, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis /usr/tivoli1 auf dem Server befinden.

- Linux-Betriebssysteme

```
define path server1 sta1 srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```

In diesem Szenario ersetzt der Speicheragent STA1 den Verzeichnisnamen /opt/tivoli1 durch den Verzeichnisnamen /opt/ibm1/, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis /opt/tivoli1 auf dem Server befinden.

Die Ergebnisse sind wie folgt:

- Windows-BetriebssystemeFILE-Datenträger c:\server\file1.dsm wird durch SERVER1 erstellt. Wenn Sie das erste Verzeichnis für die Einheitenklassen später mit folgendem Befehl ändern:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

kann SERVER1 weiterhin auf FILE-Datenträger c:\server\file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

- AIX-BetriebssystemeWird der FILE-Datenträger /usr/tivoli1/file1.dsm auf SERVER1 erstellt und wird der Befehl

```
update devclass classa directory="/usr/otherdir,/usr/tivoli2,
/usr/tivoli3"
```

ausgegeben, kann SERVER1 weiterhin auf FILE-Datenträger /usr/tivoli1/file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

- Linux-BetriebssystemeWird der FILE-Datenträger /opt/tivoli1/file1.dsm auf SERVER1 erstellt und wird der Befehl

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,
/opt/tivoli3"
```

ausgegeben, kann SERVER1 weiterhin auf FILE-Datenträger /opt/tivoli1/file1.dsm zugreifen, der Speicheragent STA1 jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

Beispiel: Eine Einheitenklasse FILE für die gemeinsame Nutzung aktualisieren

Eine FILE-Einheitenklasse (mit dem Namen PLAINFILES) für die gemeinsame Benutzung mit einem IBM Spectrum Protect-Speicheragenten vorbereiten.

```
update  devclass plainfiles shared=yes
```

Beispiel: Die Kapazität einer Einheitenklasse FILE aktualisieren

Für die Einheitenklasse FILE mit dem Namen STORFILES soll eine maximale Kapazität von 25 MB definiert werden.

```
update devclass storfiles maxcap=25m
```

AIX-Betriebssysteme

Beispiel: Einer Einheitenklasse FILE ein Verzeichnis hinzufügen

Die FILE-Einheitenklasse CLASSA aktualisieren, indem ein Verzeichnis, /usr/otherdir, zur Verzeichnisliste hinzugefügt wird. Die Verzeichnisse /opt/tivoli2 und /opt/tivoli3 wurden angegeben, als die Einheitenklasse zuerst definiert wurde.

```
update devclass classa
 directory="/opt/tivoli2,/opt/tivoli3,/usr/otherdir"
```

Linux-Betriebssysteme

Beispiel: Einer Einheitenklasse FILE ein Verzeichnis hinzufügen

Die FILE-Einheitenklasse CLASSA aktualisieren, indem ein Verzeichnis, /usr/otherdir, zur Verzeichnisliste hinzugefügt wird. Die Verzeichnisse /usr/tivoli2 und /usr/tivoli3 wurden angegeben, als die Einheitenklasse zuerst definiert wurde.

```
update devclass classa
directory="/usr/tivoli2,/usr/tivoli3,/usr/otherdir"
```

 Windows-Betriebssysteme

Beispiel: Einer Einheitenklasse FILE ein Verzeichnis hinzufügen

Die FILE-Einheitenklasse CLASSA aktualisieren, indem ein Verzeichnis, c:\otherdir, zur Verzeichnisliste hinzugefügt wird. Die Verzeichnisse d:\server und e:\server wurden angegeben, als die Einheitenklasse zuerst definiert wurde.

```
update devclass classa
 directory="d:\server,e:\server,c:\otherdir"
```

 AIX-Betriebssysteme  Windows-Betriebssysteme

UPDATE DEVCLASS (Einheitenklasse GENERICTAPE aktualisieren)

Verwenden Sie die Einheitenklasse GENERICTAPE für Bandlaufwerke, die von Einheitentreibern des Betriebssystems unterstützt werden.

Bei Verwendung dieses Einheitentyps erkennt der Server weder den Einheitentyp noch das Kassettenaufzeichnungsformat. Wenn ein E/A-Fehler auftritt, sind die Fehlerinformationen weniger ausführlich im Vergleich zu den Fehlerinformationen für einen bestimmten Einheitentyp (z. B. 8MM), da der Server den Einheitentyp nicht erkennt. Bei der Definition von Einheiten für den Server dürfen keine verschiedenen Einheitentypen in demselben Einheitentyp gemischt werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+-----------------------------------+-------------------------->
   '-LIBRary----=--Kassettenarchivname-'

>--+-----------------------+--+----------------------------+---->
   '-ESTCAPacity--=--Größe-'  '-MOUNTRetention--=--Minuten-'

>--+------------------------+--+-----------------------------+---><
   '-MOUNTWait--=--Minuten-'  '-MOUNTLimit------+-DRIVES-+-'
                                               +-Anzahl-+
                                               '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

LIBRary

Gibt den Namen des definierten Kassettenarchivobjekts an, das die Bandlaufwerke enthält, die von dieser Einheitenklasse verwendet werden können.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Geben Sie eine dem verwendeten Bandlaufwerk entsprechende Kapazität an.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

MOUNTRetention
Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES
Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl
Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)
Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

UPDATE DEVCLASS (Einheitenklasse LTO aktualisieren)

Verwenden Sie die Einheitenklasse LTO, wenn Sie LTO-Bandeinheiten verwenden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+---------------------------------+-------------------------->
   '-LIBRary---=--Kassettenarchivname-'

>--+-----------------------------+------------------------------>
   '-LBProtect--=--+-READWrite-+-'
                   +-WRITEOnly-+
                   '-No--------'

>--+--------------------------+--+----------------------+------>
   '-FORMAT--=--+-DRIVE-----+-'  '-ESTCAPacity--=--Größe-'
                +-ULTRIUM---+
                +-ULTRIUMC--+
                +-ULTRIUM2--+
```

```
                +-ULTRIUM2C-+
                +-ULTRIUM3--+
                +-ULTRIUM3C-+
                +-ULTRIUM4--+
                +-ULTRIUM4C-+
                +-ULTRIUM5--+
                +-ULTRIUM5C-+
                +-ULTRIUM6--+
                '-ULTRIUM6C-'

>--+--------------------------------------+--------------------->
   '-PREFIX--=--+-ADSM------------------+-'
                '-Banddatenträgerpräfix-'

>--+----------------------------+--+-----------------------+---->
   '-MOUNTRetention---=--Minuten-'  '-MOUNTWait--=--Minuten-'

>--+--------------------------+-------------------------------->
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'

>--+---------------------------------------------+------------><
   |  (1)   (2)                                  |
   '-------------DRIVEEncryption--=--+-ON-------+-'
                                     +-ALLOW----+
                                     +-EXTERNAL-+
                                     '-OFF------'
```

Anmerkungen:

1. Sie können nicht DRIVEENCRYPTION=ON angeben, wenn Ihre Laufwerke WORM-Datenträger verwenden (WORM - Write Once Read Many).
2. Laufwerkverschlüsselung wird nur für Ultrium 4-, Ultrium 5- und Ultrium 6-Laufwerke und -Datenträger unterstützt.

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten LTO-Bandlaufwerke enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

LBProtect

: Gibt an, ob der Schutz logischer Blöcke verwendet wird, um die Integrität von Daten sicherzustellen, die auf Band gespeichert sind. Wenn LBPROTECT auf READWRITE oder WRITEONLY gesetzt ist, verwendet der Server dieses Feature des Bandlaufwerks für den Schutz logischer Blöcke und generiert CRC-Zugriffschutzinformationen für jeden Datenblock, der auf Band geschrieben wird. Der Server überprüft auch die CRC-Zugriffschutzinformationen, wenn Daten von dem Band gelesen werden.

  Die folgenden Werte sind gültig:

  READWrite
  : Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect und dem Bandlaufwerk erforderlich ist, um CRC-Werte zu berechnen und zu vergleichen. Der Wert READWRITE hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

    Wird der Parameter LBPROTECT auf READWRITE gesetzt, müssen Sie nicht den Parameter CRCDATA in einer Speicherpooldefinition angeben, da der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust bereitstellt.

  WRITEOnly
  : Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk nur für Schreiboperationen aktiviert ist. Daten werden mit CRC-Informationen in jedem Block gespeichert. Für Leseoperationen überprüfen der Server und das Bandlaufwerk nicht die CRC-Informationen. Dieser Modus hat Auswirkungen auf die Leistung, da zusätzliche Prozessorbelegung für IBM Spectrum Protect zum Generieren der CRC-Informationen und für das Bandlaufwerk zum Berechnen und Vergleichen der CRC-Werte für Schreiboperationen erforderlich ist. Der Wert WRITEONLY hat keine Auswirkungen auf Sicherungsgruppen und Daten, die mit dem Befehl BACKUP DB generiert werden.

  No
  : Gibt an, dass der Schutz logischer Blöcke auf dem Server und dem Bandlaufwerk für Lese- und Schreiboperationen nicht aktiviert ist. Der Server aktiviert jedoch den Schutz logischer Blöcke bei Schreiboperationen für einen sich füllenden Datenträger, der bereits über Daten mit dem Schutz logischer Blöcke verfügt.

Einschränkung: Der Schutz logischer Blöcke wird nur auf IBM® LTO5-Laufwerken und unterstützten LTO6-Laufwerken unterstützt.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet.

Gehen Sie wie folgt vor, wenn alle Laufwerke von Ultrium-Einheiten auf Ultrium 2-Einheiten migriert werden:

- Löschen Sie alle vorhandenen Ultrium-Laufwerkdefinitionen und die Pfade, die ihnen zugeordnet sind.
- Definieren Sie die neuen Ultrium 2-Laufwerke und Pfade.

Sollen verschiedene Generationen von LTO-Datenträgern und -laufwerken gemischt werden, sind die folgenden Einschränkungen zu beachten.

Tabelle 1. Lese-/Schreibfunktionalität verschiedener Generationen von LTO-Laufwerken

Laufwerke	Datenträger der Generation 1	Datenträger der Generation 2	Datenträger der Generation 3	Datenträger der Generation 4	Datenträger der Generation 5	Datenträger der Generation 6
Generation 1	Lesen und schreiben	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 2	Lesen und schreiben	Lesen und schreiben	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 3 [1]	Nur lesen	Lesen und schreiben	Lesen und schreiben	nicht zutreffend	nicht zutreffend	nicht zutreffend
Generation 4 [2]	nicht zutreffend	Nur lesen	Lesen und schreiben	Lesen und schreiben	nicht zutreffend	nicht zutreffend
Generation 5 [3]	nicht zutreffend	nicht zutreffend	Nur lesen	Lesen und schreiben	Lesen und schreiben	nicht zutreffend
Generation 6 [4]	nicht zutreffend	nicht zutreffend	nicht zutreffend	Nur lesen	Lesen und schreiben	Lesen und schreiben

[1] In einem Kassettenarchiv mit einem Laufwerk der Generation 3 müssen alle Arbeitsdatenträger der Generation 1 entnommen werden und alle Speicherpooldatenträger der Generation 1 müssen in "schreibgeschützt" aktualisiert werden.

[2] In einem Kassettenarchiv mit einem Laufwerk der Generation 4 müssen alle Arbeitsdatenträger der Generation 2 entnommen werden und alle Speicherpooldatenträger der Generation 2 müssen in "schreibgeschützt" aktualisiert werden.

[3] In einem Kassettenarchiv mit einem Laufwerk der Generation 5 müssen alle Arbeitsdatenträger der Generation 3 entnommen werden und alle Speicherpooldatenträger der Generation 3 müssen in "schreibgeschützt" aktualisiert werden.

[4] In einem Kassettenarchiv mit einem Laufwerk der Generation 6 müssen alle Arbeitsdatenträger der Generation 4 entnommen werden und alle Speicherpooldatenträger der Generation 4 müssen in "schreibgeschützt" aktualisiert werden.

In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für LTO-Einheiten aufgelistet:

Tabelle 2. Aufzeichnungsformat und geschätzte Standardkapazität für LTO

Format	Geschätzte Kapazität	Beschreibung
DRIVE	-	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
ULTRIUM	100 GB	Dekomprimiertes Format, verwendet Ultrium-Kassetten
ULTRIUMC	Siehe Anmerkung 200 GB	Komprimiertes Format, verwendet Ultrium-Kassetten
ULTRIUM2	200 GB	Dekomprimiertes (Standard) Format, verwendet Ultrium 2-Kassetten
ULTRIUM2C	Siehe Anmerkung 400 GB	Komprimiertes Format, verwendet Ultrium 2-Kassetten
ULTRIUM3	400 GB	Dekomprimiertes (Standard) Format, verwendet Ultrium 3-Kassetten

Format	Geschätzte Kapazität	Beschreibung
ULTRIUM3C	Siehe Anmerkung 800 GB	Komprimiertes Format, verwendet Ultrium 3-Kassetten
ULTRIUM4	800 GB	Dekomprimiertes (Standard) Format, verwendet Ultrium 4-Kassetten
ULTRIUM4C	Siehe Anmerkung 1,6 TB	Komprimiertes Format, verwendet Ultrium 4-Kassetten
ULTRIUM5	1,5 TB	Dekomprimiertes (Standard-)Format, verwendet Ultrium 5-Kassetten
ULTRIUM5C	Siehe Anmerkung 3,0 TB	Komprimiertes Format, verwendet Ultrium 5-Kassetten
ULTRIUM6	2,5 TB	Dekomprimiertes (Standard) Format, verwendet Ultrium 6-Kassetten
ULTRIUM6C	Siehe Anmerkung 6,25 TB	Komprimiertes Format, verwendet Ultrium 6-Kassetten
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann die tatsächliche Kapazität abhängig von der Effektivität der Komprimierung größer als der aufgelistete Wert sein.		

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die durch diese Einheitenklasse kategorisiert werden. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zu geschätzten Kapazitäten siehe Tabelle 2.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Wird jedoch bei Kassettenarchivtyp EXTERNAL für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen

möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

DRIVEEncryption
: Gibt an, ob die Laufwerkverschlüsselung zulässig ist. Dieser Parameter ist wahlfrei. Laufwerkverschlüsselung wird nur für Ultrium 4-, Ultrium 5- und Ultrium 6-Laufwerke und -Datenträger unterstützt.
  Einschränkung: Ist die Verschlüsselung für eine Einheitenklasse aktiviert und ist die Einheitenklasse einem Speicherpool zugeordnet, sollte der Speicherpool nicht einen Arbeitsdatenträgerpool mit anderen Einheitenklassen gemeinsam nutzen, die nicht verschlüsselt werden können. Ist ein Band verschlüsselt und soll das Band in einem Laufwerk verwendet werden, das nicht verschlüsselt werden kann, müssen Sie das Band manuell mit einem neuen Kennsatz versehen, bevor es in diesem Laufwerk verwendet werden kann.

  ON
  : Gibt an, dass IBM Spectrum Protect der Schlüsselmanager für die Laufwerkverschlüsselung ist und die Laufwerkverschlüsselung für leere Speicherpooldatenträger nur erlaubt, wenn das Anwendungsverfahren aktiviert ist. (Andere Typen von Datenträgern werden nicht verschlüsselt. Beispielsweise werden Sicherungsgruppen, Exportdatenträger und Datenbanksicherungsdatenträger nicht verschlüsselt.) Wird ON angegeben und ein anderes Verschlüsselungsverfahren aktiviert, ist die Laufwerkverschlüsselung nicht zulässig, und Sicherungsoperationen schlagen fehl.
    Anmerkung: Sie können nicht IBM Spectrum Protect als Schlüsselmanager für die Laufwerkverschlüsselung von WORM-Datenträgern angeben (WORM - Write Once Read Many). (Wenn Sie WORM-Datenträger verwenden, können Sie nicht DRIVEENCRYPTION=ON angeben.)

  ALLOW
  : Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Die Laufwerkverschlüsselung für leere Datenträger ist jedoch zulässig, wenn ein anderes Verschlüsselungsverfahren aktiviert ist.

  EXTERNAL
  : Gibt an, dass IBM Spectrum Protect die Schlüssel für die Laufwerkverschlüsselung nicht verwaltet. Verwenden Sie diese Einstellung mit einer Verschlüsselungsmethodik, die von einem anderen Anbieter zur Verfügung gestellt wird und die mit dem Anwendungsverfahren der Verschlüsselung verwendet wird, das für das Laufwerk aktiviert ist. Geben Sie EXTERNAL an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect nicht inaktiviert. Geben Sie dagegen ALLOW an, und stellt IBM Spectrum Protect fest, dass das Anwendungsverfahren der Verschlüsselung aktiviert ist, wird die Verschlüsselung von IBM Spectrum Protect inaktiviert.

  OFF
  : Gibt an, dass die Laufwerkverschlüsselung nicht zulässig ist. Wird ein anderes Verschlüsselungsverfahren aktiviert, schlagen Sicherungen fehl. Wird das Anwendungsverfahren aktiviert, inaktiviert IBM Spectrum Protect die Verschlüsselung, und die Ausführung von Sicherungen wird versucht.

Beispiel: Den Grenzwert für Ladeanforderungen für eine Einheitenklasse LTO aktualisieren

Die Einheitenklasse LTOTAPE aktualisieren. Den Grenzwert für Ladeanforderungen in 2 ändern.

```
update devclass ltotape mountlimit=2
```

UPDATE DEVCLASS (Einheitenklasse NAS aktualisieren)

Verwenden Sie die Einheitenklasse NAS (Network Attached Storage), wenn Sie NDMP-Operationen zum Sichern von NAS-Dateiservern verwenden (NDMP - Network Data Management Protocol). Die Einheitenklasse ist für Laufwerke bestimmt, die der NAS-Dateiserver für Sicherungen unterstützt.

 AIX-Betriebssysteme  Linux-BetriebssystemeDie Einheitenklasse NAS unterstützt keine Kassettenarchive EXTERNAL.

 Windows-BetriebssystemeDie Einheitenklasse NAS unterstützt keine Kassettenarchive EXTERNAL.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+---------------------------------+-------------------------->
   '-LIBRary-----Kassettenarchivname-'

>--+-----------------------+--+-----------------------+---------->
   '-MOUNTRetention-----0-'  '-MOUNTWait---Minuten-'

>--+---------------------------+--+-----------------------+----->
   '-MOUNTLimit---+-DRIVES-+-'  '-ESTCAPacity---Größe-'
                  +-Anzahl-+
                  '-0------'

>--+---------------------------------+------------------------><
   '-PREFIX---Banddatenträgerpräfix-'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten SCSI-Bandlaufwerke enthält. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

MOUNTRetention=0
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Null (0) ist der einzige unterstützte Wert für Einheitenklassen mit DEVType=NAS.

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

PREFIX

Gibt das übergeordnete Qualifikationsmerkmal des Dateinamens an, das der Server in die Kennsätze der Datenträger mit sequenziellem Zugriff schreibt. Für jeden Datenträger mit sequenziellem Zugriff, der dieser Einheitenklasse zugeordnet ist, verwendet der Server dieses Präfix, um den Dateinamen zu erstellen. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für Banddatenträger unter Verwendung des Standardpräfixes ist ADSM.BFS.

Beispiel: Die geschätzte Kapazität für eine Einheitenklasse NAS aktualisieren

Die Einheitenklasse NASTAPE aktualisieren. Die geschätzte Kapazität in 200 GB ändern.

```
update devclass nastape library=naslib estcapacity=200G
```

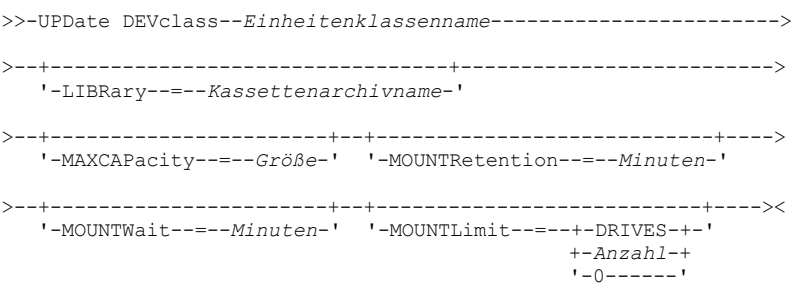
UPDATE DEVCLASS (Einheitenklasse REMOVABLEFILE aktualisieren)

Verwenden Sie die Einheitenklasse REMOVABLEFILE für Einheiten für austauschbare Datenträger, die als lokale, entfernbare Dateisysteme angeschlossen sind.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax



Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

LIBRary

Gibt den Namen des definierten Kassettenarchivobjekts an, das die von dieser Einheitenklasse verwendeten Laufwerke für austauschbare Datenträger enthält. Dieser Parameter ist wahlfrei. Informationen zum Definieren eines Kassettenarchivobjekts befinden sich unter dem Befehl DEFINE LIBRARY.

MAXCAPacity

Gibt die maximale Größe der Datenträger an, die für einen Speicherpool definiert sind, der durch diese Einheitenklasse kategorisiert wird. Dieser Parameter ist wahlfrei.

 AIX-Betriebssysteme  Windows-BetriebssystemeDa der Server nur eine Datei pro physischen austauschbaren Datenträger öffnet, ist die Kapazität so zu wählen, dass diese eine Datei die Datenträgerkapazität vollständig nutzt.

Dieser Wert muss als ganze Zahl gefolgt von einem `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte) angegeben werden.

MAXCAPACITY=5M gibt beispielsweise an, dass die maximale Kapazität eines Datenträgers in dieser Einheitenklasse 5 MB beträgt. Der zulässige Mindestwert ist 1 MB (d. h. MAXCAPACITY=1M).

MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait

Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit

Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Gültige Werte:

DRIVES

Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

Anzahl

Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

0 (Null)

Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

UPDATE DEVCLASS (Einheitenklasse SERVER aktualisieren)

Verwenden Sie die Einheitenklasse SERVER, um Speicherdatenträger oder Dateien zu verwenden, die auf einem anderen IBM Spectrum Protect-Server archiviert sind.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDdate DEVclass--Einheitenklassenname----------------------->

>--+---------------------------+--+----------------------+----->
   '-SERVERName--=--Servername-'  '-MAXCAPacity--=--Größe-'

>--+-----------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

>--+-----------------------------+----------------------------->
   '-RETRYPeriod--=----Minuten---'

>--+-------------------------------+--------------------------->
   '-RETRYInterval--=----Sekunden---'

>--+---------------------------+------------------------------->
   '-MOUNTRetention--=--Minuten-'

>--+---------------------------+-------------------------------><
   '-MOUNTLimit--=--+-Anzahl-+-'
                    '-1------'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

SERVERName
: Gibt den Namen des Servers an.Der Parameter SERVERNAME muss einem definierten Server entsprechen.
Anmerkung: Wird der Servername (SERVERNAME) eines vorhandenen Servers durch einen neuen Namen ersetzt, kann auf die Daten der Datenträger unter dem alten Servernamen (SERVERNAME) mit dieser Einheitenklasse nicht mehr zugegriffen werden.

MAXCAPacity
: Gibt die maximale Größe für Objekte bei der Erstellung auf dem Zielserver an. Dieser Parameter ist wahlfrei.

  Dieser Wert muss als ganze Zahl gefolgt von einem `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte) angegeben werden. Der zulässige Mindestwert ist 1 MB (MAXCAPACITY=1M).

PREFIX
: Gibt den Anfangsabschnitt des Archivierungsdateinamens der höheren Ebene auf dem Zielserver an. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

  Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

  Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

  - Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

    ```
    AB.CD2.E
    ```

  - Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
  - Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

  Ein Beispiel eines Archivierungsdateinamens der höheren Ebene, der das Standardpräfix verwendet, ist ADSM.volume1.

RETRYPeriod
: Gibt den Wiederholungszeitraum in Minuten an. Der Wiederholungszeitraum ist das Intervall, während dem der Server versucht, eine Verbindung zu einem Zielserver herzustellen, falls ein Übertragungsfehler vermutet wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

RETRYInterval
: Gibt das Wiederholungsintervall in Sekunden an. Das Wiederholungsintervall gibt an, wie oft Wiederholungen in einer bestimmten Zeitperiode erfolgen. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 1 bis 9999 angeben.

MOUNTRetention
: Gibt die Anzahl Minuten an, die eine inaktive Verbindung mit dem Zielserver aufrechterhalten werden soll, bevor die Verbindung geschlossen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.
Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTLimit

Gibt die maximal zulässige Anzahl gleichzeitig stattfindender Sitzungen zwischen dem Quellenserver und dem Zielserver an. Alle Versuche, auf mehr Sitzungen zuzugreifen als mit dem Grenzwert für Ladeanforderung angegeben sind, haben das Warten des Anforderers zur Folge. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 1 bis 4096 angeben.
Gültige Werte:

Zahl
: Gibt die maximal zulässige Anzahl gleichzeitig stattfindender Sitzungen zwischen dem Quellenserver und dem Zielserver an.

1
: Gibt die Anzahl der gleichzeitig stattfindenden Sitzungen zwischen dem Quellenserver und dem Zielserver an.

UPDATE DEVCLASS (Einheitenklasse VOLSAFE aktualisieren)

Verwenden Sie den Einheitentyp VOLSAFE, um mit StorageTek VolSafe-Datenträgern und -Laufwerken zu arbeiten. Diese Technologie verwendet Datenträger, die nicht überschrieben werden können. Verwenden Sie diese Datenträger daher nicht für kurzfristige Sicherungen von Clientdateien, der Serverdatenbank oder von Exportbändern.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+---------------------------------+-------------------------->
   '-LIBRary--=--Kassettenarchivname-'

>--+--------------------------+--+----------------------+------>
   '-FORMAT--=--+-DRIVE-----+-'  '-ESTCAPacity--=--Größe-'
                +-9840------+
                +-9840-C----+
                +-T9840C----+
                +-T9840C-C--+
                +-T9840D----+
                +-T9840D-C--+
                +-T10000A---+
                +-T10000A-C-+
                +-T10000B---+
                +-T10000B-C-+
                +-T10000C---+
                +-T10000C-C-+
                +-T10000D---+
                '-T10000D-C-'

>--+-------------------------------------+--------------------->
   '-PREFIX--=--+-ADSM-----------------+-'
                '-Banddatenträgerpräfix-'

>--+----------------------------+--+----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

>--+---------------------------+-------------------------------><
   '-MOUNTLimit--=--+-DRIVES-+-'
                    +-Anzahl-+
                    '-0------'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary
: Gibt den Namen des definierten Kassettenarchivobjekts an, das die VolSafe-Laufwerke enthält, die von dieser Einheitenklasse verwendet werden können. Sind Laufwerke in einem Kassettenarchiv VolSafe-aktiviert, müssen alle Laufwerke in dem Kassettenarchiv VolSafe-aktiviert sein. Für weitere Informationen zum Einheitentyp VolSafe siehe DEFINE DEVCLASS (Einheitenklasse VOLSAFE definieren).

FORMAT
: Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.
Achtung: Wird DRIVE für eine Einheitenklasse angegeben, die über inkompatible Einheiten mit sequenziellem Zugriff verfügt, müssen Datenträger in Einheiten geladen werden, die in dem Format lesen oder schreiben können, das beim ersten Laden des Datenträgers

eingerichtet wurde. Dies kann zu Verzögerungen führen, wenn die einzige Einheit mit sequenziellem Zugriff, die auf den Datenträger zugreifen kann, bereits im Gebrauch ist.
In der folgenden Tabelle sind die Aufzeichnungsformate und die geschätzten Kapazitäten für VolSafe-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate und geschätzte Standardkapazitäten für VOLSAFE-Bänder

Format	Geschätzte Kapazität	Beschreibung
DRIVE	–	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
9840	20 GB	Dekomprimiertes (Standard) Format, verwendet eine 20-GB-Kassette mit 270 Meter Band
9840-C	80 GB	Komprimiertes LZ-1 Enhanced-Format (4:1), verwendet eine 80-GB-Kassette mit 270 Meter Band
T9840C	40 GB	Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840C-C	80 GB	Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840D	75 GB	Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T9840D-C	150 GB	Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T10000A	500 GB	Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000A-C	1 TB	Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000B	1 TB	Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000B-C	2 TB	Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000C	5 TB	Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000C-C	10 TB	Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D	8 TB	Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D-C	15 TB	Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn der Standardwert der geschätzten Kapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist.

Dieser Wert muss als ganze Zahl gefolgt von einem der folgenden Einheitenanzeiger angegeben werden: `K` (Kilobyte), `M` (Megabyte), `G` (Gigabyte) oder `T` (Terabyte). Der zulässige Mindestwert ist 1 MB (ESTCAPACITY=1M).

Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt.

Soll der IBM Spectrum Protect-Server die geschätzte Kapazität für die Datenträger bestimmen, die dieser Einheitenklasse zugeordnet sind, geben Sie ESTCAPACITY="" an.

Für weitere Informationen zur geschätzten Standardkapazität von Magnetbandkassetten siehe Tabelle 1.

PREFIX

Gibt den Anfangsabschnitt des Archivierungsdateinamens der höheren Ebene auf dem Zielserver an. Dieser Parameter ist wahlfrei. Die maximale Länge dieses Präfixes beträgt 8 Zeichen.

Wenn Sie eine Namenskonvention für Datenträgerkennsätze haben, die das aktuelle Verwaltungssystem unterstützt, verwenden Sie einen Datenträgerkennsatz, der Ihrer Namenskonvention entspricht.

Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

```
AB.CD2.E
```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Archivierungsdateinamens der höheren Ebene, der das Standardpräfix verwendet, ist ADSM.volume1.

MOUNTRetention
: Gibt die Anzahl Minuten an, die ein inaktiver Datenträger mit sequenziellem Zugriff beibehalten wird, bevor er entladen wird. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 9999 angeben.

  Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

  Wird jedoch bei Kassettenarchivtyp EXTERNAL (ein durch ein externes Datenträgerverwaltungssystem verwaltetes Kassettenarchiv) für diesen Parameter ein niedriger Wert angegeben (z. B. zwei Minuten), wird die gemeinsame Benutzung von Einheiten zwischen Anwendungen verbessert.

  Anmerkung: Für Umgebungen, in denen Einheiten von mehreren Speicheranwendungen gemeinsam genutzt werden, muss die Einstellung für MOUNTRETENTION genau überlegt werden. Dieser Parameter bestimmt, wie lange ein inaktiver Datenträger in einem Laufwerk verbleibt. Einige Datenträgermanager hängen ein zugeordnetes Laufwerk nicht ab, um anstehende Anforderungen zu erfüllen. Sie müssen möglicherweise diesen Parameter optimieren, um konkurrierende Ladeanforderungen zu erfüllen, während gleichzeitig die optimale Systemleistung aufrecht erhalten wird. Normalerweise treten Probleme häufiger auf, wenn der Parameter MOUNTRETENTION auf einen Wert gesetzt wird, der zu klein ist (z. B. null).

MOUNTWait
: Gibt die maximale Anzahl der Minuten an, die der Server auf die Antwort eines Bedieners auf eine Anforderung zum Laden eines Datenträgers in ein Laufwerk in einem manuellen Kassettenarchiv oder zum Zurückstellen eines Datenträgers wartet, der in ein automatisiertes Kassettenarchiv geladen werden soll. Dieser Parameter ist wahlfrei. Wird die Ladeanforderung in der angegebenen Zeit nicht ausgeführt, wird sie abgebrochen. Sie können eine Zahl von 0 bis 9999 angeben.
  Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
: Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei. Sie können eine Zahl von 0 bis 4096 angeben.

  Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

  Gültige Werte:

  DRIVES
  : Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.
    Anmerkung: Geben Sie für Kassettenarchivtyp EXTERNAL nicht DRIVES als Wert für MOUNTLIMIT an. Die Anzahl Laufwerke für das Kassettenarchiv als Wert für MOUNTLIMIT angeben.

  Anzahl
  : Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt.

  0 (Null)
  : Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können. Alle aktuellen Transaktionen werden fortgesetzt und abgeschlossen, aber neue Transaktionen werden beendet.

 AIX-Betriebssysteme  Linux-Betriebssysteme

UPDATE DEVCLASS - z/OS Media-Server (Einheitenklasse für z/OS Media-Server aktualisieren)

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren. Eine begrenzte Gruppe von Einheitenklassentypen ist für Einheiten verfügbar, auf die über einen z/OS Media-Server zugegriffen wird.

- UPDATE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server aktualisieren)
- UPDATE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server aktualisieren)

Tabelle 1. Zugehörige Befehle für UPDATE DEVCLASS

Befehl	Beschreibung

Befehl	Beschreibung
BACKUP DEVCONFIG	Sichert IBM Spectrum Protect-Einheitendaten in einer Datei.
DEFINE DEVCLASS (z/OS Media-Server)	Definiert eine Einheitenklasse für die Verwendung von Speicher, der von einem z/OS Media-Server verwaltet wird.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DELETE DEVCLASS	Löscht eine Einheitenklasse.
QUERY DEVCLASS	Zeigt Informationen zu Einheitenklassen an.
UPDATE LIBRARY	Ändert die Attribute eines Kassettenarchivs.

 AIX-Betriebssysteme  Linux-Betriebssysteme

UPDATE DEVCLASS (Einheitenklasse 3590 für z/OS Media-Server aktualisieren)

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren, die Sie definiert haben, um mit einem z/OS Media-Server auf 3590-Einheiten zuzugreifen. Die Einheitenklasse, die sich auf Speicher für den z/OS Media-Server bezieht, erfordert eine Kassettenarchivdefinition des Typs ZOSMEDIA.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
                                          (1) (2)
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+---------------------------------+-------------------------->
   '-LIBRary---=--Kassettenarchivname-'

>--+-------------------------+--+----------------------+-------->
   '-FORMAT--=--+-DRIVE---+-'  '-ESTCAPacity--=--Größe-'
                +-3590B---+
                +-3590C---+
                +-3590E-B-+
                +-3590E-C-+
                +-3590H-B-+
                '-3590H-C-'

>--+--------------------------+---------------------------------->
   '-COMPression--=--+-Yes-+-'
                     '-No--'

>--+-----------------------------+--+-----------------------+---->
   '-MOUNTRetention--=--Minuten-'  '-MOUNTWait--=--Minuten-'

>--+-----------------------------+--+-------------------------+---->
   '-MOUNTLimit--=--+-DRIVES-+-'  '-EXPiration--=--jjjjttt-'
                    +-Anzahl-+
                    '-0------'

>--+---------------------+--+-------------------------------+----->
   '-RETention--=--Tage-'  '-PROtection--=--+-No--------+-'
                                            +-Yes-------+
                                            '-Automatic-'

>--+-------------------------+---------------------------------><
   '-UNIT--=--Einheitenname-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.
2. Der Parameter PREFIX kann mit diesem Befehl nicht aktualisiert werden. Sie müssen eine Einheitenklasse mit dem Wert erstellen, der für den Parameter PREFIX erforderlich ist.

Parameter

Einheitenklassenname (Erforderlich)
    Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.
LIBRary

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT
Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.
In der folgenden Tabelle sind die Optionen der Aufzeichnungsformate für 3590-Einheiten aufgelistet:

Tabelle 1. Aufzeichnungsformate für 3590

Format	**Beschreibung**
3590B	Dekomprimiertes (Basis-)Format
3590C	Komprimiertes Format
3590E-B	Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format
3590E-C	Komprimiertes Format, ähnlich dem 3590C-Format
3590H-B	Dekomprimiertes (Basis) Format, ähnlich dem 3590B-Format
3590H-C	Komprimiertes Format, ähnlich dem 3590C-Format
Anmerkung: Wenn das Format die Datenkomprimierung über Hardware mittels Bandlaufwerk verwendet, kann die tatsächliche Kapazität je nach Effektivität der Komprimierung zunehmen.	

ESTCAPacity
Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die durch diese Einheitenklasse kategorisiert werden. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: `K` (KB), `M` (MB), `G` (GB) oder `T` (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

COMPression
Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei.
Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass die Daten der Banddatenträger komprimiert werden.
No
Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

MOUNTRetention
Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 0 bis 9999 an.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

MOUNTWait
Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 1 bis 9999 an.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Sie können einen der folgenden Werte angeben:

DRIVES
: Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anzahl
: Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

0 (Null)
: Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

EXPiration
: Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei.

  Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

  Geben Sie das Verfallsdatum im Format *jjjjttt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als `2014007` angegeben (der siebte Tag des Jahres 2014).

  Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

RETention
: Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

  Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

  Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

  Tipp: Sie können für diesen Parameter den Wert null angeben. Dieser Wert sollte jedoch nur angegeben werden, wenn auch ein Wert für den Parameter EXPIRATION angegeben werden soll. Sie können keinen Wert für den Parameter EXPIRATION angeben, wenn Sie einen Wert ungleich null für den Parameter RETENTION angeben.

PROtection
: Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  No
  : Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

  Yes
  : Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.
    Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

    Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

  Automatic
  : Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

    Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

    Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

    Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

    Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlernachrichten generiert, wenn diese Datenträger gelöscht

werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

UNIT
Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die 3590-Band unterstützen. Dieser Parameter ist wahlfrei. Der Einheitenname kann bis zu 8 Zeichen umfassen.

 AIX-Betriebssysteme  Linux-Betriebssysteme

UPDATE DEVCLASS (Einheitenklasse 3592 für z/OS Media-Server aktualisieren)

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren, die Sie definiert haben, um mit einem z/OS Media-Server auf 3592-Einheiten zuzugreifen. Die Einheitenklasse, die sich auf Speicher für den z/OS Media-Server bezieht, erfordert eine Kassettenarchivdefinition des Typs ZOSMEDIA.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
                                          (1) (2)
>>-UPDate DEVclass--Einheitenklassenname-------------------------->

>--+-------------------------------------+---------------------->
   '-LIBRary---=--ZOSMEDIA-Speicherarchiv-'

>--+-------------------------+--+----------------------+-------->
   '-FORMAT--=--+-DRIVE---+-'  '-ESTCAPacity--=--Größe-'
                +-3592----+
                +-3592C---+
                +-3592-2--+
                +-3592-2C-+
                +-3592-3--+
                +-3592-3C-+
                +-3592-4--+
                '-3592-4C-'

>--+-------------------------+---------------------------------->
   '-COMPression--=--+-Yes-+-'
                     '-No--'

>--+-----------------------------+--+-----------------------+---->
   '-MOUNTRetention---=--Minuten-'  '-MOUNTWait--=--Minuten-'

>--+-----------------------------+--+-------------------------+---->
   '-MOUNTLimit--=--+-DRIVES-+-'  '-EXPiration--=--jjjjttt-'
                    +-Anzahl-+
                    '-0------'

>--+---------------------+--+-------------------------------+----->
   '-RETention--=--Tage-'  '-PROtection--=--+-No--------+-'
                                            +-Yes-------+
                                            '-Automatic-'

>--+------------------------+---------------------------------><
   '-UNIT--=--Einheitenname-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.
2. Der Parameter PREFIX kann mit diesem Befehl nicht aktualisiert werden. Sie müssen eine Einheitenklasse mit dem Wert erstellen, der für den Parameter PREFIX erforderlich ist.

Parameter

Einheitenklassenname (Erforderlich)

Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

LIBRary

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT

Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist DRIVE.
Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für 3592

Format	**Beschreibung**
3592	Dekomprimiertes (Basis-)Format
3592C	Komprimiertes Format
3592-2	Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format
3592-C	Komprimiertes Format, ähnlich dem 3592C-Format
3592-3	Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format
3592-3C	Komprimiertes Format, ähnlich dem 3592C-Format
3592-4	Dekomprimiertes (Basis) Format, ähnlich dem 3592-Format
3592-4C	Komprimiertes Format, ähnlich dem 3592C-Format
DRIVE	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
Anmerkung: Verwendet dieses Format die Datenkomprimierung über Hardware mittels Bandlaufwerk, kann je nach Effektivität der Komprimierung die tatsächliche Kapazität von dem aufgelisteten Wert abweichen.	

Verwenden Sie den Wert DRIVE nicht, wenn sich die Laufwerke in einem Kassettenarchiv befinden, das Laufwerke mit verschiedenen Bandtechnologien enthält. Verwenden Sie das Format, das das jeweilige Laufwerk verwendet. Um optimale Ergebnisse zu erzielen, mischen Sie nicht Generationen von Laufwerken in demselben Kassettenarchiv. Enthält ein Kassettenarchiv gemischte Generationen, können Datenträgerfehler auftreten. Beispielsweise können Laufwerke der Generation 1 und Generation 2 keine Datenträger der Generation 3 lesen. Falls möglich, führen Sie für alle Laufwerke ein Upgrade auf 3592 Generation 3 durch. Kann nicht für alle Laufwerke ein Upgrade auf 3592 Generation 3 durchgeführt werden, müssen Sie eine spezielle Konfiguration verwenden.

ESTCAPacity

Gibt die geschätzte Kapazität für die Datenträger an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: `K` (KB), `M` (MB), `G` (GB) oder `T` (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

COMPression

Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

Yes
: Gibt an, dass die Daten der Banddatenträger komprimiert werden.

No
: Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

MOUNTRetention

Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 0 bis 9999 an.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

MOUNTWait
Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 1 bis 9999 an.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Sie können einen der folgenden Werte angeben:

DRIVES
Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anzahl
Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

0 (Null)
Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

EXPiration
Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei.

Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Geben Sie das Verfallsdatum im Format *jjjjttt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als `2014007` angegeben (der siebte Tag des Jahres 2014).

Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

RETention
Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

Tipp: Sie können für diesen Parameter den Wert null angeben. Dieser Wert sollte jedoch nur angegeben werden, wenn auch ein Wert für den Parameter EXPIRATION angegeben werden soll. Sie können keinen Wert für den Parameter EXPIRATION angeben, wenn Sie einen Wert ungleich null für den Parameter RETENTION angeben.

PROtection
Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

Yes
Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.
Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Automatic
: Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

  Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

  Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

  Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

  Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlernachrichten generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

UNIT
: Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die 3592-Band unterstützen. Dieser Parameter ist wahlfrei. Dieser Name darf maximal 8 Zeichen lang sein.

 AIX-Betriebssysteme  Linux-Betriebssysteme

UPDATE DEVCLASS (Einheitenklasse ECARTRIDGE für z/OS Media-Server aktualisieren)

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren, die Sie definiert haben, um mit einem z/OS Media-Server auf StorageTek-Laufwerke, wie z. B. StorageTek T9840 oder T10000, zuzugreifen. Die Einheitenklasse, die sich auf Speicher für den z/OS Media-Server bezieht, erfordert eine Kassettenarchivdefinition des Typs ZOSMEDIA.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
                                          (1) (2)
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+-------------------------------------+---------------------->
   '-LIBRary----=--ZOSMEDIA-Speicherarchiv-'

>--+---------------------------+--+-----------------------+------>
   '-FORMAT--=---+-DRIVE-----+-'  '-ESTCAPacity--=--Größe-'
                 +-T9840C----+
                 +-T9840C-C--+
                 +-T9840D----+
                 +-T9840D-C--+
                 +-T10000A---+
                 +-T10000A-C-+
                 +-T10000B---+
                 +-T10000B-C-+
                 +-T10000C---+
                 +-T10000C-C-+
                 +-T10000D---+
                 '-T10000D-C-'

>--+---------------------------+--+-----------------------+---->
   '-MOUNTRetention----=--Minuten-'  '-MOUNTWait--=--Minuten-'
```

```
>--+--------------------------+--+-------------------------+--->
   '-MOUNTLimit--=--+-DRIVES-+-'  '-COMPression--=--+-Yes-+-'
                    +-Anzahl-+                     '-No--'
                    '-0------'

>--+-----------------------+--+--------------------+---------->
   '-EXPiration--=--jjjjttt-'  '-RETention--=--Tage-'

>--+-----------------------------+---------------------------->
   '-PROtection--=--+-No--------+-'
                    +-Yes-------+
                    '-Automatic-'

>--+-----------------------+---------------------------------><
   '-UNIT--=--Einheitenname-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.
2. Der Parameter PREFIX kann mit diesem Befehl nicht aktualisiert werden. Sie müssen eine Einheitenklasse mit dem Wert erstellen, der für den Parameter PREFIX erforderlich ist.

Parameter

Einheitenklassenname (Erforderlich)
Gibt den Namen der Einheitenklasse an, die aktualisiert werden soll.

LIBRary

Gibt den Namen eines Kassettenarchivs an, das mit dem Parameter LIBTYPE=ZOSMEDIA definiert wurde. Das Kassettenarchiv und die Bandlaufwerke, die von dieser Einheitenklasse verwendet werden können, werden von dem z/OS Media-Server gesteuert.

Dieser Parameter ist wahlfrei.

Informationen zum Definieren eines Kassettenarchivs befinden sich unter dem Befehl DEFINE LIBRARY.

FORMAT
Gibt das Aufzeichnungsformat an, das beim Schreiben von Daten auf Datenträger mit sequenziellem Zugriff verwendet werden soll. Dieser Parameter ist wahlfrei.
Die folgende Tabelle enthält die Aufzeichnungsformate.

Tabelle 1. Aufzeichnungsformate für ECARTRIDGE-Bänder

Format	Geschätzte Kapazität	Beschreibung
DRIVE	-	Der Server wählt das höchste Format aus, das von dem Laufwerk, in das ein Datenträger geladen ist, unterstützt wird. DRIVE ist der Standardwert. Achtung: Geben Sie DRIVE nicht an, wenn eine Mischung von Laufwerken innerhalb desselben Kassettenarchivs verwendet wird. Verwenden Sie diese Option beispielsweise nicht für ein Kassettenarchiv, das einige Laufwerke enthält, die ein höheres Aufzeichnungsformat als die anderen Laufwerke unterstützen.
T9840C	40 GB	Dekomprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840C-C	80 GB	Komprimiertes T9840C-Format, verwendet eine StorageTek 9840-Kassette
T9840D	75 GB	Dekomprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T9840D-C	150 GB	Komprimiertes T9840D-Format, verwendet eine StorageTek 9840-Kassette
T10000A	500 GB	Dekomprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000A-C	1 TB	Komprimiertes T10000A-Format, verwendet eine StorageTek T10000-Kassette
T10000B	1 TB	Dekomprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000B-C	2 TB	Komprimiertes T10000B-Format, verwendet eine Oracle StorageTek T10000-Kassette
T10000C	5 TB	Dekomprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000C-C	10 TB	Komprimiertes T10000C-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D	8 TB	Dekomprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette
T10000D-C	15 TB	Komprimiertes T10000D-Format, verwendet eine Oracle StorageTek T10000 T2-Kassette

Format	Geschätzte Kapazität	Beschreibung
Anmerkung: • Einige Formate verwenden eine Komprimierungsfunktion der Bandlaufwerkhardware. Je nach Effektivität der Komprimierung kann die tatsächliche Kapazität doppelt so groß (oder größer) sein wie der aufgeführte Wert. • T10000A-Laufwerke können nur das T10000A-Format lesen und schreiben. T10000B-Laufwerke können das T10000A-Format lesen, aber nicht schreiben. T10000C-Laufwerke können die T10000A- und T10000B-Formate lesen, aber nicht schreiben. T10000D-Laufwerke können die T10000A-, T10000B- und T10000C-Formate lesen, aber nicht schreiben.		

ESTCAPacity
Gibt die geschätzte Kapazität für die Datenträger mit sequenziellem Zugriff an, die dieser Einheitenklasse zugeordnet sind. Dieser Parameter ist wahlfrei.

Dieser Parameter kann angegeben werden, wenn die geschätzte Standardkapazität für die Einheitenklasse wegen der Komprimierung von Daten fehlerhaft ist. Der Wert bestimmt nicht das auf dem Datenträger gespeicherte Datenvolumen. Der Server verwendet den Wert, um die Belegung zu schätzen, bevor ein Datenträger gefüllt ist. Wenn ein Datenträger voll ist, wird für die Berechnung der Belegung das tatsächlich auf dem Band gespeicherte Datenvolumen verwendet.

Geben Sie den Wert als ganze Zahl mit einem der folgenden Einheitenanzeiger an: `K` (KB), `M` (MB), `G` (GB) oder `T` (TB). Beispiel: Geben Sie mit dem Parameter ESTCAPACITY=9G an, dass die geschätzte Kapazität 9 GB beträgt. Der zulässige Mindestwert ist 100 KB (ESTCAPACITY=100K).

MOUNTRetention
Gibt die Anzahl Minuten an, die ein inaktiver Banddatenträger beibehalten wird, bevor er entladen wird. Die Zeitspanne für die Ladedauer beginnt nach Ablauf des Inaktivitätszeitlimits. Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 0 bis 9999 an.

Dieser Parameter kann die Antwortzeit für Ladevorgänge von Datenträgern mit sequenziellem Zugriff verbessern, indem zuvor geladene Datenträger online bleiben.

MOUNTWait
Gibt die maximale Anzahl Minuten an, die der z/OS Media-Server auf das Laden eines Datenträgers wartet. Wird auf die Ladeanforderung nicht innerhalb der angegebenen Zeit geantwortet, schlägt die Ladeanforderung fehl. Ist eine Einheit erfolgreich zugeordnet und wird die Anforderung zum Öffnen der Einheit nicht innerhalb der angegebenen Zeit ausgeführt, wird die Anforderung zum Öffnen der Einheit beendet und die Ladeanforderung schlägt fehl.

Dieser Parameter ist wahlfrei. Geben Sie eine Zahl von 1 bis 9999 an.

Einschränkung: Wenn das Kassettenarchiv, das dieser Einheitenklasse zugeordnet ist, ein externes Kassettenarchiv ist (LIBTYPE=EXTERNAL), geben Sie nicht den Parameter MOUNTWAIT an.

MOUNTLimit
Gibt die maximale Anzahl Datenträger mit sequenziellem Zugriff an, die gleichzeitig für die Einheitenklasse geladen sein kann. Dieser Parameter ist wahlfrei.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

Sie können einen der folgenden Werte angeben:

DRIVES
Gibt an, dass bei jeder Zuordnung eines Mountpunkts die Anzahl der Laufwerke, die in dem Kassettenarchiv definiert und online sind, für die Berechnung des wahren Werts verwendet wird.

Anzahl
Gibt die maximale Anzahl der Laufwerke in dieser Einheitenklasse an, die gleichzeitig von dem Server verwendet werden. Dieser Wert darf niemals die Anzahl Laufwerke überschreiten, die in dem Kassettenarchiv definiert und online sind, das diese Einheitenklasse versorgt. Sie können eine Zahl von 0 bis 4096 angeben.

0 (Null)
Gibt an, dass keine neuen Transaktionen auf den Speicherpool zugreifen können.

COMPression
Gibt an, ob die Dateikomprimierung für diese Einheitenklasse verwendet wird. Dieser Parameter ist wahlfrei.
Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass die Daten der Banddatenträger komprimiert werden.

No
Gibt an, dass die Daten der Banddatenträger nicht komprimiert werden.

EXPiration
Gibt das Verfallsdatum an, das in den Bandkennsätzen für diese Einheitenklasse angegeben wird. Dieser Parameter ist wahlfrei.

Geben Sie das Datum an, an dem der Server das Band nicht mehr benötigt. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Geben Sie das Verfallsdatum im Format *jjjjttt* an (vier Stellen für das Jahr und drei Stellen für den Tag). Beispielsweise wird der 7. Januar 2014 als `2014007` angegeben (der siebte Tag des Jahres 2014).

Wenn Sie den Parameter EXPIRATION angeben, können Sie nicht den Parameter RETENTION angeben.

RETention
Gibt die Anzahl Tage an, die das Band aufbewahrt werden soll. Dieser Parameter ist wahlfrei.

Geben Sie die Anzahl der Tage (1 - 9999) an, die der Server das Band voraussichtlich verwenden wird. Der Server verwendet diese Informationen nicht; die Informationen werden für die Verwendung durch z/OS oder Bandverwaltungssysteme an den z/OS Media-Server übermittelt.

Wenn Sie den Parameter RETENTION angeben, können Sie nicht den Parameter EXPIRATION angeben.

Tipp: Sie können für diesen Parameter den Wert null angeben. Dieser Wert sollte jedoch nur angegeben werden, wenn auch ein Wert für den Parameter EXPIRATION angegeben werden soll. Sie können keinen Wert für den Parameter EXPIRATION angeben, wenn Sie einen Wert ungleich null für den Parameter RETENTION angeben.

PROtection
Gibt an, ob das RACF-Programm (falls installiert) Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Wenn Schutz zur Verfügung gestellt wird, werden RACF-Profile bei der ersten Verwendung der Datenträger erstellt. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass das RACF-Programm keine Datenträger schützt, die dieser Einheitenklasse zugeordnet sind.

Yes
Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. Für die Datenträger werden RACF-Profile erstellt, wenn der Server die Datenträger zum ersten Mal verwendet; die Profile werden jedoch nicht gelöscht, wenn Datenträger auf dem Server gelöscht werden. Die Profile müssen manuell gelöscht werden.
Tipp: Sind sensible Daten auf den Datenträgern gespeichert, die dieser Einheitenklasse zugeordnet sind, verwenden Sie PROTECTION=YES und löschen Sie RACF-Profile manuell nur nach dem Entfernen der Banddatenträger.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Automatic
Gibt an, dass das RACF-Programm Datenträger schützt, die dieser Einheitenklasse zugeordnet sind. RACF-Profile werden für Datenträger erstellt, wenn der Server zum ersten Mal die Datenträger verwendet. RACF-Profile werden gelöscht, wenn Datenträger auf dem Server gelöscht werden.

Die Profile, die für Datenträger erstellt werden, hängen von den RACF-Systemeinstellungen ab. Der zur Verfügung gestellte Schutz entspricht dem Schutz bei Verwendung von PROTECT=YES in JCL. Wenn das RACF-Programm aktiv ist und TAPEVOL und TAPEDSN inaktiv sind, schlägt die Zuordnung von Bändern fehl.

Wichtig: Wird PROTECTION=AUTOMATIC angegeben, wird beim Löschen eines Datenträgers sein RACF-Profil gelöscht. Der Datenträger ist daher nicht mehr durch das RACF-Programm geschützt. Andere Benutzer können auf die Daten auf diesen Datenträgern zugreifen.

Wenn Sie PROTECTION=AUTOMATIC angeben, gibt der z/OS Media-Server RACROUTE-Befehle aus, um Profile zu löschen, wenn ein Datenträger auf dem Server gelöscht wird. Die ausgegebenen Löschbefehle sind von den aktuellen Systemwerten für TAPEVOL und TAPEDSN abhängig. Wenn die Systemeinstellungen geändert werden, löscht der z/OS Media-Server vorhandene Profile möglicherweise nicht.

Ändern Sie nicht die Einstellung in PROTECTION=AUTOMATIC für eine Einheitenklasse, für die PROTECTION=NO definiert wurde. Es können Datenträger ohne Profile vorhanden sein, und es werden Fehlernachrichten generiert, wenn diese Datenträger gelöscht werden. Wenn ein anderer Wert für PROTECTION erforderlich ist, definieren Sie eine neue Einheitenklasse.

Die Erstellung und das Löschen von Profilen erfolgen aufgrund der Schutzeinstellungen, wenn der Datenträger zum ersten Mal verwendet und wenn er gelöscht wird. Der Server erstellt keine Profile für Datenträger, die er bereits verwendet hat. Wenn für den Schutz AUTOMATIC angegeben ist, versucht der Server, Profile zu löschen, wenn Datenträger gelöscht werden.

Die Dokumentation zu dem RACF-Programm enthält ausführliche Informationen zu den Einstellungen für TAPEVOL und TAPEDSN und zu den Profilen, die erstellt werden, wenn diese Einstellungen aktiv sind.

UNIT
Gibt einen privaten Einheitennamen für eine Gruppe von Bandeinheiten an, die ECARTRIDGE-Bänder unterstützen. Verwenden Sie den Einheitennamen, der die Untergruppe der Laufwerke im Kassettenarchiv darstellt, die mit dem z/OS-System verbunden sind. Dieser Parameter ist wahlfrei. Der Einheitenname kann bis zu 8 Zeichen umfassen.

 AIX-Betriebssysteme  Linux-Betriebssysteme

UPDATE DEVCLASS (Einheitenklasse FILE für z/OS Media-Server aktualisieren)

Mit diesem Befehl können Sie eine Einheitenklasse aktualisieren, die Sie definiert haben, um mit einem z/OS Media-Server auf Dateien im Magnetplattenspeicher als Datenträger mit sequenziellem Zugriff (wie z. B. Band) zuzugreifen. Die Einheitenklasse, die sich auf Speicher für den z/OS Media-Server bezieht, erfordert eine Kassettenarchivdefinition des Typs ZOSMEDIA.

Ein Datenträger in dieser Einheitenklasse ist eine lineare VSAM-Datei (VSAM - Virtual Storage Access Method), auf die vom z/OS Media-Server zugegriffen wird. Arbeitsdatenträger können mit einer Einheitenklasse verwendet werden und der z/OS Media-Server ordnet dynamisch die lineare VSAM-Datei zu. Es ist nicht erforderlich, Datenträger für den Server zu definieren, um die Einheitenklasse zu verwenden. Wenn Sie Datenträger definieren, definieren Sie das Qualifikationsmerkmal der höheren Ebene so, dass SMS die Zuordnungsanforderung durch den z/OS Media-Server erkennt. Bei Verwendung von definierten Datenträgern wird die Funktion zum Formatieren von Datenträgern für den Server nicht unterstützt, wenn diese Einheitenklasse verwendet wird. Der z/OS Media-Server verwendet beim Füllen von FILE-Datenträgern ein FormatWrite-Feature des DFSMS Media Manager.

Sie können Datenträger für die Einheitenklasse FILE definieren, indem Sie den Befehl DEFINE VOLUME verwenden. Der z/OS Media-Server ordnet jedoch erst dann Speicherbereich für einen definierten Datenträger zu, wenn der Datenträger für seine erste Verwendung geöffnet wird.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate DEVclass--Einheitenklassenname------------------------>

>--+-----------------------+--+------------------------+-------->
   '-MAXCAPacity--=--Größe-'  '-PRIMARYalloc--=--Größe-'

>--+--------------------------+-------------------------------->
   '-SECONDARYalloc--=--Größe-'

>--+-----------------------------------+------------------------>
   '-PREFIX--=--Dateidatenträgerpräfix-'

>--+-----------------------+-----------------------------------><
   '-MOUNTLimit--=--Anzahl-'
```

Parameter

Einheitenklassenname (Erforderlich)
: Gibt den Namen der zu definierenden Einheitenklasse an. Die maximale Länge des Einheitenklassennamens beträgt 30 Zeichen.

MAXCAPacity
: Gibt die maximale Größe der Dateidatenträger an, die für einen Speicherpool in dieser Einheitenklasse definiert sind. Dieser Parameter ist wahlfrei.

  Dieser Wert muss als ganze Zahl gefolgt von einem `K` (KB), `M` (MB), `G` (GB) oder `T` (TB) angegeben werden. Die Mindestgröße ist 1 MB (MAXCAPACITY=1M). Die maximale Größe ist 16384 GB (MAXCAPACITY=16384G).

PRIMARYalloc
: Gibt den anfänglichen Speicherbereich an, der dynamisch zugeordnet wird, wenn ein neuer Datenträger geöffnet wird. Es muss genügend Speicherbereich verfügbar sein, um den Wert für die primäre Bereichszuordnung zu erfüllen. Die SMS-Richtlinie (SMS = Storage Management Subsystem) bestimmt, ob mehrere physische Datenträger verwendet werden können, um die Anforderung zur primären Bereichszuordnung zu erfüllen.

  Dieser Parameter ist wahlfrei. Dieser Wert muss als ganze Zahl gefolgt von einem `K` (KB), `M` (MB), `G` (GB) oder `T` (TB) angegeben werden. Die Mindestgröße ist 100 KB (PRIMARYALLOC=100K). Die maximale Größe ist 16384 GB (MAXCAPACITY=16384G). Alle Werte werden auf das nächsthöhere Vielfache von 256 KB gerundet.

  Um eine ineffiziente Speichernutzung zu vermeiden, verwendet die Operation für die dynamische Zuordnung den kleineren der in den beiden Parametern PRIMARYALLOC und MAXCAPACITY angegebenen Werte.

  SMS-Routinen für die automatische Klassenauswahl können Einfluss darauf haben, ob die Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC verwendet werden.

SECONDARYalloc
: Gibt den Speicherbereich an, um den ein Dateidatenträger erweitert wird, wenn der Speicherbereich, der dem Dateidatenträger bereits zugeordnet ist, verbraucht ist. Die Datei für einen Dateidatenträger wird bis zu der Größe erweitert, die mit dem Parameter MAXCAPACITY definiert ist. Danach wird der Datenträger als voll markiert.

Da sich die sekundäre Bereichszuordnung einer linearen Datei nicht über physische Datenträger erstrecken kann, muss bei der Auswahl der Größe für die sekundäre Bereichszuordnung die Größe des physischen Datenträgers berücksichtigt werden. Beispielsweise haben physische Datenträger für ein 3390 Modell 3 eine Größe von ungefähr 2,8 GB. Um sicherzustellen, dass mit jeder Erweiterungsanforderung ungefähr der gesamte physische Datenträger belegt wird (aber nicht mehr), verwenden Sie eine Größe für die sekundäre Bereichszuordnung, die gerade unter 2,8 GB liegt. Mit einer Größe von 2600 MB für die sekundäre Bereichszuordnung wird genügend Speicherbereich für die VSAM-Datenträgerdatei, den Datenträgerkennsatz und das Datenträgerinhaltsverzeichnis zugeordnet.

Dieser Parameter ist wahlfrei. Dieser Wert muss als ganze Zahl gefolgt von einem `K` (KB), `M` (MB), `G` (GB) oder `T` (TB) angegeben werden. Der Mindestwert ist 0 KB (SECONDARYALLOC=0K). Der Maximalwert ist 16384 GB. Mit Ausnahme von 0 werden alle Werte auf das nächsthöhere Vielfache von 256 KB gerundet.

Geben Sie 0 (SECONDARYALLOC=0) an, kann der Dateidatenträger nicht über den Wert der primären Bereichszuordnung hinaus erweitert werden.

SMS-Routinen für die automatische Klassenauswahl können Einfluss darauf haben, ob die Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC verwendet werden.

Wenn Sie einen Wert für den Parameter SECONDARYALLOCATION angeben, der nicht 0 ist, oder wenn Sie den Standardwert 2600M akzeptieren, muss für die SMS DATACLAS, der die PREFIX-Kennung zugeordnet ist (z. B. Qualifikationsmerkmal der höheren Ebene), das Attribut für die erweiterte Adressierbarkeit (Extended Addressability - EA) angegeben werden. Ohne das EA-Attribut beschränkt die SMS DATACLAS die Zuordnung des linearen VSAM-FILE-Datenträgers auf den primären Bereich. (Siehe die Beschreibung des Parameters PRIMARYALLOCATION). Wenn die Datei auf die primäre Bereichszuordnung beschränkt ist, kann die Datei vom z/OS Media-Server nicht erweitert werden, und der Datenträger wird als FULL markiert, bevor die maximale Kapazität erreicht ist.

Einschränkung: Stellen Sie sicher, dass sich die für die Parameter PRIMARYALLOC und SECONDARYALLOC angegebenen Werte innerhalb praktischer Grenzwerte für die Speichereinheit befinden. Der Server kann nicht überprüfen, ob die Werte praktische Grenzwerte für die Einheit überschreiten, und der Server überprüft nicht, ob die beiden Werte zusammen die aktuelle Einstellung für MAXCAPACITY überschreiten.
Tipp: Um bei der Angabe eines hohen Werts für den Parameter MAXCAPACITY Datenträger zu füllen, geben Sie hohe Werte für die Parameter PRIMARYALLOC und SECONDARYALLOC an. Verwenden Sie höhere MVS-Datenträgergrößen, um die Möglichkeit eines Erweiterungsfehlers zu reduzieren.

PREFIX
Gibt die Kennung der oberen Ebene des Dateinamens an, mit der Dateien von Arbeitsdatenträgern zugeordnet werden. Bei allen in dieser Einheitenklasse erstellten Arbeitsdateidatenträgern verwendet der Server dieses Präfix für die Erstellung des Dateinamens. Dieser Parameter ist wahlfrei. Die maximale Länge des Präfix, einschließlich Punkte, beträgt 32 Zeichen.
Die für diesen Parameter angegebenen Werte müssen folgende Bedingungen erfüllen:

- Der Wert muss aus Qualifikationsmerkmalen bestehen, die maximal acht Zeichen (einschließlich Punkte) enthalten können. Der folgende Wert ist beispielsweise zulässig:

  ```
  AB.CD2.E
  ```

- Die Qualifikationsmerkmale müssen durch einen einzelnen Punkt voneinander getrennt werden.
- Das erste Zeichen eines Qualifikationsmerkmals muss ein alphabetisches oder ein nationales Sonderzeichen sein (@,#,$), gefolgt von alphabetischen Zeichen, nationalen Sonderzeichen, Silbentrennungsstrichen oder numerischen Zeichen.

Ein Beispiel eines Dateinamens für einen Dateidatenträger unter Verwendung des Standardpräfixes ist `ADSM.B0000021.BFS`.

Wenn Sie eine Namenskonvention für Dateinamen haben, verwenden Sie ein Präfix, das Ihrer Namenskonvention entspricht. Der folgende Wert ist beispielsweise zulässig: `TSM.SERVER2.VSAMFILE`.

Wenn Sie mehrere Serverinstanzen für IBM Spectrum Protect oder Tivoli Storage Manager for z/OS Media ausführen, müssen Sie einen eindeutigen Wert für den Parameter PREFIX für jede Einheitenklasse verwenden, die Sie aktualisieren.

MOUNTLimit
Gibt die maximale Anzahl FILE-Datenträger an, die gleichzeitig für diese Einheitenklasse geöffnet sein können. Dieser Parameter ist wahlfrei. Für Einheiten 3995, die Einheiten 3390 emulieren, darf der Wert nicht höher sein als die Anzahl der parallelen Eingabe- und Ausgabedatenströme, die auf den Medien möglich sind, die die Datenträger speichern.

Der in diesem Parameter angegebene Wert ist wichtig, wenn das Umschalten von einem Datenträger zu einem anderen eine große Beeinträchtigung darstellt. Das Umschalten kann beispielsweise erfolgen, wenn Sie Einheiten IBM® 3995 verwenden, um Einheiten 3390 zu emulieren. Der angegebene Wert darf nicht höher als die Anzahl der physischen Laufwerke sein, die auf der Einheit verfügbar sind.

Soll die Funktion für simultanes Schreiben verwendet werden, stellen Sie sicher, dass genügend Laufwerke für die Schreiboperation verfügbar sind. Ist die Anzahl der Laufwerke, die für eine simultane Schreiboperation erforderlich ist, größer als der Wert des Parameters MOUNTLIMIT für eine Einheitenklasse, schlägt die Transaktion fehl.

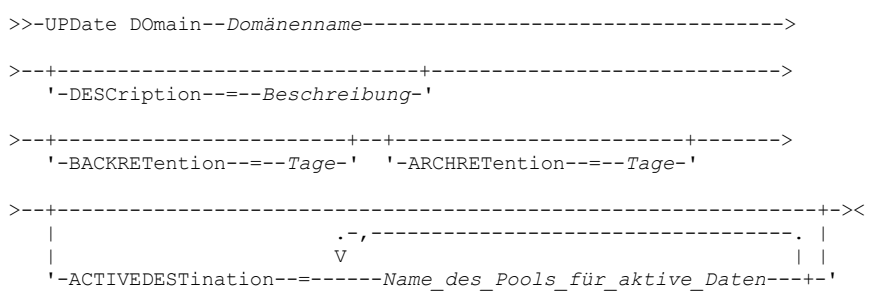
UPDATE DOMAIN (Maßnahmendomäne aktualisieren)

Mit diesem Befehl kann eine Maßnahmendomäne geändert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für die angegebene Maßnahmendomäne erforderlich.

Syntax



Parameter

Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an.

DESCription
: Beschreibt die Maßnahmendomäne unter Verwendung einer Textfolge. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine Nullzeichenfolge ("") anzugeben.

BACKRETention
: Gibt die Anzahl Tage an (ab dem Datum, an dem die Sicherungsversionen inaktiv wurden), die die Sicherungsversionen aufbewahrt werden sollen, die sich nicht mehr im Client-Dateisystem befinden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben. Der Server verwendet den Wert für den Aufbewahrungszeitraum für Sicherung, um inaktive Versionen von Dateien zu verwalten, wenn eine der folgenden Bedingungen zutrifft:

  - Eine Datei wird an eine neue Verwaltungsklasse erneut gebunden, aber die neue Verwaltungsklasse und die Standardverwaltungsklasse enthalten keine Sicherungskopiengruppe.
  - Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden. Die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.
  - Die Sicherungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist. Die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.

ARCHRETention
: Gibt die Anzahl Tage an (ab dem Datum der Archivierung), die Archivierungskopien aufbewahrt werden sollen. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 0 bis 30000 angeben. Der Server verwendet den Wert für den Aufbewahrungszeitraum für Archivierung, um Archivierungskopien von Dateien zu verwalten, wenn eine der folgenden Bedingungen zutrifft:

  - Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden. Die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.
  - Die Archivierungskopiengruppe wird aus der Verwaltungsklasse gelöscht, an die eine Datei gebunden ist. Die Standardverwaltungsklasse enthält keine Archivierungskopiengruppe.

ACTIVEDESTination
: Gibt die Namen der Pools für aktive Daten an, in denen aktive Versionen von Sicherungsdaten für Knoten gespeichert werden, die der Domäne zugeordnet sind. Dieser Parameter ist wahlfrei. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig. Sie können maximal 10 Pools für aktive Daten für eine Domäne angeben.

  Bevor der IBM Spectrum Protect-Server Daten in einen Pool für aktive Daten schreibt, überprüft er, ob der Knoten, der Eigner der Daten ist, einer Domäne zugeordnet ist, für die der Pool für aktive Daten in der ACTIVEDESTINATION-Liste aufgelistet ist. Stellt der Server fest, dass der Knoten diese Kriterien erfüllt, werden die Daten im Pool für aktive Daten gespeichert. Werden die Kriterien vom Knoten nicht erfüllt, werden die Daten nicht im Pool für aktive Daten gespeichert. Werden mit der Funktion für simultanes Schreiben Daten in einen Pool für aktive Daten geschrieben, führt der Server die Prüfung während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients unter Verwendung der IBM Spectrum Protect-API durch. Die Prüfung wird auch durchgeführt, wenn aktive Daten mit dem Befehl COPY ACTIVEDATA kopiert werden.

Beispiel: Den Aufbewahrungszeitraum für Sicherung für eine Maßnahmendomäne aktualisieren

Die Maßnahmendomäne ENGPOLDOM so aktualisieren, dass der Aufbewahrungszeitraum für Sicherung auf 90 Tage und der Aufbewahrungszeitraum für Archivierung auf zwei Jahre erweitert wird. Einen Pool für aktive Daten als Ziel für aktive Versionen von

Sicherungsdaten angeben, die zu Knoten gehören, die der Domäne zugeordnet sind. Den Namen *engactivedata* für den Pool für aktive Daten verwenden. Geben Sie den folgenden Befehl aus:

```
update domain engpoldom description='Maßnahmendomäne für Entwicklung'
backretention=90 archretention=730 activedestination=engactivedata
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE DOMAIN

Befehl	Beschreibung
COPY DOMAIN	Erstellt eine Kopie einer Maßnahmendomäne.
DEFINE DOMAIN	Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
DELETE DOMAIN	Löscht eine Maßnahmendomäne und, falls vorhanden, Maßnahmenobjekte in der Maßnahmendomäne.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.

UPDATE DRIVE (Laufwerk aktualisieren)

Mit diesem Befehl kann ein Laufwerk aktualisiert werden.

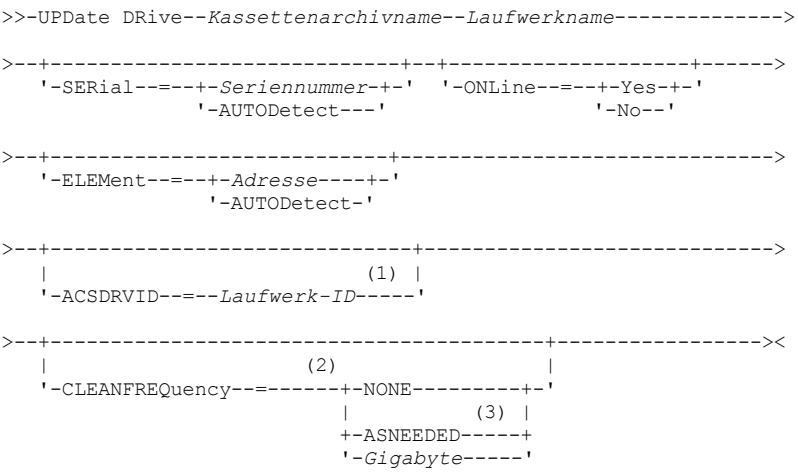
Berechtigungsklasse

Ausführliche und aktuelle Informationen zur Laufwerkunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax



Anmerkungen:

1. Der Parameter ACSDRVID ist nur für Laufwerke in ACSLS-Kassettenarchiven gültig.
2. Der Parameter CLEANFREQUENCY ist nur für Laufwerke in SCSI-Kassettenarchiven gültig.
3. Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht bei allen Bandlaufwerken. Weitere Informationen enthält die Parameterbeschreibung.

Parameter

Speicherarchivname (Erforderlich)
Gibt den Namen des Kassettenarchivs an, dem das Laufwerk zugeordnet ist.

Laufwerkname (Erforderlich)
Gibt den Namen an, der dem Laufwerk zugeordnet ist.

SERial
Gibt die Seriennummer der Laufwerke an, die aktualisiert werden. Dieser Parameter ist nur für Laufwerke in einem SCSI- oder VTL-Archiv (Virtual Tape Library) gültig. Dieser Parameter ist wahlfrei. Gültige Werte sind:

Seriennummer
Gibt die Seriennummer des Laufwerks an, das aktualisiert wird.
Anmerkung: Ist bereits ein Pfad zu diesem Laufwerk definiert, wird die eingegebene Nummer mit der Nummer verglichen, die von IBM Spectrum Protect erkannt wurde. Stimmen die Nummern nicht überein, schlägt der Befehl fehl.

AUTODETECT
Gibt an, dass die Seriennummer automatisch von IBM Spectrum Protect erkannt und verwendet wird, wenn bereits ein Pfad zu diesem Laufwerk definiert ist.

Ist kein Pfad zu diesem Laufwerk definiert, wird die Seriennummer nicht erkannt.

ONLine
Gibt an, ob das Laufwerk für die Verwendung verfügbar ist. Dieser Parameter gibt an, ob Laufwerke abgehängt und für andere Aktivitäten, wie beispielsweise für die Wartung, verwendet werden können. Dieser Parameter ist wahlfrei.

Sie können diesen Befehl ausgeben, wenn das Laufwerk in einem aktiven Prozess oder in einer aktiven Sitzung verwendet wird. Dies wird jedoch nicht empfohlen. Wenn Sie einen Befehl ausgeben, um das Laufwerk abzuhängen, während es im Gebrauch ist, wird eine Fehlernachricht ausgegeben. Der geladene Datenträger beendet den aktuellen Prozess. Wenn dieser Datenträger Teil einer Serie von Datenträgern für eine bestimmte Transaktion war, steht das Laufwerk nicht zur Verfügung, um das Laden der Serie abzuschließen. Sind keine anderen Laufwerke verfügbar, schlägt der Prozess fehl.

Achtung: Ist ein Laufwerk im Gebrauch, geben Sie nicht den Parameter ELEMENT mit dem Parameter ONLINE an. Das Laufwerk wird nicht aktualisiert, und der Befehl schlägt fehl.

Der Laufwerkstatus wird nicht geändert, auch wenn der Server angehalten und erneut gestartet wird. Ist ein Laufwerk offline, wenn der Server erneut gestartet wird, wird in einer Warnung angegeben, dass das Laufwerk manuell in den Online-Status versetzt werden muss. Werden alle Laufwerke in einem Kassettenarchiv in den Offline-Status geändert, können Prozesse, die einen Mountpunkt für ein Kassettenarchiv benötigen, nicht ausgeführt werden (sie reihen sich nicht in die Warteschlange für einen Mountpunkt ein).

YES
Gibt an, dass das Laufwerk für die Verwendung verfügbar (angehängt) ist.

No
Gibt an, dass das Laufwerk nicht für die Verwendung verfügbar ist (das Laufwerk ist abgehängt).

ELEMent
Gibt die Elementadresse des Laufwerks in einem SCSI- oder VTL-Archiv an. Der Server verwendet die Elementadresse, um die physische Adresse des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Dieser Parameter ist nur für ein Laufwerk in einem SCSI- oder VTL-Archiv gültig, wenn der Befehl von einem IBM Spectrum Protect-Kassettenarchivmanagerserver ausgegeben wird. Gültige Werte sind:

Adresse
Gibt die Elementadresse des Laufwerks an, das aktualisiert wird.

Zum Lokalisieren der Elementadresse für die Archivkonfiguration die Informationen des Herstellers zu Rate ziehen.

Hinweis: Ist bereits ein Pfad zu diesem Laufwerk definiert, wird die eingegebene Nummer mit der Nummer verglichen, die zuvor von IBM Spectrum Protect erkannt wurde. Stimmen die Nummern nicht überein, schlägt dieser Befehl fehl.

AUTODETECT
Gibt an, dass die Elementnummer automatisch von IBM Spectrum Protect erkannt und verwendet wird, wenn bereits ein Pfad zu diesem Laufwerk definiert ist.

Ist kein Pfad zu diesem Laufwerk definiert, wird die Elementnummer nicht erkannt.

Einschränkung: Wenn das Kassettenarchiv, in dem sich das Laufwerk befindet, den SCSI-Befehl "Read Element Status" nicht unterstützt, und für den Parameter ELEMENT der Wert AUTODETECT angegeben wird, schlägt der Befehl mit einer IBM Spectrum Protect-Fehlernachricht fehl.

ACSDRVID
Gibt die ID des Laufwerks an, auf das in einem ACSLS-Kassettenarchiv zugegriffen wird. Die Laufwerk-ID ist eine Zahlengruppe, die die physische Adresse eines Laufwerks in einem ACSLS-Kassettenarchiv angibt. Diese Laufwerk-ID muss als *a,l,p,d,* angegeben werden, wobei *a* die ACSID, *l* das LSM (Library Storage Module), *p* die Anzeigennummer und *d* die Laufwerk-ID ist. Der Server benötigt die Laufwerk-ID, um die physische Adresse des Laufwerks mit der SCSI-Adresse des Laufwerks zu verbinden. Die StorageTek-Dokumentation enthält ausführliche Informationen.

CLEANFREQuency
Gibt an, wie oft der Server die Laufwerkreinigung aktiviert. Dieser Parameter ist wahlfrei. Um die Reinigung für ein automatisiertes Kassettenarchiv nahezu vollständig zu automatisieren, müssen Sie eine Reinigungskassette in den Datenträgerbestand des Kassettenarchivs zurückgestellt haben. Bei Verwendung der speicherarchivbasierten Reinigung wird NONE empfohlen, wenn Ihr Speicherarchivtyp diese Funktion unterstützt. Dieser Parameter ist nur für Laufwerke in SCSI-Kassettenarchiven gültig, und ist für extern

verwaltete Kassettenarchive, wie beispielsweise 3494-Kassettenarchive oder StorageTek-Kassettenarchive, die unter ACSLS verwaltet werden, nicht gültig.
Wichtig: Es gibt einige Besonderheiten, die beachtet werden müssen, wenn die vom Server aktivierte Laufwerkreinigung bei einem SCSI-Kassettenarchiv verwendet werden soll, das eine automatische Laufwerkreinigungsunterstützung in seiner Einheitenhardware zur Verfügung stellt.

NONE
Gibt an, dass der Server die Reinigung dieses Laufwerks nicht verfolgt. Diesen Parameter für Kassettenarchive verwenden, die über ihre eigene automatische Reinigungsunterstützung verfügen.

ASNEEDED
Gibt an, dass der Server das Laufwerk mit einer zurückgestellten Reinigungskassette nur lädt, wenn ein Laufwerk dem Einheitentreiber mitteilt, dass eine Reinigung erforderlich ist.

Der Parameterwert CLEANFREQUENCY=ASNEEDED funktioniert nicht bei allen Bandlaufwerken. Detaillierte Laufwerkdaten finden Sie auf der Website für unterstützte Einheiten für Ihr Betriebssystem. Wird ASNEEDED nicht unterstützt, können Sie den Gigabyte-Wert für die automatische Reinigung verwenden.

Für IBM 3592- und LTO-Laufwerke wird die speicherarchivbasierte Reinigung empfohlen. Wird die speicherarchivbasierte Reinigung nicht unterstützt, muss ASNEEDED verwendet werden. Gigabyte wird nicht empfohlen.

Einschränkung: IBM Spectrum Protect steuert nicht die Laufwerke, die mit dem NAS-Dateiserver verbunden sind. Ist ein Laufwerk nur mit einem NAS-Dateiserver verbunden (keine Verbindung zu einem Speicheragenten oder Server), geben Sie nicht ASNEEDED für die Häufigkeit der Reinigung an.

Gigabyte
Gibt in Gigabyte an, wieviel Daten auf dem Laufwerk verarbeitet werden, bevor der Server das Laufwerk mit einer Reinigungskassette lädt. Der Server setzt den Zähler für die verarbeiteten Gigabyte zurück, wenn eine Reinigungskassette in das Laufwerk geladen wird.
Wichtig: Bei CLEANFREQUENCY=Gigabyte kann die Laufwerkreinigung erfolgen, bevor die Einstellung für Gigabyte erreicht ist, wenn das Laufwerk den Einheitentreiber benachrichtigt, dass eine Reinigung erforderlich ist.

Lesen Sie die Empfehlungen des Laufwerkherstellers bezüglich der Reinigung. Werden Empfehlungen für die Reinigungshäufigkeit in Stunden der Verwendung gegeben, führen Sie wie folgt eine Umrechnung in einen Gigabytewert durch:

1. Verwenden Sie den Wert für Byte pro Sekunde des Laufwerks, um einen Wert für Gigabyte pro Stunde zu ermitteln.
2. Multiplizieren Sie den Wert für Gigabyte pro Stunde mit den empfohlenen Stunden der Verwendung zwischen den Reinigungen.
3. Verwenden Sie das Ergebnis als Wert für die Reinigungshäufigkeit.

Tipp: Geben Sie für IBM 3590 einen Wert für die Reinigungshäufigkeit an, um eine adäquate Reinigung der Laufwerke sicherzustellen. Lesen Sie die Empfehlungen des Laufwerkherstellers bezüglich der Reinigung. Bei Verwendung der von IBM empfohlenen Reinigungshäufigkeit wird die Reinigung der Laufwerke nicht zu oft durchgeführt.

Beispiel: Die Elementadresse für ein Laufwerk aktualisieren

Für das Laufwerk DRIVE3, das sich im Kassettenarchiv AUTO befindet, soll die Elementadresse in 119 geändert werden.

```
update drive auto drive3 element=119
```

Beispiel: Ein Laufwerk abhängen

Das Laufwerk DRIVE3, das sich in dem Kassettenarchiv MANLIB befindet, aktualisieren, um es abzuhängen.

```
update drive manlib drive3 online=no
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE DRIVE

Befehl	Beschreibung
CLEAN DRIVE	Markiert ein Laufwerk für die Reinigung.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE DRIVE	Löscht ein Laufwerk aus einem Kassettenarchiv.
QUERY DRIVE	Zeigt Informationen zu Laufwerken an.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.

UPDATE FILESPACE (Knotenreplikationsregeln für Dateibereich aktualisieren)

Verwenden Sie diesen Befehl, um Replikationsregeln für den Dateibereich zu aktualisieren. Sie können auch die Replikation der Daten, für die eine Dateibereichsregel gilt, aktivieren oder inaktivieren.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Clientknoten mit dem zu aktualisierenden Dateibereich gehört.

Syntax

Anmerkungen:

1. Sie können keine Dateibereichs-ID angeben, wenn Sie Platzhalterzeichen für den Namen des Clientknotens verwenden.
2. Jede Regel kann nur einmal angegeben werden.
3. Sie müssen entweder den Parameter REPLRULE oder REPLSTATE in diesem Befehl angeben.
4. Die Regeln ACTIVE_DATA und ACTIVE_DATA_HIGH_PRIORITY sind nur gültig, wenn Sie `DATATYPE=BACKUP` angeben.

Parameter

Knotenname (Erforderlich)
: Gibt den Clientknoten an, zu dem der Dateibereich gehört. Dieser Name kann mithilfe von Platzhalterzeichen angegeben werden. Dateibereichs-IDs können jedoch zwischen Clientknoten für denselben Dateibereich unterschiedlich sein. Daher können Sie nicht Platzhalterzeichen für den Namen des Clientknotens und die Dateibereichs-ID als Wert für den Parameter NAMETYPE angeben.

Dateibereichsname (Erforderlich)
: Gibt den Namen des Dateibereichs an, der aktualisiert werden soll. Sie können Platzhalterzeichen oder eine durch Kommas dargestellte Liste verwenden, um Namen anzugeben.

  Bei einem Server, der über Clients mit Unicode-fähigen Dateibereichen verfügt, muss möglicherweise der Server die eingegebenen Dateibereichsnamen konvertieren. Beispielsweise muss der Server gegebenenfalls einen Namen aus der Zeichenumsetztabelle des Servers in Unicode konvertieren. Ausführliche Informationen befinden sich in der Beschreibung des Parameters NAMETYPE. Geben Sie nur

ein einzelnes Platzhalterzeichen für den Namen an, können Sie den Parameter CODETYPE verwenden, um die Operation auf Unicode-Dateibereiche oder Nicht-Unicode-Dateibereiche zu beschränken.

Bei Dateibereichsnamen muss die Groß-/Kleinschreibung berücksichtigt werden. Um die korrekte Schreibweise für den Dateibereich zu bestimmen, der aktualisiert werden soll, verwenden Sie den Befehl QUERY FILESPACE.

NAMEType
Gibt an, wie der Server die Dateibereichsnamen interpretieren soll, die Sie eingeben. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients verwenden, die über die Betriebssysteme Windows, Macintosh OS X und NetWare verfügen.
Verwenden Sie diesen Parameter nur, wenn Sie einen teilweise oder vollständig qualifizierten Dateibereichsnamen eingeben. Der Standardwert lautet SERVER. Sie können einen der folgenden Werte angeben:

SERVER
Der Server verwendet die Zeichenumsetztabelle des Servers, um Dateibereichsnamen zu interpretieren.
UNIcode
Der Server konvertiert Dateibereichsnamen aus der Serverzeichenumsetztabelle in die Zeichenumsetztabelle UTF-8. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Zeichenumsetztabelle des Servers ab. Die Konvertierung kann fehlschlagen, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind oder wenn der Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Schlägt die Konvertierung fehl, kann der Name Fragezeichen, Leerzeichen oder Auslassungen (...) enthalten.
FSID
Der Server interpretiert Dateibereichsnamen als Dateibereichs-IDs.

CODEType
Gibt den Typ der Dateibereiche an, die bei der Knotenreplikationsverarbeitung berücksichtigt werden sollen. Der Standardwert lautet BOTH. Dieser Standardwert bedeutet, dass Dateibereiche unabhängig von der Art der Zeichenumsetztabelle eingeschlossen werden.
Verwenden Sie diesen Parameter nur, wenn Sie ein einzelnes Platzhalterzeichen für den Dateibereichsnamen eingeben. Sie können einen der folgenden Werte angeben:

UNIcode
Gibt nur Dateibereiche an, die in Unicode sind.
NONUNIcode
Gibt nur Dateibereiche an, die nicht in Unicode sind.
BOTH
Gibt alle Dateibereiche unabhängig von der Art der Zeichenumsetztabelle an.

DATAType (Erforderlich)
Gibt den Datentyp an, für den eine Replikationsregel gilt. Bei der Angabe mehrerer Datentypen müssen die Datentypen durch Kommas und ohne Leerzeichen voneinander getrennt werden. Sie können die folgenden Werte angeben:

BACKup
Gibt den Typ 'Sicherungsdaten' an.
ARCHive
Gibt den Typ 'Archivierungsdaten' an.
SPACEManaged
Gibt den Typ 'Speicherverwaltete Daten' an.

REPLRule
Gibt die Replikationsregel an, die für einen Datentyp gilt. Sie können keine Platzhalterzeichen verwenden. Werden mehrere Datentypen angegeben, gilt die Replikationsregel für jeden Datentyp. Wenn Sie beispielsweise `DATATYPE=BACKUP,ARCHIVE` angeben, gilt die Replikationsregel für Sicherungsdaten und Archivierungsdaten.
Einschränkung: Der Parameter REPLRULE ist optional. Wird er jedoch nicht angegeben, müssen Sie den Parameter REPLSTATE angeben.

Sie können Replikationsregeln für normale Priorität oder Replikationsregeln für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

Beispiel: Angenommen, ein Dateibereich enthält aktive Sicherungsdaten und Archivierungsdaten. Die Replikation der aktiven Sicherungsdaten hat eine höhere Priorität als die der Archivierungsdaten. Um die aktiven Sicherungsdaten zu priorisieren, geben Sie `DATATYPE=BACKUP REPLRULE=ACTIVE_DATA_HIGH_PRIORITY` an. Um Archivierungsdaten eine normale Priorität zuzuordnen, geben Sie den Befehl UPDATE FILESPACE erneut aus und geben Sie `DATATYPE=ARCHIVE REPLRULE=ALL_DATA` an.

Sie können die folgenden Regeln angeben:

ALL_DATA
Repliziert Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.
ACTIVE_DATA
Repliziert nur die aktiven Sicherungsdaten in einem Dateibereich. Die Daten werden mit einer normalen Priorität repliziert.
Achtung: Wenn Sie ACTIVE_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

- Wenn eine frühere Serverversion als Version 7.1.1 auf dem Quellen- oder Zielreplikationsserver installiert ist.
- Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
- Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Serverversion vor Version 7.1.1 ausführen.

Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

ALL_DATA_HIGH_PRIORITY
: Repliziert Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Die Daten werden mit einer hohen Priorität repliziert.

ACTIVE_DATA_HIGH_PRIORITY

: Diese Regel entspricht der Replikationsregel ACTIVE_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden.

DEFAULT
: Daten werden gemäß der Clientknotenregel für den Datentyp repliziert.

: Beispiel: Angenommen, Sie möchten die Archivierungsdaten in allen Dateibereichen replizieren, die zu einem Clientknoten gehören. Die Replikation der Archivierungsdaten hat eine hohe Priorität. Eine Methode zur Ausführung dieser Task ist die Angabe von `DATATYPE=ARCHIVE REPLRULE=DEFAULT` für jeden Dateibereich. Stellen Sie sicher, dass die Clientreplikationsregel für Archivierungsdaten auf ALL_DATA_HIGH_PRIORITY oder DEFAULT gesetzt ist. Lautet die Clientreplikationsregel DEFAULT, muss die Serverreplikationsregel für Archivierungsdaten auf ALL_DATA_HIGH_PRIORITY gesetzt werden.

NONE
: Daten werden nicht repliziert. Sollen beispielsweise die speicherverwalteten Daten in einem Dateibereich nicht repliziert werden, geben Sie `DATATYPE=SPACEMANAGED REPLRULE=NONE` an.

REPLState
: Gibt den Replikationsstatus für einen Datentyp an. Wenn Sie mehrere Datentypen angegeben haben, gilt der Status für alle Datentypen. Haben Sie beispielsweise `DATATYPE=BACKUP,ARCHIVE` angegeben, gilt der Status für Sicherungs- und Archivierungsdaten.

: Der Parameter REPLSTATE ist optional. Wird er jedoch nicht angegeben, müssen Sie den Parameter REPLRULE angeben. Sie können einen der folgenden Werte für den Parameter REPLSTATE angeben:

: ENabled
: Gibt an, dass der Datentyp für die Replikation aktiviert ist.

: DISabled
: Gibt an, dass die Replikation erst stattfindet, wenn sie aktiviert wurde.

: PURGEdata
: Gibt an, dass Daten auf dem Zielreplikationsserver gelöscht werden. Der Typ der Daten, die gelöscht werden, ist der Datentyp, der mit dem Parameter DATATYPE angegeben wurde. Geben Sie beispielsweise `DATATYPE=BACKUP,ARCHIVE` und `REPLSTATE=PURGEDATA` an, werden Sicherungs- und Archivierungsdaten aus dem Dateibereich auf dem Zielreplikationsserver gelöscht.

: Nach dem Löschen der Daten wird der Parameter REPLSTATE auf DISABLED gesetzt. Damit wird eine zukünftige Replikation des Datentyps oder der Datentypen verhindert. Die Replikationsregel für den Datentyp wird auf DEFAULT gesetzt.

: Hinweis: Mit der PURGEDATA-Verarbeitung werden keine Dateibereiche gelöscht. Nur Daten werden gelöscht. Der Dateibereich wird in der Ausgabe des Befehls QUERY OCCUPANCY als leer angezeigt.

Beispiel: Replikationsregeln für zwei Datentypen aktualisieren

NODE1 verfügt über drei Dateibereiche: /a, /b und /c. Die Replikationsregeln für alle Dateibereiche sind auf ALL_DATA gesetzt. Sie möchten jedoch die Sicherungs- und Archivierungsdaten im Dateibereich /a replizieren, bevor die Daten in den anderen Dateibereichen repliziert werden.

```
update filespace node1 /a datatype=backup,archive replrule=
       all_data_high_priority
```

Beispiel: Replikationsregeln für zwei Datentypen aktualisieren

NODE2 verfügt über zwei Dateibereiche: /a und /b. Sie möchten die Replikation aller Daten im Dateibereich /b vorübergehend aussetzen.

```
update filespace node2 /b datatype=backup,archive,spacemanaged
 replstate=disabled
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE FILESPACE

Befehl	Beschreibung

Befehl	Beschreibung
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
SET REPLRETENTION	Gibt den Aufbewahrungszeitraum für Replikationsprotokollsätze an.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.
UPDATE REPLRULE	Aktiviert oder inaktiviert Replikationsregeln.
VALIDATE REPLICATION	Überprüft die Replikation für Dateibereiche und Datentypen.

UPDATE LIBRARY (Kassettenarchiv aktualisieren)

Verwenden Sie diesen Befehl, um eine Kassettenarchivdefinition zu aktualisieren.

AIX-BetriebssystemeWindows-BetriebssystemeUm den Einheitennamen, die ACS-Nummer oder den Pfadnamen des externen Managers eines Kassettenarchivs zu aktualisieren, müssen Sie den Befehl UPDATE PATH verwenden.

Linux-BetriebssystemeUm den Einheitennamen oder den Pfadnamen des externen Managers eines Kassettenarchivs zu aktualisieren, müssen Sie den Befehl UPDATE PATH verwenden.

Syntax- und Parameterbeschreibungen sind für die folgenden Kassettenarchivtypen verfügbar.

- UPDATE LIBRARY (349X-Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (ACSLS-Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (Externes Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (Kassettenarchiv FILE aktualisieren)
- UPDATE LIBRARY (Manuelles Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (SCSI-Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (Gemeinsam genutztes Kassettenarchiv aktualisieren)
- UPDATE LIBRARY (VTL-Speicherarchiv aktualisieren)

Ausführliche und aktuelle Informationen zur Kassettenarchivunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Windows-Betriebssysteme

Um Banddatenträger in SCSI-Speicherarchiven automatisch zu kennzeichnen, verwenden Sie den Parameter AUTOLABEL in den Befehlen DEFINE LIBRARY und UPDATE LIBRARY. Wird dieser Parameter verwendet, ist es nicht erforderlich, eine Gruppe von Bändern vorab zu kennzeichnen. Außerdem ist die Verwendung dieses Parameters effizienter als die Verwendung des Befehls LABEL LIBVOLUME, der es erfordert, dass Datenträger separat bereitgestellt werden. Wenn Sie den Parameter AUTOLABEL verwenden, müssen Sie Bänder zurückstellen, indem Sie CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME angeben.

Ein Kennsatz darf keine eingebetteten Leerzeichen oder Punkte enthalten und muss gültig sein, wenn er als Dateiname auf den Datenträgern verwendet wird.

Sie müssen CD-ROM-, Zip- oder Jaz-Datenträger mit den Dienstprogrammen des Einheitenherstellers oder den Windows-Dienstprogrammen kennzeichnen, da IBM Spectrum Protect keine Dienstprogramme zum Formatieren oder Kennzeichnen dieser Datenträgertypen bereitstellt. Die Dienstprogramme des Betriebssystems schließen das Plattenverwaltungsprogramm (Disk Administrator) (eine grafische Benutzerschnittstelle) und den Befehl zum Zuordnen von Kennsätzen ein.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE LIBRARY

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.

Befehl	Beschreibung
CHECKIN LIBVOLUME	Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.
DELETE DRIVE	Löscht ein Laufwerk aus einem Kassettenarchiv.
DELETE LIBRARY	Löscht ein Kassettenarchiv.
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
LABEL LIBVOLUME	Kennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.
QUERY DRIVE	Zeigt Informationen zu Laufwerken an.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE DRIVE	Ändert die Attribute eines Laufwerks.
UPDATE LIBVOLUME	Ändert den Status eines Speicherdatenträgers.
UPDATE PATH	Ändert die zu einem Pfad gehörigen Attribute.

UPDATE LIBRARY (349X-Kassettenarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein 349X-Kassettenarchiv zu aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate LIBRary--Speicherarchivname--+--------------------+--->
                                       '-SHAREd--=----Yes---'

>--+-------------------------+---------------------------------->
   '-RESETDrives--=--+-Yes-+-'
                     '-No--'

>--+-----------------------------+----------------------------->
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'

>--+---------------------------------+-------------------------><
   '-WORMSCRatchcategory--=--Anzahl-'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

SHAREd
: Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.
: Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

AUTOLabel
: Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No
: Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes
: Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE
: Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

WORMSCRatchcategory
: Gibt die Kategorienummer an, die für WORM-Arbeitsdatenträger in dem Kassettenarchiv verwendet werden soll. Dieser Parameter ist erforderlich, wenn WORM-Datenträger verwendet werden. Es kann eine Zahl von 1 bis 65279 angegeben werden. Diese Zahl muss eindeutig sein. Sie kann nicht mit anderen Anwendungen oder definierten Kassettenarchiven gemeinsam genutzt werden, und sie muss sich von den anderen Kategorienummern in diesem Kassettenarchiv unterscheiden. Dieser Parameter ist nur bei Verwendung von WORM-Datenträgern 3592 gültig.
Einschränkung: Dieser Parameter kann nur aktualisiert werden, wenn der Parameter WORM für die Einheitenklasse auf YES gesetzt ist und für WORMSCRATCHCATEGORY gegenwärtig kein Wert definiert ist.

RESETDrives
: Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

 AIX-Betriebssysteme  Windows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

Konfiguration der Speicherarchiveinheit	**Verhalten für persistente Reserve**
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt.	Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.	Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben.

AIX-BetriebssystemeWindows-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

No
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

 Linux-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

No
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

Beispiel: Neue Einheiten einem gemeinsam genutzten Kassettenarchiv hinzufügen

Das gemeinsam benutzte 3494-Kassettenarchiv 3494LIB2 mit neuen Einheitennamen aktualisieren.AIX-Betriebssysteme Linux-Betriebssysteme

```
update library 3494lib2 device=/dev/lmcp1,/dev/lmcp2,/dev/lmcp3
```

Windows-Betriebssysteme

```
update library 3494lib device=lb3.0.0.0,lb4.0.0.0,lb5.0.0.0
```

UPDATE LIBRARY (ACSLS-Kassettenarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein ACSLS-Kassettenarchiv zu aktualisieren.

Berechtigungsklasse

Windows-BetriebssystemeUm ACSLS-Funktionen verwenden zu können, ist die Installation von StorageTek Library Attach-Software erforderlich.

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate LIBRary--Speicherarchivname--+--------------------+--->
                                       '-SHAREd--=----Yes---'

>--+-------------------------+---------------------------------->
   '-RESETDrives--=--+-Yes-+-'
                     '-No--'

>--+-----------------------------+--+------------------+-------><
   '-AUTOLabel--=--+-No---------+-'  '-ACSID--=--Nummer-'
                   +-Yes--------+
                   '-OVERWRITE-'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

SHAREd
: Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.
  Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

RESETDrives
: Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

  AIX-BetriebssystemeWindows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

  Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

  Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

  - Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
  - Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
  - Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

  In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

Konfiguration der Speicherarchiveinheit	Verhalten für persistente Reserve

Konfiguration der Speicherarchiveinheit	Verhalten für persistente Reserve
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt.	Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.	Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben.

 AIX-Betriebssysteme  Windows-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

No
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

 Linux-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

No
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

AUTOLabel
: Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No
: Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes
: Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE
: Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

ACSID (Erforderlich)
: Gibt die Nummer dieses StorageTek-Kassettenarchivs an, das von ACSSA (Automatic Cartridge System System Administrator) zugeordnet wird. Hierbei kann es sich um eine Zahl von 0 bis 126 handeln. Geben Sie den Befehl QUERY ACS auf dem System aus, um die Nummer für die Kassettenarchiv-ID abzufragen. Dieser Parameter ist erforderlich.

Die StorageTek-Dokumentation enthält weitere Informationen.

Beispiel: Eine ID-Nummer für ein ACSLS-Kassettenarchiv aktualisieren

Das ACSLS-Kassettenarchiv ACSLSLIB mit einer neuen ID-Nummer aktualisieren.

```
update library acslslib acsid=1
```

UPDATE LIBRARY (Externes Kassettenarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein externes Kassettenarchiv zu aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate LIBRary--Speicherarchivname--------------------------->

>--+-----------------------------+----------------------------><
   '-AUTOLabel--=--+-No---------+-'
                   +-Yes--------+
```

```
                    '-OVERWRITE-'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

AUTOLabel
: Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

  Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

  No
  : Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

  Yes
  : Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

  OVERWRITE
  : Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

Beispiel: Den Pfadnamen eines externen Kassettenarchivs aktualisieren

Das externe Kassettenarchiv EXTLIB mit einem neuen Pfadnamen für den Datenträgermanager aktualisieren.  AIX-Betriebssysteme
 Linux-Betriebssysteme

```
update library extlib externalmanager=/v/server/mediamanager
```

 Windows-Betriebssysteme

```
update library extlib externalmanager=c:\server\mediamanager
```

UPDATE LIBRARY (Kassettenarchiv FILE aktualisieren)

Verwenden Sie diese Syntax, um ein Kassettenarchiv FILE zu aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate LIBRary--Speicherarchivname--+--------------------+--><
                                       '-SHAREd--=----Yes---'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

SHAREd
: Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.
  Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

Beispiel: Ein Kassettenarchiv FILE aktualisieren, das gemeinsam genutzt werden soll

Ein Kassettenarchiv FILE mit dem Namen FILE2 aktualisieren, damit es gemeinsam genutzt wird.

```
update library file2 shared=yes
```

UPDATE LIBRARY (Manuelles Kassettenarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein manuelles Kassettenarchiv zu aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate LIBRary--Speicherarchivname--------------------------->

>--+-------------------------+---------------------------------->
   '-RESETDrives--=--+-Yes-+-'
                     '-No--'

>--+-----------------------------+----------------------------><
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

RESETDrives
: Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

   AIX-Betriebssysteme  Windows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

   Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

  Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

  - Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
  - Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
  - Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

   AIX-BetriebssystemeWindows-Betriebssysteme

  Yes
  : Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

  No
  : Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

   Linux-Betriebssysteme

  Yes
  : Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

  No
  : Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

  Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

AUTOLabel
: Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

  Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

  No
  : Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

  Yes
  : Gibt an, dass der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

  OVERWRITE
  : Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

UPDATE LIBRARY (SCSI-Kassettenarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein SCSI-Kassettenarchiv zu aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate LIBRary--Speicherarchivname---------------------------->

>----LIBType--=--+-SCSI-+----+--------------------+-------------->
                 '-VTL--'    '-SHAREd--=----Yes---'

>--+------------------------+---------------------------------->
   '-RESETDrives--=--+-Yes-+-'
                     '-No--'

>--+-----------------------------+------------------------------>
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'

>--+-----------------------------+------------------------------>
   '-RELABELSCRatch--=--+-No--+-'
                        '-Yes-'

>--+-----------------------------+------------------------------><
   '-SERial--=--+-Seriennummer-+-'
                '-AUTODetect---'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das aktualisiert werden soll.

LIBType (Erforderlich)
: Gibt den Kassettenarchivtyp an, der aktualisiert werden soll. Gültige Werte:

  VTL
  : Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt, der durch ein virtuelles Bandarchiv (Virtual Tape Library - VTL) dargestellt wird. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet IBM Spectrum Protect die Datenträgerwechslereinheit. Dieser Wert ist wirksam, wenn er für Speicherarchive mit dem aktuellen Speicherarchivtyp SCSI angegeben wird.
    Anmerkung: Die Auswahl des Kassettenarchivtyps VTL setzt voraus, dass die folgenden Bedingungen zutreffen:

    - Ihre Umgebung enthält keine gemischten Datenträger.
    - Pfade sind zwischen allen Laufwerken in dem Kassettenarchiv und allen definierten Servern, einschließlich Speicheragenten, die das Kassettenarchiv verwenden, definiert

    Wenn beide Bedingungen nicht zutreffen, kann die Leistung in demselben Maße wie beim Speicherarchivtyp SCSI abnehmen. Dies ist besonders in Zeiten hoher Belastung der Fall, wenn die meisten Laufwerke gleichzeitig verwendet werden.

  SCSI
  : Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet IBM Spectrum Protect die Datenträgerwechslereinheit. Dieser Wert ist wirksam, wenn er für Speicherarchive mit dem aktuellen Speicherarchivtyp VTL angegeben wird.

SHAREd
: Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.
  Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

RESETDrives
: Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

 AIX-Betriebssysteme  Windows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

 Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

- Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
- Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
- Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

In der folgenden Tabelle sind die drei möglichen Konfigurationen für Laufwerke beschrieben, die an NAS-Einheiten angeschlossen werden können.

Tabelle 1. Konfigurationen für Laufwerke, die an NAS-Einheiten angeschlossen sind

Konfiguration der Speicherarchiveinheit	**Verhalten für persistente Reserve**
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und die Bandlaufwerke werden vom Server und der NAS-Einheit gemeinsam genutzt.	Die Zurückstellung der Laufwerkreservierung wird unterstützt, wenn die NAS-Einheit die persistente Reserve unterstützt und diese aktiviert ist. Weitere Informationen zum Definieren der persistenten Reserve finden Sie in der Dokumentation für Ihre NAS-Einheit.
Die Speicherarchiveinheit wird an den IBM Spectrum Protect-Server angeschlossen, und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.	Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben.
Die Speicherarchiveinheit wird an die NAS-Einheit angeschlossen und der Zugriff erfolgt indirekt durch NDMP (Network Data Management Protocol), und auf die Bandlaufwerke wird nur von der NAS-Einheit zugegriffen.	Die Zurückstellung der Laufwerkreservierung wird nicht unterstützt. Wenn Sie die persistente Reserve auf der NAS-Einheit für diese Laufwerke aktivieren und eine Reservierung von der NAS-Einheit definiert ist, aber nie aufgehoben wird, müssen Sie eine andere Methode verwenden, um die Reservierung aufzuheben.

 AIX-Betriebssysteme  Windows-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

No
: Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

 Linux-Betriebssysteme

Yes
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

No
: Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

AUTOLabel
: Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No
: Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes
: Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE
: Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

SERial
: Gibt die Seriennummer des Speicherarchivs an, das aktualisiert wird. Dieser Parameter ist wahlfrei. Gültige Werte sind:

Seriennummer
: Gibt die Seriennummer des Speicherarchivs an, das aktualisiert wird.

Wurde bereits ein Pfad zu diesem Speicherarchiv definiert, wird die eingegebene Nummer mit der Nummer verglichen, die von IBM Spectrum Protect erkannt wurde. Stimmen die Nummern nicht überein, schlägt der Befehl fehl. Wurde kein Pfad definiert, wird diese Seriennummer beim Definieren eines Pfads geprüft.

AUTODetect
Gibt an, dass die Seriennummer automatisch von IBM Spectrum Protect erkannt und verwendet wird, wenn bereits ein Pfad zu diesem Speicherarchiv definiert wurde.

Wurde kein Pfad zu diesem Kassettenarchiv definiert, wird die Seriennummer nicht erkannt.

RELABELSCRatch
Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden. Wird dieser Parameter auf YES gesetzt, wird eine Operation LABEL LIBVOLUME gestartet und der vorhandene Datenträgerkennsatz wird überschrieben. Dieser Parameter ist optional und für die Verwendung mit einem VTL-Speicherarchiv (VTL = Virtual Tape Library) bestimmt.
Anmerkung: Haben Sie sowohl virtuelle als auch reale Datenträger in Ihrem VTL, werden beide Typen mit einem neuen Kennsatz versehen, wenn dieser Parameter aktiviert ist. Enthält das VTL reale Datenträger, kann die Angabe dieser Option Auswirkungen auf die Leistung haben.

No
Gibt an, dass der Server Datenträger nicht mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

Yes
Gibt an, dass der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

UPDATE LIBRARY (Gemeinsam genutztes Kassettenarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein gemeinsam genutztes Kassettenarchiv zu aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate LIBRary--Speicherarchivname---------------------------->

>--PRIMarylibmanager--=--Servername----------------------------><
```

Parameter

Speicherarchivname (Erforderlich)
Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

PRIMarylibmanager
Gibt den Namen des Servers an, der für die Steuerung des Zugriffs auf Kassettenarchivressourcen zuständig ist. Sie müssen diesen Server mit dem Befehl DEFINE SERVER definieren, bevor Sie ihn als Kassettenarchivmanager verwenden können.

Beispiel: Den Kassettenarchivmanagerserver für ein Kassettenarchiv ändern

Für einen Kassettenarchivclientserver den Namen des Kassettenarchivmanagerservers in CASTOR ändern.

```
update library ltolib primarylibmanager=castor
```

UPDATE LIBRARY (VTL-Speicherarchiv aktualisieren)

Verwenden Sie diese Syntax, um ein Speicherarchiv zu aktualisieren, das als VTL definiert ist.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate LIBRary--Speicherarchivname---------------------------->
```

```
>----LIBType--=---+-VTL--+----+--------------------+------------>
                  '-SCSI-'    '-SHAREd--=----Yes---'

>--+------------------------+-------------------------------->
   '-RESETDrives--=--+-Yes-+-'
                     '-No--'

>--+----------------------------+------------------------------>
   '-AUTOLabel--=--+-No--------+-'
                   +-Yes-------+
                   '-OVERWRITE-'

>--+----------------------------+------------------------------>
   '-RELABELSCRatch--=---+-No--+-'
                         '-Yes-'

>--+----------------------------+----------------------------><
   '-SERial--=--+-Seriennummer-+-'
                '-AUTODetect---'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Kassettenarchivs an, das definiert werden soll. Die maximale Länge dieses Namens beträgt 30 Zeichen.

LIBType (Erforderlich)
: Gibt den Typ des Speicherarchivs an, das definiert wird. Gültige Werte:

  SCSI
  : Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet IBM Spectrum Protect die Datenträgerwechslereinheit. Dieser Wert ist wirksam, wenn er für Speicherarchive mit dem aktuellen Speicherarchivtyp VTL angegeben wird.

  VTL
  : Gibt an, dass das Speicherarchiv über einen SCSI-gesteuerten Datenträgerwechsler verfügt, der durch ein virtuelles Bandarchiv (Virtual Tape Library - VTL) dargestellt wird. Zum Bereitstellen von Datenträgern in Laufwerken bei diesem Typ von Speicherarchiv verwendet IBM Spectrum Protect die Datenträgerwechslereinheit. Dieser Wert ist wirksam, wenn er für Speicherarchive mit dem aktuellen Speicherarchivtyp SCSI angegeben wird.
  Anmerkung: Wählen Sie den Speicherarchivtyp VTL nur aus, wenn die folgenden Bedingungen zutreffen:

  - Ihre Umgebung enthält keine gemischten Datenträger.
  - Pfade sind zwischen allen Laufwerken in dem Speicherarchiv und allen definierten Servern, einschließlich Speicheragenten, die das Speicherarchiv verwenden, definiert.

  Wenn beide Bedingungen nicht zutreffen, kann die Leistung in demselben Maße wie beim Speicherarchivtyp SCSI abnehmen. Dies ist besonders in Zeiten hoher Belastung der Fall, wenn die meisten Laufwerke gleichzeitig verwendet werden.

SHAREd
: Gibt an, dass dieses Speicherarchiv mit anderen Servern in einem Speicherbereichsnetz (SAN) gemeinsam genutzt wird. Dieser Befehl muss von dem Server ausgegeben werden, der als primärer Speicherarchivmanager für das gemeinsam genutzte Speicherarchiv definiert ist. Dieser Parameter ist für Speicherarchive erforderlich, die für einen Speicherarchivmanager definiert sind, und ist für Speicherarchive erforderlich, die für NDMP-Operationen verwendet werden. Geben Sie SHARED=YES an, um ein Speicherarchiv zu aktualisieren, das gegenwärtig nicht gemeinsam genutzt wird.
  Wichtig: Hat ein Speicherarchiv einen Pfad von einer Einheit zum Versetzen von Daten (beispielsweise einem NAS-Dateiserver), aber keine Verbindung zu dem Server, kann das Speicherarchiv nicht mit einem anderen Server gemeinsam genutzt werden.

RESETDrives
: Gibt an, ob der Server eine Laufwerkreservierung mit persistenter Reserve zurückstellt, wenn der Server erneut gestartet wird oder wenn die Verbindung für einen Kassettenarchivclient oder einen Speicheragenten erneut hergestellt wird.

  AIX-BetriebssystemeWindows-BetriebssystemeWird die persistente Reserve nicht unterstützt, führt der Server eine Zurücksetzung des Pfads auf die Zieleinheit aus.

  Linux-BetriebssystemeWird die persistente Reserve nicht unterstützt, kann der Server den Pfad nicht auf die Zieleinheit zurücksetzen.

  Für die Unterstützung der persistenten Reservierung gelten die folgenden Einschränkungen:

  - Wenn Sie den IBM Spectrum Protect-Einheitentreiber verwenden, wird die persistente Reserve nur für einige Bandlaufwerke unterstützt. Ausführliche Informationen befinden sich in Technote 1470319.
  - Wenn Sie den IBM® Einheitentreiber verwenden, muss die persistente Reserve auf der Einheitentreiberebene aktiviert werden. Informationen zur Treiberkonfiguration befinden sich im *IBM Tape Device Drivers Installation and User's Guide*.
  - Wenn Sie ein virtuelles Bandarchiv verwenden, das ein unterstütztes Laufwerk emuliert, unterstützt es möglicherweise nicht die persistente Reserve.

  AIX-BetriebssystemeWindows-Betriebssysteme

Yes
Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung verwendet wird.

No
Gibt an, dass eine Laufwerkzurückstellung durch persistente Reserve oder eine Zielzurücksetzung nicht verwendet wird. In einer Clusterumgebung muss der Parameter RESETDRIVES bei SHARED=NO auf YES gesetzt werden.

 Linux-Betriebssysteme

Yes
Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve verwendet wird.

No
Gibt an, dass eine Laufwerkzurückstellung mit persistenter Reserve nicht verwendet wird.

Anmerkung: Ein Kassettenarchivmanager kann eine Laufwerkreservierung nicht unterbrechen, wenn das System, das über die Laufwerkreservierung verfügt, nicht für die Verwendung der persistenten Reservierung konfiguriert ist.

AUTOLabel
Gibt an, ob der Server versucht, Banddatenträger automatisch zu kennzeichnen. Dieser Parameter ist wahlfrei.

Um diese Option zu verwenden, müssen Sie die Bänder mit CHECKLABEL=BARCODE im Befehl CHECKIN LIBVOLUME zurückstellen.

No
Gibt an, dass der Server nicht versucht, Datenträger zu kennzeichnen.

Yes
Gibt an, daß der Server nur Datenträger ohne Kennsatz mit einem Kennsatz versieht.

OVERWRITE
Gibt an, dass der Server versucht, einen vorhandenen Kennsatz zu überschreiben. Der Server überschreibt vorhandene Kennsätze *nur dann*, wenn sowohl der vorhandene Kennsatz als auch das Barcodeetikett noch nicht in einem Serverspeicherpool oder einer Datenträgerhistoryliste definiert sind.

RELABELSCRatch
Gibt an, ob der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht wurden und wieder als Arbeitsdatenträger verwendet werden. Wird dieser Parameter auf YES gesetzt, wird eine Operation LABEL LIBVOLUME gestartet und der vorhandene Datenträgerkennsatz wird überschrieben.
Anmerkung: Haben Sie sowohl virtuelle als auch reale Datenträger in Ihrem VTL, werden beide Typen mit einem neuen Kennsatz versehen, wenn dieser Parameter aktiviert ist. Enthält das VTL reale Datenträger, kann die Angabe dieser Option Auswirkungen auf die Leistung haben.

Yes
Gibt an, dass der Server Datenträger mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

No
Gibt an, dass der Server Datenträger nicht mit einem neuen Kennsatz versieht, die gelöscht und wieder als Arbeitsdatenträger verwendet werden.

SERial
Gibt die Seriennummer des Speicherarchivs an, das aktualisiert wird. Dieser Parameter ist wahlfrei. Gültige Werte sind:

Seriennummer
Gibt die Seriennummer des Speicherarchivs an, das aktualisiert wird.

Wurde bereits ein Pfad zu diesem Speicherarchiv definiert, wird die eingegebene Nummer mit der Nummer verglichen, die von IBM Spectrum Protect erkannt wurde. Stimmen die Nummern nicht überein, schlägt der Befehl fehl. Wurde kein Pfad definiert, wird diese Seriennummer beim Definieren eines Pfads geprüft.

AUTODetect
Gibt an, dass die Seriennummer automatisch von IBM Spectrum Protect erkannt und verwendet wird, wenn bereits ein Pfad zu diesem Speicherarchiv definiert wurde.

Wurde kein Pfad zu diesem Speicherarchiv definiert, wird die Seriennummer nicht erkannt.

UPDATE LIBVOLUME (Status eines Speicherdatenträgers ändern)

Mit diesem Befehl kann der Status eines Speicherdatenträgers mit sequenziellem Zugriff in einem Speicherarchiv geändert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate LIBVolume--Speicherarchivname--Datenträgername--STATus--=--+-PRIvate-+-->
                                                                    '-SCRatch-'

>--+----------------------+-----------------------------------><
   '-OWNer--=--Servername-'
```

Parameter

Speicherarchivname (Erforderlich)
: Gibt den Namen des Speicherarchivs an.

Datenträgername (Erforderlich)
: Gibt den Namen des Speicherdatenträgers an.

STATus (Erforderlich)
: Gibt eine Änderung im Status eines Speicherdatenträgers an. Gültige Werte sind:

  PRIvate
  : Gibt an, dass der Server den Speicherdatenträger in einen privaten Datenträger ändert.

  SCRatch
  : Gibt an, dass der Server den Speicherdatenträger in einen Arbeitsdatenträger ändert.

  Einschränkung: Sie können nicht den Status eines Datenträgers von 'privat' in 'Arbeitsdatenträger' ändern, wenn der Datenträger zu einem Speicherpool gehört oder in der Protokolldatei für Datenträger definiert ist. Sie können den Status ändern, wenn beim Zurückstellen von Datenträgern in das Speicherarchiv ein Fehler unterlaufen ist und den Datenträgern der falsche Status zugeordnet wurde.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeOWNer
: AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeGibt an, welcher Server der Eigner eines privaten Datenträgers in einem Kassettenarchiv ist, das in einem SAN gemeinsam benutzt wird. Der Eigner eines privaten Datenträgers in einem gemeinsam benutzten Kassettenarchiv (SAN) kann geändert werden, wenn der Befehl von dem Kassettenarchivmanager-Server ausgegeben wird. Wird dieser Parameter nicht angegeben, ist der Kassettenarchivmanager-Server der Eigner des privaten Datenträgers. Wichtig: Verwenden Sie nicht OWNER als Wert für Arbeitsdatenträger. Sie können OWNER jedoch verwenden, wenn Sie einen Arbeitsdatenträger in einen privaten Datenträger ändern.

Beispiel: Den Status eines Datenträgers aktualisieren

Für den Datenträger WPDV00 im Speicherarchiv AUTO soll der Status PRIVATE vergeben werden.

```
update libvolume auto wpdv00 status=private
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE LIBVOLUME

Befehl	Beschreibung
AUDIT LIBRARY	Stellt sicher, dass sich ein automatisiertes Kassettenarchiv in einem konsistenten Status befindet.
CHECKIN LIBVOLUME	Stellt einen Speicherdatenträger in ein automatisiertes Kassettenarchiv.
CHECKOUT LIBVOLUME	Nimmt einen Speicherdatenträger aus einem automatisierten Kassettenarchiv.
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeLABEL LIBVOLUME	AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeKennzeichnet Datenträger in manuellen oder automatisierten Kassettenarchiven.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.
QUERY LIBVOLUME	Zeigt Informationen zu einem Datenträger im Kassettenarchiv an.

UPDATE MACHINE (Maschineninformationen aktualisieren)

Mit diesem Befehl können Maschinendaten aktualisiert werden.Diese Informationen werden in der Wiederherstellungsplandatei berücksichtigt, um den Benutzer bei der Wiederherstellung der Client-Maschinen zu unterstützen.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-UPDate MACHine--Maschinenname--------------------------------->

>--+-------------------------------+--+----------------------+--->
   '-DESCription--=--Beschreibung-'  '-BUilding--=--Gebäude-'

>--+----------------------+--+---------------+------------------->
   '-FLoor--=--Stockwerk-'  '-ROom--=--Raum-'

>--+--------------------+--+------------------------+----------><
   '-PRIority--=--Zahl-'  '-ADSMServer--=--+-Yes-+-'
                                           '-No--'
```

Parameter

Maschinenname (Erforderlich)
: Gibt den Namen der Maschine an, die aktualisiert werden soll.

DESCription
: Gibt eine Beschreibung der Maschine an. Dieser Parameter ist wahlfrei. Der Text kann bis zu 255 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.Soll vorhandener Text entfernt werden, geben Sie eine Nullzeichenfolge ("") an.

BUilding
: Gibt den Namen oder die Nummer des Gebäudes an, in dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.Soll vorhandener Text entfernt werden, geben Sie eine Nullzeichenfolge ("") an.

FLoor
: Gibt den Namen oder die Nummer des Stockwerks an, auf dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.Soll vorhandener Text entfernt werden, geben Sie eine Nullzeichenfolge ("") an.

ROom
: Gibt den Namen oder die Nummer des Raums an, in dem sich diese Maschine befindet. Dieser Parameter ist wahlfrei. Der Text kann bis zu 16 Zeichen umfassen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.Soll vorhandener Text entfernt werden, geben Sie eine Nullzeichenfolge ("") an.

PRIority
: Gibt die Zurückschreibungspriorität für die Maschine als ganze Zahl von 1 bis 99 an. Die höchste Priorität ist 1. Dieser Parameter ist wahlfrei. Verwenden Sie diesen Wert für die Vergabe von Prioritäten bei der Wiederherstellung von Clientmaschinen.

ADSMServer
: Gibt an, ob die Maschine einen IBM Spectrum Protect-Server enthält. Dieser Parameter ist wahlfrei. Gültige Werte:

  No
  : Diese Maschine enthält keinen IBM Spectrum Protect-Server.

  Yes
  : Diese Maschine enthält einen IBM Spectrum Protect-Server. Es kann nur eine Maschine definiert werden, die einen IBM Spectrum Protect-Server enthält.

Beispiel: Informationen zu einer bestimmten Maschine aktualisieren

In die Maschineninformationen von DISTRICT5 soll ein Eintrag aufgenommen werden, der besagt, dass die Maschine den Server enthält.

```
update machine district5 adsmserver=yes
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE MACHINE

Befehl	Beschreibung
DEFINE MACHINE	Definiert eine Maschine für DRM.
DELETE MACHINE	Löscht eine Maschine.
INSERT MACHINE	Fügt Maschinenkenndaten oder Wiederherstellungsanweisungen in die IBM Spectrum Protect-Datenbank ein.
QUERY MACHINE	Zeigt Informationen über Maschinen an.

UPDATE MGMTCLASS (Verwaltungsklasse aktualisieren)

Mit diesem Befehl kann eine Verwaltungsklasse geändert werden. Um Clients die Verwendung der aktualisierten Verwaltungsklasse zu ermöglichen, muß die Maßnahmengruppe aktiviert werden, die die Verwaltungsklasse enthält.

Wichtig: Der Befehl UPDATE MGMTCLASS schlägt fehl, wenn ein Kopienspeicherpool als Zielort für Dateien angegeben wird, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

Syntax

```
>>-UPDate MGmtclass---------------------------------------------->

>--Domänenname--Name_der_Maßnahmengruppe--Klassenname----------->

>--+-------------------------------------+----------------------->
   '-SPACEMGTECHnique--=--+-AUTOmatic-+-'
                          +-SELective-+
                          '-NONE------'

>--+------------------------+---------------------------------->
   '-AUTOMIGNonuse--=--Tage-'

>--+-----------------------------+------------------------------>
   '-MIGREQUIRESBkup--=--+-Yes-+-'
                         '-No--'

>--+-----------------------------+------------------------------>
   '-MIGDESTination--=--Poolname-'

>--+-------------------------------+---------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Verwaltungsklasse gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, zu der die Verwaltungsklasse gehört. Eine Verwaltungsklasse, die zu der aktiven Maßnahmengruppe (ACTIVE) gehört, kann nicht aktualisiert werden.

Klassenname (Erforderlich)
: Gibt die Verwaltungsklasse an, die aktualisiert werden soll.

SPACEMGTECHnique
: Gibt an, ob eine Datei, die diese Verwaltungsklasse verwendet, für die Umlagerung ausgewählt werden kann. Dieser Parameter ist wahlfrei. Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungsclients. Gültige Werte:

  AUTOmatic
  : Gibt an, dass die Datei sowohl für die automatische Umlagerung als auch für die selektive Umlagerung auswählbar ist.

  SELective
  : Gibt an, dass die Datei nur für die selektive Umlagerung auswählbar ist.

  NONE
  : Gibt an, dass die Datei nicht für die Umlagerung auswählbar ist.

AUTOMIGNonuse
: Gibt die Anzahl Tage an, die nach der letzten Verwendung einer Datei verstreichen müssen, bevor die Datei für die automatische Umlagerung ausgewählt werden kann. Dieser Parameter ist wahlfrei. Lautet der Wert für SPACEMGTECHNIQUE nicht AUTOMATIC, ignoriert der Server dieses Attribut. Zulässige Werte sind ganze Zahlen von 0 bis 9999.

  Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungsclients.

MIGREQUIRESBkup
: Gibt an, ob eine Sicherungsversion einer Datei vorhanden sein muß, damit die Datei umgelagert werden kann. Dieser Parameter ist wahlfrei. Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungsclients. Gültige Werte:

  Yes
  : Gibt an, dass eine Sicherungsversion vorhanden sein muss.

  No

Gibt an, dass eine Sicherungsversion wahlfrei ist.

MIGDESTination
: Gibt den primären Speicherpool an, in dem der Server anfänglich Dateien speichert, die von IBM Spectrum Protect for Space Management-Clients umgelagert werden. Dieser Parameter ist nur für IBM Spectrum Protect for Space Management-Clients gültig, nicht für Clients für Sichern/Archivieren oder Anwendungsclients.

  Der Befehl schlägt fehl, wenn ein Kopienspeicherpool als Zielort angegeben wird.

DESCription
: Beschreibung der Verwaltungsklasse. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine Nullzeichenfolge ("") anzugeben.

Beispiel: Die Maßnahmendomäne und den Speicherpool einer bestimmten Verwaltungsklasse aktualisieren

Für die Verwaltungsklasse ACTIVEFILES in Maßnahmengruppe VACATION in der Maßnahmendomäne EMPLOYEE_RECORDS den Speicherpool ändern, in dem umgelagerte Dateien gespeichert werden.

```
update mgmtclass employee_records vacation
activefiles migdestination=diskpool2
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE MGMTCLASS

Befehl	Beschreibung
ASSIGN DEFMGMTCLASS	Ordnet eine Verwaltungsklasse als Standardklasse für eine angegebene Maßnahmengruppe zu.
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
DELETE MGMTCLASS	Löscht eine Verwaltungsklasse und ihre Kopiengruppen aus einer Maßnahmendomäne und einer Maßnahmengruppe.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.

UPDATE NODE (Attribute eines Knotens aktualisieren)

Verwenden Sie diesen Befehl, um die Attribute eines registrierten Knotens zu ändern.

Sie müssen den Befehl RENAME NODE verwenden, um den Namen eines registrierten Knotens zu ändern.

Wenn Sie die Knotenauthentifizierungsmethode oder die Einstellung für SSLREQUIRED des Knotens aktualisieren und ein Administrator mit demselben Namen vorhanden ist, ändern sich diese Einstellungen für die Administrator-ID.

Sie müssen über die Berechtigung auf Systemebene verfügen, um die Knotenauthentifizierungsmethode oder die Einstellung für SSLREQUIRED des Knotens und eine Administrator-ID mit demselben Namen zu aktualisieren. Wenn die Administrator-ID mit demselben Namen die Clienteignerberechtigung über den Knoten hat, der aktualisiert wird, ist die Berechtigung auf Systemebene nicht erforderlich. Sie müssen über uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne verfügen, zu der der Clientknoten gehört.

Für Benutzer von LDAP-Servern (LDAP = Lightweight Directory Access Protocol):

- Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.

- Wenn Sie den Authentifizierungsmodus in LDAP ändern und der Knotenname mit einer Benutzer-ID mit Administratorberechtigung übereinstimmt, stellen Sie möglicherweise ein nicht erwartetes Verhalten fest, wenn eine automatische Kennwortänderung stattfindet, weil das Kennwort unter Umständen zweimal aktualisiert wird. Dies hat zur Folge, dass das Kennwort für die Benutzer-ID mit Administratorberechtigung unbekannt ist. Es kann aber auch vorkommen, dass die Kennwortaktualisierungsoperation fehlschlägt.

Wenn Sie einen Knoten registrieren oder aktualisieren, können Sie angeben, ob beschädigte Dateien auf dem Knoten von einem Zielreplikationsserver wiederhergestellt werden können. Dateien können nur wiederhergestellt werden, wenn alle folgenden Bedingungen erfüllt sind:

- Version 7.1.1 oder höher ist auf dem Quellen- und Zielreplikationsserver installiert.
- Der Systemparameter REPLRECOVERDAMAGED ist auf ON gesetzt. Der Systemparameter kann mit dem Befehl SET REPLRECOVERDAMAGED definiert werden.
- Der Quellenserver schließt mindestens eine Datei ein, die auf dem Knoten, der repliziert wird, als beschädigt markiert ist.
- Die Knotendaten wurden repliziert, bevor die Beschädigung aufgetreten ist.

In der folgenden Tabelle wird beschrieben, wie sich Parametereinstellungen auf die Wiederherstellung beschädigter, replizierter Dateien auswirken.

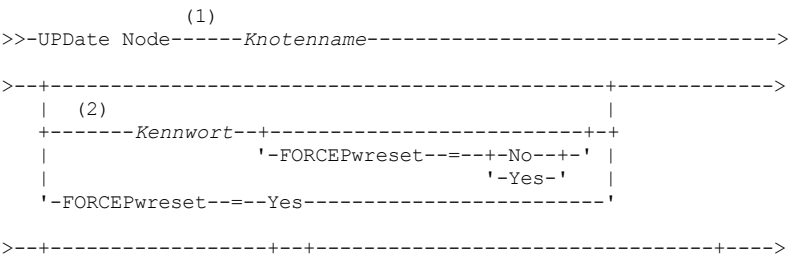
Tabelle 1. Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken

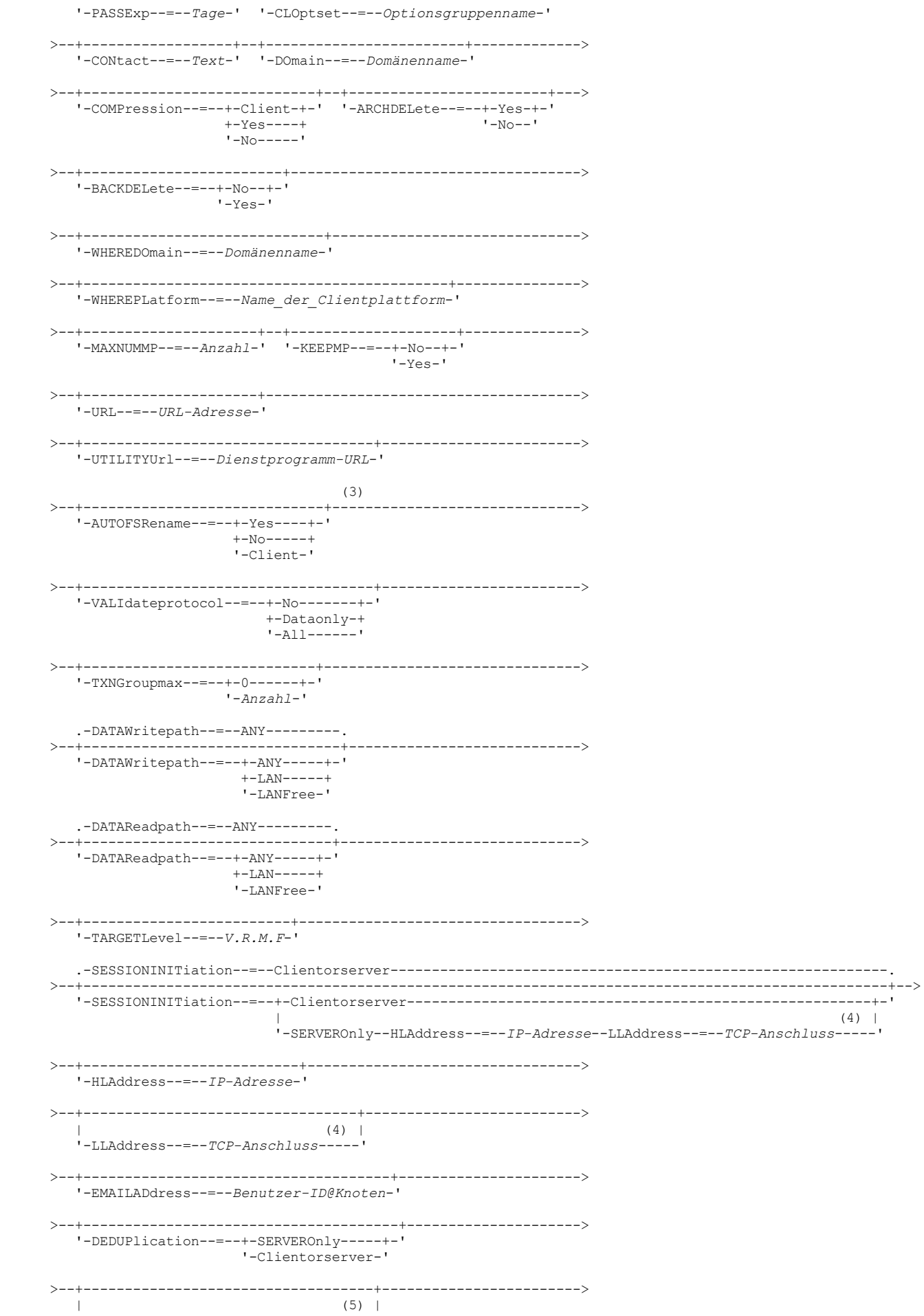
Einstellung für den Systemparameter REPLRECOVERDAMAGED	**Wert des Parameters RECOVERDAMAGED im Befehl REPLICATE NODE**	**Wert des Parameters RECOVERDAMAGED in den Befehlen REGISTER NODE und UPDATE NODE**	**Ergebnis**
OFF	YES, NO oder nicht angegeben	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.
OFF	ONLY	YES oder NO	Eine Fehlernachricht wird angezeigt, weil Dateien nicht wiederhergestellt werden können, wenn der Systemparameter REPLRECOVERDAMAGED auf OFF gesetzt ist.
ON	YES	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.
ON	NO	YES oder NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.
ON	ONLY	YES oder NO	Beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt, aber es findet keine Standardknotenreplikation statt.
ON	Nicht angegeben	YES	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden vom Zielreplikationsserver wiederhergestellt.
ON	Nicht angegeben	NO	Während der Knotenreplikation findet eine Standardreplikation statt und beschädigte Dateien werden nicht vom Zielreplikationsserver wiederhergestellt.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Clientknoten gehört.

Syntax




'-PASSExp--=--Tage-' '-CLOptset--=--Optionsgruppenname-'
>--+-----------------+--+-----------------------+-------------->
'-CONtact--=--Text-' '-DOmain--=--Domänenname-'
>--+---------------------------+--+-------------------------+--->
'-COMPression--=--+-Client-+-' '-ARCHDELete--=--+-Yes-+-'
+-Yes----+ '-No--'
'-No-----'
>--+-------------------------+---------------------------------->
'-BACKDELete--=--+-No--+-'
'-Yes-'
>--+-----------------------------+------------------------------>
'-WHEREDOmain--=--Domänenname-'
>--+---+--------------->
'-WHEREPLatform--=--Name_der_Clientplattform-'
>--+---------------------+--+--------------------+-------------->
'-MAXNUMMP--=--Anzahl-' '-KEEPMP--=--+-No--+-'
'-Yes-'
>--+---------------------+-->
'-URL--=--URL-Adresse-'
>--+-------------------------------------+----------------------->
'-UTILITYUrl--=--Dienstprogramm-URL-'
(3)
>--+-----------------------------+------------------------------>
'-AUTOFSRename--=--+-Yes----+-'
+-No-----+
'-Client-'
>--+-----------------------------------+----------------------->
'-VALIdateprotocol--=--+-No-------+-'
+-Dataonly-+
'-All------'
>--+---------------------------+-------------------------------->
'-TXNGroupmax--=--+-0------+-'
'-Anzahl-'
.-DATAWritepath--=--ANY---------.
>--+-------------------------------+---------------------------->
'-DATAWritepath--=--+-ANY-----+-'
+-LAN-----+
'-LANFree-'
.-DATAReadpath--=--ANY---------.
>--+-------------------------------+---------------------------->
'-DATAReadpath--=--+-ANY-----+-'
+-LAN-----+
'-LANFree-'
>--+-------------------------+---------------------------------->
'-TARGETLevel--=--V.R.M.F-'
.-SESSIONINITiation--=--Clientorserver---.
>--+---+-->
'-SESSIONINITiation--=--+-Clientorserver---+-'
| (4) |
'-SERVEROnly--HLAddress--=--IP-Adresse--LLAddress--=--TCP-Anschluss-----'
>--+-------------------------+---------------------------------->
'-HLAddress--=--IP-Adresse-'
>--+---------------------------------+-------------------------->
| (4) |
'-LLAddress--=--TCP-Anschluss-----'
>--+-------------------------------------+---------------------->
'-EMAILADdress--=--Benutzer-ID@Knoten-'
>--+-------------------------------------+---------------------->
'-DEDUPlication--=--+-SERVEROnly-----+-'
'-Clientorserver-'
>--+---------------------------------+-------------------------->
| (5) |

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.
2. Kennwörter sind bei diesem Befehl optional, wenn Sie nicht die Authentifizierungsmethode von LDAP in LOCAL ändern.
3. Der Parameter VALIDATEPROTOCOL ist veraltet.
4. HLADDRESS und LLADDRESS müssen zuvor definiert oder im Befehl UPDATE NODE oder REGISTER NODE angegeben werden, um SESSIONINITIATION=SERVERONLY zu verwenden.
5. Der Parameter BACKUPINITIATION wird ignoriert, wenn das Betriebssystem des Clientknotens nicht unterstützt wird.
6. Wenn Sie den Parameter REPLSTATE angeben und den Parameter REPLMODE nicht angeben, wird der Replikationsmodus des Knotens auf SEND gesetzt.
7. Wenn Sie den Parameter REPLMODE angeben, müssen Sie auch den Parameter REPLSTATE angeben.
8. Der Parameter SYNCLDAPDELETE gilt nur, wenn ein Knoten, der sich mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifiziert, zur lokalen Authentifizierung zurückkehrt.
9. Der Parameter SSLREQUIRED ist veraltet.

Parameter

Knotenname (Erforderlich)
Gibt den Namen des Clientknotens an, der aktualisiert werden soll. Dieser Name kann mit Hilfe von Platzhalterzeichen angegeben werden. Einschränkung: Wenn ein Kennwort mit dem Befehl UPDATE NODE aktualisiert wird, können Sie kein Platzhalterzeichen beim Parameter `Knotenname` verwenden.

Kennwort
Gibt das neue Kennwort für den Clientknoten an. Dieser Parameter ist in den meisten Fällen optional. Wenn die Authentifizierungsmethode des Knotens von LDAP in LOCAL geändert wird, ist ein Kennwort erforderlich. Wenn LDAP als Knotenauthentifizierungsmethode verwendet wird, geben Sie bei Verwendung des Befehls UPDATE NODE kein Kennwort an. Das Kennwort darf maximal 64 Zeichen lang sein. Die Gültigkeitsdauer von Kennwörtern richtet sich nach der Kennwortablaufdauer.

FORCEPwreset
Gibt an, ob ein Client zum Ändern oder Zurücksetzen des Kennworts gezwungen werden soll. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass die Kennwortablaufdauer über den Befehl SET PASSEXP definiert wird. Einen Client nicht zwingen, das Kennwort zu ändern oder zurückzusetzen, während er versucht, sich beim Server anzumelden.

Yes
Gibt an, dass das Kennwort des Clientknotens oder des Administrators bei der nächsten Anmeldung abläuft. Der Client muss das Kennwort bei der nächsten Anmeldung ändern oder zurücksetzen.
Einschränkungen:

- Für Knoten, die mit einem LDAP-Server authentifiziert werden, wird der Kennwortablauf mithilfe von LDAP-Serverdienstprogrammen definiert. Geben Sie daher nicht FORCEPWRESET=YES an, wenn AUTHENTICATION=LDAP angegeben werden soll.
- Soll ein Knoten für die Authentifizierung mit einem LDAP-Server aktualisiert werden, und haben Sie FORCEPWRESET=YES angegeben, müssen Sie das Kennwort ändern, bevor Sie FORCEPWRESET=NO und AUTHENTICATION=LDAP angeben können.

PASSExp
Gibt die Anzahl der Tage an, die das Kennwort gültig ist. Für die Kennwortablaufdauer kann ein Wert von 0 bis 9999 Tage definiert werden. Der Wert 0 bedeutet, dass das Kennwort niemals abläuft. Dieser Parameter ist wahlfrei. Wird dieser Parameter nicht angegeben, wird die Kennwortablaufdauer nicht geändert.

Sie können die Kennwortablaufdauer mit dem Befehl UPDATE NODE oder SET PASSEXP ändern. Um eine allgemeine Ablaufdauer für alle Administratoren und Clientknoten zu definieren, geben Sie den Befehl SET PASSEXP aus. Sie können den Befehl SET PASSEXP auch verwenden, um die Kennwortablaufdauer selektiv festzulegen. Wenn Sie eine Kennwortablaufdauer selektiv mit dem Befehl REGISTER NODE, UPDATE NODE oder SET PASSEXP festlegen, wird die Ablaufdauer von der jeweiligen allgemeinen Kennwortablaufdauer ausgeschlossen, die mit dem Befehl SET PASSEXP erstellt wurde.

Sie können den Befehl RESET PASSEXP verwenden, um die Kennwortablaufdauer auf die allgemeine Kennwortablaufdauer zurückzusetzen. Dieser Parameter gilt nicht für Kennwörter, die sich mit einem LDAP-Verzeichnisserver authentifizieren.

CLOptset
Gibt den Namen der Optionsgruppe an, die der Client verwenden soll. Dieser Parameter ist wahlfrei. Um eine Clientoptionsgruppe zu entfernen, geben Sie den Parameter CLOPTSET mit einer Nullzeichenfolge ("") an.

CONtact
Gibt eine Informationszeichenfolge an, die den Clientknoten identifiziert. Dieser Parameter ist wahlfrei. Die maximale Länge der Zeichenfolge beträgt 255 Zeichen. Die Kontaktinformationen in Anführungszeichen einschließen, wenn sie Leerzeichen enthalten. Sollen zuvor definierte Kontaktinformationen entfernt werden, geben Sie eine Nullzeichenfolge ("") an.

DOmain
Gibt den Namen der Maßnahmendomäne an, für die der Clientknoten registriert werden soll. Dieser Parameter ist wahlfrei.
Einschränkung: Für Server mit aktiviertem Aufbewahrungsschutz für Daten kann ein archivierter registrierter Knoten nicht erneut einer anderen Maßnahmendomäne zugeordnet werden.

COMPression
Gibt an, ob der Clientknoten seine Dateien komprimiert, bevor sie zum Sichern und Archivieren an den Server gesendet werden. Dieser Parameter ist wahlfrei.
Einschränkung: Dieser Parameter kann nicht für einen NAS-Knoten angegeben werden.

Sie können einen der folgenden Werte angeben:

Client
Gibt an, dass der Client festlegt, ob Dateien komprimiert werden sollen.

Yes
Gibt an, dass der Clientknoten seine Dateien komprimiert, bevor sie zum Sichern und Archivieren an den Server gesendet werden.

No
Gibt an, dass der Clientknoten seine Dateien nicht komprimiert, bevor sie zum Sichern und Archivieren an den Server gesendet werden.

ARCHDELete
Gibt an, ob der Clientknoten seine eigenen Archivierungsdateien aus dem Server löschen darf. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass der Clientknoten seine eigenen Archivierungsdateien aus dem Server löschen darf.
No
Gibt an, dass der Clientknoten seine eigenen Archivierungsdateien nicht aus dem Server löschen darf.

BACKDELete
Gibt an, ob der Clientknoten seine eigenen Sicherungsdateien aus dem Server löschen darf. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass der Clientknoten seine eigenen Sicherungsdateien nicht aus dem Server löschen darf.
Yes
Gibt an, dass der Clientknoten seine eigenen Sicherungsdateien aus dem Server löschen darf.

WHEREDOmain
Gibt den Namen der Maßnahmendomäne an, die in Kombination mit dem Knotennamen als Filter verwendet werden soll, um zu aktualisierende Knoten auszuwählen. Dieser Parameter ist wahlfrei.

WHEREPLatform
Gibt den Namen der Clientplattform an, die in Kombination mit dem Knotennamen als Filter verwendet werden soll, um zu aktualisierende Knoten auszuwählen. Dieser Parameter ist wahlfrei.

MAXNUMMP
Gibt die maximale Anzahl der Mountpunkte an, die ein Knoten nur für Operationen, wie beispielsweise Sicherung, Archivierung und IBM Spectrum Protect for Space Management-Umlagerung, auf dem Server oder dem Speicheragenten verwenden kann. Der Parameter ist optional und gilt nicht für Knoten mit dem Typ NAS oder SERVER. Der Standardwert ist 1. Sie können eine ganze Zahl im Bereich von 0 bis 999 angeben. Der Wert 0 gibt an, dass ein Knoten keinen Mountpunkt für eine Operation zum Speichern von Clientdaten anfordern kann. Der Wert für MAXNUMMP wird während der Operationen zum Lesen von Clientdaten, wie beispielsweise Zurückschreiben, Abrufen und Zurückrufen durch IBM Spectrum Protect for Space Management, nicht ausgewertet oder umgesetzt. Mountpunkte, die für Operationen zum Lesen von Daten verwendet werden, werden jedoch in Bezug auf versuchte gleichzeitig ablaufende Datenspeicherungsoperationen für denselben Clientknoten ausgewertet und können verhindern, dass die Datenspeicherungsoperationen Mountpunkte anfordern können.

Für Datenträger in einem Speicherpool, dem der Einheitentyp FILE oder CENTERA zugeordnet ist, kann der Server über mehrere Sitzungen verfügen, um gleichzeitig denselben Datenträger zu lesen, und über eine Sitzung verfügen, um auf diesen Datenträger zu schreiben. Um den gemeinsamen Zugriff zu erweitern und einen effizienten Zugriff für Knoten mit Daten in Speicherpools des Typs FILE oder CENTERA zur Verfügung zu stellen, erhöhen Sie den Wert des Parameters MAXNUMMP.

Für Knoten, die mit aktivierter Funktion für simultanes Schreiben Daten in primären Speicherpools speichern, müssen Sie den Wert des Parameters MAXNUMMP anpassen, um die korrekte Anzahl der Mountpunkte für jede Clientsitzung anzugeben. Eine Clientsitzung erfordert einen Mountpunkt für den primären Speicherpool und einen Mountpunkt für jeden Kopienspeicherpool und jeden Pool für aktive Daten.

URL
Gibt die URL des IBM Spectrum Protect-Web-Clients an, die auf dem Clientsystem konfiguriert ist. Sie können die URL in einem Web-Browser und im Operations Center verwenden, um den Clientknoten über Fernzugriff zu verwalten.

Dieser Parameter ist wahlfrei. Die URL muss den DNS-Namen oder die IP-Adresse des Clientsystems und die Anschlussnummer enthalten, die auf dem Clientsystem für den IBM Spectrum Protect-Web-Client definiert ist. Beispiel: `http://client.mycorp.com:1581`

Soll der Wert für diesen Parameter entfernt werden, geben Sie leere einfache Anführungszeichen oder leere Anführungszeichen ohne Leerzeichen an ('' für einfache Anführungszeichen oder "" für Anführungszeichen).

UTILITYUrl
Gibt die Adresse der IBM Spectrum Protect-Clientverwaltungsservices an, die auf dem Clientsystem konfiguriert sind. Diese URL wird vom Operations Center verwendet, um auf Clientprotokolldateien zuzugreifen, sodass Sie im Operations Center Clientprobleme über Fernzugriff diagnostizieren können.

Dieser Parameter ist wahlfrei. Sie können eine URL mit maximal 200 Zeichen angeben. Die URL muss mit `https` beginnen. Sie enthält den DNS-Namen oder die IP-Adresse des Clientsystems und die Anschlussnummer, die auf dem Clientsystem für die IBM Spectrum Protect-Clientverwaltungsservices definiert ist. Beispiel: `https://client.mycorp.com:9028`

Wird keine Anschlussnummer angegeben, verwendet das Operations Center die Anschlussnummer 9028. Dies ist die Standardanschlussnummer, wenn Sie die Clientverwaltungsservices auf dem Clientsystem installieren.

KEEPMP
Gibt an, ob der Clientknoten den Mountpunkt für die gesamte Sitzung beibehält. Der Parameter ist wahlfrei.Sie können einen der folgenden Werte angeben:

No

Gibt an, dass der Clientknoten den Mountpunkt während der Sitzung freigibt. Haben Maßnahmendefinitionen zur Folge, dass Daten in einem Plattenspeicherpool gespeichert werden, nachdem Daten in einem Speicherpool mit sequenziellem Zugriff gespeichert wurden, werden alle von der Sitzung belegten Mountpunkte freigegeben.

Yes

Gibt an, dass der Clientknoten den Mountpunkt während der gesamten Sitzung beibehalten muss. Haben Maßnahmendefinitionen zur Folge, dass Daten in einem Plattenspeicherpool gespeichert werden, nachdem Daten in einem Speicherpool mit sequenziellem Zugriff gespeichert wurden, werden alle von der Sitzung belegten Mountpunkte nicht freigegeben.

AUTOFSRename

Gibt an, ob der Client zum Umbenennen von Dateibereichen aufgefordert wird, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt. Das Auffordern und Umbenennen (falls zulässig) findet nur statt, wenn der Client eine der folgenden Operationen ausführt: Archivieren, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung. Beim Umbenennen werden die Namen von bestehenden gesicherten Dateibereichen, die nicht in Unicode sind, im Serverspeicher geändert. Anschließend werden die Dateibereiche in Unicode gesichert. Sie können diesen Parameter für Unicode-fähige IBM Spectrum Protect-Clients mit den Betriebssystemen Windows, Macintosh OS X und NetWare verwenden.
Wichtig: Nachdem der Client mit Unterstützung für Unicode installiert wurde, werden alle neuen Dateibereiche, die der Client sichert, im Serverspeicher mit der Zeichenumsetztabelle UTF-8 gespeichert. UTF-8 ist eine byte-orientierte Verschlüsselungsform, die durch den Unicode Standard angegeben wird.

Sie können einen der folgenden Werte angeben:

Yes

Vorhandene Dateibereiche werden vom Server automatisch umbenannt, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine der folgenden Operationen ausführt: Archivieren, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung. Das Umbenennen findet statt, wenn der Client die grafische Benutzerschnittstelle, die Befehlszeile oder den Client-Scheduler verwendet.
Beispielsweise wird ein Laufwerk vom Server wie folgt umbenannt:

- Ursprünglicher Name: D_DRIVE
- Neuer Name: D_DRIVE_OLD

Der neue Name gibt an, dass der Dateibereich auf dem Server in einem Format gespeichert wird, das kein Unicode ist.

No

Dateibereiche werden vom Server nicht automatisch umbenannt, wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine der folgenden Operationen ausführt: Archivieren, selektive Sicherung, vollständige Teilsicherung oder partielle Teilsicherung.

Client

Die Option AUTOFSRENAME in der Clientoptionsdatei bestimmt, ob Dateibereiche umbenannt werden.

Standardmäßig ist die Clientoption auf PROMPT gesetzt. Wenn für das Clientsystem ein Upgrade auf einen Client erfolgt, der Unicode unterstützt, und der Client eine IBM Spectrum Protect-Operation mit der grafischen Benutzerschnittstelle oder der Befehlszeile ausführt, zeigt das Programm dem Benutzer einmalig eine Bedienerführung an und fordert den Benutzer zur Angabe auf, ob Dateibereiche umbenannt werden sollen.

Wenn der Client-Scheduler eine Operation ausführt, fordert das Programm nicht zur Angabe einer Auswahl für das Umbenennen auf, und es werden keine Dateibereiche umbenannt. Sicherungen von vorhandenen Dateibereichen werden wie zuvor gesendet (nicht in Unicode).

VALIdateprotocol (veraltet)

Gibt an, ob IBM Spectrum Protect eine zyklische Blockprüfung ausführt, um die Daten zu validieren, die zwischen dem Client und dem Server gesendet werden. Der Parameter ist wahlfrei.
Wichtig: Ab IBM Spectrum Protect Version 8.1.2 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter VALIDATEPROTOCOL wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

TXNGroupmax

Gibt die Anzahl Dateien an, die als Gruppe zwischen einem Client und einem Server zwischen Transaktions-COMMIT-Punkten übertragen werden. Die Clientleistung kann verbessert werden, indem ein höherer Wert für diese Option verwendet wird.

Der Wert 0 gibt an, dass der Knoten den globalen Serverwert verwendet, der in der Serveroptionsdatei definiert ist. Soll ein anderer Wert als der globale Serverwert verwendet werden, geben Sie einen Wert von 4 bis 65.000 für diesen Parameter an. Der Knotenwert hat Vorrang vor dem Serverwert.

Tipp: Die Vergrößerung des Werts für TXNGROUPMAX führt zu einer Erhöhung der Auslastung des Wiederherstellungsprotokolls. Eine höhere Auslastung des Wiederherstellungsprotokolls kann das Risiko erhöhen, dass der Protokollspeicherbereich nicht mehr ausreicht. Werten Sie die Leistung jedes Knotens aus, bevor Sie den Parameter ändern.

DATAWritepath

Gibt den Übertragungspfad an, der verwendet wird, wenn der Client während Speicheroperationen (Sicherung oder Archivierung) Daten an den Server und/oder den Speicheragenten sendet. Der Parameter ist wahlfrei.

Hinweis: Ist kein Pfad verfügbar, kann der Knoten keine Daten senden. Wenn Sie z. B. die LAN-unabhängige Option auswählen, aber kein LAN-unabhängiger Pfad definiert ist, schlägt die Operation fehl.

Sie können einen der folgenden Werte angeben:

ANY
: Gibt an, dass Daten über einen beliebigen verfügbaren Pfad an den Server und/oder Speicheragenten gesendet werden. Ein LAN-unabhängiger Pfad wird verwendet, wenn einer verfügbar ist. Ist kein LAN-unabhängiger Pfad verfügbar, werden die Daten über das LAN übertragen.

LAN
: Gibt an, dass Daten über das LAN gesendet werden.

LANFree
: Gibt an, dass Daten über einen LAN-unabhängigen Pfad gesendet werden.

DATAReadpath
: Gibt den Übertragungspfad an, der verwendet wird, wenn der Server und/oder Speicheragent während Operationen wie Zurückschreiben oder Abrufen Daten für einen Client lesen. Der Parameter ist wahlfrei.
Hinweis: Ist kein Pfad verfügbar, können keine Daten gelesen werden. Wenn Sie z. B. die LAN-unabhängige Option auswählen, aber kein LAN-unabhängiger Pfad definiert ist, schlägt die Operation fehl. Der Wert für den Übertragungspfad gilt auch für Übernahmeverbindungen. Wird der Wert auf LANFree gesetzt, kann für den Knoten auf dem sekundären Server keine Übernahme erfolgen.

  Sie können einen der folgenden Werte angeben:

  ANY
  : Gibt an, dass der Server und/oder Speicheragent einen beliebigen verfügbaren Pfad verwenden, um Daten zu lesen. Ein LAN-unabhängiger Pfad wird verwendet, wenn einer verfügbar ist. Ist kein LAN-unabhängiger Pfad verfügbar, werden die Daten über das LAN gelesen.

  LAN
  : Gibt an, dass Daten über das LAN gelesen werden.

  LANFree
  : Gibt an, dass Daten über einen LAN-unabhängigen Pfad gelesen werden.

SESSIONINITiation
: Steuert, ob der Server oder der Client Sitzungen einleitet. Der Parameter ist wahlfrei.

  Clientorserver
  : Gibt an, dass der Client Sitzungen mit dem Server einleiten kann, indem über den TCP/IP-Anschluss kommuniziert wird, der mit der Serveroption TCPPORT definiert wird. Die Zeitplanung über Serversystemanfrage kann ebenfalls verwendet werden, um den Client aufzufordern, eine Verbindung zum Server herzustellen.

  SERVEROnly
  : Gibt an, dass der Server keine Clientanforderungen für Sitzungen akzeptiert. Alle Sitzungen müssen durch die Zeitplanung über Serversystemanfrage an dem Anschluss eingeleitet werden, der mit dem Befehl REGISTER oder UPDATE NODE für den Client definiert wird. Sie können den Clientakzeptor (dsmcad) nicht verwenden, um den Scheduler zu starten, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist.

    HLAddress
    : Gibt die Client-IP-Adresse an, die der Server anspricht, um geplante Ereignisse einzuleiten. Dieser Parameter muss verwendet werden, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server anzusprechen.

      Die Adresse kann entweder im numerischen Format oder im Hostnamenformat angegeben werden. Wird eine numerische Adresse verwendet, wird sie ohne Prüfung durch einen Domänennamensserver gesichert. Ist die Adresse nicht korrekt, kann dies zu Fehlern führen, wenn der Server versucht, den Client anzusprechen. Adressen im Hostnamensformat werden mit einem Domänennamensserver geprüft. Geprüfte Namen werden mit Domänennamenservices (Domain Name Services) gesichert und aufgelöst, wenn der Server den Client kontaktiert.

    LLAddress
    : Gibt die Clientanschlussnummer an, an der der Client für Sitzungen von dem Server empfangsbereit ist. Dieser Parameter muss verwendet werden, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server anzusprechen.

      Der Wert für diesen Parameter muss mit dem Wert der Clientoption TCPCLIENTPORT übereinstimmen. Der Standardwert ist 1501.

HLAddress
: Gibt die Client-IP-Adresse an, die der Server anspricht, um geplante Ereignisse einzuleiten. Dieser optionale Parameter wird nur verwendet, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet

wurden, um den Server zu kontaktieren. Wird SESSIONINITIATION=SERVERONLY nicht verwendet, hat diese Option keine Auswirkung.

Die Adresse kann entweder im numerischen Format oder im Hostnamenformat angegeben werden. Wird eine numerische Adresse verwendet, wird sie ohne Prüfung durch einen Domänennamensserver gesichert. Ist die Adresse nicht korrekt, kann dies zu Fehlern führen, wenn der Server versucht, den Client anzusprechen. Adressen im Hostnamensformat werden mit einem Domänennamensserver geprüft. Geprüfte Namen werden mit Domänennamenservices (Domain Name Services) gesichert und aufgelöst, wenn der Server den Client kontaktiert.

LLAddress

Gibt die Clientanschlussnummer an, an der der Client für Sitzungen von dem Server empfangsbereit ist. Dieser optionale Parameter wird nur verwendet, wenn SESSIONINITIATION auf SERVERONLY gesetzt ist, unabhängig von den Adressen, die zuvor vom Client verwendet wurden, um den Server zu kontaktieren. Wird SESSIONINITIATION=SERVERONLY nicht verwendet, hat diese Option keine Auswirkung.

Der Wert für diesen Parameter muss mit dem Wert der Clientoption TCPCLIENTPORT übereinstimmen. Der Standardwert ist 1501.

EMAILADdress
: Dieser Parameter wird für weitere Kontaktinformationen verwendet. Die mit diesem Parameter angegebenen Informationen werden von IBM Spectrum Protect nicht verwendet.

DEDUPlication
: Gibt an, wo die Datendeduplizierung für diesen Knoten stattfinden kann. Sie können einen der folgenden Werte angeben:

  SERVEROnly
  : Gibt an, dass von diesem Knoten gespeicherte Daten nur auf dem Server dedupliziert werden können.

  Clientorserver
  : Gibt an, dass von diesem Knoten gespeicherte Daten entweder auf dem Client oder auf dem Server dedupliziert werden können. Um die Datendeduplizierung auf dem Client auszuführen, müssen Sie auch den Wert YES für die Clientoption DEDUPLICATION angeben. Sie können diese Option in der Clientoptionsdatei oder in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server angeben.

TARGETLevel

Gibt das Clientimplementierungspaket für diesen Knoten an. Für V.R.M.F (Version.Release.Modifikation.Fix-Level) kann ein gültiges Releasepaket angegeben werden. Beispiel: `TARGETLevel=6.2.0.0`.

Sie müssen jedes Segment mit einer Zahl angeben, die für ein Implementierungspaket zutreffend ist. Sie können keinen Stern in einem Feld als Ersetzung für eine gültige Zahl verwenden. Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge (" ") angeben. Der Parameter ist wahlfrei.
Einschränkung: Der Parameter TARGETLEVEL gilt nicht für Knoten mit dem Typ NAS oder SERVER.

BACKUPINITiation
: Gibt an, ob die ID eines Benutzers ohne Rootberechtigung auf dem Clientknoten Dateien auf dem Server sichern kann. Der Parameter ist wahlfrei.Der Standardwert ALL gibt an, dass IDs der Benutzer ohne Rootberechtigung Daten auf dem Server sichern können. Sie können einen der folgenden Werte auswählen:

  All
  : Gibt an, dass die IDs der Benutzer ohne Rootberechtigung Dateien auf dem Server sichern können. ALL ist der Standardwert, wenn BACKUPINITIATION nicht angegeben wird.

  ROOT
  : Gibt an, dass nur die Rootbenutzer-ID Dateien auf dem Server sichern kann.
  Einschränkung: Das Attribut wird vom Server ignoriert, wenn der Client für Sichern/Archivieren eine Verbindung von einem anderen Betriebssystem als AIX, Linux, Solaris oder Mac OS herstellt.

BKREPLRuledefault, ARREPLRuledefault und SPREPLRuledefault
: Gibt die Replikationsregel an, die für einen Datentyp gilt, wenn die Dateibereichsregeln für den Datentyp auf DEFAULT gesetzt sind:

  BKREPLRuledefault
  : Gibt die Replikationsregel für Sicherungsdaten an.

  ARREPLRuledefault
  : Gibt die Replikationsregel für Archivierungsdaten an.

  SPREPLRuledefault
  : Gibt die Replikationsregel für speicherverwaltete Daten an.

  Sie können Replikationsregeln für normale Priorität oder Replikationsregeln für hohe Priorität angeben. In einem Replikationsprozess, der sowohl Daten mit normaler Priorität als auch Daten mit hoher Priorität einschließt, werden Daten mit hoher Priorität zuerst repliziert. Bevor Sie eine Regel angeben, beachten Sie die Reihenfolge, in der die Daten repliziert werden sollen.

  Beispiel: Angenommen, ein Clientknoten enthält aktive Sicherungsdaten und Archivierungsdaten. Die Replikation der aktiven Sicherungsdaten hat eine höhere Priorität als die der Archivierungsdaten. Um beide Datentypen zu priorisieren, geben Sie `BKREPLRULEDEFAULT=ACTIVE_DATA_HIGH_PRIORITY ARREPLRULEDEFAULT=ALL_DATA` an.

Sie können die folgenden Regeln angeben:

ALL_DATA
: Repliziert aktive und inaktive Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Die Daten werden mit einer normalen Priorität repliziert.

ACTIVE_DATA
: Repliziert nur aktive Sicherungsdaten. Die Daten werden mit einer normalen Priorität repliziert. Diese Regel ist nur für BKREPLRULEDEFAULT gültig.
Achtung:

  Wenn Sie ACTIVE_DATA angeben und eine oder mehrere der folgenden Bedingungen wahr sind, werden inaktive Sicherungsdaten auf dem Zielreplikationsserver gelöscht und inaktive Sicherungsdaten auf dem Quellenreplikationsserver nicht repliziert.

  - Wenn eine Releaseversion vor Version 7.1.1 entweder auf dem Quellenreplikationsserver oder auf dem Zielreplikationsserver installiert ist.
  - Wenn Sie den Befehl REPLICATE NODE mit dem Parameter `FORCERECONCILE=YES` verwenden.
  - Wenn Sie die Erstreplikation eines Dateibereichs nach der Konfiguration der Replikation, der Zurückschreibung der Datenbank oder der Durchführung eines Upgrades für den Quellen- und den Zielreplikationsserver von einer Releaseversion vor Version 7.1.1 ausführen.

  Wenn die vorherigen Bedingungen nicht wahr sind, werden alle Dateien, die neu sind oder sich seit der letzten Replikation geändert haben (einschließlich inaktiver Dateien) repliziert und Dateien werden gelöscht, wenn sie verfallen.

ALL_DATA_HIGH_PRIORITY
: Repliziert aktive und inaktive Sicherungsdaten, Archivierungsdaten oder speicherverwaltete Daten. Daten werden mit einer hohen Priorität repliziert.

ACTIVE_DATA_HIGH_PRIORITY
: Diese Regel entspricht der Replikationsregel ACTIVE_DATA, mit der Ausnahme, dass Daten mit einer hohen Priorität repliziert werden. Diese Regel ist nur für BKREPLRULEDEFAULT gültig.

DEFAULT
: Repliziert Daten gemäß der Serverreplikationsregel für Sicherungsdaten.

  Beispiel: Angenommen, Sie möchten die Archivierungsdaten in allen Dateibereichen replizieren, die zu einem Clientknoten gehören. Die Replikation der Archivierungsdaten hat eine hohe Priorität. Eine Methode zur Ausführung dieser Task ist die Angabe von `ARREPLRULEDEFAULT=DEFAULT`. Stellen Sie sicher, dass die Dateibereichsregeln für Archivierungsdaten ebenfalls auf DEFAULT gesetzt sind und die Serverregel für Archivierungsdaten auf ALL_DATA_HIGH_PRIORITY gesetzt ist.

  Einschränkung: Wenn ein Knoten für die Replikation konfiguriert ist, werden die Dateibereichsregeln auf DEFAULT gesetzt, nachdem der Knoten Daten auf dem Quellenreplikationsserver gespeichert hat.

NONE
: Daten des angegebenen Typs werden nicht repliziert.

  Sollen beispielsweise speicherverwaltete Daten, die zu einem Clientknoten gehören, nicht repliziert werden, geben Sie `SPREPLRULEDEFAULT=NONE` an.

REPLState
: Gibt an, ob Daten, die zu dem Clientknoten gehören, für die Replikation bereit sind. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  ENabled
  : Gibt an, dass der Clientknoten für die Replikation bereit ist.

  DISabled
  : Gibt an, dass die Replikation erst stattfindet, wenn sie aktiviert wurde.

  Die Systemantwort auf diese Einstellungen hängt davon ab,

  ob die Clientknotendefinition nur auf dem Quellenreplikationsserver vorhanden ist und Sie den Clientknoten zum ersten Mal für die Replikation konfigurieren
  : Wenn Sie den Replikationsstatus auf ENABLED oder DISABLED setzen, wird der Replikationsmodus des Knotens auf dem Quellenreplikationsserver automatisch auf SEND gesetzt, nachdem der Befehl UPDATE NODE ausgegeben wurde. Wenn die Replikation zum ersten Mal erfolgt, wird eine Clientknotendefinition automatisch auf dem Zielserver erstellt. Der Replikationsstatus des Clientknotens auf dem Zielserver wird automatisch auf ENABLED gesetzt. Der Replikationsmodus wird auf RECEIVE gesetzt.

  ob die Clientknotendefinition auf dem Quellen- und dem Zielreplikationsserver vorhanden ist und die Knotendaten zuvor repliziert wurden
  : Damit die Replikation ausgeführt werden kann, muss der Replikationsstatus des Clientknotens sowohl auf dem Quellen- als auch auf dem Zielserver auf ENABLED gesetzt werden. Lautet beispielsweise der Replikationsstatus eines Clientknotens auf dem Quellenserver ENABLED und der Replikationsstatus auf dem Zielserver DISABLED, findet keine Replikation statt.

  ob die Clientknotendefinition auf dem Quellen- und dem Zielreplikationsserver vorhanden ist und die Knotendaten zuvor vom Quellenreplikationsserver exportiert und auf den Zielreplikationsserver importiert wurden
  : In diesem Fall konfigurieren Sie die Clientknoten, um die Daten zwischen den beiden Servern zu synchronisieren. Wenn die Replikation zum ersten Mal erfolgt, wird der Replikationsstatus des Clientknotens auf dem Zielserver automatisch auf ENABLED gesetzt. Daten auf dem Quellen- und Zielserver werden synchronisiert.

Einschränkung: Um Daten zu synchronisieren, müssen Sie zusätzlich zum Parameter REPLSTATE den Parameter REPLMODE angeben.

Sie können den Parameter REPLMODE nur angeben, wenn der Clientknoten noch nie repliziert wurde:

- Wenn die Clientknotendefinition nur auf dem Quellenreplikationsserver vorhanden ist, wird der Replikationsmodus des Knotens auf dem Quellenreplikationsserver automatisch auf SEND gesetzt, wenn der Befehl UPDATE NODE ausgegeben wird. Der Replikationsmodus des Knotens auf dem Zielreplikationsserver wird automatisch auf RECEIVE gesetzt.
- Wenn Daten, die zu dem Knoten gehören, zuvor repliziert wurden, lautet der Replikationsmodus des Knotens auf dem Quellenreplikationsserver SEND. Der Replikationsmodus des Knotens auf dem Zielreplikationsserver lautet RECEIVE.

REPLMode
Gibt an, ob die Daten synchronisiert werden sollen, die zu diesem Clientknoten gehören. Geben Sie diesen Parameter nur an, wenn Daten, die zu dem Clientknoten gehören, vom Quellenreplikationsserver exportiert und auf den Zielreplikationsserver importiert wurden. Die Synchronisation erfolgt während der Replikation.

Um Daten zu synchronisieren, müssen Sie den Befehl UPDATE NODE sowohl auf dem Quellen- als auch auf dem Zielreplikationsserver ausgeben und die Parameter REPLMODE und REPLSTATE angeben. Der Wert, den Sie für den Parameter REPLMODE angeben, hängt davon ab, ob der Server eine Quelle oder ein Ziel für replizierte Daten ist.

Sie können einen der folgenden Werte angeben:

SYNCSEnd
Gibt an, dass Daten, die zu diesem Clientknoten gehören, während der Replikation mit Daten auf dem Zielserver synchronisiert werden. Geben Sie diesen Wert nur auf dem Server an, der die Daten exportiert hat. Nach Beendigung der Synchronisation wird der Replikationsmodus für den Clientknoten auf dem Quellenserver automatisch auf SEND gesetzt. Der Replikationsmodus lautet so lange SEND, bis Sie den Knoten mit dem Befehl REMOVE REPLNODE entfernen.

SYNCRECeive
Gibt an, dass Daten, die zu diesem Clientknoten gehören, während der Replikation mit Daten auf einem Quellenserver synchronisiert werden. Geben Sie diesen Wert nur auf dem Server an, der die Daten importiert hat. Nach Beendigung der Synchronisation wird der Replikationsmodus für den Clientknoten auf dem Zielserver automatisch auf RECEIVE gesetzt. Der Replikationsmodus lautet so lange RECEIVE, bis Sie den Knoten mit dem Befehl REMOVE REPLNODE entfernen.

Einschränkungen:

- Sie können den Parameter REPLMODE nur definieren, wenn der anfängliche Replikationsstatus NONE lautet. Um Daten zu synchronisieren, ändern Sie den Replikationsstatus in ENABLED oder DISABLED und geben Sie einen Wert für den Parameter REPLMODE an.
- Daten können nur synchronisiert werden, wenn Sie `DATES=ABSOLUTE` im Befehl IMPORT NODE angegeben haben. Wenn Sie `DATES=RELATIVE` angegeben haben, um Daten zu importieren, müssen Sie den Knoten vor der Replikation umbenennen oder seine Daten löschen. Wenn Sie nicht einen dieser Schritte ausführen, können Daten verloren gehen.
- Wurde der Parameter REPLMODE nicht korrekt definiert, müssen Sie den Befehl REMOVE REPLNODE ausgeben, bevor die Clientknotendefinition aktualisiert wird. Beispiel: Angenommen, Sie haben die Definition eines Clientknotens aktualisiert, dessen Daten repliziert werden sollten. Die Daten, die zu dem Knoten gehören, wurden zuvor auf den Zielreplikationsserver exportiert. Sie haben ENABLED als Einstellung des Parameters REPLSTATE angegeben. Sie haben jedoch nicht SYNCSEND auf dem Quellenreplikationsserver angegeben. Daher wurde der Parameter REPLMODE automatisch auf SEND gesetzt, und Daten, die zu dem Knoten gehören, konnten nicht synchronisiert oder repliziert werden.

  Mit dem Befehl REMOVE REPLNODE werden der Replikationsstatus und der Replikationsmodus auf NONE gesetzt. Geben Sie nach der Ausführung des Befehls REMOVE REPLNODE den Befehl UPDATE NODE mit den korrekten Parametern und Werten erneut aus.

RECOVERDamaged
Gibt an, ob beschädigte Dateien für diesen Knoten von einem Zielreplikationsserver wiederhergestellt werden können. Der Parameter ist wahlfrei.Der Standardwert ist YES. Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver für diesen Knoten aktiviert ist.

No
Gibt an, dass die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver für diesen Knoten nicht aktiviert ist. Tipp: Der Wert des Parameters RECOVERDAMAGED ist nur eine von mehreren Einstellungen, die bestimmen, ob beschädigte Dateien wiederhergestellt werden. Informationen zur Angabe der Einstellungen finden Sie in Einstellungen, die sich auf die Wiederherstellung beschädigter Dateien auswirken.

ROLEOVERRIDE

Gibt an, ob die zurückgemeldete Rolle des Clients für die Zurückmeldung der PVU-Schätzung (PVU - Prozessor-Value-Unit) überschrieben werden soll. Der Standardwert ist USEREPORTED.

Die vom Client zurückgemeldete Rolle ist entweder 'Clienteinheit' (z. B. eine Workstation) oder 'Servereinheit' (z. B. Datei-/Druckserver, Anwendungsserver, Datenbank). Standardmäßig meldet der Client seine Rolle auf der Basis des Clienttyps und des Betriebssystems zurück. Alle Clients melden anfänglich ihre Rolle als 'Servereinheit' zurück, mit Ausnahme von IBM Spectrum Protect-Clients für Sichern/Archivieren, auf denen Microsoft Windows-Workstationverteilungen (Windows Vista) und Macintosh OS X ausgeführt werden.

Geben Sie einen der folgenden Werte an:

Client
: Gibt eine Clienteinheit an.

Server
: Gibt eine Servereinheit an.

Other
: Gibt an, dass dieser Knoten nicht für die Zurückmeldung der PVU-Schätzung verwendet werden soll. Der Wert 'Other' kann nützlich sein, wenn mehrere Knoten für ein physisches System implementiert sind (z. B. virtuelle Umgebungen, Testknoten, Knoten im Ruhezustand und Knoten, die nicht in der Produktion oder im Clustering sind).

Usereported
: Die zurückgemeldete Rolle verwenden, die vom Client bereitgestellt wird.

AUTHentication
: Dieser Parameter bestimmt die von Ihnen verwendete Kennwortauthentifizierungmethode (LDAP oder LOCAL).

LOcal
: Gibt an, dass der Knoten die lokale IBM Spectrum Protect-Serverdatenbank zum Speichern von Kennwörtern verwendet.

LDap
: Gibt an, dass der Knoten einen LDAP-Verzeichnisserver für die Authentifizierung von Kennwörtern verwendet. Kennwörter werden nicht in der IBM Spectrum Protect-Datenbank gespeichert.

SYNCldapdelete
: Dieser Parameter gilt nur, wenn ein Knoten, der sich mit einem Lightweight Directory Access Protocol-Server (LDAP-Server) authentifiziert, zur Authentifizierung mit dem IBM Spectrum Protect-Server wechseln soll. Der Parameter gibt an, ob der Knoten auf dem LDAP-Server entfernt werden soll.

Yes
: Gibt an, dass der Knoten entfernt wird.
Einschränkung: Sie dürfen nicht den Wert YES angeben. (Der Wert YES ist nur für die Benutzer der vorherigen LDAP-Authentifizierungsmethode gültig, die in Kennwörter und Anmeldeverfahren verwalten beschrieben wird.)

No
: Gibt an, dass der Knoten nicht entfernt wird. Dies ist der Standardwert.

SSLrequired (veraltet)

: Gibt an, ob der Knoten das Protokoll Secure Sockets Layer (SSL) für die Kommunikation mit dem IBM Spectrum Protect-Server verwenden muss. Der Parameter ist wahlfrei.Wenn Sie Kennwörter mit einem LDAP-Verzeichnisserver authentifizieren, müssen Sie die Sitzungen mit SSL oder einer anderen Netzsicherheitsmethode schützen.

Wichtig: Ab Version 8.1.2 wird dieser Parameter nicht mehr verwendet. Die durch diesen Parameter aktivierte Validierung wird durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter SSLREQUIRED wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

SESSIONSECurity
: Gibt an, ob der Knoten die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

STRict
: Gibt an, dass die striktesten Sicherheitseinstellungen für den Knoten durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem Server und dem Knoten verwendet. Um anzugeben, ob der Server TLS 1.2 für die gesamte Sitzung oder nur für die Authentifizierung verwendet, lesen Sie die Informationen zur Clientoption SSL.
Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der Knoten mit dem Server authentifizieren kann:

- Der Knoten und der Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.
- Der Knoten muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen dem Server und dem Knoten konfiguriert werden.

Knoten, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem Server authentifizieren.

TRANSitional
: Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Knoten durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Knoten nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Knoten weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Knoten jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der

Knoten kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Knoten erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Knoten nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Knoten, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Knoten nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. virtuelle Datenträger, wenn sich der Knoten beim IBM Spectrum Protect-Server als Knoten von einem anderen Server authentifiziert.

SPLITLARGEObjects
Gibt an, ob große Objekte, die von diesem Knoten gespeichert werden, automatisch vom Server in kleinere Teile aufgeteilt werden, um die Serververarbeitung zu optimieren. Die Angabe von 'Yes' hat zur Folge, dass der Server große Objekte (über 10 GB) in kleinere Teile aufteilt, wenn sie von einem Clientknoten gespeichert werden. Bei Angabe von 'No' wird dieser Prozess übergangen. Geben Sie 'No' nur an, wenn Ihr primäres Ziel die Maximierung des Durchsatzes von Sicherungen direkt auf Band ist. Der Standardwert ist 'Yes'.

Beispiel: Der Knoten SIMON soll sich mit einem LDAP-Verzeichnisserver authentifizieren und die Verbindung über SSL herstellen

```
update node simon authentication=ldap sslrequired=yes
```

Wenn Sie den Parameter SSLREQUIRED angeben, wird der Server nicht automatisch für SSL konfiguriert. Sie müssen die Anweisungen zum Herstellen der Verbindung mit SSL befolgen, damit das Beispiel funktioniert.

Beispiel: Alle Knoten für die Kommunikation mit einem Server unter Verwendung der Sitzungssicherheit 'strict' aktualisieren

Alle Knoten für die Verwendung der striktesten Sicherheitseinstellungen aktualisieren, um sich mit dem Server zu authentifizieren.

```
update node * sessionsecurity=strict
```

Beispiel: Einen Knoten mit Informationen zu einem Software-Release für eine zukünftige Implementierung aktualisieren

Das Feature für die Clientimplementierung unterstützt Sie bei der Aktualisierung eines Clients für Sichern/Archivieren auf ein neues Release. Die Informationen, die von dem Befehl UPDATE NODE generiert werden, können Ihnen bei der Planung einer Implementierung helfen. Die Informationen werden für eine zukünftige Implementierung gespeichert und können mit dem Befehl QUERY NODE angezeigt werden. Nach einer Implementierung können Sie den Befehl QUERY NODE ausgeben, um die aktuelle Version und die Zielversion anzuzeigen. In diesem Beispiel soll der Knoten `LARRY` in Version 6.3.0.0 des Clients für Sichern/Archivieren aktualisiert werden.

```
update node LARRY targetlevel=6.3.0.0
```

Beispiel: Die Sicherung eines Knotens aktualisieren, um Daten zu komprimieren und zu verhindern, dass der Client archivierte Dateien löscht

Den Knoten `LARRY` so aktualisieren, dass die Daten auf dem Knoten `LARRY` komprimiert werden, wenn sie von IBM Spectrum Protect gesichert bzw. archiviert werden; außerdem soll dem Client nicht gestattet sein, archivierte Dateien zu löschen.

```
update node larry compression=yes archdelete=no
```

Beispiel: Die Anzahl der Dateien eines Knotens aktualisieren, die als Gruppe übertragen werden können

Den Knoten `LARRY` aktualisieren und den Wert für TXNGroupmax auf 1.000 erhöhen.

```
update node larry txngroupmax=1000
```

Beispiel: Einen Knoten aktualisieren und die Deduplizierung auf dem Client zulassen

Den Knoten `BOB` aktualisieren, damit er Daten auf dem Client deduplizieren kann.

```
update node bob deduplication=clientorserver
```

Beispiel: Die Rolle des Knotens BOB in eine Servereinheit für die Zurückmeldung der PVU-Schätzung aktualisieren

Sollen PVU-Werte akkumuliert werden, werden nur Servereinheitenrollen aufgezeichnet. Sie können einen Knoten von 'Clienteinheit' in 'Servereinheit' aktualisieren, indem Sie den Befehl UPDATE NODE ausgeben. In diesem Beispiel wird der Knoten `BOB` in eine Servereinheit aktualisiert.

```
update node bob role=server
```

Beispiel: Eine Knotendefinition auf einem Quellenreplikationsserver aktualisieren

NODE1 ist für einen Quellenreplikationsserver definiert. Die Daten, die zu NODE1 gehören, wurden zuvor auf einen Zielreplikationsserver exportiert. Die Replikationsregel für Sicherungsdaten, die zu NODE1 gehören, aktualisieren, sodass aktive Sicherungsdaten mit einer hohen Priorität repliziert werden. Die Replikation für den Knoten aktivieren. Die Datensynchronisation mit dem Zielreplikationsserver definieren.

```
update node node1 bkreplruledefault=active_data_high_priority
replstate=enabled replmode=syncsend
```

Beispiel: Eine Knotendefinition aktualisieren, um die Wiederherstellung beschädigter Dateien zu aktivieren

Den Knoten PAYROLL aktualisieren, um die Wiederherstellung beschädigter Dateien durch einen Zielreplikationsserver zu aktivieren.

```
update node payroll recoverdamaged=yes
```

Zugehörige Befehle

Tabelle 2. Zugehörige Befehle für UPDATE NODE

Befehl	Beschreibung
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY PVUESTIMATE	Zeigt eine Schätzung der Clienteinheiten und Servereinheiten an, die verwaltet werden.
QUERY REPLNODE	Zeigt Informationen zum Replikationsstatus eines Clientknotens an.
REGISTER ADMIN	Definiert einen neuen Administrator, ohne Administratorberechtigung zu erteilen.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
REMOVE REPLNODE	Entfernt einen Knoten aus der Replikation.
RENAME NODE	Ändert den Namen eines Clientknotens.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
RESET PASSEXP	Setzt die Kennwortablaufdauer für Knoten oder Administratoren zurück.
SET DEDUPVERIFICATIONLEVEL	Gibt den Prozentsatz der Bereiche an, die vom Server während der clientseitigen Deduplizierung geprüft werden sollen.
SET PASSEXP	Gibt die Anzahl Tage an, nach denen ein Kennwort abläuft und geändert werden muss.
SET REPLRECOVERDAMAGED	Gibt an, ob die Knotenreplikation aktiviert ist, um beschädigte Dateien durch einen Zielreplikationsserver wiederherzustellen.
UPDATE ADMIN	Ändert das Kennwort eines Administrators bzw. die zu einem Administrator gehörigen Kontaktinformationen.
UPDATE FILESPACE	Ändert Knotenreplikationsregeln für Dateibereiche.

Zugehörige Informationen:
Ssl (Clientoption)

UPDATE NODEGROUP (Knotengruppe aktualisieren)

Verwenden Sie diesen Befehl, um die Beschreibung einer Knotengruppe zu ändern.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Maßnahmenberechtigung erforderlich.

Syntax

```
>>-UPDate NODEGroup--Gruppenname--------------------------------->

>--DESCription--=--Beschreibung--------------------------------><
```

Parameter

Gruppenname
: Gibt den Namen der Knotengruppe an, deren Beschreibung aktualisiert werden soll.

DESCription (Erforderlich)
: Gibt eine Beschreibung der Knotengruppe an. Dieser Parameter ist erforderlich. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Enthält die Beschreibung Leerzeichen, schließen Sie die gesamte Beschreibung in Anführungszeichen ein.

Beispiel: Die Beschreibung einer Knotengruppe aktualisieren

Die Knotengruppe `group1` mit einer neuen Beschreibung aktualisieren.

```
update nodegroup group1 description="Personalabteilung"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE NODEGROUP

Befehl	Beschreibung
DEFINE BACKUPSET	Definiert eine zuvor generierte Sicherungsgruppe für einen Server.
DEFINE NODEGROUP	Definiert eine Gruppe von Knoten.
DEFINE NODEGROUPMEMBER	Fügt einer Knotengruppe einen Clientknoten hinzu.
DELETE BACKUPSET	Löscht eine Sicherungsgruppe.
DELETE NODEGROUP	Löscht eine Knotengruppe.
DELETE NODEGROUPMEMBER	Löscht einen Clientknoten aus einer Knotengruppe.
GENERATE BACKUPSET	Generiert eine Sicherungsgruppe mit den Daten eines Clients.
QUERY BACKUPSET	Zeigt Sicherungsgruppen an.
QUERY NODEGROUP	Zeigt Informationen zu Knotengruppen an.
UPDATE BACKUPSET	Aktualisiert den einer Sicherungsgruppe zugeordneten Aufbewahrungszeitraum.

UPDATE PATH (Pfad ändern)

Verwenden Sie diesen Befehl, um eine Pfaddefinition zu aktualisieren.

Syntax- und Parameterbeschreibungen sind für die folgenden Pfadtypen verfügbar.

- UPDATE PATH (Pfad ändern, wenn das Ziel ein Laufwerk ist)
- UPDATE PATH (Pfad ändern, wenn das Ziel ein Kassettenarchiv ist)
- AIX-BetriebssystemeLinux-BetriebssystemeUPDATE PATH (Pfad aktualisieren, wenn das Ziel ein ZOSMEDIA-Kassettenarchiv ist)

Ausführliche und aktuelle Informationen zur Einheitenunterstützung befinden sich auf der Website für unterstützte Einheiten für Ihr Betriebssystem:

- AIX-BetriebssystemeWindows-BetriebssystemeSupported devices for AIX and Windows
- Linux-BetriebssystemeSupported devices for Linux

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE PATH

Befehl	Beschreibung
DEFINE DATAMOVER	Definiert eine Einheit zum Versetzen von Daten für den IBM Spectrum Protect-Server.
DEFINE DRIVE	Ordnet ein Laufwerk einem Kassettenarchiv zu.
DEFINE LIBRARY	Definiert ein automatisiertes oder manuelles Kassettenarchiv.
DEFINE PATH	Definiert einen Pfad von einer Quelle zu einem Ziel.

Befehl	Beschreibung
DELETE PATH	Löscht einen Pfad von einer Quelle zu einem Ziel.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
UPDATE DATAMOVER	Ändert die Definition einer Einheit zum Versetzen von Daten.

UPDATE PATH (Pfad ändern, wenn das Ziel ein Laufwerk ist)

Verwenden Sie diese Syntax, wenn Sie die Definition eines Pfads zu einem Laufwerk aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate PATH--Quellenname--Zielname--------------------------->

>--SRCType--=--+-DATAMover-+--+------------------------+-------->
               '-SERVer----'  '-AUTODetect--=--+-No--+-'
                                               '-Yes-'

>--DESTType--=--DRive--LIBRary--=--Kassettenarchivname---------->

>--+--------------------------+--+--------------------+--------->
   '-DEVIce--=--Einheitenname-'  '-ONLine--=--+-Yes-+-'
                                              '-No--'

>--+-----------------------------------+----------------------><
   |               .-,---------------. |
   |               V                 | |
   '-DIRectory--=----Verzeichnisname-+-'
```

Parameter

Quellenname (Erforderlich)
: Gibt den Namen der Quelle des Pfads an. Dieser Parameter ist erforderlich.

Zielname (Erforderlich)
: Gibt den Namen des Ziels an. Dieser Parameter ist erforderlich.

SRCType (Erforderlich)
: Gibt den Typ der Quelle an. Dieser Parameter ist erforderlich. Gültige Werte:

  DATAMover
  : Gibt an, dass eine Einheit zum Versetzen von Daten die Quelle ist.

  SERVer
  : Gibt an, dass ein Server oder ein Speicheragent die Quelle ist.

AUTODetect
: Gibt an, ob die Seriennummer für ein Laufwerk oder Kassettenarchiv automatisch in IBM Spectrum Protect erkannt, gemeldet und aktualisiert wird. Dieser Parameter ist wahlfrei. Dieser Parameter ist nur für Pfade gültig, die von dem lokalen Server zu einem Laufwerk oder Kassettenarchiv definiert sind. Gültige Werte:

  No
  : Gibt an, dass die Seriennummer nicht automatisch aktualisiert wird.

  Yes
  : Gibt an, dass die Seriennummer automatisch aktualisiert wird, um dieselbe Seriennummer widerzuspiegeln, die das Laufwerk an IBM Spectrum Protect meldet.
  Wichtig:

  1. Wurde zuvor keine Seriennummer eingegeben, erhält AUTODETECT den Standardwert YES. Wurde zuvor eine Seriennummer eingegeben, erhält AUTODETECT den Standardwert NO.
  2. AUTODETECT=YES in diesem Befehl überschreibt die Seriennummer, die in dem Befehl DEFINE DRIVE definiert wurde.
  3. Wenn Sie DESTTYPE=DRIVE und AUTODETECT=YES definieren, wird die Elementnummer des Laufwerks in der IBM Spectrum Protect-Datenbank automatisch geändert, um dieselbe Elementnummer widerzuspiegeln, die der Seriennummer dieses Laufwerks entspricht. Dies gilt für Laufwerke in einem SCSI-Kassettenarchiv. Weitere Informationen zu der Elementnummer befinden sich in der Beschreibung des Befehls DEFINE DRIVE.
  4. Je nach Leistungsspektrum der Einheit wird der Parameter AUTODETECT möglicherweise nicht unterstützt.

DESTType=DRive (Erforderlich)

Gibt an, dass ein Laufwerk das Ziel ist. Ist das Ziel ein Laufwerk, müssen Sie einen Kassettenarchivnamen angeben. Dieser Parameter ist erforderlich.

LIBRary

Gibt den Namen des Kassettenarchivs an, dem das Laufwerk zugeordnet ist. Das Kassettenarchiv und seine Laufwerke müssen bereits für den Server definiert sein. Verläuft der Pfad von einer NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv, muss das Kassettenarchiv den Typ (LIBTYPE) SCSI, 349x oder ACSLS haben.

DEVIce

Gibt den Namen der Einheit an, die der Quelle bekannt ist, oder FILE an, wenn die Einheit ein logisches Laufwerk in einem Kassettenarchiv FILE ist.

AIX-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk. Für Beispiele siehe Tabelle 1.

Tabelle 1. Beispiele für Einheitennamen

Quelle zum Ziel	**Beispiel**
Server zu einem Laufwerk (kein FILE-Laufwerk)	AIX-Betriebssysteme`/dev/rmt3`
Speicheragent zu einem Laufwerk (kein FILE-Laufwerk)	`mt3`
Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist	`FILE`
NAS-Einheit zum Versetzen von Daten zu einem Laufwerk	NetApp NAS-Dateiserver: `rst01` EMC Celerra NAS-Dateiserver: `c436t0l1` IBM® System Storage N Series: `rst01`

Linux-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk. Für Beispiele siehe Tabelle 2.

Tabelle 2. Beispiele für Einheitennamen

Quelle zum Ziel	**Beispiel**
Server zu einem Laufwerk (kein FILE-Laufwerk)	`/dev/tsmscsi/mt3`
Speicheragent zu einem Laufwerk (kein FILE-Laufwerk)	`/dev/tsmscsi/mt3`
Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist	`FILE`
NAS-Einheit zum Versetzen von Daten zu einem Laufwerk	NetApp NAS-Dateiserver: `rst01` EMC Celerra NAS-Dateiserver: `c436t0l1` IBM System Storage N Series: `rst01`

Windows-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk. Für Beispiele siehe Tabelle 3.

Tabelle 3. Beispiele für Einheitennamen

Quelle zum Ziel	**Beispiel**
Server zu einem Laufwerk (kein FILE-Laufwerk)	 Windows-Betriebssystememt3
Server zu einem Laufwerk (REMOVABLEFILE-Laufwerk)	`e:`
Speicheragent zu einem Laufwerk (kein FILE-Laufwerk)	`mt3`
Speicheragent zu einem Laufwerk, wenn das Laufwerk ein logisches Laufwerk in einem FILE-Kassettenarchiv ist	`FILE`
NAS-Einheit zum Versetzen von Daten zu einem Laufwerk	NetApp NAS-Dateiserver: `rst01` EMC Celerra NAS-Dateiserver: `c436t0l1` IBM System Storage N Series: `rst01`

Wichtig:

- Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei /etc/ibmatl.conf angegeben ist. Weitere Informationen enthält das Handbuch *IBM Tape Device Drivers Installation and User's Guide*, das von der Site der IBM Systemunterstützung unter http://www.ibm.com/support/docview.wss?uid=ssg1S7002972 heruntergeladen werden kann.
- Informationen über Namen für Einheiten, die mit einem NAS-Dateiserver verbunden sind, enthält die Produktinformation für den Dateiserver. Beispiel: Stellen Sie für einen NetApp-Dateiserver unter Verwendung von Telnet eine Verbindung zu dem Dateiserver her und geben Sie den Befehl SYSCONFIG aus. Verwenden Sie diesen Befehl, um Einheitennamen für Laufwerke zu bestimmen:

  ```
  sysconfig -t
  ```

ONLine

Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Gültige Werte:

Yes

Gibt an, dass der Pfad für die Verwendung verfügbar ist.

No

Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.

Ist beispielsweise der Pfad von einer Einheit zum Versetzen von Daten zu einem Laufwerk online, aber ist entweder die Einheit zum Versetzen von Daten oder das Laufwerk offline, kann der Pfad nicht verwendet werden.

DIRectory

Gibt die Verzeichnisposition(en) für einen Speicheragenten für den Zugriff auf die Dateien in einem FILE-Kassettenarchiv an. Der Parameter DIRECTORY wird auch für Einheiten des Typs REMOVABLEFILE verwendet. Für Einheiten des Typs REMOVABLEFILE stellt der Parameter DIRECTORY in Verbindung mit dem Parameter DRIVE dem Server (kein Speicheragent) Informationen zur Verfügung, die den Zugriff auf die Einheit beschreiben. Dieser Parameter ist wahlfrei.
Auf Speicheragenten ist dieser Parameter nur gültig, wenn *alle* folgenden Bedingungen zutreffen:

- Der Quellentyp ist SERVER (d. h., ein Speicheragent, der für diesen Server als Server definiert wurde).
- Der Quellenname ist der Name eines Speicheragenten, *nicht* der Servername.
- Das Ziel ist ein logisches Laufwerk, das Teil eines FILE-Kassettenarchivs ist.
- Wurden mehrere Verzeichnisse für die Einheitenklasse angegeben, die dem FILE-Kassettenarchiv zugeordnet ist, muss dieselbe Anzahl Verzeichnisse mit dem Parameter DIRectory des Befehls DEFINE PATH für jedes Laufwerk in dem FILE-Kassettenarchiv angegeben werden. Verzeichnisse des Speicheragenten werden auf dem Server nicht geprüft. Werden falsche Verzeichnisse angegeben, kann dies einen Laufzeitfehler verursachen.

Der Verzeichnisname/die Verzeichnisnamen identifiziert/identifizieren die Position(en), an der/denen der Speicheragent die Dateien liest und schreibt, die Speicherdatenträger für die Einheitenklasse FILE darstellen, die dem FILE-Kassettenarchiv zugeordnet ist. Der Standardwert für DIRECTORY ist das Verzeichnis des Servers zum Zeitpunkt der Befehlsausgabe.

Verwenden Sie eine Namenskonvention, mit der Sie das Verzeichnis einem bestimmten physischen Laufwerk zuordnen können. Damit kann sichergestellt werden, dass Ihre Konfiguration für die gemeinsame Benutzung des FILE-Kassettenarchivs zwischen dem Server und dem Speicheragenten gültig ist. Befindet sich der Speicheragent auf einem Windows-System, verwenden Sie eine allgemeine Namenskonvention. Verfügt der Speicheragent nicht über die Berechtigung für den Zugriff auf fernen Speicher, treten Mountfehler im Speicheragenten auf.

 Das dem Speicheragentendienst zugeordnete Konto muss ein Konto in der Gruppe der lokalen Administratoren oder ein Konto in der Gruppe der Domänenadministratoren sein. Befindet sich das Konto in der Gruppe der lokalen Administratoren, müssen Benutzer-ID und Kennwort den Angaben eines Kontos entsprechen, das über Berechtigungen für den Zugriff auf Speicher verfügt, der von der Maschine bereitgestellt wird, die den fernen Sharepunkt verwaltet. Wenn beispielsweise ein SAMBA-Server Zugriff auf fernen Speicher bereitstellt, müssen Benutzer-ID und Kennwort in der SAMBA-Konfiguration der Benutzer-ID und dem Kennwort des lokalen Administrators entsprechen, der dem Speicheragentendienst zugeordnet ist.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
define path sta1 file1 srctype=server desttype=drive
library=file1 device=file directory=\\192.168.1.10\filedir\dir1
```

In dem vorherigen Beispiel baut der Befehl DEFINE DEVCLASS das gemeinsam genutzte Dateisystem in dem Verzeichnis auf, auf das der Server als D:\FILEDIR\DIR1 zugreift. Der Speicheragent verwendet jedoch den UNC-Namen \\192.168.1.10\FILEDIR\DIR1. Das bedeutet, dass die Maschine mit TCP/IP-Adresse 192.168.1.10 dasselbe Verzeichnis gemeinsam nutzt, wobei FILEDIR als gemeinsam genutzter Name verwendet wird. Außerdem verfügt der Speicheragentendienst über ein Konto, das auf diesen Speicher zugreifen kann. Der Zugriff ist möglich, weil das Konto einem lokalen Konto mit derselben Benutzer-ID und demselben Kennwort wie 192.168.1.10 zugeordnet ist oder weil es einem Domänenkonto zugeordnet ist, das sowohl auf dem Speicheragenten als auch auf 192.168.1.10 verfügbar ist. Sie können gegebenenfalls 192.168.1.10 durch einen symbolischen Namen wie folgt ersetzen:

```
Beispiel.IhreFirma.com
```

Wichtig:

- IBM Spectrum Protect erstellt keine Shares oder Berechtigungen und lädt nicht das Zieldateisystem. Sie müssen diese Aktionen ausführen, bevor der Speicheragent gestartet wird.
- Sie können eine Verzeichnisliste nur ändern, indem Sie die gesamte Liste ersetzen.
- Sie müssen sicherstellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können. Für den Zugriff auf FILE-Datenträger ersetzen Speicheragenten Namen aus der Verzeichnisliste in der Einheitenklassendefinition durch die Namen in der Verzeichnisliste für die zugeordnete Pfaddefinition. Der folgende Abschnitt verdeutlicht die Bedeutung übereinstimmender Einheitenklassen und Pfade, um sicherzustellen, dass Speicheragenten auf neu erstellte FILE-Datenträger zugreifen können.
  Beispiel: Sie möchten folgende drei Verzeichnisse für ein FILE-Kassettenarchiv verwenden:
  - c:\server
  - d:\server
  - e:\server

   
  - /opt/tivoli1
  - /opt/tivoli2
  - /opt/tivoli3

1. Sie verwenden den folgenden Befehl, um ein FILE-Kassettenarchiv mit dem Namen CLASSA mit einem Laufwerk mit dem Namen *CLASSA1* auf *SERVER1* zu definieren: Windows-Betriebssysteme

   ```
   define devclass classa devtype=file
   directory="c:\server,d:\server,e:\server"
   shared=yes mountlimit=1
   ```

   AIX-BetriebssystemeLinux-Betriebssysteme

   ```
   define devclass classa devtype=file
   directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
   shared=yes mountlimit=1
   ```

2. Sie wollen, dass der Speicheragent `STA1` das FILE-Kassettenarchiv verwenden kann. Daher definieren Sie folgenden Pfad für Speicheragent `STA1`: Windows-Betriebssysteme

   ```
   define path server1 sta1 srctype=server desttype=drive device=file
   directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
   \\192.168.1.10\e\server" library=classa
   ```

   Windows-BetriebssystemeIn diesem Szenario ersetzt der Speicheragent `STA1` den Verzeichnisnamen c:\server durch den Verzeichnisnamen \\192.168.1.10\c\server, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis c:\server auf dem Server befinden.

   AIX-BetriebssystemeLinux-Betriebssysteme

   ```
   define path server1 sta1 srctype=server desttype=drive device=file
   directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
   ```

   AIX-BetriebssystemeLinux-BetriebssystemeIn diesem Szenario ersetzt der Speicheragent `STA1` den Verzeichnisnamen /opt/tivoli1 durch den Verzeichnisnamen /opt/ibm1/, um auf FILE-Datenträger zuzugreifen, die sich in dem Verzeichnis /opt/tivoli1 auf dem Server befinden.

3. Windows-BetriebssystemeFILE-Datenträger c:\server\file1.dsm wird durch SERVER1 erstellt. Wenn Sie das erste Verzeichnis für die Einheitenklassen später mit folgendem Befehl ändern:

   ```
   update devclass classa directory="c:\otherdir,d:\server,e:\server"
   ```

   kann *SERVER1* weiterhin auf FILE-Datenträger c:\server\file1.dsm zugreifen, der Speicheragent `STA1` jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.
4. AIX-BetriebssystemeLinux-BetriebssystemeWird der FILE-Datenträger /opt/tivoli1/file1.dsm auf *SERVER1* erstellt und wird der Befehl

   ```
   update devclass classa directory="/opt/otherdir,/opt/tivoli2,
   /opt/tivoli3"
   ```

   ausgegeben, kann *SERVER1* weiterhin auf FILE-Datenträger /opt/tivoli1/file1.dsm zugreifen, der Speicheragent `STA1` jedoch nicht, weil in der PATH-Verzeichnisliste kein übereinstimmender Verzeichnisname mehr vorhanden ist. Ist kein Verzeichnisname in der Verzeichnisliste verfügbar, die der Einheitenklasse zugeordnet ist, kann der Speicheragent den Zugriff auf einen FILE-Datenträger in diesem Verzeichnis verlieren. Obwohl der Server zum Lesen noch auf den Datenträger zugreifen kann, kann der fehlgeschlagene Zugriff des Speicheragenten auf den FILE-Datenträger dazu führen, dass Operationen nur auf einem LAN-Pfad wiederholt werden können oder dass sie fehlschlagen.

Beispiel: Einen Pfad von einer Einheit zum Versetzen von Daten, die ein NAS-Dateiserver ist, zu einem Bandlaufwerk aktualisieren

Einen Pfad von einer Einheit zum Versetzen von Daten, die ein NAS-Dateiserver ist, zu dem Laufwerk *TAPEDRV2* aktualisieren, das von der Einheit zum Versetzen von Daten für Sicherungs- und Zurückschreibungsoperationen verwendet wird. In diesem Beispiel hat die NAS-Einheit zum Versetzen von Daten den Namen *NAS1*, das Kassettenarchiv ist *NASLIB* und der Einheitenname für das Laufwerk lautet *rst0l*.

```
update path nas1 tapedrv2 srctype=datamover desttype=drive library=naslib
    device=rst0l
```

UPDATE PATH (Pfad ändern, wenn das Ziel ein Kassettenarchiv ist)

Verwenden Sie diese Syntax, wenn Sie die Definition eines Pfads zu einem Kassettenarchiv aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate PATH--Quellenname--Zielname--------------------------->

>--SRCType--=--+-DATAMover-+--+-----------------------+-------->
               '-SERVer----'  '-AUTODetect--=--+-No--+-'
                                               '-Yes-'

>--DESTType--=--LIBRary--+-------------------------------+------->
                         +-DEVIce--=--Einheitenname-----+
                         '-EXTERNALManager--=--Pfadname-'

>--+--------------------+---------------------------------------><
   '-ONLine--=--+-Yes-+-'
                '-No--'
```

Parameter

Quellenname (Erforderlich)
Gibt den Namen der Quelle des Pfads an. Dieser Parameter ist erforderlich.

Zielname (Erforderlich)
Gibt den Namen des Ziels an. Dieser Parameter ist erforderlich.
Wichtig: Um einen Pfad von einer NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv zu definieren, muss das Kassettenarchiv den Typ (LIBTYPE) SCSI, 349X oder Automated Cartridge System Library Software (ACSLS) haben.

SRCType (Erforderlich)
Gibt den Typ der Quelle an. Dieser Parameter ist erforderlich. Gültige Werte:

DATAMover
Gibt an, dass eine Einheit zum Versetzen von Daten die Quelle ist.

SERVer
Gibt an, dass ein Server oder ein Speicheragent die Quelle ist.

AUTODetect
Gibt an, ob die Seriennummer für ein Laufwerk oder Kassettenarchiv automatisch in IBM Spectrum Protect erkannt, gemeldet und aktualisiert wird. Dieser Parameter ist wahlfrei. Dieser Parameter ist nur für Pfade gültig, die von dem lokalen Server zu einem Kassettenarchiv definiert sind. Gültige Werte:

No
Gibt an, dass die Seriennummer nicht automatisch aktualisiert wird.

Yes
Gibt an, dass die Seriennummer automatisch aktualisiert wird, um dieselbe Seriennummer widerzuspiegeln, die das Laufwerk an IBM Spectrum Protect meldet.
Wichtig:

1. Wurde zuvor keine Seriennummer eingegeben, erhält AUTODETECT den Standardwert YES. Wurde zuvor eine Seriennummer eingegeben, erhält AUTODETECT den Standardwert NO.
2. AUTODETECT=YES in diesem Befehl überschreibt die Seriennummer, die in dem Befehl DEFINE DRIVE definiert wurde.
3. Je nach Leistungsspektrum der Einheit wird der Parameter AUTODETECT möglicherweise nicht unterstützt.

DESTType=LIBRary (Erforderlich)
Gibt an, dass ein Kassettenarchiv das Ziel ist. Dieser Parameter ist erforderlich.

DEVIce
Gibt den Namen der Einheit an, die der Quelle bekannt ist, oder FILE an, wenn die Einheit ein logisches Laufwerk in einem Kassettenarchiv FILE ist.
 AIX-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk oder das Kassettenarchiv. Für Beispiele siehe Tabelle 1.

Tabelle 1. Beispiele für Einheitennamen

Quelle zum Ziel	Beispiel
Server zu einem Kassettenarchiv	 AIX-Betriebssysteme/dev/lb4  Linux-Betriebssysteme/dev/tsmscsi/lb4
NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv	mc0

 Linux-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk oder das Kassettenarchiv. Für Beispiele siehe Tabelle 2.

Tabelle 2. Beispiele für Einheitennamen

Quelle zum Ziel	Beispiel
Server zu einem Kassettenarchiv	/dev/tsmscsi/lb4
NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv	mc0

Windows-BetriebssystemeDie Quelle verwendet den Einheitennamen für den Zugriff auf das Laufwerk oder das Kassettenarchiv. Für Beispiele siehe Tabelle 3.

Tabelle 3. Beispiele für Einheitennamen

Quelle zum Ziel	Beispiel
Server zu einem Kassettenarchiv	Windows-Betriebssystemelb4.1
NAS-Einheit zum Versetzen von Daten zu einem Kassettenarchiv	mc0

Wichtig:

- Für 349X-Kassettenarchive ist der Aliasname ein symbolischer Name, der in der Datei /etc/ibmatl.conf angegeben ist. Weitere Informationen enthält das Handbuch *IBM Tape Device Drivers Installation and User's Guide*, das von der Site der IBM® Systemunterstützung unter http://www.ibm.com/support/docview.wss?uid=ssg1S7002972 heruntergeladen werden kann.
- Informationen über Namen für Einheiten, die mit einem NAS-Dateiserver verbunden sind, enthält die Produktinformation für den Dateiserver. Beispiel: Stellen Sie für einen NetApp-Dateiserver unter Verwendung von Telnet eine Verbindung zu dem Dateiserver her und geben Sie den Befehl SYSCONFIG aus. Verwenden Sie diesen Befehl, um den Einheitennamen für ein Kassettenarchiv zu bestimmen:

  ```
  sysconfig -m
  ```

EXTERNALManager
: Gibt den Standort des externen Kassettenarchivmanagers an, an den IBM Spectrum Protect Zugriffsanforderungen für Datenträger senden kann. Der Wert dieses Parameters muss zwischen einfachen Anführungszeichen stehen. Geben Sie beispielsweise Folgendes ein:
AIX-Betriebssysteme

  ```
  /usr/lpp/GESedt-acsls/bin/elmdt
  ```

Linux-Betriebssysteme

  ```
  /opt/GESedt-acsls/bin/elmdt
  ```

Windows-Betriebssysteme

  ```
  C:\Programme\GES\EDT-ACSLS\bin\elmdt.exe
  ```

  Dieser Parameter ist erforderlich, wenn das Kassettenarchiv ein externes Kassettenarchiv ist.

ONLine
: Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Gültige Werte:

  Yes
  : Gibt an, dass der Pfad für die Verwendung verfügbar ist.

  No
  : Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

  Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.

  Wichtig: Ist der Pfad zu einem Kassettenarchiv offline, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während der Pfad zu dem Kassettenarchiv offline ist, wird das Kassettenarchiv nicht initialisiert.

AIX-BetriebssystemeLinux-Betriebssysteme

UPDATE PATH (Pfad aktualisieren, wenn das Ziel ein ZOSMEDIA-Kassettenarchiv ist)

Verwenden Sie diese Syntax, wenn Sie einen Pfad zu einem ZOSMEDIA-Kassettenarchiv aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate PATH--Quellenname--Zielname--SRCType--=--SERVer------->

>--DESTType--=--LIBRary--ZOSMEDIASERVER--=--Servername---------->

>--+-------------------+-------------------------------------><
   '-ONLine--=--+-Yes-+-'
                '-No--'
```

Parameter

Quellenname (Erforderlich)
: Gibt den Namen der Quelle des Pfads an.

Zielname (Erforderlich)
: Gibt den Namen des Ziels an.

SRCType=SERVer (Erforderlich)
: Gibt an, dass der IBM Spectrum Protect-Server oder ein Speicheragent die Quelle ist.

DESTType=LIBRary (Erforderlich)
: Gibt an, dass ein Kassettenarchiv das Ziel ist.

ZOSMEDIAServer (Erforderlich)
: Gibt den Namen eines Servers an, der einen Tivoli Storage Manager for z/OS Media-Server darstellt.

ONLine
: Gibt an, ob der Pfad für die Verwendung verfügbar ist. Dieser Parameter ist wahlfrei. Gültige Werte:

  Yes
  : Gibt an, dass der Pfad für die Verwendung verfügbar ist.

  No
  : Gibt an, dass der Pfad nicht für die Verwendung verfügbar ist.

  Die Quelle und das Ziel müssen verfügbar sein, um den Pfad verwenden zu können.

  Wichtig: Ist der Pfad zu einem Kassettenarchiv offline, kann der Server nicht auf das Kassettenarchiv zugreifen. Wird der Server angehalten und erneut gestartet, während der Pfad zu dem Kassettenarchiv offline ist, wird das Kassettenarchiv während der Serverinitialisierung nicht initialisiert. Der Pfad muss in ONLINE=YES aktualisiert werden, um auf das Kassettenarchiv zuzugreifen.

UPDATE POLICYSET (Beschreibung einer Maßnahmengruppe aktualisieren)

Mit diesem Befehl kann die Beschreibung einer Maßnahmengruppe geändert werden. Die Beschreibung der aktiven (ACTIVE) Maßnahmengruppe kann nicht geändert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

Syntax

```
>>-UPDate POlicyset--Domänenname--Name_der_Maßnahmengruppe------>

>--DESCription--=--Beschreibung-------------------------------><
```

Parameter

Domänenname (Erforderlich)
: Gibt die Maßnahmendomäne an, zu der die Maßnahmengruppe gehört.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt die Maßnahmengruppe an, die aktualisiert werden soll. Die aktive Maßnahmengruppe (ACTIVE) kann nicht geändert werden.

DESCription (Erforderlich)
: Gibt den Text an, der die Maßnahmengruppe beschreibt. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine Nullzeichenfolge ("") anzugeben.

Beispiel: Eine Maßnahmengruppe aktualisieren

Für die Maßnahmengruppe `VACATION` (Maßnahmendomäne `EMPLOYEE_RECORDS`) soll die Beschreibung "Schedule Planning Information" vergeben werden.

```
update policyset employee_records vacation
description="schedule planning information"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE POLICYSET

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.

Befehl	Beschreibung
COPY MGMTCLASS	Erstellt eine Kopie einer Verwaltungsklasse.
DEFINE DOMAIN	Definiert eine Maßnahmendomäne, der Clients zugeordnet werden können.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DEFINE POLICYSET	Definiert eine Maßnahmengruppe innerhalb der angegebenen Maßnahmendomäne.
DELETE POLICYSET	Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
VALIDATE POLICYSET	Prüft und berichtet Bedingungen, die der Administrator in Betracht ziehen muss, bevor er die Maßnahmengruppe aktiviert.

UPDATE PROFILE (Profilbeschreibung aktualisieren)

Mit diesem Befehl kann auf einem Konfigurationsmanager eine Profilbeschreibung aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-UPDate PROFIle--Profilname--DESCription--=--Beschreibung---><
```

Parameter

Profilname (Erforderlich)
: Gibt das Profil an, das aktualisiert werden soll.

DESCription (Erforderlich)
: Gibt eine Beschreibung für das Profil an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Soll eine Beschreibung entfernt werden, eine Nullzeichenfolge ("") angeben.

Beispiel: Die Beschreibung eines Profils aktualisieren

Die Beschreibung für Profil DELTA aktualisieren.

```
update profile delta description="PAYROLL domain"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE PROFILE

Befehl	Beschreibung
COPY PROFILE	Erstellt eine Kopie eines Profils.
DEFINE PROFASSOCIATION	Ordnet Objekte einem Profil zu.
DEFINE PROFILE	Definiert ein Profil für die Verteilung von Informationen an verwaltete Server.
DELETE PROFASSOCIATION	Löscht die Zuordnung zwischen einem Objekt und einem Profil.
DELETE PROFILE	Löscht ein Profil aus einem Konfigurationsmanager.
LOCK PROFILE	Verhindert die Verteilung eines Konfigurationsprofils.
QUERY PROFILE	Zeigt Informationen über Konfigurationsprofile an.
SET CONFIGMANAGER	Gibt an, ob ein Server ein Konfigurationsmanager ist.
UNLOCK PROFILE	Ermöglicht die Verteilung eines gesperrten Profils an verwaltete Server.

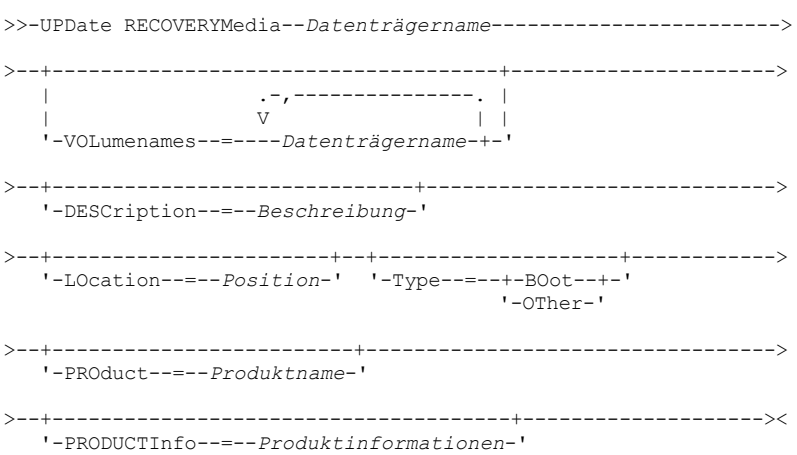
UPDATE RECOVERYMEDIA (Wiederherstellungsdatenträger aktualisieren)

Mit diesem Befehl können Informationen über Wiederherstellungsdatenträger aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Datenträgername (Erforderlich)
: Gibt den Namen des Wiederherstellungsdatenträgers an, der aktualisiert werden soll.

VOLumenames
: Gibt die Namen der Datenträger an, die die wiederherstellbaren Daten enthalten (z. B. Abbildkopien des Betriebssystems). Wird TYPE=BOOT angegeben, müssen die Boot-Datenträger in der Reihenfolge angegeben werden, in der sie zur Wiederherstellungszeit geladen werden sollen. Die Datenträgernamensliste kann bis zu 255 Zeichen umfassen. Die Liste in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Sollen alle Datenträgernamen entfernt werden, eine Nullzeichenfolge ("") angeben.

DESCription
: Gibt die Beschreibung der Wiederherstellungsdatenträger an. Dieser Parameter ist wahlfrei. Es können bis zu 255 Zeichen verwendet werden. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

LOcation
: Beschreibt den Standort der Wiederherstellungsdatenträger. Dieser Parameter ist wahlfrei. Es können bis zu 255 Zeichen verwendet werden. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.Soll eine Positionsbeschreibung entfernt werden, eine Nullzeichenfolge ("") für den Wert angeben.

Type
: Gibt den Typ von Wiederherstellungsdatenträger an. Dieser Parameter ist wahlfrei. Gültige Werte:

  BOot
  : Gibt an, daß dies ein Boot-Datenträger ist. Der Benutzer muß Datenträgernamen angeben, wenn der Typ BOOT lautet.

  OTher
  : Gibt an, daß dies kein Boot-Datenträger ist. Beispielsweise eine CD, die Handbücher zum Betriebssystem enthält.

PROduct
: Gibt den Namen des Produkts an, das auf diesen Datenträger geschrieben hat. Dieser Parameter ist wahlfrei. Es können bis zu 16 Zeichen verwendet werden. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.Soll ein Produktname entfernt werden, eine Nullzeichenfolge ("") für den Wert angeben.

PRODUCTInfo
: Gibt alle Informationen über das Produkt an, das auf die Datenträger geschrieben hat, die möglicherweise für die Wiederherstellung der Maschine benötigt werden. Dieser Parameter ist wahlfrei. Es können bis zu 255 Zeichen verwendet werden. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.Sollen zuvor definierte Produktinformationen entfernt werden, eine Nullzeichenfolge ("") für den Wert angeben.

Beispiel: Die Standortbeschreibung eines Wiederherstellungsdatenträgers aktualisieren

Die Standortbeschreibung für den Wiederherstellungsdatenträger DIST5RM in "Corporate Headquarters Data Vault" aktualisieren.

```
update recoverymedia dist5rm
location="Corporate Headquarters Data Vault"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE RECOVERYMEDIA

Befehl	Beschreibung
DEFINE RECOVERYMEDIA	Definiert die Datenträger, die für die Wiederherstellung einer Maschine erforderlich sind.
DELETE RECOVERYMEDIA	Löscht Wiederherstellungsdatenträger.
QUERY RECOVERYMEDIA	Zeigt die für die Maschinenwiederherstellung verfügbaren Datenträger an.

UPDATE REPLRULE (Replikationsregeln aktualisieren)

Verwenden Sie diesen Befehl, um eine Replikationsregel zu aktivieren oder zu inaktivieren.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-UPDate REPLRule--Regelname----STate--=--+-ENabled--+-------><
                                           '-DISabled-'
```

Parameter

Regelname (Erforderlich)

Gibt den Namen der Replikationsregel an, die aktualisiert werden soll. Sie können Platzhalterzeichen verwenden, um eine oder mehrere Regeln anzugeben. Sie können eine der folgenden Regeln angeben:

- ALL_DATA
- ACTIVE_DATA
- ALL_DATA_HIGH_PRIORITY
- ACTIVE_DATA_HIGH_PRIORITY

STate (Erforderlich)

Gibt an, ob die Replikation für die Regel zulässig ist. Sie können einen der folgenden Werte angeben:

ENabled
: Gibt an, dass die Daten, für die die Regel gilt, für die Replikation bereit sind.

DISabled
: Gibt an, dass die Replikation erst stattfindet, wenn sie aktiviert wurde.

Beispiel: Die Replikation für Sicherungsdaten inaktivieren

Die Replikation von aktiven Sicherungsdaten mit normaler Priorität für alle Dateibereiche in allen Clientknoten inaktivieren, die für die Replikation konfiguriert sind.

```
update replrule active_data state=disabled
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE REPLRULE

Befehl	Beschreibung
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY REPLICATION	Zeigt Informationen zu Knotenreplikationsprozessen an.
QUERY REPLRULE	Zeigt Informationen zu Knotenreplikationsregeln an.

Befehl	Beschreibung
SET ARREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für Archivierungsdaten an.
SET BKREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für Sicherungsdaten an.
SET SPREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für speicherverwaltete Daten an.
UPDATE FILESPACE	Ändert Knotenreplikationsregeln für Dateibereiche.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.
VALIDATE REPLICATION	Überprüft die Replikation für Dateibereiche und Datentypen.

UPDATE SCHEDULE (Zeitplan aktualisieren)

Mit diesem Befehl kann ein Zeitplan für einen Client oder Verwaltungsbefehl aktualisiert werden.

Der Befehl UPDATE SCHEDULE kann zwei Formen haben, je nachdem, ob der Zeitplan Client-Operationen oder Verwaltungsbefehle betrifft. Innerhalb dieser beiden Formen können Sie entweder Zeitpläne mit klassischer Darstellung oder Zeitpläne mit erweiterter Darstellung auswählen. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für UPDATE SCHEDULE

Befehl	Beschreibung
COPY SCHEDULE	Erstellt eine Kopie eines Zeitplans.
DEFINE SCHEDULE	Definiert einen Zeitplan für eine Clientoperation oder einen Verwaltungsbefehl.
DELETE SCHEDULE	Löscht einen Zeitplan aus der Datenbank.
QUERY EVENT	Zeigt Informationen über geplante und abgeschlossene Ereignisse für ausgewählte Clients an.
QUERY SCHEDULE	Zeigt Informationen über Zeitpläne an.
SET MAXCMDRETRIES	Gibt die maximale Anzahl Wiederholungen nach der fehlgeschlagenen Ausführung eines geplanten Befehls an.
SET MAXSCHEDSESSIONS	Gibt die maximale Anzahl Client-/Serversitzungen an, die bei der Arbeit mit einem Verarbeitungszeitplan verfügbar sind.
SET RETRYPERIOD	Gibt die Zeitspanne zwischen Wiederholungsversuchen des Client-Schedulers an.

- UPDATE SCHEDULE (Clientzeitplan aktualisieren)
  Mit dem Befehl UPDATE SCHEDULE können ausgewählte Parameter für einen Clientzeitplan aktualisiert werden.
- UPDATE SCHEDULE (Verwaltungszeitplan aktualisieren)
  Mit diesem Befehl können ausgewählte Parameter für einen Verwaltungszeitplan aktualisiert werden.

UPDATE SCHEDULE (Clientzeitplan aktualisieren)

Mit dem Befehl UPDATE SCHEDULE können ausgewählte Parameter für einen Clientzeitplan aktualisiert werden.

Dieser Befehl ändert nicht die Clientzuordnungen, die für diesen Zeitplan vorgenommen wurden. Alle dem Originalzeitplan zugeordneten Clients verarbeiten den geänderten Zeitplan.

Nicht alle Clients können alle geplanten Operationen ausführen, auch wenn Sie den Zeitplan auf dem Server definieren und ihn dem Client zuordnen können. Ein Macintosh-Client kann beispielsweise keinen Zeitplan ausführen, wenn es sich bei der Aktion um das Zurückschreiben oder Abrufen von Dateien oder um das Ausführen einer ausführbaren Prozedur handelt. Eine ausführbare Prozedur wird auch als Befehlsdatei, Stapeldatei oder Prozedur auf anderen Client-Betriebssystemen bezeichnet.

Berechtigungsklasse

Zum Aktualisieren eines Clientzeitplans ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der der Zeitplan gehört.

Syntax für einen klassischen Clientzeitplan

```
                    (1)
>>-UPDate SCHedule--------Domänenname--Zeitplanname------------>
```

```
>--+-----------------+--+-----------------------------+-------->
   '-Type--=--Client-'  '-DESCription--=--Beschreibung-'

>--+-------------------------------------------------------------+-->
   '-ACTion--=--+-Incremental--------------------------------+-'
                +-Selective----------------------------------+
                +-Archive--+-------------------------------+---+
                |          |               .-""-------. |   |
                |          '-SUBACTion--=--+----------+-'   |
                |                          '-FASTBack-'     |
                +-Backup--+-------------------------------+-+
                |         |               .-""----------. | |
                |         '-SUBACTion--=--+--------------+-' |
                |                         +-FASTBack----+   |
                |                         +-SYSTEMSTate-+   |
                |                         '-VM----------'   |
                +-REStore------------------------------------+
                +-RETrieve-----------------------------------+
                +-IMAGEBACkup--------------------------------+
                +-IMAGEREStore-------------------------------+
                +-Command------------------------------------+
                +-Macro--------------------------------------+
                '-Deploy-------------------------------------'

>--+---------------------------------+------------------------->
   '-OPTions--=--Optionszeichenfolge-'

>--+---------------------------------+--+--------------------+---->
   '-OBJects--=--Objektzeichenfolge-'  '-PRIority--=--Zahl-'

>--+---------------------+--+--------------------+-------------->
   '-STARTDate--=--Datum-'  '-STARTTime--=--Zeit-'

>--+--------------------+--+-----------------------------+------->
   '-DURation--=--Zahl-'  '-DURUnits--=--+-Minutes----+-'
                                         +-Hours------+
                                         +-Days-------+
                                         '-INDefinite-'

>--+-----------------------+--+------------------------+-------->
   '-MAXRUNtime--=--Anzahl-'  '-SCHEDStyle--=--Classic-'

>--+-----------------+--+--------------------------------+------------>
   '-PERiod--=--Zahl-'  '-PERUnits--=--+-Hours---+-'
                                       +-Days----+
                                       +-Weeks---+
                                       +-Months--+
                                       +-Years---+
                                       '-Onetime-'

>--+-----------------------------+------------------------------->
   '-DAYofweek--=--+-ANY--------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
                   +-Friday----+
                   '-SAturday--'

>--+--------------------------+-------------------------------><
   '-EXPiration--=--+-Never-+-'
                    '-Datum-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.

Syntax für einen erweiterten Clientzeitplan

```
                      (1)
>>-UPDate SCHedule--------Domänenname--Zeitplanname------------>

>--+-----------------+--+-----------------------------+-------->
   '-Type--=--Client-'  '-DESCription--=--Beschreibung-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.

Parameter

Domänenname (Erforderlich)
Gibt den Namen der Maßnahmendomäne an, zu der dieser Zeitplan gehört.
Zeitplanname (Erforderlich)
Gibt den Namen des Zeitplans an, der aktualisiert werden soll.
Type=Client
Gibt an, daß ein Client-Zeitplan aktualisiert wird. Dieser Parameter ist wahlfrei. Der Standardwert ist CLIENT.
DESCription
Gibt eine Beschreibung des Zeitplans an. Dieser Parameter ist wahlfrei. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine leere Zeichenfolge ("") anzugeben.
ACTion
Gibt die Aktion an, die bei der Verarbeitung dieses Zeitplans ausgeführt wird.Gültige Werte:

Incremental
Gibt an, daß der Zeitplan alle Dateien sichert, die neu sind oder sich seit der letzten Teilsicherung geändert haben. Mit "Incremental" werden auch alle Dateien gesichert, für die alle vorhandenen Sicherungen möglicherweise verfallen sind.
Selective
Gibt an, daß der Zeitplan nur Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.
Archive
Gibt an, daß der Zeitplan Dateien archiviert, die mit dem Parameter OBJECTS angegeben werden.
Backup
Gibt an, dass der Zeitplan Dateien sichert, die mit dem Parameter OBJECTS angegeben werden.
REStore
Gibt an, daß der Zeitplan Dateien zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.

Wenn Sie ACTION=RESTORE für eine geplante Operation angeben, und ist die Option REPLACE auf PROMPT gesetzt, erfolgt keine Aufforderung. Wird die Option auf PROMPT gesetzt, werden die Dateien übersprungen.

Wenn Sie eine zweite Dateispezifikation angeben, agiert diese zweite Dateispezifikation als Zielort für die Zurückschreibung. Müssen mehrere Gruppen von Dateien zurückgeschrieben werden, planen Sie eine für jede Dateispezifikation, die zurückgeschrieben werden muss.

RETrieve
Gibt an, dass der Zeitplan Dateien abruft, die mit dem Parameter OBJECTS angegeben werden.
Hinweis: Eine zweite Datei, die angegeben wird, dient als Abrufzielort. Müssen mehrere Gruppen von Dateien abgerufen werden, erstellen Sie einen separaten Zeitplan für jede Dateigruppe.
IMAGEBACkup
Gibt an, daß der Zeitplan logische Datenträger sichert, die mit dem Parameter OBJECTS angegeben werden.
IMAGEREStore
Gibt an, daß der Zeitplan logische Datenträger zurückschreibt, die mit dem Parameter OBJECTS angegeben werden.
Command
Gibt an, dass der Zeitplan einen Client-Betriebssystembefehl oder ein Script verarbeitet, der bzw. das mit dem Parameter OBJECTS angegeben wird.
Macro
Gibt an, daß ein Client ein Makro verarbeitet, dessen Dateiname im Parameter OBJECTS angegeben ist.
SUBACTion
Sie können einen der folgenden Werte angeben:

""
Wenn eine Nullzeichenfolge (zwei Anführungszeichen) mit ACTION=BACKUP angegeben wird, ist die Sicherung eine Teilsicherung.
FASTBAck
Gibt an, dass eine FastBack-Clientoperation, die durch den Parameter ACTION angegeben wird, für die Verarbeitung geplant werden soll. Der Wert des Parameters ACTION muss ARCHIVE oder BACKUP sein.
SYSTEMSTate
Gibt an, dass eine Clientsystemstatussicherung geplant ist.
VApp
Gibt an, dass eine vApp-Clientsicherung geplant ist. Eine vApp ist eine Sammlung von vorimplementierten virtuellen Maschinen.
VM
Gibt an, dass eine VMware-Clientsicherungsoperation geplant ist.

Deploy
Gibt an, ob Client-Workstations mit Implementierungspaketen aktualisiert werden sollen, die mit dem Parameter OBJECTS angegeben werden. Der Parameter OBJECTS muss zwei Spezifikationen enthalten: die Paketdateien, die abgerufen werden sollen, und die Position, an der sie abgerufen werden sollen. Stellen Sie sicher, dass die Objekte die Reihenfolge *`Dateien Position`* haben. Beispiel:

```
define schedule standard deploy_1 action=DEPLOY objects=
"\\IBM_ANR_WIN\c$\tsm\maintenance\client\v6r2\Windows\X32\v620\v6200\*
..\IBM_ANR_WIN\"
```

Die Werte für die folgenden Optionen sind eingeschränkt, wenn Sie ACTION=DEPLOY angeben:

PERUNITS
: Geben Sie `PERUNITS=ONETIME` an. Wenn Sie `PERUNITS=PERIOD` angeben, wird der Parameter ignoriert.

DURUNITS
: Geben Sie `MINUTES`, `HOURS` oder `DAYS` für den Parameter DURUNITS an. Geben Sie nicht INDEFINITE an.

SCHEDSTYLE
: Geben Sie die Standarddarstellung CLASSIC an.

Der Befehl SCHEDULE schlägt fehl, wenn die Parameter nicht den erforderlichen Parameterwerten wie V.R.M.F entsprechen.

OPTions
: Gibt die Clientoptionen an, die für den geplanten Befehl angegeben werden, wenn der Zeitplan verarbeitet wird. Dieser Parameter ist wahlfrei.
Für diesen Parameter können nur die Optionen angegeben werden, die für den geplanten Befehl gültig sind. Informationen zu den Optionen, die in der Befehlszeile gültig sind, befinden sich im entsprechenden Clienthandbuch. Alle Optionen, für die im Clienthandbuch angegeben ist, dass sie nur in der Anfangsbefehlszeile gültig sind, führen zu einem Fehler oder werden ignoriert, wenn der Zeitplan vom Server ausgeführt wird. Geben Sie beispielsweise die folgenden Optionen nicht an, da sie keinen Einfluss darauf haben, wann der Client den geplanten Befehl verarbeitet:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Windows-BetriebssystemeWenn Sie einen Scheduler-Service definieren, indem Sie den Befehl DSMCUTIL oder den Assistenten für die GUI des Clients für Sichern/Archivieren verwenden, geben Sie eine Optionsdatei an. Sie können die Optionen in dieser Optionsdatei nicht überschreiben, indem Sie den geplanten Befehl ausgeben. Sie müssen die Optionen in Ihrem Schedulerservice ändern.

Enthält die Optionszeichenfolge mehrere Optionen oder Optionen mit eingebetteten Leerzeichen, schließen Sie die gesamte Optionszeichenfolge in Hochkommas ein. Schließen Sie einzelne Optionen, die Leerzeichen enthalten, in Anführungszeichen ein. Vor der Option muss ein führendes Minuszeichen stehen. Fehler können auftreten, wenn die Optionszeichenfolge Leerzeichen enthält, die nicht korrekt in Anführungszeichen eingeschlossen sind.

Die folgenden Beispiele zeigen, wie einige Clientoptionen angegeben werden:

- Geben Sie Folgendes ein, um `subdir=yes` und `domain all-local -systemobject` anzugeben:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Geben Sie Folgendes ein, um `domain all-local -c: -d:` anzugeben:
  - `options='-domain="all-local -c: -d:"'`

 Windows-BetriebssystemeTipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

OBJects
: Gibt die Objekte an, für die die angegebene Aktion ausgeführt wird. Verwenden Sie ein einzelnes Leerzeichen zwischen jedem Objekt. Außer bei ACTION=INCREMENTAL ist dieser Parameter erforderlich. Ist die Aktion eine Sicherungs-, Archivierungs-, Abruf- oder Zurückschreibungsoperation, sind die Objekte Dateibereiche, Verzeichnisse oder logische Datenträger. Dient die Aktion zur Ausführung eines Befehls oder Makros, ist das Objekt der Name des auszuführenden Befehls oder Makros.

Wenn ACTION=INCREMENTAL ohne Angabe eines Werts für diesen Parameter angegeben wird, wird der geplante Befehl ohne angegebene Objekte aufgerufen, und der Befehl versucht, die Objekte wie in der Clientoptionsdatei definiert zu verarbeiten. Um alle Dateibereiche oder Verzeichnisse für eine Aktion auszuwählen, müssen sie explizit in der Objektzeichenfolge aufgeführt werden. Wird nur ein Stern in die Objektzeichenfolge eingegeben, erfolgt die Sicherung nur für das Verzeichnis, bei dem der Scheduler gestartet wurde.

Wichtig:

- Wenn Sie eine zweite Dateispezifikation angeben, und handelt es sich nicht um einen gültigen Zielort, empfangen Sie diesen Fehler:

  ```
  ANS1082E Ungültige
  Zieldateispezifikation <Dateispezifikation> eingegeben.
  ```

- Geben Sie mehr als zwei Dateispezifikationen an, empfangen Sie diesen Fehler:

```
ANS1102E Zu viele Befehlszeilenparameter an das Programm übergeben!
```

Wird für diesen Parameter ACTION=ARCHIVE, INCREMENTAL oder SELECTIVE angegeben, können Sie maximal 20 Dateispezifikationen auflisten.

Schließen Sie die Objektzeichenfolge in Anführungszeichen ein, wenn sie Leerzeichen enthält, und schließen Sie dann die Anführungszeichen in Hochkommas ein. Enthält die Objektzeichenfolge mehrere Dateinamen, schließen Sie jeden Dateinamen in Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Fehler können auftreten, wenn Dateinamen ein Leerzeichen enthalten, das nicht korrekt in Anführungszeichen eingeschlossen ist.

 Wenn Sie Zeichen verwenden, die für Windows-Benutzer eine besondere Bedeutung haben, wie z. B. Kommas, schließen Sie das gesamte Argument in doppelte Anführungszeichen ein und schließen Sie dann die gesamte Zeichenfolge in Hochkommas ein. Die folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

- Geben Sie Folgendes ein, um C:\FILE 2, D:\GIF FILES und E:\MY TEST FILE anzugeben:
  - `OBJECTS='"C:\FILE 2" "D:\GIF FILES" "E:\MY TEST FILE"'`
- Geben Sie Folgendes ein, um D:\TEST FILE anzugeben:
  - `OBJECTS='"D:\TEST FILE"'`
- Geben Sie Folgendes ein, um D:TEST,FILE anzugeben:
  - `OBJECTS='""D:\TEST,FILE""'`

 AIX-Betriebssysteme  Linux-BetriebssystemeDie folgenden Beispiele zeigen, wie einige Dateinamen angegeben werden:

- Geben Sie Folgendes ein, um /home/file 2, /home/gif files und /home/my test file anzugeben:
  - `OBJECTS='"/home/file 2" "/home/gif files" "/home/my test file"'`
- Geben Sie Folgendes ein, um /home/test file anzugeben:
  - `OBJECTS='"/home/test file"'`

 Tipp:

Für Windows-Clients, die im Stapelbetrieb ausgeführt werden: Ist die Verwendung von Anführungszeichen erforderlich, verwenden Sie den Dialogmodus oder Escapezeichen des Betriebssystems. Weitere Informationen liefern die folgenden Abschnitte:

- Eine Serie von Befehlen des Verwaltungsclients verarbeiten
- Einzelne Befehle mit dem Verwaltungsclient verarbeiten

PRIority

Gibt den Prioritätswert für einen Zeitplan an. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 10, wobei 1 die höchste Priorität und 10 die niedrigste Priorität angibt. Der Standardwert ist 5.

Wenn zwei oder mehr Zeitpläne dieselbe Fensterstartzeit haben, legt der angegebene Wert fest, wann IBM Spectrum Protect den Zeitplan verarbeitet. Der Zeitplan mit der höchsten Priorität startet zuerst. Ein Zeitplan mit PRIORITY=3 startet beispielsweise vor einem Zeitplan mit PRIORITY=5.

STARTDate

Gibt das Datum für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Diesen Parameter zusammen mit dem Parameter STARTTIME verwenden, um anzugeben, wann das Anfangsstartfenster des Zeitplans startet.
Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage **oder** +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY +3 **oder** +3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

STARTTime

Gibt die Uhrzeit für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter gibt in Verbindung mit dem Parameter STARTDATE den Beginn des Anfangsstartfensters an. Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW+02:00 oder STARTTIME=+02:00 ausgegeben, beginnt das Startfenster um 7:00 Uhr.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW-02:00 **oder** -02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW-02:00 oder STARTTIME=-02:00 ausgegeben, beginnt das Startfenster um 3:00 Uhr.

DURation
Gibt die Anzahl Einheiten an, die die Länge des Startfensters der geplanten Operation definiert. Dieser Parameter ist wahlfrei. Dieser Wert muß zwischen 1 und 999 liegen. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter DURUNITS verwenden, um die Länge des Startfensters anzugeben. Werden beispielsweise DURATION=20 und DURUNITS=MINUTES angegeben, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Standardlänge des Startfensters beträgt 1 Stunde. Die Länge des Fensters muß kürzer sein, als der Zeitraum zwischen Fenstern.

Dieser Wert wird ignoriert, wenn DURUNITS=INDEFINITE angegeben wird.

Tipp: Definieren Sie Zeitpläne mit einer Dauer von mehr als 10 Minuten. Damit erhält der IBM Spectrum Protect-Scheduler genügend Zeit, den Zeitplan zu verarbeiten und den Client abzufragen.

DURUnits
Gibt die Zeiteinheiten an, mit denen die Dauer des Fensters bestimmt wird, in dem der Zeitplan starten kann. Dieser Parameter ist wahlfrei. Der Standardwert ist HOURS.

Diesen Parameter zusammen mit dem Parameter DURATION verwenden, um anzugeben, wie lange das Startfenster geöffnet bleibt, um den Zeitplan zu verarbeiten. Gilt beispielsweise DURATION=20 und DURUNITS=MINUTES, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Verarbeitung des Zeitplans muß nicht unbedingt innerhalb dieses Fensters enden. Wenn der Zeitplan aus irgendeinem Grund wiederholt werden muß, müssen die Wiederholungsversuche vor Ablauf des Startfensters beginnen; andernfalls wird die Operation nicht erneut gestartet.

Der Standardwert für die Länge des Startfensters ist 1 Stunde. Sie können einen der folgenden Werte angeben:

Minutes
Gibt an, daß die Dauer des Fensters in Minuten definiert wird.

Hours
Gibt an, daß die Dauer des Fensters in Stunden definiert wird.

Days
Gibt an, daß die Dauer des Fensters in Tagen definiert wird.

INDefinite
Gibt an, daß die Dauer des Startfensters der geplanten Operation unbegrenzt ist. Der Zeitplan kann bis zu seinem Verfall zu einem beliebigen Zeitpunkt nach der geplanten Startzeit ausgeführt werden. Sie können DURUNITS=INDEFINITE nur angeben, wenn Sie PERUNITS=ONETIME angeben. Der Wert INDEFINITE ist für erweiterte Zeitpläne nicht zulässig.

MAXRUNtime
Gibt die maximale Ausführungszeit an. Hierbei handelt es sich um die Anzahl Minuten, in denen alle Clientsitzungen, die von der geplanten Operation gestartet werden, abgeschlossen werden sollten. Sind Sitzungen nach Ablauf der maximalen Ausführungszeit noch aktiv, gibt der Server eine Warnung aus, aber die Ausführung der Sitzungen wird fortgesetzt.
Tipp: Die maximale Ausführungszeit wird ab dem Beginn des Startfensters und nicht ab der Zeit berechnet, zu der Sitzungen innerhalb des Startfensters gestartet werden.
Einschränkungen:

- Der Wert des Parameters wird nicht an Server verteilt, die von einem Manager für unternehmensweite Konfiguration verwaltet werden.
- Der Wert des Parameters wird nicht mit dem Befehl EXPORT exportiert.

Der Parameter ist wahlfrei. Sie können eine Zahl im Bereich von 0 bis 1440 angeben. Der Wert 0 bedeutet, dass die maximale Ausführungszeit unendlich ist und keine Warnung ausgegeben wird. Die maximale Ausführungszeit muss größer als die Dauer des Startfensters sein, die mit den Parametern DURATION und DURUNITS definiert wird.

Ist beispielsweise die Startzeit einer geplanten Operation 21:00 Uhr und beträgt die Dauer des Startfensters 2 Stunden, erstreckt sich das Startfenster von 21:00 Uhr bis 23:00 Uhr. Beträgt die maximale Ausführungszeit 240 Minuten (4 Stunden), sollten alle Clientsitzungen für diese Operation um 1:00 Uhr abgeschlossen sein. Sind eine oder mehrere Sitzungen nach 1:00 Uhr noch aktiv, gibt der Server eine Warnung aus.
Tipp: Alternativ können Sie den Wert 1:00 Uhr für *Ausführungszeitsalert* im IBM Spectrum Protect Operations Center angeben.

SCHEDStyle

Dieser Parameter ist wahlfrei. SCHEDSTYLE definiert entweder das Intervall zwischen den Zeiten, zu denen ein Zeitplan ausgeführt werden kann, oder die Tage, an denen der Zeitplan ausgeführt werden kann. Die Darstellung kann entweder classic oder enhanced sein. Dieser Parameter muss angegeben werden, wenn Sie die Darstellung eines Zeitplans von klassisch in erweitert oder zurück in klassisch ändern. Andernfalls wird der Wert für den vorhandenen Zeitplan verwendet.

Für klassische Zeitpläne sind diese Parameter zulässig: PERIOD, PERUNITS und DAYOFWEEK. Diese Parameter sind nicht zulässig: MONTH, DAYOFMONTH und WEEKOFMONTH. War die vorherige Zeitplandarstellung erweitert, werden die Parameter MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK zurückgesetzt. DAYOFWEEK, PERIOD und PERUNITS werden auf die Standardwerte gesetzt, es sei denn, sie werden mit dem Aktualisierungsbefehl angegeben.

Für erweiterte Zeitpläne sind diese Parameter zulässig: MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK. Diese Parameter sind nicht zulässig: PERIOD und PERUNITS. War die vorherige Zeitplandarstellung klassisch, werden die Parameter DAYOFWEEK, PERIOD und PERUNITS zurückgesetzt. MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK werden auf die Standardwerte gesetzt, es sei denn, sie werden mit dem Aktualisierungsbefehl angegeben.

PERiod

Gibt den Zeitraum zwischen Startfenstern für diesen Zeitplan an. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Zulässige Werte sind ganze Zahlen von 1 bis 999. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter PERUNITS verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle fünf Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Zeitraum zwischen den Startfenstern muß länger sein als die Dauer jedes Fensters. Der Standardwert ist 1 Tag.

Dieser Wert wird ignoriert, wenn PERUNITS=ONETIME angegeben wird.

PERUnits

Gibt die Zeiteinheiten an, mit denen der Zeitraum zwischen Startfenstern für diesen Zeitplan bestimmt wird. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Der Standardwert ist DAYS.
Diesen Parameter zusammen mit dem Parameter PERIOD verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle 5 Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Standardwert ist 1 Tag. Sie können einen der folgenden Werte angeben:

Hours
: Gibt an, daß der Zeitraum zwischen Startfenstern in Stunden angegeben wird.

Days
: Gibt an, daß der Zeitraum zwischen Startfenstern in Tagen angegeben wird.

Weeks
: Gibt an, daß der Zeitraum zwischen Startfenstern in Wochen angegeben wird.

Months
: Gibt an, daß der Zeitraum zwischen Startfenstern in Monaten angegeben wird.

  Wird PERUNITS=MONTHS angegeben, wird die geplante Operation jeden Monat an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/04/1998 lautet, wird der Zeitplan danach am 4. jedes Monats verarbeitet. Wenn das Datum jedoch für den nächsten Monat nicht gültig ist, wird die geplante Operation am letzten gültigen Datum in dem Monat verarbeitet. Danach basieren nachfolgende Operationen auf diesem neuen Datum. Wenn das Startdatum beispielsweise 03/31/1998 lautet, wird die Operation des nächsten Monats für den 04/30/1998 geplant. Danach werden alle folgenden Operationen bis Februar am 30. des Monats ausgeführt. Da Februar nur 28 Tage hat, wird die Operation für das Datum 02/28/1999 geplant. Nachfolgende Operationen werden am 28. des Monats verarbeitet.

Years
: Gibt an, daß der Zeitraum zwischen Startfenstern für den Zeitplan in Jahren angegeben wird.

  Wird PERUNITS=YEARS angegeben, wird die geplante Operation jährlich in demselben Monat und an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/29/2004 lautet, wird die geplante Operation des nächsten Jahres am 02/28/2005 ausgeführt, da Februar nur 28 Tage hat. Danach werden folgende Operationen für den 28. Februar geplant.

Onetime
: Gibt an, daß der Zeitplan einmal verarbeitet wird. Dieser Wert überschreibt den für den Parameter PERIOD angegebenen Wert.

DAYofweek

Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können verschiedene Optionen für den Parameter DAYofweek angeben, abhängig davon, ob die Zeitplandarstellung als 'Klassisch' oder 'Erweitert' definiert wurde:

Klassischer Zeitplan
: Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können entweder einen Tag der Woche oder WEEKDAY, WEEKEND oder ANY angeben. Fallen Startdatum und Startzeit auf einen Tag, der nicht einem angegebenen Tag entspricht, werden das Startdatum und die Startzeit in 24-Stunden-Schritten vorverlegt, bis die Angabe im Parameter DAYOFWEEK erfüllt ist.

  Wird für DAYOFWEEK nicht ANY angegeben, werden die Zeitpläne, je nach Angabe für PERIOD und PERUNITS, möglicherweise nicht zum erwarteten Zeitpunkt verarbeitet. Der Standardwert ist ANY.

Erweiterter Zeitplan
: Gibt die Tage der Woche an, an denen der Zeitplan ausgeführt werden soll. Sie können entweder mehrere Tage, die durch Kommas und ohne Leerzeichen voneinander getrennt werden, oder WEEKDAY, WEEKEND oder ANY angeben. Werden mehrere Tage angegeben, wird der Zeitplan an jedem angegebenen Tag ausgeführt. Wird WEEKDAY oder WEEKEND angegeben, müssen Sie auch entweder WEEKOFMONTH=FIRST oder WEEKOFMONTH=LAST angeben, und der Zeitplan wird nur einmal pro Monat ausgeführt.

  Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag der Woche oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter DAYOFWEEK muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

Gültige Werte für den Parameter DAYofweek sind:

ANY
: Das Startfenster kann an einem beliebigen Wochentag beginnen.

WEEKDay
: Das Startfenster kann am Montag, Dienstag, Mittwoch, Donnerstag oder Freitag beginnen.

WEEKEnd
: Das Startfenster kann am Samstag oder Sonntag beginnen.

SUnday
: Das Startfenster beginnt am Sonntag.

Monday
: Das Startfenster beginnt am Montag.

TUesday
: Das Startfenster beginnt am Dienstag.

Wednesday
: Das Startfenster beginnt am Mittwoch.

THursday
: Das Startfenster beginnt am Donnerstag.

Friday
: Das Startfenster beginnt am Freitag.

SAturday
: Das Startfenster beginnt am Samstag.

MONth

Gibt die Monate des Jahres an, in denen der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Geben Sie mehrere Werte an, indem Sie Kommas und keine Leerzeichen verwenden. Der Standardwert lautet ANY. Er bedeutet, dass der Zeitplan während aller Monate des Jahres ausgeführt wird.

DAYOFMonth

Gibt den Tag des Monats an, an dem der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Sie können entweder ANY oder eine Zahl von -31 bis 31, ausschließlich Null, angeben. Ein negativer Wert gibt einen Tag an, bei dem vom Ende des Monats zurückgezählt wird. Beispiel: Der letzte Tag des Monats ist -1, der vorletzte Tag des Monats ist -2. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan an jedem angegebenen Tag des Monats ausgeführt. Geben mehrere Werte denselben Tag an, wird der Zeitplan nur einmal an diesem Tag ausgeführt.

Der Standardwert ist ANY. Dies bedeutet, dass der Zeitplan an jedem Tag des Monats oder an den Tagen ausgeführt wird, die durch andere Parameter des erweiterten Zeitplans bestimmt werden. Der Parameter DAYOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFWEEK oder WEEKOFMONTH verwendet wird.

Gibt ein vorhandener Zeitplan einen anderen Wert als ANY für DAYOFWEEK und WEEKOFMONTH an, und wird DAYOFMONTH aktualisiert, werden DAYOFWEEK und WEEKOFMONTH auf ANY zurückgesetzt.

WEEKofmonth
: Gibt die Woche des Monats an, in der der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Eine Woche wird als beliebige 7-Tage-Periode betrachtet, die nicht an einem bestimmten Tag der Woche beginnt. Sie können FIRST, SECOND, THIRD, FOURTH, LAST oder ANY angeben. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan während jeder angegebenen Woche des Monats ausgeführt. Geben mehrere Werte dieselbe Woche an, wird der Zeitplan nur einmal während dieser Woche ausgeführt.

Der Standardwert ist ANY. ANY bedeutet, dass der Zeitplan während jeder Woche des Monats oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter WEEKOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

EXPiration
Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NEVER. Sie können einen der folgenden Werte angeben:

Never
Gibt an, dass der Zeitplan nie abläuft.

Ablaufdatum
Gibt das Datum im Format MM/DD/YYYY an, an dem dieser Zeitplan abläuft. Wenn ein Ablaufdatum angegeben wird, läuft der Zeitplan um 23:59:59 Uhr am angegebenen Datum ab.

Beispiel: Die Priorität eines Zeitplans aktualisieren

Für den Zeitplan MONTHLY_BACKUP, der zur Maßnahmendomäne STANDARD gehört, soll der Wert für die Priorität auf 1 gesetzt werden.

```
update schedule standard monthly_backup priority=1
```

Beispiel: Das Ablaufdatum eines Zeitplans aktualisieren

Der Zeitplan WEEKLY_BACKUP, der zur Maßnahmendomäne EMPLOYEE_RECORDS gehört, soll am 29. März 1999 (03/29/1999) ablaufen.

```
update schedule employee_records weekly_backup expiration=03/29/1999
```

Beispiel: Einen Zeitplan aktualisieren, so dass die Archivierung am letzten Freitag eines Monats erfolgt

Einen Zeitplan, bei dem Dateien vierteljährlich am letzten Freitag des Monats archiviert werden, in einen Zeitplan aktualisieren, bei dem die Dateien am letzten Tag der angegebenen Monate archiviert werden.

```
update schedule employee_records quarterly_archive dayofmonth=-1
```

WEEKOFMONTH und DAYOFWEEK werden auf ANY zurückgesetzt.

UPDATE SCHEDULE (Verwaltungszeitplan aktualisieren)

Mit diesem Befehl können ausgewählte Parameter für einen Verwaltungszeitplan aktualisiert werden.

Die Befehle MACRO und QUERY ACTLOG können nicht geplant werden.

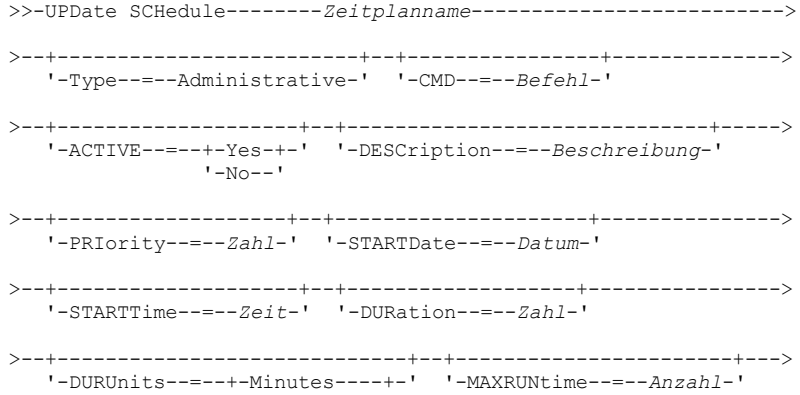
Ein verwalteter Verwaltungszeitplan, der von einem Konfigurationsmanager aktualisiert wird, wird während der Konfigurationsaktualisierungsverarbeitung auf den verwalteten Servern in einen inaktiven Status versetzt. Er behält einen inaktiven Status, bis er auf diesen Servern in einen aktiven Status aktualisiert wird.

Berechtigungsklasse

Zum Aktualisieren eines Verwaltungszeitplans ist Systemberechtigung erforderlich.

Syntax

Klassischer Verwaltungszeitplan



```
                  +-Hours------+
                  +-Days-------+
                  '-INDefinite-'

>--+-------------------------+--+-----------------+-------------->
   '-SCHEDStyle--=--Classic-'  '-PERiod--=--Zahl-'

>--+-------------------------+-------------------------------->
   '-PERUnits--=--+-Hours---+-'
                  +-Days----+
                  +-Weeks---+
                  +-Months--+
                  +-Years---+
                  '-Onetime-'

>--+-----------------------------+----------------------------->
   '-DAYofweek--=--+-ANY--------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
                   +-Friday----+
                   '-SAturday--'

>--+-------------------------+---------------------------------><
   '-EXPiration=--+-Never-+-'
                  '-Datum-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.

Syntax

```
Erweiterter Verwaltungszeitplan

                     (1)
>>-UPDate SCHedule--------Zeitplanname--------------------------->

>--+-------------------------+--+----------------+-------------->
   '-Type--=--Administrative-'  '-CMD--=--Befehl-'

>--+--------------------+--+------------------------------+----->
   '-ACTIVE--=--+-Yes-+-'  '-DESCription--=--Beschreibung-'
                '-No--'

>--+--------------------+--+---------------------+--------------->
   '-PRIority--=--Zahl-'  '-STARTDate--=--Datum-'

>--+---------------------+--+--------------------+---------------->
   '-STARTTime--=--Zeit-'  '-DURation--=--Zahl-'

>--+-------------------------+--+----------------------+------>
   '-DURUnits--=--+-Minutes-+-'  '-MAXRUNtime--=--Anzahl-'
                  +-Hours---+
                  '-Days----'

>--+-------------------------+--+--------------------------+----->
   '-SCHEDStyle--=--Enhanced-'  '-MONth--=--+-ANY-------+-'
                                            +-JAnuary---+
                                            +-February--+
                                            +-MARch-----+
                                            +-APril-----+
                                            +-May-------+
                                            +-JUNe------+
                                            +-JULy------+
                                            +-AUgust----+
                                            +-September-+
                                            +-October---+
                                            +-November--+
                                            '-December--'

>--+-------------------------+--+-----------------------------+--->
   '-DAYOFMonth--=--+-ANY-+-'  '-WEEKofmonth--=--+-ANY----+-'
                    '-Day-'                      +-FIrst--+
                                                 +-Second-+
```

```
                                                +-Third--+
                                                +-FOurth-+
                                                '-Last---'

>--+-----------------------------+------------------------------>
   '-DAYofweek--=--+-ANY-------+-'
                   +-WEEKDay---+
                   +-WEEKEnd---+
                   +-SUnday----+
                   +-Monday----+
                   +-TUesday---+
                   +-Wednesday-+
                   +-THursday--+
                   +-Friday----+
                   '-SAturday--'

>--+------------------------+---------------------------------><
   '-EXPiration=--+-Never-+-'
                  '-Datum-'
```

Anmerkungen:

1. Bei diesem Befehl muss mindestens ein wahlfreier Parameter angegeben werden.

Parameter

Zeitplanname (Erforderlich)
: Gibt den Namen des Zeitplans an, der aktualisiert werden soll.

Type=Administrative (Erforderlich)
: Gibt an, daß ein Zeitplan für Verwaltungsbefehle aktualisiert wird.

CMD
: Gibt den Verwaltungsbefehl an, der für die Verarbeitung geplant werden soll. Dieser Parameter ist wahlfrei. Der angegebene Befehl kann bis zu 512 Zeichen enthalten. Den Befehl in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

  Es können keine Umleitungszeichen mit diesem Parameter angegeben werden.

ACTIVE
: Gibt an, ob der Verwaltungsbefehl für die Verarbeitung auswählbar ist. Dieser Parameter ist wahlfrei. Ein Zeitplan für Verwaltungsbefehle wird erst verarbeitet, wenn er sich im aktiven Status befindet. Gültige Werte:

  YES
  : Gibt an, daß der Verwaltungsbefehl für die Verarbeitung auswählbar ist.

  NO
  : Gibt an, daß der Verwaltungsbefehl nicht für die Verarbeitung auswählbar ist.

DESCription
: Gibt eine Beschreibung des Zeitplans an. Dieser Parameter ist wahlfrei. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Soll eine zuvor definierte Beschreibung gelöscht werden, ist eine leere Zeichenfolge ("") anzugeben.

PRIority
: Gibt den Prioritätswert für einen Zeitplan an. Dieser Parameter ist wahlfrei. Zulässige Werte sind ganze Zahlen von 1 bis 10, wobei 1 die höchste Priorität und 10 die niedrigste Priorität angibt. Der Standardwert ist 5.

  Wenn zwei oder mehr Zeitpläne dieselbe Fensterstartzeit haben, legt der angegebene Wert fest, wann IBM Spectrum Protect den Zeitplan verarbeitet. Der Zeitplan mit der höchsten Priorität startet zuerst. Ein Zeitplan mit PRIORITY=3 startet beispielsweise vor einem Zeitplan mit PRIORITY=5.

STARTDate
: Gibt das Datum für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist das aktuelle Datum. Diesen Parameter zusammen mit dem Parameter STARTTIME verwenden, um anzugeben, wann das Anfangsstartfenster des Zeitplans startet.
  Sie können das Datum unter Verwendung der folgenden Werte angeben:

Wert	**Beschreibung**	**Beispiel**
MM/TT/JJJJ	Ein bestimmtes Datum	09/15/1998
TODAY	Das aktuelle Datum	TODAY
TODAY+Tage **oder** +Tage	Das aktuelle Datum plus der Anzahl der angegebenen Tage. Die maximale Anzahl Tage, die angegeben werden können, beträgt 9999.	TODAY +3 **oder** +3.
EOLM (Ende des letzten Monats)	Der letzte Tag des Vormonats.	EOLM

Wert	Beschreibung	Beispiel
EOLM-Tage	Der letzte Tag des Vormonats minus angegebene Tage.	EOLM-1 Um Dateien einzuschließen, die am Tag vor dem letzten Tag des Vormonats aktiv waren.
BOTM (Anfang dieses Monats)	Der erste Tag des aktuellen Monats.	BOTM
BOTM+Tage	Der erste Tag des aktuellen Monats plus angegebene Tage.	BOTM+9 Um Dateien einzuschließen, die am zehnten Tag des aktuellen Monats aktiv waren.

STARTTime

Gibt die Uhrzeit für den Anfang des Fensters an, in dem der Zeitplan zuerst verarbeitet wird. Dieser Parameter ist wahlfrei. Standardwert ist die aktuelle Uhrzeit. Dieser Parameter gibt in Verbindung mit dem Parameter STARTDATE den Beginn des Anfangsstartfensters an. Sie können die Uhrzeit unter Verwendung der folgenden Werte angeben:

Wert	Beschreibung	Beispiel
HH:MM:SS	Eine bestimmte Uhrzeit	10:30:08
NOW	Die aktuelle Uhrzeit	NOW
NOW+HH:MM **oder** +HH:MM	Die aktuelle Uhrzeit plus den angegebenen Stunden und Minuten	NOW+02:00 **oder** +02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW+02:00 oder STARTTIME=+02:00 ausgegeben, beginnt das Startfenster um 7:00 Uhr.
NOW-HH:MM **oder** -HH:MM	Die aktuelle Uhrzeit minus den angegebenen Stunden und Minuten	NOW-02:00 **oder** -02:00. Wird dieser Befehl um 5:00 Uhr mit der Angabe STARTTIME=NOW-02:00 oder STARTTIME=-02:00 ausgegeben, beginnt das Startfenster um 3:00 Uhr.

DURation

Gibt die Anzahl Einheiten an, die die Länge des Startfensters der geplanten Operation definiert. Dieser Parameter ist wahlfrei. Dieser Wert muß zwischen 1 und 999 liegen. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter DURUNITS verwenden, um die Länge des Startfensters anzugeben. Werden beispielsweise DURATION=20 und DURUNITS=MINUTES angegeben, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Standardlänge des Startfensters beträgt 1 Stunde. Die Länge des Fensters muß kürzer sein, als der Zeitraum zwischen Fenstern.

Dieser Wert wird ignoriert, wenn DURUNITS=INDEFINITE angegeben wird.

DURUnits

Gibt die Zeiteinheiten an, mit denen die Dauer des Fensters bestimmt wird, in dem der Zeitplan starten kann. Dieser Parameter ist wahlfrei. Der Standardwert ist HOURS.

Diesen Parameter zusammen mit dem Parameter DURATION verwenden, um anzugeben, wie lange das Startfenster geöffnet bleibt, um den Zeitplan zu verarbeiten. Gilt beispielsweise DURATION=20 und DURUNITS=MINUTES, muß der Zeitplan innerhalb von 20 Minuten nach dem Startdatum und der Startzeit beginnen. Die Verarbeitung des Zeitplans muß nicht unbedingt innerhalb dieses Fensters enden. Wenn der Zeitplan aus irgendeinem Grund wiederholt werden muß, müssen die Wiederholungsversuche vor Ablauf des Startfensters beginnen; andernfalls wird die Operation nicht erneut gestartet.

Der Standardwert für die Länge des Startfensters ist 1 Stunde. Sie können einen der folgenden Werte angeben:

Minutes
: Gibt an, daß die Dauer des Fensters in Minuten definiert wird.

Hours
: Gibt an, daß die Dauer des Fensters in Stunden definiert wird.

Days
: Gibt an, daß die Dauer des Fensters in Tagen definiert wird.

INDefinite
: Gibt an, daß die Dauer des Startfensters der geplanten Operation unbegrenzt ist. Der Zeitplan kann bis zu seinem Verfall zu einem beliebigen Zeitpunkt nach der geplanten Startzeit ausgeführt werden. Sie können DURUNITS=INDEFINITE nur angeben, wenn Sie PERUNITS=ONETIME angeben. Der Wert INDEFINITE ist für erweiterte Zeitpläne nicht zulässig.

MAXRUNtime

Gibt die maximale Ausführungszeit an. Hierbei handelt es sich um die Anzahl Minuten, in denen Serverprozesse, die von geplanten Befehlen gestartet werden, abgeschlossen werden müssen. Sind Prozesse nach Ablauf der maximalen Ausführungszeit noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.
Tipps:

- Möglicherweise werden die Prozesse nicht sofort beendet, wenn sie von der zentralen Zeitplanung abgebrochen werden. Sie werden beendet, wenn sie die Benachrichtigung über den Abbruch von der zentralen Zeitplanung registrieren.
- Die maximale Ausführungszeit wird ab dem Zeitpunkt berechnet, an dem der Serverprozess startet. Wenn mit dem Befehl für den Zeitplan mehr als ein Prozess gestartet wird, wird die maximale Ausführungszeit für jeden Prozess ab dem Zeitpunkt berechnet, an dem der jeweilige Prozess startet.
- Dieser Parameter gilt nicht für einige Prozesse, wie z. B. Prozesse zum Identifizieren doppelter Daten, deren Ausführung nach Ablauf der maximalen Ausführungszeit fortgesetzt werden kann.
- Dieser Parameter gilt nicht, wenn der geplante Befehl keinen Serverprozess startet.
- Einigen Befehlen kann eine andere Abbruchzeit zugeordnet werden. Beispielsweise kann der Befehl MIGRATE STGPOOL einen Parameter einschließen, der die Länge der Zeit angibt, die die Speicherpoolumlagerung ausgeführt wird, bevor die Umlagerung automatisch abgebrochen wird. Wenn Sie einen Befehl planen, für den eine Abbruchzeit definiert ist, und Sie außerdem eine maximale Ausführungszeit für den Zeitplan definieren, werden die Prozesse zu der Abbruchzeit abgebrochen, die zuerst erreicht wird.

Einschränkungen:

- Der Wert des Parameters wird nicht an Server verteilt, die von einem Manager für unternehmensweite Konfiguration verwaltet werden.
- Der Wert des Parameters wird nicht mit dem Befehl EXPORT exportiert.

Dieser Parameter ist wahlfrei. Sie können eine Zahl im Bereich von 0 bis 1440 angeben. Der Wert 0 bedeutet, dass die maximale Ausführungszeit unendlich ist und die zentrale Zeitplanung keine Prozesse abbricht. Die maximale Ausführungszeit muss größer als die Dauer des Startfensters sein, die mit den Parametern DURATION und DURUNITS definiert wird.

Ist beispielsweise die Startzeit eines geplanten Befehls 21:00 Uhr und beträgt die Dauer des Startfensters 2 Stunden, erstreckt sich das Startfenster von 21:00 Uhr bis 23:00 Uhr. Beträgt die maximale Ausführungszeit 240 Minuten (4 Stunden), müssen alle zutreffenden Serverprozesse, die von dem Befehl gestartet werden, um 1:00 Uhr abgeschlossen sein. Sind ein oder mehrere zutreffende Prozesse nach 1:00 Uhr noch aktiv, werden die Prozesse von der zentralen Zeitplanung abgebrochen.
Tipp: Alternativ können Sie eine *Endzeit* von 1:00 Uhr im IBM Spectrum Protect Operations Center angeben.

SCHEDStyle
Dieser Parameter ist wahlfrei. SCHEDSTYLE definiert entweder das Intervall zwischen den Zeiten, zu denen ein Zeitplan ausgeführt werden soll, oder die Tage, an denen der Zeitplan ausgeführt werden soll. Die Darstellung kann entweder classic oder enhanced sein. Dieser Parameter muss angegeben werden, wenn Sie die Darstellung eines Zeitplans von klassisch in erweitert oder zurück in klassisch ändern. Andernfalls wird der Wert für den vorhandenen Zeitplan verwendet.

Für klassische Zeitpläne sind diese Parameter zulässig: PERIOD, PERUNITS und DAYOFWEEK. Diese Parameter sind nicht zulässig: MONTH, DAYOFMONTH und WEEKOFMONTH. War die vorherige Zeitplandarstellung erweitert, werden die Parameter MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK zurückgesetzt. DAYOFWEEK, PERIOD und PERUNITS werden auf die Standardwerte gesetzt, es sei denn, sie werden mit dem Aktualisierungsbefehl angegeben.

Für erweiterte Zeitpläne sind diese Parameter zulässig: MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK. Diese Parameter sind nicht zulässig: PERIOD und PERUNITS. War die vorherige Zeitplandarstellung klassisch, werden die Parameter DAYOFWEEK, PERIOD und PERUNITS zurückgesetzt. MONTH, DAYOFMONTH, WEEKOFMONTH und DAYOFWEEK werden auf die Standardwerte gesetzt, es sei denn, sie werden mit dem Aktualisierungsbefehl angegeben.

PERiod
Gibt den Zeitraum zwischen Startfenstern für diesen Zeitplan an. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Zulässige Werte sind ganze Zahlen von 1 bis 999. Der Standardwert ist 1.

Diesen Parameter zusammen mit dem Parameter PERUNITS verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle fünf Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Zeitraum zwischen den Startfenstern muß länger sein als die Dauer jedes Fensters. Der Standardwert ist 1 Tag.

Dieser Wert wird ignoriert, wenn PERUNITS=ONETIME angegeben wird.

PERUnits
Gibt die Zeiteinheiten an, mit denen der Zeitraum zwischen Startfenstern für diesen Zeitplan bestimmt wird. Dieser Parameter ist wahlfrei. Dieser Parameter wird nur für klassische Zeitpläne verwendet. Der Standardwert ist DAYS.
Diesen Parameter zusammen mit dem Parameter PERIOD verwenden, um den Zeitraum zwischen Startfenstern anzugeben. Werden beispielsweise PERIOD=5 und PERUNITS=DAYS angegeben (mit der Annahme DAYOFWEEK=ANY), wird die Operation alle 5 Tage nach dem Anfangsstartdatum und der Anfangsstartzeit geplant. Der Standardwert ist 1 Tag. Sie können einen der folgenden Werte angeben:

Hours
Gibt an, daß der Zeitraum zwischen Startfenstern in Stunden angegeben wird.
Days
Gibt an, daß der Zeitraum zwischen Startfenstern in Tagen angegeben wird.
Weeks
Gibt an, daß der Zeitraum zwischen Startfenstern in Wochen angegeben wird.
Months
Gibt an, daß der Zeitraum zwischen Startfenstern in Monaten angegeben wird.

Wird PERUNITS=MONTHS angegeben, wird die geplante Operation jeden Monat an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/04/1998 lautet, wird der Zeitplan danach am 4. jedes Monats verarbeitet. Wenn das Datum jedoch für den nächsten Monat nicht gültig ist, wird die geplante Operation am letzten gültigen Datum in dem Monat verarbeitet. Danach basieren nachfolgende Operationen auf diesem neuen Datum. Wenn das Startdatum beispielsweise 03/31/1998 lautet, wird die Operation des nächsten Monats für den 04/30/1998 geplant. Danach werden alle folgenden Operationen bis Februar am 30. des Monats ausgeführt. Da Februar nur 28 Tage hat, wird die Operation für das Datum 02/28/1999 geplant. Nachfolgende Operationen werden am 28. des Monats verarbeitet.

Years
: Gibt an, daß der Zeitraum zwischen Startfenstern für den Zeitplan in Jahren angegeben wird.

  Wird PERUNITS=YEARS angegeben, wird die geplante Operation jährlich in demselben Monat und an demselben Datum verarbeitet. Wenn das Startdatum der geplanten Operation beispielsweise 02/29/2004 lautet, wird die geplante Operation des nächsten Jahres am 02/28/2005 ausgeführt, da Februar nur 28 Tage hat. Danach werden folgende Operationen für den 28. Februar geplant.

Onetime
: Gibt an, daß der Zeitplan einmal verarbeitet wird. Dieser Wert überschreibt den für den Parameter PERIOD angegebenen Wert.

DAYofweek
: Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können verschiedene Optionen für den Parameter DAYofweek angeben, abhängig davon, ob die Zeitplandarstellung als 'Klassisch' oder 'Erweitert' definiert wurde:

  Klassischer Zeitplan
  : Gibt den Wochentag an, an dem das Startfenster für den Zeitplan beginnt. Dieser Parameter ist wahlfrei. Sie können entweder einen Tag der Woche oder WEEKDAY, WEEKEND oder ANY angeben. Fallen Startdatum und Startzeit auf einen Tag, der nicht einem angegebenen Tag entspricht, werden das Startdatum und die Startzeit in 24-Stunden-Schritten vorverlegt, bis die Angabe im Parameter DAYOFWEEK erfüllt ist.

    Wird für DAYOFWEEK nicht ANY angegeben, werden die Zeitpläne, je nach Angabe für PERIOD und PERUNITS, möglicherweise nicht zum erwarteten Zeitpunkt verarbeitet. Der Standardwert ist ANY.

  Erweiterter Zeitplan
  : Gibt die Tage der Woche an, an denen der Zeitplan ausgeführt werden soll. Sie können entweder mehrere Tage, die durch Kommas und ohne Leerzeichen voneinander getrennt werden, oder WEEKDAY, WEEKEND oder ANY angeben. Werden mehrere Tage angegeben, wird der Zeitplan an jedem angegebenen Tag ausgeführt. Wird WEEKDAY oder WEEKEND angegeben, müssen Sie auch entweder WEEKOFMONTH=FIRST oder WEEKOFMONTH=LAST angeben, und der Zeitplan wird nur einmal pro Monat ausgeführt.

    Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag der Woche oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter DAYOFWEEK muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

  Gültige Werte für den Parameter DAYofweek sind:

  ANY
  : Das Startfenster kann an einem beliebigen Wochentag beginnen.

  WEEKDay
  : Das Startfenster kann am Montag, Dienstag, Mittwoch, Donnerstag oder Freitag beginnen.

  WEEKEnd
  : Das Startfenster kann am Samstag oder Sonntag beginnen.

  SUnday
  : Das Startfenster beginnt am Sonntag.

  Monday
  : Das Startfenster beginnt am Montag.

  TUesday
  : Das Startfenster beginnt am Dienstag.

  Wednesday
  : Das Startfenster beginnt am Mittwoch.

  THursday
  : Das Startfenster beginnt am Donnerstag.

  Friday
  : Das Startfenster beginnt am Freitag.

  SAturday
  : Das Startfenster beginnt am Samstag.

MONth
: Gibt die Monate des Jahres an, in denen der Zeitplan ausgeführt werden soll. Dieser Parameter wird nur für erweiterte Zeitpläne verwendet. Geben Sie mehrere Werte an, indem Sie Kommas und keine Leerzeichen verwenden. Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan in jedem Monat des Jahres ausgeführt wird.

DAYOFMonth

Gibt den Tag des Monats an, an dem der Zeitplan ausgeführt werden soll. Dieser Parameter kann nur für erweiterte Zeitpläne angegeben werden. Sie können entweder ANY oder eine Zahl von -31 bis 31, ausschließlich Null, angeben. Ein negativer Wert gibt einen Tag an, bei dem vom Ende des Monats zurückgezählt wird. Beispiel: Der letzte Tag des Monats ist -1, der vorletzte Tag des Monats ist -2 usw. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan an jedem angegebenen Tag des Monats ausgeführt. Geben mehrere Werte denselben Tag an, wird der Zeitplan nur einmal an diesem Tag ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan an jedem Tag des Monats oder an den Tagen ausgeführt wird, die durch andere Parameter des erweiterten Zeitplans bestimmt werden. Der Parameter DAYOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFWEEK oder WEEKOFMONTH verwendet wird.

WEEKofmonth
Gibt die Woche des Monats an, in der der Zeitplan ausgeführt werden soll. Dieser Parameter kann nur für erweiterte Zeitpläne angegeben werden. Eine Woche wird als beliebige 7-Tage-Periode betrachtet, die nicht an einem bestimmten Tag der Woche beginnt. Sie können FIRST, SECOND, THIRD, FOURTH, LAST oder ANY angeben. Sie können mehrere Werte angeben, die durch Kommas und ohne Leerzeichen voneinander getrennt werden müssen. Werden mehrere Werte angegeben, wird der Zeitplan während jeder angegebenen Woche des Monats ausgeführt. Geben mehrere Werte dieselbe Woche an, wird der Zeitplan nur einmal während dieser Woche ausgeführt.

Der Standardwert ist ANY. Dieser Wert bedeutet, dass der Zeitplan während jeder Woche des Monats oder an dem Tag bzw. an den Tagen ausgeführt wird, der bzw. die durch andere Parameter des erweiterten Zeitplans bestimmt wird bzw. werden. Der Parameter WEEKOFMONTH muss den Wert ANY haben (entweder standardmäßig oder mit dem Befehl angegeben), wenn er mit dem Parameter DAYOFMONTH verwendet wird.

EXPiration
Gibt das Datum an, nach dem dieser Zeitplan nicht mehr verwendet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NEVER. Sie können einen der folgenden Werte angeben:

Never
Gibt an, dass der Zeitplan nie abläuft.
Ablaufdatum
Gibt das Datum im Format MM/DD/YYYY an, an dem dieser Zeitplan abläuft. Wenn ein Ablaufdatum angegeben wird, läuft der Zeitplan um 23:59:59 Uhr am angegebenen Datum ab.

Beispiel: Einen Sicherungszeitplan aktualisieren, so dass die Sicherung alle drei Tage erfolgt

Der bestehende Verwaltungszeitplan BACKUP_BACKUPPOOL soll dahingehend aktualisiert werden, daß (ab heute) der primäre Speicherpool BACKUPPOOL alle drei Tage um 22 Uhr abends in den Kopienspeicherpool COPYSTG gesichert werden soll.

```
update schedule backup_backuppool type=administrative cmd="backup stgpool
    backuppool copystg" active=yes starttime=22:00 period=3
```

Beispiel: Einen Sicherungszeitplan aktualisieren, so dass die Sicherung an jedem ersten und dritten Freitag erfolgt

Den Zeitplan BACKUP_ARCHIVEPOOL aktualisieren, der den primären Speicherpool ARCHIVEPOOL im Kopienspeicherpool RECOVERYPOOL sichert. Der vorhandene Zeitplan wird am ersten und zehnten Tag in jedem Monat ausgeführt. Den Zeitplan so aktualisieren, dass er am ersten und dritten Freitag in jedem Monat ausgeführt wird.

```
update schedule backup_archivepool
dayofweek=friday weekofmonth=first,third
```

DAYOFMONTH wird auf ANY zurückgesetzt.

UPDATE SCRATCHPADENTRY (Scratchpadeintrag aktualisieren)

Mit diesem Befehl können Sie Daten in einer Zeile im Scratchpad aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-UPDate SCRATCHPadentry--übergeordnete_Kategorie-------------->

>--untergeordnete_Kategorie--Betreff--Line -=--Nummer----------->

>--Data--=--Daten-----------------------------------------------><
```

Parameter

übergeordnete_Kategorie (Erforderlich)
: Gibt die übergeordnete Kategorie an, in der Daten aktualisiert werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

untergeordnete_Kategorie (Erforderlich)
: Gibt die untergeordnete Kategorie an, in der Daten aktualisiert werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Betreff (Erforderlich)
: Gibt den Betreff an, unter dem Daten aktualisiert werden sollen. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden.

Line (Erforderlich)
: Gibt die Nummer der Zeile an, in der Daten aktualisiert werden sollen.

Data (Erforderlich)
: Gibt die neuen Daten an, die in der Zeile gespeichert werden sollen. Vorherige Daten werden gelöscht. Sie können bis zu 1000 Zeichen eingeben. Schließen Sie die Daten in Anführungszeichen ein, wenn die Daten ein oder mehrere Leerzeichen enthalten. Bei den Daten muss die Groß-/Kleinschreibung beachtet werden.

Beispiel: Scratchpadeintrag aktualisieren

Aktualisieren Sie Kontaktinformationen für die Abwesenheit eines Administrators, Jane, in einer Datenbank, in der Informationen zu den Standorten aller Administratoren gespeichert sind:

```
update scratchpadentry admin_info location jane line=2 data=
"Nicht im Büro bis 18.11."
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE SCRATCHPADENTRY

Befehl	Beschreibung
DEFINE SCRATCHPADENTRY	Erstellt eine Zeile mit Daten im Scratchpad.
DELETE SCRATCHPADENTRY	Löscht eine Zeile mit Daten aus dem Scratchpad.
QUERY SCRATCHPADENTRY	Zeigt Informationen an, die im Scratchpad enthalten sind.
SET SCRATCHPADRETENTION	Gibt den Zeitraum an, den Scratchpadeinträge aufbewahrt werden.

UPDATE SCRIPT (IBM Spectrum Protect-Prozedur aktualisieren)

Mit diesem Befehl kann eine Befehlszeile geändert oder einer IBM Spectrum Protect-Prozedur eine neue Befehlszeile hinzugefügt werden.

Einschränkung: Die Ausgabe eines Befehls innerhalb einer IBM Spectrum Protect-Prozedur kann nicht umgeleitet werden. Führen Sie stattdessen die Prozedur aus und geben Sie dann die Befehlsumleitung an. Soll beispielsweise die Ausgabe von script1 in das Verzeichnis c:\temp\test.out übertragen werden, führen Sie wie im folgenden Beispiel die Prozedur aus und geben Sie die Befehlsumleitung an:

```
run script1 > c:\temp\test.out
```

Berechtigungsklasse

Um diesen Befehl ausgeben zu können, muß der Administrator die Prozedur zuvor definiert oder die Systemberechtigung haben.

Syntax

```
>>-UPDate SCRipt--Prozedurname----------------------------------->

>--+-----------------------------------+------------------------>
   '-Befehlszeile--+-----------------+-'
                   '-Line -=--Nummer-'

>--+-------------------------------+--------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Prozedurname (Erforderlich)
: Gibt den Namen der Prozedur an, die aktualisiert werden soll.

Befehlszeile

Gibt einen neuen oder aktualisierten Befehl an, der in einer Prozedur verarbeitet werden soll. Wird dieser Befehl ausgegeben, muss ein Befehl und/oder eine Beschreibung aktualisiert werden.

Der Befehl kann Substitutionsvariablen enthalten und über mehrere Zeilen fortgesetzt werden, wenn als letztes Zeichen in dem Befehl ein Fortsetzungszeichen (-) angegeben wird. Für den Befehl können bis zu 1200 Zeichen angegeben werden. Den Befehl in Anführungszeichen einschließen, wenn er Leerzeichen enthält. Wird dieser Parameter angegeben, kann der folgende Parameter wahlweise angegeben werden.

Sie haben die Optionen, Befehle seriell, parallel oder seriell und parallel auszuführen, indem Sie den Prozedurbefehl SERIAL oder PARALLEL für diesen Parameter angeben. Sie können mehrere Befehle parallel ausführen und auf deren Beendigung warten, bevor Sie mit dem nächsten Befehl fortfahren. Befehle werden seriell ausgeführt, bis der parallele Befehl gefunden wird.

Ablaufanweisungen mit bedingter Logik können verwendet werden. Diese Anweisungen schließen IF, EXIT und GOTO ein.

Line
: Gibt die Zeilennummer für den Befehl an. Wird keine Zeilennummer angegeben, wird die Befehlszeile an die bestehende Befehlszeilenfolge angehängt. Der angehängten Befehlszeile wird eine Zeilennummer zugeordnet, die um fünf höher ist als die letzte Befehlszeilennummer. Hat beispielsweise die letzte Zeile in der Prozedur die Nummer 015, wird der angehängten Befehlszeile die Zeilennummer 020 zugeordnet.

  Bei Angabe einer Zeilennummer ersetzt der Befehl eine vorhandene Zeile (wenn die Nummer mit der einer bestehenden Zeile identisch ist). Andernfalls fügt der Befehl die angegebene Zeile ein (wenn die Zeilennummer nicht einer vorhandenen Zeilennummer in der Befehlszeilenfolge entspricht).

DESCription
: Gibt eine Beschreibung für die Prozedur an. Für die Beschreibung können bis zu 255 Zeichen angegeben werden. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

Beispiel: Einen Befehl am Ende eines Scripts hinzufügen

Angenommen, Sie haben das folgende Script mit drei Zeilen (QSAMPLE) definiert und möchten den Befehl QUERY SESSION am Ende des Scripts hinzufügen.

```
 001  /* Dies ist eine Beispielprozedur */
 005  QUERY STATUS
 010  QUERY PROCESS
```

```
update script qsample "query session"
```

Nach der Verarbeitung des Befehls besteht das Script aus den folgenden Zeilen:

```
 001  /* Dies ist eine Beispielprozedur */
 005  QUERY STATUS
 010  QUERY PROCESS
  015  QUERY SESSION
```

Beispiel: Eine bestimmte Zeile in einem Script aktualisieren

Unter Verwendung des Scripts aus dem vorherigen Beispiel Zeile 010 ändern, so dass der Befehl QUERY STGPOOL an Stelle des Befehls QUERY PROCESS verarbeitet wird:

```
update script qsample "query stgpool" line=010
```

Nach der Verarbeitung des Befehls besteht das Script aus den folgenden Zeilen:

```
 001  /* Dies ist eine Beispielprozedur */
 005  QUERY STATUS
 010  QUERY STGPOOL
  015  QUERY SESSION
```

Beispiel: Einen Befehl in der Mitte eines Scripts einfügen

Unter Verwendung des Scripts aus dem vorherigen Beispiel eine neue Befehlszeile (QUERY NODE) hinter der Befehlszeile QUERY STATUS in dem Script QSAMPLE einfügen:

```
update script qsample "query node"
line=007
```

Nach der Verarbeitung des Befehls besteht das Script aus den folgenden Zeilen:

```
 001  /* Dies ist eine Beispielprozedur */
 005  QUERY STATUS
 007  QUERY NODE
 010  QUERY STGPOOL
  015  QUERY SESSION
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE SCRIPT

Befehl	Beschreibung
COPY SCRIPT	Erstellt eine Kopie einer Prozedur.
DEFINE SCRIPT	Definiert eine Prozedur für den IBM Spectrum Protect-Server.
DELETE SCRIPT	Löscht eine Prozedur oder einzelne Zeilen aus einer Prozedur.
QUERY SCRIPT	Zeigt Informationen über Prozeduren an.
RENAME SCRIPT	Vergibt einen neuen Namen für eine Prozedur.
RUN	Führt ein Script aus.

Zugehörige Tasks:
Befehle parallel oder seriell ausführen
Logikablaufanweisungen in ein Script einschließen
Tasks gleichzeitig auf mehreren Servern ausführen
Server-Script definieren
Zugehörige Verweise:
Rückkehrcodes für die Verwendung in IBM Spectrum Protect-Scripts

UPDATE SERVER (Server aktualisieren, der für die Übertragung zwischen Servern definiert ist)

Mit diesem Befehl kann eine Serverdefinition aktualisiert werden.

Einschränkung: Ist dieser Server ein Quellenserver für eine Operation mit virtuellem Datenträger, kann das Ändern dieser Werte Auswirkungen auf die Fähigkeit des Quellenservers haben, auf die Daten zuzugreifen und die Daten zu verwalten, die auf dem entsprechenden Zielserver gespeichert sind. Wird der Servername mit dem Befehl SET SERVERNAME geändert, kann dies abhängig vom Betriebssystem zusätzliche Auswirkungen haben. Nachfolgend sind einige Beispiele aufgeführt:

- Kennwörter können ungültig gemacht werden
- Einheitendaten können betroffen sein
- Angaben aus der Registrierungsdatenbank zu Windows-Betriebssystemen können sich ändern

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax für:

- **Unternehmensweite Konfiguration**
- **Unternehmensweite Ereignisprotokollierung**
- **Befehlsweiterleitung**
- **Speicheragent**
- **Quellen- und Zielserver für Knotenreplikation**
- AIX-BetriebssystemeLinux-Betriebssysteme**z/OS Media-Server**

```
>>-UPDate--SERver--Servername-------------------------------------->

>--+-----------------------------+------------------------------->
   '-SERVERPAssword--=--Kennwort-'

>--+---------------------------+--------------------------------->
   '-HLAddress--=--IP-Adresse-'

>--+-----------------------------+--+----------------------+---->
   '-LLAddress--=--TCP-Anschluss-'  '-COMMmethod--=--TCPIP-'

>--+-------------+--+--------------------------+----------------->
   '-URL--=--URL-'  '-ALLOWReplace--=--+-Yes-+-'
                                       '-No--'

>--+-----------------------------+------------------------------->
   '-DESCription--=--Beschreibung-'

>--+-----------------------+----------------------------------->
   '-FORCESync--=--+-Yes-+-'
                   '-No--'
```

```
>--+-----------------------------------+----------------------->
   |  (1)                              |
   '-------VALIdateprotocol--=--+-No--+-'
                                '-All-'

>--+-----------------+-------------------------------------------->
   '-SSL--=--+-No--+-'
             '-Yes-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+-----------------------------------+---------------------->
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'

   .-TRANSFERMethod--=--Tcpip--------.
>--+-------------------------------+------------------------><
   '-TRANSFERMethod--=--+-Tcpip----+-'
                        |      (2) |
                        '-Fasp-----'
```

Anmerkungen:

1. Der Parameter VALIDATEPROTOCOL ist veraltet und gilt nur für Speicheragentendefinitionen.
2. Linux-BetriebssystemeDer Parameter TRANSFERMETHOD ist nur auf Betriebssystemen Linux x86_64 verfügbar.

Syntax für virtuelle Datenträger

```
>>-UPDate--SERver--Servername--+----------------------+-------->
                               '-PAssword--=--Kennwort-'

>--+--------------------------+--------------------------------->
   '-HLAddress--=--IP-Adresse-'

>--+-----------------------------+--+----------------------+---->
   '-LLAddress--=--TCP-Anschluss-'  '-COMMmethod--=--TCPIP-'

>--+-------------+--+-------------------------+----------------->
   '-URL--=--URL-'  '-DELgraceperiod--=--Tage-'

>--+-------------------------+--+-------------+----------------->
   '-NODEName--=--Knotenname-'  '-SSL--=--Yes-'

   .-SESSIONSECurity--=--TRANSitional-----.
>--+-----------------------------------+---------------------->
   '-SESSIONSECurity--=--+-STRict-------+-'
                         '-TRANSitional-'

>--+-----------------------+------------------------------------>
   '-FORCESync--=--+-Yes-+-'
                   '-No--'

>--+-----------------------------+--------------------------><
   '-DESCription--=--Beschreibung-'
```

Parameter

Servername (Erforderlich)
: Gibt den Namen des Servers an, der aktualisiert werden soll. Dieser Parameter ist erforderlich.

PAssword
: Gibt das Kennwort an, das für die Anmeldung am Zielserver für virtuelle Datenträger verwendet wird. Dieser Parameter ist wahlfrei.

SERVERPAssword
: Gibt das Serverkennwort an, das für unternehmensweite Konfiguration, Befehlsweiterleitung und Ereignisprotokollierung zwischen Servern verwendet wird. Das Kennwort muss mit dem Serverkennwort übereinstimmen, das mit dem Befehl SET SERVERPASSWORD definiert wurde. Dieser Parameter ist wahlfrei.

HLAddress
: Gibt die IP-Adresse des Servers an (in der Schreibweise mit Trennzeichen). Dieser Parameter ist wahlfrei.

LLAddress
: Gibt die Adresse der unteren Ebene des Servers an. Diese Adresse stimmt normalerweise mit der Adresse in der Serveroption TCPPORT des Zielservers überein. Bei SSL=YES muss der Anschluss bereits für die SSL-Übertragung auf dem Zielserver definiert sein.

COMMmethod
: Gibt die Übertragungsmethode an, mit der die Verbindung zum Server hergestellt wird. Dieser Parameter ist wahlfrei.

URL
: Gibt die URL-Adresse an, die für den Zugriff auf diesen Server vom Administration Center aus verwendet wird. Der Parameter ist wahlfrei.

DELgraceperiod
Gibt die Anzahl Tage an, die ein Objekt auf dem Zielserver verbleibt, nachdem es zum Löschen markiert wurde. Sie können einen Wert von 0 bis 9999 angeben. Der Standardwert ist 5. Dieser Parameter ist optional.

NODEName
Gibt einen Knotennamen an, den der Server für die Verbindung zum Zielserver verwenden soll. Dieser Parameter ist wahlfrei.

DESCription
Gibt eine Beschreibung des Servers an. Dieser Parameter ist wahlfrei. Die Beschreibung kann bis zu 255 Zeichen umfassen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ('') angeben.

FORCESync
Gibt an, ob der Serverprüfschlüssel zurückgesetzt werden soll, wenn sich der Quellenserver das nächste Mal beim Zielserver anmeldet. Mit einem gültigen Prüfschlüssel kann ein Quellenserver Objekte auf den Zielserver stellen, den Wert für die Verweildauer bis zum Löschen verwalten und das Kennwort aktualisieren, wenn das aktuelle Kennwort bekannt ist und der Prüfschlüssel übereinstimmt. Der Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass ein neuer Prüfschlüssel an den Zielserver gesendet und vom Zielserver akzeptiert wird, wenn ein gültiges Kennwort empfangen wird.

No
Gibt an, dass kein neuer Prüfschlüssel an den Zielserver gesendet wird.

VALIdateprotocol (veraltet)
Gibt an, ob eine zyklische Blockprüfung die Daten validiert, die zwischen dem Speicheragenten und dem IBM Spectrum Protect-Server gesendet werden. Der Parameter ist wahlfrei. Der Standardwert ist NO.
Wichtig: Ab IBM Spectrum Protect Version 8.1.2 wird die durch diesen Parameter aktivierte Validierung durch das TLS 1.2-Protokoll ersetzt, das durch den Parameter SESSIONSECURITY durchgesetzt wird. Der Parameter VALIDATEPROTOCOL wird ignoriert. Aktualisieren Sie Ihre Konfiguration für die Verwendung des Parameters SESSIONSECURITY.

ALLOWReplace
Gibt an, ob eine durch einen verwalteten Server definierte Serverdefinition durch eine Definition vom Konfigurationsmanager ersetzt werden kann. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

Yes
Gibt an, dass eine Serverdefinition durch eine Definition vom Konfigurationsmanager ersetzt werden kann.

No
Gibt an, dass eine Serverdefinition nicht durch die Definition vom Konfigurationsmanager ersetzt werden kann.

SSL
Gibt den Kommunikationsmodus des Servers an.
Wichtig: Ab Version 8.1.2 wird SSL verwendet, um einen Teil der Kommunikation mit dem angegebenen Server zu verschlüsseln, auch wenn Sie NO angeben.
Die folgenden Bedingungen und Hinweise gelten, wenn Sie den Parameter SSL angeben:

- Selbst signierte Zertifikate der Partnerserver müssen sich in der Schlüsseldatenbankdatei (cert.kdb) jedes Servers befinden, bevor die Server gestartet werden.
- Sie können mehrere Servernamen mit verschiedenen Parametern für denselben Zielserver definieren.

Sie können einen der folgenden Werte angeben:

No
Gibt eine SSL-Sitzung für die gesamte Kommunikation mit dem angegebenen Server an, außer wenn der Server Objektdaten sendet oder empfängt. Objektdaten werden mithilfe von TCP/IP gesendet und empfangen. Wird ausgewählt, dass die Objektdaten nicht verschlüsselt werden, ähnelt die Serverleistung der Kommunikation über eine TCP/IP-Sitzung und die Sitzung ist sicher.

Yes
Gibt eine SSL-Sitzung für die gesamte Kommunikation mit dem angegebenen Server an, auch wenn der Server Objektdaten sendet und empfängt.

SESSIONSECurity
Gibt an, ob der Server, der definiert wird, die sichersten Einstellungen verwenden muss, um mit einem IBM Spectrum Protect-Server zu kommunizieren. Dieser Parameter ist wahlfrei.

Sie können einen der folgenden Werte angeben:

STRict
Gibt an, dass die striktesten Sicherheitseinstellungen für den Server, der definiert wird, durchgesetzt werden. Der Wert STRICT verwendet das sicherste Kommunikationsprotokoll, das verfügbar ist. Dies ist derzeit TLS 1.2. Das TLS 1.2-Protokoll wird für SSL-Sitzungen zwischen dem angegebenen Server und einem IBM Spectrum Protect-Server verwendet.
Für die Verwendung des Werts STRICT müssen die folgenden Anforderungen erfüllt werden, um sicherzustellen, dass sich der angegebene Server mit dem IBM Spectrum Protect-Server authentifizieren kann:

- Der Server, der definiert wird, und der IBM Spectrum Protect-Server müssen IBM Spectrum Protect-Software verwenden, die den Parameter SESSIONSECURITY unterstützt.

- Der Server, der definiert wird, muss für die Verwendung des TLS 1.2-Protokolls für SSL-Sitzungen zwischen sich selbst und dem IBM Spectrum Protect-Server konfiguriert werden.

Server, für die der Wert STRICT definiert ist und die diese Anforderungen nicht erfüllen, können sich nicht mit dem IBM Spectrum Protect-Server authentifizieren.

TRANSitional
: Gibt an, dass die vorhandenen Sicherheitseinstellungen für den Server durchgesetzt werden. Dies ist der Standardwert. Dieser Wert ist für die temporäre Verwendung bestimmt, während Sie Ihre Sicherheitseinstellungen aktualisieren, um die Anforderungen für den Wert STRICT zu erfüllen.

  Ist SESSIONSECURITY=TRANSITIONAL definiert und hat der Server nie die Anforderungen für den Wert STRICT erfüllt, authentifiziert sich der Server weiterhin mithilfe des Werts TRANSITIONAL. Wenn ein Server jedoch die Anforderungen für den Wert STRICT erfüllt, wird der Wert des Parameters SESSIONSECURITY automatisch von TRANSITIONAL in STRICT aktualisiert. Der Server kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt. Nachdem sich ein Server erfolgreich mit einem Kommunikationsprotokoll authentifiziert hat, das mehr Sicherheit bietet, kann sich der Server nicht mehr mit einem weniger sicheren Protokoll authentifizieren. Beispiel: Wenn ein Server, der nicht SSL verwendet, aktualisiert wird und sich mithilfe von TLS 1.2 erfolgreich authentifiziert, kann sich der Server nicht mehr ohne SSL-Protokoll oder mithilfe von TLS 1.1 authentifizieren. Diese Einschränkung gilt auch bei Verwendung von Funktionen wie z. B. virtuelle Datenträger, Befehlsweiterleitung oder Export zwischen Servern, wenn sich ein Knoten oder Administrator beim IBM Spectrum Protect-Server als Knoten oder Administrator von einem anderen Server authentifiziert.

Linux-BetriebssystemeTRANSFERMethod
: Linux-BetriebssystemeGibt die Methode an, die für die Datenübertragung zwischen Servern verwendet wird. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  Tcpip
  : Gibt an, dass TCP/IP für die Übertragung von Daten verwendet wird. Dies ist der Standardwert.

  Fasp
  : Gibt an, dass die Aspera FASP-Technologie (Fast Adaptive Secure Protocol) für die Übertragung von Daten verwendet wird. Mit der Aspera FASP-Technologie kann die Datenübertragung in einem Weitverkehrsnetz (WAN) optimiert werden.
  Einschränkungen:

  - Bevor Sie die Aspera FASP-Technologie aktivieren, müssen Sie bestimmen, ob die Technologie für Ihre Systemumgebung geeignet ist, und die entsprechenden Lizenzen installieren. Anweisungen finden Sie unter Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann. Wenn die Lizenzen fehlen oder abgelaufen sind, schlagen Datenübertragungsoperationen fehl.
  - Wenn die WAN-Leistung Ihre Geschäftsanforderungen erfüllt, aktivieren Sie nicht die Aspera FASP-Technologie.
  - Wenn Sie TRANSFERMETHOD=FASP im Befehl PROTECT STGPOOL oder REPLICATE NODE angeben, überschreibt dieser Wert den Parameter TRANSFERMETHOD in den Befehlen DEFINE SERVER und UPDATE SERVER.

Beispiel: Karenzzeit bis zum Löschen für einen Server aktualisieren

Die Definition von SERVER2 aktualisieren, um anzugeben, dass Objekte noch 10 Tage auf dem Zielserver verbleiben sollen, nachdem sie zum Löschen markiert wurden.

```
update server server2 delgraceperiod=10
```

Beispiel: Den URL für einen Server aktualisieren

Die Definition von NEWSERVER aktualisieren, um seine URL-Adresse als http://newserver:1580/ anzugeben.

```
update server newserver url=http://newserver:1580/
```

Beispiel: Alle Server für die Kommunikation mit einem IBM Spectrum Protect-Server unter Verwendung der Sitzungssicherheit 'strict' aktualisieren

Die Definition aller Server für die Verwendung der striktesten Sicherheitseinstellungen aktualisieren, um sich mit dem IBM Spectrum Protect-Server zu authentifizieren.

```
update server * sessionsecurity=strict
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE SERVER

Befehl	Beschreibung
DEFINE DEVCLASS	Definiert eine Einheitenklasse.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
DELETE DEVCLASS	Löscht eine Einheitenklasse.

Befehl	Beschreibung
DELETE FILESPACE	Löscht Daten, die Clientdateibereichen zugeordnet sind. Ist ein Dateibereich Teil einer Kollokationsgruppe und wird der Dateibereich aus einem Knoten entfernt, wird der Dateibereich aus der Kollokationsgruppe entfernt.
DELETE SERVER	Löscht die Definition eines Servers.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY SERVER	Zeigt Informationen über Server an.
RECONCILE VOLUMES	Stimmt Definitionen von virtuellen Datenträgern auf dem Quellenserver mit Archivierungsobjekten des Zielservers ab.
REGISTER NODE	Definiert einen Clientknoten für den Server und legt Optionen für diesen Benutzer fest.
REMOVE NODE	Entfernt einen Client aus der Liste der registrierten Knoten für eine bestimmte Maßnahmendomäne.
UPDATE DEVCLASS	Ändert die Attribute einer Einheitenklasse.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.

UPDATE SERVERGROUP (Beschreibung einer Servergruppe aktualisieren)

Mit diesem Befehl kann die Beschreibung einer Server-Gruppe aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-UPDate SERVERGroup--Gruppenname------------------------------>

>--DESCription--=--Beschreibung--------------------------------><
```

Parameter

Gruppenname (Erforderlich)
: Gibt die Server-Gruppe an, die aktualisiert werden soll.

DESCription (Erforderlich)
: Gibt eine Beschreibung der Server-Gruppe an. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält.

Beispiel: Die Beschreibung einer Servergruppe aktualisieren

Die Beschreibung der Servergruppe WEST_COMPLEX in "Western Region Complex" aktualisieren.

```
update servergroup west_complex
 description="western region complex"
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE SERVERGROUP

Befehl	Beschreibung
COPY SERVERGROUP	Erstellt eine Kopie einer Servergruppe.
DEFINE SERVERGROUP	Definiert eine neue Servergruppe.
DELETE SERVERGROUP	Löscht eine Servergruppe.
QUERY SERVERGROUP	Zeigt Informationen über Servergruppen an.
RENAME SERVERGROUP	Benennt eine Servergruppe um.

UPDATE SPACETRIGGER (Speicherbereichsauslöser aktualisieren)

Mit diesem Befehl können Einstellungen für Auslöser aktualisiert werden, die festlegen, wann und wie der Server Speicherbereichsmängel in Speicherpools behebt, die die Einheitenklassen FILE mit sequenziellem Zugriff und DISK mit wahlfreiem Zugriff verwenden.

Für Speicherpools mit dem Parameter RECLAMATIONTYPE=SNAPLOCK werden keine Speicherbereichsauslöser aktiviert.

Wichtig: Bei Speicherbereichsauslöserfunktionen und Berechnungen des Speicherbereichs im Speicherpool wird der Speicherbereich berücksichtigt, der in jedem Verzeichnis verbleibt. Idealerweise sollten Sie jedem Verzeichnis ein separates Dateisystem zuordnen. Wenn Sie mehrere Verzeichnisse für eine Einheitenklasse angeben und sich die Verzeichnisse in demselben Dateisystem befinden, berechnet der Server den Speicherbereich durch Hinzufügen von Werten, die den Speicherbereich darstellen, der in jedem Verzeichnis verbleibt. Diese Speicherbereichsberechnungen sind ungenau. Anstatt einen Speicherpool mit ausreichend Speicherbereich für eine Operation auszuwählen, kann der Server den falschen Speicherpool auswählen und frühzeitig über keinen Speicherbereich mehr verfügen. Bei Speicherbereichsauslösern kann eine ungenaue Berechnung zu einem Fehler bei der Erweiterung des Speicherbereichs führen, der in einem Speicherpool verfügbar ist. Ein Fehler bei der Erweiterung des Speicherbereichs in einem Speicherpool ist eine der Bedingungen, die zur Inaktivierung eines Auslösers führen kann. Wird ein Auslöser inaktiviert, da der Speicherbereich in einem Speicherpool nicht erweitert werden konnte, können Sie den Auslöser erneut aktivieren, indem Sie den folgenden Befehl angeben: `update spacetrigger stg`. Es sind keine weiteren Änderungen an dem Speicherbereichsauslöser erforderlich.

Weitere Informationen befinden sich unter dem Befehl DEFINE SPACETRIGGER.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate SPACETrigger--STG--+---------------------+------------>
                            '-Fullpct--=--Prozent-'

>--+-----------------------------+-------------------------------->
   '-SPACEexpansion---=--Prozent-'

>--+-----------------------------+-------------------------------->
   '-EXPansionprefix---=--Präfix-'

>--+-------------------------------+---------------------------><
   '-STGPOOL---=--Speicherpoolname-'
```

Parameter

STG (Erforderlich)
: Gibt einen Speicherbereichsauslöser für den Speicherpool an.

Fullpct
: Dieser Parameter gibt den Auslastungsprozentsatz des Speicherpools an.

  Wird dieser Wert überschritten, erstellt der Speicherbereichsauslöser neue Datenträger.

  Sie können die Auslastung des Speicherpools bestimmen, indem Sie den Befehl QUERY STGPOOL mit FORMAT=DETAILED ausgeben. Der Prozentsatz der Speicherpoolauslastung für den Speicherpool wird im Feld "Ausl. für Speicherbereichsauslöser" angezeigt. Die Berechnung dieses Prozentsatzes schließt keine potenziellen Arbeitsdatenträger ein. Die Berechnung der prozentualen Auslastung bei der Umlagerung und Wiederherstellung schließt jedoch potenzielle Arbeitsdatenträger ein.

SPACEexpansion
: Für Speicherbereichsauslöser für Speicherpools des Typs FILE mit sequenziellem Zugriff wird dieser Parameter bei der Bestimmung der Anzahl zusätzlicher Datenträger verwendet, die in dem Speicherpool erstellt werden. Datenträger werden unter Verwendung des Werts für MAXCAPACITY aus der Einheitenklasse des Speicherpools erstellt. Für Speicherbereichsauslöser für DISK-Speicherpools mit wahlfreiem Zugriff erstellt der Speicherbereichsauslöser einen einzelnen Datenträger unter Verwendung von EXPANSIONPREFIX.

EXPansionprefix
: Dieser Parameter gibt das Präfix an, das der Server zum Erstellen neuer Speicherpooldateien verwendet. Dieser Parameter ist wahlfrei und gilt nur für Einheitenklassen DISK mit wahlfreiem Zugriff. Das Standardpräfix ist der Serverinstallationspfad.
  Das Präfix kann ein oder mehrere Verzeichnistrennzeichen enthalten. Beispiel: AIX-Betriebssysteme Linux-Betriebssysteme

  ```
  /opt/tivoli/tsm/server/bin/
  ```

  Windows-Betriebssysteme

  ```
  c:\Programme\tivoli\tsm\
  ```

  AIX-Betriebssysteme Linux-BetriebssystemeEs können bis zu 250 Zeichen angegeben werden. Wenn Sie ein ungültiges Präfix angeben, kann die automatische Erweiterung fehlschlagen.

Windows-BetriebssystemeSie können bis zu 200 Zeichen angeben. Wird der Server als Windows-Dienst ausgeführt, ist das Standardpräfix das Verzeichnis c:\wnnt\system32. Wenn Sie ein ungültiges Präfix angeben, kann die automatische Erweiterung fehlschlagen.

Dieser Parameter ist für Speicherbereichsauslöser für FILE-Speicherpools mit sequenziellem Zugriff nicht gültig. Es werden Präfixe der Verzeichnisse verwendet, die mit der zugeordneten Einheitenklasse angegeben sind.

STGPOOL
Gibt den Speicherpool an, der diesem Speicherbereichsauslöser zugeordnet ist. Wird der Parameter STGPOOL nicht angegeben, wird der standardmäßige Speicherbereichsauslöser für den Speicherpool aktualisiert.

Dieser Parameter gilt nicht für Speicherpools mit dem Parameter RECLAMATIONTYPE=SNAPLOCK.

Beispiel: Den Speicherbereich für einen Speicherpool vergrößern

Den Speicherbereich in einem Speicherpool um 50 Prozent vergrößern, wenn der Speicherpool zu 80 Prozent mit vorhandenen Datenträgern belegt ist. Speicherbereich wird in den Verzeichnissen erstellt, die der Einheitenklasse zugeordnet sind.

```
update spacetrigger stg spaceexpansion=50 stgpool=file
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE SPACETRIGGER

Befehl	Beschreibung
DEFINE SPACETRIGGER	Definiert einen Speicherbereichsauslöser zum Erweitern des Speicherbereichs für einen Speicherpool.
DELETE SPACETRIGGER	Löscht den Speicherbereichsauslöser für den Speicherpool.
QUERY SPACETRIGGER	Zeigt Informationen zu einem Speicherbereichsauslöser für den Speicherpool an.

UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)

Mit diesem Befehl können Sie einen vorhandenen Schwellenwert für die Statusüberwachung aktualisieren.

Mit Statusüberwachungsschwellenwerten werden die definierten Bedingungen mit den Serverabfragen für die Statusüberwachung verglichen und die Ergebnisse in die Statusüberwachungstabelle eingefügt.

Es können mehrere Schwellenwerte für eine Aktivität definiert werden. Sie können beispielsweise einen Schwellenwert erstellen, der einen Warnstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 80 % ist. Sie können dann einen anderen Schwellenwert erstellen, der einen Fehlerstatus bereitstellt, wenn die Auslastung der Speicherpoolkapazität größer als 90 % ist.

Anmerkung: Wenn bereits ein Schwellenwert für eine Bedingung EXISTS definiert ist, können Sie keinen anderen Schwellenwert mit einem der anderen Bedingungstypen definieren.

Syntax

```
>>-UPDate STAtusthreshold--Schwellenwertname--+----------------------------------+-->
                                              '-Activity--=--Name der Aktivität-'

>--+--------------------------+--+----------------+-------------><
   '-Condition--=--+-EXists-+-'  '-Value--=--Wert-'
                   +-GT-----+
                   +-GE-----+
                   +-LT-----+
                   +-LE-----+
                   '-EQual--'

>--+------------------------+-----------------------------------><
   '-STatus--=--+-Normal--+-'
                +-Warning-+
                '-Error---'
```

Parameter

Schwellenwertname (Erforderlich)
Gibt den Schwellenwertnamen an, der aktualisiert werden soll. Der Name darf 48 Zeichen nicht überschreiten.

Activity

Geben Sie diesen Wert an, um die Aktivität für einen vorhandenen Schwellenwert zu ändern. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

PROCESSSUMMARY
: Gibt die Anzahl Prozesse an, die gegenwärtig aktiv sind.

SESSIONSUMMARY
: Gibt die Anzahl Sitzungen an, die gegenwärtig aktiv sind.

CLIENTSESSIONSUMMARY
: Gibt die Anzahl Clientsitzungen an, die gegenwärtig aktiv sind.

SCHEDCLIENTSESSIONSUMMARY
: Gibt die Anzahl geplanter Clientsitzungen an.

DBUTIL
: Gibt die prozentuale Datenbankauslastung an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

DBFREESPACE
: Gibt den freien Speicherbereich in Gigabyte an, der in der Datenbank verfügbar ist.

DBUSEDSPACE
: Gibt den verwendeten Datenbankbereich in Gigabyte an.

ARCHIVELOGFREESPACE
: Gibt den freien Speicherbereich in Gigabyte an, der im Archivprotokoll verfügbar ist.

STGPOOLUTIL
: Gibt die prozentuale Auslastung des Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

STGPOOLCAPACITY
: Gibt die Speicherpoolkapazität in Gigabyte an.

AVGSTGPOOLUTIL
: Gibt die durchschnittliche prozentuale Speicherpoolauslastung für alle Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

TOTSTGPOOLCAPACITY
: Gibt die Gesamtspeicherpoolkapazität in Gigabyte für alle verfügbaren Speicherpools an.

TOTSTGPOOLS
: Gibt die Anzahl der definierten Speicherpools an.

TOTRWSTGPOOLS
: Gibt die Anzahl der definierten Speicherpools an, die lesbar oder änderbar sind.

TOTNOTRWSTGPOOLS
: Gibt die Anzahl der definierten Speicherpools an, die nicht lesbar oder änderbar sind.

STGPOOLINUSEANDDEFINED
: Gibt die Gesamtzahl der definierten Datenträger an, die im Gebrauch sind.

ACTIVELOGUTIL
: Gibt die aktuelle prozentuale Auslastung der aktiven Protokolldatei an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

ARCHLOGUTIL
: Gibt die aktuelle Auslastung des Archivprotokolls an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

CPYSTGPOOLUTIL
: Gibt die prozentuale Auslastung eines Kopienspeicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

PMRYSTGPOOLUTIL
: Gibt die prozentuale Auslastung eines primären Speicherpools an. Der Standardschwellenwert für Warnung ist 80 % und der Standardschwellenwert für Fehler ist 90 %.

DEVCLASSPCTDRVOFFLINE
: Gibt die prozentuale Auslastung von Laufwerken an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTDRVPOLLING
: Gibt den Sendeaufruf für Laufwerke nach Einheitenklasse an. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTLIBPATHSOFFLINE
: Gibt die Kassettenarchivpfade an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTPATHSOFFLINE
: Gibt den Prozentsatz der Einheitenklassenpfade an (nach Einheitenklasse), die offline sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTDISKSNOTRW
: Gibt den Prozentsatz der Platten an, die für die Einheitenklasse DISK nicht beschreibbar sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

DEVCLASSPCTDISKSUNAVAILABLE
: Gibt den Prozentsatz der Plattendatenträger an (nach Einheitenklasse), die nicht verfügbar sind. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

FILEDEVCLASSPCTSCRUNALLOCATABLE
: Gibt den Prozentsatz der Arbeitsdatenträger an, die der Server für eine bestimmte Einheitenklasse FILE, die nicht gemeinsam genutzt wird, nicht zuordnen kann. Der Standardschwellenwert für Warnung ist 25 % und der Standardschwellenwert für Fehler ist 50 %.

Condition
: Geben Sie diesen Wert an, um die Bedingung eines vorhandenen Schwellenwerts zu ändern. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

  EXists
  : Erstellt einen Statusüberwachungsanzeiger, wenn die Aktivität vorhanden ist.

  GT
  : Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis größer als der angegebene Wert ist.

  GE
  : Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis größer-gleich dem angegebenen Wert ist.

  LT
  : Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis kleiner als der angegebene Wert ist.

  LE
  : Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis kleiner-gleich dem angegebenen Wert ist.

  EQual
  : Erstellt einen Statusüberwachungsanzeiger, wenn das Aktivitätsergebnis gleich dem angegebenen Wert ist.

Value
: Geben Sie diesen Parameter an, um den Wert zu ändern, der mit der Aktivitätsausgabe für die angegebene Bedingung verglichen wird. Sie können eine ganze Zahl im Bereich von 0 bis 999999999999999 angeben.

STatus
: Geben Sie diesen Wert an, um den Status des Anzeigers zu ändern, der bei der Statusüberwachung erstellt wird, wenn die Bedingung, die ausgewertet wird, erfüllt ist. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

  Normal
  : Gibt an, dass der Statusanzeiger einen normalen Statuswert hat.

  Warnung
  : Gibt an, dass der Statusanzeiger einen Warnstatuswert hat.

  Fehler
  : Gibt an, dass der Statusanzeiger einen Fehlerstatuswert hat.

Einen vorhandenen Statusschwellenwert aktualisieren

Mit dem folgenden Befehl einen Statusschwellenwert für die durchschnittliche prozentuale Speicherpoolauslastung aktualisieren:

```
update statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=90 condition=gt status=error
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE STATUSTHRESHOLD

Befehl	Beschreibung
DELETE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung löschen)	Löscht einen Schwellenwert für die Statusüberwachung.
QUERY MONITORSTATUS (Überwachungsstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY MONITORSETTINGS (Konfigurationseinstellungen für die Überwachung von Alerts und des Serverstatus abfragen)	Zeigt Informationen zu den Einstellungen für die Überwachung von Alerts und des Serverstatus an.
QUERY STATUSTHRESHOLD (Schwellenwerte für Statusüberwachung abfragen)	Zeigt Informationen zu Schwellenwerten für die Statusüberwachung an.
SET STATUSMONITOR (Gibt an, ob Statusüberwachung aktiviert werden soll)	Gibt an, ob die Statusüberwachung aktiviert werden soll.
SET STATUSATRISKINTERVAL (Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll)	Gibt an, ob die Auswertung des Aktivitätsintervalls zur Bestimmung der Gefährdung von Clients aktiviert werden soll.
SET STATUSREFRESHINTERVAL (Aktualisierungsintervall für Statusüberwachung definieren)	Gibt das Aktualisierungsintervall für die Statusüberwachung an.
SET STATUSSKIPASFAILURE (Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll)	Gibt an, ob die Bewertung übersprungener Dateien als Fehler zur Bestimmung der Gefährdung von Clients verwendet werden soll.

Befehl	Beschreibung
UPDATE STATUSTHRESHOLD (Schwellenwert für Statusüberwachung aktualisieren)	Ändert die Attribute eines vorhandenen Schwellenwerts für die Statusüberwachung.

UPDATE STGPOOL (Speicherpool aktualisieren)

Mit diesem Befehl kann ein Speicherpool geändert werden.

Einschränkung: Wenn ein Client die Funktion für gleichzeitiges Schreiben und die Datendeduplizierung verwendet, wird das Feature für die Datendeduplizierung während der Ausführung von Sicherungen in einem Speicherpool inaktiviert.

Der Befehl UPDATE STGPOOL verwendet sieben Formen. Syntax und Parameter der jeweiligen Form werden separat definiert.

Tabelle 1. Zugehörige Befehle für UPDATE STGPOOL

Befehl	Beschreibung
BACKUP STGPOOL	Sichert einen primären Speicherpool in einem Kopienspeicherpool.
COPY ACTIVEDATA	Kopiert aktive Sicherungsdaten.
DEFINE COLLOCGROUP	Definiert eine Kollokationsgruppe.
DEFINE COLLOCMEMBER	Fügt einen Clientknoten oder Dateibereich einer Kollokationsgruppe hinzu.
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DELETE COLLOCGROUP	Löscht eine Kollokationsgruppe.
DELETE COLLOCMEMBER	Löscht einen Clientknoten oder Dateibereich aus einer Kollokationsgruppe.
DELETE STGPOOL	Löscht einen Speicherpool aus dem Serverspeicher.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
MOVE MEDIA	Versetzt Speicherpooldatenträger, die von einem automatisierten Kassettenarchive verwaltet werden.
QUERY COLLOCGROUP	Zeigt Informationen zu Kollokationsgruppen an.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY NODEDATA	Zeigt Informationen zur Position und Größe von Daten für einen Clientknoten an.
QUERY SHREDSTATUS	Zeigt Informationen zu Daten an, die auf das Schreddern warten.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
RESTORE STGPOOL	Schreibt Dateien aus Kopienspeicherpools in einen primären Speicherpool zurück.
RESTORE VOLUME	Schreibt Dateien, die auf angegebenen Datenträgern in einem primären Speicherpool gespeichert sind, aus Kopienspeicherpools zurück.
SET DRMDBBACKUPEXPIREDAYS	Gibt die Kriterien für den Verfall von Datenbanksicherungsserien an.
SHRED DATA	Startet manuell den Prozess zum Schreddern gelöschter Daten.
UPDATE COLLOCGROUP	Aktualisiert die Beschreibung einer Kollokationsgruppe.

- UPDATE STGPOOL (Cloud-Containerspeicherpool aktualisieren)
  Mit diesem Befehl können Sie einen Containerspeicherpool in einer Cloudumgebung aktualisieren. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.
- UPDATE STGPOOL (Verzeichniscontainerspeicherpool aktualisieren)
  Mit diesem Befehl kann ein Verzeichniscontainerspeicherpool aktualisiert werden.
- UPDATE STGPOOL (Containerkopienspeicherpool aktualisieren)
  Mit diesem Befehl kann ein Containerkopienspeicherpool aktualisiert werden.
- UPDATE STGPOOL (Primären Speicherpool mit wahlfreiem Zugriff aktualisieren)
  Mit diesem Befehl kann ein Speicherpool mit wahlfreiem Zugriff aktualisiert werden.
- UPDATE STGPOOL (Primären Speicherpool mit sequenziellem Zugriff aktualisieren)
  Mit diesem Befehl kann ein primärer Speicherpool mit sequenziellem Zugriff aktualisiert werden.

- UPDATE STGPOOL (Kopienspeicherpool mit sequenziellem Zugriff aktualisieren)
  Mit diesem Befehl kann ein Kopienspeicherpool mit sequenziellem Zugriff aktualisiert werden.
- UPDATE STGPOOL (Pool für aktive Daten mit sequenziellem Zugriff aktualisieren)
  Mit diesem Befehl kann ein Pool für aktive Daten aktualisiert werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme

UPDATE STGPOOL (Cloud-Containerspeicherpool aktualisieren)

Mit diesem Befehl können Sie einen Containerspeicherpool in einer Cloudumgebung aktualisieren. Cloud-Containerspeicherpools werden unter Linux on System z nicht unterstützt.

Die bevorzugte Methode zum Definieren und Konfigurieren eines Cloud-Containerspeicherpools ist die Verwendung des Operations Center. Anweisungen und Hinweise für das Operations Center und die Befehlszeilenschnittstelle finden Sie in Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate STGpool--Poolname--+------------------------------+--->
                            '-DESCription--=--Beschreibung-'

>--+------------------------------+------------------------------>
   '-CLOUDType--=--+-SWift------+-'
                   +-SOftlayer-+
                   '-V1Swift---'

>--+------------------------+--+--------------------------+---->
   '-CLOUDUrl--=--Cloud-URL-'  |                      (1) |
                               '-IDentity--=--Cloud-ID-----'

>--+-----------------------+-------------------------------------->
   '-PAssword--=--Kennwort-'

>--+---------------------------------+------------------------->
   '-CLOUDLocation--=--+-OFfpremise-+-'
                       '-ONpremise--'

>--+-------------------------------+----------------------------->
   |                           (2) |
   '-BUCKETName--=--Bucketname-----'

>--+-----------------------------+------------------------------->
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                +-UNAVailable-+
                '-DESTroyed---'

>--+-------------------------------------------+----------------->
   '-MAXWriters--=--+-NOLimit----------------+-'
                    '-maximale_Anzahl_Writer-'

>--+---------------------+-------------------------------------->
   '-REUsedelay--=--Tage-'

>--+-----------------------------------------------------+-------><
   |                      .-COMPRession--=--Yes-----. |
   '-ENCRypt--=--+-Yes-+--+-------------------------+-'
                 '-No--'  '-COMPRession--=--+-Yes-+-'
                                            '-No--'
```

Anmerkungen:

1. Wenn Sie CLOUDTYPE=AZURE angegeben haben, geben Sie nicht den Parameter IDENTITY an.
2. Dieser Parameter ist nur gültig, wenn Sie CLOUDTYPE=S3 angeben.

Parameter

Poolname (Erforderlich)
    Gibt den Speicherpool an, der aktualisiert werden soll. Dieser Parameter ist erforderlich.
DESCription

Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Die Beschreibung in Anführungszeichen einschließen, wenn sie Leerzeichen enthält. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("") angeben.

CLOUDType

Gibt den Typ der Cloudumgebung an, in der ein Speicherpool konfiguriert wird. Dieser Parameter ist wahlfrei. Geben Sie einen der folgenden Werte an:

SOftlayer
: Gibt an, dass der Speicherpool ein Cloud-Computing-System 'SoftLayer' verwendet.

SWift
: Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 2 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

V1Swift
: Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 1 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

Einschränkung: Wenn Sie den Befehl DEFINE STGPOOL verwendet haben, um einen Speicherpool mit CLOUDTYPE=S3 (S3 = Simple Storage Service) zu definieren, können Sie mithilfe des Befehls UPDATE STGPOOL nicht zu einem anderen Cloudtyp wechseln. Außerdem können Sie nicht den Cloudtyp eines Nicht-S3-Speicherpools in S3 ändern, indem Sie den Befehl UPDATE STGPOOL verwenden.

CLOUDUrl

Gibt die URL der Cloudumgebung an, in der der Speicherpool konfiguriert wird. Auf der Basis Ihres Cloud-Providers können Sie eine Regionsendpunkt-URL, eine Accesser-IP-Adresse, einen Endpunkt für öffentliche Authentifizierung (Public Authentication Endpoint) oder einen ähnlichen Wert für diesen Parameter verwenden. Stellen Sie sicher, dass das Protokoll wie z. B. `https://` oder `http://` am Anfang der URL eingefügt wird. Die maximale Länge der Webadresse beträgt 870 Zeichen. Der Parameter CLOUDURL wird erst geprüft, wenn die erste Sicherung beginnt.

Weitere Informationen zum Ermitteln dieser Werte erhalten Sie, wenn Sie Ihren Cloud-Service-Provider in der Liste auf der Seite Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren auswählen.

Tipp: Um mehrere IBM® Cloud Object Storage-Accesser zu verwenden, listen Sie die Accesser-IP-Adressen getrennt durch einen vertikalen Balken (|) ohne Leerzeichen auf. Beispiel: *CLOUDURL=<Accesser-URL1>|<Accesser-URL2>|<Accesser-URL3>*. Die Verwendung mehrerer Accesser verbessert die Leistung. Wenn Sie die IBM SoftLayer Cloud Object Store S3-Lösung verwenden, wird nur ein Accesser benötigt.

IDentity

Gibt die Benutzer-ID für die Cloud an, die im Parameter STGTYPE=CLOUD angegeben ist. Dieser Parameter ist für alle unterstützten Cloud-Computing-Systeme außer Azure erforderlich. Wenn Sie CLOUDTYPE=AZURE angegeben haben, geben Sie nicht den Parameter IDENTITY an. Auf der Basis Ihres Cloud-Providers können Sie eine Zugriffsschlüssel-ID, einen Benutzernamen, einen Tenantnamen und Benutzernamen oder einen ähnlichen Wert für diesen Parameter verwenden. Die maximale Länge der Benutzer-ID beträgt 255 Zeichen.

PAssword (Erforderlich)

Gibt das Kennwort für die Cloud an, die im Parameter STGTYPE=CLOUD angegeben ist. Auf der Basis Ihres Cloud-Providers können Sie ein SAS-Token (SAS = Shared Access Signature), einen geheimen Zugriffsschlüssel, einen API-Schlüssel, ein Kennwort oder einen ähnlichen Wert für diesen Parameter verwenden. Dieser Parameter ist erforderlich. Die maximale Länge des Kennworts beträgt 255 Zeichen. Die Parameter IDENTITY und PASSWORD werden erst geprüft, wenn die erste Sicherung beginnt.

CLOUDLocation

Gibt die physische Position der Cloud an, die im Parameter CLOUD angegeben ist. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

- OFfpremise
- ONpremise

BUCKETName

Gibt den Namen für ein Amazon Web Services-Bucket (AWS-Bucket) oder eine IBM Cloud Object Storage-Vault an, das bzw. die mit diesem Speicherpool verwendet werden soll. AWS-Buckets und IBM Cloud Object Storage-Vaults werden auf dieselbe Art und Weise wie Container in einem Cloud-Containerspeicherpool verwendet. Dieser Parameter ist optional und ist nur gültig, wenn dieser Speicherpool den Cloudtyp S3 hat. Wenn der von Ihnen angegebene Name nicht vorhanden ist, erstellt der Server ein Bucket oder eine Vault mit dem angegebenen Namen, bevor das Bucket bzw. die Vault verwendet wird. Beachten Sie die Einschränkungen Ihres Cloud-Providers bei der Benennung, wenn Sie diesen Parameter angeben. Überprüfen Sie die Berechtigungen für das Bucket oder die Vault und stellen Sie sicher, dass die Berechtigungsnachweise für diesen Speicherpool über die Berechtigung zum Lesen, Schreiben, Auflisten und Löschen von Objekten in diesem Bucket oder dieser Vault haben.

Einschränkung: Sie können das Bucket oder die Vault nicht ändern, wenn in diesem Speicherpool Cloud-Container vorhanden sind.

ACCess

Gibt an, wie Clientknoten und Serverprozesse auf den Speicherpool zugreifen. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

READWrite
: Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff für den Speicherpool haben.

READOnly
: Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff für den Speicherpool haben.

UNAVailable

Gibt an, dass Clientknoten und Serverprozesse nicht auf den Speicherpool zugreifen können. Aus diesem Grund schlagen Sicherungen und Zurückschreibungen für diesen Speicherpool fehl. Mit diesem Wert können Sie angeben, dass der Cloud-Service-Provider vorübergehend nicht verfügbar ist.

DESTroyed
Gibt an, dass Clientknoten und Serverprozesse nicht auf den Speicherpool zugreifen können, da der Cloud-Service-Provider permanent nicht verfügbar ist. Sicherungen und Zurückschreibungen schlagen für diesen Speicherpool fehl, aber alle Versuche, Objekte und Container aus diesem Speicherpool zu löschen, werden erfolgreich ausgeführt.

MAXWriters
Gibt die maximale Anzahl der Schreibsitzungen an, die gleichzeitig für den Speicherpool ausgeführt werden können. Geben Sie eine maximale Anzahl von Schreibsitzungen an, um zu steuern, dass die Leistung des Cloudspeicherpools keine negativen Auswirkungen auf andere Systemressourcen hat. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

NOLimit
Gibt an, dass für die Anzahl der Writer, die Sie verwenden können, kein Grenzwert für die maximale Größe vorhanden ist. Dieser Wert ist der Standardwert.

maximale_Anzahl_Writer
Begrenzt die maximale Anzahl der Writer, die Sie verwenden können. Geben Sie eine ganze Zahl im Bereich von 1 bis 99999 an.

REUsedelay
Gibt die Anzahl Tage an, die verstreichen müssen, nachdem alle deduplizierten Speicherbereiche aus einem Cloudspeicherpool entfernt wurden. Dieser Parameter steuert die Dauer, die deduplizierte Speicherbereiche einem Cloudspeicherpool zugeordnet sind. Wenn der für den Parameter angegebene Wert abläuft, werden die deduplizierten Speicherbereiche aus dem Cloudspeicherpool gelöscht. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

1
Gibt an, dass deduplizierte Speicherbereiche nach 1 Tag aus einem Cloudspeicherpool gelöscht werden.

Tage
Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben.

Tipp: Setzen Sie diesen Parameter auf einen Wert, der größer als die für den Befehl SET DRMDBBACKUPEXPIREDAYS angegebene Anzahl ist. Wird dieser Parameter auf einen höheren Wert gesetzt, können Sie sicherstellen, dass Verweise auf Dateien im Speicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird.

ENCRypt
Gibt an, ob der Server Clientdaten verschlüsselt, bevor er sie in den Speicherpool schreibt. Sie können die folgenden Werte angeben:

Yes
Gibt an, dass Clientdaten vom Server verschlüsselt werden.

No
Gibt an, dass Clientdaten nicht vom Server verschlüsselt werden.

Dieser Parameter ist wahlfrei. Der Standardwert ist von der physischen Position der Cloud abhängig, die durch den Parameter CLOUDLOCATION angegeben wird. Wenn sich die Cloud außerhalb des Unternehmens (off premise) befindet, werden Daten standardmäßig vom Server verschlüsselt. Wenn sich die Cloud vor Ort (on premises) befindet, werden Daten standardmäßig nicht vom Server verschlüsselt.

COMPRession
Gibt an, ob Daten in dem Speicherpool komprimiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass Daten in dem Speicherpool nicht komprimiert werden.

Yes
Gibt an, dass Daten in dem Speicherpool komprimiert werden. Dies ist der Standardwert.

Beispiel 1: Einen Cloudspeicherpool aktualisieren, um eine maximale Anzahl von Datensitzungen anzugeben

Einen Cloudspeicherpool mit dem Namen STGPOOL1 aktualisieren und ein Maximum von 10 Datensitzungen angeben.

```
update stgpool stgpool1 maxwriters=10
```

Beispiel 2: Die Beschreibung eines Cloudspeicherpools aktualisieren

Einen Cloudspeicherpool mit dem Namen STGPOOL2 aktualisieren. Die vorhandene Beschreibung aus dem Speicherpool entfernen.

```
update stgpool stgpool2 cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password description=""
```

Zugehörige Tasks:
Cloud-Containerspeicherpool für die Datenspeicherung konfigurieren
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

UPDATE STGPOOL (Verzeichniscontainerspeicherpool aktualisieren)

Mit diesem Befehl kann ein Verzeichniscontainerspeicherpool aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate STGpool--Poolname--+------------------------------+--->
                             '-DESCription--=--Beschreibung-'

   .-ACCess--=--READWrite-------.
>--+----------------------------+------------------------------>
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                '-UNAVailable-'

   .-MAXSIze--=--NOLimit-----------------.
>--+-----------------------------------+---------------------->
   '-MAXSIze--=--+-maximale_Dateigröße-+-'
                 '-NOLimit-------------'

   .-MAXWriters--=--NOLimit--------------------.
>--+-----------------------------------------+---------------->
   '-MAXWriters--=--+-maximale_Anzahl_Writer-+-'
                    '-NOLimit----------------'

>--+--------------------------+-------------------------------->
   '-NEXTstgpool--=--Poolname-'

>--+----------------------------------+---------------------->
   '-PROTECTstgpool--=--Zielspeicherpool-'

>--+-------------------------------------------------------+---->
   |                          .-,------------------------. |
   |                          V                          | |
   '-PROTECTLOCalstgpools--=----lokaler Zielspeicherpool-+-'

   .-REUsedelay--=--1----.
>--+--------------------+--+--------------------+-------------->
   '-REUsedelay--=--Tage-'  '-ENCRypt--=--+-Yes-+-'
                                          '-No--'

   .-COMPRession--=--Yes-----.
>--+-------------------------+--------------------------------><
   '-COMPRession--=--+-Yes-+-'
                     '-No--'
```

Parameter

Poolname (Erforderlich)
: Gibt den Speicherpool an, der aktualisiert werden soll. Dieser Parameter ist erforderlich. Die maximale Länge des Namens beträgt 30 Zeichen.

DESCription
: Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("") angeben.

ACCess
: Gibt an, wie Clientknoten und Serverprozesse auf Dateien in dem Speicherpool zugreifen. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  READWrite
  : Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff für den Speicherpool haben. Dies ist der Standardwert.

  READOnly
  : Gibt an, dass Clientknoten und Serverprozesse nur Lesezugriff für den Speicherpool haben.

  UNAVailable
  : Gibt an, dass Clientknoten und Serverprozesse nicht auf den Speicherpool zugreifen können.

MAXSIze
: Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Der Standardwert ist NOLIMIT. Geben Sie einen der folgenden Werte an:

NOLimit
Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

maximale_Dateigröße
Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl im Bereich von 1 bis 999999 gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 GB ist. Verwenden Sie einen der folgenden Maßstabsfaktoren:

Tabelle 1. Maßstabsfaktor für die maximale Dateigröße

Maßstabsfaktor	Bedeutung
K	Kilobyte
M	Megabyte
G	Gigabyte
T	Terabyte

Tipp: Wenn Sie keine Maßeinheit für die maximale Dateigröße angeben, wird der Wert in Byte angegeben.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

Tabelle 2. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool

Angegebener Pool	Ergebnis
Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben.	Die Datei wird vom Server nicht gespeichert.
Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben.	Der Server speichert die Datei in dem Speicherpool, den Sie angegeben haben.

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, aktualisieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSIze=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Werden während der Datendeduplizierungsverarbeitung mehrere Dateien gesendet, betrachtet der Server die Größe des Datendeduplizierungsprozesses als Dateigröße. Wenn die Gesamtgröße aller Dateien in dem Prozess die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

MAXWriters
Gibt die maximale Anzahl E/A-Threads an, die gleichzeitig für den Speicherpool ausgeführt werden können. Geben Sie eine maximale Anzahl E/A-Threads an, um die Anzahl E/A-Threads zu steuern, die gleichzeitig in den Verzeichniscontainerspeicherpool geschrieben werden. Dieser Parameter ist wahlfrei. Verwenden Sie als Best Practice den Standardwert NOLIMIT. Sie können einen der folgenden Werte angeben:

NOLimit
Gibt an, dass keine maximale Anzahl E/A-Threads in den Speicherpool geschrieben wird.

maximale_Anzahl_Writer
Begrenzt die maximale Anzahl der E/A-Threads, die Sie verwenden können. Geben Sie eine ganze Zahl im Bereich von 1 bis 99999 an.

NEXTstgpool
Gibt den Namen eines Speicherpools mit wahlfreiem Zugriff oder eines primären sequenziellen Speicherpools an, in dem Dateien gespeichert werden, wenn der Verzeichniscontainerspeicherpool voll ist. Dieser Parameter ist wahlfrei.
Einschränkungen:

- Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
- Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
- Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
- Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.

PROTECTstgpool
Gibt den Namen des Verzeichniscontainerspeicherpools auf dem Zielserver an, in dem die Daten gesichert werden, wenn Sie den Befehl PROTECT STGPOOL für diesen Speicherpool verwenden. Dieser Parameter ist wahlfrei.

PROTECTLOCalstgpools
Gibt den Namen des Containerkopienspeicherpools auf einer lokalen Einheit an, in dem die Daten gesichert werden. Dieser Containerkopienspeicherpool ist ein lokaler Zielspeicherpool, wenn Sie den Befehl PROTECT STGPOOL verwenden. Sie können maximal zwei zu aktualisierende Containerkopienspeicherpoolnamen angeben. Mehrere Namen ohne Leerzeichen durch Kommas voneinander trennen. Die maximale Länge jedes Namens beträgt 30 Zeichen. Dieser Parameter ist wahlfrei.
Um Containerkopienspeicherpools hinzuzufügen oder zu entfernen, geben Sie die Namen der Containerkopienspeicherpools an, die eingeschlossen werden sollen. Lautet der vorhandene Containerkopienspeicherpool beispielsweise COPY1 und soll COPY2 hinzugefügt

werden, geben Sie PROTECTLOCALSTGPOOLS=COPY1,COPY2 an. Sollen alle vorhandenen Containerkopienspeicherpools entfernt werden, die dem primären Speicherpool zugeordnet sind, geben Sie eine Nullzeichenfolge ("") an. Beispiel: COPYSTGPOOLS="".

REUsedelay
Gibt die Anzahl Tage an, die verstreichen müssen, bevor alle deduplizierten Speicherbereiche aus einem Verzeichniscontainerspeicherpool entfernt werden. Dieser Parameter steuert die Dauer, die deduplizierte Speicherbereiche einem Verzeichniscontainerspeicherpool zugeordnet sind. Wenn der für den Parameter angegebene Wert abläuft, werden die deduplizierten Speicherbereiche aus dem Verzeichniscontainerspeicherpool gelöscht. Der Standardwert ist 1. Geben Sie einen der folgenden Werte an:

Tage
Geben Sie eine ganze Zahl im Bereich von 0 bis 9999 an.

1
Gibt an, dass deduplizierte Speicherbereiche nach 1 Tag aus einem Verzeichniscontainerspeicherpool gelöscht werden.

Tipp: Setzen Sie diesen Parameter auf einen Wert, der größer als der Wert ist, der als Datenbanksicherungsperiode angegeben ist, um sicherzustellen, dass Datenbereiche noch gültig sind, wenn die Datenbank auf eine andere Stufe zurückgeschrieben wird.

ENCRypt
Gibt an, ob der Server Clientdaten verschlüsselt, bevor der Server die Daten in den Speicherpool schreibt. Sie können die folgenden Werte angeben:

Yes
Gibt an, dass Clientdaten vom Server verschlüsselt werden.

No
Gibt an, dass Clientdaten nicht vom Server verschlüsselt werden.

COMPRession
Gibt an, ob Daten in dem Speicherpool komprimiert werden. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

No
Gibt an, dass Daten in dem Speicherpool nicht komprimiert werden.

Yes
Gibt an, dass Daten in dem Speicherpool komprimiert werden. Dies ist der Standardwert.

Beispiel: Einen Speicherpool aktualisieren, um eine maximale Anzahl Datensitzungen anzugeben

Einen Speicherpool mit dem Namen STGPOOL1 aktualisieren und ein Maximum von 10 Datensitzungen angeben.

```
update stgpool stgpool1 maxwriters=10
```

Beispiel: Einen Speicherpool aktualisieren, um die maximale Größe anzugeben

Einen Speicherpool mit dem Namen STGPOOL2 aktualisieren. Der Speicherpool gibt als maximale Dateigröße 100 Megabyte an, die der Server im Speicherpool speichern kann.

```
update stgpool stgpool2 maxsize=100M
```

Beispiel: Die Beschreibung eines Speicherpools aktualisieren

Einen Speicherpool mit dem Namen STGPOOL3 aktualisieren. Die vorhandene Beschreibung aus dem Speicherpool entfernen.

```
update stgpool stgpool3 description=""
```

Tabelle 3. Zugehörige Befehle für UPDATE STGPOOL

Befehl	Beschreibung
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DEFINE STGPOOLDIRECTORY	Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.
QUERY CONTAINER	Zeigt Informationen zu einem Container an.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REPAIR STGPOOL	Repariert einen Verzeichniscontainerspeicherpool.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeUPDATE STGPOOLDIRECTORY	Ändert die Attribute eines Speicherpoolverzeichnisses.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

UPDATE STGPOOL (Containerkopienspeicherpool aktualisieren)

Mit diesem Befehl kann ein Containerkopienspeicherpool aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

Syntax

```
>>-UPDate STGpool--Poolname--+----------------------+---------->
                            '-MAXSCRatch--=--Anzahl-'

>--+------------------------------+---------------------------->
   '-DESCription--=--Beschreibung-'

>--+----------------------------+------------------------------>
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                '-UNAVailable-'

>--+--------------------------+--+--------------------+------->
   '-PROTECTPRocess--=--Anzahl-'  '-RECLaim--=--Prozent-'

>--+-------------------------------------------+---------------->
   '-RECLAIMLIMit--=--+-NOLimit--------------+-'
                      '-Datenträgergrenzwert-'

>--+---------------------+-------------------------------------><
   '-REUsedelay--=--Tage-'
```

Parameter

Poolname (Erforderlich)
: Gibt den Namen des Speicherpools an, der aktualisiert werden soll.

MAXSCRatch
: Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Sie können eine ganze Zahl im Bereich von 0 bis 100000000 angeben. Wenn der Server Arbeitsdatenträger nach Bedarf anfordern kann, müssen Sie nicht jeden zu verwendenden Datenträger definieren.

  Mit dem Wert dieses Parameters wird die Gesamtzahl der im Speicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Speicherpools geschätzt.

DESCription
: Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("") angeben.

ACCess
: Gibt an, wie Serverprozesse, wie z. B. Speicherpoolschutz und Reparatur, auf Daten in dem Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  READWrite
  : Gibt an, dass der Server Lese- und Schreibzugriff auf Datenträger in dem Speicherpool hat.

  READOnly
  : Gibt an, dass der Server nur Lesezugriff auf Datenträger in dem Speicherpool hat. Der Server kann Daten in dem Speicherpool verwenden, um Bereiche in Verzeichniscontainerspeicherpools zurückzuschreiben. Operationen, mit denen Daten in den Containerkopienspeicherpool geschrieben werden, sind nicht zulässig.

  UNAVailable
  : Gibt an, dass der Server nicht auf Daten zugreifen kann, die auf Datenträgern im Speicherpool gespeichert sind.

PROTECTPRocess
: Gibt die maximale Anzahl paralleler Prozesse an, die verwendet werden, wenn Sie den Befehl PROTECT STGPOOL ausgeben, um Daten aus einem Verzeichniscontainerspeicherpool in diesen Pool zu kopieren. Dieser Parameter ist wahlfrei. Geben Sie einen Wert im Bereich von 1 bis 20 ein.

  Die Zeit, die für die Ausführung der Kopieroperation erforderlich ist, kann durch die Verwendung mehrerer Prozesse verringert werden. Sind mehrere Prozesse aktiv, müssen jedoch in einigen Fällen ein oder mehrere Prozesse auf die Verwendung eines Datenträgers warten, der bereits von einem anderen Prozess verwendet wird.

  Berücksichtigen Sie bei der Festlegung dieses Werts die Anzahl der logischen und physischen Laufwerke, die dieser Operation zugeordnet werden können. Für den Zugriff auf einen Banddatenträger verwendet der Server einen Mountpunkt und ein Laufwerk. Die Anzahl

verfügbarer Mountpunkte und Laufwerke ist von dem Mountlimit der Einheitenklasse für den Speicherpool und von anderen Server- und Systemaktivitäten abhängig.

Wenn Sie die Voranzeigeoption im Befehl PROTECT STGPOOL verwenden, wird nur ein Prozess verwendet und es werden keine Mountpunkte oder Laufwerke benötigt.

RECLaim
: Gibt an, wann ein Datenträger für die Konsolidierung und Wiederverwendung auswählbar ist. Geben Sie die Auswählbarkeit als Prozentsatz des Speicherbereichs eines Datenträgers an, der von Bereichen belegt ist, die nicht mehr im zugeordneten Verzeichniscontainerspeicherpool gespeichert werden. Bei der Konsolidierung werden alle Bereiche, die noch im zugeordneten Verzeichniscontainerspeicherpool gespeichert werden, von auswählbaren Datenträgern auf andere Datenträger versetzt. Die Konsolidierung erfolgt nur, wenn mit einem Befehl PROTECT STGPOOL Daten in diesem Speicherpool gespeichert werden.

  Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 1 bis 100 angeben. Der Wert 100 gibt an, dass keine Datenträger in diesem Speicherpool konsolidiert werden.

  Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

  Wird der Wert für 'Reclaim' auf 50 Prozent oder höher gesetzt, belegen Daten, die von zwei konsolidierten Datenträgern versetzt werden, maximal das Äquivalent eines neuen Datenträgers.

  Gehen Sie mit Vorsicht vor, wenn Sie die Konsolidierung mit Containerkopienspeicherpools verwenden, die über ausgelagerte Datenträger verfügen. Wenn ein ausgelagerter Datenträger für die Konsolidierung auswählbar wird, werden die Bereiche auf dem Datenträger vom Server an den Standort vor Ort zurückversetzt. Wenn vor Ort ein Katastrophenfall eintritt, kann der Server Bereiche vom ausgelagerten Datenträger anfordern, wenn die zurückgeschriebene Datenbank auf Bereiche auf dem ausgelagerten Datenträger verweist. Stellen Sie daher zu Zwecken der Wiederherstellung nach einem Katastrophenfall sicher, dass Sie die Ausführung von Datenbanksicherungen planen, nachdem Speicherpoolschutzzeitpläne und DRM-Versetzungszeitpläne ausgeführt wurden, und stellen Sie sicher, dass alle Datenbanksicherungsdatenträger zusammen mit den DRM-Datenträgern ausgelagert werden.

  Tipp: Definieren Sie verschiedene Konsolidierungswerte für Containerkopienspeicherpools an einem anderen Standort und Containerkopienspeicherpools vor Ort. Da Containerkopienspeicherpools deduplizierte Daten speichern, sind die Datenbereiche auf mehrere Banddatenträger verteilt. Wenn Sie einen Schwellenwert für die Konsolidierung für eine Kopie an einem anderen Standort auswählen, beachten Sie sorgfältig die Anzahl verfügbarer Mountpunkte und die Anzahl Banddatenträger, die abgerufen werden müssen, wenn ein Katastrophenfall eintritt. Wird ein höherer Schwellenwert definiert, bedeutet dies, dass Sie mehr Datenträger abrufen müssen als bei einem niedrigeren Konsolidierungswert. Bei Verwendung eines niedrigeren Schwellenwerts wird die Anzahl der Mountpunkte reduziert, die in einem Katastrophenfall erforderlich sind. Die bevorzugte Methode ist die Angabe des Konsolidierungswerts 60 für Kopien an einem anderen Standort. Für Kopien vor Ort liegt er im Bereich von 90 bis 100.

RECLAIMLIMit
: Gibt die maximale Anzahl von Datenträgern an, die der Server konsolidiert, wenn Sie den Befehl PROTECT STGPOOL ausgeben und die Option RECLAIM=YESLIMITED oder RECLAIM=ONLYLIMITED angeben. Dieser Parameter ist nur für Containerkopienspeicherpools gültig. Dieser Parameter ist wahlfrei. Sie können einen der folgenden Werte angeben:

  NOLimit
  : Gibt an, dass alle Datenträger im Containerkopienspeicherpool für die Konsolidierung verarbeitet werden.

  Datenträgergrenzwert
  : Gibt die maximale Anzahl der Datenträger im Containerkopienspeicherpool an, die konsolidiert werden. Der von Ihnen angegebene Wert bestimmt, wie viele neue Arbeitsbänder nach Abschluss der Konsolidierungsverarbeitung verfügbar sind. Sie können eine Zahl im Bereich von 1 bis 100000 angeben.

REUsedelay
: Gibt die Anzahl Tage an, die nach dem Löschen aller Bereiche von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerstatus versetzt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl im Bereich von 0 bis 9999 angeben. Der Wert 0 bedeutet, dass ein Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerstatus versetzt werden kann, sobald alle Bereiche auf dem Datenträger gelöscht wurden.
  Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Bereiche im Speicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Wenn Sie Disaster Recovery Manager verwenden, muss die für diesen Parameter angegebene Anzahl Tage mit der für den Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl übereinstimmen.

Beispiel: Einen Containerkopienspeicherpool aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern

Den Speicherpool mit dem Namen CONTAINER1_COPY2 aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern.

```
update stgpool container1_copy2 reusedelay=30
```

Beispiel: Einen Containerkopienspeicherpool aktualisieren, um die Anzahl der konsolidierten Banddatenträger auf 10 zu begrenzen

Den Speicherpool mit dem Namen CONTAINER1_COPY2 aktualisieren, um den Konsolidierungsgrenzwert in 10 Datenträger zu ändern.

```
update stgpool container1_copy2 reclaimlimit=10
```

Tabelle 1. Zugehörige Befehle für UPDATE STGPOOL (Containerkopienspeicherpool aktualisieren)

Befehl	Beschreibung
DEFINE STGPOOL (Containerkopie)	Definiert einen Containerkopienspeicherpool, in dem Kopien von Daten aus einem Verzeichniscontainerspeicherpool gespeichert werden.
PROTECT STGPOOL	Schützt einen Verzeichniscontainerspeicherpool.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.
REPAIR STGPOOL	Repariert einen Verzeichniscontainerspeicherpool.
UPDATE STGPOOL (Verzeichniscontainer)	Aktualisiert einen Verzeichniscontainerspeicherpool.

UPDATE STGPOOL (Primären Speicherpool mit wahlfreiem Zugriff aktualisieren)

Mit diesem Befehl kann ein Speicherpool mit wahlfreiem Zugriff aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

Syntax

```
   |                    V                                  | |
   '-ACTIVEDATApools--=----Name_des_Pools_für_aktive_Daten-+-'

   .-SHRED--=--0----------------------.
>--+-----------------------------------+----------------------><
   '-SHRED--=--Anzahl_Überschreibungen-'
```

Parameter

Poolname (Erforderlich)
: Gibt den Speicherpool an, der aktualisiert werden soll. Dieser Parameter ist erforderlich.

DESCription
: Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("") angeben.

ACCess
: Gibt an, wie Clientknoten und Serverprozesse (wie Umlagerung und Wiederherstellung) auf Dateien im Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

  READWrite
  : Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien haben, die auf Datenträgern in dem Speicherpool gespeichert sind.

  READOnly
  : Gibt an, dass Clientknoten Dateien auf den Datenträgern im Speicherpool nur lesen können.

    Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

    Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *readonly (schreibgeschützt)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

  UNAVailable
  : Gibt an, dass Clientknoten nicht auf Dateien, die auf Datenträgern im Speicherpool gespeichert sind, zugreifen können.

    Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Außerdem können sie Dateien aus diesem Speicherpool in einen anderen Speicherpool versetzen oder kopieren. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

    Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *unavailable (nicht verfügbar)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

MAXSIze
: Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

  NOLimit
  : Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

  maximale_Dateigröße
  : Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl zwischen 1 und 999999 Terabyte gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 Gigabyte ist. Maßstabsfaktoren sind:

Maßstabsfaktor	Bedeutung
K	Kilobyte
M	Megabyte
G	Gigabyte
T	Terabyte

  Der Client schätzt die Größe der Dateien, die an den Server gesendet werden. Die Schätzung des Clients wird verwendet und nicht das tatsächliche Datenvolumen, das an den Server gesendet wird. Clientoptionen, wie z. B. Deduplizierung, Komprimierung und Verschlüsselung, können zur Folge haben, dass das tatsächliche Datenvolumen, das an den Server gesendet wird, größer oder kleiner als die Größenschätzung ist. Beispielsweise kann eine komprimierte Datei kleiner als die Schätzung sein, sodass weniger Daten als der Schätzwert gesendet werden. Des Weiteren kann eine Binärdatei nach der Komprimierungsverarbeitung größer sein, sodass mehr Daten als der Schätzwert gesendet werden.

  Die folgende Tabelle enthält Informationen zur Speicherposition einer Datei, wenn ihre Größe den Wert des Parameters MAXSIZE überschreitet.

Tabelle 1. Speicherposition einer Datei gemäß der Dateigröße und dem angegebenen Pool

Dateigröße	Angegebener Pool	Ergebnis
Überschreitet die maximale Größe	Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben	Die Datei wird vom Server nicht gespeichert
	Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben	Der Server speichert die Datei im nächsten Speicherpool, der die Dateigröße akzeptiert

Wenn Sie den Parameter für den nächsten Speicherpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat. Verfügt mindestens ein Pool über keinen Grenzwert hinsichtlich der Größe, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Bei mehreren Dateien, die in einer einzelnen Transaktion gesendet werden, betrachtet der Server die Größe der Transaktion als Dateigröße. Wenn die Gesamtgröße aller Dateien in der Transaktion die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

CRCData
: Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

  Yes
  : Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da mehr Aufwand erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

  No
  : Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

NEXTstgpool
: Gibt einen primären Speicherpool an, in den Dateien umgelagert werden. Dieser Parameter ist wahlfrei.

  Soll ein bestehender Speicherpool aus der Speicherhierarchie entfernt werden, ist eine Nullzeichenfolge ("") für diesen Wert anzugeben.

  Wird kein nächster Speicherpool angegeben, gilt Folgendes:

  - Der Server kann keine Dateien aus diesem Speicherpool umlagern
  - Der Server kann keine Dateien, die die maximale Größe für diesen Speicherpool überschreiten, in einem anderen Speicherpool speichern

  Einschränkungen:

  - Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
  - Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
  - Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
  - Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.

HIghmig
: Gibt an, dass der Server die Umlagerung für diesen Speicherpool startet, wenn der Datenumfang in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100 angeben.

  Wenn der Speicherpool die obere Umlagerungsschwelle überschreitet, kann der Server die Umlagerung von Dateien in den nächsten Speicherpool (wie im Parameter NEXTSTGPOOL definiert) nach Knotennamen starten. Bei Angabe von HIGHMIG=100 wird die Umlagerung für diesen Speicherpool verhindert.

LOwmig
: Gibt an, dass der Server die Umlagerung für diesen Speicherpool stoppt, wenn der Datenumfang in dem Pool diesen Prozentsatz der geschätzten Kapazität des Pools erreicht. Sie können eine ganze Zahl von 0 bis 99 für diesen optionalen Parameter angeben.

  Wenn die Umlagerung nach Knoten oder Dateibereich erfolgt (abhängig von der Kollokation), kann der Wert für den Speicherpool unter den für diesen Parameter angegebenen Wert fallen. Um den Speicherpool zu leeren, definieren Sie LOWMIG=0.

CAChe
: Gibt an, ob der Umlagerungsprozess eine Cachekopie einer Datei in diesem Speicherpool zurücklässt, nachdem die Datei in den nächsten Speicherpool umgelagert wurde. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

  Yes
  : Caching ist aktiviert.

  No
  : Caching ist inaktiviert.

Die Verwendung von Cache kann die Abrufbarkeit von Dateien verbessern, kann jedoch die Leistung anderer Prozesse negativ beeinflussen.

MIGPRocess
Gibt die Anzahl Prozesse an, die zum Umlagern von Dateien aus diesem Speicherpool verwendet werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 999 angeben.

Während der Umlagerung werden diese Prozesse parallel ausgeführt, um die Umlagerungsgeschwindigkeit zu verbessern.

Tipps:

- Die Anzahl der Umlagerungsprozesse ist von den folgenden Einstellungen abhängig:
  - Einstellung des Parameters MIGPROCESS
  - Kollokationseinstellung des nächsten Pools
  - Anzahl der Knoten oder Anzahl der Kollokationsgruppen mit Daten in dem Speicherpool, der umgelagert wird

  Für dieses Beispiel wird angenommen, dass `MIGPROCESS =6` angegeben und der Parameter COLLOCATE für den nächsten Pool auf NODE gesetzt ist, aber nur zwei Knoten mit Daten in dem Speicherpool vorhanden sind. Die Umlagerungsverarbeitung besteht nur aus zwei, nicht sechs Prozessen. Wird der Parameter COLLOCATE auf GROUP gesetzt und befinden sich beide Knoten in derselben Gruppe, besteht die Umlagerungsverarbeitung nur aus einem Prozess. Wird der Parameter COLLOCATE auf NO oder FILESPACE gesetzt und hat jeder Knoten zwei Dateibereiche mit Sicherungsdaten, besteht die Umlagerungsverarbeitung nur aus vier Prozessen.
- Beachten Sie bei der Angabe dieses Parameters, ob die Funktion für simultanes Schreiben für die Serverdatenumlagerung aktiviert ist. Jeder Umlagerungsprozess erfordert einen Mountpunkt und ein Laufwerk für jeden Kopienspeicherpool und Pool für aktive Daten, der für den Zielspeicherpool definiert ist.

MIGDelay
Gibt die Mindestanzahl Tage an, die eine Datei in einem Speicherpool verbleiben muss, bevor sie für die Umlagerung ausgewählt werden kann. Um einen Wert zu berechnen, der mit dem angegebenen Wert für MIGDELAY verglichen wird, zählt der Server:

- Die Anzahl der Tage, die die Datei im Speicherpool war
- Die Anzahl der Tage (falls zutreffend), seit die Datei von einem Client abgerufen wurde

Der kleinere der beiden Werte wird mit dem angegebenen Wert für MIGDELAY verglichen. Beispiel: Sind alle folgenden Bedingungen wahr, wird eine Datei nicht umgelagert:

- Eine Datei war fünf Tage in einem Speicherpool.
- Auf die Datei wurde innerhalb der letzten drei Tage von einem Client zugegriffen.
- Der für den Parameter MIGDELAY angegebene Wert beträgt vier Tage.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Standardwert 0 gibt an, dass die Umlagerung nicht verzögert werden soll.

Soll der Server die Anzahl der Tage ab dem Tag zählen, an dem eine Datei gespeichert wurde, und nicht ab dem Tag, an dem sie abgerufen wurde, die Serveroption NORETRIEVEDATE verwenden.

MIGContinue
Gibt an, ob der Server Dateien umlagern darf, die der Verzögerungszeit für die Umlagerung nicht entsprechen. Dieser Parameter ist wahlfrei.

Da angegeben werden kann, dass Dateien eine Mindestanzahl Tage in dem Speicherpool verbleiben müssen, kann der Server alle auswählbaren Dateien in den nächsten Speicherpool umlagern, obwohl sie dem Wert für die untere Umlagerungsschwelle nicht entsprechen. Mit diesem Parameter kann angegeben werden, ob der Server den Umlagerungsprozess fortsetzen darf, indem Dateien umgelagert werden, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sie können einen der folgenden Werte angeben:

Yes
Muss die untere Umlagerungsschwelle eingehalten werden, gibt dieser Wert an, dass der Server mit der Umlagerung von Dateien fortfährt, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sind mehrere Umlagerungsprozesse für den Speicherpool zulässig, werden einige Dateien, die der Verzögerungszeit für die Umlagerung nicht entsprechen, unter Umständen unnötigerweise umgelagert. Während ein Prozess Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte ein zweiter Prozess mit der Umlagerung von Dateien beginnen, die der Verzögerungszeit für die Umlagerung nicht entsprechen, um die untere Umlagerungsschwelle einzuhalten. Der erste Prozess, der noch Dateien umlagert, die der Verzögerungszeit für die Umlagerung entsprechen, könnte selbst die Einhaltung der unteren Umlagerungsschwelle bewirkt haben.

No
Gibt an, dass der Server die Umlagerung stoppt, wenn keine auswählbaren Dateien mehr für die Umlagerung verfügbar sind; dies gilt auch vor Erreichen der unteren Umlagerungsschwelle. Der Server lagert nur Dateien um, die der Verzögerungszeit für die Umlagerung entsprechen.

AUTOCopy

Gibt an, wann IBM Spectrum Protect Operationen für gleichzeitiges Schreiben in Kopienspeicherpools und Pools für aktive Daten ausführt. Dieser Parameter betrifft die folgenden Operationen:

- Clientspeichersitzungen
- Serverimportprozesse
- Serverdatenumlagerungsprozesse

Tritt ein Fehler auf, wenn Daten während eines Umlagerungsprozesses gleichzeitig in einen Kopienspeicherpool oder einen Pool für aktive Daten geschrieben werden, stoppt der Server das Schreiben in die fehlerhaften Speicherpools für den Rest des Prozesses. Der Server speichert jedoch weiterhin Dateien in dem primären Speicherpool und in allen verbleibenden Kopienspeicherpools oder Pools für aktive Daten. Diese Pools bleiben für die Dauer des Umlagerungsprozesses aktiv. Kopienspeicherpools werden mit dem Parameter COPYSTGPOOLS angegeben. Pools für aktive Daten werden mit dem Parameter ACTIVEDATAPOOLS angegeben.

Sie können einen der folgenden Werte angeben:

None
: Gibt an, dass die Funktion für simultanes Schreiben inaktiviert ist.

CLient
: Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen oder Serverimportprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverimportprozessen werden Daten nur gleichzeitig in Kopienspeicherpools geschrieben. Daten werden während der Ausführung von Serverimportprozessen nicht in Pools für aktive Daten geschrieben.

MIGRation
: Gibt an, dass Daten nur während der Umlagerung in diesen Speicherpool gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverdatenumlagerungsprozessen werden Daten in Kopienspeicherpools und Pools für aktive Daten nur dann gleichzeitig geschrieben, wenn die Daten in diesen Pools nicht vorhanden sind. Knoten, deren Daten umgelagert werden, müssen sich in einer Domäne befinden, die einem Pool für aktive Daten zugeordnet ist. Befinden sich die Knoten nicht in einer Domäne, die einem Pool für aktive Daten zugeordnet ist, können die Daten nicht in den Pool geschrieben werden.

All
: Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen oder Serverdatenumlagerungsprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Mit diesem Wert wird sichergestellt, dass Daten immer dann gleichzeitig geschrieben werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

COPYSTGpools
: Gibt die Namen von Kopienspeicherpools an, in die der Server gleichzeitig Daten schreibt. Sie können maximal drei Kopienpoolnamen angeben, die durch Kommas voneinander getrennt werden müssen. Leerzeichen zwischen den Namen der Kopienpools sind nicht zulässig. Um einen oder mehrere Kopienspeicherpools hinzuzufügen oder zu entfernen, geben Sie den oder die Poolnamen an, der bzw. die in der aktualisierten Liste enthalten sein soll(en). Enthält die vorhandene Kopienpoolliste beispielsweise COPY1 und COPY2 und soll COPY3 hinzugefügt werden, geben Sie COPYSTGPOOLS=COPY1,COPY2,COPY3 an. Um alle vorhandenen Kopienspeicherpools zu entfernen, die dem primären Speicherpool zugeordnet sind, geben Sie eine Nullzeichenfolge ("") für den Wert an (beispielsweise COPYSTGPOOLS="").

  Wenn Sie einen Wert für den Parameter COPYSTGPOOLS angeben, können Sie auch einen Wert für den Parameter COPYCONTINUE angeben. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

  Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

  Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Kopienspeicherpools und den Wert für COPYCONTINUE aus dem primären Speicherpool. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

  Der Server kann bei den folgenden Operationen Daten gleichzeitig in Kopienspeicherpools schreiben:

  - Sicherungs- und Archivierungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder Anwendungsclients, die die IBM Spectrum Protect-API verwenden
  - Umlagerungsoperationen durch IBM Spectrum Protect for Space Management-Clients
  - Importoperationen, die das Kopieren von exportierten Dateidaten von externen Datenträgern in einen primären Speicherpool einbeziehen, der einer Kopienspeicherpoolliste zugeordnet ist

  Einschränkungen: Die Funktion für simultanes Schreiben wird für die folgenden Speicheroperationen nicht unterstützt:

  - Wenn die Operation die LAN-unabhängige Datenversetzung verwendet. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
  - NAS-Sicherungsoperationen. Sind für den primären Speicherpool, der in DESTINATION oder TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Kopienspeicherpools definiert, werden
    - die Kopienspeicherpools ignoriert.
    - die Daten nur im primären Speicherpool gespeichert.

Achtung: Die mit dem Parameter COPYSTGPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl BACKUP STGPOOL ersetzen. Wird der Parameter COPYSTGPOOLS verwendet, verwenden Sie weiterhin den Befehl BACKUP STGPOOL, um sicherzustellen, dass die Kopienspeicherpools vollständige Kopien des primären Speicherpools sind. Es gibt Fälle, in denen eine Kopie möglicherweise nicht erstellt wird. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

COPYContinue

Gibt an, wie der Server auf einen Fehler beim Schreiben in einen der Kopienspeicherpools reagiert, die im Parameter COPYSTGPOOLS aufgelistet sind. Dieser Parameter ist wahlfrei. Wenn Sie den Parameter COPYCONTINUE angeben, muss entweder eine COPYSTGPOOLS-Liste vorhanden sein oder der Parameter COPYSTGPOOLS muss ebenfalls angegeben werden.
Sie können die folgenden Werte angeben:

Yes

Ist der Parameter COPYCONTINUE auf YES gesetzt, stoppt der Server das Schreiben in die fehlerhaften Kopienpools für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Kopienpools fort. Die Liste der Kopienspeicherpools ist nur für die Dauer der Clientsitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.

No

Ist der Parameter COPYCONTINUE auf NO gesetzt, wird die aktuelle Transaktion vom Server nicht ausgeführt und die Speicheroperation nicht fortgesetzt.

Einschränkungen:

- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf Pools für aktive Daten. Tritt für einen der Pools für aktive Daten ein Schreibfehler auf, stoppt der Server das Schreiben in den fehlerhaften Pool für aktive Daten für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Pools für aktive Daten und Kopienspeicherpools fort. Die Liste der Pools für aktive Daten ist nur für die Dauer der Sitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Ausführung eines Serverimportprozesses. Werden Daten gleichzeitig geschrieben und tritt für den primären Speicherpool oder einen Kopienspeicherpool ein Schreibfehler auf, schlägt der Serverimportprozess fehl.
- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Serverdatenumlagerung. Werden Daten gleichzeitig geschrieben und tritt für einen Kopienspeicherpool oder Pool für aktive Daten ein Schreibfehler auf, wird der fehlerhafte Speicherpool entfernt und der Datenumlagerungsprozess wird fortgesetzt. Bei Schreibfehlern für den primären Speicherpool schlägt der Umlagerungsprozess fehl.

ACTIVEDATApools

Gibt die Namen der Pools für aktive Daten an, in die der Server während einer Clientsicherungsoperation gleichzeitig Daten schreibt. Der Parameter ACTIVEDATAPOOLS ist optional. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Pools für aktive Daten aus dem Zielspeicherpool, der in der Kopiengruppe angegeben ist. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann nur während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients, die die IBM Spectrum Protect-API verwenden, Daten gleichzeitig in Pools für aktive Daten schreiben.
Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat "NATIVE" oder "NONBLOCK" verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
   - NETAPPDUMP
   - CELERRADUMP
   - NDMPDUMP
2. Das simultane Schreiben in Pools für aktive Daten wird nicht unterstützt, wenn die LAN-unabhängige Datenversetzung verwendet wird. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch berücksichtigt.
3. Die Funktion für simultanes Schreiben wird nicht unterstützt, wenn eine NAS-Sicherungsoperation eine Inhaltsverzeichnisdatei schreibt. Sind für den primären Speicherpool, der in TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Pools für aktive Daten definiert, werden
   - die Pools für aktive Daten ignoriert.
   - die Daten nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.
5. Daten, die importiert werden, werden nicht in Pools für aktive Daten gespeichert. Verwenden Sie nach einer Importoperation den Befehl COPY ACTIVEDATA, um die importierten Daten in einem Pool für aktive Daten zu speichern.

Achtung: Die mit dem Parameter ACTIVEDATAPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl COPY ACTIVEDATA ersetzen. Wird der Parameter ACTIVEDATAPOOLS verwendet, verwenden Sie den Befehl COPY ACTIVEDATA, um sicherzustellen, dass die Pools für aktive Daten alle aktiven Daten des primären Speicherpools enthalten.

SHRED

Gibt an, ob Daten beim Löschen physisch überschrieben werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 10 angeben.

Wird der Wert Null angegeben, löscht der Server die Daten aus der Datenbank. Der Speicher, in dem die Daten gespeichert waren, wird jedoch nicht überschrieben, und die Daten sind weiterhin im Speicher vorhanden, bis dieser Speicher für andere Daten wiederverwendet wird. Möglicherweise können die Daten nach dem Löschen erkannt und wiederhergestellt werden. Die Änderung des Werts (beispielsweise das Zurücksetzen auf 0) hat keinen Einfluss auf Daten, die gelöscht wurden und gegenwärtig darauf warten, überschrieben zu werden.

Wenn Sie einen Wert größer als 0 angeben, löscht der Server die Daten sowohl logisch als auch physisch. Der Server überschreibt den Speicher, in dem die Daten gespeichert waren, so oft wie angegeben wurde. Durch das Überschreiben wird es schwieriger, die Daten zu erkennen und wiederherzustellen, nachdem sie gelöscht wurden.

Um sicherzustellen, dass alle Kopien der Daten geschreddert werden, geben Sie einen SHRED-Wert größer als Null für den im Parameter NEXTSTGPOOL angegebenen Speicherpool an. Geben Sie nicht COPYSTGPOOLS oder ACTIVEDATAPOOLS an. Durch die Angabe relativ hoher Werte für die Anzahl Überschreibungen wird im Allgemeinen die Sicherheitsstufe erhöht, aber sie kann umgekehrt die Leistung beeinflussen.

Das Überschreiben gelöschter Daten wird asynchron ausgeführt, nachdem die Löschoperation abgeschlossen ist. Daher bleibt der durch die gelöschten Daten belegte Speicherbereich für einige Zeit belegt. Der Speicherbereich ist nicht als freier Speicherbereich für neue Daten verfügbar.

Ein SHRED-Wert größer als null kann nicht verwendet werden, wenn der Parameter CACHE den Wert YES hat. Soll das Schreddern für einen vorhandenen Speicherpool aktiviert werden, für den das Caching bereits aktiviert ist, müssen Sie den Wert des Parameters CACHE in NO ändern. Vorhandene zwischengespeicherte Dateien verbleiben im Speicher, so dass nachfolgende Abrufanforderungen schnell erfüllt werden können. Wird Speicherbereich zum Speichern neuer Daten benötigt, werden die vorhandenen zwischengespeicherten Dateien gelöscht, so dass der von ihnen belegte Speicherbereich für die neuen Daten verwendet werden kann. Die vorhandenen zwischengespeicherten Dateien werden nach dem Löschen nicht geschreddert.
Wichtig: Nachdem eine Exportoperation die Identifizierung von Dateien für den Export beendet hat, werden alle Änderungen des Werts SHRED für den Speicherpool ignoriert. Eine Exportoperation, die ausgesetzt ist, behält während der gesamten Operation den ursprünglichen SHRED-Wert. Möglicherweise möchten Sie Ihre Exportoperation abbrechen, wenn Änderungen des Werts SHRED für den Speicherpool die Operation gefährden. Sie können den Exportbefehl nach einer erforderlichen Bereinigung erneut ausgeben.

Beispiel: Einen Speicherpool mit wahlfreiem Zugriff aktualisieren, um das Caching zu erlauben

Den Speicherpool mit wahlfreiem Zugriff mit dem Namen BACKUPPOOL aktualisieren, um Caching zu erlauben, wenn der Server Dateien in den nächsten Speicherpool umlagert.

```
update stgpool backuppool cache=yes
```

UPDATE STGPOOL (Primären Speicherpool mit sequenziellem Zugriff aktualisieren)

Mit diesem Befehl kann ein primärer Speicherpool mit sequenziellem Zugriff aktualisiert werden.

Einschränkungen:

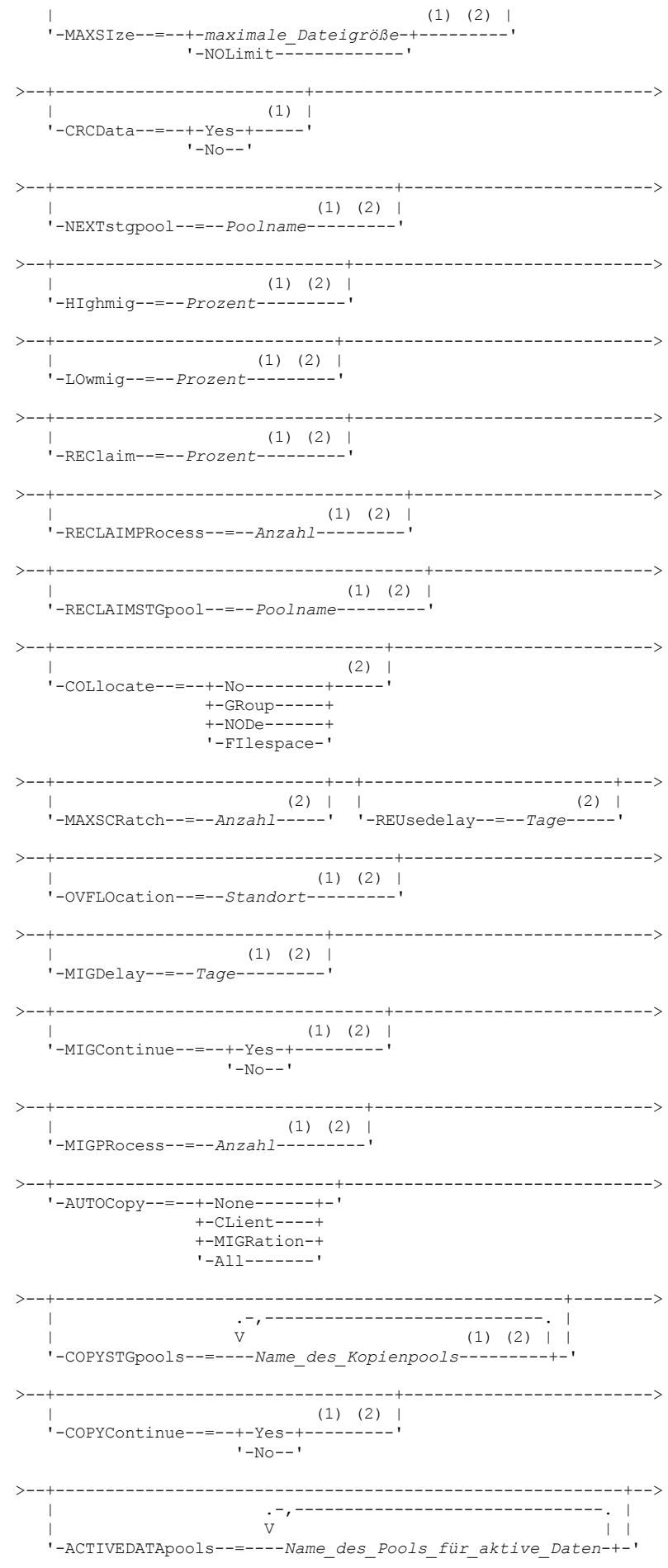
1. Sie können diesen Befehl nicht verwenden, um das Datenformat für den Speicherpool zu ändern.
2. Hat DATAFORMAT den Wert NETAPPDUMP, CELERRADUMP oder NDMPDUMP, können Sie nur die folgenden Attribute ändern:
   - DESCRIPTION
   - ACCESS
   - COLLOCATE
   - MAXSCRATCH
   - REUSEDELAY

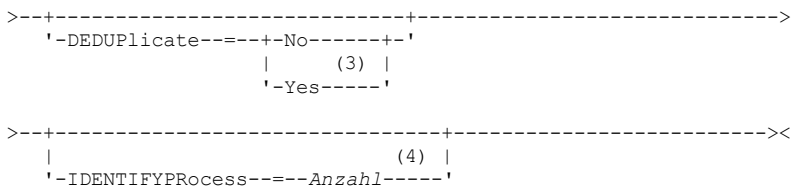
Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

Syntax

```
>>-UPDate STGpool--Poolname--+------------------------------+--->
                             '-DESCription--=--Beschreibung-'

>--+---------------------------+-------------------------------->
   '-ACCess--=--+-READWrite---+-'
                +-READOnly----+
                '-UNAVailable-'

>--+-------------------------------------------+-------------->
```


(1) (2)
'-MAXSIze--=--+-maximale_Dateigröße-+---------'
'-NOLimit-------------'
(1)
'-CRCData--=--+-Yes-+-----'
'-No--'
(1) (2)
'-NEXTstgpool--=--Poolname---------'
(1) (2)
'-HIghmig--=--Prozent---------'
(1) (2)
'-LOwmig--=--Prozent---------'
(1) (2)
'-RECIaim--=--Prozent---------'
(1) (2)
'-RECLAIMPRocess--=--Anzahl---------'
(1) (2)
'-RECLAIMSTGpool--=--Poolname---------'
(2)
'-COLlocate--=--+-No--------+-----'
+-GRoup-----+
+-NODe------+
'-FIlespace-'
(2)
'-MAXSCRatch--=--Anzahl-----'
(2)
'-REUsedelay--=--Tage-----'
(1) (2)
'-OVFLOcation--=--Standort---------'
(1) (2)
'-MIGDelay--=--Tage---------'
(1) (2)
'-MIGContinue--=--+-Yes-+---------'
'-No--'
(1) (2)
'-MIGPRocess--=--Anzahl---------'
'-AUTOCopy--=--+-None------+-'
+-CLient----+
+-MIGRation-+
'-All-------'
.-,-----------------------------.
V (1) (2)
'-COPYSTGpools--=----Name_des_Kopienpools---------+-'
(1) (2)
'-COPYContinue--=--+-Yes-+---------'
'-No--'
.-,-------------------------------.
V
'-ACTIVEDATApools--=----Name_des_Pools_für_aktive_Daten-+-'



Anmerkungen:

1. Dieser Parameter ist für Speicherpools, die das Datenformat NETAPPDUMP, CELERRADUMP oder NDMPDUMP verwenden, nicht verfügbar.
2. Dieser Parameter ist für CENTERA-Speicherpools nicht verfügbar.
3. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
4. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

Parameter

Poolname (Erforderlich)
Gibt den Namen des Speicherpools an, der aktualisiert werden soll.

DESCription
Gibt eine Beschreibung des Speicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("") angeben.

ACCess
Gibt an, wie Clientknoten und Serverprozesse (wie Umlagerung und Wiederherstellung) auf Dateien im Speicherpool zugreifen können. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

READWrite
Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien haben, die auf Datenträgern in dem Speicherpool gespeichert sind.

READOnly
Gibt an, dass Clientknoten Dateien auf den Datenträgern im Speicherpool nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *readonly (schreibgeschützt)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

UNAVailable
Gibt an, dass Clientknoten nicht auf Dateien, die auf Datenträgern im Speicherpool gespeichert sind, zugreifen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Außerdem können sie Dateien aus diesem Speicherpool in einen anderen Speicherpool versetzen oder kopieren. Für die Datenträger in dem Speicherpool sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig.

Wenn dieser Speicherpool als untergeordneter Speicherpool angegeben (mit dem Parameter NEXTSTGPOOL) und als *unavailable (nicht verfügbar)* definiert wurde, wird der Speicherpool übersprungen, wenn Serverprozesse versuchen, Dateien in den Speicherpool zu schreiben.

MAXSIze
Gibt die maximale Größe einer physischen Datei an, die der Server in dem Speicherpool speichern kann. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

NOLimit
Gibt an, dass für die im Speicherpool gespeicherten physischen Dateien keine Größenbeschränkung besteht.

maximale_Dateigröße
Begrenzt die maximale Größe für physische Dateien. Geben Sie eine ganze Zahl zwischen 1 und 999999 Terabyte gefolgt von einem Maßstabsfaktor an. MAXSIZE=5G gibt z. B. an, dass die maximale Dateigröße für diesen Speicherpool 5 Gigabyte ist. Maßstabsfaktoren sind:

Maßstabsfaktor	Bedeutung
K	Kilobyte
M	Megabyte
G	Gigabyte
T	Terabyte

Der Client schätzt die Größe der Dateien, die an den Server gesendet werden. Die Schätzung des Clients wird verwendet und nicht das tatsächliche Datenvolumen, das an den Server gesendet wird. Clientoptionen, wie z. B. Deduplizierung, Komprimierung und Verschlüsselung, können zur Folge haben, dass das tatsächliche Datenvolumen, das an den Server gesendet wird, größer oder kleiner als die Größenschätzung ist. Beispielsweise kann eine komprimierte Datei kleiner als die Schätzung sein, sodass weniger Daten als der Schätzwert gesendet werden. Des Weiteren kann eine Binärdatei nach der Komprimierungsverarbeitung größer sein, sodass mehr Daten als der Schätzwert gesendet werden.

Wenn die physische Größe des Speicherpools den Wert des Parameters MAXSIZE überschreitet, zeigt die folgende Tabelle an, wo Dateien normalerweise gespeichert werden.

Tabelle 1. Position einer Datei gemäß der Dateigröße und dem angegebenen Pool

Dateigröße	**Angegebener Pool**	**Ergebnis**
Überschreitet die maximale Größe	Es ist kein Pool als nächster Speicherpool in der Hierarchie angegeben	Die Datei wird vom Server nicht gespeichert
	Ein Pool ist als nächster Speicherpool in der Hierarchie angegeben	Der Server speichert die Datei im nächsten Speicherpool, der die Dateigröße akzeptiert

Tipp: Wenn Sie auch den Parameter NEXTstgpool angeben, definieren Sie einen einzelnen Speicherpool in Ihrer Hierarchie so, dass er keine Begrenzung hinsichtlich der maximalen Dateigröße hat, indem Sie den Parameter MAXSIze=NOLimit angeben. Wenn mindestens ein Pool keine Größenbegrenzung hat, wird sichergestellt, dass der Server die Datei unabhängig von ihrer Größe speichern kann.

Bei mehreren Dateien, die in einer einzelnen Transaktion gesendet werden, betrachtet der Server die Größe der Transaktion als Dateigröße. Wenn die Gesamtgröße aller Dateien in der Transaktion die maximale Größe überschreitet, werden die Dateien vom Server nicht in dem Speicherpool gespeichert.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

CRCData
: Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

  Yes
  : Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

  No
  : Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

  Tipp:

  Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

  Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

  - IBM® LTO5 und höher
  - IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
  - Oracle StorageTek T10000C- und T10000D-Laufwerke

NEXTstgpool
: Gibt einen primären Speicherpool an, in den Dateien umgelagert werden. Sie können keine Daten aus einem Speicherpool mit sequenziellem Zugriff in einen Speicherpool mit wahlfreiem Zugriff umlagern. Dieser Parameter ist wahlfrei. Der nächste Speicherpool muss ein primärer Speicherpool sein.

  Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("") angeben.

  Verfügt dieser Speicherpool nicht über einen nächsten Speicherpool, kann der Server nicht Dateien aus diesem Speicherpool umlagern und Dateien, die die maximale Größe für diesen Speicherpool überschreiten, nicht in einem anderen Speicherpool speichern.

  Ist in dem aktuellen Speicherpool nicht genügend Speicherbereich verfügbar, erlaubt der Parameter NEXTSTGPOOL für Speicherpools mit sequenziellem Zugriff nicht das Speichern von Daten im nächsten Pool. In diesem Fall gibt der Server eine Nachricht aus, und die

Transaktion schlägt fehl.

Für nächste Speicherpools mit dem Einheitentyp FILE führt der Server eine vorläufige Überprüfung durch, um zu bestimmen, ob genügend Speicherbereich verfügbar ist. Ist kein Speicherbereich verfügbar, springt der Server zum nächsten Speicherpool in der Hierarchie. Ist Speicherbereich verfügbar, versucht der Server, Daten in diesem Pool zu speichern. Die Speicheroperation kann jedoch fehlschlagen, wenn zum Zeitpunkt der tatsächlichen Speicheroperation der Speicherbereich nicht mehr verfügbar ist.

Einschränkungen:

- Um sicherzustellen, dass keine Speicherpoolkette erstellt wird, die zu einer Endlosschleife führt, geben Sie mindestens einen Speicherpool in der Hierarchie ohne Wert an.
- Wenn Sie einen Pool mit sequenziellem Zugriff als nächsten Speicherpool angeben, muss der Pool entweder das Datenformat NATIVE oder NONBLOCK haben.
- Geben Sie keinen Verzeichniscontainer- oder Cloud-Containerspeicherpool an.
- Verwenden Sie diesen Parameter nicht, um einen Speicherpool für die Datenumlagerung anzugeben.
- Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

HIghmig
: Gibt an, dass der Server die Umlagerung startet, wenn die Speicherpoolauslastung diesen Prozentsatz erreicht. Für Plattenspeicherpools mit sequenziellem Zugriff (FILE) ist die Auslastung das Verhältnis der Daten in einem Speicherpool zur Summe der geschätzten Datenkapazität des Pools, einschließlich der Kapazität aller für den Pool angegebenen Arbeitsdatenträger. Für Speicherpools, die Banddatenträger verwenden, ist die Auslastung das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100 angeben.

  Wenn der Speicherpool die obere Umlagerungsschwelle überschreitet, kann der Server die Umlagerung von Dateien in den nächsten definierten Speicherpool nach Datenträger starten. Die obere Umlagerungsschwelle kann auf 100 gesetzt werden, um die Umlagerung für den Speicherpool zu verhindern.

  Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

LOwmig
: Gibt an, dass der Server die Umlagerung stoppt, wenn die Speicherpoolauslastung diesen Prozentsatz erreicht oder unter diesem Prozentsatz liegt. Für Plattenspeicherpools mit sequenziellem Zugriff (FILE) ist die Auslastung das Verhältnis der Daten in einem Speicherpool zur Summe der geschätzten Datenkapazität des Pools, einschließlich der Kapazität aller für den Pool angegebenen Arbeitsdatenträger. Für Speicherpools, die Banddatenträger verwenden, ist die Auslastung das Verhältnis der Datenträger, die Daten enthalten, zur Gesamtzahl der Datenträger in dem Speicherpool. Die Gesamtzahl der Datenträger schließt die maximale Anzahl Arbeitsdatenträger ein. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 99 angeben.

  Wenn der Speicherpool die untere Umlagerungsschwelle erreicht, wird die Umlagerung von Dateien von einem anderen Datenträger von dem Server nicht gestartet. Die Angabe von 0 für die untere Umlagerungsschwelle erlaubt eine Umlagerung, um den Speicherpool zu leeren.

  Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

RECLaim
: Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

  Bei der Wiederherstellung wird der zerstückelte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien von einem Datenträger auf einen anderen wieder verwendbar, wodurch der ursprüngliche Datenträger wiederverwendet werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben.

  Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

  Einen Wert von 50 Prozent oder höher für diesen Parameter angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

  AIX-Betriebssysteme  Windows-BetriebssystemeFür Speicherpools, die eine Einheitenklasse WORM verwenden, kann der Standardwert 100 verringert werden. Damit wird es dem Server ermöglicht, Daten bei Bedarf auf weniger Datenträger zusammenzulegen.

Datenträger, die durch die Wiederherstellung geleert werden, können aus dem Kassettenarchiv entnommen werden, wodurch Schächte für neue Datenträger freigegeben werden. Da die Datenträger nur einmal beschrieben werden können, ist eine Wiederverwendung der Datenträger nicht möglich.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMPRocess
Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein. Sie können einen oder mehrere Wiederherstellungsprozesse für jeden primären Speicherpool mit sequenziellem Zugriff angeben.
Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Wenn der Parameter RECLAIMSTGPOOL nicht angegeben ist oder der Wiederherstellungsspeicherpool dieselbe Einheitenklasse wie der Speicherpool hat, der wiederhergestellt wird, benötigt jeder Prozess zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für die beiden Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 16 haben.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

RECLAIMSTGpool
Gibt einen anderen primären Speicherpool als Ziel für wiederhergestellte Daten aus diesem Speicherpool an. Dieser Parameter ist wahlfrei. Wenn der Server Datenträger für den Speicherpool zurückfordert, werden nicht verfallene Daten von den Datenträgern, die zurückgefordert werden, in den Speicherpool versetzt, der mit diesem Parameter angegeben wird.

Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("") angeben.

Ein Wiederherstellungsspeicherpool ist besonders nützlich für einen Speicherpool, der nur ein Laufwerk in seinem Kassettenarchiv hat. Wird dieser Parameter angegeben, versetzt der Server alle Daten von den zurückgeforderten Datenträgern in den Wiederherstellungsspeicherpool, unabhängig von der Anzahl der Laufwerke in dem Kassettenarchiv.

Um die Daten aus dem Wiederherstellungsspeicherpool wieder in den ursprünglichen Speicherpool zu versetzen, ist die Speicherpoolhierarchie zu verwenden. Den ursprünglichen Speicherpool als nächsten Speicherpool für den Wiederherstellungsspeicherpool angeben.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

COLlocate
Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger. Die Kollokation kann sich auch auf die Anzahl Prozesse zum Umlagern von Platten in den sequenziellen Pool auswirken.

Sie können eine der folgenden Optionen angeben:

No
: Gibt an, dass die Kollokation inaktiviert ist. Während der Umlagerung von Platte werden Prozesse auf einer Dateibereichsebene erstellt.

GRoup
: Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

  Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

  Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

  - Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
  - Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.
  - Während der Umlagerung von Platte erstellt der Server Umlagerungsprozesse auf der Kollokationsgruppenebene für gruppierte Knoten und auf der Knotenebene für nicht gruppierte Knoten.

  Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

  - Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
  - Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.
  - Während der Umlagerung von Platte erstellt der Server Umlagerungsprozesse auf der Kollokationsgruppenebene für gruppierte Dateibereiche.

  Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

NODe
: Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

  Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

  Bei COLLOCATE=NODE erstellt der Server Prozesse auf der Knotenebene, wenn Daten von Platte umgelagert werden.

FIlespace
: Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

  Bei COLLOCATE=FILESPACE erstellt der Server Prozesse auf der Dateibereichsebene, wenn Daten von Platte umgelagert werden.

MAXSCRatch
: Gibt die maximale Anzahl Arbeitsdatenträger an, die der Server anfordern kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

  Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Speicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Speicherpools geschätzt.

  Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Wenn Arbeitsdatenträger mit dem Einheitentyp FILE gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

REUsedelay
Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Wert 0 bedeutet, dass ein Datenträger wieder beschrieben bzw. als Arbeitsdatenträger zurückgegeben werden kann, sobald alle Dateien auf dem Datenträger gelöscht wurden.

Durch Angabe dieses Parameters kann sichergestellt werden, dass die Datenbank auf einem früheren Stand wiederhergestellt werden kann und Datenbankverweise auf Dateien im Speicherpool weiterhin gültig wären.

OVFLOcation
Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl MOVE MEDIA aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("") angeben.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGDelay
Gibt die Mindestanzahl Tage an, die eine Datei in einem Speicherpool verbleiben muss, bevor sie für die Umlagerung ausgewählt werden kann. Alle Dateien auf einem Datenträger müssen für die Umlagerung auswählbar sein, bevor der Server den Datenträger für die Umlagerung auswählt. Um einen Wert zu berechnen, der mit dem angegebenen Wert für MIGDELAY verglichen wird, zählt der Server die Anzahl der Tage, die die Datei im Speicherpool war.

Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben.

Soll der Server die Anzahl der Tage nur ab dem Tag zählen, an dem eine Datei gespeichert wurde, und nicht ab dem Tag, an dem sie abgerufen wurde, die Serveroption NORETRIEVEDATE verwenden.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGContinue
Gibt an, ob der Server Dateien umlagern darf, die der Verzögerungszeit für die Umlagerung nicht entsprechen. Dieser Parameter ist wahlfrei.

Da angegeben werden kann, dass Dateien eine Mindestanzahl Tage in dem Speicherpool verbleiben müssen, kann der Server alle auswählbaren Dateien in den nächsten Speicherpool umlagern, obwohl sie dem Wert für die untere Umlagerungsschwelle nicht entsprechen. Mit diesem Parameter kann angegeben werden, ob der Server die Umlagerung fortsetzen darf, indem Dateien umgelagert werden, die der Verzögerungszeit für die Umlagerung nicht entsprechen.

Sie können einen der folgenden Werte angeben:

Yes
Muss die untere Umlagerungsschwelle eingehalten werden, gibt dieser Wert an, dass der Server die Umlagerung von Dateien fortsetzt, die noch nicht die Anzahl Tage in dem Speicherpool gespeichert sind, die durch die Umlagerungsverzögerung angegeben ist.

No
Gibt an, dass der Server die Umlagerung stoppt, wenn keine auswählbaren Dateien mehr für die Umlagerung verfügbar sind; dies gilt auch vor Erreichen der unteren Umlagerungsschwelle. Der Server lagert nur Dateien um, die die durch die Umlagerungsverzögerung angegebene Anzahl Tage in dem Speicherpool gespeichert sind.

Einschränkung: Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

MIGPRocess

Gibt die Anzahl paralleler Prozesse für das Umlagern der Dateien von den Datenträgern in diesen Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein.

Bei der Berechnung des Werts für diesen Parameter ist die Anzahl der sequenziellen Speicherpools, die von der Umlagerung betroffen sind, und die Anzahl der logischen und physischen Laufwerke zu berücksichtigen, die der Operation zugeordnet werden können. Für den Zugriff auf einen Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk. Die Anzahl der verfügbaren Mountpunkte und Laufwerke ist von anderen IBM Spectrum Protect- und Systemaktivitäten sowie von den Grenzwerten für Ladeanforderungen der Einheitenklassen für die Speicherpools mit sequenziellem Zugriff abhängig, die von der Umlagerung betroffen sind.

Beispiel: Angenommen, Sie möchten gleichzeitig die Dateien von Datenträgern in zwei primären sequenziellen Speicherpools umlagern und Sie möchten drei Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Hat der Speicherpool, in den Dateien umgelagert werden, dieselbe Einheitenklasse wie der Speicherpool, aus dem Dateien umgelagert werden, benötigt jeder Prozess zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um sechs Umlagerungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 12 Mountpunkte und 12 Laufwerke. Die Einheitenklasse für die Speicherpools muss einen Grenzwert für Ladeanforderungen von mindestens 12 haben.

Überschreitet die angegebene Anzahl der Umlagerungsprozesse die Anzahl der verfügbaren Mountpunkte oder Laufwerke, warten die Prozesse, die keine Mountpunkte oder Laufwerke anfordern können, bis Mountpunkte oder Laufwerke verfügbar werden. Werden Mountpunkte oder Laufwerke innerhalb der MOUNTWAIT-Zeit nicht verfügbar, werden die Umlagerungsprozesse beendet. Informationen zur Angabe der MOUNTWAIT-Zeit befinden sich in DEFINE DEVCLASS (Einheitenklasse definieren).

Der IBM Spectrum Protect-Server startet die angegebene Anzahl der Umlagerungsprozesse, unabhängig von der Anzahl der Datenträger, die für die Umlagerung ausgewählt werden können. Geben Sie beispielsweise zehn Umlagerungsprozesse an und können nur sechs Datenträger für die Umlagerung ausgewählt werden, startet der Server zehn Prozesse, von denen vier beendet werden, ohne dass ein Datenträger verarbeitet wird.

Anmerkung: Beachten Sie bei der Angabe dieses Parameters, ob die Funktion für simultanes Schreiben für die Serverdatenumlagerung aktiviert ist. Jeder Umlagerungsprozess erfordert einen Mountpunkt und ein Laufwerk für jeden Kopienspeicherpool und Pool für aktive Daten, der für den Zielspeicherpool definiert ist.

AUTOCopy
: Gibt an, wann IBM Spectrum Protect Operationen mit simultanem Schreiben ausführt. Dieser Parameter betrifft die folgenden Operationen:

  - Clientspeichersitzungen
  - Serverimportprozesse
  - Serverdatenumlagerungsprozesse

  Wenn die Option AUTOCOPY auf `ALL` oder `CLIENT` gesetzt wird und mindestens ein Speicherpool vorhanden ist, der in der Option COPYSTGPOOLS oder ACTIVEDATAPOOLS aufgelistet ist, wird die clientseitige Deduplizierung inaktiviert.

  Tritt ein Fehler auf, wenn Daten während eines Umlagerungsprozesses gleichzeitig in einen Kopienspeicherpool oder einen Pool für aktive Daten geschrieben werden, stoppt der Server das Schreiben in die fehlerhaften Speicherpools für den Rest des Prozesses. Der Server speichert jedoch weiterhin Dateien in dem primären Speicherpool und in allen verbleibenden Kopienspeicherpools oder Pools für aktive Daten. Diese Pools bleiben für die Dauer des Umlagerungsprozesses aktiv. Kopienspeicherpools werden mit dem Parameter COPYSTGPOOLS angegeben. Pools für aktive Daten werden mit dem Parameter ACTIVEDATAPOOLS angegeben.

  Sie können einen der folgenden Werte angeben:

  None
  : Gibt an, dass die Funktion für simultanes Schreiben inaktiviert ist.

  CLient
  : Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen oder Serverimportprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverimportprozessen werden Daten nur gleichzeitig in Kopienspeicherpools geschrieben. Daten werden während der Ausführung von Serverimportprozessen nicht in Pools für aktive Daten geschrieben.

  MIGRation
  : Gibt an, dass Daten nur während der Umlagerung in diesen Speicherpool gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Während der Ausführung von Serverdatenumlagerungsprozessen werden Daten in Kopienspeicherpools und Pools für aktive Daten nur dann gleichzeitig geschrieben, wenn die Daten in diesen Pools nicht vorhanden sind. Knoten, deren Daten umgelagert werden, müssen sich in einer Domäne befinden, die einem Pool für aktive Daten zugeordnet ist. Befinden sich die Knoten nicht in einer Domäne, die einem Pool für aktive Daten zugeordnet ist, können die Daten nicht in den Pool geschrieben werden.

  All
  : Gibt an, dass Daten während der Ausführung von Clientspeichersitzungen, Serverimportprozessen oder Serverdatenumlagerungsprozessen gleichzeitig in Kopienspeicherpools und Pools für aktive Daten geschrieben werden. Mit diesem Wert wird sichergestellt, dass Daten immer dann gleichzeitig geschrieben werden, wenn dieser Pool ein Ziel für eine der auswählbaren Operationen ist.

COPYSTGpools

Gibt die Namen von Kopienspeicherpools an, in die der Server gleichzeitig Daten schreibt. Sie können maximal drei Kopienpoolnamen angeben, die durch Kommas voneinander getrennt werden müssen. Leerzeichen zwischen den Namen der Kopienpools sind nicht zulässig. Um einen oder mehrere Kopienspeicherpools hinzuzufügen oder zu entfernen, geben Sie den oder die Poolnamen an, der bzw. die in der aktualisierten Liste enthalten sein soll(en). Enthält die vorhandene Kopienpoolliste beispielsweise COPY1 und COPY2 und soll COPY3 hinzugefügt werden, geben Sie COPYSTGPOOLS=COPY1,COPY2,COPY3 an. Um alle vorhandenen Kopienspeicherpools zu entfernen, die dem primären Speicherpool zugeordnet sind, geben Sie eine Nullzeichenfolge ("") für den Wert an (beispielsweise COPYSTGPOOLS="").

Wenn Sie einen Wert für den Parameter COPYSTGPOOLS angeben, können Sie auch einen Wert für den Parameter COPYCONTINUE angeben. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Kopienspeicherpools und den Wert für COPYCONTINUE aus dem primären Speicherpool. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

Der Server kann während der Ausführung der folgenden Operationen Daten gleichzeitig in Kopienspeicherpools schreiben:

- Sicherungs- und Archivierungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder Anwendungsclients, die die IBM Spectrum Protect-API verwenden
- Umlagerungsoperationen durch IBM Spectrum Protect for Space Management-Clients
- Importoperationen, die das Kopieren von exportierten Dateidaten von externen Datenträgern in einen primären Speicherpool einbeziehen, der einer Kopienspeicherpoolliste zugeordnet ist

Einschränkungen:

1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat NATIVE oder NONBLOCK verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
    - NETAPPDUMP
    - CELERRADUMP
    - NDMPDUMP
2. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
3. Die Funktion für simultanes Schreiben wird für NAS-Sicherungsoperationen nicht unterstützt. Sind für den primären Speicherpool, der in DESTINATION oder TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Kopienspeicherpools definiert, werden die Kopienspeicherpools ignoriert und die Daten werden nur im primären Speicherpool gespeichert.
4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.

Achtung: Die mit dem Parameter COPYSTGPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl BACKUP STGPOOL ersetzen. Wird der Parameter COPYSTGPOOLS verwendet, verwenden Sie weiterhin den Befehl BACKUP STGPOOL, um sicherzustellen, dass die Kopienspeicherpools vollständige Kopien des primären Speicherpools sind. Es gibt Fälle, in denen eine Kopie möglicherweise nicht erstellt wird. Weitere Informationen enthält die Beschreibung des Parameters COPYCONTINUE.

COPYContinue
: Gibt an, wie der Server auf einen Fehler beim Schreiben in einen der Kopienspeicherpools reagiert, die im Parameter COPYSTGPOOLS aufgelistet sind. Dieser Parameter ist wahlfrei. Der Standardwert ist YES. Wenn Sie den Parameter COPYCONTINUE angeben, muss entweder eine COPYSTGPOOLS-Liste vorhanden sein oder der Parameter COPYSTGPOOLS muss ebenfalls angegeben werden.

  Der Parameter COPYCONTINUE hat keine Auswirkung auf die Funktion für simultanes Schreiben während der Umlagerung.

  Sie können die folgenden Werte angeben:

  Yes
  : Ist der Parameter COPYCONTINUE auf YES gesetzt, stoppt der Server das Schreiben in die fehlerhaften Kopienpools für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Kopienpools fort. Die Liste der Kopienspeicherpools ist nur für die Dauer der Clientsitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.

  No
  : Ist der Parameter COPYCONTINUE auf NO gesetzt, wird die aktuelle Transaktion vom Server nicht ausgeführt und die Speicheroperation nicht fortgesetzt.

  Einschränkungen:

  - Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf Pools für aktive Daten. Tritt für einen der Pools für aktive Daten ein Schreibfehler auf, stoppt der Server das Schreiben in den fehlerhaften Pool für aktive Daten für den Rest der Sitzung, aber setzt das Speichern von Dateien im primären Pool und in allen übrigen Pools für aktive Daten und Kopienspeicherpools fort. Die Liste der Pools für aktive Daten ist nur für die Dauer der Sitzung aktiv und gilt für alle primären Speicherpools in einer bestimmten Speicherpoolhierarchie.
  - Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Ausführung eines Serverimportprozesses. Werden Daten gleichzeitig geschrieben und tritt für den primären Speicherpool oder einen Kopienspeicherpool ein Schreibfehler auf, schlägt der Serverimportprozess fehl.

- Die Einstellung des Parameters COPYCONTINUE hat keine Auswirkungen auf die Funktion für simultanes Schreiben während der Serverdatenumlagerung. Werden Daten gleichzeitig geschrieben und tritt für einen Kopienspeicherpool oder Pool für aktive Daten ein Schreibfehler auf, wird der fehlerhafte Speicherpool entfernt und der Datenumlagerungsprozess wird fortgesetzt. Bei Schreibfehlern für den primären Speicherpool schlägt der Umlagerungsprozess fehl.

ACTIVEDATApools
: Gibt die Namen der Pools für aktive Daten an, in die der Server während einer Clientsicherungsoperation gleichzeitig Daten schreibt. Der Parameter ACTIVEDATAPOOLS ist optional. Leerzeichen zwischen den Namen der Pools für aktive Daten sind nicht zulässig.

  Die kombinierte Gesamtzahl der Speicherpools, die in den Parametern COPYSGTPOOLS und ACTIVEDATAPOOLS angegeben sind, darf drei nicht überschreiten.

  Wenn eine Datenspeicheroperation von einem primären Speicherpool zu einem nächsten Speicherpool wechselt, übernimmt der nächste Speicherpool die Liste der Pools für aktive Daten aus dem Zielspeicherpool, der in der Kopiengruppe angegeben ist. Der primäre Speicherpool wird durch die Kopiengruppe der Verwaltungsklasse angegeben, die an die Daten gebunden ist.

  Der Server kann nur während Sicherungsoperationen durch IBM Spectrum Protect-Clients für Sichern/Archivieren oder durch Anwendungsclients, die die IBM Spectrum Protect-API verwenden, Daten gleichzeitig in Pools für aktive Daten schreiben. Einschränkungen:

  1. Dieser Parameter ist nur für primäre Speicherpools verfügbar, die das Datenformat NATIVE oder NONBLOCK verwenden. Dieser Parameter ist für Speicherpools nicht verfügbar, die die folgenden Datenformate verwenden:
     - NETAPPDUMP
     - CELERRADUMP
     - NDMPDUMP
  2. Das simultane Schreiben in Pools für aktive Daten wird nicht unterstützt, wenn die Operation die LAN-unabhängige Datenversetzung verwendet. Operationen mit simultanem Schreiben haben Vorrang vor der LAN-unabhängigen Datenversetzung; dadurch werden die Operationen über das LAN ausgeführt. Die Konfiguration für das simultane Schreiben wird jedoch akzeptiert.
  3. Die Funktion für simultanes Schreiben wird nicht unterstützt, wenn eine NAS-Sicherungsoperation eine Inhaltsverzeichnisdatei schreibt. Sind für den primären Speicherpool, der in TOCDESTINATION in der Kopiengruppe der Verwaltungsklasse angegeben ist, Pools für aktive Daten definiert, werden die Pools für aktive Daten ignoriert und die Daten werden nur im primären Speicherpool gespeichert.
  4. Die Funktion für simultanes Schreiben kann mit CENTERA-Speichereinheiten nicht verwendet werden.
  5. Daten, die importiert werden, können nicht in Pools für aktive Daten gespeichert werden. Verwenden Sie nach einer Importoperation den Befehl COPY ACTIVEDATA, um die importierten Daten in einem Pool für aktive Daten zu speichern.

  Achtung: Die mit dem Parameter ACTIVEDATAPOOLS zur Verfügung gestellte Funktion soll nicht den Befehl COPY ACTIVEDATA ersetzen. Wird der Parameter ACTIVEDATAPOOLS verwendet, verwenden Sie den Befehl COPY ACTIVEDATA, um sicherzustellen, dass die Pools für aktive Daten alle aktiven Daten des primären Speicherpools enthalten.

DEDUPlicate
: Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.

IDENTIFYPRocess
: Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Datendeduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools mit einer Einheitenklasse gültig, der der Einheitentyp FILE zugeordnet ist. Geben Sie einen Wert von 1 bis 50 ein.
  Hinweis: Datendeduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Datendeduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Datendeduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Datendeduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

Beispiel: Die mountfähigen Arbeitsdatenträger des primären Speicherpools mit sequenziellem Zugriff aktualisieren

Den primären Speicherpool mit sequenziellem Zugriff mit dem Namen TAPEPOOL1 aktualisieren, um das Laden von maximal 10 Arbeitsdatenträgern zu erlauben.

```
update stgpool tapepool1 maxscratch=10
```

UPDATE STGPOOL (Kopienspeicherpool mit sequenziellem Zugriff aktualisieren)

Mit diesem Befehl kann ein Kopienspeicherpool mit sequenziellem Zugriff aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

Syntax

Anmerkungen:

1. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
2. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

Parameter

Poolname (Erforderlich)
: Gibt den Namen des Kopienspeicherpools an, der aktualisiert werden soll.

DESCription
: Gibt eine Beschreibung des Kopienspeicherpools an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("") angeben.

ACCess
: Gibt an, wie Clientknoten und Serverprozesse (wie Wiederherstellung) auf Dateien im Kopienspeicherpool zugreifen können. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

  READWrite
  : Gibt an, dass Dateien auf die Datenträger im Kopienspeicherpool geschrieben und daraus gelesen werden können.

  READOnly
  : Gibt an, dass Clientknoten Dateien, die auf den Datenträgern im Kopienspeicherpool gespeichert sind, nur lesen können.

    Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Kopienspeicherpool verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Kopienspeicherpool sind jedoch keine neuen Schreiboperationen durch Datenträger außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht im Kopienspeicherpool gesichert werden.

  UNAVailable
  : Gibt an, dass Clientknoten nicht auf Dateien zugreifen können, die auf Datenträgern im Kopienspeicherpool gespeichert sind.

    Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Kopienspeicherpool verwenden, um Dateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem

Kopienspeicherpool sind jedoch keine neuen Schreiboperationen durch Datenträger außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht im Kopienspeicherpool gesichert werden.

COLlocate
Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger.

Sie können eine der folgenden Optionen angeben:

No
Gibt an, dass die Kollokation inaktiviert ist.

GRoup
Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.

Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

NODe
Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

FIlespace
Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

RECLaim
Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

Bei der Wiederherstellung wird der zerstückelte Speicherbereich auf Datenträgern durch Versetzen der restlichen aktiven Dateien von einem Datenträger auf einen anderen wieder verwendbar, wodurch der ursprüngliche Datenträger wiederverwendet werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Wert 100 bedeutet, dass Datenträger nicht zurückgefordert werden.

Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

Wird der Standardwert 100 geändert, einen Wert von 50 Prozent oder höher angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

Wenn ein ausgelagerter Kopienspeicherpooldatenträger für die Wiederherstellung ausgewählt werden kann, versucht der Wiederherstellungsprozess, die aktiven Dateien auf einem zurückforderbaren Datenträger aus einem primären Speicherpool oder einem Kopienspeicherpool vor Ort abzurufen. Der Prozess schreibt dann diese Dateien auf einen verfügbaren Datenträger in dem ursprünglichen Kopienspeicherpool. Tatsächlich werden diese Dateien wieder an den Standort vor Ort versetzt. Die Dateien können jedoch nach einem Katastrophenfall auch vom ausgelagerten Datenträger abgerufen werden, wenn eine Datenbanksicherung verwendet wird, die auf die Dateien auf dem ausgelagerten Datenträger verweist. Wegen der Art, mit der ausgelagerte Datenträger bei der Wiederherstellung bearbeitet werden, sollte die Wiederherstellung bei Kopienspeicherpools mit Vorsicht verwendet werden.

RECLAIMPRocess
Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein.
Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

- Die Anzahl sequenzieller Speicherpools
- Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Jeder Prozess benötigt zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für jeden Speicherpool muss einen Grenzwert für Ladeanforderungen von mindestens 8 haben.

Sie können einen oder mehrere Wiederherstellungsprozesse für jeden Kopienspeicherpool angeben. Sie können mehrere gleichzeitig ablaufende Wiederherstellungsprozesse für einen einzelnen Kopienspeicherpool angeben. Damit wird eine bessere Nutzung Ihrer verfügbaren Bandlaufwerke oder FILE-Datenträger erreicht. Wenn die gleichzeitig ablaufende Verarbeitung mehrerer Prozesse nicht erforderlich ist, geben Sie den Wert 1 für den Parameter RECLAIMPROCESS an.

OFFSITERECLAIMLimit
Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool zurückgefordert wird. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

NOLimit
Gibt an, dass der Speicherbereich auf allen ausgelagerten Datenträgern wiederhergestellt werden soll.

Anzahl
Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich wiederhergestellt werden soll. Sie können eine ganze Zahl von 0 bis 99999 angeben. Der Wert 0 bedeutet, dass für keine ausgelagerten Datenträger der Speicherbereich wiederhergestellt wird.
Tipp:

Um den Wert für OFFSITERECLAIMLIMIT zu bestimmen, verwenden Sie die statistischen Informationen in der Nachricht, die am Ende der Wiederherstellungsoperation für den ausgelagerten Datenträger ausgegeben wird. Die statistischen Informationen umfassen die folgenden Elemente:

- Die Anzahl der ausgelagerten Datenträger, die verarbeitet wurden
- Die Anzahl der parallelen Prozesse, die verwendet wurden
- Die Gesamtzeit, die für die Verarbeitung benötigt wurde

Die Reihenfolge, in der ausgelagerte Datenträger wiederhergestellt werden, basiert auf dem Umfang des freien Speicherplatzes auf einem Datenträger. (Freier Speicherplatz umfasst den Speicherbereich, der auf dem Datenträger nie verwendet wurde, und den Speicherbereich, der aufgrund des Löschens von Dateien frei geworden ist.) Datenträger mit dem größten freien Speicherplatz werden zuerst wiederhergestellt.

Beispiel: Angenommen, ein Kopienspeicherpool enthält drei Datenträger: VOL1, VOL2 und VOL3. VOL1 hat den größten freien Speicherplatz, und VOL3 hat den kleinsten freien Speicherplatz. Weiter wird angenommen, dass der Prozentsatz des freien Speicherplatzes auf jedem der drei Datenträger größer als der Wert des Parameters RECLAIM ist. Wird kein Wert für den Parameter OFFSITERECLAIMLIMIT angegeben, werden alle drei Datenträger wiederhergestellt, wenn die Wiederherstellung ausgeführt wird. Wird

der Wert 2 angegeben, werden nur VOL1 und VOL2 bei der Wiederherstellung wiederhergestellt. Wird der Wert 1 angegeben, wird nur VOL1 wiederhergestellt.

MAXSCRatch
: Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern nach Bedarf erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

  Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Kopienspeicherpool verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Kopienspeicherpools geschätzt.

  Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Lautet jedoch der Zugriffsmodus für einen Arbeitsdatenträger OFFSITE, wird der Datenträger erst dann aus dem Kopienspeicherpool gelöscht, wenn der Zugriffsmodus geändert wird. Ein Administrator kann den Server nach leeren ausgelagerten Arbeitsdatenträgern abfragen und diese an den Standort vor Ort zurückgeben.

  Wenn Arbeitsdatenträger mit dem Einheitentyp FILE leer werden und gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

  Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der IBM Spectrum Protect-Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

REUsedelay
: Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Wert 0 bedeutet, dass ein Datenträger wieder beschrieben bzw. als Arbeitsdatenträger zurückgegeben werden kann, sobald alle Dateien auf dem Datenträger gelöscht wurden.
  Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Kopienspeicherpool noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl entsprechen.

OVFLOcation
: Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl MOVE MEDIA aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

  Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("") angeben.

CRCData
: Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

  Yes
  : Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

  No
  : Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

  Tipp:

  Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

  Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

  - IBM® LTO5 und höher
  - IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
  - Oracle StorageTek T10000C- und T10000D-Laufwerke

DEDUPlicate

Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.

IDENTIFYPRocess
Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Datendeduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 1 bis 50 ein. Hinweis: Datendeduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Datendeduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Datendeduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Datendeduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

Beispiel: Einen Kopienspeicherpool aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern und Dateien nach Clientknoten zusammenzufassen

Den Kopienspeicherpool TAPEPOOL2 aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern und Dateien nach Clientknoten zusammenzufassen.

```
update stgpool tapepool2 reusedelay=30 collocate=node
```

Zugehörige Verweise:
SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsserie angeben)

UPDATE STGPOOL (Pool für aktive Daten mit sequenziellem Zugriff aktualisieren)

Mit diesem Befehl kann ein Pool für aktive Daten aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung für den Speicherpool, der aktualisiert werden soll, erforderlich.

Syntax

Anmerkungen:

1. Dieser Parameter ist nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.
2. Dieser Parameter ist nur verfügbar, wenn der Parameter DEDUPLICATE den Wert YES hat.

Parameter

Poolname (Erforderlich)
Gibt den Namen des Pools für aktive Daten an, der aktualisiert werden soll.

DESCription
Gibt eine Beschreibung des Pools für aktive Daten an. Dieser Parameter ist wahlfrei. Die maximale Länge der Beschreibung beträgt 255 Zeichen. Wenn die Beschreibung Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden.Soll eine vorhandene Beschreibung entfernt werden, eine Nullzeichenfolge ("") angeben.

ACCess
Gibt an, wie Clientknoten und Serverprozesse (wie Wiederherstellung) auf Dateien im Pool für aktive Daten zugreifen können. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

READWrite
Gibt an, dass Dateien auf die Datenträger im Pool für aktive Daten geschrieben und daraus gelesen werden können.

READOnly
Gibt an, dass Clientknoten Dateien, die auf den Datenträgern im Pool für aktive Daten gespeichert sind, nur lesen können.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Pool für aktive Daten verwenden, um aktive Versionen von Sicherungsdateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Pool für aktive Daten sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht in den Pool für aktive Daten kopiert werden.

UNAVailable
Gibt an, dass Clientknoten nicht auf Dateien zugreifen können, die auf Datenträgern im Pool für aktive Daten gespeichert sind.

Serverprozesse können Dateien innerhalb der Datenträger im Speicherpool versetzen. Der Server kann Dateien im Pool für aktive Daten verwenden, um aktive Versionen von Sicherungsdateien in primäre Speicherpools zurückzuschreiben. Für die Datenträger in dem Pool für aktive Daten sind jedoch keine neuen Schreiboperationen von Datenträgern außerhalb des Speicherpools zulässig. Ein Speicherpool kann nicht in den Pool für aktive Daten kopiert werden.

COLlocate
Gibt an, ob der Server versucht, Daten, die zu den folgenden Kandidaten gehören, auf möglichst wenig Datenträgern zu speichern:

- Ein einzelner Clientknoten
- Eine Gruppe von Dateibereichen
- Eine Gruppe von Clientknoten
- Ein Clientdateibereich

Dieser Parameter ist wahlfrei.

Die Kollokation reduziert die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff für Zurückschreibungs-, Abruf- und Rückrufoperationen. Die Kollokation erfordert jedoch mehr Serverzeit, um Dateien zum Speichern zusammenzufassen, sowie eine größere Anzahl Datenträger.

Sie können eine der folgenden Optionen angeben:

No
Gibt an, dass die Kollokation inaktiviert ist.

GRoup
Gibt an, dass die Kollokation auf Gruppenebene für Clientknoten oder Dateibereiche aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten für Knoten oder Dateibereiche, die zu derselben Kollokationsgruppe gehören, auf so wenig Datenträgern wie möglich zu speichern.

Wenn Sie COLLOCATE=GROUP angeben, aber keine Kollokationsgruppen definieren, oder wenn Sie keine Knoten oder Dateibereiche zu einer Kollokationsgruppe hinzufügen, werden Daten nach Knoten durch Kollokation zusammengefasst. Ziehen Sie die Verwendung von Bändern in Betracht, wenn Sie Clientknoten oder Dateibereiche in Kollokationsgruppen zusammenfassen.

Besteht beispielsweise ein bandbasierter Speicherpool aus Daten von Knoten, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst die Daten für gruppierte Knoten nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Knoten gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Knoten können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten für nicht gruppierte Knoten nach Knoten zusammen. Wenn möglich, speichert der Server die Daten für einen einzelnen Knoten auf einem einzelnen Band. Alle verfügbaren Bänder, die bereits Daten für den Knoten enthalten, werden verwendet, bevor verfügbarer Speicherbereich auf einem anderen Band verwendet wird.

Besteht ein bandbasierter Speicherpool aus Daten aus gruppierten Dateibereichen, und geben Sie COLLOCATE=GROUP an, führt der Server die folgenden Aktionen aus:

- Fasst nur die Daten für gruppierte Dateibereiche nach Gruppe zusammen. Wenn möglich, fasst der Server die Daten, die zu einer Gruppe von Dateibereichen gehören, auf einem einzelnen Band oder auf möglichst wenige Bänder zusammen. Daten für einen einzelnen Dateibereich können auch auf mehrere Bänder verteilt werden, die einer Gruppe zugeordnet sind.
- Fasst die Daten nach Knoten zusammen (für Dateibereiche, die nicht explizit für eine Dateibereichskollokationsgruppe definiert sind). Beispiel: Knoten1 hat die Dateibereiche A, B, C, D und E. Die Dateibereiche A und B gehören zu einer Dateibereichskollokationsgruppe, die Dateibereiche C, D und E dagegen nicht. Die Dateibereiche A und B werden nach Dateibereichskollokationsgruppe zusammengefasst, während die Dateibereiche C, D und E nach Knoten zusammengefasst werden.

Daten werden auf so wenig Datenträger mit sequenziellem Zugriff wie möglich zusammengefasst.

NODe
: Gibt an, dass die Kollokation auf Clientknotenebene aktiviert ist. Für Kollokationsgruppen versucht der Server, Daten eines Knotens auf so wenig Datenträgern wie möglich zu speichern. Verfügt der Knoten über mehrere Dateibereiche, versucht der Server nicht, diese Dateibereiche durch Kollokation zusammenzufassen. Für die Kompatibilität mit früheren Versionen wird COLLOCATE=YES noch vom Server akzeptiert, um die Kollokation auf der Clientknotenebene anzugeben.

  Enthält ein Speicherpool Daten für einen Knoten, der Teil einer Kollokationsgruppe ist, und geben Sie COLLOCATE=NODE an, werden die Daten nach Knoten durch Kollokation zusammengefasst.

FIlespace
: Gibt an, dass die Kollokation auf der Dateibereichsebene für Clientknoten aktiviert ist. Der Server versucht, Daten eines Knotens und eines Dateibereichs auf so wenig Datenträgern wie möglich zu speichern. Verfügt ein Knoten über mehrere Dateibereiche, versucht der Server, Daten für verschiedene Dateibereiche auf verschiedenen Datenträgern zu speichern.

RECLaim
: Gibt an, wann der Server einen Datenträger auf der Basis des Prozentsatzes wiederherstellbaren Speicherbereichs auf einem Datenträger zurückfordert. Der wiederherstellbare Speicherbereich ist der Speicherbereich, der durch Dateien belegt ist, die verfallen sind oder aus der IBM Spectrum Protect-Datenbank gelöscht wurden.

  Bei der Wiederherstellung werden der fragmentierte Speicherbereich und der durch inaktive Sicherungsdateien belegte Speicherbereich auf Datenträgern durch Versetzen der restlichen nicht verfallenen Dateien und der aktiven Sicherungsdateien von einem Datenträger auf einen anderen Datenträger wieder verwendbar. Mit dieser Aktion kann der ursprüngliche Datenträger wiederverwendet werden. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 1 bis 100 angeben. Der Wert 100 bedeutet, dass Datenträger nicht zurückgefordert werden.

  Der Server bestimmt, dass der Datenträger ein Kandidat für die Wiederherstellung ist, wenn der Prozentsatz des wiederherstellbaren Speicherbereichs auf einem Datenträger größer als der Wiederherstellungsschwellenwert des Speicherpools ist.

  Wird der Standardwert 60 geändert, einen Wert von 50 Prozent oder höher angeben, so dass Dateien, die auf zwei Datenträgern gespeichert sind, auf einem einzigen Ausgabedatenträger gespeichert werden können.

  Wenn ein ausgelagerter Datenträger des Pools für aktive Daten für die Wiederherstellung ausgewählt werden kann, versucht der Wiederherstellungsprozess, die aktiven Dateien auf einem zurückforderbaren Datenträger aus einem primären Speicherpool oder einem Pool für aktive Daten vor Ort abzurufen. Der Prozess schreibt dann diese Dateien auf einen verfügbaren Datenträger in dem ursprünglichen Pool für aktive Daten. Tatsächlich werden diese Dateien wieder an den Standort vor Ort versetzt. Die Dateien können jedoch nach einem Katastrophenfall auch vom ausgelagerten Datenträger abgerufen werden, wenn eine Datenbanksicherung verwendet wird, die auf die Dateien auf dem ausgelagerten Datenträger verweist. Wegen der Art, mit der ausgelagerte Datenträger bei der Wiederherstellung bearbeitet werden, sollte die Wiederherstellung bei Pools mit aktiven Daten mit Vorsicht verwendet werden.

RECLAIMPRocess
: Gibt die Anzahl paralleler Prozesse für das Wiederherstellen der Datenträger in diesem Speicherpool an. Dieser Parameter ist wahlfrei. Geben Sie einen Wert von 1 bis 999 ein.
  Berücksichtigen Sie bei der Berechnung des Werts für diesen Parameter die folgenden Ressourcen, die für die Wiederherstellungsverarbeitung erforderlich sind:

  - Die Anzahl sequenzieller Speicherpools
  - Die Anzahl logischer und physischer Laufwerke, die der Operation zugeordnet werden kann

  Für den Zugriff auf Datenträger mit sequenziellem Zugriff verwendet IBM Spectrum Protect einen Mountpunkt und, falls der Einheitentyp nicht FILE lautet, ein physisches Laufwerk.

  Beispiel: Angenommen, Sie möchten die Datenträger aus zwei Speicherpools mit sequenziellem Zugriff gleichzeitig wiederherstellen und Sie möchten vier Prozesse für jeden der Speicherpools angeben. Die Speicherpools haben dieselbe Einheitenklasse. Jeder Prozess benötigt zwei Mountpunkte und, wenn der Einheitentyp nicht FILE lautet, zwei Laufwerke. (Ein Laufwerk ist für den Eingabedatenträger und das andere Laufwerk für den Ausgabedatenträger bestimmt.) Um acht Wiederherstellungsprozesse gleichzeitig auszuführen, benötigen Sie mindestens 16 Mountpunkte und 16 Laufwerke. Die Einheitenklasse für jeden Speicherpool muss einen Grenzwert für Ladeanforderungen von mindestens 8 haben.

Sie können einen oder mehrere Wiederherstellungsprozesse für jeden Pool für aktive Daten angeben. Sie können mehrere gleichzeitig ablaufende Wiederherstellungsprozesse für einen einzelnen Pool für aktive Daten angeben. Damit wird eine bessere Nutzung Ihrer verfügbaren Bandlaufwerke oder FILE-Datenträger erreicht. Wenn die gleichzeitig ablaufende Verarbeitung mehrerer Prozesse nicht erforderlich ist, geben Sie den Wert 1 für den Parameter RECLAIMPROCESS an.

OFFSITERECLAIMLimit
Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich während der Wiederherstellung für diesen Speicherpool zurückgefordert wird. Dieser Parameter ist wahlfrei. Sie können die folgenden Werte angeben:

NOLimit
Gibt an, dass der Speicherbereich auf allen ausgelagerten Datenträgern wiederhergestellt werden soll.

Anzahl
Gibt die Anzahl ausgelagerter Datenträger an, deren Speicherbereich wiederhergestellt werden soll. Sie können eine ganze Zahl von 0 bis 99999 angeben. Der Wert 0 bedeutet, dass für keine ausgelagerten Datenträger der Speicherbereich wiederhergestellt wird.
Tipp:

Um den Wert für OFFSITERECLAIMLIMIT zu bestimmen, verwenden Sie die statistischen Informationen in der Nachricht, die am Ende der Wiederherstellungsoperation für den ausgelagerten Datenträger ausgegeben wird. Die statistischen Informationen umfassen die folgenden Elemente:

- Die Anzahl der ausgelagerten Datenträger, die verarbeitet wurden
- Die Anzahl der parallelen Prozesse, die verwendet wurden
- Die Gesamtzeit, die für die Verarbeitung benötigt wurde

Die Reihenfolge, in der ausgelagerte Datenträger wiederhergestellt werden, basiert auf dem Umfang des freien Speicherplatzes auf einem Datenträger. (Freier Speicherplatz umfasst den Speicherbereich, der auf dem Datenträger nie verwendet wurde, und den Speicherbereich, der aufgrund des Löschens von Dateien frei geworden ist.) Datenträger mit dem größten freien Speicherplatz werden zuerst wiederhergestellt.

Beispiel: Angenommen, ein Pool für aktive Daten enthält drei Datenträger: VOL1, VOL2 und VOL3. VOL1 hat den größten freien Speicherplatz, und VOL3 hat den kleinsten freien Speicherplatz. Weiter wird angenommen, dass der Prozentsatz des freien Speicherplatzes auf jedem der drei Datenträger größer als der Wert des Parameters RECLAIM ist. Wird kein Wert für den Parameter OFFSITERECLAIMLIMIT angegeben, werden alle drei Datenträger wiederhergestellt, wenn die Wiederherstellung ausgeführt wird. Wird der Wert 2 angegeben, werden nur VOL1 und VOL2 bei der Wiederherstellung wiederhergestellt. Wird der Wert 1 angegeben, wird nur VOL1 wiederhergestellt.

MAXSCRatch
Gibt die maximale Anzahl der Arbeitsdatenträger an, die der Server für diesen Speicherpool anfordern kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 100000000 angeben. Wird dem Server das Anfordern von Arbeitsdatenträgern nach Bedarf erlaubt, muss der Benutzer nicht jeden zu verwendenden Datenträger definieren.

Mit dem für diesen Parameter angegebenen Wert wird die Gesamtzahl der im Pool für aktive Daten verfügbaren Datenträger und die entsprechende geschätzte Kapazität des Pools für aktive Daten geschätzt.

Arbeitsdatenträger werden automatisch aus dem Speicherpool gelöscht, sobald sie leer sind. Lautet jedoch der Zugriffsmodus für einen Arbeitsdatenträger OFFSITE, wird der Datenträger erst dann aus dem Pool für aktive Daten gelöscht, wenn der Zugriffsmodus geändert wird. Ein Administrator kann den Server nach leeren ausgelagerten Arbeitsdatenträgern abfragen und diese an den Standort vor Ort zurückgeben.

Wenn Arbeitsdatenträger mit dem Einheitentyp FILE leer werden und gelöscht werden, wird der von den Datenträgern belegte Speicherbereich von dem Server freigegeben und an das Dateisystem zurückgegeben.

Tipp: Für serverübergreifende Operationen, die virtuelle Datenträger verwenden und ein kleines Datenvolumen speichern, sollte ein Wert für den Parameter MAXSCRATCH angegeben werden, der höher als der Wert ist, der normalerweise für Schreiboperationen für andere Datenträgertypen angegeben wird. Nach einer Schreiboperation auf einem virtuellen Datenträger markiert IBM Spectrum Protect den Datenträger als FULL, auch wenn der Wert des Parameters MAXCAPACITY in der Einheitenklassendefinition noch nicht erreicht wurde. Der IBM Spectrum Protect-Server behält virtuelle Datenträger nicht im Status FILLING und hängt keine Daten an. Ist der Wert des Parameters MAXSCRATCH zu niedrig, können serverübergreifende Operationen fehlschlagen.

REUsedelay
Gibt die Anzahl Tage an, die nach dem Löschen aller Dateien von einem Datenträger verstreichen müssen, bevor der Datenträger neu beschrieben oder wieder in den Arbeitsdatenträgerpool zurückgestellt werden kann. Dieser Parameter ist wahlfrei. Sie können eine ganze Zahl von 0 bis 9999 angeben. Der Wert 0 bedeutet, dass ein Datenträger wieder beschrieben bzw. als Arbeitsdatenträger zurückgegeben werden kann, sobald alle Dateien auf dem Datenträger gelöscht wurden.
Tipp: Mit diesem Parameter kann sichergestellt werden, dass Datenbankverweise auf Dateien im Pool für aktive Daten noch gültig sind, wenn die Datenbank auf einen früheren Stand zurückgeschrieben wird. Dieser Parameter muss auf einen Wert gesetzt werden, der größer als die Anzahl der Tage ist, die die älteste Datenbanksicherung aufbewahrt werden soll. Die für diesen Parameter angegebene Anzahl Tage muss der im Befehl SET DRMDBBACKUPEXPIREDAYS angegebenen Anzahl entsprechen.

OVFLOcation
Gibt den Überlaufstandort für den Speicherpool an. Der Server ordnet diesen Standortnamen einem Datenträger zu, der durch den Befehl MOVE MEDIA aus dem Kassettenarchiv ausgegeben wird. Dieser Parameter ist wahlfrei. Der Standortname darf maximal 255 Zeichen lang sein. Den Standortnamen in Anführungszeichen einschließen, wenn er Leerzeichen enthält.

Soll ein vorhandener Wert entfernt werden, eine Nullzeichenfolge ("") angeben.

CRCData
: Gibt an, ob eine zyklische Blockprüfung (Cyclic Redundancy Check = CRC) Speicherpooldaten auswertet, wenn auf dem Server eine Datenträgerprüfung (Audit volume) verarbeitet wird. Dieser Parameter ist nur für Speicherpools mit dem Datenformat NATIVE gültig. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Wird CRCDATA auf YES gesetzt und ein Befehl AUDIT VOLUME geplant, kann die Integrität der Daten, die in Ihrer Speicherhierarchie gespeichert sind, ständig sichergestellt werden. Sie können die folgenden Werte angeben:

  Yes
  : Gibt an, dass Daten mit CRC-Informationen gespeichert werden. Damit können bei einer Datenträgerprüfung Speicherpooldaten ausgewertet werden. Dieser Modus hat Auswirkungen auf die Leistung, da eine zusätzliche Verarbeitung erforderlich ist, um die CRC-Werte zu berechnen und zwischen dem Speicherpool und dem Server zu vergleichen.

  No
  : Gibt an, dass Daten ohne CRC-Informationen gespeichert werden.

  Tipp:

  Für Speicherpools, die dem Einheitentyp 3592, LTO oder ECARTRIDGE zugeordnet sind, bietet der Schutz logischer Blöcke einen besseren Schutz vor Datenverlust als die CRC-Überprüfung für einen Speicherpool. Wenn Sie die CRC-Überprüfung für einen Speicherpool angeben, werden Daten nur während der Ausführung von Datenträgerprüfungsoperationen überprüft. Fehler werden identifiziert, nachdem Daten auf Band geschrieben wurden.

  Um den Schutz logischer Blöcke zu aktivieren, geben Sie den Wert READWRITE für den Parameter LBPROTECT in den Befehlen DEFINE DEVCLASS und UPDATE DEVCLASS für den Einheitentyp 3592, LTO oder ECARTRIDGE an. Der Schutz logischer Blöcke wird nur für die folgenden Typen von Laufwerken und Datenträgern unterstützt:

  - IBM® LTO5 und höher
  - IBM 3592-Laufwerke der Generation 3 und höher mit 3592-Datenträgern der Generation 2 und höher
  - Oracle StorageTek T10000C- und T10000D-Laufwerke

DEDUPlicate
: Gibt an, ob die in diesem Speicherpool gespeicherten Daten dedupliziert werden. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind.

IDENTIFYPRocess
: Gibt die Anzahl paralleler Prozesse an, die für die serverseitige Datendeduplizierung verwendet werden sollen. Dieser Parameter ist wahlfrei und nur für Speicherpools gültig, die mit einer Einheitenklasse FILE definiert sind. Geben Sie einen Wert von 1 bis 50 ein. Hinweis: Datendeduplizierungsprozesse können entweder aktiv oder inaktiv sein. Prozesse, die gegenwärtig Dateien bearbeiten, sind aktiv. Prozesse, die auf Dateien warten, die bearbeitet werden sollen, sind inaktiv. Prozesse bleiben inaktiv, bis Datenträger mit Daten, die dedupliziert werden sollen, verfügbar werden. Die Ausgabe des Befehls QUERY PROCESS für einen Datendeduplizierungsprozess umfasst die Gesamtzahl Byte und Dateien, die seit dem ersten Start des Prozesses verarbeitet wurden. Wenn beispielsweise ein Datendeduplizierungsprozess vier Dateien verarbeitet, dann inaktiv wird und anschließend fünf weitere Dateien verarbeitet, beträgt die Gesamtzahl der verarbeiteten Dateien neun. Prozesse werden nur beendet, wenn sie abgebrochen werden oder wenn die Anzahl Datendeduplizierungsprozesse für den Speicherpool in einen Wert geändert wird, der kleiner als die gegenwärtig angegebene Anzahl ist.

Beispiel: Einen Pool für aktive Daten aktualisieren

Den Pool für aktive Daten TAPEPOOL2 aktualisieren, um die Verzögerungszeit für die Datenträgerwiederverwendung in 30 Tage zu ändern und Dateien nach Clientknoten zusammenzufassen.

```
update stgpool tapepool3 reusedelay=30 collocate=node
```

Zugehörige Verweise:
SET DRMDBBACKUPEXPIREDAYS (Verfall für DB-Sicherungsserie angeben)
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

UPDATE STGPOOLDIRECTORY (Speicherpoolverzeichnis aktualisieren)

Mit diesem Befehl kann ein Speicherpoolverzeichnis aktualisiert werden.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Speicherberechtigung oder eingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate STGPOOLDIRectory--Poolname--Verzeichnis--------------->

                                .-MAXPRocess--=--4------.
>----ACCess--=--+-READWrite---+----+----------------------+---->
```

```
                +-READOnly----+    '-MAXProcess--=--Anzahl-'
                +-DEStroyed---+
                '-UNAVailable-'

   .-Wait--=--No------.
>--+------------------+---------------------------------------><
   '-Wait--=--+-No--+-'
              '-Yes-'
```

Parameter

Poolname (Erforderlich)
: Gibt den Speicherpool an, der das zu aktualisierende Verzeichnis enthält. Dieser Parameter ist erforderlich.

Verzeichnis (Erforderlich)
: Gibt ein Dateisystemverzeichnis des Speicherpools an. Dieser Parameter ist erforderlich.

ACCess (Erforderlich)
: Gibt an, wie Clientknoten und Serverprozesse auf Dateien in dem Speicherpoolverzeichnis zugreifen können. Dieser Parameter ist erforderlich. Die folgenden Werte sind gültig:

  READWrite
  : Gibt an, dass Dateien aus dem Speicherpoolverzeichnis gelesen und in das Speicherpoolverzeichnis geschrieben werden können.

  READOnly
  : Gibt an, dass Dateien aus dem Speicherpoolverzeichnis gelesen werden können.

  DEStroyed
  : Gibt an, dass Dateien dauerhaft beschädigt sind und aus dem Speicherpoolverzeichnis gelöscht werden müssen. Verwenden Sie diesen Zugriffsmodus, um anzugeben, dass ein gesamtes Speicherpoolverzeichnis wiederhergestellt werden muss.
    Tipps:

    - Markieren Sie Speicherpoolverzeichnisse als `DESTROYED`, bevor Sie die Datenwiederherstellung ausführen. Wenn das Speicherpoolverzeichnis als DESTROYED markiert ist, können Sie Datenbereiche auf dem Zielreplikationsserver wiederherstellen.
    - Verwenden Sie den Parameter MAXPROCESS, um die Anzahl paralleler Prozesse anzugeben, die Sie zur Aktualisierung eines Speicherpoolverzeichnisses verwenden können.

  UNAVailable
  : Gibt an, dass auf Dateien in dem Speicherpoolverzeichnis im Speicherpool nicht zugegriffen werden kann.

MAXPRocess
: Gibt die maximale Anzahl paralleler Prozesse für die Aktualisierung eines Speicherpoolverzeichnisses an. Dieser Parameter ist wahlfrei. Sie können einen Wert im Bereich von 1 bis 99 angeben. Der Standardwert ist 4.
  Einschränkung: Dieser Parameter kann nur bei Angabe des Parameters ACCESS=DESTROYED verwendet werden.

  Wenn Sie den Parameter ACCESS=DESTROYED angeben, wird jeder Container im Speicherpoolverzeichnis durch einen einzelnen Prozess aktualisiert. Falls die maximale Anzahl paralleler Prozesse größer oder gleich der Anzahl der Container ist, die aktualisiert werden müssen, wird für jeden Container nur ein einzelner Prozess erstellt. Überschreitet die Anzahl der Container den Wert des Parameters MAXPROCESS, wartet der Befehl die Beendigung von untergeordneten Prozessen ab, bevor neue Prozesse beginnen können.

Wait
: Dieser optionale Parameter gibt an, ob darauf gewartet werden soll, dass der IBM Spectrum Protect-Server die Verarbeitung dieses Befehls im Vordergrund beendet. Der Standardwert ist NO. Sie können die folgenden Werte angeben:

  No
  : Der Server verarbeitet diesen Befehl im Hintergrund und Sie können mit anderen Tasks fortfahren, während der Befehl verarbeitet wird. Nachrichten, die sich auf den Hintergrundprozess beziehen, werden entweder in der Aktivitätenprotokolldatei oder an der Serverkonsole angezeigt, je nachdem, wo die Nachrichten protokolliert werden.

  Yes
  : Der Server verarbeitet diesen Befehl im Vordergrund. Die Verarbeitung der Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Nachrichten werden in der Aktivitätenprotokolldatei und/oder an der Serverkonsole angezeigt, abhängig davon, wo die Nachrichten protokolliert werden.
    Einschränkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

Beispiel: Ein Speicherpoolverzeichnis aktualisieren, um es zu löschen

Aktualisieren Sie ein Speicherpoolverzeichnis mit dem Namen DIR1 im Speicherpool POOL1, um es als dauerhaft beschädigt zu markieren.

```
update stgpooldirectory pool1 dir1 access=destroyed
```

Beispiel: Ein Speicherpoolverzeichnis aktualisieren, um es in einem Cloud-Containerspeicherpool zu löschen

Aktualisieren Sie ein Speicherpoolverzeichnis mit dem Namen DIR3 im Cloud-Containerspeicherpool CLOUDLOCALDISK1, um es als gelöscht zu markieren.

```
update stgpooldirectory cloudlocaldisk1 dir3 access=destroyed
```

Beispiel: Ein Speicherpoolverzeichnis aktualisieren, um es als nicht verfügbar zu markieren

Wenn das Speicherpoolverzeichnis nicht verfügbar ist, werden vom Server keine Daten aus dem Verzeichnis gelesen und keine Daten in das Verzeichnis geschrieben. Um den Zugriffsmodus für das Speicherpoolverzeichnis `dir1` in dem Speicherpool `pool1` in 'nicht verfügbar' zu aktualisieren, geben Sie den folgenden Befehl aus:

```
update stgpooldirectory pool1 dir1 access=unavailable
```

Tabelle 1. Zugehörige Befehle für UPDATE STGPOOLDIRECTORY

Befehl	Beschreibung
DEFINE STGPOOL	Definiert einen Speicherpool als benannte Sammlung von Serverspeicherdatenträgern.
DEFINE STGPOOLDIRECTORY	Definiert ein Speicherpoolverzeichnis für einen Verzeichniscontainer- oder Cloud-Containerspeicherpool.
DELETE STGPOOLDIRECTORY	Löscht ein Speicherpoolverzeichnis aus einem Verzeichniscontainer- oder Cloud-Containerspeicherpool.
QUERY STGPOOLDIRECTORY	Zeigt Informationen zu Speicherpoolverzeichnissen an.

UPDATE VIRTUALFSMAPPING (Zuordnung eines virtuellen Dateibereichs aktualisieren)

Verwenden Sie diesen Befehl, um eine Definition für die Zuordnung des virtuellen Dateibereichs zu aktualisieren.

Einschränkung: Sie können den Befehl UPDATE VIRTUALFSMAPPING nicht verwenden, um eine Zuordnung des virtuellen Dateibereichs für eine EMC Celerra- oder EMC VNX-NAS-Einheit zu aktualisieren. Sie müssen den Befehl DEFINE VIRTUALFSMAPPING verwenden.

Der NAS-Einheit muss eine Definition für eine Einheit zum Versetzen von Daten zugeordnet sein, da bei der Aktualisierung der Zuordnung eines virtuellen Dateibereichs durch den Server der Server die NAS-Einheit anspricht, um das virtuelle Dateisystem und den Dateisystemnamen zu prüfen.

Berechtigungsklasse

Um diesen Befehl auszugeben, muss der Benutzer eine der folgenden Berechtigungsklassen haben:

- Systemberechtigung
- Uneingeschränkte Maßnahmenberechtigung
- Eingeschränkte Maßnahmenberechtigung für die Domäne, der der NAS-Knoten zugeordnet ist

Syntax

```
>>-UPDate VIRTUALFSMapping--Knotenname--Name_des_virtuellen_Dateibereichs-->

>--+--------------------------------------+--------------------->
   '-FILESystem--=--neuer_Dateisystemname-'

>--+-------------------------------------------------------------+-><
   |                          .-NAMEType--=--SERVER----------.  |
   '-PATH--=--neuer_Pfadname--+------------------------------+-'
                              '-NAMEType--=--+-SERVER------+-'
                                             '-HEXadecimal-'
```

Parameter

Knotenname (Erforderlich)

Gibt den NAS-Knoten an, auf dem sich das Dateisystem und der Pfad befinden. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

Name_des_virtuellen_Dateibereichs (Erforderlich)

Gibt die zu aktualisierende Zuordnung des virtuellen Dateibereichs an. Sie können keine Platzhalterzeichen verwenden und keine Liste mit Namen angeben.

FILESystem

Gibt den neuen Namen des Dateisystems an, in dem sich der Pfad befindet. Der Dateisystemname muss auf dem angegebenen NAS-Knoten vorhanden sein. Der Dateisystemname darf keine Platzhalterzeichen enthalten. Der Dateisystemname sollte nur geändert werden, wenn der Dateisystemname auf der NAS-Einheit geändert wird oder wenn beispielsweise das Verzeichnis in ein anderes Dateisystem versetzt wird. Dieser Parameter ist wahlfrei.

PATH

Gibt den neuen Pfad vom Stamm des Dateisystems zum Verzeichnis an. Der Pfad kann nur auf ein Verzeichnis verweisen. Der Pfad sollte nur geändert werden, wenn der Pfad auf der NAS-Einheit geändert wurde; beispielsweise, wenn das Verzeichnis in einen anderen Pfad versetzt wird. Die maximale Länge des Pfads beträgt 1024 Zeichen. Bei dem Pfadnamen muss die Groß-/Kleinschreibung beachtet werden. Dieser Parameter ist wahlfrei.

NAMEType

Gibt an, wie der Server den angegebenen Pfadnamen interpretieren soll. Geben Sie diesen Parameter nur an, wenn Sie einen Pfad angeben. Dieser Parameter ist nützlich, wenn ein Pfad Zeichen enthält, die nicht Teil der Codepage sind, in der der Server ausgeführt wird. Der Standardwert lautet SERVER.

Gültige Werte:

SERVER
: Die Codepage, in der der Server ausgeführt wird, wird zum Interpretieren des Pfads verwendet.

HEXadecimal
: Der Server interpretiert den eingegebenen Pfad als hexadezimale Darstellung des Pfads. Diese Option sollte verwendet werden, wenn ein Pfad Zeichen enthält, die nicht eingegeben werden können. Diese Situation kann beispielsweise auftreten, wenn für das NAS-Dateisystem eine Sprache definiert ist, die von der Sprache abweicht, in der der Server ausgeführt wird.

Beispiel: Den Pfad für die Zuordnung des virtuellen Dateibereichs ändern

Die Zuordnung des virtuellen Dateibereichs mit dem Namen /mikeshomedir für den NAS-Knoten NAS1 aktualisieren, indem der Pfad geändert wird.

```
update virtualfsmapping nas1 /mikeshomedir path=/new/home/mike
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE VIRTUALFSMAPPING

Befehl	Beschreibung
DEFINE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs definieren.
DELETE VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs löschen.
QUERY VIRTUALFSMAPPING	Zuordnung eines virtuellen Dateibereichs abfragen.

UPDATE VOLHISTORY (History-Daten für sequentielle Datenträger aktualisieren)

Mit diesem Befehl können Datenträgerhistorydaten für einen Datenträger aktualisiert werden, der durch eine Datenbanksicherungs- oder Exportoperation erstellt wurde. Dieser Befehl gilt nicht für Speicherpooldatenträger.

Verwenden Sie den Befehl UPDATE BACKUPSET, um angegebene Datenträgerinformationen für Sicherungsgruppen in der Protokolldatei für Datenträger zu aktualisieren. Sie dürfen nicht diesen Befehl UPDATE VOLHISTORY verwenden, um Datenträgerinformationen für Sicherungsgruppen in der Protokolldatei für Datenträger zu aktualisieren.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung oder uneingeschränkte Speicherberechtigung erforderlich.

Syntax

```
>>-UPDate VOLHistory--Datenträgername---------------------------->

>--DEVclass--=--Einheitenklassenname---------------------------->

>--+-----------------------+------------------------------------>
   '-LOcation--=--Standort-'

>--+-----------------------------------+----------------------><
   '-ORMSTate--=--+-MOuntable-------+-'
```

```
+-NOTMOuntable----+
+-COUrier---------+
+-VAult-----------+
'-COURIERRetrieve-'
```

Parameter

Datenträgername (Erforderlich)
: Gibt den Datenträgernamen an. Der Datenträger muss für eine Datenbanksicherung oder eine Exportoperation verwendet worden sein.

DEVclass (Erforderlich)
: Gibt den Namen der Einheitenklasse für den Datenträger an.

LOcation
: Gibt den Standort des Datenträgers an. Dieser Parameter ist erforderlich, wenn der Parameter ORMSTATE nicht angegeben wird. Die maximale Textlänge beträgt 255 Zeichen. Den Text in Anführungszeichen einschließen, wenn er Leerzeichen enthält.
Tipp: Der Befehl UPDATE VOLHISTORY unterstützt Aktualisierungen von Standortinformationen und ORMSTATE für Datenträger für Datenbankmomentaufnahmesicherungen.

ORMSTate
: Gibt eine Änderung im Status eines Datenbanksicherungsdatenträgers an. Dieser Parameter ist erforderlich, wenn der Parameter LOCATION nicht angegeben wird. Dieser Parameter wird nur für Systeme unterstützt, die mit Disaster Recovery Manager lizenziert sind. Gültige Statusangaben sind:

  MOuntable
  : Der Datenträger enthält gültige Daten und kann für die Verarbeitung vor Ort verwendet werden.

  NOTMOuntable
  : Der Datenträger ist vor Ort, enthält gültige Daten und kann nicht für die Verarbeitung vor Ort verwendet werden.

  COUrier
  : Der Datenträger wird ausgelagert.

  VAult
  : Der Datenträger ist ausgelagert, enthält gültige Daten und kann nicht für die Verarbeitung vor Ort verwendet werden.

  COURIERRetrieve
  : Der Datenträger wird versetzt, so dass er wieder vor Ort ist.

Beispiel: Den Standort eines Datenträgers aktualisieren, der für die Datenbanksicherung verwendet wird

In die Standortinformationen des Datenträgers BACKUP1, der für eine Datenbanksicherung verwendet wurde, soll die Angabe aufgenommen werden, dass der Datenträger ausgelagert wurde.

```
update volhistory backup1 devclass=tapebkup
location="700 w. magee rd."
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE VOLHISTORY

Befehl	Beschreibung
BACKUP VOLHISTORY	Zeichnet Datenträger-History-Daten in externen Dateien auf.
DELETE VOLHISTORY	Löscht History-Daten sequenzieller Datenträger aus der Datenträger-History-Datei.
MOVE DRMEDIA	Versetzt DRM-Datenträger vor Ort und lagert sie aus.
PREPARE	Erstellt eine Wiederherstellungsplandatei.
QUERY DRMEDIA	Zeigt Informationen zu Datenträgern für die Wiederherstellung nach einem Katastrophenfall an.
QUERY VOLHISTORY	Zeigt History-Daten sequenzieller Datenträger an, die vom Server gesammelt wurden.

UPDATE VOLUME (Speicherpooldatenträger ändern)

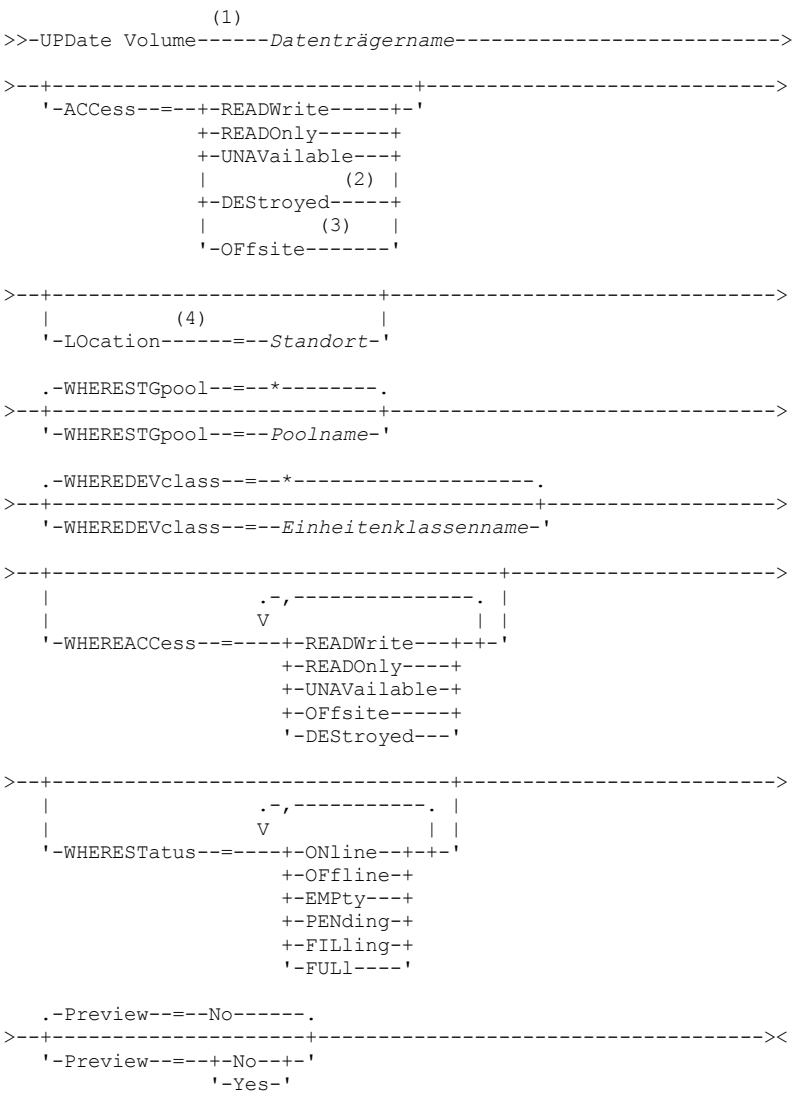
Mit diesem Befehl kann der Zugriffsmodus für einen oder mehrere Datenträger in Speicherpools geändert werden.

Eine Fehlerbedingung, die sich auf einen Datenträger bezieht, kann korrigiert werden, indem dem Datenträger der Zugriffsmodus READWRITE zugeordnet wird. Mit diesem Befehl lassen sich außerdem die Standortinformationen für einen oder mehrere Datenträger in Speicherpools mit sequentiellem Zugriff ändern.

Berechtigungsklasse

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

Syntax



Anmerkungen:

1. Mindestens ein Attribut (ACCESS oder LOCATION) muß aktualisiert werden.
2. Dieser Wert ist nur für Datenträger in primären Speicherpools gültig.
3. Dieser Wert ist nur für Datenträger in Kopienspeicherpools gültig.
4. Dieser Parameter ist nur für Datenträger in Speicherpools mit sequentiellem Zugriff gültig.

Parameter

Datenträgername (Erforderlich)
Gibt den Speicherpooldatenträger an, der aktualisiert werden soll. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

ACCess
Gibt an, wie Clientknoten und Serverprozesse (wie Umlagerung) auf Dateien auf dem Speicherpooldatenträger zugreifen können. Dieser Parameter ist wahlfrei. Gültige Werte:

READWrite
Gibt an, dass Clientknoten und Serverprozesse Lese- und Schreibzugriff auf Dateien des Datenträgers haben.

Handelt es sich bei dem zu aktualisierenden Datenträger um einen leeren Arbeitsdatenträger, der den Zugriffsmodus OFFSITE (ausgelagert) hatte, löscht der Server den Datenträger aus der Datenbank.

READOnly
Gibt an, daß Client-Knoten und Server-Prozesse nur Lesezugriff auf Dateien des Datenträgers haben.

Handelt es sich bei dem zu aktualisierenden Datenträger um einen leeren Arbeitsdatenträger, der den Zugriffsmodus OFFSITE (ausgelagert) hatte, löscht der Server den Datenträger aus der Datenbank.

UNAVailable
Gibt an, dass weder Clientknoten noch Serverprozesse Zugriff auf Dateien haben, die auf dem Datenträger gespeichert sind.

Bevor ein Datenträger mit wahlfreiem Zugriff als nicht verfügbar gekennzeichnet wird, muß der Datenträger abgehängt werden. Nachdem ein Datenträger mit wahlfreiem Zugriff als nicht verfügbar gekennzeichnet wurde, kann der Datenträger nicht angehängt werden.

Wird ein Datenträger mit sequentiellem Zugriff als nicht verfügbar gekennzeichnet, versucht der Server nicht, den Datenträger zu laden.

Handelt es sich bei dem zu aktualisierenden Datenträger um einen leeren Arbeitsdatenträger, der den Zugriffsmodus OFFSITE (ausgelagert) hatte, löscht der Server den Datenträger aus der Datenbank.

DEStroyed
Gibt an, daß ein Datenträger für einen primären Speicherpool auf Dauer zerstört ist. Weder Client-Knoten noch Server-Prozesse können auf Dateien zugreifen, die auf dem Datenträger gespeichert sind. Mit diesem Zugriffsmodus kann angezeigt werden, dass ein gesamter Datenträger mit Hilfe des Befehls RESTORE STGPOOL zurückgeschrieben werden muss. Nachdem alle Dateien auf einem zerstörten Datenträger auf andere Datenträger zurückgeschrieben wurden, löscht der Server automatisch den zerstörten Datenträger aus der Datenbank.

Nur Datenträger in primären Speicherpools können in DESTROYED aktualisiert werden.

Bevor ein Datenträger mit wahlfreiem Zugriff in DESTROYED aktualisiert wird, muß der Datenträger abgehängt werden. Nachdem ein Datenträger mit wahlfreiem Zugriff in DESTROYED aktualisiert wurde, kann der Datenträger nicht angehängt werden.

Wird ein Datenträger mit sequentiellem Zugriff in DESTROYED aktualisiert, versucht der Server nicht, den Datenträger zu laden.

Enthält ein Datenträger keine Dateien und wird der Zugriffsmodus in DESTROYED geändert, löscht der Server den Datenträger aus der Datenbank.

OFfsite
Gibt an, dass sich ein Datenträger eines Kopienspeicherpools oder Speicherpools für aktive Daten an einem ausgelagerten Standort befindet, an dem er nicht geladen werden kann. Nur Datenträger in Kopienspeicherpools oder Speicherpools für aktive Daten können den Zugriffsmodus OFFSITE haben.

Werden für beide Parameter (ACCESS und LOCATION) Werte angegeben, kann jedoch der Zugriffsmodus für einen bestimmten Datenträger nicht geändert werden, dann wird auch das Attribut für den Datenträgerstandort nicht geändert. Wird beispielsweise ACCESS=OFFSITE und ein Wert für LOCATION für einen Datenträger aus dem primären Speicherpool angegeben, wird weder der Wert für den Zugriff noch der Wert für den Standort aktualisiert, da einem Datenträger aus dem primären Speicherpool nicht der Zugriffsmodus OFFSITE zugeordnet werden kann.

LOcation
Gibt den Standort des Datenträgers an. Dieser Parameter ist wahlfrei. Er kann nur für Datenträger in Speicherpools mit sequenziellem Zugriff angegeben werden. Die maximale Länge des Standorts beträgt 255 Zeichen. Wenn die Beschreibung des Standorts Leerzeichen enthält, muß sie in Anführungszeichen stehen. Soll ein zuvor definierter Standort entfernt werden, eine Nullzeichenfolge ("") angeben.

WHERESTGpool
Gibt den Namen des Speicherpools an, dessen Dateien aktualisiert werden sollen. Mit diesem Parameter kann die Aktualisierung auf den gewünschten Speicherpool beschränkt werden. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Speicherpoolname angegeben, werden die Datenträger aller Speicherpools aktualisiert.

WHEREDEVclass
Gibt den Namen der Einheitenklasse für die zu aktualisierenden Datenträger an. Mit diesem Parameter kann die Aktualisierung auf die gewünschte Einheitenklasse beschränkt werden. Dieser Parameter ist wahlfrei. Namen können mit Hilfe von Platzhalterzeichen angegeben werden. Wird kein Einheitenklassenname angegeben, werden Datenträger mit beliebiger Einheitenklasse aktualisiert.

WHEREACCess
Gibt den aktuellen Zugriffsmodus der zu aktualisierenden Datenträger an. Mit diesem Parameter kann die Aktualisierung auf Datenträger beschränkt werden, die gegenwärtig den angegebenen Zugriffsmodus haben. Dieser Parameter ist wahlfrei. Es können mehrere Zugriffsmodi angegeben werden, indem die Modi ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, wird die Aktualisierung nicht auf den aktuellen Zugriffsmodus eines Datenträgers beschränkt. Gültige Werte:

READWrite
Datenträger mit dem Zugriffsmodus READWRITE aktualisieren.

READOnly
Datenträger mit dem Zugriffsmodus READONLY aktualisieren.

UNAVailable
Datenträger mit dem Zugriffsmodus UNAVAILABLE aktualisieren.

OFfsite
Datenträger mit dem Zugriffsmodus OFFSITE aktualisieren.

DEStroyed
Datenträger mit dem Zugriffsmodus DESTROYED aktualisieren.

WHERESTatus
: Gibt den Status der zu aktualisierenden Datenträger an. Mit diesem Parameter kann die Aktualisierung auf Datenträger beschränkt werden, die einen angegebenen Status haben. Dieser Parameter ist wahlfrei. Es können mehrere Statuswerte angegeben werden, indem die Werte ohne Leerzeichen durch Kommas voneinander getrennt werden. Wird kein Wert für diesen Parameter angegeben, wird die Aktualisierung nicht auf einen Datenträgerstatus beschränkt. Gültige Werte:

  ONline
  : Datenträger mit dem Status ONLINE aktualisieren.

  OFfline
  : Datenträger mit dem Status OFFLINE aktualisieren.

  EMPty
  : Datenträger mit dem Status EMPTY aktualisieren.

  PENding
  : Datenträger mit dem Status PENDING aktualisieren. Dabei handelt es sich um Datenträger, deren sämtliche Dateien gelöscht wurden, bei denen die für den Parameter REUSEDELAY angegebene Zeitspanne jedoch noch nicht abgelaufen ist.

  FILling
  : Datenträger mit dem Status FILLING aktualisieren.

  FULl
  : Datenträger mit dem Status FULL aktualisieren.

Preview
: Gibt an, ob die Aktualisierungsoperation vorab angezeigt werden soll, ohne Datenträger tatsächlich zu aktualisieren. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, daß die Datenträger tatsächlich aktualisiert werden sollen.

  Yes
  : Gibt an, daß die Aktualisierungsoperation nur vorab angezeigt werden soll. Bei dieser Option werden die Datenträger, die aktualisiert werden sollen, zum Zeitpunkt der Operationsausführung angezeigt.

Beispiel: Einen Banddatenträger nicht verfügbar machen

Den Banddatenträger DSMT20 aktualisieren, um ihn für Client-Knoten und Server-Prozesse als nicht verfügbar zu kennzeichnen.

```
update volume dsmt20 access=unavailable
```

Beispiel: Den Zugriffsmodus aller ausgelagerten Datenträger in einem bestimmten Speicherpool aktualisieren

Alle leeren, ausgelagerten Datenträger im Speicherpool TAPEPOOL2 aktualisieren. Der Zugriffsmodus soll auf READWRITE gesetzt werden; außerdem sollen die Standortinformationen für die aktualisierten Datenträger gelöscht werden.

```
update volume * access=readwrite location="" wherestgpool=tapepool2
    whereaccess=offsite wherestatus=empty
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für UPDATE VOLUME

Befehl	Beschreibung
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
DELETE VOLUME	Löscht einen Datenträger aus einem Speicherpool.
QUERY VOLUME	Zeigt Informationen über Speicherpooldatenträger an.
VARY	Gibt an, ob ein Plattendatenträger für die Verwendung durch den Server verfügbar ist.

VALIDATE-Befehle

Mit dem Befehl VALIDATE kann überprüft werden, ob ein Objekt für IBM Spectrum Protect vollständig oder gültig ist.

- Linux-BetriebssystemeVALIDATE ASPERA (Aspera FASP-Konfiguration validieren)
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeVALIDATE CLOUD (Cloudberechtigungsnachweise prüfen)
- VALIDATE LANFREE (LAN-unabhängige Pfade prüfen)
- VALIDATE POLICYSET (Maßnahmengruppe prüfen)
- VALIDATE REPLICATION (Replikation für einen Clientknoten überprüfen)
- VALIDATE REPLPOLICY (Die Maßnahmen auf dem Zielreplikationsserver prüfen)

Linux-Betriebssysteme

VALIDATE ASPERA (Aspera FASP-Konfiguration validieren)

Mit diesem Befehl können Sie ermitteln, ob die Aspera FASP-Technologie (FASP = Fast Adaptive Secure Protocol) verwendet werden kann, um die Datenübertragung in Ihrer Systemumgebung zu optimieren. Sie können insbesondere feststellen, ob die Aspera FASP-Technologie einen besseren Netzdurchsatz als die TCP/IP-Technologie erzielen würde.

Dieser Befehl prüft außerdem die folgenden Aspekte:

- Ordnungsgemäße Konfiguration der Systemumgebung für die Verwendung der Aspera FASP-Technologie
- Installation der erforderlichen Lizenzen für die Aktivierung der Aspera FASP-Technologie

Mit der Aspera FASP-Technologie wird die Datenübertragung für die Knotenreplikation oder den Speicherpoolschutz in einem Weitverkehrsnetz (WAN) optimiert. Ihr System muss jedoch nicht zwingend für die Knotenreplikation oder den Speicherpoolschutz konfiguriert sein, damit der Befehl VALIDATE ASPERA ausgeführt werden kann. Falls Ihr System für die Knotenreplikation oder den Speicherpoolschutz in einer lokalen Umgebung konfiguriert ist, können Sie durch Ausgabe des Befehls bewerten, ob die Daten auf einem fernen Server erfolgreich repliziert werden können.

Dieser Befehl ist nur bei Linux x86_64-Betriebssystemen verfügbar.

Führen Sie die folgenden Tasks aus, bevor Sie den Befehl ausgeben:

1. Stellen Sie sicher, dass in Ihrer Systemumgebung mindestens ein Server definiert ist. Geben Sie den Befehl PING SERVER aus, um sicherzustellen, dass Konnektivität zum definierten Server besteht. Geben Sie beispielsweise für einen Server namens VMRH6T den folgenden Befehl aus:

   ```
   ping server vmrh6t
   ```

2. Um den Befehl VALIDATE ASPERA zur Ermittlung der Netzdurchsatzgeschwindigkeit einzusetzen, installieren Sie auf dem Quellen- und dem Zielserver Testlizenzen mit einer Gültigkeit von 30 Tagen oder uneingeschränkte Volllizenzen. Installieren Sie beispielsweise Lizenzen auf dem Quellenserver und dem Zielserver VMRH6 bzw. VMRH6T. Im Abschnitt Bestimmen, ob Aspera FASP-Technologie die Datenübertragung in Ihrer Systemumgebung optimieren kann ist beschrieben, wie Sie Lizenzen beziehen und installieren können.

Um eine Umgebung zu simulieren, die mehrere Sitzungen verwendet, können Sie mehrere Instanzen des Befehls VALIDATE ASPERA gleichzeitig ausführen. Falls Sie die Ausführung mehrerer Sitzungen planen, kann es sinnvoll sein, die Bandbreite jeder Netzverbindung zu begrenzen, um sicherzustellen, dass für alle Netzverbindungen ausreichend Bandbreite verfügbar ist. Zum Begrenzen der Bandbreite geben Sie die Serveroption FASPTARGETRATE wie im Abschnitt FASPTARGETRATE beschrieben an.

Sie können das aktuelle Übertragungsvolumen abfragen, indem Sie den Befehl QUERY PROCESS ausgeben:

```
query process
```

Die Prozessnummer können Sie der Ausgabe des Befehls QUERY PROCESS entnehmen. Sie können den Prozess abbrechen, indem Sie den Befehl CANCEL PROCESS ausgeben und hierbei die Prozessnummer angeben. Beispiel:

```
cancel process 3
```

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-VALidate ASPera--+--------------------+---------------------->
                    '---Zielservername---'

                               .-Wait--=--No------.
>--+-----------------------+--+------------------+-------------><
   '-DURation--=--Sekunden-'  '-Wait--=--+-No--+-'
                                         '-Yes-'
```

Parameter

Zielservername
: Gibt einen zuvor definierten Server an. Dieser Parameter ist wahlfrei. Für die Angabe dieses Parameters gelten die folgenden Richtlinien:

  - Um festzustellen, ob Aspera FASP einen Knotenreplikationsprozess optimieren kann, geben Sie einen Zielserver an, der für die Knotenreplikation konfiguriert ist.
  - Um festzustellen, ob Aspera FASP einen Speicherpoolschutzprozess optimieren kann, geben Sie einen Zielserver an, der für den Speicherpoolschutz konfiguriert ist.

- Um festzustellen, ob Aspera FASP die Datenübertragung an einen fernen Server optimieren kann, der definiert, aber nicht für den Speicherpoolschutz oder die Knotenreplikation konfiguriert ist, geben Sie diesen Zielserver an.
- Falls Sie keinen Zielserver angeben, besagt die Befehlsausgabe, ob der Quellenserver ordnungsgemäß für die Datenübertragung mit Aspera FASP konfiguriert ist. In der Ausgabe ist außerdem angegeben, ob auf dem Quellenserver eine gültige Lizenz für Aspera FASP installiert ist.

DURation
: Gibt in Sekunden die zur Auswertung des Durchsatzes zugeordnete Zeit für die Übertragung von Daten im Netz an. Dieser Parameter ist wahlfrei. Der Standardwert ist 120 Sekunden. Sie können einen Wert im Bereich von 120 bis 3600000 Sekunden angeben. Die zugeordnete Zeit wird zwischen Aspera FASP- und TCP/IP-Datenübertragungen aufgeteilt.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Befehlsverarbeitung beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

  No
  : Gibt an, dass der Server den Befehl im Hintergrund verarbeitet. Während der Verarbeitung des Befehls können andere Tasks ausgeführt werden. Bei Angabe von NO werden die Ausgabenachrichten im Aktivitätenprotokoll angezeigt.

  Yes
  : Gibt an, dass der Server den Befehl im Vordergrund verarbeitet. Die Verarbeitung der Operation muss beendet sein, bevor mit anderen Tasks fortgefahren werden kann. Bei Angabe von YES werden die Ausgabenachrichten im Verwaltungsbefehlszeilenclient angezeigt.
  Einschränkung: Sie können nicht WAIT=YES an der Serverkonsole angeben.

Beispiel: Informationen zum Status einer Aspera FASP-Konfiguration anzeigen

Führen Sie auf dem Quellenserver den Befehl `VALIDATE ASPERA` aus. Um sicherzustellen, dass Nachrichten im Verwaltungsbefehlszeilenclient angezeigt werden, geben Sie WAIT=YES an. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
validate aspera wait=yes
```

```
ANR3836I Überprüfung der Aspera FASP-Verbindung von VMRH6 zu localhost.
Mit FASP übertragenes Volumen: 0 MB pro Sekunde. Mit TCP/IP übertragenes
Volumen: 0 MB pro Sekunde. Latenzzeit: 0 Mikrosekunden. Status: OK. Tage bis
zum Ablauf der Lizenz: Never.
```

Beispiel: Installation der erforderlichen Lizenzen überprüfen

Führen Sie auf dem Quellenserver den Befehl `VALIDATE ASPERA` aus und geben Sie den Zielreplikationsserver an. Um sicherzustellen, dass Nachrichten im Verwaltungsbefehlszeilenclient angezeigt werden, geben Sie WAIT=YES an. Für Feldbeschreibungen siehe Feldbeschreibungen.

```
validate aspera vmrh6t wait=yes
```

```
ANR0984I Prozess 8 für VALIDATE ASPERA im FOREGROUND um 09:35:21
AM gestartet.
ANR3672E Die Lizenzdatei, die zum Aktivieren der Aspera FASP-Technologie
(FASP = Fast Adaptive Secure Protocol) erforderlich ist, wurde auf dem
Server VMRH6 nicht gefunden.
ANR3836I Überprüfung der Aspera FASP-Verbindung von VMRH6 zu localhost.
Mit FASP übertragenes Volumen: 0 MB pro Sekunde. Mit TCP/IP übertragenes
Volumen: 0 MB pro Sekunde. Latenzzeit: 0 Mikrosekunden. Status: Ungültige
Konfiguration. Tage bis zum Ablauf der Lizenz: Abgelaufen.
ANR0985I Prozess 8 für VALIDATE ASPERA, der im FOREGROUND ausgeführt wird, mit
Beendigungsstatus FAILURE um 09:35:21 AM beendet.
ANR1893E Prozess 8 für VALIDATE ASPERA wurde mit dem Beendigungsstatus
FAILURE beendet.
```

Feldbeschreibungen

Status
: Der Status der Konfiguration. Die folgenden Werte sind gültig:

- `OK` gibt an, dass keine Probleme erkannt wurden.
- `Ungültige Konfiguration` gibt an, dass eine Konfigurationsdatei, eine Lizenzdatei oder eine Aspera FASP-Bibliotheksdatei fehlt.
- `Lizenzproblem` gibt an, dass eine Lizenz fehlt, ungültig ist oder abgelaufen ist.
- `Serverfehler` gibt an, dass alle Ports belegt sind, dass ein Fehler beim Schreib-/Lesezugriff im Netz aufgetreten ist oder dass keine Daten in die Aspera FASP-Protokolldatei geschrieben werden können.
- `Ungültige Zielkonfiguration` gibt an, dass eine Konfigurationsdatei, Lizenzdatei oder Aspera FASP-Bibliotheksdatei auf dem Zielserver fehlt.
- `Fehler auf Zielserver` gibt an, dass alle Ports belegt sind, dass ein Fehler beim Schreib-/Lesezugriff im Netz aufgetreten ist oder dass keine Daten in die Aspera FASP-Protokolldatei geschrieben werden können.
- `Lizenzproblem auf Zielserver` gibt an, dass eine Lizenz auf dem Zielserver ungültig oder abgelaufen ist.

- `Nicht unterstütztes Betriebssystem` gibt an, dass auf einem oder beiden Servern ein anderes Betriebssystem als Linux x86_64 installiert ist.
- `Unbekannt` gibt an, dass ein unerwarteter Fehler aufgetreten ist. Prüfen Sie die Protokollnachrichten, um den Fehler zu ermitteln.

Tage bis zum Ablauf der Lizenz
: Die folgenden Werte sind gültig:

- `Never` gibt an, dass eine uneingeschränkte Volllizenz installiert ist.
- `Heute` gibt an, dass eine Testlizenz mit einer Gültigkeit von 30 Tagen installiert ist, die heute abläuft.
- `Abgelaufen` gibt an, dass eine Testlizenz mit einer Gültigkeit von 30 Tagen installiert, jedoch abgelaufen ist.
- Eine *Anzahl* gibt an, dass eine Testlizenz mit einer Gültigkeit von 30 Tagen installiert ist, die in der angegebenen Anzahl von Tagen abläuft.
- `Lizenz nicht gefunden` gibt an, dass keine Lizenz gefunden wurde.

Übertragenes Volumen mit TCP/IP
: Die Geschwindigkeit der Datenübertragung mit TCP/IP-Technologie in Megabyte pro Sekunde.

Übertragenes Volumen mit FASP
: Die Geschwindigkeit der Datenübertragung mit Aspera FASP-Technologie in Megabyte pro Sekunde.

Latenzzeit
: Die Latenzzeit der Datenübertragung in Mikrosekunden.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE ASPERA

Befehl	Beschreibung
CANCEL SESSION	Bricht aktive Sitzungen mit dem Server ab.
DEFINE SERVER	Definiert einen Server für die Übertragung zwischen Servern.
PING SERVER	Testet die Verbindungen zwischen Servern.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemePROTECT STGPOOL	AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeSchützt einen Verzeichniscontainerspeicherpool.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.

VALIDATE CLOUD (Cloudberechtigungsnachweise prüfen)

Bevor Sie einen Speicherpool definieren, verwenden Sie diesen Befehl, um sicherzustellen, dass die Berechtigungsnachweise für einen Cloud-Containerspeicherpool gültig sind und dem Benutzer die erforderlichen Berechtigungen erteilt wurden.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
                    .-CLOUDType--=--SWift---------.
>>-VALidate CLOud--+-----------------------------+-------------->
                    '-CLOUDType--=--+-AZure-----+-'
                                    +-S3--------+
                                    +-SOftlayer-+
                                    +-SWift-----+
                                    '-V1Swift---'

                                                 (1)
>--CLOUDUrl--=--Cloud-URL--IDentity--=--Cloud-ID----------------->

>--PAssword--=--Kennwort--+-------------------------------+---><
                          |                           (2) |
                          '-BUCKETName--=--Bucketname-----'
```

Anmerkungen:

1. Wenn Sie CLOUDTYPE=AZURE angeben, geben Sie nicht den Parameter IDENTITY an.
2. Der Parameter BUCKETNAME ist nur gültig, wenn Sie CLOUDTYPE=S3 angeben.

Parameter

CLOUDType
Gibt den Typ der Cloudumgebung an, in der der Speicherpool konfiguriert wird.
Sie können einen der folgenden Werte angeben:

AZure
Gibt an, dass der Speicherpool ein Cloud-Computing-System 'Microsoft Azure' verwendet.
S3
Gibt an, dass der Speicherpool ein Cloud-Computing-System mit dem Protokoll 'Simple Storage Service' (S3) verwendet, wie z. B. IBM® Cloud Object Storage oder Amazon Web Services (AWS) S3.
SOftlayer
Gibt an, dass der Speicherpool ein Cloud-Computing-System 'IBM SoftLayer' (IBM Bluemix) mit einem Cloud-Computing-System 'OpenStack Swift' verwendet.
SWift
Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 2 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.
V1Swift
Gibt an, dass der Speicherpool ein Cloud-Computing-System 'OpenStack Swift' verwendet. Dieser Wert gibt auch an, dass der Speicherpool Version 1 des Protokolls für die Authentifizierung bei der Cloud verwendet. Die URL der Cloud enthält normalerweise die Versionsnummer des verwendeten Protokolls.

Dieser Parameter ist wahlfrei. Wird der Parameter nicht angegeben, wird der Standardwert SWIFT verwendet.

CLOUDUrl (Erforderlich)
Gibt die URL der Cloudumgebung an, in der Sie den Speicherpool konfigurieren. Auf der Basis Ihres Cloud-Providers können Sie einen BLOB-Dienstendpunkt, eine Regionsendpunkt-URL, eine Accesser-IP-Adresse, einen Endpunkt für öffentliche Authentifizierung (Public Authentication Endpoint) oder einen ähnlichen Wert für diesen Parameter verwenden. Stellen Sie sicher, dass das Protokoll wie z. B. `https://` oder `http://` am Anfang der URL eingefügt wird. Die maximale Länge der Webadresse beträgt 870 Zeichen. Der Parameter CLOUDURL wird geprüft, wenn die erste Sicherung beginnt.

IDentity (Erforderlich)
Gibt die Benutzer-ID für die Cloud an. Dieser Parameter ist für alle unterstützten Cloud-Computing-Systeme außer Azure erforderlich. Wenn Sie CLOUDTYPE=AZURE angeben, geben Sie nicht den Parameter IDENTITY an. Auf der Basis Ihres Cloud-Providers können Sie eine Zugriffsschlüssel-ID, einen Benutzernamen, einen Tenantnamen und Benutzernamen oder einen ähnlichen Wert für diesen Parameter verwenden. Die maximale Länge der Benutzer-ID beträgt 255 Zeichen.

PAssword (Erforderlich)
Gibt das Kennwort für die Cloud an. Auf der Basis Ihres Cloud-Providers können Sie ein SAS-Token (SAS = Shared Access Signature), einen geheimen Zugriffsschlüssel, einen API-Schlüssel, ein Kennwort oder einen ähnlichen Wert für diesen Parameter verwenden. Dieser Parameter ist erforderlich. Die maximale Länge des Kennworts beträgt 255 Zeichen.

BUCKETName
Gibt den Namen für ein AWS S3-Bucket oder eine IBM Cloud Object Storage-Vault an, das bzw. die anstelle des Standardbuckets oder der Standardvault mit diesem Speicherpool verwendet werden soll. Dieser Parameter ist optional und ist nur gültig, wenn Sie CLOUDTYPE=S3 angeben. Wenn ein Bucket oder eine Vault mit dem angegebenen Namen vorhanden ist, wird dieses Bucket oder diese Vault getestet, um sicherzustellen, dass die korrekten Berechtigungen definiert sind. Ist das Bucket oder die Vault nicht vorhanden, wird mit dem Parameter nur verifiziert, dass kein Bucket oder keine Vault mit diesem Namen vorhanden ist. Beachten Sie die Einschränkungen bei der Benennung für Ihren Cloud-Provider, wenn Sie diesen Parameter angeben. Überprüfen Sie die Berechtigungen für das Bucket oder die Vault und stellen Sie sicher, dass die Berechtigungsnachweise über die Berechtigung zum Lesen, Schreiben, Auflisten und Löschen von Objekten in diesem Bucket oder dieser Vault haben.
Tipp: Wird der Parameter BUCKETNAME nicht angegeben, wird die global eindeutige Replikations-ID als Standardbucketname verwendet. Der Standardwert ist

`ibmsp` *`GUID`*

. Dabei ist *GUID* der Wert für REPLICATION GLOBALLY UNIQUE ID, minus der Punkte, in der Ausgabe des Befehls QUERY REPLSERVER. Lautet die global eindeutige Replikations-ID beispielsweise 52.82.39.20.64.d0.11.e6.9d.77.0a.00.27.00.00.00, ist der Standardbucketname ibmsp.5282392064d011e69d770a0027000000.

Beispiel: Berechtigungsnachweise eines S3-Cloud-Containerspeicherpools prüfen

Die Berechtigungsnachweise des Cloud-Containerspeicherpools prüfen.

```
validate cloud
cloudtype=s3 cloudurl=http://123.234.123.234:5000/v2.0
password=protect8991 bucketname=ibmsp.5282392064d011e69d770a0027000000
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE CLOUD

Befehl	Beschreibung
DEFINE STGPOOL (Cloud-Container)	Definiert einen Cloud-Containerspeicherpool.
QUERY REPLSERVER	Zeigt Informationen zu Replikationsservern an.

Befehl	Beschreibung
UPDATE STGPOOL (Cloud-Container)	Aktualisiert einen Cloud-Containerspeicherpool.

VALIDATE LANFREE (LAN-unabhängige Pfade prüfen)

Verwenden Sie diesen Befehl, um zu bestimmen, welche Ziele für einen bestimmten Knoten, der einen spezifischen Speicheragenten verwendet, für die LAN-unabhängige Datenversetzung verwendet werden können.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax

```
>>-VALidate LAnfree--Knotenname--Speicheragentenname-----------><
```

Parameter

Knotenname (Erforderlich)
: Der Name des Knotens, der ausgewertet werden soll.

Speicheragentenname (Erforderlich)
: Der Name des Speicheragenten, der ausgewertet werden soll.

Beispiel: Eine aktuelle LAN-unabhängige Konfiguration prüfen

Die aktuellen Serverdefinitionen und die Konfiguration des Knotens TIGER für die Verwendung des Speicheragenten AIX_STA1 für LAN-unabhängige Datenoperationen prüfen.

```
validate lanfree tiger aix_sta1

Knoten- Speicher- Operation Verw.-   Ziel-      LAN-        Erläuterung
name    agent               Klasse   name       unabhängig?
------ -------- ---------- --------- ---------- --------- -----------
TIGER   AIX_STA1  BACKUP    STANDARD OUTPOOL     NO         Keine verfügbaren
                                                            Onlinepfade.
TIGER   AIX_STA1  BACKUP    STANDARD PRIMARY     NO         Zielspeicher-
                                                            pool ist für
                                                            simultanes
                                                            Schreiben
                                                            konfiguriert.
TIGER   AIX_STA1  BACKUP    STANDARD SHRPOOL     YES
TIGER   AIX_STA1  BACKUP    NOARCH   LFFILE      NO         Speicherpool
                                                            enthält von Clients
                                                            deduplizierte Daten
                                                            und ist für
                                                            Speicheragenten
                                                            V6.1 oder früher
                                                            nicht zugänglich.
TIGER   AIX_STA1  ARCHIVE   STANDARD OUTPOOL     NO         Keine verfügbaren
                                                            Onlinepfade.
TIGER   AIX_STA1  ARCHIVE   STANDARD PRIMARY     NO         Zielspeicher-
                                                            pool ist für
                                                            simultanes
                                                            Schreiben
                                                            konfiguriert.
TIGER   AIX_STA1  ARCHIVE   STANDARD SHRPOOL     YES
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE LANFREE

Befehl	Beschreibung
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.
QUERY DEVCLASS	Zeigt Informationen zu Einheitenklassen an.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
QUERY DRIVE	Zeigt Informationen zu Laufwerken an.
QUERY LIBRARY	Zeigt Informationen zu einem oder zu mehreren Kassettenarchiven an.

Befehl	Beschreibung
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY PATH	Zeigt Informationen zum Pfad von einer Quelle zu einem Ziel an.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
QUERY SERVER	Zeigt Informationen über Server an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
QUERY STGPOOL	Zeigt Informationen zu Speicherpools an.

VALIDATE POLICYSET (Maßnahmengruppe prüfen)

Mit diesem Befehl kann geprüft werden, ob eine Maßnahmengruppe vollständig und gültig ist, bevor sie aktiviert wird. Der Befehl untersucht die Verwaltungsklassen- und Kopiengruppendefinitionen in der Maßnahmengruppe und meldet Bedingungen, die vor der Aktivierung der Maßnahmengruppe berücksichtigt werden müssen.

Der Befehl VALIDATE POLICYSET schlägt fehl, wenn eine der folgenden Bedingungen vorhanden ist:

- Die Maßnahmengruppe hat keine Standardverwaltungsklasse.
- Eine Kopiengruppe in der Maßnahmengruppe gibt einen Kopienspeicherpool als Zielort an.
- Eine Verwaltungsklasse gibt einen Kopienspeicherpool als Zielort für Dateien an, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.
- Ein Parameter TOCDESTINATION ist angegeben, und der Speicherpool ist entweder ein Kopienpool oder der Speicherpool hat ein anderes Format als NATIVE oder NONBLOCK.

Der Server gibt für folgende Bedingungen Warnungen aus:

- Eine Kopiengruppe gibt einen Speicherpool an, der als Zielort für gesicherte oder archivierte Dateien nicht vorhanden ist.

  Wird eine Maßnahmengruppe mit Kopiengruppen aktiviert, die nicht vorhandene Speicherpools angeben, schlagen die Sicherungs- oder Archivierungsoperationen des Clients fehl.

- Eine Verwaltungsklasse gibt einen Speicherpool an, der als Zielort für Dateien, die von IBM Spectrum Protect for Space Management-Clients umgelagert werden, nicht vorhanden ist.
- Die Maßnahmengruppe verfügt nicht über eine oder mehrere Verwaltungsklassen, die in der aktuellen aktiven (ACTIVE) Maßnahmengruppe vorhanden sind.

  Wird die Maßnahmengruppe aktiviert, werden Sicherungsdateien, die an die gelöschten Verwaltungsklassen gebunden sind, erneut an die Standardverwaltungsklasse in der neuen aktiven Maßnahmengruppe gebunden.

- Die Maßnahmengruppe verfügt nicht über eine oder mehrere Kopiengruppen, die in der aktuellen aktiven (ACTIVE) Maßnahmengruppe vorhanden sind.

  Wird die Maßnahmengruppe aktiviert, werden Dateien, die an die Verwaltungsklassen mit den gelöschten Kopiengruppen gebunden sind, nicht mehr archiviert bzw. gesichert.

- Die Standardverwaltungsklasse für die Maßnahmengruppe enthält keine Sicherungs- oder Archivierungskopiengruppe.

  Wird die Maßnahmengruppe mit dieser Standardverwaltungsklasse aktiviert, können Clients, die den Standardwert verwenden, keine Dateien sichern bzw. archivieren.

- Eine Verwaltungsklasse gibt an, daß eine Sicherungsversion vorhanden sein muß, bevor eine Datei aus einem Client-Knoten umgelagert werden kann (MIGREQUIRESBKUP=YES), aber die Verwaltungsklasse enthält keine Sicherungskopiengruppe.

Ist für den Server der Aufbewahrungsschutz für Daten aktiviert, müssen die folgenden Bedingungen zutreffen:

- Alle Verwaltungsklassen in der Maßnahmengruppe, die geprüft werden soll, müssen eine Archivierungskopiengruppe enthalten.
- Ist eine Verwaltungsklasse in der aktiven Maßnahmengruppe vorhanden, muss eine Verwaltungsklasse mit demselben Namen in der Maßnahmengruppe vorhanden sein, die geprüft werden soll.
- Ist eine Archivierungskopiengruppe in der aktiven Maßnahmengruppe vorhanden, muss die entsprechende Kopiengruppe in der zu prüfenden Maßnahmengruppe über einen Wert für RETVER verfügen, der mindestens so groß wie die entsprechenden Werte in der aktiven Kopiengruppe ist.

Berechtigungsklasse

Für diesen Befehl ist Systemberechtigung, uneingeschränkte Maßnahmenberechtigung oder eingeschränkte Maßnahmenberechtigung für die Maßnahmendomäne erforderlich, zu der die Maßnahmengruppe gehört.

Syntax

```
>>-VALidate POlicyset--Domänenname--Name_der_Maßnahmengruppe--->< 
```

Parameter

Domänenname (Erforderlich)
: Gibt den Namen der Maßnahmendomäne an, der die Maßnahmengruppe zugeordnet wird.

Name_der_Maßnahmengruppe (Erforderlich)
: Gibt den Namen der Maßnahmengruppe an, die geprüft werden soll.

Beispiel: Eine bestimmte Maßnahmengruppe prüfen

Die Maßnahmengruppe `VACATION`, die sich in der Maßnahmendomäne `EMPLOYEE_RECORDS` befindet, soll ausgewertet werden.

```
validate policyset employee_records vacation
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE POLICYSET

Befehl	Beschreibung
ACTIVATE POLICYSET	Wertet eine Maßnahmengruppe aus und aktiviert sie.
COPY POLICYSET	Erstellt eine Kopie einer Maßnahmengruppe.
DEFINE COPYGROUP	Definiert eine Kopiengruppe für die Sicherungs- bzw. Archivierungsverarbeitung innerhalb einer angegebenen Verwaltungsklasse.
DEFINE MGMTCLASS	Definiert eine Verwaltungsklasse.
DELETE POLICYSET	Löscht eine Maßnahmengruppe einschließlich ihrer Verwaltungsklassen und Kopiengruppen aus einer Maßnahmendomäne.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
UPDATE COPYGROUP	Ändert ein oder mehrere Attribute einer Kopiengruppe.
UPDATE POLICYSET	Ändert die Beschreibung einer Maßnahmengruppe.

VALIDATE REPLICATION (Replikation für einen Clientknoten überprüfen)

Verwenden Sie diesen Befehl, um die Replikationsregeln zu identifizieren, die für Dateibereiche in Clientknoten gelten, die für die Replikation konfiguriert sind. Sie können mit diesem Befehl auch überprüfen, ob der Quellenreplikationsserver mit dem Zielreplikationsserver kommunizieren kann.

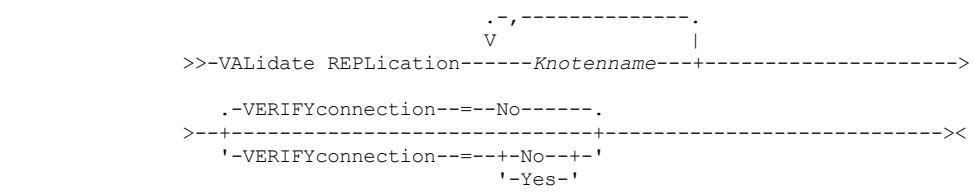
Bevor Sie mit der Replikationsverarbeitung beginnen, verwenden Sie den Befehl VALIDATE REPLICATION, um zu bestimmen, ob Ihre Replikationskonfiguration korrekt ist.

Geben Sie diesen Befehl auf dem Server aus, der als Quelle für replizierte Daten agiert.

Berechtigungsklasse

Für diesen Befehl ist die Systemberechtigung erforderlich.

Syntax



Parameter

Knotenname (Erforderlich)
: Gibt den Namen des Clientknotens an, dessen Dateibereiche angezeigt werden sollen. Werden mehrere Clientknotennamen angegeben, sind die Namen ohne Leerzeichen durch Kommas voneinander zu trennen. Namen können mit Hilfe von Platzhalterzeichen angegeben werden.

  Informationen werden nur zu den Clientknoten angezeigt, die für die Replikation aktiviert oder inaktiviert sind. Der Replikationsmodus muss SEND lauten. Um zu bestimmen, ob ein Clientknoten für die Replikation und ihren Modus aktiviert oder inaktiviert ist, geben Sie den Befehl QUERY NODE aus. Überprüfen Sie die Werte in den Feldern 'Replikationsstatus' und 'Replikationsmodus'.

VERIFYconnection
: Gibt an, ob die Verbindung zu einem Zielreplikationsserver überprüft werden soll. Die Version des Zielreplikationsservers wird ebenfalls überprüft, um sicherzustellen, dass es sich um Version 6.3 oder eine höhere Version handelt. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Sie können einen der folgenden Werte angeben:

  No
  : Die Verbindung und Version des Zielreplikationsservers werden nicht überprüft.

  Yes
  : Die Verbindung und Version des Zielreplikationsservers werden überprüft.

Beispiel: Die Replikation für einen Clientknoten überprüfen

Der Name des Clientknotens ist NODE1. Den Verbindungsstatus zwischen dem Quellen- und dem Zielreplikationsserver überprüfen.

```
validate replication node1 verifyconnection=yes

                      Knotenname: NODE1
                Dateibereichsname: \\node1\c$
                             FSID: 1
                              Typ: Bkup
      Steuernde Replikationsregel: ACTIVE_DATA
           Replikationsregelebene: Systemebene
                      Servername: DRSRV
                Verbindungsstatus: Gültige Verbindung

                      Knotenname: NODE1
                Dateibereichsname: \\node1\c$
                             FSID: 1
                              Typ: Arch
      Steuernde Replikationsregel: ALL_DATA_HIGH_PRIORITY
           Replikationsregelebene: Knotenebene
                      Servername: DRSRV
                Verbindungsstatus: Gültige Verbindung

                      Knotenname: NODE1
                Dateibereichsname: \\node1\c$
                             FSID: 1
                              Typ: SpMg
      Steuernde Replikationsregel: ALL_DATA
           Replikationsregelebene: Systemebene
                      Servername: DRSRV
                Verbindungsstatus: Gültige Verbindung
```

Die Ausgabe wird für alle Datentypen angezeigt, unabhängig davon, ob ein Dateibereich die Datentypen enthält. Beispiel: Enthält ein Dateibereich nur Sicherungs- und Archivierungsdaten, enthält die Ausgabe des Befehls VALIDATE REPLICATION auch Informationen zu speicherverwalteten Daten.

Feldbeschreibungen

Knotenname
: Der Knoten, der der Eigner der replizierten Daten ist.

Dateibereichsname

  Der Name des Dateibereichs, der zu dem Knoten gehört.

  Dateibereichsnamen können eine andere Zeichenumsetztabelle oder Locale als der Server haben. Ist dies der Fall, werden die Namen im Operations Center und in der Verwaltungsbefehlszeilenschnittstelle möglicherweise nicht korrekt angezeigt. Daten werden normal gesichert und können normal zurückgeschrieben werden, der Dateibereichsname oder Dateiname kann jedoch mit einer Kombination ungültiger Zeichen oder Leerzeichen angezeigt werden.

  Ist der Dateibereichsname Unicode-fähig, wird der Name für die Anzeige in die Zeichenumsetztabelle des Servers konvertiert. Der Erfolg der Konvertierung hängt von dem Betriebssystem, den Zeichen im Namen und der Serverzeichenumsetztabelle ab. Die Konvertierung kann unvollständig sein, wenn die Zeichenfolge Zeichen enthält, die in der Serverzeichenumsetztabelle nicht verfügbar sind, oder wenn der

Server nicht auf Systemkonvertierungsroutinen zugreifen kann. Ist die Konvertierung unvollständig, kann der Name Fragezeichen, Leerzeichen, nicht druckbare Zeichen oder Auslassungen (...) enthalten.

FSID
: Die Dateibereichs-ID des Dateibereichs. Der Server ordnet eine eindeutige FSID zu, wenn ein Dateibereich zum ersten Mal auf dem Server gespeichert wird.

Typ
: Der Datentyp. Die folgenden Werte sind gültig:

  Arch
  : Archivierungsdaten

  Bkup
  : Sicherungsdaten

  SpMg
  : Daten, die von einem IBM Spectrum Protect for Space Management-Client umgelagert wurden.

Steuernde Replikationsregel
: Der Name der Replikationsregel, die die Replikation für einen Datentyp in einem Dateibereich steuert. Um zu bestimmen, ob die Steuerungsregel eine Dateibereichsregel, eine Clientregel oder eine Serverregel ist, überprüfen Sie das Feld 'Replikationsregelebene'.

Replikationsregelebene
: Die Ebene der Steuerungsregel in der Replikationsregelhierarchie. Die folgenden Werte sind gültig:

  Dateibereich
  : Die Steuerungsregel ist einem Datentyp in dem Dateibereich zugeordnet.

  Knoten
  : Die Steuerungsregel ist einem Datentyp für einen Clientknoten zugeordnet.

  Server
  : Die Steuerungsregel ist einem Datentyp für alle Dateibereiche in allen Clientknoten zugeordnet, die für die Replikation konfiguriert sind.

Servername
: Der Name des Zielreplikationsservers, der abgefragt werden soll.

Verbindungsstatus
: Der Verbindungsstatus zwischen dem Quellen- und dem Zielreplikationsserver. Die folgenden Werte sind gültig:

  Gültige Verbindung
  : Die Kommunikation mit dem Zielreplikationsserver war erfolgreich und der Zielreplikationsserver ist ein Server mit Version 6.3.

  Zielserver nicht definiert
  : Der Zielreplikationsserver ist nicht definiert. Um den Zielreplikationsserver zu definieren, geben Sie den Befehl SET REPLSERVER aus.

  Übertragungsfehler
  : Der Quellenreplikationsserver konnte den Zielreplikationsserver nicht ansprechen. Überprüfen Sie das Aktivitätenprotokoll auf Fehlernachrichten zur fehlgeschlagenen Übertragung. Ziehen Sie die folgenden möglichen Ursachen in Betracht:

    - Die Replikationskonfiguration auf dem Quellenreplikationsserver ist nicht gültig. Einer oder mehrere der folgenden Fehler können vorhanden sein:
      - Die Serverdefinition für den Zielreplikationsserver ist nicht korrekt.
      - Wurde die Definition des Zielreplikationsservers gelöscht und erneut definiert, geben Sie den Befehl PING SERVER aus, um die Verbindung zwischen dem Quellen- und Zielreplikationsserver zu testen. Ist der Befehl PING SERVER erfolgreich, geben Sie den Befehl UPDATE SERVER aus und geben Sie FORCESYNC=YES an, um die Serverprüfschlüssel zurückzusetzen.
      - Der Servername, die Serveradresse der unteren Ebene, die Serveradresse der höheren Ebene und das Serverkennwort stimmen nicht mit den Werten überein, die in der Serverdefinition auf dem Zielreplikationsserver angegeben sind.
    - Die Replikationskonfiguration auf dem Zielreplikationsserver ist nicht gültig. Einer oder mehrere der folgenden Fehler können vorhanden sein:
      - Die Version des Zielreplikationsservers ist eine Version vor Version 6.3.
      - Die Serverdefinition für den Quellenreplikationsserver ist nicht korrekt.
      - Der Servername, die Serveradresse der unteren Ebene, die Serveradresse der höheren Ebene und das Serverkennwort stimmen nicht mit den Werten überein, die in der Serverdefinition auf dem Quellenreplikationsserver angegeben sind.
    - Die Netzkommunikation ist nicht verfügbar. Um die Verbindung zwischen dem Quellen- und Zielserver zu testen, geben Sie den Befehl PING SERVER aus.
    - Der Zielreplikationsserver ist nicht verfügbar.
    - Sitzungen zwischen dem Quellen- und Zielreplikationsserver sind inaktiviert. Um den Status der Sitzungen zu überprüfen, geben Sie den Befehl QUERY STATUS aus.

  Replikation ausgesetzt
  : Die Replikationsverarbeitung wird ausgesetzt, wenn Sie die Datenbank auf dem Quellenreplikationsserver zurückschreiben oder die Replikationsverarbeitung auf diesem Server mit dem Befehl DISABLE REPLICATION inaktivieren.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE REPLICATION

Befehl	Beschreibung
DISABLE REPLICATION	Verhindert die Verarbeitung abgehender Replikation auf einem Server.
ENABLE REPLICATION	Ermöglicht die Verarbeitung abgehender Replikation auf einem Server.
ENABLE SESSIONS	Nimmt die Serveraktivität nach einem Befehl DISABLE oder ACCEPT DATE wieder auf.
QUERY FILESPACE	Zeigt Informationen zu Daten in Dateibereichen an, die zu einem Client gehören.
QUERY NODE	Zeigt Informationen zu einem oder mehreren Clients teilweise oder vollständig an.
QUERY REPLRULE	Zeigt Informationen zu Knotenreplikationsregeln an.
QUERY SERVER	Zeigt Informationen über Server an.
QUERY STATUS	Zeigt die Einstellungen von Serverparametern an, beispielsweise die mit den SET-Befehlen ausgewählten Einstellungen.
REPLICATE NODE	Repliziert Daten in Dateibereichen, die zu einem Clientknoten gehören.
SET ARREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für Archivierungsdaten an.
SET BKREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für Sicherungsdaten an.
SET REPLSERVER	Gibt einen Zielreplikationsserver an.
SET SPREPLRULEDEFAULT	Gibt die Serverknotenreplikationsregel für speicherverwaltete Daten an.
UPDATE FILESPACE	Ändert Knotenreplikationsregeln für Dateibereiche.
UPDATE NODE	Ändert die Attribute, die einem Clientknoten zugeordnet sind.
UPDATE REPLRULE	Aktiviert oder inaktiviert Replikationsregeln.
UPDATE SERVER	Aktualisiert Informationen über einen Server.

VALIDATE REPLPOLICY (Die Maßnahmen auf dem Zielreplikationsserver prüfen)

Verwenden Sie diesen Befehl, um die Maßnahmen für Clientknoten auf dem Quellenreplikationsserver mit denselben Maßnahmen auf dem Zielreplikationsserver zu vergleichen, auf dem die Clientknotendaten repliziert werden.

Der Befehl zeigt die Unterschiede zwischen diesen Maßnahmen an. Sie können prüfen, ob die Unterschiede zwischen den Maßnahmen auf dem Quellen- und dem Zielreplikationsserver beabsichtigt sind, oder die Maßnahmen auf dem Zielreplikationsserver ändern.

Stellen Sie sicher, dass IBM Spectrum Protect Version 7.1.1 oder höher auf dem Quellen- und Zielreplikationsserver installiert ist, bevor Sie diesen Befehl ausgeben. Geben Sie diesen Befehl auf dem Quellenreplikationsserver aus.

Berechtigungsklasse

Jeder Administrator kann diesen Befehl ausgeben.

Syntax

```
>>-VALidate REPLPolicy--+------------+-------------------------><
                        '-Servername-'
```

Parameter

Servername
: Gibt den Namen des Zielreplikationsservers an, der über Maßnahmen verfügt, die geprüft werden sollen. Dieser Parameter ist wahlfrei. Wenn Sie diesen Parameter nicht angeben, definiert der Befehl den Standardreplikationsserver als Zielreplikationsserver.

Beispiel: Die Unterschiede zwischen den Replikationsmaßnahmen auf einem Quellen- und Zielreplikationsserver anzeigen

Um die Unterschiede zwischen den Maßnahmen auf dem Quellenreplikationsserver und den Maßnahmen auf dem Zielreplikationsserver CVTCVS_LXS_SRV2 anzuzeigen, auf dem die Clientdaten repliziert werden, geben Sie den folgenden Befehl auf dem Quellenreplikationsserver aus:

```
VALIDATE REPLPOLICY CVTCVS_LXS_SRV2

Name der Maßnahmendomäne            Name der Maßnahmendomäne auf       Name des Zielservers
auf diesem Server                   dem Zielserver
--------------------------  ----------------------  -----------------
STANDARD                            STANDARD                           CVTCVS_LXS_SRV2

Unterschiede in Maßnahmengruppe:
Änderung erkannt                    Wert für Quellenserver             Wert für Zielserver
--------------------------  ----------------------  -----------------
Verwaltungsklasse nur auf Ziel      Nicht zutreffend                   STANDARD2
Verwaltungsklasse nur auf Quelle    STANDARD1                          Nicht zutreffend

Unterschiede in Sicherungskopien-   STANDARD in                        STANDARD
gruppe                              Verwaltungsklasse
Änderung erkannt                    Wert für Quellenserver             Wert für Zielserver
--------------------------  ----------------------  ------------------
Versionen bestehender Daten         2                                  20


Betroffene Knoten
-------------------------------------------------------------------------
NODE1,NODE2,NODE3,NODE4,NODE5
```

Feldbeschreibungen

Name der Maßnahmendomäne auf diesem Server
: Gibt den Namen der Maßnahmendomäne auf dem Quellenreplikationsserver an, auf dem der Befehl ausgegeben wird.

Name der Maßnahmendomäne auf dem Zielserver
: Gibt den Namen der Maßnahmendomäne auf dem Zielreplikationsserver an.

Name des Zielservers
: Gibt den Namen des Zielreplikationsservers an.

Unterschiede in Maßnahmengruppe:
: Gibt die Unterschiede zwischen den Maßnahmen an, die auf dem Quellen- und dem Zielreplikationsserver definiert sind. Die Unterschiede zwischen den Maßnahmen werden unter den folgenden Feldern aufgelistet:

  Änderung erkannt
  : Gibt die Liste der Maßnahmenelemente an, die auf dem Quellen- und dem Zielreplikationsserver unterschiedlich sind.

  Wert für Quellenserver
  : Gibt den Wert für das Maßnahmenelement auf dem Quellenreplikationsserver an.

  Wert für Zielserver
  : Gibt den Wert für das Maßnahmenelement auf dem Zielreplikationsserver an.

Unterschiede in Sicherungskopiengruppe <Name der Sicherungskopiengruppe> in Standardverwaltungsklasse ODER Unterschiede in Archivierungskopiengruppe <Name der Archivierungskopiengruppe> in Standardverwaltungsklasse
: Gibt die Unterschiede zwischen den Sicherungskopiengruppen oder den Archivierungskopiengruppen in der Verwaltungsklasse an. Die Unterschiede werden unter den folgenden Feldern aufgelistet:

  Änderung erkannt
  : Gibt die Liste der Kopiengruppenfelder an, die unterschiedlich sind.

  Wert für Quellenserver
  : Gibt den Wert im Kopiengruppenfeld auf dem Quellenreplikationsserver an.

  Wert für Zielserver
  : Gibt den Wert im Kopiengruppenfeld auf dem Zielreplikationsserver an.

Betroffene Knoten
: Gibt die Namen aller Clientknoten an, die von den in dieser Ausgabe angezeigten Änderungen betroffen sind.

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VALIDATE REPLPOLICY

Befehl	Beschreibung
VALIDATE REPLICATION	Überprüft die Replikation für Dateibereiche und Datentypen.
QUERY REPLSERVER	Zeigt Informationen zu Replikationsservern an.
SET DISSIMILARPOLICIES	Aktiviert die Maßnahmen auf dem Zielreplikationsserver für die Verwaltung replizierter Daten.
QUERY DOMAIN	Zeigt Informationen über Maßnahmendomänen an.
QUERY POLICYSET	Zeigt Informationen über Maßnahmengruppen an.
QUERY COPYGROUP	Zeigt die Attribute einer Kopiengruppe an.

Befehl	Beschreibung
QUERY MGMTCLASS	Zeigt Informationen zu Verwaltungsklassen an.

VARY (Datenträger mit wahlfreiem Zugriff an-/abhängen)

Mit diesem Befehl kann ein Speicherpooldatenträger mit wahlfreiem Zugriff für den Server angehängt oder abgehängt werden.

Berechtigungsklasse

Dieser Befehl ist nur für Datenträger in Einheiten mit wahlfreiem Zugriff gültig. Dieser Befehl kann beispielsweise während der Wartung eines Datenträgers mit wahlfreiem Zugriff oder bei der Fehlerberichtigung verwendet werden. Ein Datenträger mit wahlfreiem Zugriff, der als Unavailable (nicht verfügbar) definiert ist, kann nicht angehängt werden.

Für diesen Befehl ist die System- oder die Bedienerberechtigung erforderlich.

Syntax

```
                                        .-Wait--=--No------.
>>-VARy--+-ONline--+--Datenträgername--+------------------+----><
         '-OFfline-'                   '-Wait--=--+-No--+-'
                                                  '-Yes-'
```

Parameter

ONline
: Gibt an, daß der Server den Datenträger mit wahlfreiem Zugriff verwenden kann.

OFfline
: Gibt an, daß der Server den Datenträger nicht verwenden kann.

Datenträgername (Erforderlich)
: Gibt die Datenträger-ID an. Datenträgernamen dürfen keine eingebetteten Leerzeichen oder Gleichheitszeichen enthalten.

Wait
: Gibt an, ob darauf gewartet werden soll, dass der Server die Verarbeitung dieses Befehls im Vordergrund beendet. Dieser Parameter ist wahlfrei. Der Standardwert ist NO. Gültige Werte:

  No
  : Gibt an, dass der Server diesen Befehl im Hintergrund verarbeitet, während andere Tasks ausgeführt werden. Bei dem Hintergrundprozess erstellte Nachrichten werden vom Server entweder im Aktivitätenprotokoll oder an der Serverkonsole angezeigt, je nachdem, wo Nachrichten protokolliert werden.

  Yes
  : Gibt an, dass der Server diesen Befehl im Vordergrund verarbeitet. Erst nachdem der Befehl vollständig ausgeführt wurde, kann mit anderen Aufgaben fortgefahren werden. Der Server zeigt die Ausgabenachrichten dann dem Verwaltungs-Client an, wenn der Befehl beendet ist.

  AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeVon der Serverkonsole aus kann WAIT=YES nicht angegeben werden.

Beispiel: Einen Datenträger anhängen

AIX-Betriebssysteme Linux-BetriebssystemeDen Datenträger /adsm/stgvol/1 für den Server als Speicherpooldatenträger zur Verfügung stellen. AIX-Betriebssysteme Linux-Betriebssysteme

```
vary online /adsm/stgvol/1
```

Windows-BetriebssystemeDen Datenträger j:\storage\pool001 für den Server als Speicherpooldatenträger zur Verfügung stellen. Windows-Betriebssysteme

```
vary online j:\storage\pool001
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für VARY

Befehl	Beschreibung
CANCEL PROCESS	Bricht einen Serverhintergrundprozess ab.

Befehl	Beschreibung
DEFINE VOLUME	Ordnet einen Datenträger zu, der innerhalb eines angegebenen Speicherpools als Speicher verwendet werden soll.
DELETE VOLUME	Löscht einen Datenträger aus einem Speicherpool.
QUERY PROCESS	Zeigt Informationen über Hintergrundprozesse an.
QUERY VOLUME	Zeigt Informationen über Speicherpooldatenträger an.

Serveroptionen

Bei der Installation stellt IBM Spectrum Protect eine Serveroptionsdatei zur Verfügung, die eine Reihe von Standardoptionen zum Starten des Servers enthält.

Die Datei ist:

- dsmserv.opt im Serverinstanzverzeichnis

Mit Serveroptionen kann Folgendes angepasst werden:

- Übertragung
- Serverspeicher
- Client/Server
- Datum, Nummer, Uhrzeit und Sprache
- Datenbank- und Wiederherstellungsprotokoll
- Datenübertragung
- Nachricht
- Ereignisprotokollierung
- Sicherheit und Lizenzierung

Einige andere Optionen sind für sonstige Zwecke verfügbar. Diese nicht dokumentierten Optionen sind nur für die Verwendung durch den IBM® Support bestimmt.
Sollen die aktuellen Optionseinstellungen angezeigt werden, Folgendes eingeben:

```
query option
```

- Serveroptionen ändern
  Bei der Serverinitialisierung liest der Server die Serveroptionsdatei. Wird eine Serveroption durch Editieren der Datei aktualisiert, muss der Server gestoppt und anschließend wieder gestartet werden, um die aktualisierte Serveroptionsdatei zu aktivieren.
- Arten von Serveroptionen
  Mit Serveroptionen können Sie die Arbeitsweise von einigen Funktionen und Prozessen anpassen.
- 3494SHARED
  Die Option 3494SHARED gibt an, ob ein Kassettenarchiv IBM 3494 andere Anwendungen als IBM Spectrum Protect gemeinsam benutzen kann.
- ACSACCESSID
  Die Option ACSACCESSID gibt die ID für die ACS-Zugriffssteuerung eines ACSLS-Kassettenarchivs an.
- ACSLOCKDRIVE
  Die Option ACSLOCKDRIVE gibt an, ob die Laufwerke in den ACSLS-Kassettenarchiven gesperrt sind. Durch das Sperren von Laufwerken wird die exklusive Benutzung der Laufwerke in dem ACSLS-Kassettenarchiv in einer gemeinsamen Umgebung sichergestellt. Die Leistung ist jedoch etwas besser, wenn Kassettenarchive nicht gesperrt werden. Wenn andere Anwendungen die IBM Spectrum Protect-Laufwerke nicht verwenden, ist das Sperren der Laufwerke nicht erforderlich.
- ACSQUICKINIT
  Die Option ACSQUICKINIT gibt an, ob die Initialisierung des ACSLS-Kassettenarchivs beim Serverstart eine schnelle oder vollständige Initialisierung ist. Der Standardwert ist 'Yes'. Eine schnelle Initialisierung vermeidet den Aufwand, der mit der Synchronisation des Datenträgerbestands des IBM Spectrum Protect-Servers mit dem Datenträgerbestand des ACSLS-Kassettenarchivs verbunden ist (durch eine Prüfung des Kassettenarchivs).
- ACSTIMEOUTX
  Die Option ACSTIMEOUTX gibt das Vielfache des integrierten Zeitlimitwerts für ACSLS-APIs an. Der integrierte Zeitlimitwert für die ENTER-, EJECT- und AUDIT-ACS-API beträgt 1800 Sekunden; für alle anderen ACSLS-APIs beträgt der Wert 600 Sekunden. Lautet das angegebene Vielfache beispielsweise 5, beträgt der Zeitlimitwert für die Prüf-API 9000 Sekunden und für alle anderen APIs 3000 Sekunden.
- ACTIVELOGDIRECTORY
  Die Option ACTIVELOGDIRECTORY gibt den Namen des Verzeichnisses an, in dem alle aktiven Protokolldateien gespeichert werden.
- ACTIVELOGSIZE
  Die Option ACTIVELOGSIZE definiert die Gesamtgröße der Protokolldatei.
- ADMINCOMMTIMEOUT
  Die Option ADMINCOMMTIMEOUT gibt an, wie lange der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine erwartete Verwaltungsclientnachricht wartet.

- ADMINIDLETIMEOUT
  Die Option ADMINIDLETIMEOUT gibt die Zeit in Minuten an, die eine Verwaltungsclientsitzung inaktiv sein kann, bevor der Server die Sitzung abbricht.
- ADMINONCLIENTPORT
  Die Option ADMINONCLIENTPORT gibt an, ob TCPPORT von Verwaltungssitzungen verwendet werden kann. Der Standardwert ist YES.
-  Windows-BetriebssystemeADSMGROUPNAME
  Die Option ADSMGROUPNAME gibt den Namen einer Windows-Gruppe an. Ein Clientknoten muss Teil dieser Gruppe sein, um mit dem IBM Spectrum Protect-Server über NT Unified Logon arbeiten zu können. Der Clientknoten muss außerdem als IBM Spectrum Protect-Clientknoten registriert sein.
- ALIASHALT
  Die Option ALIASHALT ermöglicht es Administratoren, dem IBM Spectrum Protect-Befehl **HALT** einen anderen Namen zuzuordnen.
- ALLOWDESAUTH
  Die Option ALLOWDESAUTH gibt an, ob die Verwendung von Data Encryption Standard (DES) für die Authentifizierung zwischen einem Server und einem Client für Sichern/Archivieren zulässig ist.
- ALLOWREORGINDEX
  Die Option ALLOWREORGINDEX gibt an, ob die vom Server eingeleitete Indexreorganisation aktiviert oder inaktiviert ist.
- ALLOWREORGTABLE
  Die Option ALLOWREORGTABLE gibt an, ob die vom Server eingeleitete Tabellenreorganisation aktiviert oder inaktiviert ist.
- ARCHFAILOVERLOGDIRECTORY
  Die Option ARCHFAILOVERLOGDIRECTORY gibt das Verzeichnis an, das der Server zum Speichern der Archivprotokolldateien verwendet, die nicht im Verzeichnis für Archivprotokolle gespeichert werden können.
- ARCHLOGCOMPRESS
  Sie können die Komprimierung von Archivprotokollen auf dem IBM Spectrum Protect-Server aktivieren oder inaktivieren. Durch die Komprimierung der Archivprotokolle wird der Speicherbedarf reduziert, der für die Speicherung erforderlich ist.
- ARCHLOGDIRECTORY
  Die Option ARCHLOGDIRECTORY gibt ein Verzeichnis an, in dem der Datenbankmanager eine Protokolldatei archivieren kann, nachdem alle in dieser Protokolldatei angegebenen Transaktionen abgeschlossen wurden.
- ARCHLOGUSEDTHRESHOLD
  Die Option ARCHLOGUSEDTHRESHOLD gibt an, wann eine automatische Datenbanksicherung in Relation zum Prozentsatz des belegten Speicherbereichs für die Archivprotokolldatei gestartet werden soll. Der Standardwert ist 80 Prozent.
- ASSISTVCRRECOVERY
  Die Option ASSISTVCRRECOVERY gibt an, ob IBM Spectrum Protect ein Laufwerk IBM 3590 bei der Wiederherstellung nach verloren gegangenen oder beschädigten VCR (Vital Cartridge Records) unterstützt. Wird YES (Standardwert) angegeben und erkennt IBM Spectrum Protect während der Ladeverarbeitung einen Fehler, geht TSM während der Entladeverarbeitung an das Datenende, um den Laufwerken die Wiederherstellung der VCR zu ermöglichen. Während der Bandoperation kann dies geringe Auswirkungen auf die Leistung haben, da das Laufwerk keine schnelle Suche mit einem verloren gegangenen oder beschädigten VCR ausführen kann. Es tritt jedoch kein Datenverlust auf.
- AUDITSTORAGE
  Als Teil einer Lizenzprüfung berechnet der Server nach Knoten den Umfang des Serverspeichers, der für Sicherungsdateien, Archivierungsdateien und speicherverwaltete Dateien verwendet wird. Bei Servern, die umfangreiche Datenmengen verwalten, kann diese Berechnung sehr viel CPU-Zeit beanspruchen und andere Serveraktivitäten blockieren. Mit der Option AUDITSTORAGE kann angegeben werden, dass bei der Lizenzprüfung der Speicher nicht berechnet werden soll.
- BACKUPINITIATIONROOT
  Die Option BACKUPINITIATIONROOT gibt an, ob der Server Knotenparameterwerte für Benutzer überschreibt, die keine berechtigten IBM Spectrum Protect-Benutzer sind.
- CHECKTAPEPOS
  Die Option CHECKTAPEPOS gibt an, ob der IBM Spectrum Protect-Server die Position von Datenblöcken auf Band überprüft.
- CLIENTDEDUPTXNLIMIT
  Die Option CLIENTDEDUPTXNLIMIT gibt die maximale Größe einer Transaktion an, wenn vom Client deduplizierte Daten gesichert oder archiviert werden.
- COMMMETHOD
  Die Option COMMMETHOD gibt eine Übertragungsmethode an, die vom Server verwendet werden soll.
- COMMTIMEOUT
  Die Option COMMTIMEOUT gibt an, wie lange der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine erwartete Clientnachricht wartet. Wenn die Zeitlänge dieses Zeitlimit überschreitet, beendet der Server die Sitzung mit dem Client. Sie können den Wert für das Zeitlimit erhöhen, damit keine Zeitlimitüberschreitung bei den Clients auftritt. Eine Zeitlimitüberschreitung kann bei Clients auftreten, wenn eine hohe Netzauslastung in Ihrer Umgebung vorhanden ist, oder wenn die Clients große Dateien sichern.
- CONTAINERRESOURCETIMEOUT
  Die Option CONTAINERRESOURCETIMEOUT gibt an, wie lange der Server auf die Ausführung einer Datenspeicheroperation für einen Containerspeicherpool wartet.
-  Windows-BetriebssystemeDATEFORMAT
  Die Option DATEFORMAT gibt das Format an, in dem Datumsangaben vom Server angezeigt werden.
- DBDIAGLOGSIZE
  Mit dieser Option können Sie die Größe des Speicherbereichs steuern, der von Diagnoseprotokolldateien verwendet wird.
- DBDIAGPATHFSTHRESHOLD
  Die Option DBDIAGPATHFSTHRESHOLD gibt den Schwellenwert für freien Speicherbereich in dem Dateisystem oder auf der Platte an, das bzw. die die Datei db2diag.log enthält.

- DBMEMPERCENT
  Verwenden Sie diese Option, um den Prozentsatz des virtuellen Adressraums anzugeben, der den Datenbankmanagerprozessen zugeordnet ist.
- DBMTCPPORT
  Die Option DBMTCPPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-DFV-Treiber für den Datenbankmanager auf Anforderungen für Clientsitzungen.
- DEDUPREQUIRESBACKUP
  Die Option DEDUPREQUIRESBACKUP gibt an, ob Datenträger in primären Speicherpools mit sequenziellem Zugriff, die für die Deduplizierung von Daten definiert sind, wiederhergestellt und doppelte Daten gelöscht werden können, bevor die Speicherpools gesichert werden.
- DEDUPTIER2FILESIZE
  Die Option DEDUPTIER2FILESIZE gibt an, bei welcher Dateigröße IBM Spectrum Protect beginnt, die Schicht 2 der Datendeduplizierung zu verwenden.
- DEDUPTIER3FILESIZE
  Die Option DEDUPTIER3FILESIZE gibt an, bei welcher Dateigröße IBM Spectrum Protect beginnt, die Schicht 3 der Datendeduplizierung zu verwenden.
- DEVCONFIG
  Die Option DEVCONFIG gibt den Namen einer Datei an, in der IBM Spectrum Protect eine Sicherungskopie der Einheitenkonfigurationsinformationen speichern soll.
- DISABLEREORGTABLE
  Die Option DISABLEREORGTABLE gibt an, ob die Onlinetabellenreorganisation für Tabellennamen inaktiviert wird, die in der Tabellenliste angegeben sind.
- DISABLESCHEDS
  Die Option DISABLESCHEDS gibt an, ob Verwaltungszeitpläne und Clientzeitpläne während der Wiederherstellung des IBM Spectrum Protect-Servers inaktiviert sind.
- DISPLAYLFINFO
  Die Option DISPLAYLFINFO gibt an, wie die Abrechnungssätze und Einträge in der Übersichtstabelle den Knotennamen angeben.
- DNSLOOKUP
  Die Option DNSLOOKUP gibt an, ob der Server System-API-Aufrufe verwendet, um die DNS-Namen (DNS = Domain Name Server) von Systemen zu bestimmen, die den Server ansprechen.
- DRIVEACQUIRERETRY
  Mit der Option DRIVEACQUIRERETRY kann angegeben werden, wie oft der Server versuchen soll, ein Laufwerk in einem Kassettenarchiv IBM 349x anzufordern. Wird das Kassettenarchiv von mehreren Anwendungen gemeinsam benutzt, scheinen seine Laufwerke für den Server verfügbar zu sein (durch die Verwendung eines Sendeaufrufprozesses im Hintergrund), obwohl sie es nicht sind.
- ENABLENASDEDUP
  Die Serveroption ENABLENASDEDUP gibt an, ob der Server Daten dedupliziert, die von einem NAS-Dateiserver gespeichert werden. Diese Option gilt nur für NetApp-Dateiserver.
- EVENTSERVER
  Die Option EVENTSERVER gibt an, ob der Server beim Systemstart eine Verbindung zum Ereignisserver herstellen soll.
- EXPINTERVAL
  Die Option EXPINTERVAL gibt das Intervall (in Stunden) an, in dem automatische Bestandsverfallsprozesse in IBM Spectrum Protect stattfinden. Beim Datenträgerbestandsverfall werden Clientsicherungs- und Archivierungsdateikopien aus dem Server gelöscht, und zwar wie von den Verwaltungsklassen angegeben, denen die Clientdateien zugeordnet sind. Findet nicht regelmäßig ein Datenträgerverfall statt, wird kein Speicherpoolbereich von abgelaufenen Clientdateien zurückgefordert, so dass für den Server mehr Speicherbereich benötigt wird, als für die Maßnahme eigentlich nötig wäre.
- EXPQUIET
  Die Option EXPQUIET gibt an, ob IBM Spectrum Protect detaillierte Nachrichten während der Verfallsverarbeitung sendet.
- Linux-BetriebssystemeWindows-BetriebssystemeFASPBEGPORT
  Die Option FASPBEGPORT gibt die Anfangsnummer des Bereichs von Anschlussnummern an, die für die Netzkommunikation mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) verwendet werden.
- Linux-BetriebssystemeWindows-BetriebssystemeFASPENDPORT
  Die Option FASPENDPORT gibt die Endnummer des Bereichs von Anschlussnummern an, die für die Netzkommunikation mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) verwendet werden.
- Linux-BetriebssystemeWindows-BetriebssystemeFASPTARGETRATE
  Die Option FASPTARGETRATE gibt die Zielgeschwindigkeit für die Datenübertragung mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) an. Mit der Angabe der Zielgeschwindigkeit begrenzen Sie die Bandbreite jeder Netzverbindung, die die Aspera FASP-Technologie verwendet. Auf diese Weise können Sie sicherstellen, dass genügend Bandbreite für alle Netzverbindungen verfügbar ist.
- FFDCLOGLEVEL
  Die Option FFDCLOGLEVEL gibt den Typ von allgemeinen Servernachrichten an, die im FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) angezeigt werden.
- FFDCLOGNAME
  Die Option FFDCLOGNAME gibt einen Namen für das FFDC-Protokoll (FFDC = First-Failure Data Capture) an.
- FFDCMAXLOGSIZE
  Die Option FFDCMAXLOGSIZE gibt die Größe für die FFDC-Protokolldatei (FFDC = First-Failure Data Capture) an.
- FFDCNUMLOGS
  Die Option FFDCNUMLOGS gibt die Anzahl der Protokolldateien an, die für die Umlaufprotokollierung verwendet werden können. Der Standardwert ist 10.

- FILEEXIT
  Die Option FILEEXIT gibt eine Datei an, an die aktivierte Ereignisse weitergeleitet werden. Jedes protokollierte Ereignis ist ein Satz in der Datei.
- FILETEXTEXIT
  Die Option FILETEXTEXIT gibt eine Datei an, an die aktivierte Ereignisse weitergeleitet werden. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.
- FSUSEDTHRESHOLD
  Die Option FSUSEDTHRESHOLD gibt den Prozentsatz des Dateisystems an, der von der Datenbank ausgefüllt werden kann, bevor eine Alertnachricht ausgegeben wird.
- IDLETIMEOUT
  Die Option IDLETIMEOUT gibt die Zeit in Minuten an, die eine Clientsitzung inaktiv sein kann, bevor der Server die Sitzung abbricht. Sie können den Wert für das Zeitlimit erhöhen, damit bei hoher Netzauslastung in Ihrer Umgebung keine Zeitlimitüberschreitung bei den Clients auftritt. Beachten Sie jedoch, dass bei einer großen Anzahl von inaktiven Sitzungen andere Benutzer möglicherweise keine Verbindung zu dem Server herstellen können.
- KEEPALIVE
  Die Option KEEPALIVE gibt an, ob die TCP-Keepalive-Funktion (TCP = Transmission Control Protocol) für abgehende TCP-Sockets aktiviert ist. Die TCP-Keepalive-Funktion sendet eine Übertragung von einer Einheit zu einer anderen Einheit, um zu überprüfen, ob die Verbindung zwischen den beiden Einheiten betriebsbereit ist.
- KEEPALIVETIME
  Die Option KEEPALIVETIME gibt an, wie oft TCP eine Keepalive-Übertragung sendet, wenn eine Antwort empfangen wird. Diese Option gilt nur, wenn die Option KEEPALIVE auf YES gesetzt wurde.
- KEEPALIVEINTERVAL
  Die Option KEEPALIVEINTERVAL gibt an, wie oft eine Keepalive-Übertragung gesendet wird, wenn keine Antwort empfangen wird. Diese Option gilt nur, wenn die Option KEEPALIVE auf YES gesetzt wurde.
- LANGUAGE
  Die Option LANGUAGE steuert die Initialisierung von länderspezifischen Angaben. Die länderspezifischen Angaben enthalten unter anderem die Landessprache sowie die Datums-, Uhrzeit- und Zahlenformate, die für die Konsole und den Server verwendet werden sollen.
- LDAPCACHEDURATION
  Die Option LDAPCACHEDURATION bestimmt die Zeit, die der IBM Spectrum Protect-Server Informationen zur LDAP-Kennwortauthentifizierung zwischenspeichert.
- LDAPURL
  Die Option LDAPURL gibt die Position Ihres Lightweight Directory Access Protocol-Servers (LDAP-Servers) an. Definieren Sie die Option LDAPURL nach der Konfiguration des LDAP-Servers.
- MAXSESSIONS
  Die Option MAXSESSIONS gibt die maximal zulässige Anzahl gleichzeitig stattfindender Clientsitzungen für den Server an.
- MESSAGEFORMAT
  Die Option MESSAGEFORMAT gibt an, ob eine Nachrichtennummer in allen Zeilen angezeigt wird, wenn sich die Nachricht über mehrere Zeilen erstreckt.
- MIRRORLOGDIRECTORY
  Die Option MIRRORLOGDIRECTORY gibt das Verzeichnis zum Spiegeln des Pfads für aktive Protokolldateien an.
- MOVEBATCHSIZE
  Die Option MOVEBATCHSIZE gibt die Anzahl Clientdateien an, die innerhalb derselben Servertransaktion als Stapel gruppiert und versetzt werden sollen. Dieses Versetzen von Daten resultiert aus Speicherpoolsicherungen und -zurückschreibungen, Umlagerungsoperationen, Wiederherstellungsoperationen und MOVE DATA-Operationen. Diese Option arbeitet zusammen mit der Option MOVESIZETHRESH.
- MOVESIZETHRESH
  Die Option MOVESIZETHRESH gibt den Grenzwert für die Datenmenge an (in Megabyte), die innerhalb derselben Servertransaktion als Stapel versetzt werden soll. Wenn diese Schwelle erreicht ist, werden dem aktuellen Stapel keine weiteren Dateien hinzugefügt. Nachdem der aktuelle Stapel versetzt wurde, wird eine neue Transaktion gestartet.
- MSGINTERVAL
  Die Option MSGINTERVAL gibt die Zeit in Minuten zwischen Nachrichten an, in denen ein Bediener zum Einlegen eines Bands für den Server aufgefordert wird.
-  NAMEDPIPENAME
  Die Option NAMEDPIPENAME gibt eine Übertragungsmethode an, mit der Prozesse miteinander kommunizieren können, ohne wissen zu müssen, wo sich die Sende- und Empfangsprozesse befinden. Der Name fungiert als Aliasname und verbindet die beiden Prozesse unabhängig davon, ob sie sich auf demselben Rechner oder in verbundenen Domänen befinden.
- NDMPCONNECTIONTIMEOUT
  Die Serveroption NDMPCONNECTIONTIMEOUT gibt die Zeit in Stunden an, die der IBM Spectrum Protect-Server auf den Empfang von Statusaktualisierungen während der Ausführung von NDMP-Zurückschreibungsoperationen über das LAN wartet. NDMP-Zurückschreibungsoperationen mit großen NAS-Dateisystemen können einen langen Inaktivitätszeitraum aufweisen. Der Standardwert ist 6 Stunden.
- NDMPCONTROLPORT
  Die Option NDMPCONTROLPORT gibt die Anschlussnummer an, die für interne Übertragungen für bestimmte NDMP-Operationen (NDMP = Network Data Management Protocol) verwendet werden soll. Der IBM Spectrum Protect-Server arbeitet nicht als allgemeiner NDMP-Bandserver.
- NDMPENABLEKEEPALIVE
  Die Serveroption NDMPENABLEKEEPALIVE gibt an, ob der IBM Spectrum Protect-Server TCP-Keepalive (TCP = Transmission Control Protocol) für NDMP-Steuerverbindungen (NDMP = Network Data Management Protocol) zu NAS-Einheiten (NAS = Network-attached Storage) aktiviert. Der Standardwert ist NO.

- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeNDMPKEEPIDLEMINUTES
  Die Serveroption NDMPKEEPIDLEMINUTES gibt die Zeit in Minuten an, bevor das Betriebssystem das erste TCP-Keepalive-Paket (TCP = Transmission Control Protocol) für eine NDMP-Steuerverbindung (NDMP = Network Data Management Protocol) überträgt. Der Standardwert ist 120 Minuten.
- NDMPPORTRANGE
  Die Option NDMPPORTRANGE gibt den Bereich der Anschlussnummern an, in dem IBM Spectrum Protect navigiert, um eine Anschlussnummer zum Akzeptieren einer Sitzung von einer NAS-Einheit für die Datenübertragung zu erhalten. Der Standardwert 0,0 bedeutet, dass IBM Spectrum Protect einen Anschluss vom Betriebssystem zur Verfügung stellen lässt (ephemerer Anschluss).
- NDMPPREFDATAINTERFACE
  Diese Option gibt die IP-Adresse an, die der Schnittstelle zugeordnet ist, in der der Server alle NDMP-Sicherungsdaten (NDMP = Network Data Management Protocol) empfangen soll.
- NOPREEMPT
  Der Server ermöglicht bestimmten Operationen das Zugriffsvorrecht für Datenträger und Einheiten. Durch Angabe von NOPREEMPT kann das Zugriffsvorrecht inaktiviert werden. In diesem Fall hat dann keine Operation das Zugriffsvorrecht auf einen Datenträger und lediglich einer Datenbanksicherungsoperation kann das Zugriffsvorrecht für eine Einheit vor einer anderen Operation eingeräumt werden.
- NORETRIEVEDATE
  Die Option NORETRIEVEDATE gibt an, dass der Server das Abrufdatum einer Datei in einem Plattenspeicherpool nicht aktualisiert, wenn ein Client die Datei zurückschreibt oder abruft. Diese Option und der Speicherpoolparameter MIGDELAY steuern, wann der Server Dateien umgelagert.
- Windows-BetriebssystemeNPAUDITFAILURE
  Die Option NPAUDITFAILURE gibt an, ob ein Ereignis an das Ereignisprotokoll gesendet wird, wenn ein Knoten sich bei dem Server anmeldet und dabei einen Namen verwendet, der sich zwar in der Windows-Gruppe befindet, aber nicht mit dem Windows-Kontoanmeldenamen übereinstimmt. Um sicherzustellen, dass ein Knoten nur auf seine eigenen Daten zugreifen kann, müssen der Knotenname und der Windows-Kontoname übereinstimmen.
- Windows-BetriebssystemeNPAUDITSUCCESS
  Die Option NPAUDITSUCCESS gibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknotenbenutzer über SECUREPIPE eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann.
- Windows-BetriebssystemeNPBUFFERSIZE
  Die Option NPBUFFERSIZE gibt die Größe des Kommunikationspuffers für benannte Pipes an.
- Windows-BetriebssystemeNUMBERFORMAT
  Die Option NUMBERFORMAT gibt das Format an, in dem der Server Zahlen anzeigt.
- NUMOPENVOLSALLOWED
  Die Option NUMOPENVOLSALLOWED gibt die Anzahl der FILE-Eingabedatenträger in einem deduplizierten Speicherpool an, die gleichzeitig geöffnet sein können.
- PUSHSTATUS
  Die Option PUSHSTATUS wird auf Peripherieservern verwendet, um sicherzustellen, dass Statusinformationen an den Hub-Server gesendet werden. Aktualisieren Sie diese Option nur, wenn Sie die Konfiguration des Operations Center im vorkonfigurierten Zustand zurückschreiben müssen, in dem die IBM Spectrum Protect-Server nicht als Hub-Server oder Peripherieserver definiert sind.
- QUERYAUTH
  Die Option QUERYAUTH gibt die Administratorberechtigungsstufe an, die für die Ausgabe des Befehls QUERY oder SQL SELECT erforderlich ist. Standardmäßig kann jeder Administrator die Befehle QUERY und SELECT ausgeben. Mit dieser Option kann die Verwendung dieser Befehle eingeschränkt werden.
- RECLAIMDELAY
  Mit dieser Option wird die Wiederherstellung eines SnapLock-Datenträgers verzögert. Damit wird es ermöglicht, dass verbleibende Daten verfallen können, so dass keine Notwendigkeit zur Wiederherstellung des Datenträgers besteht.
- RECLAIMPERIOD
  Mit dieser Option können Sie die Anzahl der Tage für den Wiederherstellungszeitraum eines SnapLock-Datenträgers definieren.
- REORGBEGINTIME
  Die Option REORGBEGINTIME gibt die früheste Zeit an, zu der der IBM Spectrum Protect-Server eine Tabellen- oder Indexreorganisation starten kann.
- REORGDURATION
  Die Option REORGDURATION gibt ein Intervall an, in dem die vom Server eingeleitete Tabellen- oder Indexreorganisation gestartet werden kann.
- REPORTRETRIEVE
  Die Option REPORTRETRIEVE erstellt Berichte zu Zurückschreibungs- oder Abrufoperationen, die von Clientknoten oder Administratoren ausgeführt werden. Der Standardwert ist NO.
- REPLBATCHSIZE
  Die Option REPLBATCHSIZE gibt die Anzahl Clientdateien an, die innerhalb derselben Servertransaktion als Stapel repliziert werden sollen. Diese Option betrifft nur die Knotenreplikationsprozesse und arbeitet mit der Option REPLSIZETHRESH, um die Knotenreplikationsverarbeitung zu verbessern.
- REPLSIZETHRESH
  Die Option REPLSIZETHRESH gibt einen Schwellenwert (in Megabyte) für das replizierte Datenvolumen innerhalb derselben Servertransaktion an.
- REQSYSAUTHOUTFILE
  Die Option REQSYSAUTHOUTFILE gibt an, ob die Systemberechtigung für Verwaltungsbefehle erforderlich ist, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben.
- RESOURCETIMEOUT
  Die Option RESOURCETIMEOUT gibt an, wie lange der Server auf eine Ressource wartet, bevor die anstehende Anforderung einer

Ressource abgebrochen wird. Tritt eine Zeitlimitüberschreitung auf, wird die Anforderung der Ressource abgebrochen.

- RESTOREINTERVAL
  Die Option RESTOREINTERVAL gibt an, wie lange eine wiederanlauffähige Zurückschreibungssitzung in der Serverdatenbank gesichert werden kann. Solange die Zurückschreibungssitzung in der Datenbank gesichert ist, kann sie ab dem Punkt, an dem sie gestoppt wurde, erneut gestartet werden.
- RETENTIONEXTENSION
  Die Option RETENTIONEXTENSION gibt die Anzahl der Tage an, um die das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitert werden soll. Mit dieser Option kann der Server das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitern, um eine übermäßige Wiederherstellung zu vermeiden.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeSANDISCOVERY
  Die Option SANDISCOVERY gibt an, ob die SAN-Erkennungsfunktion von IBM Spectrum Protect aktiviert ist.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeSANDISCOVERYTIMEOUT
  Die Option SANDISCOVERYTIMEOUT gibt die Zeit an, die für die Antwort von Hostbusadaptern zulässig ist, wenn sie von dem SAN-Erkennungsprozess abgefragt werden. Sobald die für SANDISCOVERYTIMEOUT angegebene Zeit erreicht wird, tritt bei dem Prozess eine Zeitlimitüberschreitung auf.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeSANREFRESHTIME
  Die Option SANREFRESHTIME gibt die Zeit an, die vergeht, bevor die zwischengespeicherten SAN-Erkennungsinformationen aktualisiert werden. Die Option SANREFRESHTIME hat den Standardwert 0, der angibt, dass kein SAN-Erkennungscache vorhanden ist. Bei jeder Ausführung einer SAN-Erkennungsoperation durch den Server werden die Informationen direkt von dem Hostbusadapter abgerufen.
- SEARCHMPQUEUE
  Die Option SEARCHMPQUEUE gibt die Reihenfolge an, in der der Server Anforderungen in der Ladewarteschlange ausführt. Wird die Option angegeben, versucht der Server zuerst, Anforderungen für Datenträger auszuführen, die bereits geladen sind. Diese Anforderungen können vor anderen Anforderungen ausgeführt werden, auch wenn die anderen Anforderungen schon länger auf den Mountpunkt warten. Wird diese Option nicht angegeben, führt der Server Anforderungen in der Reihenfolge aus, in der sie empfangen werden.
-  Windows-BetriebssystemeSECUREPIPES
  Bei Verwendung des Protokolls mit benannten Pipes führt das Aktivieren von SECUREPIPES dazu, dass der Server die über ADSMGROUPNAME angegebene Windows-Gruppe prüft, um einen Clientknoten/Benutzer zu authentifizieren.
- SERVERDEDUPTXNLIMIT
  Die Option SERVERDEDUPTXNLIMIT gibt die maximale Größe von Objekten an, die auf dem Server dedupliziert werden können.
- SHMPORT
   AIX-Betriebssysteme  Linux-BetriebssystemeDie Option SHMPORT gibt die TCP/IP-Anschlussadresse eines Servers bei Verwendung von gemeinsam benutztem Speicher an. Jede Übertragung mit gemeinsam benutztem Speicher beginnt mit einer TCP/IP-Verbindung.
   Windows-BetriebssystemeDie Option SHMPORT gibt den Anschluss an, an dem der Server für Verbindungen mit gemeinsam genutztem Speicher empfangsbereit ist.
- SHREDDING
  Die Option SHREDDING gibt an, ob das Schreddern von gelöschten sensiblen Daten automatisch oder manuell ausgeführt wird. Das Schreddern gilt nur für Daten in Speicherpools, die explizit für die Unterstützung des Schredderns konfiguriert wurden.
- SNMPHEARTBEATINTERVAL
  Die Option SNMPHEARTBEATINTERVAL gibt das Intervall zwischen den Abfragen des IBM Spectrum Protect-Servers in Minuten an.
- SNMPMESSAGECATEGORY
  Die Option SNMPMESSAGECATEGORY gibt die Abfangarten an, die verwendet werden, wenn Nachrichten des Servers über den SNMP-Subagenten (SNMP = Simple Network Management Protocol) an den SNMP-Manager weitergeleitet werden.
- SNMPSUBAGENT
  Die Option SNMPSUBAGENT gibt die Parameter an, die erforderlich sind, damit der IBM Spectrum Protect-Subagent mit dem SNMP-Dämon (SNMP = Simple Network Management Protocol) kommunizieren kann. Diese Option betrifft nur das Konfigurieren des SNMP-Subagenten, damit dieser mit dem SNMP-Agenten kommunizieren kann; die Option wird vom Server ignoriert.
- SNMPSUBAGENTHOST
  Die Option SNMPSUBAGENTHOST gibt den Standort des IBM Spectrum Protect SNMP-Subagenten (SNMP = Simple Network Management Protocol) an. Der Standardwert für diese Option lautet 127.0.0.1.
- SNMPSUBAGENTPORT
  Die Option SNMPSUBAGENTPORT gibt die Anschlussnummer des IBM Spectrum Protect SNMP-Subagenten (SNMP = Simple Network Management Protocol) an.
- SSLFIPSMODE
  Die Option SSLFIPSMODE gibt an, ob der FIPS-Modus (Federal Information Processing Standards) für Secure Sockets Layer (SSL) aktiv ist. Der Standardwert ist NO.
- SSLINITTIMEOUT
  Die Option SSLINITTIMEOUT gibt die Zeit in Minuten an, die der Server darauf wartet, dass eine SSL-Sitzung (SSL = Secure Sockets Layer) die Initialisierung beendet, bevor der Server die Sitzung abbricht.
- SSLTCPADMINPORT
  Die Option SSLTCPADMINPORT gibt die Anschlussadresse an, an der der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen nur für SSL-aktivierte Sitzungen wartet. Die Sitzungen gelten für den Verwaltungsbefehlszeilenclient.
- SSLTCPPORT
  Die Option SSLTCPPORT gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) nur für SSL-fähige Sitzungen an. Der TCP/IP-Kommunikationstreiber des Servers wartet an diesem Anschluss auf Anforderungen für SSL-aktivierte Sitzungen vom Client.
- TCPADMINPORT
  Die Option TCPADMINPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für andere TCP/IP-Sitzungen und SSL-fähige Sitzungen als Clientsitzungen wartet. Dazu gehören Verwaltungssitzungen,

Sitzungen zwischen Servern, Speicheragentensitzungen, Speicherarchivclientsitzungen, Sitzungen verwalteter Server und Ereignisserversitzungen.

- AIX-BetriebssystemeLinux-BetriebssystemeTCPBUFSIZE
  Die Option TCPBUFSIZE gibt die Größe des Puffers an, der für TCP/IP-Sendeanforderungen verwendet wird. Während einer Zurückschreibung werden Clientdaten aus der IBM Spectrum Protect-Sitzungskomponente in einen TCP-DFV-Treiber versetzt. Die Option TCPBUFSIZE bestimmt, ob der Server die Daten direkt aus dem Sitzungspuffer sendet oder die Daten in den TCP-Puffer kopiert. Eine Puffergröße von 32 KB zwingt den Server dazu, Daten in den Kommunikationspuffer zu kopieren und den Inhalt des Puffers zu löschen, wenn er gefüllt ist.
- TCPNODELAY
  Die Option TCPNODELAY gibt an, ob der Server die Verzögerung beim Senden von aufeinanderfolgenden kleinen Paketen im Netz inaktiviert.
- TCPPORT
  Die Option TCPPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für Clientsitzungen wartet. Der TCP/IP-Kommunikationstreiber des Servers ist an diesem Anschluss sowohl für TCP/IP-Sitzungen als auch für SSL-fähige Sitzungen vom Client empfangsbereit.
- TCPWINDOWSIZE
  Die Option TCPWINDOWSIZE gibt den Umfang (in Kilobyte) der Empfangsdaten an, die bei einer TCP/IP-Verbindung gleichzeitig gepuffert werden können. Der sendende Host kann erst dann weitere Daten senden, wenn er eine Bestätigung und eine Aktualisierung des TCP-Empfangsfensters empfängt. Jedes TCP-Paket enthält das entsprechende TCP-Empfangsfenster in der Verbindung. Bei einem größeren Fenster kann der Sender mit dem Senden von Daten fortfahren. Außerdem wird möglicherweise die Übertragungsleistung verbessert, besonders in schnellen Netzen mit hoher Latenzzeit.
- TECBEGINEVENTLOGGING
  Die Option TECBEGINEVENTLOGGING gibt an, ob die Ereignisprotokollierung für den TIVOLI-Empfänger beim Serverstart beginnen soll. Wird die Option TECHOST angegeben, wird für TECBEGINEVENTLOGGING standardmäßig der Wert YES angenommen.
- TECHOST
  Die Option TECHOST gibt den Hostnamen oder die IP-Adresse für den Tivoli-Ereignisserver an.
- TECPORT
  Die Option TECPORT gibt die TCP/IP-Anschlussadresse an, an der der Tivoli-Ereignisserver empfangsbereit ist. Diese Option ist nur erforderlich, wenn sich der Tivoli-Ereignisserver auf einem System befindet, auf dem der Service 'Port Mapper' nicht ausgeführt wird.
- TECUTF8EVENT
  Die Option TECUTF8EVENT ermöglicht es dem IBM Spectrum Protect-Administrator, Informationen im UTF–8-Datenformat an den Tivoli Enterprise Console (TEC)-Server zu senden. Der Standardwert ist 'No'. Mit dem Befehl QUERY OPTION können Sie abfragen, ob diese Option aktiviert ist.
- THROUGHPUTDATATHRESHOLD
  Die Option THROUGHPUTDATATHRESHOLD gibt eine Durchsatzschwelle an, die eine Clientsitzung erreichen muss, damit sie nicht abgebrochen wird, wenn die Zeitschwelle erreicht wird.
- THROUGHPUTTIMETHRESHOLD
  Die Option THROUGHPUTTIMETHRESHOLD gibt die Zeitschwelle für eine Sitzung an, nach deren Ablauf die Sitzung aufgrund zu geringen Durchsatzes abgebrochen werden kann.
- Windows-BetriebssystemeTIMEFORMAT
  Die Option TIMEFORMAT gibt das Format an, in dem Uhrzeitangaben vom Server angezeigt werden.
- TXNGROUPMAX
  Die Option TXNGROUPMAX gibt die Anzahl der Objekte an, die als Gruppe zwischen einem Client und dem Server zwischen Transaktions-COMMIT-Punkten übertragen werden. Der Mindestwert beträgt 4 Objekte und der Maximalwert beträgt 65000 Objekte. Der Standardwert ist 4096 Objekte. Bei den übertragenen Objekten handelt es sich um tatsächliche Dateien, Verzeichnisse oder beides. Der Server zählt jede Datei oder jedes Verzeichnis als ein Objekt.
- UNIQUETDPTECEVENTS
  Die Option UNIQUETDPTECEVENTS generiert eine eindeutige Tivoli Enterprise Console (TEC)-Ereignisklasse für jede einzelne IBM Spectrum Protect-Nachricht, einschließlich Client-, Server- und IBM Spectrum Protect Data Protection-Clientnachrichten. Der Standardwert ist 'No'.
- UNIQUETECEVENTS
  Die Option UNIQUETECEVENTS generiert eine eindeutige Tivoli Enterprise Console (TEC)-Ereignisklasse für jede einzelne IBM Spectrum Protect-Nachricht. Der Standardwert ist 'No'.
- USEREXIT
  Die Option USEREXIT gibt einen benutzerdefinierten Ausgang an, dem die Steuerung für die Verwaltung eines Ereignisses übergeben wird.
- VERBCHECK
  Die Option VERBCHECK gibt an, dass der Server eine zusätzliche Fehlerprüfung für die Struktur der Befehle durchführt, die vom Client gesendet werden. Diese Option sollte nur aktiviert werden, wenn der Client nicht ordnungsgemäß gebildete Anforderungen an den Server sendet, die zum Absturz des Servers führen. Ist diese Option aktiviert, hat dies einen Protokollfehler an Stelle eines Serverabsturzes zur Folge.
- VOLUMEHISTORY
  Die Option VOLUMEHISTORY gibt den Namen von Dateien an, die automatisch aktualisiert werden sollen, wenn History-Informationen von sequenziellen Datenträgern des Servers sich ändern. Für diese Option gibt es keinen Standardwert.

Serveroptionen ändern

Bei der Serverinitialisierung liest der Server die Serveroptionsdatei. Wird eine Serveroption durch Editieren der Datei aktualisiert, muss der Server gestoppt und anschließend wieder gestartet werden, um die aktualisierte Serveroptionsdatei zu aktivieren.

Informationen zu diesem Vorgang

Einige Optionen können dynamisch mit dem Befehl SETOPT geändert werden, ohne dass der Server gestoppt und gestartet werden muss. Für ausführliche Informationen siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

AIX-BetriebssystemeLinux-BetriebssystemeDie Datei dsmserv.opt.smp (wird ebenfalls bei der Installation zur Verfügung gestellt) enthält das Format der Optionsdatei und alle Standardeinstellungen. Alle Optionen in der Datei dsmserv.opt.smp können geändert werden. Soll der Server die geänderten Optionen verwenden, müssen Sie die Datei in dsmserv.opt umbenennen. Zum Aktivieren einer Option in der Serveroptionsdatei ist das der Option vorausgehende *>>> zu entfernen. Der Server ignoriert alle Optionen, denen *>>> vorausgeht.

Windows-BetriebssystemeSie können Serveroptionen ändern, indem Sie den Optionsdateieditor verwenden, der in der IBM Spectrum Protect-Konsole enthalten ist. Mit diesem Editor werden Kommunikationsparameter erkannt und Werte auf ihre Gültigkeit hin überprüft, und er bietet Hilfe für alle Optionen. Das Arbeiten mit dem Optionsdateieditor stellt die bevorzugte Methode für das Ändern von Serveroptionen dar, aber es kann auch mit einem Texteditor gearbeitet werden.

Arten von Serveroptionen

Mit Serveroptionen können Sie die Arbeitsweise von einigen Funktionen und Prozessen anpassen.

- Serverübertragungsoptionen
  Sie können Serveroptionen verwenden, um Serverübertragungsmethoden und ihre Kenndaten anzugeben.
- Optionen für den Serverspeicher
  IBM Spectrum Protect stellt eine Reihe von Optionen bereit, mit denen Sie bestimmte Operationen für Einheiten und Serverspeicher konfigurieren können.
- Client/Server-Optionen
  Sie können Serveroptionen verwenden, um die Client/Server-Verarbeitung zu steuern.
- Optionen für Datum, Zahlen, Uhrzeit und Sprache
  Sie können Serveroptionen verwenden, um Anzeigeformate für Datums-, Uhrzeit- und Zahlenangaben sowie für die Landessprache anzugeben.
- Datenbankoptionen
  Mit Serveroptionen können Sie bestimmte Aspekte bei der Datenbankverarbeitung steuern.
- Datenübertragungsoptionen
  Mit Serveroptionen können Sie steuern, wie IBM Spectrum Protect Daten gruppiert und überträgt.
- Nachrichtenoptionen
  Mit Serveroptionen lässt sich die Nachrichtenausgabe in IBM Spectrum Protect flexibler gestalten.
- Optionen für die Aufzeichnung des Ereignisprotokolls
  Optionen können bei der Verwaltung von Ereignisprotokollempfängern helfen.
- Optionen für Sicherheit und Lizenzierung
  Sie können Serveroptionen verwenden, um Serversicherheits- und -lizenzprüfungen anzupassen.
- Weitere Optionen
  Sie können eine Vielzahl anderer Serveroptionen verwenden, um IBM Spectrum Protect anzupassen.

Serverübertragungsoptionen

Sie können Serveroptionen verwenden, um Serverübertragungsmethoden und ihre Kenndaten anzugeben.

Tabelle 1. Übertragungsoptionen

Option	Beschreibung
ADMINCOMMTIMEOUT	Die Zeit, die der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine Verwaltungsclientnachricht wartet
ADMINIDLETIMEOUT	Die Zeit, die eine Verwaltungsclientsitzung inaktiv sein kann
ADMINONCLIENTPORT	Der Anschluss, der bestimmt, ob Verwaltungssitzungen den in der Option TCPPORT angegebenen Anschluss verwenden können
COMMMETHOD	Übertragungsmethode des Servers
DBMTCPPORT	Die Nummer des Anschlusses, an dem der TCP/IP-DFV-Treiber für den Datenbankmanager auf Anforderungen für Clientsitzungen wartet

Option	Beschreibung
DNSLOOKUP	Steuerung der Verwendung von Domänennamenservices (Domain Name Services = DNS) zum Suchen der Namen der Systeme, die den Server ansprechen
LDAPCACHEDURATION	Bestimmt die Dauer, die Authentifizierungssitzungen für denselben Knoten oder Administrator übersprungen werden. Möglicherweise stellen Sie eine geringe Leistungsverbesserung fest, wenn Sitzungen übersprungen werden.
LDAPURL	Gibt den LDAP-Verzeichnisserver an. Jede Einstellung muss den Namen des LDAP-Verzeichnisservers, eine Anschlussnummer und den Basis-DN des Namensbereichs (oder Suffix) enthalten, den der Server verwaltet.
Windows-BetriebssystemeNAMEDPIPENAME	Windows-Betriebssysteme Übertragungsmethode mit benannten Pipes
NDMPCONTROLPORT	Der interne Übertragungsanschluss, der für bestimmte NDMP-Operationen (NDMP = Network Data Management Protocol) verwendet wird
NDMPENABLEKEEPALIVE	Der TCP-Keepalive-Mechanismus
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme NDMPKEEPIDLEMINUTES	AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeDie Leerlaufzeit, bevor das erste TCP-Keepalive-Paket gesendet wird
Windows-BetriebssystemeNPBUFFERSIZE	Windows-BetriebssystemeDie Größe des Kommunikationspuffers für benannte Pipes
SHMPORT	AIX-Betriebssysteme Linux-BetriebssystemeDie TCP/IP-Anschlussadresse eines Servers bei Verwendung von gemeinsam genutztem Speicher Windows-BetriebssystemeDer Anschluss, an dem der Server für Verbindungen mit gemeinsam genutztem Speicher empfangsbereit ist
SNMPHEARTBEATINTERVAL	Intervall in Minuten zwischen den Abfragen des IBM Spectrum Protect-Servers
SNMPMESSAGECATEGORY	Die beim Weiterleiten von Nachrichten von dem Server verwendeten Abfangarten
SNMPSUBAGENT	Die Parameter, die erforderlich sind, damit der IBM Spectrum Protect-Subagent mit dem SNMP-Dämon kommunizieren kann
SNMPSUBAGENTHOST	Der Standort des IBM Spectrum Protect SNMP-Subagenten
SNMPSUBAGENTPORT	Die Anschlussadresse des IBM Spectrum Protect SNMP-Subagenten
SSLFIPSMODE	Gibt an, ob der FIPS-Modus (Federal Information Processing Standards) für Secure Sockets Layer (SSL) aktiv ist
SSLTCPADMINPORT	Die Anschlussadresse, an der der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für SSL-aktivierte Sitzungen für den Verwaltungsbefehlszeilenclient wartet

Option	Beschreibung
SSLTCPPORT	Die SSL-Anschlussnummer, an der der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für SSL-aktivierte Sitzungen aus den folgenden Quellen wartet: • Befehlszeilenclient für Sichern/Archivieren • GUI des Clients für Sichern/Archivieren • Verwaltungsclient • Anwendungsprogrammierschnittstelle (API)
TCPADMINPORT	Die TCP/IP-Anschlussnummer für Verwaltungssitzungen
AIX-BetriebssystemeLinux-BetriebssystemeTCPBUFSIZE	AIX-Betriebssysteme Linux-BetriebssystemeDie Größe des Puffers, der für TCP/IP-Sendeanforderungen verwendet wird
TCPPORT	Die TCP/IP-Anschlussnummer für Clientsitzungen
TCPWINDOWSIZE	Das TCP/IP-Schiebefenster des Clientknotens

Optionen für den Serverspeicher

IBM Spectrum Protect stellt eine Reihe von Optionen bereit, mit denen Sie bestimmte Operationen für Einheiten und Serverspeicher konfigurieren können.

Tabelle 1. Optionen für den Serverspeicher

Option	Beschreibung
3494SHARED	Ermöglicht die gemeinsame Nutzung eines Speicherarchivs 3494 mit anderen Anwendungen als IBM Spectrum Protect.
ACSACCESSID	Die ID für die ACS-Zugriffssteuerung.
ACSLOCKDRIVE	Ermöglicht das Sperren der Laufwerke in den ACSLS-Speicherarchiven.
ACSQUICKINIT	Ermöglicht eine schnelle oder vollständige Initialisierung des ACSLS-Speicherarchivs.
ACSTIMEOUTX	Das Vielfache des integrierten Zeitlimitwerts für die ACSLS-API.
ASSISTVCRRECOVERY	Gibt an, ob der Server ein Laufwerk IBM 3590 bei der Wiederherstellung nach verloren gegangenen oder beschädigten VCR (Vital Cartridge Records) unterstützt.
CHECKTAPEPOS	Gibt an, ob der Server die Datenposition auf Band überprüft.
CLIENTDEDUPTXNLIMIT	Gibt die maximale Größe einer Transaktion an, wenn clientseitig deduplizierte Daten gesichert oder archiviert werden.
DEDUPREQUIRESBACKUP	Gibt an, ob Datenträger in primären Speicherpools mit sequenziellem Zugriff, die für die Datendeduplizierung definiert sind, wiederhergestellt werden können und ob doppelte Daten gelöscht werden können, bevor die Speicherpools gesichert werden.
DEDUPTIER2FILESIZE	Dateigröße, bei der die Schicht 2-Verarbeitung für die Datendeduplizierung verwendet wird.
DEDUPTIER3FILESIZE	Dateigröße, bei der die Schicht 3-Verarbeitung für die Datendeduplizierung verwendet wird.
DEVCONFIG	Der Name der Datei, in der Sicherungskopien der Einheitenkonfigurationsinformationen gespeichert werden.
DRIVEACQUIRERETRY	Gibt an, wie oft der Server versucht, ein Laufwerk in einem Speicherarchiv IBM 349x anzufordern, das von mehreren Anwendungen gemeinsam genutzt wird.
ENABLENASDEDUP	Gibt an, ob der Server Daten dedupliziert, die von einem NetApp NAS-Dateiserver gespeichert werden
NUMOPENVOLSALLOWED	Die Anzahl der FILE-Eingabedatenträger in einem deduplizierten Speicherpool, die gleichzeitig geöffnet sein können.
RECLAIMDELAY	Die Anzahl der Tage, um die die Wiederherstellung eines SnapLock-Datenträgers verzögert wird.

Option	Beschreibung
RECLAIMPERIOD	Die Anzahl der Tage für den Wiederherstellungszeitraum eines SnapLock-Datenträgers
RESOURCETIMEOUT	Angabe, wie lange der Server auf eine Ressource wartet, bevor die anstehende Anforderung der Ressource abgebrochen wird.
RETENTIONEXTENSION	Die Anzahl der Tage, um die das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers verlängert werden soll.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeSANDISCOVERY	AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeAngabe, ob die IBM Spectrum Protect-SAN-Erkennungsfunktion aktiviert ist.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme SANDISCOVERYTIMEOUT	AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeDie Zeit, bevor bei dem SAN-Erkennungsprozess eine Zeitlimitüberschreitung auftritt.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme SANREFRESHTIME	AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeDie Zeit, bevor zwischengespeicherte SAN-Erkennungsinformationen aktualisiert werden.
SEARCHMPQUEUE	Die Reihenfolge, in der der Server Anforderungen in der Ladewarteschlange ausführt.
SERVERDEDUPTXNLIMIT	Gibt die maximale Größe von Objekten an, die auf dem Server dedupliziert werden können

Client/Server-Optionen

Sie können Serveroptionen verwenden, um die Client/Server-Verarbeitung zu steuern.

Tabelle 1. Client/Server-Optionen

Option	Beschreibung
COMMTIMEOUT	Die Anzahl Sekunden, die der Server auf eine Antwort von einem Client wartet, bevor die Clientsitzung wegen Zeitüberschreitung beendet wird.
DISABLESCHEDS	Angabe, ob Verwaltungszeitpläne und Clientzeitpläne während der Wiederherstellung des IBM Spectrum Protect-Servers inaktiviert werden
IDLETIMEOUT	Die Anzahl Minuten, die eine Clientsitzung inaktiv sein darf, bevor der Server die Clientsitzung wegen Zeitüberschreitung beendet.
MAXSESSIONS	Die maximal zulässige Anzahl gleichzeitig stattfindender Clientsitzungen für den Server.
THROUGHPUTDATATHRESHOLD	Die Durchsatzschwelle, die eine Clientsitzung erreichen muss, damit sie nicht abgebrochen wird, wenn die Zeitschwelle erreicht wird
THROUGHPUTTIMETHRESHOLD	Die Zeitschwelle für eine Sitzung, nach deren Ablauf die Sitzung aufgrund zu geringen Durchsatzes abgebrochen werden kann
VERBCHECK	Angabe, ob eine zusätzliche Fehlerprüfung für Befehle erfolgt, die vom Client gesendet werden

Optionen für Datum, Zahlen, Uhrzeit und Sprache

Sie können Serveroptionen verwenden, um Anzeigeformate für Datums-, Uhrzeit- und Zahlenangaben sowie für die Landessprache anzugeben.

Tabelle 1. Optionen für Datum, Zahlen, Uhrzeit und Sprache

Option	Beschreibung
Windows-BetriebssystemeDATEFORMAT	Windows-BetriebssystemeDas Anzeigeformat für Datumsangaben
LANGUAGE	Clientnachrichten werden in der Landessprache angezeigt.
Windows-Betriebssysteme NUMBERFORMAT	Windows-BetriebssystemeDas Anzeigeformat für Zahlen
Windows-BetriebssystemeTIMEFORMAT	Windows-BetriebssystemeDas Anzeigeformat für Uhrzeitangaben

Datenbankoptionen

Mit Serveroptionen können Sie bestimmte Aspekte bei der Datenbankverarbeitung steuern.

Tabelle 1. Datenbankoptionen

Option	Beschreibung
ACTIVELOGDIRECTORY	Das neue Verzeichnis für die Position, an der die aktive Protokolldatei gespeichert wird. Verwenden Sie diese Option, um die Position der aktiven Protokolldatei zu ändern.
ACTIVELOGSIZE	Die maximale Größe der aktiven Protokolldatei.
ALLOWREORGINDEX	Vom Server eingeleitete Indexreorganisation.
ALLOWREORGTABLE	Vom Server eingeleitete Tabellenreorganisation.
ARCHLOGDIRECTORY	Das Verzeichnis, in dem der Datenbankmanager eine Protokolldatei archivieren kann, nachdem alle in dieser Protokolldatei angegebenen Transaktionen abgeschlossen wurden.
ARCHFAILOVERLOGDIRECTORY	Das Verzeichnis, in dem der Server Archivprotokolldateien speichert, die nicht im Verzeichnis für Archivprotokolle gespeichert werden können.
DBDIAGLOGSIZE	Die maximale Größe der Diagnoseprotokolldateien des Datenbankmanagers.
DBDIAGPATHFSTHRESHOLD	Der Schwellenwert für freien Speicherbereich in dem Dateisystem oder auf der Platte, das bzw. die die Diagnoseprotokolldateien des Datenbankmanagers enthält.
DBMEMPERCENT	Der Prozentsatz des Systemspeichers, der der Datenbank zugeordnet ist.
DISABLEREORGTABLE	Inaktivierung der Tabellenreorganisation für bestimmte Tabellen.
FSUSEDTHRESHOLD	Der Prozentsatz des Dateisystems, der von der Datenbank verwendet werden kann, bevor eine Alertnachricht ausgegeben wird.
MIRRORLOGDIRECTORY	Das Verzeichnis zum Spiegeln des Pfads für aktive Protokolldateien.
REORGBEGINTIME	Die früheste Zeit, zu der der IBM Spectrum Protect-Server eine Tabellen- oder Indexreorganisation starten kann.
REORGDURATION	Das Intervall, in dem eine vom Server eingeleitete Tabellen- oder Indexreorganisation starten kann.

Datenübertragungsoptionen

Mit Serveroptionen können Sie steuern, wie IBM Spectrum Protect Daten gruppiert und überträgt.

Tabelle 1. Gruppenoptionen

Option	Beschreibung
MOVEBATCHSIZE	Die Anzahl Dateien, die innerhalb einer Transaktion als Stapel gruppiert und versetzt werden sollen.
MOVESIZETHRESH	Gibt den Grenzwert für die innerhalb einer Transaktion als Stapel zu versetzende Datenmenge an.
NDMPPORTRANGE	Die IP-Adresse, die der Schnittstelle zugeordnet ist, in der der Server alle NDMP-Sicherungsdaten (NDMP = Network Data Management Protocol) empfängt
NDMPPREFDATAINTERFACE	Die IP-Adresse, die der Schnittstelle zugeordnet ist, in der der Server alle NDMP-Sicherungsdaten (NDMP = Network Data Management Protocol) empfängt
REPLBATCHSIZE	Die Anzahl Dateien, die innerhalb derselben Servertransaktion als Stapel repliziert werden sollen.
REPLSIZETHRESH	Gibt den Grenzwert für die innerhalb derselben Servertransaktion als Stapel zu replizierende Datenmenge an.
TXNGROUPMAX	Die Anzahl Dateien, die als Gruppe zwischen einem Client und dem Server zwischen Transaktions-COMMIT-Punkten übertragen werden.

Nachrichtenoptionen

Mit Serveroptionen lässt sich die Nachrichtenausgabe in IBM Spectrum Protect flexibler gestalten.

Tabelle 1. Nachrichtenoptionen

Option	Beschreibung
EXPQUIET	Angabe, ob IBM Spectrum Protect detaillierte Informationsnachrichten während der Verfallsverarbeitung sendet

Option	Beschreibung
MESSAGEFORMAT	Angabe, ob eine Nachrichtennummer in allen Zeilen angezeigt wird, wenn sich die Nachricht über mehrere Zeilen erstreckt
MSGINTERVAL	Die Zeit in Minuten zwischen Nachrichten, in denen ein Bediener zum Einlegen eines Bands für IBM Spectrum Protect aufgefordert wird

Optionen für die Aufzeichnung des Ereignisprotokolls

Optionen können bei der Verwaltung von Ereignisprotokollempfängern helfen.

Tabelle 1. Optionen für die Aufzeichnung des Ereignisprotokolls

Option	Beschreibung
EVENTSERVER	Angabe, ob der Server beim Serverstart eine Verbindung zum Ereignisserver herstellen soll.
FILEEXIT	Eine Datei, an die aktivierte Ereignisse weitergeleitet werden (binäres Format)
FILETEXTEXIT	Eine Datei, an die aktivierte Ereignisse weitergeleitet werden (lesbares Format)
REPORTRETRIEVE	Zeichnet Clientzurückschreibungs- und -abrufoperationen auf
TECBEGINEVENTLOGGING	Angabe, ob die Ereignisprotokollierung für den TIVOLI-Empfänger beim Serverstart beginnen soll.
TECHOST	Der Hostname oder die IP-Adresse für den Tivoli Enterprise Console-Ereignisserver (TEC-Ereignisserver)
TECPORT	Die TCP/IP-Anschlussadresse, an der der Tivoli Enterprise Console-Ereignisserver empfangsbereit ist
TECUTF8EVENT	Ein Tivoli Enterprise Console-Ereignis, das vom IBM Spectrum Protect-Server im UTF8-Format gesendet wurde
UNIQUETDPTECEVENTS	Ereignisse von einem IBM Spectrum Protect Data Protection-Client, die als eindeutige Ereignisse an die Tivoli Enterprise Console gesendet werden
UNIQUETECEVENTS	Ereignisse, die als eindeutige Ereignisse an die Tivoli Enterprise Console gesendet werden
USEREXIT	Ein benutzerdefinierter Exit, dem die Steuerung für die Verwaltung eines Ereignisses übergeben wird

Optionen für Sicherheit und Lizenzierung

Sie können Serveroptionen verwenden, um Serversicherheits- und -lizenzprüfungen anzupassen.

Tabelle 1. Optionen für Sicherheit und Lizenzierung

Option	Beschreibung
Windows-Betriebssysteme ADSMGROUPNAME	Windows-BetriebssystemeDer Name einer Windows-Gruppe
AUDITSTORAGE	Gibt an, dass der Server als Teil einer Lizenzprüfung den Umfang des belegten Sicherungs-, Archivierungs- und Speicherverwaltungsspeichers nach Knoten berechnet
BACKUPINITIATIONROOT	Gibt an, ob der Server Knotenparameterwerte für Benutzer überschreibt, die keine berechtigten IBM Spectrum Protect-Benutzer sind.
LDAPURL	Gibt den LDAP-Verzeichnisserver an. Jede Einstellung muss den Namen des LDAP-Verzeichnisservers, eine Anschlussnummer und den Basis-DN des Namensbereichs (oder Suffix) enthalten, den der Server verwaltet.
Windows-Betriebssysteme NPAUDITFAILURE	Windows-BetriebssystemeGibt an, dass ein Knoten nur auf seine eigenen Daten zugreifen kann
Windows-Betriebssysteme NPAUDITSUCCESS	Windows-BetriebssystemeGibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknotenbenutzer über SECUREPIPE eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann
QUERYAUTH	Die Administratorberechtigungsstufe, die für die Ausgabe des Befehls QUERY oder SQL SELECT erforderlich ist
REQSYSAUTHOUTFILE	Gibt an, ob die Systemberechtigung für Verwaltungsbefehle erforderlich ist, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben

Option	Beschreibung
Windows-BetriebssystemeSECUREPIPES	Windows-BetriebssystemeGibt bei Verwendung des Protokolls für benannte Pipes an, dass der Server die Windows-Gruppe überprüft, um einen Client zu authentifizieren
SHREDDING	Gibt an, ob das Schreddern von gelöschten sensiblen Daten automatisch oder manuell ausgeführt wird

Zugehörige Verweise:
Serverübertragungsoptionen

Weitere Optionen

Sie können eine Vielzahl anderer Serveroptionen verwenden, um IBM Spectrum Protect anzupassen.

Tabelle 1. Weitere Optionen

Option	Beschreibung
ALIASHALT	Ermöglicht es Administratoren, dem IBM Spectrum Protect-Befehl HALT einen anderen Namen zuzuordnen
DISPLAYLFINFO	Gibt an, ob Abrechnungssätze und Einträge in der Übersichtstabelle den Speicheragentennamen angeben
EXPINTERVAL	Das Intervall zwischen automatischen Datenträgerbestandsverfallsprozessen.
FFDCLOGNAME	Der Name für das FFDC-Protokoll (FFDC = First-Failure Data Capture)
FFDCMAXLOGSIZE	Die maximale Größe des FFDC-Protokolls (FFDC = First-Failure Data Capture)
NOPREEMPT	Gibt an, dass keine Operation das Zugriffsvorrecht auf einen Datenträger besitzen soll. Lediglich einer Datenbanksicherungsoperation kann das Zugriffsvorrecht vor einer anderen Operation eingeräumt werden.
NORETRIEVEDATE	Gibt an, dass der Server das Abrufdatum einer Datei in einem Plattenspeicherpool nicht aktualisiert, wenn ein Client die Datei zurückschreibt oder abruft
RESTOREINTERVAL	Gibt an, wie lange eine wiederanlauffähige Zurückschreibungssitzung in der Serverdatenbank gesichert werden kann
VOLUMEHISTORY	Der Name der Datei, die automatisch aktualisiert werden soll, wenn sich History-Informationen von sequenziellen Datenträgern des Servers ändern

3494SHARED

Die Option 3494SHARED gibt an, ob ein Kassettenarchiv IBM® 3494 andere Anwendungen als IBM Spectrum Protect gemeinsam benutzen kann.

Der Standardwert lautet NO. Dieser Standardwert bedeutet, dass keine andere Anwendung als IBM Spectrum Protect das 3494-Kassettenarchiv verwenden kann. Wird diese Option auf YES gesetzt, bestimmt IBM Spectrum Protect für jede Ladeanforderung, ob alle Laufwerke in Gebrauch sind. Nach Beendigung der Abfrage wählt IBM Spectrum Protect ein verfügbares Laufwerk aus, das nicht von einer anderen Anwendung verwendet wird. Die gemeinsame Benutzung sollte nur aktiviert werden, wenn mehr als zwei Laufwerke in dem Kassettenarchiv vorhanden sind. Wird gerade ein Kassettenarchiv IBM 3494 mit anderen Anwendungen gemeinsam benutzt, muss diese Option angegeben werden.

Syntax

```
>>-3494SHARED--+-Yes-+-----------------------------------------><
               '-No--'
```

Parameter

Yes
: Gibt an, dass andere Anwendungen das 3494-Kassettenarchiv verwenden können.

No
: Gibt an, dass keine anderen Anwendungen das 3494-Kassettenarchiv verwenden können.

Beispiele

Die gemeinsame Benutzung eines 3494-Kassettenarchivs aktivieren:

```
3494shared yes
```

ACSACCESSID

Die Option ACSACCESSID gibt die ID für die ACS-Zugriffssteuerung eines ACSLS-Kassettenarchivs an.

Syntax

```
>>-ACSACCESSID--Name-----------------------------------------><
```

Parameter

Name
: Gibt eine ID an, die aus 1 bis 64 Zeichen besteht. Die Standard-ID ist der Name des lokalen Hosts.

Beispiele

```
acsaccessid region
```

ACSLOCKDRIVE

Die Option ACSLOCKDRIVE gibt an, ob die Laufwerke in den ACSLS-Kassettenarchiven gesperrt sind. Durch das Sperren von Laufwerken wird die exklusive Benutzung der Laufwerke in dem ACSLS-Kassettenarchiv in einer gemeinsamen Umgebung sichergestellt. Die Leistung ist jedoch etwas besser, wenn Kassettenarchive nicht gesperrt werden. Wenn andere Anwendungen die IBM Spectrum Protect-Laufwerke nicht verwenden, ist das Sperren der Laufwerke nicht erforderlich.

Syntax

```
>>-ACSLOCKDRIVE--+-Yes-+--------------------------------------><
                 '-No--'
```

Parameter

Yes
: Gibt an, dass die Laufwerke gesperrt sind.

No
: Gibt an, dass die Laufwerke nicht gesperrt sind.

Beispiele

```
acslockdrive yes
```

ACSQUICKINIT

Die Option ACSQUICKINIT gibt an, ob die Initialisierung des ACSLS-Kassettenarchivs beim Serverstart eine schnelle oder vollständige Initialisierung ist. Der Standardwert ist 'Yes'. Eine schnelle Initialisierung vermeidet den Aufwand, der mit der Synchronisation des Datenträgerbestands des IBM Spectrum Protect-Servers mit dem Datenträgerbestand des ACSLS-Kassettenarchivs verbunden ist (durch eine Prüfung des Kassettenarchivs).

Syntax

```
>>-ACSQUICKINIT--+-Yes-+---------------------------------------><
                '-No--'
```

Parameter

Yes

Gibt an, dass eine schnelle Initialisierung des ACSLS-Kassettenarchivs ausgeführt wird. Wird die Option auf Yes gesetzt, übergeht IBM Spectrum Protect die Überprüfung des Datenträgerbestands im Kassettenarchiv. Das Kassettenarchiv wird schnell initialisiert und IBM Spectrum Protect schneller zur Verfügung gestellt als bei einer vollständigen Initialisierung.

Diese Option sollte auf Yes gesetzt werden, wenn bekannt ist, dass sich der Datenträgerbestand des physischen Kassettenarchivs und der Datenträgerbestand im IBM Spectrum Protect-Kassettenarchiv nicht geändert haben und eine Prüfung nicht erforderlich ist.

No

Gibt an, dass eine vollständige Initialisierung des ACSLS-Kassettenarchivs und des Datenträgerbestands im Kassettenarchiv ausgeführt wird. Wird die Option auf No gesetzt, synchronisiert IBM Spectrum Protect seinen Datenträgerbestand im Kassettenarchiv mit dem Bestand, der vom ACSLS-Kassettenarchivmanager zurückgemeldet wird.

Beispiele

```
acsquickinit yes
```

ACSTIMEOUTX

Die Option ACSTIMEOUTX gibt das Vielfache des integrierten Zeitlimitwerts für ACSLS-APIs an. Der integrierte Zeitlimitwert für die ENTER-, EJECT- und AUDIT-ACS-API beträgt 1800 Sekunden; für alle anderen ACSLS-APIs beträgt der Wert 600 Sekunden. Lautet das angegebene Vielfache beispielsweise 5, beträgt der Zeitlimitwert für die Prüf-API 9000 Sekunden und für alle anderen APIs 3000 Sekunden.

Syntax

```
>>-ACSTIMEOUTX--Wert-----------------------------------------><
```

Parameter

Wert
Gibt das Vielfache des integrierten Zeitlimitwerts für die ACSLS-API an. Der Bereich liegt zwischen 1 und 100. Der Standardwert ist 1.

Beispiele

```
acstimeoutx 1
```

ACTIVELOGDIRECTORY

Die Option ACTIVELOGDIRECTORY gibt den Namen des Verzeichnisses an, in dem alle aktiven Protokolldateien gespeichert werden.

Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSERV FORMAT ausgeführt wird. Unter normalen Betriebsbedingungen muss die Option nicht geändert werden. In DSMSERV FORMAT (Datenbank und Protokoll formatieren) befinden sich Anleitungen zur Verwendung dieser Option.

Syntax

```
>>-ACTIVELOGDirectory--Verzeichnisname------------------------><
```

Parameter

Verzeichnisname
Gibt einen vollständig qualifizierten Verzeichnisnamen an. Das Verzeichnis muss vorhanden sein, es muss leer sein, und auf das Verzeichnis muss durch die Benutzer-ID des Datenbankmanagers zugegriffen werden können. Wird das Verzeichnis für aktive Protokolldateien geändert, versetzt IBM Spectrum Protect die vorhandenen aktiven Protokolldateien an die Position, die durch dieses Verzeichnis angegeben ist. Die maximale Anzahl Zeichen beträgt 175.

Beispiele

AIX-Betriebssysteme Linux-Betriebssysteme

```
activelogdirectory /tsm/activelogdir
```

Windows-Betriebssysteme

```
activelogdirectory c:\tsmserv1\activelogdir
```

ACTIVELOGSIZE

Die Option ACTIVELOGSIZE definiert die Gesamtgröße der Protokolldatei.

Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSERV FORMAT ausgeführt wird. Unter normalen Betriebsbedingungen muss die Option nicht geändert werden. In DSMSERV FORMAT (Datenbank und Protokoll formatieren) befinden sich Anleitungen zur Verwendung dieser Option.

Syntax

```
                  .-16GB-----.
>>-ACTIVELOGSize--+-Megabyte-+--------------------------------><
```

Parameter

Megabyte
: Gibt die Größe der aktiven Protokolldatei in Megabyte an. Der Mindestwert ist 2048 MB (2 GB); der Maximalwert ist 524.288 MB (512 GB). Wenn eine ungerade Zahl angegeben wird, wird der Wert auf die nächste gerade Zahl aufgerundet. Der Standardwert ist 16.384 MB (16 GB).
Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Richtlinien für den Speicherbedarf befinden sich in der folgenden Tabelle:

Tabelle 1. Schätzung des Datenträger- und Dateispeicherbedarfs

Wert der Option ACTIVELOGSize	Reservieren Sie diesen freien Speicherbereich im Verzeichnis für aktive Protokolldateien, zusätzlich zum Speicherbereich von ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

Beispiele

```
activelogsize 8192
```

ADMINCOMMTIMEOUT

Die Option ADMINCOMMTIMEOUT gibt an, wie lange der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine erwartete Verwaltungsclientnachricht wartet.

Wenn die Zeitlänge dieses Zeitlimit überschreitet, beendet der Server die Sitzung mit dem Verwaltungsclient. Sie können den Wert für das Zeitlimit erhöhen, um zu verhindern, dass bei Verwaltungsclientsitzungen eine Zeitlimitüberschreitung auftritt.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
                     .-60-------.
>>-ADMINCOMMTimeout--+-Sekunden-+------------------------------><
```

Parameter

Sekunden
: Gibt die maximale Anzahl Sekunden an, die ein Server auf eine Antwort des Verwaltungsclients wartet. Der Standardwert ist 60. Der Mindestwert ist 1.

Beispiele

```
admincommtimeout 60
```

ADMINIDLETIMEOUT

Die Option ADMINIDLETIMEOUT gibt die Zeit in Minuten an, die eine Verwaltungsclientsitzung inaktiv sein kann, bevor der Server die Sitzung abbricht.

Bei einer hohen Netzauslastung in Ihrer Umgebung können Sie den Wert für das Zeitlimit erhöhen, um zu verhindern, dass bei Verwaltungsclients eine Zeitlimitüberschreitung auftritt. Eine große Anzahl von inaktiven Sitzungen kann jedoch verhindern, dass andere Benutzer eine Verbindung zum Server herstellen können.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
                    .-15------.
>>-ADMINIDLETIMEOUT--+-Minuten-+------------------------------><
```

Parameter

Minuten
: Gibt die maximale Anzahl Minuten an, die ein Server auf einen inaktiven Verwaltungsclient wartet. Der Standardwert ist 15 Minuten. Der Mindestwert ist 1 Minute.

Beispiele

```
adminidletimeout 20
```

ADMINONCLIENTPORT

Die Option ADMINONCLIENTPORT gibt an, ob TCPPORT von Verwaltungssitzungen verwendet werden kann. Der Standardwert ist YES.

Syntax

```
>>-ADMINONCLIENTPORT--+-YES-+----------------------------------><
                      '-NO--'
```

Parameter

YES
: Ist die Option auf YES gesetzt, oder haben TCPPORT und TCPADMINPORT denselben Wert (Standardwert), können Verwaltungssitzungen TCPPORT verwenden.

NO
: Ist die Option auf NO gesetzt, und weicht der Wert für TCPADMINPORT von dem Wert für TCPPORT ab, können Verwaltungssitzungen TCPPORT nicht verwenden.

Beispiele

Angeben, dass TCPPORT von Verwaltungssitzungen verwendet werden kann.

```
adminonclientport yes
```

 Windows-Betriebssysteme

ADSMGROUPNAME

Die Option ADSMGROUPNAME gibt den Namen einer Windows-Gruppe an. Ein Clientknoten muss Teil dieser Gruppe sein, um mit dem IBM Spectrum Protect-Server über NT Unified Logon arbeiten zu können. Der Clientknoten muss außerdem als IBM Spectrum Protect-Clientknoten registriert sein.

Syntax

```
>>-ADSMGROUPname--Gruppenname---------------------------------><
```

Parameter

Gruppenname
: Gibt einen Windows-Gruppennamen an.

Beispiele

IDD als Windows-Gruppe angeben:

```
adsmgroup idd
```

ALIASHALT

Die Option ALIASHALT ermöglicht es Administratoren, dem IBM Spectrum Protect-Befehl **HALT** einen anderen Namen zuzuordnen.

Der Verwaltungsclient erkennt einen Aliasnamen für den Befehl HALT, wenn der Client mit der angegebenen Option CHECKALIASHALT gestartet wird. Für ausführliche Informationen siehe Verwaltungsclientoptionen.

Syntax

```
>>-ALIASHALT--neuer_Name----------------------------------------><
```

Parameter

neuer_Name
: Gibt den Aliasnamen des Befehls HALT zum Herunterfahren des IBM Spectrum Protect-Servers an. Die Mindestlänge für *Neuer Name* beträgt 1; die maximale Länge beträgt 16.

Beispiele

```
aliashalt tsmhalt
```

ALLOWDESAUTH

Die Option ALLOWDESAUTH gibt an, ob die Verwendung von Data Encryption Standard (DES) für die Authentifizierung zwischen einem Server und einem Client für Sichern/Archivieren zulässig ist.

Um die Verwendung von DES zu verhindern, geben Sie den Wert NO für die Option ALLOWDESAUTH an.
Um den IBM Spectrum Protect-Server für die Konformität mit dem Standard NIST SP800-131A zu konfigurieren, setzen Sie diese Option auf NO.
Einschränkungen:

- Auf dem Client für Sichern/Archivieren muss Version 6.3 oder höher ausgeführt werden, wenn Sie sich mit dem Wert NO für die Option ALLOWDESAUTH bei einem Server authentifizieren.
- Die automatische Implementierung des Clients für Sichern/Archivieren schlägt fehl, wenn diese Option auf NO gesetzt wird.

Syntax

```
   .-ALLOWDESAUTH--Yes-----.
>>-+-----------------------+-----------------------------------><
   '-ALLOWDESAUTH--+-No--+-'
                   '-Yes-'
```

Parameter

Yes
: Gibt an, dass der Server die Authentifizierung mit Clients für Sichern/Archivieren zulässt, die die DES-basierte Verschlüsselung verwenden. Der Standardwert ist YES.

No
: Gibt an, dass der Server alle Clients für Sichern/Archivieren zurückweist, die versuchen, sich mit der DES-basierten Verschlüsselung zu authentifizieren.

Beispiele

Angeben, dass der Server alle Clients für Sichern/Archivieren zurückweist, die versuchen, sich mit der DES-Verschlüsselung zu authentifizieren:

```
allowdesauth no
```

Angeben, dass der Server die Authentifizierung mit Clients für Sichern/Archivieren zulässt, die die DES-Verschlüsselung verwenden:

```
allowdesauth yes
```

ALLOWREORGINDEX

Die Option ALLOWREORGINDEX gibt an, ob die vom Server eingeleitete Indexreorganisation aktiviert oder inaktiviert ist.

Der Standardwert ist YES.

Syntax

```
>>-ALLOWREORGINDEX--+-Yes-+-------------------------------------><
                    '-No--'
```

Parameter

Yes
: Gibt an, dass die vom Server eingeleitete Indexreorganisation aktiviert ist.

No
: Gibt an, dass die vom Server eingeleitete Indexreorganisation inaktiviert ist.

Beispiel

Angeben, dass die vom Server eingeleitete Indexreorganisation aktiviert ist.

```
allowreorgindex yes
```

ALLOWREORGTABLE

Die Option ALLOWREORGTABLE gibt an, ob die vom Server eingeleitete Tabellenreorganisation aktiviert oder inaktiviert ist.

Der Standardwert ist YES.

Syntax

```
>>-ALLOWREORGTABLE--+-Yes-+-------------------------------------><
                    '-No--'
```

Parameter

Yes
: Gibt an, dass die vom Server eingeleitete Tabellenreorganisation aktiviert ist.

No
: Gibt an, dass die vom Server eingeleitete Tabellenreorganisation inaktiviert ist.

Beispiele

Angeben, dass die vom Server eingeleitete Tabellenreorganisation inaktiviert ist.

```
allowreorgtable no
```

ARCHFAILOVERLOGDIRECTORY

Die Option ARCHFAILOVERLOGDIRECTORY gibt das Verzeichnis an, das der Server zum Speichern der Archivprotokolldateien verwendet, die nicht im Verzeichnis für Archivprotokolle gespeichert werden können.

Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSERV FORMAT ausgeführt wird. Normalerweise muss das Verzeichnis nicht geändert werden.

Syntax

```
>>-ARCHFailoverlogdirectory--Verzeichnisname-------------------><
```

Parameter

Verzeichnisname
: Gibt einen vollständig qualifizierten Verzeichnisnamen an. Die maximale Anzahl Zeichen beträgt 175.

Beispiele

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
archfailoverlogdirectory /tsm/archfailoverlog
```

 Windows-Betriebssysteme

```
archfailoverlogdirectory c:\tsmserv1\archfailoverlog
```

ARCHLOGCOMPRESS

Sie können die Komprimierung von Archivprotokollen auf dem IBM Spectrum Protect-Server aktivieren oder inaktivieren. Durch die Komprimierung der Archivprotokolle wird der Speicherbedarf reduziert, der für die Speicherung erforderlich ist.

Die Serveroption ARCHLOGCOMPRESS gibt an, ob Protokolldateien, die in das Archivverzeichnis für Protokolle geschrieben werden, komprimiert werden.

Syntax

```
                    .-No--.
>>-ARCHLOGCOMPress--+-----+-----------------------------------><
                    '-Yes-'
```

Parameter

No
: Gibt an, dass Protokolldateien, die in das Archivprotokollverzeichnis geschrieben werden, nicht komprimiert werden. Der Standardwert ist 'No'.

Yes
: Gibt an, dass Protokolldateien, die in das Archivprotokollverzeichnis geschrieben werden, komprimiert werden.

Einschränkung: Gehen Sie mit Vorsicht vor, wenn Sie die Serveroption ARCHLOGCOMPRESS auf Systemen mit kontinuierlich hoher Datenträgerverwendung und hoher Auslastung aktivieren. Die Aktivierung dieser Option in dieser Systemumgebung kann Verzögerungen beim Archivieren von Protokolldateien aus dem Dateisystem für aktive Protokolldateien in das Archivprotokolldateisystem zur Folge haben. Diese Verzögerung kann zur Folge haben, dass für das Dateisystem für aktive Protokolldateien der Speicherbereich knapp wird. Stellen Sie sicher, dass der verfügbare Speicherbereich im Dateisystem für aktive Protokolldateien überwacht wird, nachdem die Komprimierung für das Archivprotokoll aktiviert wurde. Wenn die Belegung des Dateisystems für das Verzeichnis für aktive Protokolldateien derart hoch ist, dass fast kein Speicherbereich mehr verfügbar ist, muss die Serveroption ARCHLOGCOMPRESS inaktiviert werden. Mit dem Befehl SETOPT kann die Komprimierung für das Archivprotokoll sofort inaktiviert werden, ohne dass der Server angehalten werden müsste.

Beispiel

Um die Komprimierung von Protokolldateien zu aktivieren, die in das Archivprotokollverzeichnis geschrieben werden, geben Sie die folgende Option an:

```
archlogcompress yes
```

ARCHLOGDIRECTORY

Die Option ARCHLOGDIRECTORY gibt ein Verzeichnis an, in dem der Datenbankmanager eine Protokolldatei archivieren kann, nachdem alle in dieser Protokolldatei angegebenen Transaktionen abgeschlossen wurden.

Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSERV FORMAT ausgeführt wird.

Syntax

```
>>-ARCHLOGDirectory--Verzeichnisname--------------------------><
```

Parameter

Verzeichnisname
: Gibt einen vollständig qualifizierten Verzeichnisnamen an. Die maximale Anzahl Zeichen beträgt 175.

Beispiele

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
archlogdirectory /tsm/archlog
```

 Windows-Betriebssysteme

```
archlogdirectory d:\tsmserv1\archlog
```

ARCHLOGUSEDTHRESHOLD

Die Option ARCHLOGUSEDTHRESHOLD gibt an, wann eine automatische Datenbanksicherung in Relation zum Prozentsatz des belegten Speicherbereichs für die Archivprotokolldatei gestartet werden soll. Der Standardwert ist 80 Prozent.

Mit der Option ARCHLOGUSEDTHRESHOLD werden häufige automatische Sicherungen verhindert. Wenn sich beispielsweise das Verzeichnis für Archivprotokolldateien in einem Dateisystem oder auf einem Laufwerk mit 400 GB befindet, wird eine Datenbanksicherung ausgelöst, wenn weniger als 80 GB freier Speicherbereich verfügbar ist. Wiederholte Datenbanksicherungen können zur Folge haben, dass der Server eine übermäßige Anzahl Arbeitsbänder verwendet.

Syntax

```
                          .-80---.
>>-ARCHLOGUSEDTHRESHOLD--+-Wert-+-----------------------------><
```

Parameter

Wert
: Der Prozentsatz des belegten Speicherbereichs für die Archivprotokolldatei, bevor eine automatische Sicherung gestartet wird.

Angeben, dass eine automatische Sicherung gestartet werden soll, wenn 90 Prozent des Speicherbereichs für die Archivprotokolldatei belegt sind.

```
archlogusedthreshold 90
```

ASSISTVCRRECOVERY

Die Option ASSISTVCRRECOVERY gibt an, ob IBM Spectrum Protect ein Laufwerk IBM® 3590 bei der Wiederherstellung nach verloren gegangenen oder beschädigten VCR (Vital Cartridge Records) unterstützt. Wird YES (Standardwert) angegeben und erkennt IBM Spectrum Protect während der Ladeverarbeitung einen Fehler, geht TSM während der Entladeverarbeitung an das Datenende, um den Laufwerken die Wiederherstellung der VCR zu ermöglichen. Während der Bandoperation kann dies geringe Auswirkungen auf die Leistung haben, da das Laufwerk keine schnelle Suche mit einem verloren gegangenen oder beschädigten VCR ausführen kann. Es tritt jedoch kein Datenverlust auf.

Syntax

```
>>-ASSISTVCRRECovery--+-Yes-+-----------------------------------><
                      '-No--'
```

Parameter

Yes
: Gibt an, dass der Server die Wiederherstellung unterstützt.

No
: Gibt an, dass der Server die Wiederherstellung nicht unterstützt.

Beispiele

Unterstützung bei der Wiederherstellung inaktivieren:

```
assistvcrrecovery no
```

AUDITSTORAGE

Als Teil einer Lizenzprüfung berechnet der Server nach Knoten den Umfang des Serverspeichers, der für Sicherungsdateien, Archivierungsdateien und speicherverwaltete Dateien verwendet wird. Bei Servern, die umfangreiche Datenmengen verwalten, kann diese Berechnung sehr viel CPU-Zeit beanspruchen und andere Serveraktivitäten blockieren. Mit der Option AUDITSTORAGE kann angegeben werden, dass bei der Lizenzprüfung der Speicher nicht berechnet werden soll.

Anmerkung: Diese Option wurde zuvor NOAUDITSTORAGE genannt.

Syntax

```
>>-AUDITSTorage--+-Yes-+---------------------------------------><
                 '-No--'
```

Parameter

Yes
: Gibt an, dass der Speicher bei der Lizenzprüfung berechnet werden soll. Der Standardwert ist 'Yes'.

No
: Gibt an, dass der Speicher bei der Lizenzprüfung nicht berechnet werden soll.

Beispiele

```
auditstorage    yes
```

BACKUPINITIATIONROOT

Die Option BACKUPINITIATIONROOT gibt an, ob der Server Knotenparameterwerte für Benutzer überschreibt, die keine berechtigten IBM Spectrum Protect-Benutzer sind.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
>>-BACKUPINITIATIONROOT--+-ON--+-------------------------------><
                         '-OFf-'
```

Parameter

ON
: Gibt an, dass das Starten von Sicherungsoperationen in Sitzungen von Clients unter AIX-, Linux-, Mac OS X- und Solaris-Betriebssystemen verhindert wird, wenn die Benutzer keine berechtigten IBM Spectrum Protect-Benutzer sind. Dies ist der Standardwert. Der Server überschreibt den Wert für den Parameter BACKUPINITIATION in den Befehlen REGISTER NODE und UPDATE NODE.
Tipp: Eine Übersicht über berechtigte IBM Spectrum Protect-Benutzer finden Sie in Tasks für Rootbenutzer und berechtigte Benutzer des UNIX- und Linux-Clients.

OFf
: Gibt an, dass der Knotenwert für den Parameter BACKUPINITIATION verwendet wird. Der Parameter BACKUPINITIATION wird in den Befehlen REGISTER NODE und UPDATE NODE angegeben.

Beispiel

Angeben, dass der Knotenwert für den Parameter BACKUPINITIATION verwendet wird.

```
backupinitiationroot off
```

CHECKTAPEPOS

Die Option CHECKTAPEPOS gibt an, ob der IBM Spectrum Protect-Server die Position von Datenblöcken auf Band überprüft.

Die Option CHECKTAPEPOS gilt nur für Operationen, die Bandlaufwerke verwenden. Sie gilt nicht für Einheitenklassen mit sequenziellem Zugriff, die keine Bänder angeben, wie beispielsweise FILE. Wenn die Serverinformationen zur Position nicht mit der Position übereinstimmen, die von dem Laufwerk ermittelt wird, wird eine Fehlernachricht angezeigt, die Transaktion rückgängig gemacht, und die Daten werden nicht in der Datenbank festgeschrieben.

Mit der Option CHECKTAPEPOS können Sie den Modus 'Nur anhängen' für IBM LTO-Laufwerke der Generation 5 und später sowie für alle Laufwerke aktivieren, die diese Funktion unterstützen. Ist die Funktion aktiviert, gibt das Laufwerk einen Fehler aus, nachdem es Anweisungen zum Überschreiben von Daten auf dem gegenwärtig geladenen Datenträger empfangen hat. Das Band wird vom IBM Spectrum Protect-Server auf den korrekten Block neu positioniert und der Server setzt das Schreiben von Daten fort. Der Modus 'Nur anhängen' stellt einen zusätzlichen Schutz bereit, indem die meisten Situationen, in denen Daten überschrieben werden können, verhindert werden. Wenn Sie ein Laufwerk verwenden, das diese Funktion unterstützt, können Sie mit IBM Spectrum Protect und/oder dem Laufwerk die Datenposition auf dem Band überprüfen.

Anmerkung: Wenn Sie SAN-Bandbeschleunigungsfunktionen in der Struktur verwenden, setzen Sie CHECKTAPEPOS auf 'DRIVEonly' oder 'No', um falsche positive Positionierungsfehler zu vermeiden. Die IBM Spectrum Protect-Serveroption CHECKTAPEPOS erfordert kein für den Modus 'Nur anhängen' fähiges Laufwerk.

Änderungen an der Option CHECKTAPEPOS haben erst Auswirkungen auf Ladevorgänge, nachdem die Aktualisierung für das Laufwerk abgeschlossen wurde.

Der Standardwert ist YES.

Syntax

```
>>-CHECKTAPEPOS--+-Yes-------+---------------------------------><
                 +-No--------+
                 +-TSMonly---+
                 '-DRIVEonly-'
```

Parameter

Yes
: Gibt an, dass der IBM Spectrum Protect-Server die Datenposition auf Band überprüft. Für Laufwerke, die den Modus 'Nur anhängen' unterstützen, gibt dieser Parameter an, dass es IBM Spectrum Protect dem Laufwerk ermöglicht, ebenfalls die Datenposition während jeder WRITE-Operation zu überprüfen, um das Überschreiben von Daten zu verhindern. Yes ist der Standardwert.

No
: Gibt an, dass die Überprüfung der Datenposition inaktiviert ist.

TSMonly
: Gibt an, dass der IBM Spectrum Protect-Server die Datenposition auf Band überprüft. Der Server verwendet nicht den Modus 'Nur anhängen', auch wenn das Laufwerk die Funktion unterstützt.

DRIVEonly
: Gibt an, dass der IBM Spectrum Protect-Server den Modus 'Nur anhängen' für Laufwerke aktiviert, die diese Funktion unterstützen. Der Server überprüft nicht die Datenposition auf Band.

Beispiel

Die Datenposition auf Band überprüfen und den Modus 'Nur anhängen' für ein unterstütztes Laufwerk aktivieren:

```
checktapepos yes
```

CLIENTDEDUPTXNLIMIT

Die Option CLIENTDEDUPTXNLIMIT gibt die maximale Größe einer Transaktion an, wenn vom Client deduplizierte Daten gesichert oder archiviert werden.

Wenn die clientseitige Deduplizierung für große Objekte verwendet wird, können lange laufende Transaktionen, die zur Aktualisierung der Datenbank erforderlich sind, eine umfangreiche Datenbankaktivität zur Folge haben. Eine umfangreiche Datenbankaktivität kann die folgenden Symptome zur Folge haben:

- Reduzierter Durchsatz bei Clientsicherungs- und -archivierungsoperationen
- Ressourcenkonflikt aufgrund gleichzeitig ablaufender Serveroperationen
- Exzessive Wiederherstellungsprotokollaktivität

Das Ausmaß, in dem diese Symptome auftreten, hängt von der Anzahl und Größe der Objekte ab, die unter Verwendung der clientseitigen Deduplizierung von Daten gespeichert werden, von der Intensität und dem Typ der gleichzeitig ablaufenden Operationen auf dem IBM Spectrum Protect-Server und von der IBM Spectrum Protect-Serverkonfiguration.

Mit der Serveroption CLIENTDEDUPTXNLIMIT können Sie eine maximale Größe (in Gigabyte) für Transaktionen angeben, wenn vom Client deduplizierte Daten gesichert oder archiviert werden. Wenn ein Objekt oder eine Gruppe von Objekten in einer einzelnen Transaktion den mit

CLIENTDEDUPTXNLIMIT angegebenen Grenzwert überschreitet, werden die Objekte nicht vom Client dedupliziert, und die Transaktion kann fehlschlagen. Sie können einen Wert von 32 bis 102400 GB angeben. Der Standardwert ist 5120 GB.

Wenn ein Objekt oder eine Gruppe von Objekten in einer einzelnen Transaktion den mit CLIENTDEDUPTXNLIMIT angegebenen Grenzwert überschreitet, werden die Objekte oder wird die Gruppe von Objekten nicht vom Client dedupliziert. Die Objekte werden jedoch an den Server gesendet. Diese Objekte können auf dem Server dedupliziert werden, abhängig davon, ob der Zielspeicherpool für die Deduplizierung von Daten konfiguriert ist, und abhängig von dem Wert der Option SERVERDEDUPTXNLIMIT. Objekte in einem für die Deduplizierung aktivierten Speicherpool, die kleiner als der Wert der Option SERVERDEDUPTXNLIMIT sind, werden von einem Serverprozess zum Identifizieren doppelter Daten dedupliziert.

Der geeignete Wert für diese Option hängt von der IBM Spectrum Protect-Serverkonfiguration und der gleichzeitig stattfindenden Serveraktivität ab. Sie können einen hohen Wert für diese Option angeben, wenn Sie den Ressourcenkonflikt minimieren. Um den Ressourcenkonflikt zu minimieren, führen Sie Operationen, wie beispielsweise Sicherung, Archivierung, Identifizierung doppelter Daten (Befehl IDENTIFY DUPLICATES) und Wiederherstellung, zu unterschiedlichen Zeiten aus.

Um diese Serveroption zu aktualisieren, ohne den Server zu stoppen und erneut zu starten, verwenden Sie den Befehl SETOPT.

Syntax

```
                          .-5120-----.
>>-CLIENTDEDUPTXNlimit--+-Gigabyte-+--------------------------><
```

Parameter

Gigabyte
: Gibt die maximale Größe (in Gigabyte) von Objekten an, die unter Verwendung der clientseitigen Deduplizierung von Daten gesichert oder archiviert werden können. Sie können einen Wert von 32 bis 102400 angeben. Der Standardwert ist 5120.

Beispiele

Die clientseitige Deduplizierung von Daten für alle Objekte über 80 GB inaktivieren:

```
clientdeduptxnlimit 80
```

COMMMETHOD

Die Option COMMMETHOD gibt eine Übertragungsmethode an, die vom Server verwendet werden soll.

Sie können den Server für die Verwendung mehrerer Übertragungsmethoden konfigurieren. Die am häufigsten verwendeten Übertragungsmethoden sind TCPIP, V6TCPIP und SHAREDMEM. Um mehrere Übertragungsmethoden anzugeben, aktivieren Sie jede Methode, indem Sie eine Zeilengruppe COMMMETHOD zur Optionsdatei dsmserv.opt hinzufügen.

Wichtig: Bei der Aktivierung einer Übertragungsmethode müssen Sie auch die Optionen, die für die Übertragungsmethode bestimmt sind, zur Optionsdatei hinzufügen.

Syntax

```
                .-TCPIP-----.
>>-COMMMethod--+-NAMEDPIPE-+-----------------------------------><
               +-NONE------+
               +-SHAREDMEM-+
               +-SNMP------+
               +-TCPIP-----+
               '-V6TCPIP---'
```

Parameter

Es kann eine der folgenden Übertragungsmethoden gewählt werden:

Windows-BetriebssystemeNAMEDPIPES
: Windows-BetriebssystemeGibt die Übertragungsmethode mit benannten Pipes an.

NONE
: Gibt an, dass keine Übertragungsmethode verwendet wird. Diese Option lässt nicht zu, dass Benutzer den Server ansprechen, und eignet sich deshalb zum Experimentieren mit Maßnahmenbefehlen.

SHAREDMEM
: Gibt die Übertragungsmethode für gemeinsam benutzten Speicher an. Bei dieser Methode wird gleichzeitig derselbe Speicherbereich zum Senden von Daten zwischen mehreren Anwendungen verwendet. Sowohl der Server als auch der Client für Sichern/Archivieren müssen für

die Unterstützung der Übertragungsmethode für gemeinsam benutzten Speicher konfiguriert und auf demselben Computer installiert sein.

SNMP
: Gibt SNMP als Übertragungsmethode an.

TCPIP
: Gibt TCP/IP als Übertragungsmethode an. Diese Option ist der Standardwert. Wird TCPIP angegeben, wird ausschließlich TCP/IP Version 4 verwendet.

V6TCPIP
: Gibt TCP/IP als Übertragungsmethode an. Sind TCP/IP Version 4 und Version 6 konfiguriert, verwendet IBM Spectrum Protect beide Protokolle gleichzeitig. Wird COMMMETHOD TCPIP und COMMMETHOD V6TCPIP angegeben, überschreibt V6TCPIP die Angabe von TCPIP. Eine gültige DNS-Umgebung (DNS = Domain Name Server) muss vorhanden sein, damit bei Angabe dieser Option TCP/IP V4 oder TCP/IP V6 verwendet werden kann.

Beispiele

Beispiel für die Angabe mehrerer Übertragungsmethoden, die vom Server verwendet werden sollen (TCP/IP und TCP/IP Version 6):

```
commmethod tcpip
commmethod v6tcpip
```

COMMTIMEOUT

Die Option COMMTIMEOUT gibt an, wie lange der Server während einer Operation, die eine Datenbankaktualisierung zur Folge hat, auf eine erwartete Clientnachricht wartet. Wenn die Zeitlänge dieses Zeitlimit überschreitet, beendet der Server die Sitzung mit dem Client. Sie können den Wert für das Zeitlimit erhöhen, damit keine Zeitlimitüberschreitung bei den Clients auftritt. Eine Zeitlimitüberschreitung kann bei Clients auftreten, wenn eine hohe Netzauslastung in Ihrer Umgebung vorhanden ist, oder wenn die Clients große Dateien sichern.

Die Serveroption COMMTIMEOUT wird für Sitzungen verwendet, die keine Verwaltungssitzungen sind. Für Verwaltungsclientsitzungen siehe die Option ADMINCOMMTIMEOUT.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden.

Syntax

```
                .-60-------.
>>-COMMTimeout--+-Sekunden-+-----------------------------------><
```

Parameter

Sekunden
: Gibt die maximale Anzahl Sekunden an, die ein Server auf eine Antwort vom Client wartet. Der Standardwert ist 60. Der Mindestwert ist 1.

Beispiele

```
commtimeout 60
```

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

CONTAINERRESOURCETIMEOUT

Die Option CONTAINERRESOURCETIMEOUT gibt an, wie lange der Server auf die Ausführung einer Datenspeicheroperation für einen Containerspeicherpool wartet.

Syntax

Wenn eine Zeitlimitüberschreitung auftritt, verbleiben alle in dem Containerspeicherpool gespeicherten Daten in dem Containerspeicherpool. Die Datenspeicheroperation wird beendet und die Anforderung für die Containerressource wird abgebrochen.

```
                            .-180-----.
>>-CONTAINERRESOURCETimeout--+-Minuten-+-----------------------><
```

Parameter

Minuten
: Gibt die maximale Anzahl Minuten an, die ein Server wartet, bevor eine Operation abgebrochen wird. Der Standardwert ist 180 Minuten. Der Mindestwert ist 1 Minute.

Beispiel

Angeben, dass der Server 4 Stunden wartet, bevor eine Datenspeicheroperation für einen Containerspeicherpool abgebrochen wird.

```
containerresourcetimeout 240
```

Windows-Betriebssysteme

DATEFORMAT

Die Option DATEFORMAT gibt das Format an, in dem Datumsangaben vom Server angezeigt werden.

Der Wert für DATEFORMAT wird von dem Format der länderspezifischen Angaben überschrieben, wenn die länderspezifischen Angaben beim Serverstart initialisiert werden. Die länderspezifischen Angaben werden in der Option LANGUAGE angegeben.

Syntax

```
>>-DATEformat--n-----------------------------------------------><
```

Parameter

n
: Eine Zahl von 1 bis 5 auswählen, um das vom Server verwendete Datumsformat anzugeben. Der Standardwert ist 1.

  1
  : MM/DD/YYYY

  2
  : DD-MM-YYYY

  3
  : YYYY-MM-DD

  4
  : DD.MM.YYYY

  5
  : YYYY.MM.DD

Beispiele

```
dateformat 4
```

DBDIAGLOGSIZE

Mit dieser Option können Sie die Größe des Speicherbereichs steuern, der von Diagnoseprotokolldateien verwendet wird.

Der Datenbankmanager verwendet Diagnoseprotokolldateien zum Protokollieren von Nachrichten. Sie müssen die Größe der Protokolldateien steuern, damit sie nicht das Dateisystem füllen. Verwenden Sie die Option DBDIAGLOGSIZE, um die Größe des Speicherbereichs zu definieren, der von den Protokolldateien verwendet wird.
Wenn Sie einen Wert im Bereich von 2 bis 9999 definieren, werden maximal 10 rollierende Diagnoseprotokolldateien aufbewahrt. Jeder Dateiname gibt die Reihenfolge an, in der die Datei erstellt wurde. Wenn eine Datei voll ist, wird die nächste Datei erstellt. Wenn die zehnte Datei voll ist, wird die älteste Datei gelöscht und eine neue Datei erstellt. Das folgende Beispiel zeigt, wie die rollierenden Protokolldateien aussehen können:

```
db2diag.14.log, db2diag.15.log, ... , db2diag.22.log, db2diag.23.log
```

Wenn db2diag.23.log voll ist, wird db2diag.14.log gelöscht und db2diag.24.log erstellt.
Der Server überprüft stündlich den Dateibereich, der die Diagnoseprotokolldateien enthält. Nachrichten werden alle 12 Stunden angezeigt, wenn eine der folgenden Bedingungen auftritt:

- Der verfügbare Speicherplatz in dem Dateisystem, in dem sich die Diagnoseprotokolldateien befinden, beträgt weniger als 20 % des gesamten Dateisystembereichs.
- Der verfügbare Speicherplatz in dem Dateisystem, in dem sich das Serverinstanzverzeichnis befindet, beträgt weniger als 1 GB.

Wenn Sie den Wert 0 angeben, wird nur eine Protokolldatei (db2diag.log) für alle Diagnosenachrichten verwendet. Für die Größe der Protokolldatei gibt es keine Begrenzung.
Einschränkung: Sie müssen die Größe der Diagnoseprotokolldateien überwachen, um sicherzustellen, dass sie nicht den gesamten verfügbaren Speicherbereich im Dateisystem verwenden. Ist nicht genügend Speicherbereich verfügbar, erfolgt möglicherweise keine Reaktion durch den Server.

Syntax

```
                  .-1024-----.
>>-DBDIAGLOGSize--+-Megabyte-+--------------------------------><
```

Parameter

Megabyte
: Gibt die Größe des Speicherbereichs in Megabyte an, der von Diagnoseprotokolldateien verwendet wird. Geben Sie einen Wert im Bereich von 2 bis 9999 oder den Wert 0 an. Der Standardwert ist 1024.

  Wenn Sie einen Wert im Bereich von 2 bis 9999 angeben, werden rollierende Protokolldateien verwendet, und der Wert gibt die Gesamtgröße aller 10 Protokolldateien in Megabyte an. Der Wert wird auf 1024 zurückgesetzt, wenn der Server erneut gestartet wird.

  Wenn Sie den Wert 0 angeben, wird eine Protokolldatei verwendet, und es gibt für die Größe der Protokolldatei keine Begrenzung.

  Sollen Nachrichten archiviert werden, geben Sie den Wert 0 an, um sicherzustellen, dass die Datei db2diag.log den gesamten verfügbaren Speicherbereich ohne die Verwendung rollierender Protokolldateien verwenden kann.

  Nachdem Sie den Wert des Parameters Megabyte mit der Option DBDIAGLOGSIZE auf 0 gesetzt haben, werden Nachrichten anfänglich in rollierende Protokolldateien geschrieben. Nach dem Neustart des Servers werden Nachrichten in die Datei db2diag.log geschrieben.

  Tipp: Wenn Sie einen Wert im Bereich von 2 bis 9999 mithilfe der Serveroptionsdatei dsmserv.opt angeben, wird der Wert beim Serverstart nicht automatisch zurückgesetzt. Der Wert bleibt unverändert, bis er mit dem Befehl SETOPT geändert oder aus der Datei dsmserv.opt entfernt wird.

Beispiel: Eine maximale Größe von 5120 Megabyte angeben

Die Größe der Diagnoseprotokolldateien mit 5120 Megabyte (5 GB) angeben:

```
dbdiaglogsize 5120
```

Beispiel: Nachrichten in einer einzelnen Protokolldatei archivieren

Nachrichten archivieren, indem angegeben wird, dass die Nachrichten in die Datei db2diag.log geschrieben werden:

```
dbdiaglogsize 0
```

Zugehörige Informationen:
Produktinformation zu DB2 Version 10.5

DBDIAGPATHFSTHRESHOLD

Die Option DBDIAGPATHFSTHRESHOLD gibt den Schwellenwert für freien Speicherbereich in dem Dateisystem oder auf der Platte an, das bzw. die die Datei db2diag.log enthält.

Wenn der freie Speicherbereich kleiner-gleich dem angegebenen Schwellenwert ist, wird die Fehlernachricht ANR1545W angezeigt. Standardmäßig wird die Nachricht angezeigt, wenn das Dateisystem oder die Platte 20 % oder weniger freien Plattenspeicherplatz hat.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
>>-DBDIAGPATHFSTHreshold--Prozent------------------------------><
```

Parameter

Prozent
: Gibt den Prozentsatz des verfügbaren Speicherbereichs im Dateisystem an. Gültige Werte sind 0 bis 100. Der Standardwert ist 20.
  Tipp: Um die besten Ergebnisse zu erzielen, geben Sie keine niedrigen oder hohen Werte für den Parameter Prozent an. Ein niedriger Wert kann zur Folge haben, dass das Dateisystem voll ist, bevor Sie das Problem korrigieren können. Ein volles Dateisystem kann die Serverdatenbank beschädigen. Ein hoher Wert kann dazu führen, dass viele Nachrichten ANR1545W im Serveraktivitätenprotokoll angezeigt werden.

Beispiel

Den Schwellenwert auf 10% setzen.

```
setopt DBDIAGPATHFSTH 10
```

DBMEMPERCENT

Verwenden Sie diese Option, um den Prozentsatz des virtuellen Adressraums anzugeben, der den Datenbankmanagerprozessen zugeordnet ist.

Werden andere Anwendungen als der IBM Spectrum Protect-Server auf dem System ausgeführt, stellen Sie sicher, dass der Wert einen angemessenen Speicher für die anderen Anwendungen vorsieht.

Syntax

```
>>-DBMEMPERCENT--+-Prozent-+-----------------------------------><
                 '-AUTO----'
```

Parameter

Prozent
: Definieren Sie einen Wert von 10 bis 99.

AUTO
: Der Datenbankmanager setzt den Prozentsatz automatisch auf einen Wert, der zwischen 75 Prozent und 95 Prozent des Systemarbeitsspeichers liegt. Der Standardwert ist AUTO.

Beispiele

```
dbmempercent 50
```

DBMTCPPORT

Die Option DBMTCPPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-DFV-Treiber für den Datenbankmanager auf Anforderungen für Clientsitzungen.

Die angegebene Anschlussnummer muss für die Verwendung durch den Datenbankmanager reserviert werden.

Standardmäßig verwendet der IBM Spectrum Protect-Server die Interprozesskommunikation (IPC), um Verbindungen für die ersten beiden Verbindungspools mit maximal 480 Verbindungen für jeden Pool herzustellen. Nachdem die ersten 960 Verbindungen hergestellt wurden, verwendet der IBM Spectrum Protect-Server TCP/IP für alle weiteren Verbindungen.

Syntax

```
>>-DBMTCPPort--Anschlussnummer-------------------------------><
```

Parameter

Anschlussnummer
: Gibt die Nummer des TCP/IP-Anschlusses an, an dem der Datenbankmanager auf die Übertragung vom Server wartet. Gültige Werte sind ganze Zahlen von 1024 bis 65535.

  Die Standardanschlussnummer ist der Wert der Serveroption TCPPORT plus 50.000. Hat die Serveroption TCPPORT beispielsweise den Wert 1500, lautet die Standardanschlussnummer für DBMTCPPORT 51500.

  Ist die Serveroption TCPPORT größer als 9999, fügen Sie die letzten vier Ziffern des Werts dem Wert 50000 hinzu. Hat die Option TCPPORT beispielsweise den Wert 11500, wird 1550 dem Wert 50000 hinzugefügt. Daraus ergibt sich eine Anschlussnummer für DBMTCPPORT mit dem Wert 51500.

Beispiel

```
dbmtcpport 51500
```

DEDUPREQUIRESBACKUP

Die Option DEDUPREQUIRESBACKUP gibt an, ob Datenträger in primären Speicherpools mit sequenziellem Zugriff, die für die Deduplizierung von Daten definiert sind, wiederhergestellt und doppelte Daten gelöscht werden können, bevor die Speicherpools gesichert werden.

Lautet der Wert dieser Option YES (Standardwert), müssen Sie Daten in Kopienspeicherpools sichern, die nicht für die Deduplizierung von Daten definiert sind. Verwenden Sie den Befehl BACKUP STGPOOL, um Daten in Kopienspeicherpools zu sichern.

Beachten Sie, dass die Wiederherstellung eines Datenträgers in einem Speicherpool, der für die Deduplizierung von Daten definiert ist, möglicherweise nicht erfolgt, wenn der Datenträger zum ersten Mal auswählbar ist. Der Server führt zusätzliche Überprüfungen durch, um sicherzustellen, dass Daten aus einem Speicherpool, der für die Deduplizierung von Daten definiert ist, in einen Kopienspeicherpool gesichert wurden. Diese Überprüfungen erfordern mehrere BACKUP STGPOOL-Instanzen, bevor der Server einen Datenträger wiederherstellt. Nachdem der Server geprüft hat, dass die Daten gesichert wurden, wird der Datenträger wiederhergestellt.

Sie können diese Option mit dem Befehl SETOPT dynamisch ändern.

Achtung: Um die Möglichkeit eines Datenverlusts zu minimieren, ändern Sie nicht die Standardeinstellung für diese Serveroption. Geben Sie den Wert NO nur an, wenn Sie keine Kopienspeicherpools haben und Sie keine Speicherpoolsicherungen ausführen.

Syntax

```
>>-DEDUPREQUIRESBACKUP--+-Yes-+--------------------------------><
                        '-No--'
```

Parameter

Yes
: Gibt an, dass der Speicherpool gesichert werden muss, bevor Datenträger wiederhergestellt und doppelte Daten gelöscht werden können. Dies ist der Standardwert.

No
: Gibt an, dass Datenträger in primären Speicherpools mit sequenziellem Zugriff, die für die Deduplizierung von Daten definiert sind, wiederhergestellt und doppelte Daten gelöscht werden können, wenn die Speicherpools nicht gesichert werden.

Beispiele

Angeben, dass primäre Speicherpools mit sequenziellem Zugriff, die für die Deduplizierung von Daten definiert sind, nicht gesichert werden müssen.

```
deduprequiresbackup no
```

DEDUPTIER2FILESIZE

Die Option DEDUPTIER2FILESIZE gibt an, bei welcher Dateigröße IBM Spectrum Protect beginnt, die Schicht 2 der Datendeduplizierung zu verwenden.

Syntax

```
>>-DEDUPTIER2FILESIZE--nnn-------------------------------------><
```

Parameter

nnn
: Gibt die Dateigröße in Gigabyte an, bei der der IBM Spectrum Protect-Server beginnt, die Schicht 2 der Datendeduplizierung zu verwenden. Sie können einen Wert von 20 bis 9999 angeben. Der Standardwert ist 100.
Anmerkung: Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert größer als der Wert für die Option SERVERDEDUPTXNLIMIT ist, wird diese Option für die Serverdatendeduplizierung ignoriert. Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert größer als der Wert für die Option CLIENTDEDUPTXNLIMIT ist, wird diese Option für die Clientdatendeduplizierung ignoriert.

Beispiele

```
deduptier2filesize 550
```

DEDUPTIER3FILESIZE

Die Option DEDUPTIER3FILESIZE gibt an, bei welcher Dateigröße IBM Spectrum Protect beginnt, die Schicht 3 der Datendeduplizierung zu verwenden.

Syntax

```
>>-DEDUPTIER3FILESIZE--nnn-------------------------------------><
```

Parameter

nnn
: Gibt die Dateigröße in Gigabyte an, bei der der IBM Spectrum Protect-Server beginnt, die Schicht 3 der Datendeduplizierung zu verwenden. Sie können einen Wert von 90 bis 9999 angeben. Der Standardwert ist 400.

  - Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert größer als der Wert für die Option SERVERDEDUPTXNLIMIT ist, wird diese Option für die Serverdatendeduplizierung ignoriert.
  - Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert größer als der Wert für die Option CLIENTDEDUPTXNLIMIT ist, wird diese Option für die Clientdatendeduplizierung ignoriert.
  - Wenn der für diese Option angegebene Wert oder der standardmäßig angenommene Wert kleiner als der Wert ist, der für die Option DEDUPTIER2FILESIZE angegeben ist oder standardmäßig angenommen wird, wird der Wert von DEDUPTIER2FILESIZE für diese Option verwendet.

Beispiele

```
deduptier3filesize 1150
```

DEVCONFIG

Die Option DEVCONFIG gibt den Namen einer Datei an, in der IBM Spectrum Protect eine Sicherungskopie der Einheitenkonfigurationsinformationen speichern soll.

IBM Spectrum Protect speichert folgende Informationen in der Einheitenkonfigurationsdatei:

- Mit dem Befehl DEFINE DEVCLASS erstellte Einheitenklassendefinitionen
- Mit dem Befehl DEFINE DRIVE erstellte Laufwerkdefinitionen
- Kassettenarchivdefinitionen, die mit dem Befehl DEFINE LIBRARY erstellt wurden
- Informationen zum Datenträgerbestand im Kassettenarchiv für die automatisierten Kassettenarchive mit LIBTYPE=SCSI
- Pfaddefinitionen, die mit dem Befehl DEFINE PATH erstellt wurden
- Serverdefinitionen, die mit dem Befehl DEFINE SERVER erstellt wurden
- Servername, der mit dem Befehl SET SERVERNAME erstellt wurde
- Serverkennwort, das mit dem Befehl SET SERVERPASSWORD erstellt wurde

Anmerkung:

- Nur Pfaddefinitionen mit SRCTYPE=SERVER werden in der Einheitenkonfigurationsdatei gesichert. Pfade mit SRCTYPE=DATAMOVER werden nicht in die Datei geschrieben.
- Informationen zur Datenträgerposition im Kassettenarchiv werden als Kommentare (/*...*/) in der Einheitenkonfigurationsdatei gespeichert, wenn die Befehle CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME und AUDIT LIBRARY für SCSI-Kassettenarchive ausgegeben werden.

Achtung: Um die Datenbank nach einem Katastrophenfall zurückzuschreiben, benötigen Sie eine Kopie der aktuellen Einheitenkonfigurationsdatei. Die Einheitenkonfigurationsdatei kann nicht erneut erstellt werden.

Es können eine oder mehrere Optionen DEVCONFIG in die Serveroptionsdatei eingeschlossen werden. Wird mit mehreren DEVCONFIG-Optionen gearbeitet, aktualisiert IBM Spectrum Protect automatisch die Einheitenkonfigurationsinformationen in jeder angegebenen Datei und erstellt eine Sicherungskopie.

Syntax

```
>>-DEVCONFig--Dateiname-----------------------------------------><
```

Parameter

Dateiname
: Gibt den Namen einer Datei an, in der eine Sicherungskopie der Einheitenkonfigurationsinformationen gespeichert werden soll.

Beispiele

```
devconfig devices.sav
```

DISABLEREORGTABLE

Die Option DISABLEREORGTABLE gibt an, ob die Onlinetabellenreorganisation für Tabellennamen inaktiviert wird, die in der Tabellenliste angegeben sind.

Um die Option DISABLEREORGTABLE zu verwenden, müssen Sie den Server anhalten, die Optionsdatei aktualisieren und dann den Server erneut starten.

Syntax

```
>>-DISABLEREORGTable----Tabellenliste-------------------------><
```

Parameter

Tabellenliste
: Gibt eine Liste der Tabellennamen an, für die die Tabellenreorganisation inaktiviert wird. Werden keine Tabellennamen mit der Option angegeben oder ist die Option nicht in der Optionsdatei enthalten, werden keine Tabellen inaktiviert.
Einschränkung: Die folgenden Tabellen sind bereits von der Tabellenreorganisationsverarbeitung ausgeschlossen und können für diese Option nicht angegeben werden:

- STAGED_EXPIRING_OBJECTS
- STAGED_OBJECT_IDS
- BF_DEREFERENCED_CHUNKS
- BF_QUEUED_CHUNKS

Beispiel

```
DISABLEREORGTABLE BF_BITFILE_EXTENTS,REPLICATING_OBJECTS
```

DISABLESCHEDS

Die Option DISABLESCHEDS gibt an, ob Verwaltungszeitpläne und Clientzeitpläne während der Wiederherstellung des IBM Spectrum Protect-Servers inaktiviert sind.

Syntax

```
>>-DISABLESCheds--+-Yes-+-------------------------------------><
                  '-No--'
```

Parameter

Yes
: Gibt an, dass Verwaltungszeitpläne und Clientzeitpläne inaktiviert sind.

No
: Gibt an, dass Verwaltungszeitpläne und Clientzeitpläne aktiviert sind.

Beispiele

```
disablescheds no
```

DISPLAYLFINFO

Die Option DISPLAYLFINFO gibt an, wie die Abrechnungssätze und Einträge in der Übersichtstabelle den Knotennamen angeben.

Ist diese Option aktiviert, geben die Abrechnungssätze und Einträge in der Übersichtstabelle Knotenname(Speicheragentenname) für den Knotennamen an. Ist diese Option nicht aktiviert, geben die Abrechnungssätze und Einträge in der Übersichtstabelle nur Knotenname für den Knotennamen an. Der Standardwert ist 'No'.

Syntax

```
>>-DISPLAYLFINFO--+-Yes-+-------------------------------------><
                  '-No--'
```

Parameter

Yes
: Gibt an, dass die Abrechnungssätze und Einträge in der Übersichtstabelle den Speicheragentennamen angeben.

No

Gibt an, dass die Abrechnungssätze und Einträge in der Übersichtstabelle den Speicheragentennamen nicht angeben. Dies ist der Standardwert.

Beispiele

```
displaylfinfo yes
```

Das Ergebnis zeigt den folgenden Abrechnungssatz mit dem angezeigten Speicheragentennamen (STA53):

```
5,0,ADSM,07/13/2004,15:35:14,COLIND-TUC(STA53),,WinNT,1,Tcp/Ip,1,0,0,0,
0,223,4063,0,0,222,7,8,3,1,4,0,0,0,0,3,0
```

In der entsprechenden Übersichtstabelle wird ebenfalls der Speicheragentenname angezeigt:

```
      START_TIME: 2004-07-13 15:35:07.000000
                END_TIME: 2004-07-13 15:35:14.000000
                ACTIVITY: BACKUP
                  NUMBER: 8
                  ENTITY: COLIND-TUC(STA53)
                COMMMETH: Tcp/Ip
                 ADDRESS: colind-tuc:2229
           SCHEDULE_NAME:
                EXAMINED: 0
                AFFECTED: 223
                  FAILED: 0
                   BYTES: 4160875
                    IDLE: 8
                  MEDIAW: 1
              PROCESSES: 1
             SUCCESSFUL: YES
           VOLUME_NAME:
            DRIVE_NAME:
          LIBRARY_NAME:
               LAST_USE:
              COMM_WAIT: 3
     NUM_OFFSITE_VOLS:
```

DNSLOOKUP

Die Option DNSLOOKUP gibt an, ob der Server System-API-Aufrufe verwendet, um die DNS-Namen (DNS = Domain Name Server) von Systemen zu bestimmen, die den Server ansprechen.

Syntax

```
>>-DNSLOOKUP--+-Yes-+-----------------------------------------><
              '-No--'
```

Parameter

Yes
: Gibt an, dass der Server die DNS-Namen von Systemen abruft, die den Server ansprechen. Yes ist der Standardwert.

No
: Gibt an, dass der Server die DNS-Namen von Systemen nicht abruft, die den Server ansprechen.

Beispiele

```
dnslookup yes
```

DRIVEACQUIRERETRY

Mit der Option DRIVEACQUIRERETRY kann angegeben werden, wie oft der Server versuchen soll, ein Laufwerk in einem Kassettenarchiv IBM® 349x anzufordern. Wird das Kassettenarchiv von mehreren Anwendungen gemeinsam benutzt, scheinen seine Laufwerke für den Server verfügbar zu sein (durch die Verwendung eines Sendeaufrufprozesses im Hintergrund), obwohl sie es nicht sind.

Diese Option ist nur gültig, wenn 3494SHARED YES in der Datei dsmserv.opt angegeben wurde. Wurde DRIVEACQUIRERETRY NEVER angegeben, müssen Sie überwachen, wie lange Jobs auf Laufwerke gewartet haben und wie lange der Server die Laufwerke abgefragt hat. Außerdem müssen Sie möglicherweise den Status dieser Laufwerke in den anderen IBM Spectrum Protect-Servern überprüfen. Möglicherweise stecken Kassetten in den Laufwerken und die anderen IBM Spectrum Protect-Server haben die Laufwerke gegebenenfalls als *Offline* markiert. Ist dies der Fall, müssen Sie die Laufwerke auf dem IBM Spectrum Protect-Server als *Offline* markieren, der die Laufwerke abfragt. Falls erforderlich, brechen Sie auch alle wartenden Jobs ab.

Syntax

```
>>-DRIVEACQuireretry--+-Forever---------+---------------------><
                     +-Never-----------+
                     '-Anzahl_Versuche-'
```

Parameter

Forever
: Die Anforderung eines Laufwerks wird so lange wiederholt, bis ein Laufwerk erfolgreich angefordert wurde. Dies ist der Standardwert.

Never
: Die Anforderung eines Laufwerks wird vom Server nicht wiederholt, und die Operation schlägt fehl.

Anzahl_Versuche
: Gibt die maximale Anzahl der Versuche (1 bis 9999) durch den Server an, ein Laufwerk anzufordern.

Beispiele

Angeben, dass der Server maximal 10 Mal versuchen soll, das Laufwerk anzufordern:

```
driveacquireretry 10
```

ENABLENASDEDUP

Die Serveroption ENABLENASDEDUP gibt an, ob der Server Daten dedupliziert, die von einem NAS-Dateiserver gespeichert werden. Diese Option gilt nur für NetApp-Dateiserver.

Lautet der Wert dieser Option NO, werden die vom Dateiserver gespeicherten Daten während des Prozesses zum Identifizieren doppelter Daten übersprungen. Lautet der Wert dieser Option YES, muss der Parameter DEDUPLICATE in der Speicherpooldefinition den Wert YES haben.

Syntax

```
>>-ENABLENASDEDUP--+-No--+-------------------------------------><
                   '-Yes-'
```

Parameter

Yes
: Gibt an, dass der IBM Spectrum Protect-Server Daten dedupliziert, die von einem NetApp-Dateiserver gespeichert werden.

No
: Gibt an, dass der Server keine Daten dedupliziert, die von einem NetApp-Dateiserver gespeichert werden.

Beispiel

Angeben, dass der Server Daten dedupliziert, die von einem NetApp-Dateiserver gespeichert werden.

```
enablenasdedup yes
```

EVENTSERVER

Die Option EVENTSERVER gibt an, ob der Server beim Systemstart eine Verbindung zum Ereignisserver herstellen soll.

Syntax

```
>>-EVENTSERVer--+-Yes-+---------------------------------------><
                '-No--'
```

Parameter

Yes
: Gibt an, dass der Server versucht, beim Systemstart eine Verbindung zum Ereignisserver herzustellen. Eine Verbindung kann nur hergestellt werden, wenn bereits ein Befehl DEFINE EVENTSERVER ausgegeben wurde. Dies ist der Standardwert.

No
: Gibt an, dass der Server nicht versucht, beim Systemstart eine Verbindung zum Ereignisserver herzustellen.

Beispiele

```
eventserver yes
```

EXPINTERVAL

Die Option EXPINTERVAL gibt das Intervall (in Stunden) an, in dem automatische Bestandsverfallsprozesse in IBM Spectrum Protect stattfinden. Beim Datenträgerbestandsverfall werden Clientsicherungs- und Archivierungsdateikopien aus dem Server gelöscht, und zwar wie von den Verwaltungsklassen angegeben, denen die Clientdateien zugeordnet sind. Findet nicht regelmäßig ein Datenträgerverfall statt, wird kein Speicherpoolbereich von abgelaufenen Clientdateien zurückgefordert, so dass für den Server mehr Speicherbereich benötigt wird, als für die Maßnahme eigentlich nötig wäre.

Der Datenträgerbestandsverfall kann auch über den Befehl EXPIRE INVENTORY gestartet werden. Durch den Datenträgerverfall wird Speicherbereich für weitere Clientsicherungs- und Archivierungsdateien in den Speicherpools verfügbar.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
                .-24------.
>>-EXPINterval--+-Stunden-+-------------------------------------><
```

Parameter

Stunden
: Gibt die Zeit in Stunden zwischen den automatischen Bestandsverfallsprozessen an. Es können 0 bis 336 Stunden (14 Tage) angegeben werden. Der Wert 0 bedeutet, dass der Datenträgerbestandsverfall mit dem Befehl EXPIRE INVENTORY gestartet werden muss. Der Standardwert ist 24.

Beispiele

```
expinterval 5
```

EXPQUIET

Die Option EXPQUIET gibt an, ob IBM Spectrum Protect detaillierte Nachrichten während der Verfallsverarbeitung sendet.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
>>-EXPQUiet--+- --No--+----------------------------------------><
             '- --Yes-'
```

Parameter

No
: Gibt an, dass der Server ausführliche Nachrichten sendet. Dies ist der Standardwert.

Yes
: Gibt an, dass der Server nur knappe Nachrichten sendet. Diese Nachrichten werden nur für Dateien gesendet, die aufgrund der Kopiengruppe in der Standardverwaltungsklasse oder aufgrund des für die Domäne gültigen Aufbewahrungszeitraums abgelaufen sind.

Beispiele

```
expquiet no
```


Linux-Betriebssysteme

FASPBEGPORT

Die Option FASPBEGPORT gibt die Anfangsnummer des Bereichs von Anschlussnummern an, die für die Netzkommunikation mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) verwendet werden.

Um den Bereich von Anschlussnummern zu definieren, geben Sie sowohl die Option FASPBEGPORT als auch die Option FASPENDPORT an.

Syntax

```
                .-15100------------------.
>>-FASPBEGPort--+-Anfangsanschlussnummer-+--------------------><
```

Parameter

Anfangsanschlussnummer
: Gibt die Anfangsanschlussnummer für die Netzkommunikation mit der Aspera FASP-Technologie an. Der Standardwert ist 15100. Bitten Sie Ihren Netzadministrator um Unterstützung bei der Definition des Bereichs der Anschlussnummern:

  - Wenn Sie das SSL-Protokoll (SSL = Secure Sockets Layer) für das Serverpaar nicht aktiviert haben, stellen Sie sicher, dass die Anschlüsse für TCP-Sockets (TCP = Transmission Control Protocol) verwendet werden können.
  - Stellen Sie sicher, dass die Anschlüsse für UDP-Verbindungen (UDP = User Datagram Protocol) verwendet werden können.
  - Stellen Sie sicher, dass die Anschlüsse mit Firewallregeln kompatibel sind.

Beispiel

Wenn Firewallregeln erfordern, dass Anschlussnummern größer als 1800 sind, geben Sie als kleinste Anschlussnummer 1801 an:

```
faspbegport 1801
```

Zugehörige Verweise:
FASPENDPORT
Linux-Betriebssysteme

FASPENDPORT

Die Option FASPENDPORT gibt die Endnummer des Bereichs von Anschlussnummern an, die für die Netzkommunikation mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) verwendet werden.

Um den Bereich von Anschlussnummern zu definieren, geben Sie sowohl die Option FASPBEGPORT als auch die Option FASPENDPORT an.

Syntax

```
                .-15199--------------.
>>-FASPENDPort--+-Endanschlussnummer-+------------------------><
```

Parameter

Endanschlussnummer
: Gibt die Endanschlussnummer für die Netzkommunikation mit der Aspera FASP-Technologie an. Der Standardwert ist 15199. Bitten Sie Ihren Netzadministrator um Unterstützung bei der Definition des Bereichs der Anschlussnummern:

  - Wenn Sie das SSL-Protokoll (SSL = Secure Sockets Layer) für das Serverpaar nicht aktiviert haben, stellen Sie sicher, dass die Anschlüsse für TCP-Sockets (TCP = Transmission Control Protocol) verwendet werden können.
  - Stellen Sie sicher, dass die Anschlüsse für UDP-Verbindungen (UDP = User Datagram Protocol) verwendet werden können.
  - Stellen Sie sicher, dass die Anschlüsse mit Firewallregeln kompatibel sind.

Beispiel

Wenn Firewallregeln erfordern, dass Anschlussnummern kleiner als 1900 sind, geben Sie als größte Anschlussnummer 1899 an:

```
faspendport 1899
```

Zugehörige Verweise:
FASPBEGPORT
Linux-Betriebssysteme

FASPTARGETRATE

Die Option FASPTARGETRATE gibt die Zielgeschwindigkeit für die Datenübertragung mit der Aspera FASP-Technologie (Fast Adaptive Secure Protocol) an. Mit der Angabe der Zielgeschwindigkeit begrenzen Sie die Bandbreite jeder Netzverbindung, die die Aspera FASP-Technologie verwendet. Auf diese Weise können Sie sicherstellen, dass genügend Bandbreite für alle Netzverbindungen verfügbar ist.

Syntax

```
                    .-250000--------------.
>>-FaspTargetRate--+-Zielgeschwindigkeit-+---------------------><
```

Parameter

Zielgeschwindigkeit
: Gibt die maximale Geschwindigkeit in Kb/s für die Datenübertragung während einer Sitzung an. Der Standardwert ist 250000. Sie können Werte im Bereich von 100 bis 100000000 angeben.

  Beispiel: Wenn Sie den Befehl PROTECT STGPOOL ausgeben, um zwei parallele Operationen mit der Standardzielgeschwindigkeit auszuführen, überschreitet der Gesamtdurchsatz nicht 500.000 Kb/s. Wenn Ihr Dateisystem zwei Operationen zum Schützen von Speicherpools mit weit höheren Geschwindigkeiten als 500.000 Kb/s des Gesamtdurchsatzes unterstützen kann und genügend Netzbandbreite verfügbar ist, können Sie die Zielgeschwindigkeit erhöhen.

  Um die entsprechende Zielgeschwindigkeit zu bestimmen, ziehen Sie Ihren Netzadministrator zu Rate.

Beispiele

Wenn die zugewiesene Netzbandbreite 150.000 Kb/s beträgt, können Sie die Zielgeschwindigkeit auf 75.000 setzen und die Standardanzahl Sitzungen (zwei) für den Befehl PROTECT STGPOOL verwenden.

```
fasptargetrate 75000
```

Wenn in einer großen Blueprint-Konfiguration die zugewiesene Netzbandbreite 6.000.000 Kb/s beträgt, können Sie die Zielgeschwindigkeit auf 750.000 setzen und acht Sitzungen für den Befehl PROTECT STGPOOL verwenden.

```
fasptargetrate 750000
```

FFDCLOGLEVEL

Die Option FFDCLOGLEVEL gibt den Typ von allgemeinen Servernachrichten an, die im FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) angezeigt werden.

Das FFDC-Protokoll enthält drei Kategorien von allgemeinen Servernachrichten. Die Definition der Option FFDCLOGLEVEL betrifft die folgenden Kategorien:

- FFDC_GENERAL_SERVER_INFO
- FFDC_GENERAL_SERVER_WARNING
- FFDC_GENERAL_SERVER_ERROR

Syntax

```
   .-FFDCLOGLevel--=--ALL-------.
>>-+-FFDCLOGLevel--=--+-ALL---+-+------------------------------><
                      +-WARN--+
                      '-ERRor-'
```

Parameter

ALL
: Gibt an, dass alle allgemeinen FFDC-Serverprotokollnachrichten im Protokoll angezeigt werden. Dieser Wert ist der Standardwert.

WARN
: Gibt an, dass die Nachrichten FFDC_GENERAL_SERVER_WARNING und FFDC_GENERAL_SERVER_ERROR im Protokoll angezeigt werden.

ERRor
: Gibt an, dass nur die Nachrichten FFDC_GENERAL_SERVER_ERROR im Protokoll angezeigt werden.

Beispiel

```
ffdcloglevel warn
```

FFDCLOGNAME

Die Option FFDCLOGNAME gibt einen Namen für das FFDC-Protokoll (FFDC = First-Failure Data Capture) an.

Die FFDC-Protokolldatei wird verwendet, um Diagnoseinformationen zum Server zu erfassen. Wenn ein Fehler auftritt, werden Daten zu dem Fehler in die FFDC-Protokolldatei geschrieben. Diese Informationen können dem IBM Support zur Fehlerdiagnose zur Verfügung gestellt werden. Die FFDC-Protokolldatei befindet sich im Serverinstanzverzeichnis.

Syntax

```
                .-dsmffdc.log-.
>>-FFDCLOGNAME--+-Dateiname---+--------------------------------><
```

Parameter

Dateiname
: Gibt einen Dateinamen für die FFDC-Protokolldatei an. Der Dateiname kann ein vollständig qualifizierter Dateiname oder ein Dateiname sein, der sich auf das Serverinstanzverzeichnis bezieht. Der Standardwert ist dsmffdc.log.

Beispiele

```
ffdclogname /tsminst1/tsmffdc.log
ffdclogname tsmffdc.log
ffdclogname c:\tsmserv1\tsmffdc.log
```

Zugehörige Verweise:
FFDCMAXLOGSIZE
FFDCNUMLOGS

FFDCMAXLOGSIZE

Die Option FFDCMAXLOGSIZE gibt die Größe für die FFDC-Protokolldatei (FFDC = First-Failure Data Capture) an.

Die FFDC-Protokolldatei wird verwendet, um Diagnoseinformationen zum Server zu erfassen. Wenn ein Fehler auftritt, werden Daten zu dem Fehler in die FFDC-Protokolldatei geschrieben. Diese Informationen können dem IBM Support zur Fehlerdiagnose zur Verfügung gestellt werden.

Syntax

```
                  .-1024-----.
>>-FFDCMAXLOGSIZE--+-Kilobyte-+--------------------------------><
```

Parameter

Kilobyte
: Gibt die maximale Größe für die FFDC-Protokolldatei an, bevor ein Umlauf erfolgt. Der Mindestwert ist 500. Der Maximalwert ist 2097151. Der Standardwert ist 1024.

  Soll die Größe der Protokolldatei unendlich sein, geben Sie den Wert -1 an. Um das Protokoll zu inaktivieren, geben Sie 0 an.

Beispiele

```
ffdcmaxlogsize 2000
```

Zugehörige Verweise:
FFDCLOGNAME
FFDCNUMLOGS

FFDCNUMLOGS

Die Option FFDCNUMLOGS gibt die Anzahl der Protokolldateien an, die für die Umlaufprotokollierung verwendet werden können. Der Standardwert ist 10.

Die Umlaufprotokollierung verwendet einen Protokolldateiring, um eine Wiederherstellung nach Transaktionsfehlern und Systemabstürzen bereitzustellen. Wenn beispielsweise die Datei dsmffcd.log voll ist, wird sie in dsmffdc.log.1 umbenannt. Ist eine Datei dsmffdc.log.1 vorhanden, wird die Datei dsmffdc.log.1 in dsmffdc.log.2 umbenannt. Ist eine Datei dsmffdc.log.2 vorhanden, wird die Datei dsmffdc.log.2 in dsmffdc.log.3 umbenannt. Dies wird fortgesetzt, bis der Wert für FFDCNUMLOGS erreicht wird. Wird eine Protokolldatei umbenannt, wenn der Wert für FFDCNUMLOGS erreicht ist, wird diese Protokolldatei gelöscht.

Der Mindestwert ist 1. Der Maximalwert ist 100. Der Standardwert ist 10.

Syntax

```
                .-10---.
>>-FFDCNUMLOGS--+-Wert-+----------------------------------------><
```

Parameter

Wert
: Gibt die Anzahl der Protokolldateien an, die für die Umlaufprotokollierung verwendet werden.

  Wird der Wert 1 angegeben und erreicht die Protokolldateigröße den Wert für FFDCMAXLOGSIZE, schreibt der Server weiter in die Protokolldatei. Alle Protokolldaten werden überschrieben und der Server schreibt weiter in die Protokolldatei.

Beispiele

```
ffdcnumlogs 20
```

FILEEXIT

Die Option FILEEXIT gibt eine Datei an, an die aktivierte Ereignisse weitergeleitet werden. Jedes protokollierte Ereignis ist ein Satz in der Datei.

Syntax

```
>>-FILEEXIT--+-No--+--Dateiname--+-REPLACE--+------------------><
             '-Yes-'             +-APPEND---+
                                 '-PRESERVE-'
```

Parameter

Yes
: Gibt an, dass das Ereignisprotokoll für den Dateiausgangsempfänger automatisch beim Serverstart gestartet wird.

No
: Gibt an, dass das Ereignisprotokoll für den Dateiausgangsempfänger nicht automatisch beim Serverstart gestartet wird. Wurde dieser Parameter angegeben, muss das Ereignisprotokoll manuell durch Eingabe des Befehls BEGIN EVENTLOGGING gestartet werden.

Dateiname
: Gibt den Namen der Datei an, in der die Ereignisse gespeichert werden.

REPLACE
: Gibt an, dass die Datei überschrieben wird, falls sie bereits vorhanden ist.

APPEND
: Gibt an, dass die Daten an die Datei angefügt werden, falls die Datei bereits vorhanden ist.

PRESERVE
: Gibt an, dass die Datei nicht überschrieben wird, falls sie bereits vorhanden ist.

Beispiele

 Windows-Betriebssysteme

```
fileexit yes \tsm\server\data replace
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
fileexit yes /tsm/server/data replace
```

FILETEXTEXIT

Die Option FILETEXTEXIT gibt eine Datei an, an die aktivierte Ereignisse weitergeleitet werden. Jedes protokollierte Ereignis ist eine lesbare Zeile fester Größe.

Syntax

```
>>-FILETEXTEXIT--+-No--+--Dateiname--+-REPLACE--+--------------><
                 '-Yes-'             +-APPEND---+
```

```
'-PRESERVE-'
```

Parameter

Yes
: Gibt an, dass das Ereignisprotokoll für den Dateiausgangsempfänger automatisch beim Serverstart gestartet wird.

No
: Gibt an, dass das Ereignisprotokoll für den Dateiausgangsempfänger nicht automatisch beim Serverstart gestartet wird. Wurde dieser Parameter angegeben, muss das Ereignisprotokoll manuell durch Eingabe des Befehls BEGIN EVENTLOGGING gestartet werden.

Dateiname
: Gibt den Namen der Datei an, in der die Ereignisse gespeichert werden.

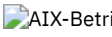
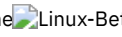
REPLACE
: Gibt an, dass die Datei überschrieben wird, falls sie bereits vorhanden ist.

APPEND
: Gibt an, dass die Daten an die Datei angefügt werden, falls die Datei bereits vorhanden ist.

PRESERVE
: Gibt an, dass die Datei nicht überschrieben wird, falls sie bereits vorhanden ist.

Beispiele

```
filetextexit yes \tsm\server\data replace
```

```
filetextexit yes /tsm/server/data replace
```

FSUSEDTHRESHOLD

Die Option FSUSEDTHRESHOLD gibt den Prozentsatz des Dateisystems an, der von der Datenbank ausgefüllt werden kann, bevor eine Alertnachricht ausgegeben wird.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden.

Wird dieser Wert auf eine niedrige Zahl gesetzt, kann das Aktivitätenprotokoll mit Nachrichten überschwemmt werden, die angeben, dass der Datenbankbereich ausgefüllt ist, auch wenn noch Speicherbereich verfügbar ist. Wird der Wert zu hoch definiert, kann der Datenbankbereich ausgefüllt sein, bevor Sie dem Dateisystem weiteren Speicherbereich hinzufügen können.

Syntax

```
>>-FSUSEDTHreshold--Prozent-----------------------------------><
```

Parameter

Prozent
: Gibt den Wert des verwendeten Speicherbereichs in der Datenbank an. Es kann ein Wert von 0 bis 100 angegeben werden. Der Standardwert ist 90.

Beispiele

```
fsusedthreshold 70
```

IDLETIMEOUT

Die Option IDLETIMEOUT gibt die Zeit in Minuten an, die eine Clientsitzung inaktiv sein kann, bevor der Server die Sitzung abbricht. Sie können den Wert für das Zeitlimit erhöhen, damit bei hoher Netzauslastung in Ihrer Umgebung keine Zeitlimitüberschreitung bei den Clients auftritt. Beachten Sie jedoch, dass bei einer großen Anzahl von inaktiven Sitzungen andere Benutzer möglicherweise keine Verbindung zu dem Server herstellen können.

Die Serveroption IDLETIMEOUT wird für Sitzungen verwendet, die keine Verwaltungssitzungen sind. Für Verwaltungsclientsitzungen siehe die Option ADMINIDLETIMEOUT.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden.

Syntax

```
                .-15------.
>>-IDLETimeout--+-Minuten-+-------------------------------------><
```

Parameter

Minuten
: Gibt die maximale Anzahl Minuten an, die ein Server auf einen inaktiven Client wartet. Der Standardwert ist 15 Minuten. Der Mindestwert ist 1 Minute.

Beispiele

```
idletimeout 15
```

KEEPALIVE

Die Option KEEPALIVE gibt an, ob die TCP-Keepalive-Funktion (TCP = Transmission Control Protocol) für abgehende TCP-Sockets aktiviert ist. Die TCP-Keepalive-Funktion sendet eine Übertragung von einer Einheit zu einer anderen Einheit, um zu überprüfen, ob die Verbindung zwischen den beiden Einheiten betriebsbereit ist.

Bei Verwendung der Knotenreplikation können Sie die Option KEEPALIVE auf dem Quellenreplikationsserver verwenden, um die TCP-Keepalive-Funktion zu aktivieren. Die Option KEEPALIVE ist auf dem Zielreplikationsserver nur erforderlich, wenn Sie die bidirektionale Replikation angeben. In diesem Fall wird der Zielserver zum Quellenreplikationsserver.

Syntax

```
              .-Yes-.
>>-KEEPALIVE--+-No--+-------------------------------------------><
```

Parameter

Yes
: Gibt an, dass die TCP-Keepalive-Funktion für abgehende TCP-Sockets aktiviert ist. Dieser Wert ist der Standardwert.
Wenn die Option KEEPALIVE aktiviert ist, werden für die Optionen KEEPALIVETIME und KEEPALIVEINTERVAL Standardwerte verwendet.

No
: Gibt an, dass die TCP-Keepalive-Funktion für abgehende TCP-Sockets nicht aktiviert ist.
Wenn Sie den Wert NO angeben, hat dies keine Auswirkungen auf aktuelle TCP-Socketverbindungen, die von Anforderungen für abgehende Verbindungen stammen, während die Option KEEPALIVE auf YES gesetzt war. Der Wert YES gilt für diese Sockets, bis die zugehörige Sitzung beendet und das Socket geschlossen wird.

Beispiel

Verwenden Sie den Befehl SETOPT, um die Keepalive-Funktion zu aktivieren, ohne den Server zu inaktivieren oder anzuhalten:

```
setopt keepalive yes
```

Zugehörige Verweise:
KEEPALIVEINTERVAL
KEEPALIVETIME

KEEPALIVETIME

Die Option KEEPALIVETIME gibt an, wie oft TCP eine Keepalive-Übertragung sendet, wenn eine Antwort empfangen wird. Diese Option gilt nur, wenn die Option KEEPALIVE auf YES gesetzt wurde.

Syntax

```
                .-300------.
>>-KEEPALIVETIME--+-Sekunden-+-----------------------------------><
```

Parameter

Sekunden

Gibt an, wie oft TCP Keepalive-Übertragungen sendet, um zu prüfen, ob eine inaktive Verbindung noch aktiv ist. Der Wert wird in Sekunden angegeben.
Sie können einen Wert im Bereich von 1 bis 4294967 angeben. Der Standardwert ist 300 (5 Minuten).

Beispiel

Die Option KEEPALIVETIME auf 120 Sekunden setzen:

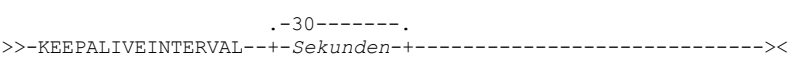
```
keepalivetime 120
```

Zugehörige Verweise:
KEEPALIVE
KEEPALIVEINTERVAL

KEEPALIVEINTERVAL

Die Option KEEPALIVEINTERVAL gibt an, wie oft eine Keepalive-Übertragung gesendet wird, wenn keine Antwort empfangen wird. Diese Option gilt nur, wenn die Option KEEPALIVE auf YES gesetzt wurde.

Syntax



Parameter

Sekunden
Gibt die Zeit in Sekunden zwischen Keepalive-Übertragungen an, wenn keine Antwort empfangen wird. Der Wert wird in Sekunden angegeben.
Sie können einen Wert im Bereich von 1 bis 4294967 angeben. Der Standardwert ist 30 Sekunden.

Beispiel

Die Option KEEPALIVEINTERVAL auf 45 Sekunden setzen:

```
keepaliveinterval 45
```

Zugehörige Verweise:
KEEPALIVE
KEEPALIVETIME

LANGUAGE

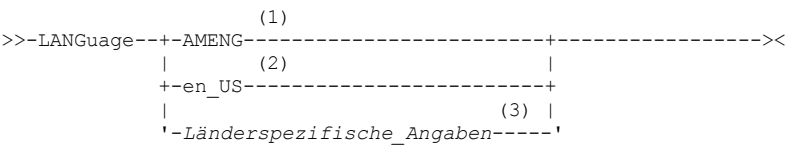
Die Option LANGUAGE steuert die Initialisierung von länderspezifischen Angaben. Die länderspezifischen Angaben enthalten unter anderem die Landessprache sowie die Datums-, Uhrzeit- und Zahlenformate, die für die Konsole und den Server verwendet werden sollen.

Werden Ihr Client und Ihr Server in unterschiedlichen Sprachen ausgeführt, sind die generierten Nachrichten möglicherweise nicht verständlich, wenn Nachrichten vom Client an den Server ausgegeben werden oder wenn der Server eine Ausgabe an den Client sendet.

AIX-BetriebssystemeLinux-BetriebssystemeKann die Locale nicht initialisiert werden, verwendet der Server standardmäßig amerikanisches Englisch.

Windows-BetriebssystemeKann die Ländereinstellung nicht initialisiert werden, verwendet der Server standardmäßig amerikanisches Englisch und die mit den Serveroptionen DATEFORMAT, TIMEFORMAT und NUMBERFORMAT definierten Formate für Datum, Uhrzeit und Zahlen.

Syntax



Anmerkungen:

1. AMENG ist nur unter HP-UX, Solaris und Windows verfügbar.

2. en_US ist nur unter AIX und Linux verfügbar.
3. Die *Ländereinstellung* ist nur unter AIX, HP-UX, Solaris, Linux und Windows verfügbar.

Parameter

Windows-BetriebssystemeAMENG
Windows-BetriebssystemeGibt an, dass amerikanisches Englisch als Standardsprache für den Server verwendet wird.
AIX-BetriebssystemeLinux-Betriebssystemeen_US
AIX-BetriebssystemeLinux-BetriebssystemeGibt an, dass amerikanisches Englisch als Standardsprache für den Server verwendet wird.

Länderspezifische_Angaben
Gibt den Namen der vom Server unterstützten Ländereinstellung an. Die folgenden Tabellen enthalten Informationen zu den unterstützten länderspezifischen Angaben nach Betriebssystem.
Anmerkung: IBM Spectrum Protect kann in jeder Locale ausgeführt werden, der Standardwert ist jedoch amerikanisches Englisch. Für die aufgelisteten Locales steht Sprachunterstützung zur Verfügung.

AIX-Betriebssysteme

Tabelle 1. Serversprachen für AIX

Sprache	Wert der Option LANGUAGE
Chinesisch, vereinfacht	zh_CN
Chinesisch, vereinfacht	Zh_CN
Chinesisch, vereinfacht (UTF-8)	ZH_CN
Chinesisch, traditionell (Big5)	Zh_TW
Chinesisch, traditionell (UTF-8)	ZH_TW
Chinesisch, traditionell (euc_tw)	zh_TW
Englisch	en_US
Englisch (UTF-8)	EN_US
Französisch	fr_FR
Französisch (UTF-8)	FR_FR
Deutsch	de_DE
Deutsch (UTF-8)	DE_DE
Italienisch	it_IT
Italienisch (UTF-8)	IT_IT
Japanisch, EUC	ja_JP
Japanisch, PC	Ja_JP
Japanisch, UTF8	JA_JP
Koreanisch	ko_KR
Koreanisch (UTF-8)	KO_KR
Portugiesisch, Brasilien	pt_BR
Portugiesisch, Brasilanisch (UTF-8)	PT_BR
Russisch	ru_RU
Russisch (UTF-8)	RU_RU
Spanisch	es_ES
Spanisch (UTF-8)	ES_ES
Anmerkung: Für das System muss die Unterstützung der Umgebung en_US installiert sein.	

Linux-Betriebssysteme

Tabelle 2. Serversprachen für Linux

LANGUAGE	Wert der Option LANGUAGE
Chinesisch, vereinfacht	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chinesisch, traditionell	Big5 / Zh_TW

LANGUAGE	Wert der Option LANGUAGE
	zh_TW
	zh_TW.utf8
Englisch, Vereinigte Staaten	en_US
	en_US.utf8
Französisch	fr_FR
	fr_FR.utf8
Deutsch	de_DE
	de_DE.utf8
Italienisch	it_IT
	it_IT.utf8
Japanisch	ja_JP
	ja_JP.utf8
Koreanisch	ko_KR
	ko_KR.utf8
Portugiesisch, Brasilien	pt_BR
	pt_BR.utf8
Russisch	ru_RU
	ru_RU.utf8
Spanisch	es_ES
	es_ES.utf8

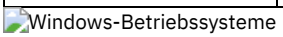
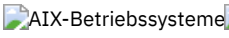


Tabelle 3. Serversprachen für Windows

Sprache	Wert der Option LANGUAGE
Chinesisch, vereinfacht	chs
Chinesisch, traditionell	cht
Englisch	ameng
Französisch	fra
Deutsch	deu
Italienisch	ita
Japanisch	jpn
Koreanisch	kor
Portugiesisch, Brasilien	ptb
Russisch	rus
Spanisch	esp

Beispiele



```
lang ja_JP
```

```
lang jpn
```

LDAPCACHEDURATION

Die Option LDAPCACHEDURATION bestimmt die Zeit, die der IBM Spectrum Protect-Server Informationen zur LDAP-Kennwortauthentifizierung zwischenspeichert.

Nach einer erfolgreichen LDAP-Bindung bestimmt der eingegebene Wert die Zeit, die Informationen zum LDAP-Verzeichnisserver verfügbar bleiben. Je höher der Wert ist, desto besser ist die Leistung des LDAP-Verzeichnisservers. Während der Cache-Periode werden Änderungen auf dem LDAP-Verzeichnisserver jedoch nicht sofort auf dem Knoten wirksam. Beispielsweise können alte Kennwörter für einige Zeit vorhanden sein, nachdem sie auf dem LDAP-Server geändert oder gesperrt wurden.

Schließen Sie die Option LDAPCACHEDURATION in einen Befehl SETOPT ein, damit die Option sofort wirksam wird.

Einschränkung: Die Option LDAPCACHEDURATION gilt nicht für Speicheragenten.

Syntax

```
>>-LDAPCACHEDURATION--Minuten---------------------------------><
```

Parameter

Minuten
: Gibt die Höchstdauer nach einer erfolgreichen LDAP-Bindung an, während der nachfolgende Sitzungen für denselben Knoten oder Administrator sekundäre LDAP-Bindungsoperationen überspringen. Die Werte befinden sich im Bereich von 0 bis 360 Minuten.

Beispiel: Den Wert für LDAPCACHEDURATION auf 6 Stunden setzen (Maximum)

Geben Sie in der Datei dsmserv.opt den folgenden Wert an:

```
ldapcacheduration 360
```

Nachdem sich ein Knoten oder Administrator mit einem externen Verzeichnisserver authentifiziert hat, wird die LDAP-Bindung für alle Sitzungen für 360 Minuten übersprungen.

LDAPURL

Die Option LDAPURL gibt die Position Ihres Lightweight Directory Access Protocol-Servers (LDAP-Servers) an. Definieren Sie die Option LDAPURL nach der Konfiguration des LDAP-Servers.

Tipp: Die Informationen in dieser Dokumentation beziehen sich auf die LDAP-Authentifizierungsmethode, die für IBM Spectrum Protect-Server der Version 7.1.7 oder höher bevorzugt wird. Anweisungen zur Verwendung der vorherigen LDAP-Authentifizierungsmethode finden Sie in Kennwörter und Anmeldeverfahren verwalten.
Es gelten die folgenden Einschränkungen:

- Die Option LDAPURL kann nicht in Kombination mit dem Befehl SETOPT verwendet werden.
- Die Option LDAPURL gilt nicht für Speicheragenten.

Syntax

```
>>-LDAPURL--Wert_für_LDAP_URL---------------------------------><
```

Parameter

Wert_für_LDAP_URL
: Gibt die URL eines einzelnen LDAP-Servers oder die URLs mehrerer LDAP-Server an. Sie können mehrere Werte eingeben. Dabei kann jeder URL-Wert maximal 1024 Zeichen umfassen. Die Anschlussnummer ist optional und nimmt standardmäßig den Wert 389 an. Jeder URL-Wert muss einen LDAP-Servernamen enthalten. Beispielsweise ist das Format des Servernamens `server1.storage.us.ibm.com` und der LDAP-Anschluss ist `341`. Der Wert der Option LDAPURL muss den folgenden Spezifikationen entsprechen:

  - Wenn Sie mehrere URLs angeben, muss sich jede URL in einer separaten Zeile befinden.
  - Wenn Sie mehrere URLs angeben, muss jede URL auf ein anderes externes Verzeichnis zeigen und alle externen Verzeichnisse müssen dieselben Daten enthalten.
  - Jede URL muss mit `ldap://` beginnen.
    Einschränkung: Die URL, die Sie angeben, darf nicht mit ldaps:// beginnen.

    IBM Spectrum Protect unterstützt LDAP-Verbindungen, die mit der LDAPv3-Standardoperation StartTLS geschützt werden. Mit dieser Operation wird ein sicherer TLS-Austausch (TLS = Transport Layer Security) über eine vorhandene LDAP-Verbindung eingerichtet. Mit der LDAP-Operation Simple Bind, die von IBM Spectrum Protect verwendet wird, wird das Kennwort beim Senden nicht geschützt. Eine sichere TLS-Verbindung ist erforderlich, um das Kennwort zu schützen.

Beispiel: Anschlusswert für einen LDAP-Server definieren

In der Datei dsmserv.opt den Anschlusswert 341 für einen LDAP-Server angeben:

```
ldapurl ldap://server1.storage.us.ibm.com:341/dc=storage,dc=us,dc=ibm,dc=com
```

MAXSESSIONS

Die Option MAXSESSIONS gibt die maximal zulässige Anzahl gleichzeitig stattfindender Clientsitzungen für den Server an.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
                .-25---------------.
>>-MAXSessions--+-Anzahl_Sitzungen-+-------------------------><
```

Parameter

Anzahl_Sitzungen
: Gibt die maximal zulässige Anzahl gleichzeitig stattfindender Clientsitzungen an. Der Standardwert ist 25 Clientsitzungen. Der Mindestwert ist zwei Clientsitzungen. Der Maximalwert wird nur durch die Größe des verfügbaren virtuellen Speichers oder Übertragungsressourcen begrenzt.

Beispiele

```
maxsessions 25
```

MESSAGEFORMAT

Die Option MESSAGEFORMAT gibt an, ob eine Nachrichtennummer in allen Zeilen angezeigt wird, wenn sich die Nachricht über mehrere Zeilen erstreckt.

Syntax

```
>>-MESsageformat--Zahl----------------------------------------><
```

Parameter

Zahl
: Eine Zahl auswählen, um anzugeben, ob eine Nachrichtennummer nur in der ersten Zeile einer mehrzeiligen Nachricht oder in allen Zeilen angezeigt werden soll.

  1
  : Die Nachrichtennummer wird nur in der ersten Zeile einer Nachricht angezeigt. Dies ist der Standardwert.

  2
  : Die Nachrichtennummer wird in jeder Nachrichtenzeile angezeigt.

Beispiele

```
messageformat 2
```

MIRRORLOGDIRECTORY

Die Option MIRRORLOGDIRECTORY gibt das Verzeichnis zum Spiegeln des Pfads für aktive Protokolldateien an.

Alle Änderungen, die am Verzeichnis für aktive Protokolldateien vorgenommen werden, werden auch in dieses Spiegelverzeichnis geschrieben. Diese Option wird an die Optionsdatei angehängt, wenn der Befehl DSMSERV FORMAT ausgeführt wird. Normalerweise muss das Verzeichnis nicht geändert werden.

Syntax

```
>>-MIRRorlogdirectory--Verzeichnisname------------------------><
```

Parameter

Verzeichnisname
: Gibt einen vollständig qualifizierten Verzeichnisnamen für den Spiegel der aktiven Protokolldatei an. Die maximale Anzahl Zeichen beträgt 175.

Beispiele

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
mirrorlogdirectory /tsm/mirrorlog
```

 Windows-Betriebssysteme

```
mirrorlogdirectory c:\tsmserv1\mirrorlog
```

MOVEBATCHSIZE

Die Option MOVEBATCHSIZE gibt die Anzahl Clientdateien an, die innerhalb derselben Servertransaktion als Stapel gruppiert und versetzt werden sollen. Dieses Versetzen von Daten resultiert aus Speicherpoolsicherungen und -zurückschreibungen, Umlagerungsoperationen, Wiederherstellungsoperationen und MOVE DATA-Operationen. Diese Option arbeitet zusammen mit der Option MOVESIZETHRESH.

Syntax

```
                .-1000-----------.
>>-MOVEBatchsize--+-Anzahl_Dateien-+--------------------------><
```

Parameter

Anzahl_Dateien
: Gibt eine Anzahl Dateien zwischen 1 und 1000 an. Der Standardwert ist 1000.

Beispiele

```
movebatchsize 100
```

MOVESIZETHRESH

Die Option MOVESIZETHRESH gibt den Grenzwert für die Datenmenge an (in Megabyte), die innerhalb derselben Servertransaktion als Stapel versetzt werden soll. Wenn diese Schwelle erreicht ist, werden dem aktuellen Stapel keine weiteren Dateien hinzugefügt. Nachdem der aktuelle Stapel versetzt wurde, wird eine neue Transaktion gestartet.

Syntax

```
                 .-4096------.
>>-MOVESizethresh--+- Megabyte-+------------------------------><
```

Parameter

Megabyte
: Gibt die Anzahl Megabyte als ganze Zahl von 1 bis 32768 an. Der Standardwert ist 4096. Diese Option wird mit der Option MOVEBATCHSIZE verwendet.

Beispiele

```
movesizethresh 500
```

MSGINTERVAL

Die Option MSGINTERVAL gibt die Zeit in Minuten zwischen Nachrichten an, in denen ein Bediener zum Einlegen eines Bands für den Server aufgefordert wird.

Syntax

```
                .-1-------.
>>-MSGINTerval--+-Minuten-+-------------------------------------><
```

Parameter

Minuten
: Gibt das Zeitintervall an, in dem der Operator vom Server dazu aufgefordert wird, ein Band einzulegen. Der Standardwert ist 1 Minute. Der Mindestwert ist 1 Minute.

Beispiele

```
msginterval 2
```

Windows-Betriebssysteme

NAMEDPIPENAME

Die Option NAMEDPIPENAME gibt eine Übertragungsmethode an, mit der Prozesse miteinander kommunizieren können, ohne wissen zu müssen, wo sich die Sende- und Empfangsprozesse befinden. Der Name fungiert als Aliasname und verbindet die beiden Prozesse unabhängig davon, ob sie sich auf demselben Rechner oder in verbundenen Domänen befinden.

Syntax

```
>>-NAMEDpipename--Name-----------------------------------------><
```

Parameter

Name
: Gibt die benannten Pipes an, die der Server verwenden soll. Benannte Pipes eignen sich besonders für eine Umgebung, in der sich Client und Server auf derselben Maschine befinden. In diesem Fall wird nämlich keine DFV-Software und keine Konfiguration benötigt.

Beispiele

```
namedpipename     \\.\PIPE\TSMPIPE
```

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

NDMPCONNECTIONTIMEOUT

Die Serveroption NDMPCONNECTIONTIMEOUT gibt die Zeit in Stunden an, die der IBM Spectrum Protect-Server auf den Empfang von Statusaktualisierungen während der Ausführung von NDMP-Zurückschreibungsoperationen über das LAN wartet. NDMP-Zurückschreibungsoperationen mit großen NAS-Dateisystemen können einen langen Inaktivitätszeitraum aufweisen. Der Standardwert ist 6 Stunden.

Syntax

```
                           .-6-------.
>>-NDMPCONNECTIONTIMEOUT--+-Stunden-+--------------------------><
```

Parameter

Stunden
: Die Anzahl der Stunden, die der IBM Spectrum Protect-Server auf den Empfang von Statusaktualisierungen wahrend der Ausführung einer NDMP-Zurückschreibungsoperation über das LAN wartet. Der Standardwert ist 6. Der Mindestwert ist 1 Stunde. Der maximale Wert ist 48 Stunden.

Beispiel

Geben Sie ein Zeitlimit von 10 Stunden an, bevor eine Zeitlimitüberschreitung für die NDMP-Verbindung auftritt:

```
ndmpconnectiontimeout  10
```

NDMPCONTROLPORT

Die Option NDMPCONTROLPORT gibt die Anschlussnummer an, die für interne Übertragungen für bestimmte NDMP-Operationen (NDMP = Network Data Management Protocol) verwendet werden soll. Der IBM Spectrum Protect-Server arbeitet nicht als allgemeiner NDMP-Bandserver.

Syntax

```
                    .-10000-----------.
>>-NDMPControlport--+-Anschlussnummer-+------------------------><
```

Parameter

Anschlussnummer
: Die Anschlussnummer, die für interne Übertragungen für bestimmte NDMP-Operationen verwendet werden soll. Die Anschlussnummer muss zwischen 1024 und 32767 liegen. Der Standardwert ist 10000.

Beispiele

```
ndmpcontrolport 9999
```

NDMPENABLEKEEPALIVE

Die Serveroption NDMPENABLEKEEPALIVE gibt an, ob der IBM Spectrum Protect-Server TCP-Keepalive (TCP = Transmission Control Protocol) für NDMP-Steuerverbindungen (NDMP = Network Data Management Protocol) zu NAS-Einheiten (NAS = Network-attached Storage) aktiviert. Der Standardwert ist NO.

TCP-Keepalive wird innerhalb der Netzunterstützung eines Betriebssystems implementiert. Mit TCP-Keepalive wird verhindert, dass eine lange laufende inaktive Verbindung von Firewall-Software geschlossen wird, die inaktive Verbindungen erkennt und schließt.
Einschränkung: Um Fehler zu verhindern, darf TCP-Keepalive in bestimmten Typen von Umgebungen nicht aktiviert werden. Ein Beispiel sind Umgebungen, die keine Firewall zwischen dem IBM Spectrum Protect-Server und einer NAS-Einheit haben. Ein anderes Beispiel sind Umgebungen mit Firewalls, die lange laufende inaktive Verbindungen tolerieren. Die Aktivierung von TCP-Keepalive in diesem Typ von Umgebung kann zur Folge haben, dass eine inaktive Verbindung versehentlich geschlossen wird, wenn der Verbindungspartner vorübergehend nicht auf TCP-Keepalive-Pakete antwortet.

Syntax

```
>>-NDMPENABLEKEEPALIVES--+-NO--+------------------------------><
                         '-YES-'
```

Parameter

NO
: TCP-Keepalive für alle NDMP-Steuerverbindungen inaktivieren. NO ist der Standardwert.

YES
: TCP-Keepalive für alle NDMP-Steuerverbindungen aktivieren. Die Standardleerlaufzeit, bevor das erste TCP-Keepalive-Paket gesendet wird, beträgt 120 Minuten.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeUm die Leerlaufzeit zu ändern, verwenden Sie die Serveroption NDMPKEEPIDLEMINUTES.

Beispiel

TCP-Keepalive für alle NDMP-Steuerverbindungen aktivieren, damit inaktive NDMP-Verbindungen nicht geschlossen werden:

```
ndmpenablekeepalive yes
```

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

NDMPKEEPIDLEMINUTES

Die Serveroption NDMPKEEPIDLEMINUTES gibt die Zeit in Minuten an, bevor das Betriebssystem das erste TCP-Keepalive-Paket (TCP = Transmission Control Protocol) für eine NDMP-Steuerverbindung (NDMP = Network Data Management Protocol) überträgt. Der Standardwert ist 120 Minuten.

Voraussetzung: Verwenden Sie diese Option nur nach dem Definieren des Werts YES für die Serveroption NDMPENABLEKEEPALIVES.

Syntax

```
                          .-120-----.
>>-NDMPKEEPIDLEMINUTES--+-Minuten-+---------------------------><
```

Parameter

Minuten
: Die Anzahl der Minuten der Inaktivität für NDMP-Steuerverbindungen, bevor TCP-Keepalive-Pakete übertragen werden. Der Standardwert ist 120. Der Mindestwert ist 1 Minute. Der maximale Wert ist 600 Minuten.

Beispiel

Eine Leerlaufzeit von 15 Minuten angeben, bevor das erste TCP-Keepalive-Paket gesendet wird:

```
ndmpkeepidleminutes  15
```

NDMPPORTRANGE

Die Option NDMPPORTRANGE gibt den Bereich der Anschlussnummern an, in dem IBM Spectrum Protect navigiert, um eine Anschlussnummer zum Akzeptieren einer Sitzung von einer NAS-Einheit für die Datenübertragung zu erhalten. Der Standardwert 0,0 bedeutet, dass IBM Spectrum Protect einen Anschluss vom Betriebssystem zur Verfügung stellen lässt (ephemerer Anschluss).

Sind alle angegebenen Anschlüsse belegt, wenn eine NAS-Einheit versucht, die Verbindung zum Server herzustellen, schlägt die Operation fehl. Wird eine einzelne Anschlussnummer ausgewählt (kein Komma und keine Anschlussnummer für den oberen Wert), ist der Standardwert für die obere Anschlussnummer die untere Anschlussnummer plus 100.

Werden NDMP-Daten (NDMP = Network Data Management Protocol) an einen nativen IBM Spectrum Protect-Pool übertragen, kann die Übertragung entweder von den NDMP-Systemen oder vom IBM Spectrum Protect-Server eingeleitet werden. Wenn eine Firewall den Server und die NAS-Einheiten trennt, kann es erforderlich sein, Anschlussnummern in Firewallregeln anzugeben, damit der Datenverkehr zu und von den NAS-Einheiten fließen kann. NAS-Einheiten teilen dem IBM Spectrum Protect-Server die Anschlussnummern mit, die sie verwenden, wenn der Server angesprochen wird. Die Anschlussnummern des Servers werden durch die NDMPPortrange-Optionen gesteuert. Die Steuerung der Anschlussnummern für NAS-Einheiten ist lieferantenspezifisch. Lesen Sie in der Dokumentation des Lieferanten.

Syntax

```
>>-NDMPPortrange-------------------------------------------------->

>--untere_Anschlussnummer-+------------------------+----------><
                          '-,Obere_Anschlussnummer-'
```

Parameter

untere_Anschlussnummer
: Die untere Anschlussnummer, bei der IBM Spectrum Protect mit der Navigation beginnt, wenn eine Anschlussnummer zum Akzeptieren einer Sitzung von einer NAS-Einheit für die Datenübertragung benötigt wird. Der Mindestwert für die Anschlussnummer ist 1024.

Obere_Anschlussnummer
: Die obere Anschlussnummer, bis zu der IBM Spectrum Protect navigieren kann, wenn eine Anschlussnummer zum Akzeptieren einer Sitzung von einer NAS-Einheit für die Datenübertragung benötigt wird. Der Maximalwert für die Anschlussnummer ist 32767. Die obere Anschlussnummer muss mit der unteren Anschlussnummer übereinstimmen oder höher als die untere Anschlussnummer sein.

Beispiele

Angeben, dass IBM Spectrum Protect im Anschlussnummernbereich 1024 - 2024 navigieren kann.

```
ndmpportrange 1024,2024
```

NDMPPREFDATAINTERFACE

Diese Option gibt die IP-Adresse an, die der Schnittstelle zugeordnet ist, in der der Server alle NDMP-Sicherungsdaten (NDMP = Network Data Management Protocol) empfangen soll.

Diese Option betrifft alle nachfolgenden Operationen zwischen NDMP-Dateiserver und Server, aber hat keinen Einfluss auf NDMP-Steuerverbindungen, die die Standardnetzschnittstelle des Systems verwenden. Der Wert dieser Option ist ein Hostname oder eine IPV4-

Adresse, der bzw. die einer der aktiven Netzschnittstellen des Systems zugeordnet ist, auf dem der IBM Spectrum Protect-Server ausgeführt wird. Diese Schnittstelle muss für IPV4 aktiviert sein.

Sie können diese Serveroption aktualisieren, ohne den Server zu stoppen und erneut zu starten, indem Sie den Befehl SETOPT verwenden.

Syntax

```
>>-NDMPPREFDATAINTERFACE--IP-Adresse--------------------------><
```

Parameter

IP-Adresse
Geben Sie eine Adresse in Schreibweise mit Trennzeichen oder im Hostnamensformat an. Wird eine Adresse in der Schreibweise mit Trennzeichen angegeben, wird die Adresse nicht mit einem Domänennamensserver geprüft. Ist die Adresse nicht korrekt, kann dies zu Fehlern führen, wenn der Server versucht, am Anfang einer Sicherung zwischen NDMP-Dateiserver und Server ein Socket zu öffnen.

Adressen im Hostnamensformat werden mit einem Domänennamensserver geprüft. Es gibt keinen Standardwert. Wird kein Wert definiert, verwenden alle NDMP-Operationen die Netzschnittstelle des IBM Spectrum Protect-Servers zum Empfangen von Sicherungsdaten während der Sicherungsoperationen zwischen NDMP-Dateiserver und Server.

Um den Optionswert zu löschen, geben Sie den Befehl SETOPT mit einem Nullwert ("") an.

Beispiele:

```
ndmpprefdatainterface  net1.tucson.ibm.com

ndmpprefdatainterface  9.11.152.89
```

NOPREEMPT

Der Server ermöglicht bestimmten Operationen das Zugriffsvorrecht für Datenträger und Einheiten. Durch Angabe von NOPREEMPT kann das Zugriffsvorrecht inaktiviert werden. In diesem Fall hat dann keine Operation das Zugriffsvorrecht auf einen Datenträger und lediglich einer Datenbanksicherungsoperation kann das Zugriffsvorrecht für eine Einheit vor einer anderen Operation eingeräumt werden.

Beispielsweise hat eine Clientoperation zum Zurückschreiben von Daten Vorrang vor einer Clientdatensicherung, wenn es darum geht, eine bestimmte Einheit zu verwenden oder auf einen bestimmten Datenträger zuzugreifen.

Syntax

```
>>-NOPREEMPT-------------------------------------------------><
```

Parameter

Keine.

Beispiele

Zugriffsvorrecht unter Serveroperationen inaktivieren:

```
nopreempt
```

NORETRIEVEDATE

Die Option NORETRIEVEDATE gibt an, dass der Server das Abrufdatum einer Datei in einem Plattenspeicherpool nicht aktualisiert, wenn ein Client die Datei zurückschreibt oder abruft. Diese Option und der Speicherpoolparameter MIGDELAY steuern, wann der Server Dateien umgelagert.

Wird NORETRIEVEDATE nicht angegeben, lagert der Server Dateien um, nachdem sie sich die in dem Parameter MIGDELAY angegebene Anzahl Tage in dem Speicherpool befunden haben. Die Anzahl Tage wird ab dem Tag gezählt, an dem die Datei in dem Speicherpool gespeichert wurde oder von einem Client abgerufen wurde, je nachdem, welches Datum aktueller ist. Wird NORETRIEVEDATE angegeben, wird das Abrufdatum einer Datei von dem Server nicht aktualisiert, und die Anzahl Tage wird ab dem Tag gezählt, an dem die Datei in den Plattenspeicherpool gestellt wurde.

Wird diese Option angegeben und ist Caching für einen Plattenspeicherpool aktiviert, ist die Wiederherstellung von Cache-Speicherbereich betroffen. Wird Speicherbereich in einem Plattenspeicherpool benötigt, der Cache-Dateien enthält, holt der Server den Speicherbereich durch das selektive Löschen von Cache-Kopien. Dateien, die die ältesten Abrufdaten haben und den meisten Speicherbereich belegen, werden zum

Löschen ausgewählt. Wird NORETRIEVEDATE angegeben, wird das Abrufdatum von dem Server nicht aktualisiert, wenn eine Datei abgerufen wird. Dies kann dazu führen, dass Cache-Kopien entfernt werden, auch wenn sie kürzlich von einem Client abgerufen wurden.

Syntax

```
>>-NORETRIEVEDATE-----------------------------------------------><
```

Parameter

Keine.

Beispiele

Angeben, dass die Abrufdaten von Dateien in Plattenspeicherpools nicht aktualisiert werden, wenn Clients die Dateien zurückschreiben und abrufen:

```
noretrievedate
```

Windows-Betriebssysteme

NPAUDITFAILURE

Die Option NPAUDITFAILURE gibt an, ob ein Ereignis an das Ereignisprotokoll gesendet wird, wenn ein Knoten sich bei dem Server anmeldet und dabei einen Namen verwendet, der sich zwar in der Windows-Gruppe befindet, aber nicht mit dem Windows-Kontoanmeldenamen übereinstimmt. Um sicherzustellen, dass ein Knoten nur auf seine eigenen Daten zugreifen kann, müssen der Knotenname und der Windows-Kontoname übereinstimmen.

Syntax

```
>>-NPAUDITFailure--+-Yes-+-------------------------------------><
                   '-No--'
```

Parameter

Yes
: Gibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn ein Knoten sich bei dem Server anmeldet und dabei einen Namen verwendet, der sich in der Windows-Gruppe befindet. Dieser Name stimmt jedoch nicht mit dem Windows-Kontoanmeldenamen überein.

No
: Gibt an, dass kein Ereignis über einen Prüffehler an das Ereignisprotokoll gesendet wird.

Beispiele

Angeben, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn ein Knoten sich bei dem Server anmeldet und dabei einen Namen verwendet, der sich in der Windows-Gruppe befindet. Dieser Name stimmt jedoch nicht mit dem Windows-Kontoanmeldenamen überein.

```
npauditfailure yes
```

Windows-Betriebssysteme

NPAUDITSUCCESS

Die Option NPAUDITSUCCESS gibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknotenbenutzer über SECUREPIPE eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann.

Syntax

```
>>-NPAUDITSuccess--+-Yes-+-------------------------------------><
                   '-No--'
```

Parameter

Yes

Gibt an, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknotenbenutzer über SECUREPIPES eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann.

No
Gibt an, dass kein Ereignis an das Windows-Protokoll gesendet wird.

Beispiele

Angeben, dass ein Ereignis an das Ereignisprotokoll gesendet wird, wenn für einen Clientknoten eine Identifikationsprüfung durchgeführt wird, bevor er auf den Server zugreifen kann.

```
npauditsuccess yes
```

 Windows-Betriebssysteme

NPBUFFERSIZE

Die Option NPBUFFERSIZE gibt die Größe des Kommunikationspuffers für benannte Pipes an.

Syntax

```
                .-8--------.
>>-NPBUFfersize--+-Kilobyte-+---------------------------------><
```

Parameter

Kilobyte
Gibt die Größe des Kommunikationspuffers für benannte Pipes in Kilobyte an. Der Standardwert ist 8.

Beispiele

Einen Kommunikationspuffer mit 16 KB für benannte Pipes angeben:

```
npbuffersize 16
```

 Windows-Betriebssysteme

NUMBERFORMAT

Die Option NUMBERFORMAT gibt das Format an, in dem der Server Zahlen anzeigt.

Der Wert von NUMBERFORMAT wird von dem Zahlenformat überschrieben, das in den länderspezifischen Angaben definiert ist, wenn die länderspezifischen Angaben beim Starten des Servers erfolgreich initialisiert wurden. Die länderspezifischen Angaben werden in der Option LANGUAGE angegeben.

Syntax

```
>>-NUMberformat--Zahl-----------------------------------------><
```

Parameter

Zahl
Eine Zahl von 1 bis 6 auswählen, um das vom Server verwendete Zahlenformat anzugeben. Der Standardwert ist 1.

1
1,000.00
2
1,000,00
3
1 000,00
4
1 000.00
5
1.000,00
6
1'000,00

Beispiele

```
numberformat 4
```

NUMOPENVOLSALLOWED

Die Option NUMOPENVOLSALLOWED gibt die Anzahl der FILE-Eingabedatenträger in einem deduplizierten Speicherpool an, die gleichzeitig geöffnet sein können.

Eingabedatenträger enthalten Daten, die während der Ausführung von Clientzurückschreibungsoperationen und Serverprozessen, wie beispielsweise Wiederherstellung und Umlagerung, gelesen werden sollen. Mit dieser Option kann die Leistung verbessert werden, indem die Häufigkeit reduziert wird, mit der Datenträger geöffnet und geschlossen werden.

Jede Sitzung innerhalb einer Clientoperation oder eines Serverprozesses kann über so viele geöffnete FILE-Datenträger verfügen, wie mit dieser Option angegeben wird. Eine Sitzung wird durch eine Clientoperation oder einen Serverprozess eingeleitet. Es können jeweils Mehrfachsitzungen gestartet werden.

Während einer Clientzurückschreibungsoperation können Datenträger für die Dauer einer Clientzurückschreibungsoperation und so lange geöffnet bleiben, wie eine Clientsitzung aktiv ist. Bei der Ausführung einer Zurückschreibungsoperation ohne Abfrage bleiben die Datenträger geöffnet, bis die Zurückschreibung ohne Abfrage beendet ist. Zu diesem Zeitpunkt werden alle Datenträger geschlossen und freigegeben. Bei einer klassischen Zurückschreibungsoperation, die im Dialogmodus gestartet wird, können die Datenträger jedoch am Ende der Zurückschreibungsoperation geöffnet bleiben. Die Datenträger werden geschlossen und freigegeben, wenn die nächste klassische Zurückschreibungsoperation angefordert wird.

Definieren Sie diesen Wert in der Serveroptionsdatei oder mit dem Befehl SETOPT.

Tipp: Mit dieser Option kann die Anzahl der jeweils verwendeten Datenträger und Mountpunkte erheblich erhöht werden. Um die Leistung zu optimieren, führen Sie diese Schritte aus:

- Um NUMOPENVOLSALLOWED zu definieren, wählen Sie einen Anfangswert aus (der Standardwert wird empfohlen). Überwachen Sie Clientsitzungen und Serverprozesse. Überprüfen Sie die höchste Anzahl der Datenträger, die für eine einzelne Sitzung oder einen einzelnen Prozess geöffnet sind. Erhöhen Sie die Einstellung von NUMOPENVOLSALLOWED, wenn die höchste Anzahl der geöffneten Datenträger dem mit NUMOPENVOLSALLOWED angegebenen Wert entspricht.
- Um zu verhindern, dass Sitzungen oder Prozesse auf einen Mountpunkt warten müssen, erhöhen Sie den Wert des Parameters MOUNTLIMIT in der Einheitenklassendefinition. Geben Sie für den Parameter MOUNTLIMIT einen so hohen Wert an, dass alle Clientsitzungen und Serverprozesse, die deduplizierte Speicherpools verwenden, die Anzahl der Datenträger öffnen können, die mit der Option NUMOPENVOLSALLOWED angegeben ist. Überprüfen Sie für Clientsitzungen das Ziel in der Kopiengruppendefinition, um die Anzahl der Knoten zu bestimmen, die Daten in dem deduplizierten Speicherpool speichern. Überprüfen Sie für Serverprozesse die Anzahl der Prozesse, die für jeden Prozess für den Speicherpool zulässig sind.
- Es kann eine Situation auftreten, in der ein Knoten gleichzeitig in einem deduplizierten Speicherpool sichert und aus einem deduplizierten Speicherpool zurückschreibt oder gleichzeitig in einem deduplizierten Speicherpool archiviert und aus einem deduplizierten Speicherpool abruft. Alle für diese Operationen erforderlichen Mountpunkte erhöhen die Gesamtzahl der Mountpunkte, die von dem Knoten benötigt werden.

  Als Ergebnis kann der Knoten möglicherweise keine weiteren Sicherungssitzungen starten, wenn für ihn bereits mehr Mountpunkte geöffnet sind als der Parameter MAXNUMMP in der Clientknotendefinition erlaubt. Diese Situation kann auftreten, obwohl der Wert für MOUNTLIMIT für die Einheitenklasse nicht überschritten wurde.

  Um zu verhindern, dass Sicherungs- und Abrufoperationen fehlschlagen, setzen Sie den Wert des Parameters MAXNUMMP in der Clientknotendefinition auf einen Wert, der mindestens so hoch wie der Wert der Option NUMOPENVOLSALLOWED ist. Erhöhen Sie diesen Wert, wenn Sie feststellen, dass der Knoten Sicherungs- oder Abrufoperationen nicht ausführt, da der Wert von MAXNUMMP überschritten wird.

Syntax

```
>>-NUMOPENVOLSallowed--Anzahl_geöffneter_Datenträger----------><
```

Parameter

Anzahl_geöffneter_Datenträger
: Gibt die Anzahl der FILE-Eingabedatenträger in einem deduplizierten Speicherpool an, die gleichzeitig geöffnet sein können. Der Standardwert ist 10. Der Mindestwert ist 3. Der Maximalwert ist 999.

Beispiele

Angeben, dass bis zu 5 Datenträger in einem deduplizierten Speicherpool gleichzeitig geöffnet sein können.

```
numopenvolsallowed 5
```

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

PUSHSTATUS

Die Option PUSHSTATUS wird auf Peripherieservern verwendet, um sicherzustellen, dass Statusinformationen an den Hub-Server gesendet werden. Aktualisieren Sie diese Option nur, wenn Sie die Konfiguration des Operations Center im vorkonfigurierten Zustand zurückschreiben müssen, in dem die IBM Spectrum Protect-Server nicht als Hub-Server oder Peripherieserver definiert sind.

Wenn Sie die Konfiguration des Operations Center im vorkonfigurierten Zustand zurückschreiben müssen, müssen Sie den folgenden Befehl auf jedem Peripherieserver ausgeben:

```
SETOPT PUSHSTATUS NO
```

QUERYAUTH

Die Option QUERYAUTH gibt die Administratorberechtigungsstufe an, die für die Ausgabe des Befehls QUERY oder SQL SELECT erforderlich ist. Standardmäßig kann jeder Administrator die Befehle QUERY und SELECT ausgeben. Mit dieser Option kann die Verwendung dieser Befehle eingeschränkt werden.

Syntax

```
>>-QUERYAuth--+-NOne-----+--------------------------------------><
              +-SYstem---+
              +-POlicy---+
              +-STorage--+
              '-OPerator-'
```

Parameter

NOne
: Jeder Administrator kann den Befehl QUERY oder SELECT ausgeben, ohne dass eine Administratorberechtigung erforderlich ist.

SYstem
: Administratoren müssen über die Berechtigung SYSTEM verfügen, um den Befehl QUERY oder SELECT ausgeben zu können.

POlicy
: Administratoren müssen über die Berechtigung POLICY für eine oder mehrere Maßnahmendomänen oder über die Berechtigung SYSTEM verfügen, um den Befehl QUERY oder SELECT ausgeben zu können.

STorage
: Administratoren müssen über die Berechtigung STORAGE für einen oder mehrere Speicherpools oder über die Berechtigung SYSTEM verfügen, um den Befehl QUERY oder SELECT ausgeben zu können.

OPerator
: Administratoren müssen über die Berechtigung OPERATOR oder SYSTEM verfügen, um den Befehl QUERY oder SELECT ausgeben zu können.

Beispiele

Um die Verwendung der Befehle QUERY und SELECT auf Administratoren mit System- oder Speicherberechtigung zu beschränken, folgendes eingeben:

```
queryauth storage
```

RECLAIMDELAY

Mit dieser Option wird die Wiederherstellung eines SnapLock-Datenträgers verzögert. Damit wird es ermöglicht, dass verbleibende Daten verfallen können, so dass keine Notwendigkeit zur Wiederherstellung des Datenträgers besteht.

Syntax

```
                .-4-----------.
>>-RECLAIMDELAY--+-Anzahl_Tage-+-------------------------------><
```

Parameter

Anzahl_Tage
: Gibt die Anzahl der Tage an, die die Wiederherstellung eines SnapLock-Datenträgers verzögert werden soll.

Bevor ein SnapLock-Datenträger wiederhergestellt wird, lässt der IBM Spectrum Protect-Server die angegebene Anzahl Tage verstreichen und bietet so die Möglichkeit, dass alle verbleibenden Dateien auf dem Datenträger verfallen können. Der standardmäßige Zeitraum für die Wiederherstellungsverzögerung sind 4 Tage. Es kann ein Wert zwischen 1 und 120 Tage definiert werden.

Beispiele

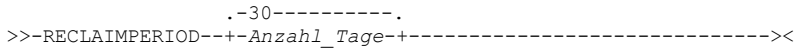
Angeben, dass die Anzahl Tage für die Verzögerung der Wiederherstellung 30 Tage beträgt:

```
reclaimdelay 30
```

RECLAIMPERIOD

Mit dieser Option können Sie die Anzahl der Tage für den Wiederherstellungszeitraum eines SnapLock-Datenträgers definieren.

Syntax



Parameter

Anzahl_Tage
Gibt die Anzahl der Tage an, die für den Wiederherstellungszeitraum eines SnapLock-Datenträgers zulässig sind.
Nachdem die Aufbewahrungsdauer eines SnapLock-Datenträgers abgelaufen ist, stellt der IBM Spectrum Protect-Server den Datenträger innerhalb der angegebenen Anzahl Tage wieder her, wenn sich noch Daten auf dem Datenträger befinden. Der standardmäßige Wiederherstellungszeitraum beträgt 30 Tage. Es kann ein Wert zwischen 7 und 365 Tage definiert werden.

Der Wiederherstellungszeitraum beginnt erst nach Ablauf des RECLAIMDELAY-Zeitraums.

Beispiele

Angeben, dass der Wiederherstellungszeitraum 45 Tage beträgt:

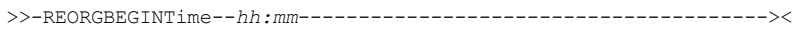
```
reclaimperiod 45
```

REORGBEGINTIME

Die Option REORGBEGINTIME gibt die früheste Zeit an, zu der der IBM Spectrum Protect-Server eine Tabellen- oder Indexreorganisation starten kann.

Planen Sie den Start der vom Server eingeleiteten Reorganisationen während eines Zeitraums, in dem die Serveraktivität niedrig ist. Verwenden Sie diese Option zusammen mit der Option REORGDURATION. Die Option REORGDURATION gibt ein Intervall an, in dem die Reorganisation starten kann.

Syntax



Parameter

hh:mm
Gibt die Zeit an, zu der der Server eine Reorganisation starten kann: Die Standardstartzeit ist 6:00. Verwenden Sie ein 24-Stunden-Format, um die Zeit anzugeben.

Zeit	Beschreibung	Werte
hh	Die Stunde des Tages	Geben Sie eine Zahl von 00 bis 23 an.
mm	Die Minute der Stunde	Geben Sie eine Zahl von 00 bis 59 an.

Beispiele

6:00 Uhr als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 06:00
```

20 Uhr 30 als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 20:30
```

12 Uhr mittags als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 12:00
```

15 Uhr 30 als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 15:30
```

Mitternacht als früheste Zeit angeben, zu der eine Reorganisation gestartet werden kann.

```
reorgbegintime 00:00
```

REORGDURATION

Die Option REORGDURATION gibt ein Intervall an, in dem die vom Server eingeleitete Tabellen- oder Indexreorganisation gestartet werden kann.

Planen Sie den Start der vom Server eingeleiteten Reorganisationen während eines Zeitraums, in dem die Serveraktivität niedrig ist. Verwenden Sie diese Option zusammen mit der Option REORGBEGINTIME. Die Option REORGBEGINTIME gibt die früheste Zeit an, zu der der Server eine Reorganisation starten kann.

Syntax

```
>>-REORGDURation--nn-----------------------------------------><
```

Parameter

nn
: Gibt die Anzahl der Stunden an, in denen eine Reorganisation gestartet werden kann. Der Mindestwert ist 1, der Maximalwert ist 24. Der Standardwert ist 24.

Beispiel

Ein Intervall von vier Stunden angeben, in denen eine Reorganisation gestartet werden kann.

```
reorgduration 4
```

REPORTRETRIEVE

Die Option REPORTRETRIEVE erstellt Berichte zu Zurückschreibungs- oder Abrufoperationen, die von Clientknoten oder Administratoren ausgeführt werden. Der Standardwert ist NO.

Syntax

```
>>-REPORTRETRIEVE--+-YES-+-------------------------------------><
                   '-NO--'
```

Parameter

YES
: Gibt an, dass Nachrichten an der Serverkonsole ausgegeben und im Aktivitätenprotokoll gespeichert werden, wenn Dateien vom IBM Spectrum Protect-Server zurückgeschrieben oder abgerufen werden. Die Nachrichten geben den Namen der Objekte an, die zurückgeschrieben oder abgerufen werden, und identifizieren den Clientknoten oder den Administrator, der die Operation ausführt.

NO
: Gibt an, dass keine Nachrichten ausgegeben werden.

Beispiele

Angeben, dass Nachrichten im Aktivitätenprotokoll ausgegeben und gespeichert werden, wenn Dateien vom IBM Spectrum Protect-Server zurückgeschrieben oder abgerufen werden:

```
reportretrieve yes
```

Die folgende Nachricht wird für eine Verwaltungsclientsitzung ausgegeben:

```
ANR0411I Sitzung 8 für Administrator COLIND-TUC, der am Knoten COLIND-TUC
angemeldet ist, hat das Sicherungsobjekt zurückgeschrieben oder abgerufen:
Knoten COLIND-TUC,Dateibereich \\colind-tuc\c$, object\CODE\TESTDATA\ XXX.OUT
```

REPLBATCHSIZE

Die Option REPLBATCHSIZE gibt die Anzahl Clientdateien an, die innerhalb derselben Servertransaktion als Stapel repliziert werden sollen. Diese Option betrifft nur die Knotenreplikationsprozesse und arbeitet mit der Option REPLSIZETHRESH, um die Knotenreplikationsverarbeitung zu verbessern.

Die Option REPLBATCHSIZE begrenzt die Anzahl der Dateien in einer Transaktion und die Option REPLSIZETHRESH begrenzt die Anzahl der Byte in einer Transaktion. Die Transaktion wird beendet, wenn entweder der Schwellenwert für REPLBATCHSIZE oder der Schwellenwert für REPLSIZETHRESH erreicht wird.

Syntax

```
                .-4096-----------.
>>-REPLBatchsize--+-Anzahl_Dateien-+--------------------------><
```

Parameter

Anzahl_Dateien
: Gibt eine Anzahl Dateien zwischen 1 und 32768 an. Der Standardwert ist 4096.

Beispiele

```
replbatchsize 25000
```

REPLSIZETHRESH

Die Option REPLSIZETHRESH gibt einen Schwellenwert (in Megabyte) für das replizierte Datenvolumen innerhalb derselben Servertransaktion an.

Das Datenvolumen basiert auf der nicht deduplizierten Größe der Datei. Dies ist die Originalgröße der Datei. Das Datenvolumen, das repliziert wird, wird durch den Schwellenwert gesteuert. Wenn das Datenvolumen den Schwellenwert überschreitet, beendet der Server die Transaktion und es werden keine weiteren Dateien dem aktuellen Stapel hinzugefügt. Eine neue Transaktion wird gestartet, nachdem der aktuelle Stapel repliziert wurde. Diese Option wird mit der Option REPLBATCHSIZE verwendet.

Beispiel: Angenommen, eine Datei hat 10 MB und wird in einem Speicherpool gespeichert, der für die Datendeduplizierung aktiviert ist, und nur 2 MB der Datei werden während der Replikation übertragen. Das replizierte Datenvolumen schließt die Größe von 10 MB der Datei ein und schließt die übertragenen 2 MB aus. Wenn das replizierte Datenvolumen den für den REPLSIZETHRESH-Schwellenwert angegebenen Wert überschreitet, wird die Transaktion beendet.

Tipp: Falls Sie Daten von einem Quellenserver in der Cloud replizieren und auf dem Zielserver häufig die Servernachricht ANR1880W empfangen, verringern Sie den Wert der Option REPLSIZETHRESH auf dem Quellenserver.

Syntax

```
                 .-4096------.
>>-REPLSizethresh--+- Megabyte-+------------------------------><
```

Parameter

Megabyte
: Gibt die Anzahl Megabyte als ganze Zahl von 1 bis 32768 an. Der Standardwert ist 4096.

Beispiele

```
replsizethresh 2000
```

REQSYSAUTHOUTFILE

Die Option REQSYSAUTHOUTFILE gibt an, ob die Systemberechtigung für Verwaltungsbefehle erforderlich ist, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben.

Diese Option gilt für folgende Befehle:

- BACKUP DEVCONFIG mit dem Parameter FILENAMES
- BACKUP VOLHISTORY mit dem Parameter FILENAMES
- DEFINE BACKUPSET
- DELETE BACKUPSET
- GENERATE BACKUPSET
- MOVE DRMEDIA mit dem Parameter CMD
- MOVE MEDIA mit dem Parameter CMD
- QUERY DRMEDIA mit dem Parameter CMD
- QUERY MEDIA mit dem Parameter CMD
- QUERY SCRIPT mit dem Parameter OUTPUTFILE

Syntax

```
>>-REQSYSauthoutfile--+-Yes-+-----------------------------------><
                      '-No--'
```

Parameter

Yes
: Die Systemberechtigung ist für Verwaltungsbefehle erforderlich, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben.

No
: Die Systemberechtigung ist für Verwaltungsbefehle nicht erforderlich, die IBM Spectrum Protect veranlassen, in eine externe Datei zu schreiben. Dies bedeutet, dass die Berechtigungsstufe zur Ausgabe des Befehls nicht geändert werden muss.

Beispiele

```
reqsysauthoutfile no
```

RESOURCETIMEOUT

Die Option RESOURCETIMEOUT gibt an, wie lange der Server auf eine Ressource wartet, bevor die anstehende Anforderung einer Ressource abgebrochen wird. Tritt eine Zeitlimitüberschreitung auf, wird die Anforderung der Ressource abgebrochen.

Anmerkung: Wird eine Gruppe von gemeinsam benutzten Kassettenarchivressourcen verwaltet, wie beispielsweise Server, die als Kassettenarchivmanager und -clients bestimmt sind, sollte diese Option für alle Teilnehmer an der gemeinsam benutzten Konfiguration auf dasselbe Zeitlimit gesetzt werden. Bei jeder Fehlerbehebung verwendet IBM Spectrum Protect immer das längste Zeitlimit.

Syntax

```
                    .-60------.
>>-RESOURCETimeout--+-Minuten-+--------------------------------><
```

Parameter

Minuten
: Gibt die maximale Anzahl Minuten an, die der Server auf eine Ressource wartet. Der Standardwert ist 60 Minuten. Der Mindestwert ist 1 Minute.

Beispiele

Angeben, dass der Server 15 Minuten auf eine Serverressource wartet:

```
resourcetimeout 15
```

RESTOREINTERVAL

Die Option RESTOREINTERVAL gibt an, wie lange eine wiederanlauffähige Zurückschreibungssitzung in der Serverdatenbank gesichert werden kann. Solange die Zurückschreibungssitzung in der Datenbank gesichert ist, kann sie ab dem Punkt, an dem sie gestoppt wurde, erneut gestartet werden.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
                    .-1440----.
>>-RESTOREINTERVAL--+-Minuten-+--------------------------------><
```

Parameter

Minuten
: Gibt an, wie lange sich eine wiederanlauffähige Zurückschreibungssitzung in der Datenbank befinden kann, bevor sie ihre Gültigkeit verliert (Angabe in Minuten). Der Mindestwert ist 0, der Höchstwert beträgt 10080 Minuten (eine Woche). Der Standardwert ist 1440 Minuten (24 Stunden). Wird der Wert auf 0 gesetzt und die Zurückschreibung unterbrochen oder abgebrochen, wird die Zurückschreibung dennoch in den Status "wiederanlauffähig" versetzt. Sie kann jedoch sofort als "Verfallskandidat" ausgewählt werden.

Beispiele

```
restoreinterval 1440
```

RETENTIONEXTENSION

Die Option RETENTIONEXTENSION gibt die Anzahl der Tage an, um die das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitert werden soll. Mit dieser Option kann der Server das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitern, um eine übermäßige Wiederherstellung zu vermeiden.

Syntax

```
>>-RETENTIONEXTENSION--Anzahl_Tage----------------------------><
```

Parameter

Anzahl_Tage
: Gibt die Anzahl der Tage an, um die das Ende des Aufbewahrungszeitraums eines SnapLock-Datenträgers erweitert werden soll. Der Mindestwert ist 30 Tage; der Maximalwert ist 9999 Tage; der Standardwert ist 365.
Wenn Sie den Wert 0 (null) für den Parameter RETVER einer Archivierungskopiengruppe angeben, ist der tatsächliche Wert, der für RETVER verwendet wird, der Wert der Option RETENTIONEXTENSION, wenn eine der folgenden Bedingungen ebenfalls zutrifft:

  - Der Zielspeicherpool für die Archivierungskopiengruppe ist ein SnapLock-Speicherpool.
  - Der Speicherpool, der das Ziel für eine Speicherpoolumlagerung oder eines Befehls MOVE DATA oder MOVE NODEDATA ist, ist ein SnapLock-Speicherpool.

  Ist ein SnapLock-Datenträger der Zieldatenträger für Daten von einem anderen SnapLock-Datenträger und ist die verbleibende Aufbewahrungsdauer der Daten auf dem Datenträger geringer als der angegebene Wert, wird das Ende des Aufbewahrungszeitraums unter Verwendung des angegebenen Werts definiert. Andernfalls wird die verbleibende Aufbewahrungsdauer der Daten verwendet, um die Aufbewahrungsdauer des Datenträgers zu definieren.
  Befindet sich ein SnapLock-Datenträger innerhalb der Wiederherstellungsperiode, aber hat der Prozentsatz des wiederherstellbaren Speicherbereichs des Datenträgers nicht den Wiederherstellungsschwellenwert des Speicherpools oder den im Parameter THRESHOLD eines Befehls RECLAIM STGPOOL angegebenen Wert überschritten, wird das Ende des Aufbewahrungszeitraums des SnapLock-Datenträgers um den Wert erweitert, der mit der Option RETENTIONEXTENSION angegeben ist.

Beispiele

Angeben, dass das Ende des Aufbewahrungszeitraums um 60 Tage erweitert wird:

```
retentionextension 60
```

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

SANDISCOVERY

Die Option SANDISCOVERY gibt an, ob die SAN-Erkennungsfunktion von IBM Spectrum Protect aktiviert ist.

Um die SAN-Erkennung verwenden zu können, müssen alle Einheiten in dem SAN eine eindeutige Einheitenseriennummer haben. Ist die Option auf ON gesetzt, führt der Server in den folgenden Situationen eine SAN-Erkennung durch:

- Wenn der Einheitenpfad geändert wird
- Wenn der Befehl QUERY SAN ausgegeben wird

Bei Verwendung der SAN-Erkennung kann der Server automatisch den Gerätedateinamen für eine Einheit korrigieren, wenn sich der Name für eine angegebene Bandeinheit ändert.

Der IBM Spectrum Protect-Server benötigt keine persistente Bindung mit der aktivierten SAN-Erkennungsfunktion. Um eine Liste der Einheiten für den Server anzuzeigen, können Sie den Befehl QUERY SAN ausgeben.

Syntax

```
   .-SANDISCOVERY--=--OFF-----------------.
>>-+-----------------------------------+-------------------><
   '-SANDISCOVERY--=--+-ON--------------+-'
                      '-UNSCANNEDPATHOFF-'
```

Parameter

ON
: Gibt an, dass der Server eine SAN-Erkennung ausführt, wenn der Einheitenpfad geändert oder der Befehl QUERY SAN ausgegeben wird.

OFF
: Gibt an, dass der Server keine SAN-Erkennung ausführt, wenn der Einheitenpfad geändert oder der Befehl QUERY SAN ausgegeben wird. Wenn der IBM Spectrum Protect-Server eine Einheit nicht öffnen kann, wird eine Nachricht ausgegeben, aber der Pfad, der der Einheit zugeordnet ist, wird nicht offline gesetzt. Dieser Wert ist der Standardwert.

UNSCANNEDPATHOFF
: Gibt an, dass der Server keine SAN-Erkennung ausführt, wenn der Einheitenpfad geändert oder der Befehl QUERY SAN ausgegeben wird. Wenn der IBM Spectrum Protect-Server eine Einheit nicht öffnen kann, wird eine Nachricht ausgegeben und der Pfad zu der Einheit wird offline gesetzt.

Beispiele

```
sandiscovery on
```

Zugehörige Befehle

Tabelle 1. Zugehörige Befehle für SANDISCOVERY

Befehl	Beschreibung
PERFORM LIBACTION	Definiert alle Laufwerke und Pfade für ein Kassettenarchiv.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

SANDISCOVERYTIMEOUT

Die Option SANDISCOVERYTIMEOUT gibt die Zeit an, die für die Antwort von Hostbusadaptern zulässig ist, wenn sie von dem SAN-Erkennungsprozess abgefragt werden. Sobald die für SANDISCOVERYTIMEOUT angegebene Zeit erreicht wird, tritt bei dem Prozess eine Zeitlimitüberschreitung auf.

Syntax

```
>>-SANDISCOVERYTIMEOUT--Wert-----------------------------------><
```

Parameter

Wert
: Gibt die Zeit an, die vergehen darf, bevor bei dem SAN-Erkennungsprozess eine Zeitlimitüberschreitung auftritt. Der Bereich liegt zwischen 15 und 1800 Sekunden. Der Standardwert ist 15 Sekunden.

Beispiele

```
sandiscoverytimeout 45
```

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

SANREFRESHTIME

Die Option SANREFRESHTIME gibt die Zeit an, die vergeht, bevor die zwischengespeicherten SAN-Erkennungsinformationen aktualisiert werden. Die Option SANREFRESHTIME hat den Standardwert 0, der angibt, dass kein SAN-Erkennungscache vorhanden ist. Bei jeder Ausführung einer

SAN-Erkennungsoperation durch den Server werden die Informationen direkt von dem Hostbusadapter abgerufen.

Anmerkung: Der Serverbefehl QUERY SAN empfängt SAN-Informationen immer zu dem Zeitpunkt, an dem der Befehl ausgegeben wird, und ignoriert den Wert, der für SANREFRESHTIME angegeben ist.

Syntax

```
                    .-0----.
>>-SANREFRESHTIME--+-Zeit-+-------------------------------------><
```

Parameter

Zeit

Die Zeit in Sekunden, bevor die zwischengespeicherten SAN-Erkennungsinformationen aktualisiert werden. Der Standardwert ist 0 und gibt an, dass SAN-Erkennungsinformationen nicht zwischengespeichert werden. Wird ein anderer Wert als 0 angegeben, beispielsweise 100 Sekunden, werden die SAN-Erkennungsinformationen 100 Sekunden nach der vorherigen SAN-Erkennungsoperation aktualisiert.

Beispiele

Die SAN-Erkennungsinformationen nach 100 Sekunden aktualisieren.

```
sanrefreshtime 100
```

Das Caching der SAN-Erkennungsinformationen inaktivieren.

```
sanrefreshtime 0
```

SEARCHMPQUEUE

Die Option SEARCHMPQUEUE gibt die Reihenfolge an, in der der Server Anforderungen in der Ladewarteschlange ausführt. Wird die Option angegeben, versucht der Server zuerst, Anforderungen für Datenträger auszuführen, die bereits geladen sind. Diese Anforderungen können vor anderen Anforderungen ausgeführt werden, auch wenn die anderen Anforderungen schon länger auf den Mountpunkt warten. Wird diese Option nicht angegeben, führt der Server Anforderungen in der Reihenfolge aus, in der sie empfangen werden.

Syntax

```
>>-SEARCHMPQUEUE-----------------------------------------------><
```

Parameter

Keine.

Beispiele

Angeben, dass der Server zuerst versucht, eine Anforderung für einen Datenträger auszuführen, der bereits geladen ist:

```
searchmpqueue
```

 Windows-Betriebssysteme

SECUREPIPES

Bei Verwendung des Protokolls mit benannten Pipes führt das Aktivieren von SECUREPIPES dazu, dass der Server die über ADSMGROUPNAME angegebene Windows-Gruppe prüft, um einen Clientknoten/Benutzer zu authentifizieren.

Anhand des in der Windows-Gruppe definierten Benutzernamens und Kennworts wird der Knoten/Benutzer für den Zugriff auf die Serverdaten authentifiziert. Der Knoten/Benutzer muss außerdem als IBM Spectrum Protect-Clientknoten registriert sein. Das Kennwort für den IBM Spectrum Protect-Clientknoten wird jedoch ignoriert und statt dessen das für den Benutzer vergebene Windows-Kennwort verwendet.

Syntax

```
>>-SECUREPipes--+-Yes-+-----------------------------------------><
                '-No--'
```

Parameter

Yes
: Gibt an, dass IBM Spectrum Protect die über ADSMGROUPNAME angegebene Windows-Gruppe prüft, um einen Clientknoten/Benutzer zu authentifizieren.

No
: Gibt an, dass IBM Spectrum Protect die über ADSMGROUPNAME angegebene Windows-Gruppe nicht prüft, um einen Clientknoten/Benutzer zu authentifizieren.

Beispiele

Angeben, dass IBM Spectrum Protect die Windows-Gruppe prüft, um Clientknoten zu authentifizieren.

```
securepipes yes
```

SERVERDEDUPTXNLIMIT

Die Option SERVERDEDUPTXNLIMIT gibt die maximale Größe von Objekten an, die auf dem Server dedupliziert werden können.

Wenn Sie Prozesse zum Identifizieren doppelter Daten (Befehl IDENTIFY DUPLICATES) für große Objekte verwenden, können lange laufende Transaktionen, die zur Aktualisierung der Datenbank erforderlich sind, eine umfangreiche Datenbankaktivität zur Folge haben. Eine umfangreiche Datenbankaktivität kann die folgenden Symptome zur Folge haben:

- Reduzierter Durchsatz bei Clientsicherungs- und -archivierungsoperationen
- Ressourcenkonflikt aufgrund gleichzeitig ablaufender Serveroperationen
- Exzessive Wiederherstellungsprotokollaktivität

Das Ausmaß, in dem diese Symptome auftreten, hängt von der Anzahl und Größe der Objekte ab, die verarbeitet werden, von der Intensität und dem Typ der gleichzeitig ablaufenden Operationen auf dem IBM Spectrum Protect-Server und von der IBM Spectrum Protect-Serverkonfiguration.

Mit der Serveroption SERVERDEDUPTXNLIMIT können Sie eine maximale Größe (in Gigabyte) für Objekte angeben, die auf dem Server dedupliziert werden können. Wenn ein Objekt oder eine Gruppe von Objekten in einer einzelnen Transaktion den mit SERVERDEDUPTXNLIMIT angegebenen Grenzwert überschreitet, werden die Objekte nicht vom Server dedupliziert. Sie können einen Wert von 32 bis 102400 GB angeben. Der Standardwert ist 5120 GB.

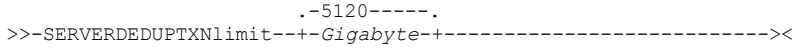
Wird der Wert dieser Option erhöht, sucht der IBM Spectrum Protect-Server nach zuvor zurückgehaltenen Objekten, deren Größe unter den neuen Transaktionsgrenzwert fällt.

Hinweis: Die Suche nach zuvor zurückgehaltenen Objekten kann einige Zeit in Anspruch nehmen. Gehen Sie mit Vorsicht vor, wenn Sie den Wert von SERVERDEDUPTXNLIMIT erhöhen. Wird der Wert dieser Option verringert, sucht IBM Spectrum Protect nicht nach zurückgehaltenen Objekten.

Der geeignete Wert für diese Option hängt von der IBM Spectrum Protect-Serverkonfiguration und der gleichzeitig stattfindenden Serveraktivität ab. Sie können einen hohen Wert für diese Option angeben, wenn Sie den Ressourcenkonflikt minimieren. Um den Ressourcenkonflikt zu minimieren, führen Sie Operationen, wie beispielsweise Sicherung, Archivierung, Identifizierung doppelter Daten und Wiederherstellung, zu unterschiedlichen Zeiten aus.

Um diese Serveroption zu aktualisieren, ohne den Server zu stoppen und erneut zu starten, verwenden Sie den Befehl SETOPT.

Syntax



Parameter

Gigabyte
: Gibt die maximale Größe (in Gigabyte) von Objekten an, die auf dem Server dedupliziert werden können. Sie können einen Wert von 32 bis 102400 angeben. Der Standardwert ist 5120.

Beispiele

Die serverseitige Deduplizierung für alle Objekte über 120 GB inaktivieren:

```
serverdeduptxnlimit 120
```

SHMPORT

AIX-BetriebssystemeLinux-BetriebssystemeDie Option SHMPORT gibt die TCP/IP-Anschlussadresse eines Servers bei Verwendung von gemeinsam benutztem Speicher an. Jede Übertragung mit gemeinsam benutztem Speicher beginnt mit einer TCP/IP-Verbindung.
Windows-BetriebssystemeDie Option SHMPORT gibt den Anschluss an, an dem der Server für Verbindungen mit gemeinsam genutztem Speicher empfangsbereit ist.

Syntax

```
>>-SHMPort--Anschlussnummer----------------------------------><
```

Parameter

Anschlussnummer
: Gibt die Anschlussnummer an. AIX-BetriebssystemeLinux-BetriebssystemeSie können einen Wert von 1024 bis 32767 angeben. Der Standardwert ist 1510. Windows-BetriebssystemeSie können einen Wert von 1 bis 32767 angeben. Der Standardwert ist 1.

Beispiele

AIX-BetriebssystemeLinux-Betriebssysteme

```
shmport  1580
```

Windows-Betriebssysteme

```
shmport  1
```

SHREDDING

Die Option SHREDDING gibt an, ob das Schreddern von gelöschten sensiblen Daten automatisch oder manuell ausgeführt wird. Das Schreddern gilt nur für Daten in Speicherpools, die explizit für die Unterstützung des Schredderns konfiguriert wurden.

Syntax

```
>>-SHREDding--+-AUTOmatic-+-----------------------------------><
              '-MANual----'
```

Parameter

AUTOmatic
: Gibt an, dass das Schreddern automatisch erfolgt, wenn sensible Daten gelöscht werden. Verwenden Sie diese Option, um sensible Daten so schnell wie möglich nach dem Löschen zu schreddern. Wird die Option SHREDDING nicht angegeben, ist dies das Standardverhalten. Tritt während des automatischen Schredderns ein E/A-Fehler auf, wird ein Fehler zurückgemeldet und das Schreddern des aktuellen Objekts wird angehalten. Kann der E/A-Fehler nicht korrigiert werden, müssen Sie möglicherweise das Schreddern manuell ausführen und das Schlüsselwort IOERROR verwenden.

MANual
: Gibt an, dass das Schreddern manuell erfolgt, und zwar nur dann, wenn der Befehl SHRED DATA aufgerufen wird. Mit dieser Option können Sie den Zeitpunkt für das Schreddern steuern und sicherstellen, dass das Schreddern nicht andere Serveraktivitäten stört.
Tipp: Wenn Sie das manuelle Schreddern angeben, führen Sie den Befehl SHRED DATA regelmäßig aus, aber mindestens so oft wie Sie andere routinemäßige Serververwaltungstasks ausführen (beispielsweise Verfallsverarbeitung, Wiederherstellung usw.). Damit können Leistungseinbußen bei bestimmten Serverprozessen (besonders bei der Umlagerung) verhindert werden. Die besten Ergebnisse werden erzielt, wenn Sie SHRED DATA nach jeder Operation ausführen (beispielsweise Verfallsverarbeitung und Umlagerung), bei der Dateien aus einem Schredderpool gelöscht werden.

Beispiele

Angeben, dass IBM Spectrum Protect automatisch Daten in einem Speicherpool schreddert, der für das Schreddern konfiguriert ist, nachdem diese Daten gelöscht wurden:

```
shredding automatic
```

SNMPHEARTBEATINTERVAL

Die Option SNMPHEARTBEATINTERVAL gibt das Intervall zwischen den Abfragen des IBM Spectrum Protect-Servers in Minuten an.

Syntax

```
                          .-5-------.
>>-SNMPHEARTBEATINTERVAL--+-Minuten-+--------------------------><
```

Parameter

Minuten
: Gibt das Intervall für das Überwachungssignal in Minuten an. Gültige Werte sind 0 bis 1440 (ein Tag). 5 Minuten sind der Standardwert.

Beispiele

```
snmpheartbeatinterval 20
```

SNMPMESSAGECATEGORY

Die Option SNMPMESSAGECATEGORY gibt die Abfangarten an, die verwendet werden, wenn Nachrichten des Servers über den SNMP-Subagenten (SNMP = Simple Network Management Protocol) an den SNMP-Manager weitergeleitet werden.

Syntax

```
>>-SNMPMESSAGECATEGORY--+-SEVERITY---+-------------------------><
                        '-INDIVIDUAL-'
```

Parameter

SEVERITY
: Gibt an, dass es vier Abfangarten gibt, und zwar abhängig von der Bewertungsstufe der Nachricht:

  1
  : Schwerwiegend

  2
  : Fehler

  3
  : Warnung

  4
  : Information

  Dies ist der Standardwert.

INDIVIDUAL
: Gibt an, dass für jede Nachricht eine separate Abfangart verwendet wird. Der numerische Teil der Nachrichten-ID gibt die Abfangart an.

Beispiele

```
snmpmessagecategory individual
```

SNMPSUBAGENT

Die Option SNMPSUBAGENT gibt die Parameter an, die erforderlich sind, damit der IBM Spectrum Protect-Subagent mit dem SNMP-Dämon (SNMP = Simple Network Management Protocol) kommunizieren kann. Diese Option betrifft nur das Konfigurieren des SNMP-Subagenten, damit dieser mit dem SNMP-Agenten kommunizieren kann; die Option wird vom Server ignoriert.

Syntax

```
>>-SNMPSUBAGENT--+--------------------+------------------------>
                 '-HOSTname--Hostname-'

>--+-------------------------------------+---------------------->
   '-COMMunityname -Benutzergemeinschaft-'

>--+-------------------+-----------------------------------------><
   '-TIMEOUT -Sekunden-'
```

Parameter

HOSTname Hostname

Gibt den TCP/IP-Namen oder die Nummer des Hosts an, der den SNMP-Agenten ausführt, zu dem der IBM Spectrum Protect SNMP-Subagent die Verbindung herstellt. Dieser Parameter ist wahlfrei. Der Standardname lautet *localhost*.

COMMunityname Benutzergemeinschaft
: Gibt den Namen der Benutzergemeinschaft auf dem System an, das den SNMP-Agenten ausführt. Dieser Parameter ist wahlfrei. Der Standardname lautet *public*.

TIMEOUT Sekunden
: Gibt die Zeitspanne an (in Sekunden), innerhalb der eine Anforderung empfangen werden muss. Dieser Parameter ist wahlfrei. Der Standardwert ist 600.

Beispiele

```
snmpsubagent hostname jimbo communityname public timeout 2600
```

SNMPSUBAGENTHOST

Die Option SNMPSUBAGENTHOST gibt den Standort des IBM Spectrum Protect SNMP-Subagenten (SNMP = Simple Network Management Protocol) an. Der Standardwert für diese Option lautet 127.0.0.1.

Syntax

```
>>-SNMPSUBAGENTHOST--Hostname----------------------------------><
```

Parameter

Hostname
: Gibt den TCP/IP-Namen oder die Nummer des Hosts an, auf dem sich der IBM Spectrum Protect SNMP-Subagent befindet. Subagent und Server müssen sich auf demselben Knoten befinden.

Beispiele

```
snmpsubagenthost 9.116.23.450
```

SNMPSUBAGENTPORT

Die Option SNMPSUBAGENTPORT gibt die Anschlussnummer des IBM Spectrum Protect SNMP-Subagenten (SNMP = Simple Network Management Protocol) an.

Syntax

```
>>-SNMPSUBAGENTPORT--Anschlussnummer--------------------------><
```

Parameter

Anschlussnummer
: Gibt die Anschlussnummer des IBM Spectrum Protect SNMP-Subagenten an. Gültige Werte sind 1000 - 32767. Der Standardwert ist 1521.

Beispiele

```
snmpsubagentport 1525
```

SSLFIPSMODE

Die Option SSLFIPSMODE gibt an, ob der FIPS-Modus (Federal Information Processing Standards) für Secure Sockets Layer (SSL) aktiv ist. Der Standardwert ist NO.

Da SSLv3 nicht vom FIPS-Modus unterstützt wird, wenn SSL mit Clients der Version 6.1 oder Version 5.5 verwendet wird, müssen Sie den FIPS-Modus inaktivieren.

Syntax

```
   .-SSLFIPSMODE--=--No------.
>>-+-------------------------+--------------------------------><
```

```
'-SSLFIPSMODE--=--+-No--+-'
                  '-Yes-'
```

Parameter

No
: Gibt an, dass der SSL FIPS-Modus auf dem Server nicht aktiv ist. Diese Einstellung ist erforderlich, wenn Clients für Sichern/Archivieren vor IBM Spectrum Protect Version 6.3 die Verbindung zum Server unter Verwendung von SSL herstellen sollen.

Yes
: Der Wert YES gibt an, dass der SSL FIPS-Modus auf dem Server aktiv ist. Diese Einstellung beschränkt die SSL-Sitzungsvereinbarung auf die Verwendung von FIPS-konformen Cipher-Suites. Die Angabe von YES wird empfohlen, wenn die SSL-Übertragung aktiviert ist und alle Clients für Sichern/Archivieren die Version 6.3 oder eine höhere Version haben.

Geben Sie Folgendes an, um den SSL FIPS-Modus auf dem Server zu inaktivieren:

```
SSLFIPSMODE no
```

SSLINITTIMEOUT

Die Option SSLINITTIMEOUT gibt die Zeit in Minuten an, die der Server darauf wartet, dass eine SSL-Sitzung (SSL = Secure Sockets Layer) die Initialisierung beendet, bevor der Server die Sitzung abbricht.

Wenn Sie diese Option angeben, wird eine SSL-Sitzung abgebrochen, wenn ein Client, ein Server oder ein Speicheragent nicht für SSL konfiguriert ist und versucht, eine SSL-Sitzung zu starten. Eine SSL-Sitzung wird auch abgebrochen, wenn eine Client-SSL-Sitzung und ein Server nicht mit derselben TLS-Version (TLS = Transport Layer Security) konfiguriert sind. In diesen Situationen kann die SSL-Sitzung möglicherweise nicht vollständig initialisiert werden. Der Server bricht die Sitzung ab, wenn das angegebene Zeitlimit erreicht wird.

Syntax

```
                  .-2-------.
>>-SSLINITTIMEout--+-Minuten-+--------------------------------><
```

Parameter

Minuten
: Gibt die maximale Anzahl Minuten an, die ein Server darauf wartet, dass eine SSL-Sitzung die Initialisierung beendet. Der Standardwert ist 2 Minuten. Der Mindestwert ist 1 Minute.

Beispiel

```
sslinittimeout 1
```

SSLTCPADMINPORT

Die Option SSLTCPADMINPORT gibt die Anschlussadresse an, an der der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen nur für SSL-aktivierte Sitzungen wartet. Die Sitzungen gelten für den Verwaltungsbefehlszeilenclient.

Anmerkung: Ab IBM Spectrum Protect Version 8.1.2 müssen Sie nicht mehr die Option SSLTCPPORT oder SSLTCPADMINPORT verwenden, um SSL-fähige Sitzungen vom Client zu ermöglichen. Die in der Option TCPPORT oder TCPADMINPORT angegebene Anschlussnummer ist sowohl für TCP/IP-Sitzungen als auch für SSL-fähige Clientsitzungen empfangsbereit.
Die folgenden Typen von Sitzungen verwenden nicht das Protokoll Secure Sockets Layer (SSL):

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLS)
- Datenbankzurückschreibungsoperationen

Ist die Option ADMINONCLIENTPORT auf NO gesetzt, erfordern SSL-fähige Sitzungen für den Verwaltungsclient unterschiedliche Anschlussnummern für die Optionen SSLTCPADMINPORT und SSLTCPPORT.

Der TCP/IP-Kommunikationstreiber muss mit COMMMETHOD TCPIP oder COMMMETHOD V6TCPIP aktiviert werden.

Syntax

```
>>-SSLTCPADMINPort--Anschlussnummer----------------------------><
```

Parameter

Anschlussnummer
Gibt die Anschlussnummer des Servers an. Gültige Werte sind 1024 - 32767. Es gibt keinen Standardwert.

Beispiele

```
ssltcpadminport 1543
```

SSLTCPPORT

Die Option SSLTCPPORT gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) nur für SSL-fähige Sitzungen an. Der TCP/IP-Kommunikationstreiber des Servers wartet an diesem Anschluss auf Anforderungen für SSL-aktivierte Sitzungen vom Client.

Wichtig: Ab IBM Spectrum Protect Version 8.1.2 müssen Sie nicht mehr die Option SSLTCPPORT oder SSLTCPADMINPORT verwenden, um SSL-fähige Sitzungen vom Client zu ermöglichen. Die in der Option TCPPORT oder TCPADMINPORT angegebene Anschlussnummer ist sowohl für TCP/IP-Sitzungen als auch für SSL-fähige Clientsitzungen empfangsbereit.
Die folgenden Typen von Sitzungen verwenden nicht SSL:

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLS)
- Datenbankzurückschreibungsoperationen

Ist die Option ADMINONCLIENTPORT auf NO gesetzt, erfordern SSL-fähige Sitzungen für den Verwaltungsclient unterschiedliche Anschlussnummern für die Optionen SSLTCPADMINPORT und SSLTCPPORT.

Wenn Sie dieselbe Anschlussnummer für die Optionen SSLTCPPORT und TCPPORT angeben, werden nur SSL-Verbindungen akzeptiert und TCP/IP-Verbindungen werden für den Anschluss inaktiviert.

Der TCP/IP-Kommunikationstreiber muss mit COMMMETHOD TCPIP oder COMMMETHOD V6TCPIP aktiviert werden.

Syntax

```
>>-SSLTCPPort--Anschlussnummer--------------------------------><
```

Parameter

Anschlussnummer
Gibt die Anschlussnummer des Servers an. Gültige Werte sind 1024 - 32767. Es gibt keinen Standardwert.

Beispiele

```
ssltcpport 1542
```

TCPADMINPORT

Die Option TCPADMINPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für andere TCP/IP-Sitzungen und SSL-fähige Sitzungen als Clientsitzungen wartet. Dazu gehören Verwaltungssitzungen, Sitzungen zwischen Servern, Speicheragentensitzungen, Speicherarchivclientsitzungen, Sitzungen verwalteter Server und Ereignisserversitzungen.

Durch die Verwendung verschiedener Anschlussnummern für die Optionen TCPPORT und TCPADMINPORT können Sie eine Gruppe mit Firewall-Regeln für Clientsitzungen und eine andere Gruppe für die zuvor aufgelisteten Sitzungstypen erstellen. Durch die Verwendung des Parameters SESSIONINITIATION im Befehl REGISTER NODE und UPDATE NODE können Sie den durch TCPPORT an der Firewall angegebenen Anschluss schließen und Knoten angeben, deren geplante Sitzungen vom Server gestartet werden. Sind die beiden Anschlussnummern verschieden, werden separate Threads für Clientsitzungen und die anderen Sitzungstypen verwendet. Sollen die beiden Optionen dieselbe Anschlussnummer verwenden (standardmäßig oder durch explizites Setzen der Optionen auf dieselbe Anschlussnummer), wird ein einzelner Serverthread für alle Sitzungsanforderungen verwendet.

Clientsitzungen, die versuchen, den durch TCPADMINPORT angegebenen Anschluss zu verwenden, werden beendet (wenn TCPPORT und TCPADMINPORT verschiedene Anschlüsse angeben). Verwaltungssitzungen sind an beiden Anschlüssen zulässig, (sofern nicht die Option ADMINONCLIENTPORT auf NO gesetzt ist), sie verwenden jedoch standardmäßig den durch TCPADMINPORT angegebenen Anschluss.

Für SSL-fähige Sitzungen, die die Option TCPADMINPORT verwenden, gelten dieselben Einschränkungen wie bei der Option SSLTCPADMINPORT. Die folgenden Typen von Sitzungen verwenden nicht das Protokoll Secure Sockets Layer (SSL):

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLS)

- Datenbankzurückschreibungsoperationen

Ist die Option ADMINONCLIENTPORT auf NO gesetzt, erfordern SSL-fähige Sitzungen für den Verwaltungsclient unterschiedliche Anschlussnummern für die Optionen TCPADMINPORT und TCPPORT.

Syntax

```
>>-TCPADMINPort--Anschlussnummer------------------------------><
```

Parameter

Anschlussnummer
Gibt die Anschlussnummer des Servers an. Gültige Werte sind 1024 - 32767. Der Standardwert ist der Wert von TCPPORT.

Beispiele

```
tcpadminport 1502
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

TCPBUFSIZE

Die Option TCPBUFSIZE gibt die Größe des Puffers an, der für TCP/IP-Sendeanforderungen verwendet wird. Während einer Zurückschreibung werden Clientdaten aus der IBM Spectrum Protect-Sitzungskomponente in einen TCP-DFV-Treiber versetzt. Die Option TCPBUFSIZE bestimmt, ob der Server die Daten direkt aus dem Sitzungspuffer sendet oder die Daten in den TCP-Puffer kopiert. Eine Puffergröße von 32 KB zwingt den Server dazu, Daten in den Kommunikationspuffer zu kopieren und den Inhalt des Puffers zu löschen, wenn er gefüllt ist.

Anmerkung: Diese Option ist nicht mit der Option TCPWINDOWSIZE verbunden.

Syntax

```
>>-TCPBufsize--Kilobyte----------------------------------------><
```

Parameter

Kilobyte
Gibt die Größe des Puffers, der für TCP/IP-Sendeanforderungen verwendet wird, in Kilobyte an.

 AIX-BetriebssystemeDer Wertebereich liegt zwischen 1 und 64. Der Standardwert ist 32.

 Linux-BetriebssystemeDer Wertebereich liegt zwischen 1 und 64. Der Standardwert ist 16.

Beispiele

```
tcpbufsize 5
```

TCPNODELAY

Die Option TCPNODELAY gibt an, ob der Server die Verzögerung beim Senden von aufeinanderfolgenden kleinen Paketen im Netz inaktiviert.

Ändern Sie den Standardwert YES nur unter einer der folgenden Bedingungen:

- Sie werden angewiesen, die Option durch Ihren Kundendienst ändern zu lassen.
- Sie kennen die Auswirkungen des TCP-Nagle-Algorithmus bei Übertragungen im Netz. Wird die Option auf NO gesetzt, wird der Nagle-Algorithmus aktiviert, der das Senden kleiner aufeinanderfolgender Pakete verzögert.

Syntax

```
>>-TCPNodelay--+-Yes-+-----------------------------------------><
               '-No--'
```

Parameter

Yes

Gibt an, dass der Server das sofortige Senden aufeinanderfolgender kleiner Pakete im Netz zulässt. Wird diese Option auf YES gesetzt, kann die Leistung in einigen Hochgeschwindigkeitsnetzen verbessert werden. Der Standardwert ist YES.

No
Gibt an, dass der Server das sofortige Senden aufeinanderfolgender kleiner Pakete im Netz nicht zulässt

Beispiele

```
tcpnodelay no
```

TCPPORT

Die Option TCPPORT gibt die Nummer des Anschlusses an, an dem der TCP/IP-Kommunikationstreiber des Servers auf Anforderungen für Clientsitzungen wartet. Der TCP/IP-Kommunikationstreiber des Servers ist an diesem Anschluss sowohl für TCP/IP-Sitzungen als auch für SSL-fähige Sitzungen vom Client empfangsbereit.

Durch die Verwendung verschiedener Anschlussnummern für die Optionen TCPPORT und TCPADMINPORT können Sie eine Gruppe mit Firewallregeln für Clientsitzungen und eine andere Gruppe für andere Sitzungstypen erstellen (Verwaltungssitzungen, Sitzungen zwischen Servern, Speicheragentensitzungen, Speicherarchivclientsitzungen, Sitzungen verwalteter Server und Ereignisserversitzungen). Sind die beiden Anschlussnummern verschieden, werden separate Threads für Clientsitzungen und die anderen Sitzungstypen verwendet. Sollen die beiden Optionen dieselbe Anschlussnummer verwenden (standardmäßig oder durch explizites Setzen der Optionen auf dieselbe Anschlussnummer), wird ein einzelner Serverthread für alle Sitzungsanforderungen verwendet.

Für SSL-fähige Clientsitzungen, die die Option TCPPORT verwenden, gelten dieselben Einschränkungen wie bei der Option SSLTCPPORT. Die folgenden Typen von Sitzungen verwenden nicht SSL:

- Network Data Management Protocol (NDMP)
- Automated Cartridge System Library Software (ACSLS)
- Datenbankzurückschreibungsoperationen

Ist die Option ADMINONCLIENTPORT auf NO gesetzt, erfordern SSL-fähige Sitzungen für den Verwaltungsclient unterschiedliche Anschlussnummern für die Optionen TCPADMINPORT und TCPPORT.
Wenn Sie dieselbe Anschlussnummer für die beiden Optionen SSLTCPPORT und TCPPORT angeben, werden nur SSL-Verbindungen akzeptiert und TCP/IP-Verbindungen werden für den Anschluss inaktiviert.

 Windows-BetriebssystemeSie können diese Option mit dem Befehl SETOPT ändern. Wenn Sie einen Anschluss ändern, ist der IBM Spectrum Protect-Server sofort an dem neuen Anschluss empfangsbereit. Alle aktuellen Verbindungen bleiben im Gebrauch, bis sie geschlossen werden.

Syntax

```
>>-TCPPort--Anschlussnummer----------------------------------><
```

Parameter

Anschlussnummer
Gibt die Anschlussnummer des Servers an. Gültige Werte sind 1024 - 32767. Der Standardwert ist 1500.

```
tcpport 1500
```

TCPWINDOWSIZE

Die Option TCPWINDOWSIZE gibt den Umfang (in Kilobyte) der Empfangsdaten an, die bei einer TCP/IP-Verbindung gleichzeitig gepuffert werden können. Der sendende Host kann erst dann weitere Daten senden, wenn er eine Bestätigung und eine Aktualisierung des TCP-Empfangsfensters empfängt. Jedes TCP-Paket enthält das entsprechende TCP-Empfangsfenster in der Verbindung. Bei einem größeren Fenster kann der Sender mit dem Senden von Daten fortfahren. Außerdem wird möglicherweise die Übertragungsleistung verbessert, besonders in schnellen Netzen mit hoher Latenzzeit.

Anmerkung:

- Um die Leistung beim Sichern zu verbessern, den Wert für TCPWINDOWSIZE auf dem Server vergrößern. Um die Leistung beim Zurückschreiben zu verbessern, den Wert für TCPWINDOWSIZE auf dem Client vergrößern.
- Das TCP-Fenster agiert als Puffer in dem Netz.
- Überschreitet die Fenstergröße den Pufferspeicherbereich auf dem Netzadapter, kann sich der Durchsatz aufgrund des erneuten Sendens von Paketen, die auf dem Adapter verlorengegangen sind, verschlechtern.
-  AIX-Betriebssysteme  Linux-BetriebssystemeDie Option TCPWINDOWSIZE ist nicht mit der Option TCPBUFFSIZE und nicht mit den Sende- und Empfangspuffern verbunden, die im Client- oder Serverspeicher zugeordnet sind.

Syntax

```
>>-TCPWindowsize--Kilobyte-------------------------------------><
```

Parameter

Kilobyte

Gibt die Größe, die für das TCP/IP-Schiebefenster für den Clientknoten verwendet werden soll, in Kilobyte an. Es kann ein Wert von 0 bis 2048 angegeben werden. Der Standardwert ist 63. Wird 0 angegeben, verwendet der Server die Standardfenstergröße, die durch das Betriebssystem definiert wird. Werte von 1 bis 2048 geben an, dass sich die Fenstergröße in dem Bereich 1 KB bis 2 MB befindet.

Beispiele

```
tcpwindowsize 63
```

TECBEGINEVENTLOGGING

Die Option TECBEGINEVENTLOGGING gibt an, ob die Ereignisprotokollierung für den TIVOLI-Empfänger beim Serverstart beginnen soll. Wird die Option TECHOST angegeben, wird für TECBEGINEVENTLOGGING standardmäßig der Wert YES angenommen.

Syntax

```
>>-TECBegineventlogging--+-Yes-+------------------------------><
                         '-No--'
```

Parameter

Yes
: Gibt an, dass die Ereignisprotokollierung beginnt, wenn der Server gestartet wird und die Option TECHOST angegeben ist.

No
: Gibt an, dass die Ereignisprotokollierung nicht beim Serverstart beginnen soll. Soll die Ereignisprotokollierung für den TIVOLI-Empfänger später beginnen (wenn die Option TECHOST angegeben wurde), muss der Befehl BEGIN EVENTLOGGING ausgegeben werden.

Beispiele

```
tecbegineventlogging yes
```

TECHOST

Die Option TECHOST gibt den Hostnamen oder die IP-Adresse für den Tivoli-Ereignisserver an.

Syntax

```
>>-TECHost--Hostname-----------------------------------------><
```

Parameter

Hostname
: Gibt den Hostnamen oder die IP-Adresse für den Tivoli-Ereignisserver an.

Beispiele

```
techost 9.114.22.345
```

TECPORT

Die Option TECPORT gibt die TCP/IP-Anschlussadresse an, an der der Tivoli-Ereignisserver empfangsbereit ist. Diese Option ist nur erforderlich, wenn sich der Tivoli-Ereignisserver auf einem System befindet, auf dem der Service 'Port Mapper' nicht ausgeführt wird.

Syntax

```
>>-TECPort--Anschlussnummer-----------------------------------><
```

Parameter

Anschlussnummer
: Gibt die Anschlussadresse des Tivoli-Ereignisservers an. Der Wert muss zwischen 0 und 32767 liegen. AIX-Betriebssysteme Linux-BetriebssystemeDiese Option ist nicht erforderlich.

Beispiele

```
tecport 1555
```

TECUTF8EVENT

Die Option TECUTF8EVENT ermöglicht es dem IBM Spectrum Protect-Administrator, Informationen im UTF–8-Datenformat an den Tivoli Enterprise Console (TEC)-Server zu senden. Der Standardwert ist 'No'. Mit dem Befehl QUERY OPTION können Sie abfragen, ob diese Option aktiviert ist.

Syntax

```
>>-TECUTF8event--+-Yes-+----------------------------------------><
                 '-No--'
```

Parameter

Yes
: Gibt an, dass der IBM Spectrum Protect-Server das TEC-Ereignis in UTF–8 verschlüsselt, bevor das Ereignis an den TEC-Server ausgegeben wird.

No
: Gibt an, dass der IBM Spectrum Protect-Server das TEC-Ereignis nicht in UTF–8 verschlüsselt. Das Ereignis wird im ASCII-Format an den TEC-Server ausgegeben.

Beispiele

```
tecutf8event yes
```

THROUGHPUTDATATHRESHOLD

Die Option THROUGHPUTDATATHRESHOLD gibt eine Durchsatzschwelle an, die eine Clientsitzung erreichen muss, damit sie nicht abgebrochen wird, wenn die Zeitschwelle erreicht wird.

Diese Option wird zusammen mit der Serveroption THROUGHPUTTIMETHRESHOLD verwendet, die den Wert für die Zeitschwelle plus die Zeit für das Warten auf Datenträger definiert. Die Zeitschwelle beginnt, wenn der Client beginnt, Daten zum Speichern an den Server zu senden (im Gegensatz zu Konfigurations- oder Sitzungsverwaltungsdaten).

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
>>-THROUGHPUTDatathreshold-- Kilobyte_pro_Sekunde--------------><
```

Parameter

Kilobyte pro Sekunde
: Gibt den Durchsatz an, den Clientsitzungen erreichen müssen, um ihren Abbruch zu vermeiden, wenn die mit THROUGHPUTTIMETHRESHOLD angegebenen Minuten verstrichen sind. Diese Schwelle enthält nicht die Zeit, die auf das Laden der Datenträger gewartet wird. Der Wert 0 gibt an, dass die Clientsitzungen nicht auf unzureichenden Durchsatz überprüft werden. Der Durchsatz wird berechnet, indem gesendete und empfangene Byte addiert und durch die Länge der Sitzung dividiert werden. Die Länge enthält nicht die Zeit, die auf das Laden der Datenträger gewartet wird, und beginnt mit dem Zeitpunkt, zu dem ein Client Daten zum Speichern an den Server sendet. Der Standardwert ist 0. Der Mindestwert ist 0; der Maximalwert ist 99999999.

Beispiele

Angeben, dass der Server 90 Minuten plus Datenträgerwartezeit warten soll, nachdem eine Sitzung mit dem Senden von Daten begonnen hat, bis überprüft wird, ob die Sitzung aufgrund zu geringen Durchsatzes abgebrochen werden soll. Erreicht eine Sitzung keine Übertragungsrate von 50 KB pro Sekunde, wird sie abgebrochen.

```
throughputtimethreshold 90
Throughputdatathreshold 50
```

THROUGHPUTTIMETHRESHOLD

Die Option THROUGHPUTTIMETHRESHOLD gibt die Zeitschwelle für eine Sitzung an, nach deren Ablauf die Sitzung aufgrund zu geringen Durchsatzes abgebrochen werden kann.

Sie können diese Serveroption mit dem Befehl SETOPT aktualisieren, ohne den Server zu stoppen und erneut zu starten. Siehe SETOPT (Serveroption für dynamisches Aktualisieren definieren).

Syntax

```
>>-THROUGHPUTTimethreshold--Minuten---------------------------><
```

Parameter

Minuten
: Gibt die Schwelle für das Überprüfen von Clientsitzungen und deren Abbruch an, wenn die Datendurchsatzschwelle nicht erreicht wird (siehe Serveroption THROUGHPUTDATATHRESHOLD). Diese Schwelle enthält nicht die Zeit, die auf das Laden der Datenträger gewartet wird. Die Zeitschwelle beginnt, wenn ein Client beginnt, Daten zum Speichern an den Server zu senden (im Gegensatz zu Konfigurations- oder Sitzungsverwaltungsdaten). Der Wert 0 gibt an, dass die Clientsitzungen nicht auf zu geringen Durchsatz überprüft werden. Der Standardwert ist 0. Der Mindestwert ist 0; der maximale Wert ist 99999999.

Beispiele

Angeben, dass der Server 90 Minuten plus Datenträgerwartezeit warten soll, nachdem eine Sitzung mit dem Senden von Daten begonnen hat, bis überprüft wird, ob die Sitzung abgebrochen werden soll. Erreicht eine Sitzung keine Übertragungsrate von 50000 Byte pro Sekunde, wird sie abgebrochen.

```
throughputtimethreshold 90
Throughputdatathreshold 50
```

Windows-Betriebssysteme

TIMEFORMAT

Die Option TIMEFORMAT gibt das Format an, in dem Uhrzeitangaben vom Server angezeigt werden.

Der Wert für die Option TIMEFORMAT wird von dem in den länderspezifischen Angaben definierten Uhrzeitformat überschrieben, wenn die länderspezifischen Angaben beim Starten des Servers erfolgreich initialisiert wurden. Die länderspezifischen Angaben werden in der Option LANGUAGE angegeben.

Syntax

```
>>-TIMEformat--Formatnummer----------------------------------><
```

Parameter

Formatnummer
: Eine Zahl von 1 bis 4 auswählen, um das vom Server verwendete Uhrzeitformat anzugeben. Der Standardwert ist 1.

1
: hh:mm:ss

2
: hh,mm,ss

3
: hh.mm.ss

4
: hh:mm:ss a.m oder p.m.

5
: a.m oder p.m. hh:mm:ss

Beispiele

```
timeformat 4
```

TXNGROUPMAX

Die Option TXNGROUPMAX gibt die Anzahl der Objekte an, die als Gruppe zwischen einem Client und dem Server zwischen Transaktions-COMMIT-Punkten übertragen werden. Der Mindestwert beträgt 4 Objekte und der Maximalwert beträgt 65000 Objekte. Der Standardwert ist 4096 Objekte. Bei den übertragenen Objekten handelt es sich um tatsächliche Dateien, Verzeichnisse oder beides. Der Server zählt jede Datei oder jedes Verzeichnis als ein Objekt.

Es ist möglich, die Leistung bei Clientsicherungsoperationen, Archivierungsoperationen, Zurückschreibungsoperationen und Abrufoperationen durch die Verwendung eines höheren Werts für diese Option zu beeinflussen:

1. Wird der Wert für die Option TXNGROUPMAX erheblich vergrößert, achten Sie auf mögliche Auswirkungen auf das Wiederherstellungsprotokoll. Ein größerer Wert für die Option TXNGROUPMAX kann zu einer erhöhten Auslastung des Wiederherstellungsprotokolls sowie zu einer längeren Zeit bis zu einer Transaktionsfestschreibung führen. Bei besonders schweren Auswirkungen können Probleme beim Betrieb des Servers auftreten.
2. Die Erhöhung des Wertes der Option TXNGROUPMAX kann den Durchsatz für Operationen verbessern, die Daten direkt auf Band speichern. Dies gilt besonders, wenn eine große Anzahl Objekte gespeichert wird. Ein höherer Wert der Option TXNGROUPMAX kann jedoch auch die Anzahl der Objekte erhöhen, die erneut gesendet werden müssen, wenn die Transaktion gestoppt wird, weil eine Eingabedatei während der Sicherung geändert wurde oder weil ein neuer Speicherdatenträger erforderlich war. Je größer der Wert der Option TXNGROUPMAX ist, desto mehr Daten müssen erneut gesendet werden.
3. Die Erhöhung des Werts für TXNGROUPMAX hat Auswirkungen auf die Flexibilität beim Stoppen der Operation, und der Client muss möglicherweise länger warten, bis die Transaktion abgeschlossen ist.

Sie können den Wert dieser Option für einzelne Clientknoten überschreiben. Siehe Parameter TXNGROUPMAX in REGISTER NODE (Knoten registrieren) und UPDATE NODE (Attribute eines Knotens aktualisieren).

Diese Option steht im Zusammenhang mit der Option TXNBYTELIMIT in der Clientoptionsdatei. TXNBYTELIMIT steuert die Anzahl Byte (im Gegensatz zur Anzahl Objekte), die zwischen Transaktions-COMMIT-Punkten übertragen werden. Bei Beendigung der Übertragung eines Objekts schreibt der Client die Transaktion fest, wenn die Anzahl der während der Transaktion übertragenen Byte den Wert von TXNBYTELIMIT erreicht oder überschreitet, unabhängig von der Anzahl der übertragenen Objekte.

Syntax

```
>>-TXNGroupmax--Anzahl_der_Objekte----------------------------><
```

Parameter

Anzahl_der_Objekte
: Gibt eine Zahl von 4 bis 65000 für die maximale Anzahl Objekte pro Transaktion an. Der Standardwert ist 4096.

Beispiele

```
txngroupmax 4096
```

UNIQUETDPTECEVENTS

Die Option UNIQUETDPTECEVENTS generiert eine eindeutige Tivoli Enterprise Console (TEC)-Ereignisklasse für jede einzelne IBM Spectrum Protect-Nachricht, einschließlich Client-, Server- und IBM Spectrum Protect Data Protection-Clientnachrichten. Der Standardwert ist 'No'.

Syntax

```
>>-UNIQUETDPtecevents--+-Yes-+---------------------------------><
                       '-No--'
```

Parameter

Yes
: Gibt an, dass eindeutige IBM Spectrum Protect Data Protection-Nachrichten an den TEC-Ereignisserver gesendet werden. UNIQUETECevents wird dynamisch auf YES gesetzt.

No
: Gibt an, dass allgemeine Nachrichten an den TEC-Ereignisserver gesendet werden.

Beispiele

```
uniquetdptecevents yes
```

UNIQUETECEVENTS

Die Option UNIQUETECEVENTS generiert eine eindeutige Tivoli Enterprise Console (TEC)-Ereignisklasse für jede einzelne IBM Spectrum Protect-Nachricht. Der Standardwert ist 'No'.

Syntax

```
>>-UNIQUETECevents--+-Yes-+-----------------------------------><
                    '-No--'
```

Parameter

Yes
: Gibt an, dass eindeutige Nachrichten an den TEC-Ereignisserver gesendet werden.

No
: Gibt an, dass allgemeine Nachrichten an den TEC-Ereignisserver gesendet werden.

Beispiele

```
uniquetecevents yes
```

USEREXIT

Die Option USEREXIT gibt einen benutzerdefinierten Ausgang an, dem die Steuerung für die Verwaltung eines Ereignisses übergeben wird.

Syntax

```
                                  (1)           (2)
>>-USEREXIT--+-Yes-+--Modulname------DLL-Name-------------------->
             '-No--'

             (3)
>--Funktion-----------------------------------------------------><
```

Anmerkungen:

1. *Modulname* ist nur unter AIX, HP-UX, Linux, Solaris und z/OS verfügbar.
2. *DLL-Name* ist nur unter Windows verfügbar.
3. *Funktion* ist nur unter Windows verfügbar.

Parameter

Yes
: Gibt an, dass das Ereignisprotokoll für den Benutzerausgangsempfänger automatisch beim Serverstart gestartet wird.

No
: Gibt an, dass das Ereignisprotokoll für den Benutzerausgangsempfänger nicht automatisch beim Serverstart gestartet wird. Wurde dieser Parameter angegeben, muss das Ereignisprotokoll manuell durch Eingabe des Befehls BEGIN EVENTLOGGING gestartet werden.

AIX-BetriebssystemeLinux-BetriebssystemeModulname
: AIX-BetriebssystemeLinux-BetriebssystemeGibt den Modulnamen des Benutzerausgangs an.

  AIX-BetriebssystemeLinux-BetriebssystemeDies ist der Name einer gemeinsam benutzten Bibliothek, die den Ausgang enthält. Der Modulname kann entweder ein vollständig qualifizierter Pfadname oder nur der Modulname selbst sein. Handelt es sich nur um den Modulnamen, wird er aus dem aktuellen Verzeichnis geladen.

Windows-BetriebssystemeDLL-Name
: Windows-BetriebssystemeGibt den DLL-Namen an, der die Benutzerausgangsfunktion enthält.

Windows-BetriebssystemeFunktion
: Windows-BetriebssystemeGibt den Namen der Benutzerausgangsfunktion in der DLL an.

Beispiele

Windows-Betriebssysteme

```
userexit yes dllname.dll dllmodulename
```

AIX-BetriebssystemeLinux-Betriebssysteme

```
userexit yes fevent.exit
```

VERBCHECK

Die Option VERBCHECK gibt an, dass der Server eine zusätzliche Fehlerprüfung für die Struktur der Befehle durchführt, die vom Client gesendet werden. Diese Option sollte nur aktiviert werden, wenn der Client nicht ordnungsgemäß gebildete Anforderungen an den Server sendet, die zum Absturz des Servers führen. Ist diese Option aktiviert, hat dies einen Protokollfehler an Stelle eines Serverabsturzes zur Folge.

Syntax

```
>>-VERBCHECK---------------------------------------------------><
```

Parameter

Keine.

Beispiele

Zusätzliche Fehlerprüfung für Befehle aktivieren, die vom Client gesendet werden:

```
verbcheck
```

VOLUMEHISTORY

Die Option VOLUMEHISTORY gibt den Namen von Dateien an, die automatisch aktualisiert werden sollen, wenn History-Informationen von sequenziellen Datenträgern des Servers sich ändern. Für diese Option gibt es keinen Standardwert.

Es können eine oder mehrere Optionen VOLUMEHISTORY in die Serveroptionsdatei eingeschlossen werden. Wird mit mehreren VOLUMEHISTORY-Optionen gearbeitet, aktualisiert der Server automatisch die Datenträger-History-Informationen in jeder angegebenen Datei und speichert eine Sicherungskopie.

Syntax

```
>>-VOLUMEHistory--Dateiname-----------------------------------><
```

Parameter

Dateiname
: Gibt den Namen der Datei an, in der der Server eine Sicherungskopie der gesammelten Datenträger-History-Informationen speichern soll.

Beispiele

```
volumehistory volhist.out
```

Serverdienstprogramme

Verwenden Sie Serverdienstprogramme, um spezielle Tasks auf dem Server auszuführen, während der Server nicht aktiv ist.

- Windows-BetriebssystemeDSMMAXSG (Blockgröße für das Schreiben von Daten erhöhen)
  Verwenden Sie das Dienstprogramm DSMMAXSG, um die maximale Übertragungslänge für Host Bus Adapter (HBAs) zu erhöhen. Damit wird die Blockgröße erhöht, die vom IBM Spectrum Protect-Server zum Schreiben von Daten auf bestimmte Typen von Bandlaufwerken und zum Abrufen von Daten von bestimmten Typen von Bandlaufwerken verwendet wird.
- DSMSERV (Server starten)
  Verwenden Sie dieses Dienstprogramm, um den IBM Spectrum Protect-Server zu starten.
- AIX-BetriebssystemeLinux-BetriebssystemeServerstartscript: rc.dsmserv
  Sie können das Script rc.dsmserv in Ihrem Systemstart verwenden, um eine Serverinstanz unter einer bestimmten Benutzer-ID automatisch zu starten.
- Linux-BetriebssystemeServerstartscript: dsmserv.rc
  Sie können das Script dsmserv.rc verwenden, um eine Serverinstanz zu stoppen oder einen Server manuell oder automatisch zu starten.

- DSMSERV DISPLAY DBSPACE (Informationen zum Datenbankspeicherbereich anzeigen)
  Verwenden Sie dieses Dienstprogramm, um Informationen zum Speicherbereich anzuzeigen, der für die Datenbank definiert ist. Die Ausgabe dieses Dienstprogramms entspricht der Ausgabe von QUERY DBSPACE, aber Sie können dieses Dienstprogramm verwenden, wenn der Server nicht aktiv ist.
- DSMSERV DISPLAY LOG (Informationen zum Wiederherstellungsprotokoll anzeigen)
  Mit diesem Dienstprogramm können Sie Informationen zu Wiederherstellungsprotokollen anzeigen, einschließlich der aktiven Protokolldatei, dem Spiegel für die aktive Protokolldatei, dem Übernahmeverzeichnis für das Archivprotokoll und dem Überlaufstandort für die Protokolle. Verwenden Sie dieses Dienstprogramm, wenn der Server nicht aktiv ist.
- DSMSERV EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)
  Verwenden Sie dieses Dienstprogramm, um den Speicherbereich für die Datenbank zu vergrößern, indem Verzeichnisse für die Datenbank hinzugefügt werden. Dieses Dienstprogramm führt dieselbe Funktion wie der Befehl EXTEND DBSPACE aus, aber Sie können es verwenden, wenn der Server nicht aktiv ist.
- DSMSERV FORMAT (Datenbank und Protokoll formatieren)
  Verwenden Sie das Dienstprogramm DSMSERV FORMAT, um die Serverdatenbank und das Wiederherstellungsprotokoll zu initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls sind keine anderen Serveraktivitäten zulässig.
- DSMSERV INSERTDB (Serverdatenbank in eine leere Datenbank versetzen)
  Verwenden Sie das Dienstprogramm DSMSERV INSERTDB, um eine Serverdatenbank in eine neue Datenbank zu versetzen. Die Datenbank kann vom ursprünglichen Server extrahiert und in eine neue Datenbank auf dem neuen Server eingefügt werden, indem eine Netzverbindung zwischen den beiden Servern verwendet wird. Die Datenbank kann auch von Datenträgern eingefügt werden, die die extrahierte Datenbank enthalten.
- DSMSERV LOADFORMAT (Datenbank formatieren)
  Verwenden Sie das Dienstprogramm DSMSERV LOADFORMAT, wenn ein Upgrade von Version 5 durchgeführt wird. Das Dienstprogramm formatiert eine leere Datenbank als Vorbereitung zum Einfügen einer extrahierten Datenbank in die leere Datenbank.
- DSMSERV REMOVEDB (Datenbank entfernen)
  Verwenden Sie das Dienstprogramm DSMSERV REMOVEDB, um eine IBM Spectrum Protect-Serverdatenbank zu entfernen.
- DSMSERV RESTORE DB (Datenbank zurückschreiben)
  Mit diesem Dienstprogramm können Sie eine Datenbank mit Hilfe einer Datenbanksicherung zurückschreiben.
-  DSMSERV UPDATE (Registry-Einträge für eine Serverinstanz erstellen)
  Verwenden Sie dieses Dienstprogramm, um Registry-Einträge für eine IBM Spectrum Protect-Serverinstanz zu erstellen, wenn die Einträge versehentlich gelöscht wurden.
-  DSMULOG (IBM Spectrum Protect-Servernachrichten in einer Benutzerprotokolldatei speichern)
  Verwenden Sie diesen Befehl, um Nachrichten der IBM Spectrum Protect-Server-Konsole in einer Benutzerprotokolldatei zu speichern. Sie können angeben, dass IBM Spectrum Protect Nachrichten in mehrere Benutzerprotokolldateien schreiben soll.

DSMMAXSG (Blockgröße für das Schreiben von Daten erhöhen)

Verwenden Sie das Dienstprogramm DSMMAXSG, um die maximale Übertragungslänge für Host Bus Adapter (HBAs) zu erhöhen. Damit wird die Blockgröße erhöht, die vom IBM Spectrum Protect-Server zum Schreiben von Daten auf bestimmte Typen von Bandlaufwerken und zum Abrufen von Daten von bestimmten Typen von Bandlaufwerken verwendet wird.

Mit diesem Dienstprogramm beträgt die maximale Blockgröße, die angegeben werden kann, 256 KB. Abhängig von Ihrer Systemumgebung kann mit der Erhöhung der Blockgröße die Geschwindigkeit verbessert werden, mit der IBM Spectrum Protect Daten für Sicherungs- und Zurückschreibungsoperationen sowie für Archivierungs- und Abrufoperationen verarbeitet. Das Dienstprogramm hat jedoch keine Auswirkungen auf die Generierung von Sicherungsgruppen.

Sie können Bandlaufwerke verwenden, die nur an SCSI- oder Fibre-Channel-HBAs angeschlossen sind und die folgenden Einheitentypen haben:

- 3590
- 3592
- DLT
- ECARTRIDGE
- LTO

Das Dienstprogramm wird im Rahmen der Installation des IBM Spectrum Protect-Servers und des Speicheragenten automatisch ausgeführt. Wenn Sie jedoch nach der Installation eines Servers oder eines Speicheragenten einen neuen HBA auf Ihrem System installieren oder wenn Sie eine neue Version eines vorhandenen HBA-Einheitentreibers installieren, mit der der Wert der maximalen Übertragungsgröße zurückgesetzt wird, müssen Sie das Dienstprogramm manuell ausführen, um die Vorteile der größeren Blockgröße zu nutzen.

Wird dieses Dienstprogramm ausgeführt, wird ein Registrierungsschlüssel für jeden HBA-Treiber auf dem System geändert. Der Name des Schlüssels ist MaximumSGList.

Einschränkung: Werden Daten unter Verwendung der Blockgröße von 256 KB auf Band gesichert oder archiviert, kann das Band nicht unter Verwendung eines HBAs angehängt oder gelesen werden, der die Blockgröße von 256 KB nicht unterstützt. Verwenden Sie beispielsweise ein 256-KB-Windows-System zum Sichern von Clientdaten auf dem IBM Spectrum Protect-Server, können Sie die Daten nicht mit einem Windows-System zurückschreiben, das eine andere Übertragungslänge unterstützt. Soll das Band angehängt oder von dem Band gelesen werden, das unter Verwendung einer Übertragungslänge von 256 KB beschrieben wurde, müssen Sie einen HBA installieren, der 256-KB-Übertragungen unterstützt.

Syntax

```
>>-dsmmaxsg---------------------------------------------------><
```

Beispiel: Die Blockgröße zum Schreiben von Daten erhöhen

Das Dienstprogramm DSMMAXSG ausführen, um die Blockgröße zu erhöhen, die von IBM Spectrum Protect verwendet wird.

```
dsmmaxsg
```

DSMSERV (Server starten)

Verwenden Sie dieses Dienstprogramm, um den IBM Spectrum Protect-Server zu starten.

Einschränkungen:

- Geben Sie maximal 1022 Zeichen in der DSMSERV-Konsolenbefehlszeilenschnittstelle ein. Text, der 1022 Zeichen überschreitet, wird abgeschnitten.
- Windows-BetriebssystemeDie folgenden Parameter schließen sich gegenseitig aus:
  - NOEXPIRE
  - RUNFILE
  - MAINTENANCE

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Syntax

```
>>-DSMSERV--+-------------------------+------------------------>
            |  (1)                    |
            '------- -u--Benutzername-'

>--+-------------------------------+---------------------------->
   |  (1)                          |
   '------- -i--Instanzverzeichnis-'

    (2).- -k--Server1-------.
>------+--------------------+--+------------------+------------->
       '- -k--Schlüsselname-'  |  (1)             |
                               '------- -noexpire-'

>--+----------------+--+-------------------+--------------------->
   |  (3)           |  '- -o--Optionsdatei-'
   '-------NOEXPIRE-'

>--+---------------+--+--------------------+------------------><
   |  (1)          |  +-RUNFILE--Dateiname-+
   '------- -quiet-'  |             (4)    |
                      '-MAINTenance--------'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.
3. Dieser Parameter gilt nur für Windows-Server.
4. Dieser Parameter gilt nur für AIX-, Linux- und Windows-Server.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme-u Benutzername
AIX-BetriebssystemeLinux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server gestartet wird. Um den Server mit der Rootbenutzer-ID zu starten, müssen Sie den Parameter -u angeben und die Anweisungen in Server mit der Rootbenutzer-ID starten befolgen.
AIX-BetriebssystemeLinux-Betriebssysteme -i Instanzverzeichnis
AIX-BetriebssystemeLinux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Das Instanzverzeichnis wird das aktuelle Arbeitsverzeichnis des Servers.
Windows-Betriebssysteme-k Schlüsselname

Windows-BetriebssystemeGibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Der Standardwert ist Server1.

AIX-BetriebssystemeLinux-Betriebssysteme-noexpire

AIX-BetriebssystemeLinux-BetriebssystemeGibt an, dass der Server keine verfallenen Dateien aus der Serverdatenbank entfernt. Die Dateien werden beim Start des Servers nicht aus dem Serverspeicher gelöscht.

Windows-BetriebssystemeNOEXPIRE

Windows-BetriebssystemeGibt an, dass der Server keine verfallenen Dateien aus der Serverdatenbank entfernt. Die Dateien werden beim Start des Servers nicht aus dem Serverspeicher gelöscht.

-o Optionsdatei

Gibt eine Optionsdatei an, die verwendet werden soll.

AIX-BetriebssystemeLinux-Betriebssysteme-quiet

AIX-BetriebssystemeLinux-BetriebssystemeGibt an, dass Nachrichten an die Konsole unterdrückt werden.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeMAINTenance

AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeGibt an, dass der Server im Verwaltungsmodus gestartet wird und Zeitpläne für Verwaltungsbefehle, Clientzeitpläne, Clientsitzungen, Wiederherstellung des Speicherbereichs, Bestandsverfall und Speicherpoolumlagerung inaktiviert sind.

Tipp: Der Verwaltungsmodus ist die bevorzugte Methode für die Ausführung des Servers während der Ausführung von Verwaltungs- oder Rekonfigurationstasks. Wenn der Server im Verwaltungsmodus ausgeführt wird, werden Operationen, die Verwaltungs- oder Rekonfigurationstasks unterbrechen könnten, automatisch inaktiviert.

RUNFILEDateiname

Gibt den Namen einer Textdatei an, die auf dem Server ausgeführt werden soll. Die Datei enthält eine Liste mit Serverbefehlen.

Achtung: Wenn der Parameter RUNFILE verwendet wird, hält der Server an, nachdem die Verarbeitung abgeschlossen wurde. Sie müssen den Server mit dem Dienstprogramm DSMSERV erneut starten.

Beispiel: Den Server starten

Starten Sie den Server für den normalen Betrieb. Geben Sie den folgenden Befehl in einer einzigen Zeile aus:

AIX-Betriebssysteme

```
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K
usr/bin/dsmserv
```

AIX-BetriebssystemeStellen Sie sicher, dass Sie hinter `SHMPSIZE=64K` ein Leerzeichen einfügen. Wenn Sie den Server mit diesem Befehl starten, werden 64-KB-Speicherseiten für den Server aktiviert. Mithilfe dieser Einstellung kann die Serverleistung optimiert werden.

Linux-Betriebssysteme

```
/opt/tivoli/tsm/server/bin/dsmserv
```

Windows-Betriebssysteme

```
C:\Programme\Tivoli\TSM\bin\dsmserv -k server2
```

Windows-Betriebssysteme

Beispiel: Einen zusätzlichen Server starten

Einen zusätzlichen Server unter Verwendung des Registrierungsschlüssels SERVER2 starten.

```
dsmserv -k server2
```

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Beispiel: Das Beispielscript laden

Die Beispielscriptdatei laden, die mit dem Server zur Verfügung gestellt wird.

```
dsmserv runfile scripts.smp
```

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Beispiel: Den Server im Verwaltungsmodus starten

Starten Sie den Server im Verwaltungsmodus, bevor Sie Verwaltungs- oder Rekonfigurationstasks ausführen.

```
dsmserv maintenance
```

Zugehörige Tasks:
Server im Verwaltungsmodus starten
AIX-Betriebssysteme

Serverstartscript: rc.dsmserv

Sie können das Script rc.dsmserv in Ihrem Systemstart verwenden, um eine Serverinstanz unter einer bestimmten Benutzer-ID automatisch zu starten.

Syntax

```
>>-rc.dsmserv--+- -u--Benutzername-+--------------------------->
               '- -U--Benutzername-'

>--+-------------------------+--------------------------------><
   '- -i--Instanzverzeichnis-'
```

Parameter

-u Benutzername
: Gibt die Instanzbenutzer-ID an, für die die Umgebung konfiguriert ist. Der Server wird unter dieser Benutzer-ID ausgeführt.

-U Benutzername
: Gibt die Instanzbenutzer-ID an, für die die Umgebung konfiguriert ist. Der Server wird unter der Benutzer-ID des Aufrufers des Befehls ausgeführt.

-i Instanzverzeichnis
: Gibt ein Instanzverzeichnis an, das das Arbeitsverzeichnis des Servers wird.

Zugehörige Tasks:
AIX: Server automatisch starten
Linux-Betriebssysteme

Serverstartscript: dsmserv.rc

Sie können das Script dsmserv.rc verwenden, um eine Serverinstanz zu stoppen oder einen Server manuell oder automatisch zu starten.

Voraussetzungen

Bevor Sie den Befehl DSMSERV.RC ausgeben, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Serverinstanz unter einer Benutzer-ID ohne Rootberechtigung mit dem Namen des Instanzeigners ausgeführt wird.
2. Kopieren Sie das Script dsmserv.rc in das Verzeichnis /etc/rc.d/init.d. Das Script dsmserv.rc befindet sich im Serverinstallationsverzeichnis, z. B. /opt/tivoli/tsm/server/bin.
3. Benennen Sie das Script um, sodass es mit dem Namen des Serverinstanzeigners übereinstimmt, z. B. `tsminst1`.
4. Wenn das Serverinstanzverzeichnis nicht Ausgangsverzeichnis/tsminst1 ist, suchen Sie in der Kopie des Scripts nach der folgenden Zeile:

   ```
   instance_dir="${Instanzausgangsverzeichnis}/tsminst1"
   ```

   Ändern Sie die Zeile so, dass sie auf Ihr Serverinstanzverzeichnis verweist, beispielsweise:

   ```
   instance_dir="/tsminst1"
   ```

5. Suchen Sie in der Kopie des Scripts nach der folgenden Zeile:

   ```
   # pidfile: /var/run/dsmserv_Instanzname.pid
   ```

   Ändern Sie den Wert für den Instanznamen in den Namen des Serverinstanzeigners. Hat beispielsweise der Serverinstanzeigner den Namen tsminst1, aktualisieren Sie die Zeile wie folgt:

   ```
   # pidfile: /var/run/dsmserv_tsminst1.pid
   ```

6. Verwenden Sie Tools, wie z. B. das Dienstprogramm CHKCONFIG, um die Ausführungsebene zu konfigurieren, auf der der Server automatisch gestartet wird. Geben Sie einen Wert an, der einem Mehrbenutzermodus mit aktiviertem Netzbetrieb entspricht. Normalerweise ist die zu verwendende Ausführungsebene 3 oder 5, abhängig vom Betriebssystem und seiner Konfiguration. Ausführliche Informationen zu Ausführungsebenen finden Sie in der Dokumentation für Ihr Betriebssystem.

Syntax

```
>>-dsmserv.rc--+---------+------------------------------------><
               +-start---+
               +-stop----+
               +-status--+
```

```
                '-restart-'
```

Parameter

start
: Startet den Server.

stop
: Stoppt den Server.

status
: Zeigt den Status des Servers an. Lautet der Status `started` (gestartet), wird auch die Prozess-ID des Serverprozesses angezeigt.

restart
: Stoppt den Server und startet ihn erneut.

Zugehörige Tasks:
Linux: Server auf Linux-Systemen automatisch starten

DSMSERV DISPLAY DBSPACE (Informationen zum Datenbankspeicherbereich anzeigen)

Verwenden Sie dieses Dienstprogramm, um Informationen zum Speicherbereich anzuzeigen, der für die Datenbank definiert ist. Die Ausgabe dieses Dienstprogramms entspricht der Ausgabe von QUERY DBSPACE, aber Sie können dieses Dienstprogramm verwenden, wenn der Server nicht aktiv ist.

Syntax

```
>>-DSMSERV--+-------------------------+------------------------->
            |  (1)                    |
            '------- -u--Benutzername-'

>--+-------------------------------+---------------------------->
   |  (1)                          |
   '------- -i--Instanzverzeichnis-'

    (2).- -k--Server1-------.
>------+---------------------+--+-------------------+------------>
       '- -k--Schlüsselname-'  '- -o--Optionsdatei-'

>--+------------+--+---------+--DISPlay DBSPace----------------><
   '- -noexpire-'  '- -quiet-'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme-u Benutzername
: AIX-BetriebssystemeLinux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.

AIX-BetriebssystemeLinux-Betriebssysteme -i Instanzverzeichnis
: AIX-BetriebssystemeLinux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.

Windows-Betriebssysteme-kSchlüsselname
: Windows-BetriebssystemeGibt den Namen eines Windows-Registrierungsschlüssels an, der zum Speichern von Informationen zu diesem Server verwendet wird. Verwenden Sie diesen Parameter nur, wenn sich mehrere Server in demselben System befinden. Der Standardwert ist SERVER1.

-o Optionsdatei
: Gibt eine Optionsdatei an, die verwendet werden soll.

-noexpire
: Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist.

-quiet
: Gibt an, dass Nachrichten an die Konsole unterdrückt werden.

Beispiel: Informationen zum Datenbankbereich anzeigen

Informationen zum Datenbankspeicherbereich anzeigen. Details zu den Informationen, die in der Ausgabe angezeigt werden, befinden sich in Feldbeschreibungen. Den folgenden Befehl ausgeben.

```
dsmserv display dbspace
```

AIX-BetriebssystemeLinux-Betriebssysteme

```
Position               Gesamtspeicher-    Verwendeter Sp.-  Freier Sp.-
                       bereich (MB)       Bereich (MB)      Bereich (MB)
-------------   ----------------   ---------------   ---------------
 /tsmdb001                    46.080,00         20.993,12         25.086,88
 /tsmdb002                    46.080,00         20.992,15         25.087,85
```

 Windows-Betriebssysteme

```
Position               Gesamtspeicher-    Verwendeter Sp.-  Freier Sp.-
                       bereich (MB)       Bereich (MB)      Bereich (MB)
-------------   ----------------   ---------------   ---------------
d:\tsm\db001                 46.080,00         20.993,12         25.086,88
d:\tsm\db002                 46.080,00         20.993,15         25.087,85
```

Feldbeschreibungen

Standort
: Das Verzeichnis oder der Pfad zum Speichern der Datenbank.

Gesamtspeicherbereich (MB)
: Die Gesamtzahl Megabyte an der Position.

Verwendeter Speicherbereich (MB)
: Die Anzahl Megabyte, die an der Position verwendet werden.

Freier Speicherbereich (MB)
:  AIX-Betriebssysteme  Linux-BetriebssystemeDer Speicherbereich, der im Dateisystem verbleibt, in dem sich der Pfad befindet.
 Windows-BetriebssystemeDer Speicherbereich, der auf dem Laufwerk verbleibt, auf dem sich das Verzeichnis befindet.

DSMSERV DISPLAY LOG (Informationen zum Wiederherstellungsprotokoll anzeigen)

Mit diesem Dienstprogramm können Sie Informationen zu Wiederherstellungsprotokollen anzeigen, einschließlich der aktiven Protokolldatei, dem Spiegel für die aktive Protokolldatei, dem Übernahmeverzeichnis für das Archivprotokoll und dem Überlaufstandort für die Protokolle. Verwenden Sie dieses Dienstprogramm, wenn der Server nicht aktiv ist.

Syntax

```
>>-DSMSERV--+-------------------------+------------------------>
            |  (1)                    |
            '------- -u--Benutzername-'

>--+--------------------------------+---------------------------->
   |  (1)                           |
   '------- -i--Instanzverzeichnis-'

    (2).- -k--Server1-------.
>------+--------------------+--+------------------+------------>
       '- -k--Schlüsselname-'  '- -o--Optionsdatei-'

>--+------------+--+---------+--DISPLAY LOG--------------------><
   '- -noexpire-'  '- -quiet-'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

Parameter

 AIX-Betriebssysteme  Linux-Betriebssysteme-u Benutzername
:  AIX-Betriebssysteme  Linux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.

 AIX-Betriebssysteme  Linux-Betriebssysteme -i Instanzverzeichnis
:  AIX-Betriebssysteme  Linux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.

Windows-Betriebssysteme-k Schlüsselname

Windows-BetriebssystemeGibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Verwenden Sie diesen Parameter nur, wenn sich mehrere Server in demselben System befinden. Der Standardwert ist SERVER1.

-o Optionsdatei
: Gibt eine Optionsdatei an, die verwendet werden soll.

-noexpire
: Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist.

-quiet
: Gibt an, dass Nachrichten an die Konsole unterdrückt werden.

Beispiele: Informationen zu Wiederherstellungsprotokollen anzeigen

Informationen zu den Wiederherstellungsprotokollen anzeigen. Details zu den Informationen, die in der Ausgabe angezeigt werden, befinden sich in Feldbeschreibungen.

```
dsmserv display log
```

AIX-BetriebssystemeLinux-Betriebssysteme

```
                     Gesamtspeicherbereich (MB): 38.912
                Verwendeter Speicherbereich (MB): 401,34
                     Freier Speicherbereich (MB): 38.358,65
          Verzeichnis für aktive Protokolldateien:  /activelog
                Verzeichnis für Archivprotokolle: /archivelog
                     Spiegelprotokollverzeichnis: /mirrorlog
          Übernahmeverzeichnis für Archivprotokolle: /archfailoverlog
```

Windows-Betriebssysteme

```
                     Gesamtspeicherbereich (MB): 38.912
                Verwendeter Speicherbereich (MB): 401,34
                     Freier Speicherbereich (MB): 38.358,65
          Verzeichnis für aktive Protokolldateien: h:\tsm\activelog
                Verzeichnis für Archivprotokolle: k:\tsm\archivelog
                     Spiegelprotokollverzeichnis: i:\tsm\mirrorlog
          Übernahmeverzeichnis für Archivprotokolle: j:\tsm\archfailoverlog
```

Feldbeschreibungen

Gesamtspeicherbereich
: Gibt die maximale Größe der aktiven Protokolldatei an.

Verwendeter Speicherbereich
: Gibt den Gesamtspeicherbereich (in Megabyte) für aktive Protokolldateien an, der gegenwärtig in der Datenbank verwendet wird.

Freier Speicherbereich
: Gibt den Speicherbereich (in MB) für aktive Protokolldateien in der Datenbank an, der nicht von nicht festgeschriebenen Transaktionen verwendet wird.

Verzeichnis für aktive Protokolldateien
: Gibt die Position an, an der aktive Protokolldateien gespeichert werden. Wird das Verzeichnis für aktive Protokolldateien geändert, versetzt der Server alle archivierten Protokolle in das Verzeichnis für Archivprotokolle und alle aktiven Protokolldateien in ein neues Verzeichnis für aktive Protokolldateien.

Spiegelprotokollverzeichnis
: Gibt die Position an, an der der Spiegel der aktiven Protokolldatei aufbewahrt wird.

Übernahmeverzeichnis für Archivprotokolle
: Gibt die Position an, an der der Server Archivprotokolle sichert, wenn die Protokolle nicht am Zielort für Archivprotokolle archiviert werden können.

DSMSERV EXTEND DBSPACE (Speicherbereich für die Datenbank vergrößern)

Verwenden Sie dieses Dienstprogramm, um den Speicherbereich für die Datenbank zu vergrößern, indem Verzeichnisse für die Datenbank hinzugefügt werden. Dieses Dienstprogramm führt dieselbe Funktion wie der Befehl EXTEND DBSPACE aus, aber Sie können es verwenden, wenn der Server nicht aktiv ist.

Einschränkung: Die Neuverteilung von Daten und die Zurückforderung von Speicherbereich als Teil einer Operation zum Erweitern des Datenbankbereichs funktioniert nur mit DB2-Tabellenbereichen der Version 9.7 oder höher, die erstellt werden, wenn Sie einen neuen Server der Version 6.3 oder höher formatieren.

Syntax

```
>>-DSMSERV--+-------------------------+------------------------->
            |  (1)                    |
            '------- -u--Benutzername-'
```

```
>--+-------------------------------+--------------------------->
   |  (1)                          |
   '------- -i--Instanzverzeichnis-'

    (2).- -k--Server1-------.
>------+--------------------+--EXTend DBSpace------------------->
       '- -k--Schlüsselname-'

   .-,--------------.
   V                |  .-RECLAIMstorage--=--Yes-----.
>----DB-Verzeichnis-+--+----------------------------+---------><
                       '-RECLAIMstorage--=--+-No--+-'
                                            '-Yes-'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme-u Benutzername
AIX-BetriebssystemeLinux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.

AIX-BetriebssystemeLinux-Betriebssysteme -i Instanzverzeichnis
AIX-BetriebssystemeLinux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.

Windows-Betriebssysteme-kSchlüsselname
Windows-Betriebssysteme Gibt den Namen eines Windows-Registrierungsschlüssels an, der zum Speichern von Informationen zu diesem Server verwendet wird. Verwenden Sie diesen Parameter nur, wenn sich mehrere Server in demselben System befinden. Der Standardwert ist SERVER1.

DB-Verzeichnis (Erforderlich)
Gibt die Verzeichnisse für den Datenbankspeicher an. Die Verzeichnisse müssen leer sein und auf die Verzeichnisse muss durch die Benutzer-ID des Datenbankmanagers zugegriffen werden können. Ein Verzeichnisname muss ein vollständig qualifizierter Name sein und darf 175 Zeichen nicht überschreiten. Schließen Sie den Namen in Anführungszeichen ein, wenn er eingebettete Leerzeichen, ein Gleichheitszeichen oder andere Sonderzeichen enthält. Wenn Sie eine Verzeichnisliste für den Datenbankspeicher angeben, beträgt die maximale Länge der Liste 1400 Zeichen.
Windows-BetriebssystemeEinschränkung: Sie können keine Pfade mit allgemeiner Namenskonvention angeben.
Tipp: Geben Sie Verzeichnisse an, die dieselbe Größe wie vorhandene Verzeichnisse haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank.

RECLAIMstorage
Gibt an, ob Daten auf neu erstellte Datenbankverzeichnisse erneut verteilt werden und Speicherbereich aus den alten Speicherpfaden zurückgefordert wird, wenn Sie der Datenbank Speicherbereich hinzufügen. Dieser Parameter ist wahlfrei. Der Standardwert ist 'Yes'.

Yes
Gibt an, dass Daten erneut verteilt werden, sodass neue Verzeichnisse für die sofortige Verwendung verfügbar sind.
Wichtig: Bei dem Neuverteilungsprozess werden erhebliche Systemressourcen verwendet. Planen Sie dies im Voraus ein. Außerdem kann der Server für eine Weile offline sein, bis der Prozess beendet ist.

No
Gibt an, dass Daten nicht auf Datenbankverzeichnisse erneut verteilt werden und Speicherbereich nicht zurückgefordert wird.

AIX-BetriebssystemeLinux-Betriebssysteme

Beispiel: Speicherbereich für die Datenbank vergrößern

Ein Verzeichnis mit dem Namen stg1 im Verzeichnis tsm_db für den Datenbankspeicherbereich hinzufügen und dann Daten erneut verteilen und Speicherbereich zurückfordern, indem der folgende Befehl ausgegeben wird:

```
dsmserv extend dbspace /tsm_db/stg1
```

Windows-Betriebssysteme

Beispiel: Speicherbereich für die Datenbank vergrößern

Laufwerk D zum Speicherbereich für die Datenbank hinzufügen und dann Daten erneut verteilen und Speicherbereich zurückfordern, indem der folgende Befehl ausgegeben wird:

```
dsmserv extend dbspace D:
```

Zugehörige Verweise:

DSMSERV FORMAT (Datenbank und Protokoll formatieren)

Verwenden Sie das Dienstprogramm DSMSERV FORMAT, um die Serverdatenbank und das Wiederherstellungsprotokoll zu initialisieren. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls sind keine anderen Serveraktivitäten zulässig.

Die in diesem Dienstprogramm angegebenen Verzeichnisse sollten sich in einem schnellen und zuverlässigen Speicher befinden. Stellen Sie die Verzeichnisse nicht in Dateisysteme, für die nicht genügend Speicherplatz zur Verfügung stehen könnte. Werden bestimmte Verzeichnisse (beispielsweise das Verzeichnis für aktive Protokolldateien) nicht verfügbar oder voll, wird der Server gestoppt.

Windows-BetriebssystemeEinschränkung: Wenn Sie eine Dateizuordnungstabelle (FAT oder FAT32) oder ein NTFS-Format (NTFS = New Technology File System) verwenden, können Sie das Stammverzeichnis dieses Systems nicht als Position eines Datenbankverzeichnisses oder Protokollverzeichnisses angeben. Stattdessen müssen Sie ein oder mehrere Unterverzeichnisse innerhalb des Stammverzeichnisses erstellen. Erstellen Sie dann die Datenbankverzeichnisse und Protokollverzeichnisse innerhalb der Unterverzeichnisse.
Windows-BetriebssystemeWichtig: Das Installationsprogramm erstellt eine Reihe von Registrierungsschlüsseln. Einer dieser Schlüssel zeigt auf das Verzeichnis, in dem ein Standardserver mit dem Namen SERVER1 erstellt wird. Soll ein zusätzlicher Server installiert werden, erstellen Sie ein Verzeichnis und verwenden Sie das Dienstprogramm DSMSERV FORMAT mit dem Parameter -k in diesem Verzeichnis. Dieses Verzeichnis wird der Standort des Servers. Das Register verfolgt die installierten Server.

Wenn ein Server anfänglich mit dem Dienstprogramm DSMSERV FORMAT oder mit dem Konfigurationsassistenten erstellt wird, werden eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien zum Speichern von Datenbankinformationen erstellt, die vom Datenbankmanager verwendet werden.

Syntax

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme-u Benutzername
AIX-BetriebssystemeLinux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird. Dieser Parameter ist wahlfrei.

AIX-BetriebssystemeLinux-Betriebssysteme -i Instanzverzeichnis
AIX-BetriebssystemeLinux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Dieses Verzeichnis wird das aktuelle Arbeitsverzeichnis des Servers. Dieser Parameter ist wahlfrei.

Windows-Betriebssysteme-k Schlüsselname

Windows-BetriebssystemeGibt den Namen eines Windows-Registrierungsschlüssels an, der zum Speichern von Informationen zu diesem Server verwendet wird. Verwenden Sie diesen Parameter nur, um zusätzliche Server auf demselben System zu installieren. Nachdem ein Server unter Verwendung dieses Parameters installiert wurde, müssen Sie den Server immer mit dem Wert dieses Parameters starten. Dieser Parameter ist wahlfrei. Der Standardwert ist SERVER1.

Einschränkung: Zusätzliche Instanzen des IBM Spectrum Protect-Servers, die auf demselben System ausgeführt werden, konkurrieren um Ressourcen und haben Auswirkungen auf die Gesamtleistung jedes IBM Spectrum Protect-Servers.

-o Optionsdatei

Gibt eine Optionsdatei an, die verwendet werden soll. Dieser Parameter ist wahlfrei.

-noexpire

Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist. Dieser Parameter ist wahlfrei.

-quiet

Gibt an, dass Nachrichten an die Konsole unterdrückt werden. Dieser Parameter ist wahlfrei.

DBDir

Gibt die relativen Pfadnamen eines oder mehrerer Verzeichnisse an, die zum Speichern von Datenbankobjekten verwendet werden. Verzeichnisnamen müssen ohne Leerzeichen durch Kommas voneinander getrennt werden. Sie können bis zu 128 Verzeichnisnamen angeben. Sie müssen entweder den Parameter DBDIR oder den Parameter DBFILE angeben.

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zugrunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank.

DBFile

Gibt den Namen einer Datei an, die die relativen Pfadnamen eines oder mehrerer Verzeichnisse enthält, die zum Speichern von Datenbankobjekten verwendet werden. Jeder Verzeichnisname muss sich auf einer separaten Zeile in der Datei befinden. Sie können bis zu 128 Verzeichnisnamen angeben. Sie müssen entweder den Parameter DBDIR oder den Parameter DBFILE angeben.

ACTIVELOGSize

Gibt die Größe der aktiven Protokolldatei in Megabyte an. Dieser Parameter ist wahlfrei. Der Mindestwert ist 2048 MB (2 GB); der Maximalwert ist 524.288 MB (512 GB). Wenn eine ungerade Zahl angegeben wird, wird der Wert auf die nächste gerade Zahl aufgerundet. Der Standardwert ist 16384 MB.

Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Richtlinien für den Speicherbedarf befinden sich in der folgenden Tabelle:

Tabelle 1. Schätzung des Datenträger- und Dateispeicherbedarfs

Wert der Option ACTIVELOGSize	**Reservieren Sie diesen freien Speicherbereich im Verzeichnis für aktive Protokolldateien, zusätzlich zum Speicherbereich von ACTIVELOGSize**
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

ACTIVELOGDirectory (Erforderlich)

Gibt das Verzeichnis an, in das der Server aktive Protokolldateien schreibt und in dem der Server die Dateien speichert. Es gibt nur eine Position für aktive Protokolldateien. Der Name muss ein vollständig qualifizierter Verzeichnisname sein. Das Verzeichnis muss vorhanden sein, es muss leer sein, und auf das Verzeichnis muss durch die Benutzer-ID des Datenbankmanagers zugegriffen werden können. Die maximale Anzahl Zeichen beträgt 175.

ARCHLogdirectory (Erforderlich)

Gibt das Verzeichnis für die Archivprotokolldateien an. Der Name muss ein vollständig qualifizierter Verzeichnisname sein. Die maximale Anzahl Zeichen beträgt 175.

ARCHFailoverlogdirectory

Gibt das Verzeichnis an, das als alternative Speicherposition verwendet werden soll, wenn das ARCHLOGDIRECTORY-Verzeichnis voll ist. Dieser Parameter ist wahlfrei. Die maximale Anzahl Zeichen beträgt 175.

MIRRorlogdirectory

Gibt das Verzeichnis an, in dem der Server die aktive Protokolldatei spiegelt (die Dateien im ACTIVELOGDIRECTORY-Verzeichnis). Dieser Parameter ist wahlfrei. Das Verzeichnis muss ein vollständig qualifizierter Verzeichnisname sein. Die maximale Anzahl Zeichen beträgt 175.

Beispiel: Eine Datenbank formatieren

AIX-BetriebssystemeLinux-Betriebssysteme

```
dsmserv format dbdir=/tsmdb001 activelogsize=8192
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Windows-Betriebssysteme

```
dsmserv -k server2 format dbdir=d:\tsm\db001 activelogsize=8192
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

DSMSERV INSERTDB (Serverdatenbank in eine leere Datenbank versetzen)

Verwenden Sie das Dienstprogramm DSMSERV INSERTDB, um eine Serverdatenbank in eine neue Datenbank zu versetzen. Die Datenbank kann vom ursprünglichen Server extrahiert und in eine neue Datenbank auf dem neuen Server eingefügt werden, indem eine Netzverbindung zwischen den beiden Servern verwendet wird. Die Datenbank kann auch von Datenträgern eingefügt werden, die die extrahierte Datenbank enthalten.

Führen Sie vor der Verwendung des Dienstprogramms DSMSERV INSERTDB die Planungs- und Vorbereitungstasks aus, wie z. B. Sichern der Datenbank und Sichern der Konfigurationsdaten. Stellen Sie sicher, dass alle Voraussetzungen erfüllt sind, bevor Sie die Serverdatenbank versetzen.

Voraussetzungen für das Einfügen mit Datenträgern

Bevor Sie das Dienstprogramm zum Einfügen der Serverdatenbank in eine leere Datenbank ausführen, stellen Sie sicher, dass Ihr System die folgenden Voraussetzungen erfüllt.

- Die Manifestdatei aus der Operation DSMUPGRD EXTRACTDB muss verfügbar sein.
- Wenn die Manifestdatei keine Einheitenkonfigurationsdaten enthält oder wenn Sie den Parameter CONFIGINFO=DEVCONFIG angeben, müssen die beiden folgenden Anweisungen zutreffen:
  - Die Serveroptionsdatei muss einen Eintrag für die Einheitenkonfigurationsdatei enthalten.
  - Die Einheitenkonfigurationsdatei muss Informationen zur Einheitenklasse enthalten, die in der Manifestdatei angegeben ist.
- Die Datenträger, die die extrahierte Datenbank enthalten, müssen für den Server der Version 8 verfügbar sein. Außerdem müssen die Berechtigungen einen Zugriff auf die Datenträger für die Benutzer-ID gewähren, die Eigner der Serverinstanz der Version 8 ist.

Syntax

```
>>-DSMSERV--+-------------------------+------------------------>
            |  (1)                    |
            '------- -u--Benutzername-'

>--+-------------------------------+---------------------------->
   |  (1)                          |
   '------- -i--Instanzverzeichnis-'

    (2).- -k--Server1-------.
>------+--------------------+--+------------------+------------>
       '- -k--Schlüsselname-'  '- -o--Optionsdatei-'

>--+------------+--+---------+--INSERTDB------------------------>
   '- -noexpire-'  '- -quiet-'

>--+-| A: Von Datenträgern einfügen |-+------------------------->
   '-| B: Im Netz einfügen |----------'

   .-PREview--=--No------.
>--+--------------------+-------------------------------------><
   '-PREview--=--+-Yes-+-'
                 '-No--'

A: Von Datenträgern einfügen

|--+-----------------------------------+------------------------>
   '-DEVclass--=--Einheitenklassenname-'

   .-CONFiginfo--=--MANifest------.
>--+------------------------------+--MANifest--=--Dateiname-----|
   '-CONFiginfo--=--+-MANifest--+-'
                    '-DEVconfig-'

B: Im Netz einfügen

   .-SESSWait--=--60------.
|--+---------------------+-------------------------------------|
   '-SESSWait--=--Minuten-'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme-u Benutzername

AIX-BetriebssystemeLinux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird. Dieser Parameter ist wahlfrei.

AIX-BetriebssystemeLinux-Betriebssysteme -i Instanzverzeichnis

AIX-BetriebssystemeLinux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Dieses Verzeichnis wird das aktuelle Arbeitsverzeichnis des Servers. Dieser Parameter ist wahlfrei.

Windows-Betriebssysteme-k Schlüsselname

Windows-BetriebssystemeGibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Dieser Parameter ist wahlfrei. Der Standardwert ist SERVER1.

-o Optionsdatei

Gibt eine Optionsdatei an, die verwendet werden soll. Dieser Parameter ist wahlfrei.

-noexpire

Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist. Dieser Parameter ist wahlfrei.

-quiet

Gibt an, dass Nachrichten an die Konsole unterdrückt werden. Dieser Parameter ist wahlfrei.

DEVclass

Gibt eine Einheitenklasse mit sequenziellem Zugriff an. Mit Ausnahme der Einheitenklasse DISK kann jede Einheitenklasse angegeben werden. Die Definition für die Einheitenklasse muss entweder in der Manifestdatei oder der Einheitenkonfigurationsdatei vorhanden sein. Dieser Parameter ist wahlfrei und wird nur verwendet, wenn die Datenbank, die in die leere Datenbank der Version 8 eingefügt werden soll, auf Datenträger extrahiert wurde. Befindet sich die Datenbank auf Datenträgern und wird keine Einheitenklasse angegeben, wird die in der Manifestdatei angegebene Einheitenklasse verwendet.

Einschränkung: Sie können keine Einheitenklasse mit dem Einheitentyp NAS oder CENTERA verwenden.

MANifest

Gibt die Position der Manifestdatei an. Verwenden Sie einen vollständig qualifizierten Dateinamen oder stellen Sie die Datei in ein lokales Verzeichnis. Beispiel: `./manifest.txt`

Dieser Parameter ist erforderlich, wenn die Datenbank, die in die leere Datenbank der Version 8 eingefügt werden soll, auf Datenträger extrahiert wurde.

CONFiginfo

Gibt die Quelle der Einheitenkonfigurationsdaten an, die von der Operation DSMSERV INSERTDB verwendet wird. Der Standardwert für diesen Parameter ist MANIFEST. Gültige Werte sind:

MANifest

Gibt an, dass Einheitenkonfigurationsdaten aus der Manifestdatei gelesen werden. Wenn die Manifestdatei keine Einheitenkonfigurationsdaten enthält, wird statt dessen die Einheitenkonfigurationsdatei verwendet.

DEVConfig

Gibt an, dass Einheitenkonfigurationsdaten aus der Einheitenkonfigurationsdatei gelesen werden.

SESSWait

Gibt die Anzahl Minuten an, die der Server der Version 8 wartet, bis er vom ursprünglichen Server angesprochen wird. Der Standardwert ist 60 Minuten.

Verwenden Sie diesen Parameter nur, wenn die Daten, die in die leere Datenbank der Version 8 eingefügt werden, mit einer Netzverbindung vom Quellenserver übertragen werden.

PREview

Gibt an, ob die Einfügeoperation vorangezeigt werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist NO.

Verwenden Sie den Parameter PREVIEW=YES, um eine Datenbank zu testen. Wenn Sie diesen Parameter verwenden, schließt die Operation alle Schritte des Prozesses ein, mit Ausnahme der tatsächlichen Einfügung von Daten in die neue Datenbank. Mit der Voranzeige der Einfügeoperation können Sie schnell prüfen, ob die Quellendatenbank lesbar ist. Außerdem können Sie alle ungültigen Datenintegritätsbedingungen identifizieren, die verhindern können, dass eine Datenbank, für die ein Upgrade durchgeführt wurde, in der Produktion eingesetzt wird.

DSMSERV LOADFORMAT (Datenbank formatieren)

Verwenden Sie das Dienstprogramm DSMSERV LOADFORMAT, wenn ein Upgrade von Version 5 durchgeführt wird. Das Dienstprogramm formatiert eine leere Datenbank als Vorbereitung zum Einfügen einer extrahierten Datenbank in die leere Datenbank.

Syntax

```
>>-DSMSERV--+-------------------------+------------------------->
            |  (1)                    |
            '------- -u--Benutzername-'

>--+-------------------------------+--------------------------->
   |  (1)                          |
   '------- -i--Instanzverzeichnis-'

    (2).- -k--Server1-------.
```

```
>------+--------------------+--+------------------+------------>
       '- -k--Schlüsselname-'  '- -o--Optionsdatei-'

>--+------------+--+---------+--LOADFORMAT----------------------->
   '- -noexpire-'  '- -quiet-'

                .-,-----------.
                V             |
>--+-DBDir--=----Verzeichnis-+-+-------------------------------->
   '-DBFile--=--Datei----------'

   .-ACTIVELOGSize--=--16384----.
>--+----------------------------+-------------------------------->
   '-ACTIVELOGSize--=--Megabyte-'

>--ACTIVELOGDirectory--=--Verzeichnis---------------------------->

>--ARCHLogdirectory--=--Verzeichnis------------------------------>

>--+---------------------------------------+----------------->
   '-ARCHFailoverlogdirectory--=--Verzeichnis-'

>--+-----------------------------------+---------------------><
   '-MIRRorlogdirectory--=--Verzeichnis-'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme-u Benutzername
AIX-BetriebssystemeLinux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird. Dieser Parameter ist wahlfrei.

AIX-BetriebssystemeLinux-Betriebssysteme -i Instanzverzeichnis
AIX-BetriebssystemeLinux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Dieses Verzeichnis wird das aktuelle Arbeitsverzeichnis des Servers. Dieser Parameter ist wahlfrei.

Windows-Betriebssysteme-k Schlüsselname
Windows-BetriebssystemeGibt den Namen eines Windows-Registrierungsschlüssels an, der zum Speichern von Informationen zu diesem Server verwendet wird. Verwenden Sie diesen Parameter nur, um zusätzliche Server auf demselben System zu installieren. Nachdem ein Server unter Verwendung dieses Parameters installiert wurde, müssen Sie den Server immer mit dem Wert dieses Parameters starten. Der Standardwert ist SERVER1.

-o Optionsdatei
Gibt eine Optionsdatei an, die verwendet werden soll. Dieser Parameter ist wahlfrei.

-noexpire
Gibt an, dass die Verfallsverarbeitung unterdrückt wird, wenn der Server gestartet wird. Dieser Parameter ist wahlfrei.

-quiet
Gibt an, dass Nachrichten an die Konsole unterdrückt werden. Dieser Parameter ist wahlfrei.

DBDir
Gibt die relativen Pfadnamen eines oder mehrerer Verzeichnisse an, die zum Speichern von Datenbankobjekten verwendet werden. Verzeichnisnamen müssen ohne Leerzeichen durch Kommas voneinander getrennt werden. Sie können bis zu 128 Verzeichnisnamen angeben. Sie müssen entweder den Parameter DBDIR oder den Parameter DBFILE angeben.
Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zugrunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank.

DBFile
Gibt den Namen einer Datei an, die die relativen Pfadnamen eines oder mehrerer Verzeichnisse enthält, die zum Speichern von Datenbankobjekten verwendet werden. Jeder Verzeichnisname muss sich auf einer separaten Zeile in der Datei befinden. Sie können bis zu 128 Verzeichnisnamen angeben. Sie müssen entweder den Parameter DBDIR oder den Parameter DBFILE angeben.

ACTIVELOGSize
Gibt die Größe der aktiven Protokolldatei in Megabyte an. Dieser Parameter ist wahlfrei. Der Mindestwert ist 2048 MB (2 GB); der Maximalwert ist 524.288 MB (512 GB). Wenn eine ungerade Zahl angegeben wird, wird der Wert auf die nächste gerade Zahl aufgerundet. Der Standardwert ist 16384 MB.
Die Größe einer aktiven Protokolldatei basiert auf dem Wert der Option ACTIVELOGSIZE. Richtlinien für den Speicherbedarf befinden sich in der folgenden Tabelle:

Tabelle 1. Schätzung des Datenträger- und Dateispeicherbedarfs

Wert der Option ACTIVELOGSize	Reservieren Sie diesen freien Speicherbereich im Verzeichnis für aktive Protokolldateien, zusätzlich zum Speicherbereich von ACTIVELOGSize
16 GB - 128 GB	5120 MB

Wert der Option ACTIVELOGSize	Reservieren Sie diesen freien Speicherbereich im Verzeichnis für aktive Protokolldateien, zusätzlich zum Speicherbereich von ACTIVELOGSize
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

ACTIVELOGDirectory (Erforderlich)
: Gibt das Verzeichnis an, in das der Server aktive Protokolldateien schreibt und in dem der Server die Dateien speichert. Es gibt nur eine Position für aktive Protokolldateien. Der Name muss ein vollständig qualifizierter Verzeichnisname sein. Das Verzeichnis muss vorhanden sein, es muss leer sein, und auf das Verzeichnis muss durch die Benutzer-ID des Datenbankmanagers zugegriffen werden können. Die maximale Anzahl Zeichen beträgt 175.

ARCHLogdirectory (Erforderlich)
: Gibt das Verzeichnis für die Archivprotokolldateien an. Der Name muss ein vollständig qualifizierter Verzeichnisname sein. Die maximale Anzahl Zeichen beträgt 175.

ARCHFailoverlogdirectory
: Gibt das Verzeichnis an, das als alternative Speicherposition verwendet werden soll, wenn das ARCHLOGDIRECTORY-Verzeichnis voll ist. Dieser Parameter ist wahlfrei. Die maximale Anzahl Zeichen beträgt 175.

MIRRorlogdirectory
: Gibt das Verzeichnis an, in dem der Server die aktive Protokolldatei spiegelt (die Dateien im ACTIVELOGDIRECTORY-Verzeichnis). Dieser Parameter ist wahlfrei. Das Verzeichnis muss ein vollständig qualifizierter Verzeichnisname sein. Die maximale Anzahl Zeichen beträgt 175.

Beispiel: Eine Datenbank formatieren

 AIX-Betriebssysteme  Linux-Betriebssysteme

```
dsmserv loadformat dbdir=/tsmdb001 activelogsize=8192
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

 Windows-Betriebssysteme

```
dsmserv -k server2 loadformat dbdir=d:\tsm\db001 activelogsize=8192
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

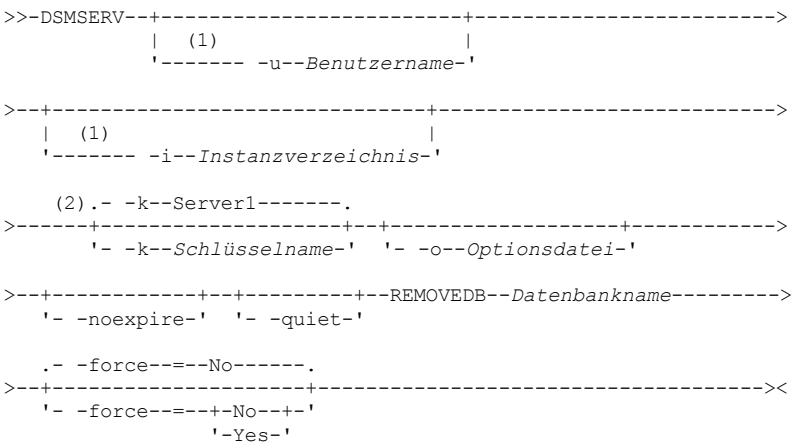
DSMSERV REMOVEDB (Datenbank entfernen)

Verwenden Sie das Dienstprogramm DSMSERV REMOVEDB, um eine IBM Spectrum Protect-Serverdatenbank zu entfernen.

Wenn Sie dieses Dienstprogramm ausführen, löschen Sie die Serverdatenbank, die aktiven Protokolldateien und die Spiegeldateien der aktiven Protokolldatei. Die Archivprotokolldateien und Übernahmeprotokolldateien des Archivprotokolls werden jedoch nur nach dem Start einer Datenbankzurückschreibung nach Zeitpunkt gelöscht.

Sie müssen den IBM Spectrum Protect-Server anhalten, bevor Sie diesen Befehl ausgeben.

Syntax



Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

Parameter

AIX-BetriebssysteLinux-Betriebssysteme-u Benutzername
AIX-BetriebssysteLinux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.
AIX-BetriebssysteLinux-Betriebssysteme -i Instanzverzeichnis
AIX-BetriebssysteLinux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.
Windows-Betriebssysteme-k Schlüsselname
Windows-BetriebssystemeGibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Der Standardwert ist SERVER1.

-o Optionsdatei
: Gibt eine Optionsdatei an, die verwendet werden soll.

-noexpire
: Gibt an, dass beim Start die Verfallsverarbeitung unterdrückt ist.

-quiet
: Gibt an, dass Nachrichten an die Konsole unterdrückt werden.

Datenbankname
: Der Datenbankname, der bei der Installation eingegeben wurde. Wurde die Datenbank manuell formatiert, ist dies der Parameter für den Datenbanknamen im Dienstprogramm DSMSERV FORMAT oder DSMSERV LOADFORMAT. Dieser Datenbankname befindet sich auch in der Datei dsmserv.opt. Dieser Parameter ist erforderlich.

-force
: Gibt an, ob die Datenbank entfernt wird, wenn offene Verbindungen vorhanden sind. Der Standardwert ist No. Dieser Parameter ist optional. Folgende Werte sind verfügbar:

  Yes
  : Gibt an, dass die Datenbank entfernt wird, unabhängig davon, ob offene Verbindungen vorhanden sind.

  No
  : Gibt an, dass die Datenbank nur entfernt wird, wenn alle Verbindungen geschlossen sind.

Beispiel: Eine Datenbank entfernen

Die IBM Spectrum Protect-Serverdatenbank TSMDB1 und alle ihre Verweise entfernen.

```
dsmserv removedb TSMDB1
```

Beispiel: Eine Datenbank mit dem Parameter 'force' entfernen

Die IBM Spectrum Protect-Serverdatenbank TSMDB1 und alle ihre Verweise entfernen, auch wenn offene Verbindungen vorhanden sind:

```
dsmserv removedb TSMDB1 force=yes
```

DSMSERV RESTORE DB (Datenbank zurückschreiben)

Mit diesem Dienstprogramm können Sie eine Datenbank mit Hilfe einer Datenbanksicherung zurückschreiben.

Einschränkung: Sie können eine Serverdatenbank nicht zurückschreiben, wenn der Release-Level der Serverdatenbanksicherung von dem Release-Level des Servers abweicht, der zurückgeschrieben wird. Beispielsweise tritt ein Fehler auf, wenn Sie eine Datenbank der Version 7.1.3 zurückschreiben und Sie einen IBM Spectrum Protect-Server der Version 8.1 verwenden.

Die Zurückschreibungsoperation verwendet Datenbanksicherungen, die mit dem Befehl BACKUP DB erstellt wurden.

Wichtig: Geben Sie nach einer Zurückschreibungsoperation nach Zeitpunkt den Befehl AUDIT VOLUME aus, um alle DISK-Datenträger zu prüfen und alle Inkonsistenzen zwischen den Datenbankinformationen und den Speicherpooldatenträgern zu beseitigen. Überprüfen Sie vor dem Zurückschreiben der Datenbank die Datenträgerhistorydatei, um die Datenträger in Speicherpools mit sequenziellem Zugriff zu bestimmen, die seit dem Zeitpunkt, für den die Datenbank zurückgeschrieben wurde, gelöscht oder wiederverwendet wurden.

- DSMSERV RESTORE DB (Datenbank mit dem neuesten Stand zurückschreiben)
  Verwenden Sie das Dienstprogramm DSMSERV RESTORE DB, um unter bestimmten Bedingungen eine Datenbank mit ihrem aktuellen Status zurückzuschreiben.
- DSMSERV RESTORE DB (Datenbank nach Zeitpunkt zurückschreiben)
  Verwenden Sie diesen Befehl, um eine Datenbank nach Zeitpunkt zurückzuschreiben. Eine Datenträgerhistorydatei und eine Einheitenkonfigurationsdatei müssen verfügbar sein.

DSMSERV RESTORE DB (Datenbank mit dem neuesten Stand zurückschreiben)

Verwenden Sie das Dienstprogramm DSMSERV RESTORE DB, um unter bestimmten Bedingungen eine Datenbank mit ihrem aktuellen Status zurückzuschreiben.

Folgende Bedingungen müssen erfüllt sein:

- Eine unbeschädigte Datenträgerhistorydatei ist verfügbar.
- Die Wiederherstellungsprotokolle sind verfügbar.
- Eine Einheitenkonfigurationsdatei mit den gültigen Einheitendaten ist verfügbar.

Einschränkung: Sie können eine Serverdatenbank nicht zurückschreiben, wenn der Release-Level der Serverdatenbanksicherung von dem Release-Level des Servers abweicht, der zurückgeschrieben wird. Beispielsweise tritt ein Fehler auf, wenn Sie eine Datenbank der Version 7.1.3 zurückschreiben und Sie einen IBM Spectrum Protect-Server der Version 8.1 verwenden.

IBM Spectrum Protect fordert Datenträgerladevorgänge an, um die neueste Sicherungsserie zu laden, und verwendet dann die Wiederherstellungsprotokolle, um die Datenbank mit ihrem aktuellen Status zu aktualisieren.

Momentaufnahmesicherungen der Datenbank können nicht verwendet werden, um eine Datenbank mit ihrem aktuellen Status zurückzuschreiben.

Syntax

```
>>-DSMSERV--+-------------------------+------------------------>
            |  (1)                    |
            '------- -u--Benutzername-'

>--+-------------------------------+---------------------------->
   |  (1)                          |
   '------- -i--Instanzverzeichnis-'

    (2).- -k--Server1-------.
>------+---------------------+--+-------------------+------------>
       '- -k--Schlüsselname-'  '- -o--Optionsdatei-'

>--+---------------+--RESTORE DB------------------------------->
   |  (1)          |
   '------- -quiet-'

>--+-----------------------------+----------------------------->
   '-RECOVerydir--=--Verzeichnis-'

>--+-----------------------------+----------------------------->
   '-ACTIVELOGDir--=--Verzeichnis-'

                                  .-PReview--=--No------.
>--+-----------------------------+--+--------------------+----->
   '-ON--=--Zielverzeichnisdatei-'  '-PReview--=--+-Yes-+-'
                                                  '-No--'

   .-RESTOREKeys--=--No-------.
>--+--------------------------+--------------------------------->
   '-RESTOREKeys--=--+-No---+-'
                     +-YES--+
                     '-ONLY-'

>--+---------------------------+------------------------------><
   '-PASSword--=--Kennwortname-'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme-u Benutzername
AIX-BetriebssystemeLinux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.

AIX-BetriebssystemeLinux-Betriebssysteme -i Instanzverzeichnis
AIX-BetriebssystemeLinux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Dieses Instanzverzeichnis wird das aktuelle Arbeitsverzeichnis des Servers.

Windows-Betriebssysteme-k Schlüsselname
Windows-BetriebssystemeGibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Der Standardwert ist SERVER1.

-o Optionsdatei
Gibt eine Optionsdatei an, die verwendet werden soll.

AIX-BetriebssystemeLinux-Betriebssysteme-quiet
AIX-BetriebssystemeLinux-BetriebssystemeGibt an, dass Nachrichten an die Konsole unterdrückt werden.

RECOVerydir
Gibt ein Verzeichnis an, in dem Wiederherstellungsprotokollinformationen von den Datenbanksicherungsdatenträgern gespeichert werden sollen. Dieses Verzeichnis muss über ausreichend Speicherplatz verfügen, um diese Transaktionswiederherstellungsinformationen zu speichern, und es muss ein leeres Verzeichnis sein. Wird dieser Parameter nicht angegeben, ist der Standardwert das Verzeichnis, das mit einem der folgenden Parameter im Dienstprogramm DSMSERV FORMAT oder DSMSERV LOADFORMAT angegeben ist:

- ARCHFAILOVERLOGDIRECTORY, falls angegeben
- ARCHLOGDIRECTORY, wenn ARCHFAILOVERLOGDIRECTORY nicht angegeben ist

ACTIVELOGDir
Gibt ein Verzeichnis an, in dem die Protokolldateien gespeichert werden sollen, die zum Verfolgen der aktiven Datenbankoperationen verwendet werden. Dieses Verzeichnis muss nur angegeben werden, wenn zu einem anderen Verzeichnis für aktive Protokolldateien als dem bereits konfigurierten Verzeichnis umgeschaltet werden soll.

On
Gibt eine Datei an, in der die Verzeichnisse aufgelistet sind, in die die Datenbank zurückgeschrieben wird. Geben Sie jedes Verzeichnis in einer separaten Zeile in der Datei an. Beispielsweise gibt der Parameter ON die Datei restorelist.txt an, die die folgende Liste enthält:
 AIX-Betriebssysteme  Linux-Betriebssysteme

```
/tsmdb001
/tsmdb002
/tsmdb003
```

 Windows-Betriebssysteme

```
e:\tsm\db001
f:\tsm\db002
g:\tsm\db003
```

Wird dieser Parameter nicht angegeben, werden die Ursprungsverzeichnisse verwendet, die in der Datenbanksicherung aufgezeichnet wurden.
Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zugrunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank.

PReview
Gibt an, dass die Datenträgerhistorydateien geprüft und die Datenbanksicherungsdatenträger aus der Datenträgerhistorydatei ausgewertet werden.

1. Welche Gruppe von Datenbanksicherungsdatenträgern entspricht am besten den aktuellen Kriterien, die für die Zurückschreibungsverarbeitung angegeben sind? Die Datenträgerhistorydaten stellen ausführliche Informationen zur Sicherungsserien-ID, zur Operations-ID (Gesamtsicherung, Teilsicherung 1, Teilsicherung 2, usw.), zum Datum der Datenbanksicherung und zur Einheitenklasse bereit. Diese Informationen und die im Befehl DSMSERV RESTORE DB angegebenen Parameter bestimmen, was für die Ausführung der Zurückschreibung verwendet wird. Die Datenträgerhistorydatei wird geprüft, um die neueste Datenbanksicherung zu suchen und dann die Daten mit dieser Sicherung zurückzuschreiben.
2. Sind selbst beschreibende Daten für die ausgewählte Gruppe von Datenbanksicherungsdatenträgern verfügbar? Überprüfen Sie die Datenträgerhistorydaten auf diese Sicherungsserie. Beim Datenabgleich wird der Inhalt der selbst beschreibenden Daten mit den Angaben aus den Datenträgerhistoryeinträgen verglichen. Die Überprüfung schließt das Laden eines oder mehrerer Datenträger ein, die von der Datenträgerhistory angegeben werden. Anschließend werden die selbst beschreibenden Daten, die in den Datenbanksicherungsdatenträgern enthalten waren, mit den Angaben in der Datenträgerhistory für die Datenbanksicherung abgeglichen. Sind die Informationen aus der Datenträgerhistorydatei und die selbst beschreibenden Daten nicht konsistent, werden Nachrichten ausgegeben, um das Problem zu identifizieren. Beispiel: Es wurden nicht alle Werte angegeben bzw. es sind nicht alle Werte verfügbar oder es wurden keine selbst beschreibenden Daten gefunden.

Sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung konsistent, wird eine Nachricht ausgegeben, die angibt, dass die Datenbanksicherung für die Zurückschreibungsverarbeitung verwendet werden kann.

Sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung nicht konsistent oder wurden die selbst beschreibenden Daten für die Sicherung nicht gefunden, werden Fehlernachrichten ausgegeben, die angeben, was überprüft wurde und was nicht gefunden wurde.

Wird der Parameter PREVIEW nicht angegeben oder wird der Parameter auf NO gesetzt und sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung konsistent, wird die Zurückschreibung fortgesetzt.

Wird der Parameter PREVIEW nicht angegeben oder wird der Parameter auf NO gesetzt und schlagen der Datenabgleich und die Überprüfung fehl, wird die Datenbankzurückschreibung nicht ausgeführt. Stellen Sie weitere Datenträger zur Verfügung, auf die von der Datenträgerhistorydatei verwiesen wird, oder entfernen Sie die unvollständige Sicherungsserie oder Operation, damit der IBM Spectrum Protect-Server eine andere bevorzugte Serie oder Operation auswählt und die Verarbeitung fortsetzt.

Wird der Parameter PREVIEW auf YES gesetzt, werden von dem Prozess nur die Auswertung der Datenträgerhistorydatei sowie der Datenabgleich und die Validierung mit der ausgewählten Datenbanksicherung ausgeführt.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeRESTOREKeys

AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeGibt an, ob der Masterverschlüsselungsschlüssel des Servers, der zum Verschlüsseln von Speicherpooldaten verwendet wird, zurückgeschrieben werden soll, wenn die Datenbank zurückgeschrieben wird. Dieser Parameter ist optional und gilt nur, wenn Sie verschlüsselte Containerspeicherpools in einer Cloudumgebung verwenden. Wenn der Masterschlüssel des Servers beim Zurückschreiben der Datenbank geschützt ist, ist der Standardwert YES. Wenn der Masterschlüssel des Servers beim Zurückschreiben der Datenbank nicht geschützt ist, ist der Standardwert NO. Sie können einen der folgenden Werte angeben:

No
: Gibt an, dass der Masterschlüssel des Servers beim Zurückschreiben der Datenbank nicht zurückgeschrieben wird.

Yes
: Gibt an, dass der Masterschlüssel des Servers beim Zurückschreiben der Datenbank zurückgeschrieben wird. Sie müssen ein Kennwort für diesen Parameter angeben.

Only
: Gibt an, dass nur der Masterschlüssel des Servers zurückgeschrieben wird. Die Datenbank wird nicht zurückgeschrieben.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemePASSword
: AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeGibt das Kennwort an, das zum Schützen der Datenbanksicherung verwendet wird. Dieser Parameter gilt nur, wenn Sie verschlüsselte Containerspeicherpools in einer Cloudumgebung verwenden. Wenn Sie ein Kennwort für die Datenbanksicherung angeben, müssen Sie dasselbe Kennwort im Befehl RESTORE DB zum Zurückschreiben der Datenbank angeben. Sie müssen ein Kennwort verwenden, wenn Sie den Parameter RESTOREKEYS=YES oder RESTOREKEYS=ONLY angeben.

Beispiel: Die Datenbank mit ihrem aktuellen Status zurückschreiben

Die Datenbank mit ihrem aktuellen Status unter Verwendung des bereits konfigurierten Verzeichnisses für aktive Protokolldatei zurückschreiben.

```
dsmserv restore db
```

Beispiel: Masterschlüssel des Servers zurückschreiben, ohne die Datenbank zurückzuschreiben

Den folgenden Befehl ausgeben, um den Masterschlüssel des Servers zurückzuschreiben, ohne die Datenbank zurückzuschreiben:

```
dsmserv restore db restorekeys=only
```

DSMSERV RESTORE DB (Datenbank nach Zeitpunkt zurückschreiben)

Verwenden Sie diesen Befehl, um eine Datenbank nach Zeitpunkt zurückzuschreiben. Eine Datenträgerhistorydatei und eine Einheitenkonfigurationsdatei müssen verfügbar sein.

Einschränkung: Sie können eine Serverdatenbank nicht zurückschreiben, wenn der Release-Level der Serverdatenbanksicherung von dem Release-Level des Servers abweicht, der zurückgeschrieben wird. Beispielsweise tritt ein Fehler auf, wenn Sie eine Datenbank der Version 7.1.3 zurückschreiben und Sie einen IBM Spectrum Protect-Server der Version 8.1 verwenden.

Sie können Gesamt- und Teilsicherungen der Datenbank oder Momentaufnahmesicherungen der Datenbank verwenden, um eine Datenbank nach Zeitpunkt zurückzuschreiben.

Tipp: Wenn Sie eine IBM Spectrum Protect-Serverdatenbank der Version 7 oder höher mit dem Stand eines bestimmten Zeitpunkts zurückschreiben, ist die bevorzugte Methode die Ausgabe des Befehls DSMSERV REMOVE DB vor der Ausgabe des Befehls DSMSERV RESTORE DB. Damit wird sichergestellt, dass das System einen ordnungsgemäßen Status aufweist. Das System löscht und entkatalogisiert die Datenbank im Hintergrund. Wenn Sie Daten mit dem Stand eines bestimmten Zeitpunkts zurückschreiben, werden alle erforderlichen Protokolle und das Datenbankimage von den Sicherungsdatenträgern abgerufen.

Syntax

```
>>-DSMSERV--+-------------------------+------------------------->
            |  (1)                    |
            '------- -u--Benutzername-'

>--+-------------------------------+---------------------------->
   |  (1)                          |
   '------- -i--Instanzverzeichnis-'

    (2).- -k--Server1-------.
>------+--------------------+--+-------------------+------------>
       '- -k--Schlüsselname-'  '- -o--Optionsdatei-'

>--+---------------+--RESTORE DB--TODate--=--Datum-------------->
   |  (1)          |
   '------- -quiet-'

   .-TOTime--=--23:59:59-.  .-Source--=--DBBackup-------.
>--+---------------------+--+---------------------------+------->
```

```
   '-TOTime--=--Zeit-----'  '-Source--=--+-DBBackup---+-'
                                         '-DBSnapshot-'

>--+-----------------------------+-----------------------------><
   '-RECOVerydir--=--Verzeichnis-'

>--+-----------------------------+-----------------------------><
   '-ACTIVELOGDir--=--Verzeichnis-'

                                    .-PReview--=--No------.
>--+-----------------------------+--+---------------------+----->
   '-ON--=--Zielverzeichnisdatei-'  '-PReview--=--+-Yes-+-'
                                                  '-No--'

   .-RESTOREKeys--=--No-------.
>--+--------------------------+-------------------------------><
   '-RESTOREKeys--=--+-No---+-'
                     +-YES--+
                     '-ONLY-'

>--+--------------------------+-------------------------------><
   '-PASSword--=--Kennwortname-'
```

Anmerkungen:

1. Dieser Parameter gilt nur für AIX- und Linux-Server.
2. Dieser Parameter gilt nur für Windows-Server.

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme-u Benutzername
AIX-BetriebssystemeLinux-BetriebssystemeGibt einen Benutzernamen an, zu dem umgeschaltet werden soll, bevor der Server initialisiert wird.

AIX-BetriebssystemeLinux-Betriebssysteme -i Instanzverzeichnis
AIX-BetriebssystemeLinux-BetriebssystemeGibt ein Instanzverzeichnis an, das verwendet werden soll. Dies wird das aktuelle Arbeitsverzeichnis des Servers.

Windows-Betriebssysteme-k Schlüsselname
Windows-BetriebssystemeGibt den Namen des Windows-Registrierungsschlüssels an, aus dem Informationen zum Server abgerufen werden sollen. Der Standardwert ist SERVER1.

-o Optionsdatei
Gibt eine Optionsdatei an, die verwendet werden soll.

AIX-BetriebssystemeLinux-Betriebssysteme-quiet
AIX-BetriebssystemeLinux-BetriebssystemeGibt an, dass Nachrichten an die Konsole unterdrückt werden.

TODate (Erforderlich)
Gibt das Datum an, auf das die Datenbank zurückgeschrieben werden soll. Die folgenden Werte sind gültig:

MM/TT/JJJJ
Gibt an, dass eine Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben werden soll, die vor diesem angegebenen Datum erstellt wurde.

TODAY
Gibt an, dass eine Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben werden soll, die vor dem aktuellen Datum erstellt wurde.

TODAY-Tage oder -Tage
Gibt an, dass eine Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben werden soll, die die angegebene Anzahl Tage vor dem aktuellen Datum erstellt wurde.

TOTime
Gibt die Uhrzeit an, auf die die Datenbank zurückgeschrieben werden soll. Dieser Parameter ist wahlfrei. Der Standardwert ist das Ende des Tages (23:59:59). Gültige Werte:

HH:MM:SS
Gibt an, dass die Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben werden soll, die zu oder vor der angegebenen Zeit an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

NOW
Gibt an, dass die Datenbank unter Verwendung einer Sicherungsserie zurückgeschrieben werden soll, die zu oder vor der aktuellen Zeit an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

Wird beispielsweise das Dienstprogramm DSMSERV RESTORE DB um 9:00 mit TOTIME=NOW ausgegeben, wird die Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben, die um oder vor 9:00 an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

NOW-Stunden:Minuten oder -Stunden:Minuten

Gibt an, dass die Datenbank unter Verwendung einer Sicherungsserie zurückgeschrieben werden soll, die zu oder vor der aktuellen Zeit minus einer angegebenen Anzahl Stunden und (wahlweise) Minuten an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

Wird beispielsweise das Dienstprogramm DSMSERV RESTORE DB um 9:00 mit TOTIME=NOW-3:30 oder TOTIME+-3:30 ausgegeben, wird die Datenbank unter Verwendung der letzten Sicherungsserie zurückgeschrieben, die um oder vor 5:30 an dem Datum erstellt wurde, das im Parameter TODATE angegeben ist.

Source
Gibt an, ob die Datenbank unter Verwendung von Datenträgern mit Gesamt- und Teilsicherungen der Datenbank oder von Datenträgern mit Momentaufnahmesicherungen der Datenbank zurückgeschrieben wird. Dieser Parameter ist wahlfrei. Der Standardwert ist DBBackup. Die folgenden Werte sind gültig:

DBBackup
Gibt an, dass die Datenbank wie folgt zurückgeschrieben wird:

1. Die Datenträgerhistorydatei wird gelesen, um die erforderlichen Datenträger mit Gesamt- und Teilsicherungen der Datenbank zu lokalisieren.
2. Ladevorgänge werden angefordert und die Daten von den Datenträgern mit Gesamt- und Teilsicherungen der Datenbank nach Bedarf geladen, um den Datenbankdatenträger auf die angegebene Zeit zurückzuschreiben.

DBSnapshot
Gibt an, dass die Datenbank wie folgt zurückgeschrieben wird:

1. Die Datenträgerhistorydatei wird gelesen, um die erforderlichen Datenträger mit Momentaufnahmesicherungen der Datenbank zu lokalisieren.
2. Ladevorgänge werden angefordert und Daten von den Datenträgern mit Momentaufnahmesicherungen der Datenbank nach Bedarf geladen, um den Datenträger auf die angegebene Zeit zurückzuschreiben.

RECOVerydir
Gibt ein Verzeichnis an, in dem Wiederherstellungsprotokollinformationen von den Datenbanksicherungsdatenträgern gespeichert werden sollen. Diese Protokollinformationen werden verwendet, um eine Transaktionskonsistenz der Serverdatenbank als Teil der Wiederherstellungsverarbeitung zu erreichen. Dieses Verzeichnis muss über ausreichend Speicherplatz verfügen, um diese Transaktionswiederherstellungsinformationen zu speichern, und es muss ein leeres Verzeichnis sein. Wird dieser Parameter nicht angegeben, ist der Standardwert das Verzeichnis, das mit einem der folgenden Parameter im Dienstprogramm DSMSERV FORMAT oder DSMSERV LOADFORMAT angegeben ist:

- ARCHFAILOVERLOGDIRECTORY, falls angegeben
- ARCHLOGDIRECTORY, wenn ARCHFAILOVERLOGDIRECTORY nicht angegeben ist

ACTIVELOGDir
Gibt ein Verzeichnis an, in dem die Protokolldateien gespeichert werden sollen, die zum Verfolgen der aktiven Datenbankoperationen verwendet werden. Geben Sie dieses Verzeichnis nur an, wenn zu einem anderen Verzeichnis für aktive Protokolldateien als dem bereits konfigurierten Verzeichnis umgeschaltet werden soll.

On
Gibt eine Datei an, in der die Verzeichnisse aufgelistet sind, in die die Datenbank zurückgeschrieben wird. Geben Sie jedes Verzeichnis in einer separaten Zeile in der Datei an. Beispielsweise gibt der Parameter ON die Datei restorelist.txt an, die die folgende Liste enthält:
AIX-BetriebssystemeLinux-Betriebssysteme

```
/tsmdb001
/tsmdb002
/tsmdb003
```

Windows-Betriebssysteme

```
e:\tsm\db001
f:\tsm\db002
g:\tsm\db003
```

Wird dieser Parameter nicht angegeben, werden die Ursprungsverzeichnisse verwendet, die in der Datenbanksicherung aufgezeichnet wurden.
Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zugrunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Sind ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse, reduzieren sie das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank.

PReview
Gibt an, dass die Datenträgerhistorydateien geprüft und die Datenbanksicherungsdatenträger aus der Datenträgerhistorydatei ausgewertet werden.

1. Welche Gruppe von Datenbanksicherungsdatenträgern entspricht am besten den zeitpunktgesteuerten Kriterien, die für die Zurückschreibungsverarbeitung angegeben sind? Die Datenträgerhistorydaten stellen ausführliche Informationen zur Sicherungsserien-ID, zur Operations-ID (Gesamtsicherung, Teilsicherung 1, Teilsicherung 2, usw.), zum Datum der Datenbanksicherung und zur Einheitenklasse bereit. Diese Informationen und die im Befehl DSMSERV RESTORE DB angegebenen

Parameter bestimmen, was für die Ausführung der Zurückschreibung verwendet wird. Die Datenträgerhistorydatei wird geprüft, um die beste Datenbanksicherung zu suchen, die den angegebenen zeitpunktgesteuerten Kriterien entspricht, und dann die Zurückschreibung mit dieser Sicherung auszuführen.

2. Sind selbst beschreibende Daten für die ausgewählte Gruppe von Datenbanksicherungsdatenträgern verfügbar? Überprüfen Sie die Datenträgerhistorydaten auf diese Sicherungsserie. Beim Datenabgleich wird der Inhalt der selbst beschreibenden Daten mit den Angaben aus den Datenträgerhistoryeinträgen verglichen. Die Überprüfung schließt das Laden eines oder mehrerer Datenträger ein, die von der Datenträgerhistory angegeben werden. Anschließend werden die selbst beschreibenden Daten, die in den Datenbanksicherungsdatenträgern enthalten waren, mit den Angaben in der Datenträgerhistory für die Datenbanksicherung abgeglichen. Sind die Informationen aus der Datenträgerhistorydatei und die selbst beschreibenden Daten nicht konsistent, werden Nachrichten ausgegeben, um das Problem zu identifizieren. Beispiel: Es wurden nicht alle Werte angegeben bzw. es sind nicht alle Werte verfügbar oder es wurden keine selbst beschreibenden Daten gefunden.

Sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung konsistent, wird eine Nachricht ausgegeben, die angibt, dass die Datenbanksicherung für die Zurückschreibungsverarbeitung verwendet werden kann.

Sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung nicht konsistent oder wurden die selbst beschreibenden Daten für die Sicherung nicht gefunden, werden Fehlernachrichten ausgegeben, die angeben, was überprüft wurde und was nicht gefunden wurde.

Wird der Parameter PREVIEW nicht angegeben oder wird der Parameter auf NO gesetzt und sind die Datenträgerhistorydaten und die selbst beschreibenden Daten aus der Datenbanksicherung konsistent, wird die Zurückschreibung fortgesetzt.

Wird der Parameter PREVIEW nicht angegeben oder wird der Parameter auf NO gesetzt und schlagen der Datenabgleich und die Überprüfung fehl, wird die Datenbankzurückschreibung nicht ausgeführt. Stellen Sie weitere Datenträger zur Verfügung, auf die von der Datenträgerhistorydatei verwiesen wird, oder entfernen Sie die unvollständige Sicherungsserie oder Operation, damit der IBM Spectrum Protect-Server eine andere bevorzugte Serie oder Operation auswählt und die Verarbeitung fortsetzt.

Wird der Parameter PREVIEW auf YES gesetzt, werden von dem Prozess nur die Auswertung der Datenträgerhistorydatei sowie der Datenabgleich und die Validierung mit der ausgewählten Datenbanksicherung ausgeführt.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeRESTOREKeys
AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeGibt an, ob der Masterverschlüsselungsschlüssel des Servers, der zum Verschlüsseln von Speicherpooldaten verwendet wird, zurückgeschrieben werden soll, wenn die Datenbank zurückgeschrieben wird. Dieser Parameter ist optional und gilt nur, wenn Sie verschlüsselte Containerspeicherpools in einer Cloudumgebung verwenden. Wenn der Masterschlüssel des Servers beim Zurückschreiben der Datenbank geschützt ist, ist der Standardwert YES. Wenn der Masterschlüssel des Servers beim Zurückschreiben der Datenbank nicht geschützt ist, ist der Standardwert NO. Sie können einen der folgenden Werte angeben:

No
: Gibt an, dass der Masterschlüssel des Servers beim Zurückschreiben der Datenbank nicht zurückgeschrieben wird.

Yes
: Gibt an, dass der Masterschlüssel des Servers beim Zurückschreiben der Datenbank zurückgeschrieben wird. Sie müssen ein Kennwort für diesen Parameter angeben.

Only
: Gibt an, dass nur der Masterschlüssel des Servers zurückgeschrieben wird. Die Datenbank wird nicht zurückgeschrieben.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemePASSword
AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeGibt das Kennwort an, das zum Schützen der Datenbanksicherung verwendet wird. Dieser Parameter gilt nur, wenn Sie verschlüsselte Containerspeicherpools in einer Cloudumgebung verwenden. Wenn Sie ein Kennwort für die Datenbanksicherung angeben, müssen Sie dasselbe Kennwort im Befehl RESTORE DB zum Zurückschreiben der Datenbank angeben. Sie müssen ein Kennwort verwenden, wenn Sie den Parameter RESTOREKEYS=YES oder RESTOREKEYS=ONLY angeben.

Beispiel: Die Datenbank mit einer bestimmten Zeitangabe zurückschreiben

Die Datenbank mit ihrem Status am 12. Mai 2011 um 14:25 zurückschreiben.

```
dsmserv restore db todate=05/12/2011 totime=14:45
```

Beispiel: Masterschlüssel des Servers zurückschreiben, ohne die Datenbank zurückzuschreiben

Den folgenden Befehl ausgeben, um den Masterschlüssel des Servers zurückzuschreiben, ohne die Datenbank zurückzuschreiben:

```
dsmserv restore db restorekeys=only
```

Windows-Betriebssysteme

DSMSERV UPDATE (Registry-Einträge für eine Serverinstanz erstellen)

Verwenden Sie dieses Dienstprogramm, um Registry-Einträge für eine IBM Spectrum Protect-Serverinstanz zu erstellen, wenn die Einträge versehentlich gelöscht wurden.

Führen Sie dieses Dienstprogramm im Instanzverzeichnis für die Datenbank aus (in dem Dateien, wie beispielsweise dsmserv.dsk, für den Server gespeichert sind). Das Dienstprogramm erstellt die ursprünglichen Registry-Einträge für den Server erneut.

Syntax

```
            .- -k--Server1-------.
>>-DSMSERV--+--------------------+--UPDATE--------------------><
            '- -k--Schlüsselname-'
```

Parameter

-k Schlüsselname
: Gibt den Namen des Windows-Registrierungsschlüssels an, in dem Informationen zum Server gespeichert werden sollen. Der Standardwert ist Server1.

Beispiel: Registry-Einträge für eine Serverinstanz erneut erstellen

Führen Sie das Dienstprogramm aus, um Registry-Einträge für die Serverinstanz Server2 erneut zu erstellen.

```
"c:\Programme\Tivoli\TSM\server\bin\dsmserv" -k server2 update
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

DSMULOG (IBM Spectrum Protect-Servernachrichten in einer Benutzerprotokolldatei speichern)

Verwenden Sie diesen Befehl, um Nachrichten der IBM Spectrum Protect-Server-Konsole in einer Benutzerprotokolldatei zu speichern. Sie können angeben, dass IBM Spectrum Protect Nachrichten in mehrere Benutzerprotokolldateien schreiben soll.

Wichtig: Stellen Sie die Benutzerprotokolle nicht in das Dateisystem /usr oder /opt, da Speicherbeschränkungen in dem Dateisystem das Starten des Servers verhindern können.

Syntax

```
>>-DSMULOG--+------------------------+------------------------><
            | .-,------------------. |
            | V                    | |
            '---Protokolldateiname-+-'
```

Parameter

Protokolldateiname (Erforderlich)
: Gibt den Namen einer oder mehrerer Benutzerprotokolldateien an, in die IBM Spectrum Protect Serverkonsolnachrichten schreibt. Wenn Sie mehrere Dateinamen angeben, wird in jede Datei einen Tag lang geschrieben. Anschließend fährt der Server mit der nächsten Datei fort, um Protokollnachrichten zu speichern. Wenn in alle Dateien in der Liste geschrieben wurde, schreibt der Server wieder in die erste Datei und alle in dieser Datei enthaltenen Nachrichten werden überschrieben.

Beispiel: Konsolnachrichten in einer Benutzerprotokolldatei speichern

Verwenden Sie den Befehl DSMULOG, um Konsolnachrichten in einer Benutzerprotokolldatei zu speichern.
Geben Sie die Benutzerprotokolldateien an, in denen Konsolnachrichten gespeichert werden sollen.

```
dsmulog /u/admin/log1 /u/admin/log2 /u/admin/log3
```

Einheitendienstprogramme für den IBM Spectrum Protect-Server

Für Tasks, die sich auf das Konfigurieren von Speichereinheiten für den Server beziehen, können Sie Einheitendienstprogramme verwenden.

Einheitendienstprogramme

-  AIX-Betriebssystemetsmdlst (Informationen zu Einheiten anzeigen)
- Linux-Betriebssystemeautoconf (Einheiten automatisch konfigurieren)
-  Windows-Betriebssystemetsmdlst (Informationen zu Einheiten anzeigen)

 AIX-Betriebssysteme

tsmdlst (Informationen zu Einheiten anzeigen)

Mit dem Dienstprogramm tsmdlst können Sie Einheitennamen und andere Informationen zu Datenträgerwechslern und Bandeinheiten, die durch den IBM Spectrum Protect gesteuert werden, anzeigen.

Das Dienstprogramm tsmdlst ist Bestandteil des IBM Spectrum Protect-Einheitentreiberpakets, das für den Server und den Speicheragenten identisch ist. Sie müssen den IBM Spectrum Protect-Einheitentreiber installieren, um das Dienstprogramm tsmdlst für den Speicheragenten ausführen zu können.

Nach der Konfiguration von Einheiten können Sie das Dienstprogramm tsmdlst ausführen, um Einheitendaten anzuzeigen. Das Dienstprogramm speichert diese Informationen in Dateien, die Sie abrufen können. Die Dateien haben den Namen lbinfo für Datenträgerwechsler und den Namen mtinfo für Bandeinheiten. Nachdem eine Einheit hinzugefügt oder rekonfiguriert wurde, können Sie diese Dateien aktualisieren, indem Sie das Dienstprogramm tsmdlst erneut ausführen.

Das Dienstprogramm tsmdlst und die von ihm generierten Ausgabedateien befinden sich im Verzeichnis devices/bin, das standardmäßig /opt/tivoli/tsm/devices/bin lautet. Bevor Sie das Dienstprogramm tsmdlst ausführen, müssen Sie sicherstellen, dass entweder der IBM Spectrum Protect-Server gestoppt wurde oder alle Aktivitäten der Einheiten gestoppt wurden. Wird eine Einheit gerade vom IBM Spectrum Protect-Server verwendet, wenn das Dienstprogramm tsmdlst ausgeführt wird, erhalten Sie einen Fehler, der angibt, dass die Einheit aktiv ist.

Optionen

/t
: Zeigt Tracenachrichten für das Dienstprogramm tsmdlst an.

/?
: Zeigt Nutzungsinformationen zum Dienstprogramm tsmdlst und zu seinen Parametern an.

 AIX-Betriebssysteme

Beispiel: Informationen zu allen Einheiten anzeigen

Informationen zu allen Einheiten anzeigen, die durch den IBM Spectrum Protect-Einheitentreiber konfiguriert wurden:

```
tsmdlst

TSM Device Name Vendor   Product ID       Firmware World Wide Name         Serial Number
--------------- -------- ---------------- -------- ----------------------- --------------
/dev/lb4        ATL      P3000            0100     N/A                     1651639999

TSM Device Name Vendor   Product ID       Firmware World Wide Name         Serial Number
--------------- -------- ---------------- -------- ----------------------- --------------
/dev/mt0        QUANTUM  DLT-S4            2A2A    50:0e:09:e0:00:16:ca:47 QD0619AMD00052
/dev/mt1        QUANTUM  DLT-S4            2A2A    50:0e:09:e0:00:16:cd:e5 QD0624AMD00184
/dev/mt22       QUANTUM  DLT7000           0100    N/A                     1651639000
/dev/mt23       QUANTUM  DLT7000           0100    N/A                     1651639002
```

 Linux-Betriebssysteme

autoconf (Einheiten automatisch konfigurieren)

Verwenden Sie das Dienstprogramm autoconf, um Einheiten für die Verwendung mit dem IBM Spectrum Protect-Server zu konfigurieren.

Das Dienstprogramm autoconf führt die folgenden Tasks aus:

- Lädt den Treiber in den Kernel
- Erstellt die erforderlichen Dateien für den IBM Spectrum Protect-Einheitentreiber
- Erstellt Einheitendatendateien für Speicherarchive und Bandeinheiten

Das Dienstprogramm autoconf ist im Paket für den Einheitentreiber enthalten und wird im Verzeichnis /opt/tivoli/tsm/devices/bin installiert.

Optionen

-a
: Fügt den IBM Spectrum Protect-Einheitendateien Lese- und Schreibberechtigung hinzu, um allen Benutzern den Zugriff auf die Einheiten zu ermöglichen. Geben Sie diesen Wert an, um Einheiten zu konfigurieren, wenn der IBM Spectrum Protect-Server von einem Benutzer ohne Rootberechtigung gestartet wird.

-g
: Fügt den IBM Spectrum Protect-Einheitendateien Lese- und Schreibberechtigung hinzu, um jedem Benutzer in derselben Gruppe die Verwendung der Einheiten als Rootbenutzer zu ermöglichen.

-t
: Aktiviert die Tracefunktion für das Dienstprogramm autoconf.

-?

Zeigt Informationen zum Dienstprogramm autoconf und zu seinen Parametern an.

Beispiel: Einheiten mit dem Dienstprogramm 'autoconf' konfigurieren

Führen Sie das Dienstprogramm autoconf aus, um IBM Spectrum Protect-Einheiten zu konfigurieren:

```
> /opt/tivoli/tsm/devices/bin/autoconf
```

Linux-Betriebssysteme

Beispiel: Einheiten mithilfe des Dienstprogramms 'autoconf' für einen Server konfigurieren, der von einer Benutzer-ID ohne Rootberechtigung gestartet wird

Führen Sie autoconf aus, um IBM Spectrum Protect-Einheiten zu konfigurieren. Verwenden Sie die Option a, da der Server von einer Benutzer-ID gestartet wird, die nicht der Rootbenutzer ist.

```
> /opt/tivoli/tsm/devices/bin/autoconf -a

Added the read and write permissions for all users to /dev/sg4.
Added the read and write permissions for all users to /dev/sg5.
Added the read and write permissions for all users to /dev/sg6.
Added the read and write permissions for all users to /dev/sg7.
Added the read and write permissions for all users to /dev/sg8.
Added the read and write permissions for all users to /dev/sg9.
Added the read and write permissions for all users to /dev/sg10.
Added the read and write permissions for all users to /dev/sg11.
Added the read and write permissions for all users to /dev/sg12.
Added the read and write permissions for all users to /dev/sg13.
Added the read and write permissions for all users to /dev/sg14.
Added the read and write permissions for all users to /dev/sg15.
Added the read and write permissions for all users to /dev/sg16.
Added the read and write permissions for all users to /dev/sg17.
Added the read and write permissions for all users to /dev/sg18.
Added the read and write permissions for all users to /dev/sg19.
Added the read and write permissions for all users to /dev/sg20.
Added the read and write permissions for all users to /dev/sg21.
Added the read and write permissions for all users to /dev/sg22.
Added the read and write permissions for all users to /dev/sg23.
Added the read and write permissions for all users to /dev/sg24.
Added the read and write permissions for all users to /dev/sg25.
Added the read and write permissions for all users to /dev/sg26.
Added the read and write permissions for all users to /dev/sg27.
Added the read and write permissions for all users to /dev/sg28.
Added the read and write permissions for all users to /dev/sg29.

Tape Drives:
====================
Index Minor Host CHN ID  LUN Type Vendor_ID Device_Serial_Number       Product_ID       Rev.
000   004   003  000 004 000 001  IBM       1068000439                 ULTRIUM-HH5      C5X1
001   007   003  000 008 001 001  HP        01UbWSD-04                 Ultrium 2-SCSI   R210
002   008   003  000 008 002 001  HP        01UbWSD-05                 Ultrium 2-SCSI   R210
003   010   003  000 008 004 001  HP        01UbWSD-07                 Ultrium 3-SCSI   R210
004   012   003  000 008 006 001  HP        01UbWSD-01                 Ultrium 3-SCSI   R210
005   013   003  000 008 007 001  HP        01UbWSD-02                 Ultrium 3-SCSI   R210
006   014   003  000 008 008 001  HP        01UbWSD-08                 Ultrium 3-SCSI   R210
007   015   003  000 008 009 001  HP        01UbWSD-09                 Ultrium 3-SCSI   R210
008   016   003  000 008 010 001  HP        01UbWSD-0a                 Ultrium 3-SCSI   R210
009   017   003  000 008 011 001  HP        01UbWSD-0b                 Ultrium 3-SCSI   R210
010   018   003  000 008 012 001  HP        01UbWSD-0c                 Ultrium 3-SCSI   R210
011   019   003  000 008 013 001  HP        01UbWSD-0d                 Ultrium 3-SCSI   R210
012   020   003  000 005 000 001  IBM       1068000913                 ULTRIUM-HH5      C5X1
013   022   003  000 009 001 001  QUANTUM   01UbWSD-0f                 SDLT320          R210
014   023   003  000 009 002 001  QUANTUM   01UbWSD-0g                 SDLT320          R210
015   024   003  000 009 003 001  QUANTUM   01UbWSD-0h                 SDLT320          R210
016   025   003  000 009 004 001  QUANTUM   01UbWSD-0i                 SDLT320          R210
017   026   003  000 006 000 001  IBM       1068001573                 ULTRIUM-HH4      B5Q1
018   027   003  000 007 000 001  IBM       1068001545                 ULTRIUM-HH4      B5Q1
019   028   003  000 010 000 001  HP        HU19477PAE                 Ultrium 5-SCSI   I65W

Medium Changer Devices:
============================
Index Minor Host CHN ID  LUN Type Vendor_ID Device_Serial_Number       Product_ID       Rev.
000   005   003  000 004 001 008  NEC       2Y11BB0023                 LL-2B01          0004
001   006   003  000 008 000 008  HP        01UbWSD-03                 VLS              1.00
002   009   003  000 008 003 008  HP        01UbWSD-06                 ThinStor AutoLdr T133
003   011   003  000 008 005 008  HP        01UbWSD-00                 ESL E-Series     2.00
004   021   003  000 009 000 008  HP        01UbWSD-0e                 MSL6000 Series   0430
005   029   003  000 010 001 008  HP        3615-0101                  MSL G3 Series    1120
```

Windows-Betriebssysteme

tsmdlst (Informationen zu Einheiten anzeigen)

Mit dem Dienstprogramm tsmdlst können Sie Einheitennamen und andere Informationen zu Datenträgerwechslern und Bandeinheiten auf dem System anzeigen.

Optionen

Nach der Konfiguration von Einheiten können Sie das Dienstprogramm tsmdlst ausführen, um Einheitendaten anzuzeigen. Das Dienstprogramm befindet sich im Einheitenverzeichnis 'server', das standardmäßig \Programme\Tivoli\TSM\server lautet.

/computer=Computername
: Gibt den Namen des Computers an, für den Einheiten aufgelistet werden. Der Standardwert ist das lokale System.

/detail
: Zeigt Details zu Einheiten in der Liste an. Standardmäßig wird eine Zusammenfassung angezeigt.

/all
: Zeigt Informationen zu allen Einheitentypen an. Standardmäßig sind nur Bandlaufwerke und Bandarchive in den Ergebnissen enthalten.

/nogenerictapecheck
: Überspringt den Schritt zum Öffnen erkannter Laufwerke, um zu bestimmen, ob sie für den IBM Spectrum Protect-Einheitentyp GENERICTAPE unterstützt werden.

/nohbacheck
: Überspringt den Schritt für die HBA-API-Erkennung. Damit kann die Verarbeitung beschleunigt werden. Diese Option kann hilfreich sein, wenn das Debugging erforderlich ist.

/trace
: Wird für Diagnosezwecke verwendet. Speichert Traceausgabe in der Datei tsmdlst_trace.txt.

/?
: Zeigt Nutzungsinformationen zum Dienstprogramm tsmdlst und zu seinen Parametern an.

/xinquiry
: Stellt eine alternative Methode zum Abrufen der Seriennummer und des weltweiten Namens bereit. Diese Option wird nur für Einheiten verwendet, die vom IBM® Bandeinheitentreiber unterstützt werden. Die folgenden Parameter gelten speziell für die Option /xinquiry:

  /processAll
  : Gibt an, dass der Prozess so lange ausgeführt wird, bis alle Einheiten verarbeitet wurden.

  /maxRetries=#
  : Gibt die maximale Anzahl Versuche an, jedes Laufwerk zu öffnen. Diese Option erfordert die Option /processAll.

  /genpathfile
  : Verwenden Sie diese Option, um eine Liste mit Einheiten und Seriennummern zu generieren. Informationen für die Optionen /genmacropathsync und /genmacropathoffline werden in die Datei tsmdlst_pathfile.txt geschrieben.

  /includelib
  : Wenn dieser Parameter mit der Option /genpathfile angegeben wird, schließt die Liste der Einheiten zusätzlich zu Laufwerken auch Speicherarchive ein.

/genmacropathsync
: Generiert ein Makro, um IBM Spectrum Protect-Pfade für den Speicheragenten auf der Basis der Seriennummer zu synchronisieren. Ein Laufwerk muss eine für IBM Spectrum Protect definierte Seriennummer haben, damit diese Option funktioniert.

/genmacropathoffline
: Generiert ein Makro, um IBM Spectrum Protect-Pfade für den Speicheragenten auf der Basis der Zugänglichkeit eines Laufwerks in den Online- oder Offline-Status zu aktualisieren. Auf ein Laufwerk kann zugegriffen werden, wenn ein Betriebssystemaufruf zum Öffnen zu einem der folgenden Ergebnisse führt: ERROR_SUCCESS, ERROR_BUSY oder ERROR_ACCESS_DENIED. Diese Option kann nur für Einheiten verwendet werden, die den IBM Einheitentreiber verwenden. Ein symbolischer Name, wie z. B. `\\.\tape0`, ist zum Öffnen einer Einheit erforderlich.
  Die folgenden Optionen werden nur mit den Optionen /genmacropathsync und /genmacropathoffline verwendet:

  /server=Servername
  : Gibt den Namen des Servers an, den der Speicheragent verwendet.

  /stagent=Name des Speicheragenten
  : Gibt den Namen des Speicheragenten an.

  /tcps=Adresse
  : Gibt die IBM Spectrum Protect-Serveradresse an.

  /tcpp=Port
  : Gibt den IBM Spectrum Protect-Server-Port an. Der Standardwert ist 1500.

  /id=ID
  : Gibt die IBM Spectrum Protect-Administrator-ID an.

  /pass=Kennwort
  : Gibt das IBM Spectrum Protect-Administratorkennwort an.

  /devicetype=Laufwerktyp
  : Gibt den Einheitentyp des Laufwerks an, beispielsweise `LTO`. Bei dieser Option muss die Groß-/Kleinschreibung beachtet werden. Die Option ist optional.

  /libraryname=Speicherarchivname

Filtert den Speicherarchivnamen des Laufwerks, z. B. `LTO3584`. Bei dieser Option muss die Groß-/Kleinschreibung beachtet werden. Die Option ist optional.

/execmacropathsync
: Gibt das Makro zum Synchronisieren des Pfads an den IBM Spectrum Protect-Server aus.

/execmacropathoffline
: Gibt das Makro zum Aktualisieren des Pfads in den Online- oder Offline-Status an den IBM Spectrum Protect-Server aus.

/addpaths
: Fügt Anweisungen DEFINE und UPDATE PATH hinzu. Diese Option wird mit der Option /genmacropathsync verwendet.

/verbose
: Listet Laufwerk- und Pfadinformationen, die vom IBM Spectrum Protect-Server zurückgegeben werden, und den Inhalt der Pfaddatei auf.

/encodednames
: Wird ein Pfad auf `online=no` gesetzt, werden Zeitmarke, Fehler und Einheit als aktualisierter Einheitenname verschlüsselt.

Beispiel: Informationen zu Einheiten anzeigen

Informationen zu Bandeinheiten und Bandarchiven für das lokale System WANTON anzeigen, indem das Dienstprogramm tsmdlst ausgeführt wird:

```
tsmdlst
```

Der angezeigte Einheitenname ist der Aliasname, der im Befehl DEFINE PATH und im Befehl UPDATE PATH verwendet werden kann. Der Aliasname ist nicht der tatsächliche Einheitenname.

```
Computer Name:      WANTON
OS Version:         6.2
OS Build #:         9200
TSM Device Driver:  TSMScsi - Not Running

4 HBAs were detected.

Manufacturer         Model    Driver      Version     Firmware NodeWWN           Description
-------------------------------------------------------------------------------------------------------------
-----
QLogic Corporation   QLE2562  ql2300.sys  9.1.11.28   7.03.00  20000024FF25F846  QLogic QLE2562 Fibre Channel
Adapter
QLogic Corporation   QLE2562  ql2300.sys  9.1.11.28   7.03.00  20000024FF25F847  QLogic QLE2562 Fibre Channel
Adapter
QLogic Corporation   QLE2562  ql2300.sys  9.1.11.28   7.03.00  20000024FF25F7FE  QLogic QLE2562 Fibre Channel
Adapter
QLogic Corporation   QLE2562  ql2300.sys  9.1.11.28   7.03.00  20000024FF25F7FF  QLogic QLE2562 Fibre Channel
Adapter

TSM Name     ID  LUN  Bus  Port  SSN                 WWN                TSM Type     Driver   Device Identifier
-------------------------------------------------------------------------------------------------------------
------
mt0.0.0.7    0   0    0    7     000001327176        5005076300566011   3592         IBM      IBM      03592E06
2883
lb0.1.0.7    0   1    0    7     0000013400480405    5005076300566011   LIBRARY      IBM      IBM      03584L22
E01q
mt1.0.0.7    1   0    0    7     000001327147        5005076300566012   3592         IBM      IBM      03592E06
2883
mt2.0.0.7    2   0    0    7     000001327349        5005076300566013   3592         IBM      IBM      03592E06
2883
mt3.0.0.7    3   0    0    7     000001327140        5005076300566014   3592         IBM      IBM      03592E06
2883
mt4.0.0.7    4   0    0    7     1068000254          500507630F51FA05   LTO          IBM      IBM      ULT3580-
TD5 D8D4
lb4.1.0.7    4   1    0    7     0000078216780402    500507630F51FA05   LIBRARY      IBM      IBM      03584L32
C460
mt5.0.0.7    5   0    0    7     1068000039          500507630F51FA06   LTO          IBM      IBM      ULT3580-
TD5 D8D4
mt6.0.0.7    6   0    0    7     1068000047          500507630F51FA07   LTO          IBM      IBM      ULT3580-
TD5 D8D4
mt7.0.0.7    7   0    0    7     1068000017          500507630F51FA08   LTO          IBM      IBM      ULT3580-
TD5 D8D4
```

Server-Scripts und Makros für die Automatisierung

Sie können allgemeine Verwaltungstasks automatisieren, indem Sie IBM Spectrum Protect-Server-Scripts und Makros des Verwaltungsclients erstellen. Server-Scripts werden in der Serverdatenbank gespeichert und können für die Ausführung mit einem Befehl für Verwaltungszeitpläne geplant werden. Makros des Verwaltungsclients werden als Dateien auf dem Verwaltungsclient gespeichert. Makros können nicht serverübergreifend verteilt und nicht auf dem Server geplant werden.

- Server-Scripts
  Sie können allgemeine Verwaltungstasks mithilfe von Scripts, die in der Serverdatenbank gespeichert sind, automatisieren. Sie können die

Verarbeitung eines Scripts mithilfe des Verwaltungsbefehlsschedulers auf dem Server planen.

- Makros des Verwaltungsclients
  Ein Makro ist eine Datei, die mindestens einen Verwaltungsclientbefehl enthält. Sie können ein Makro vom Verwaltungsclient aus nur im Stapelmodus oder im interaktiven Modus ausführen. Makros werden als Datei auf dem Verwaltungsclient gespeichert. Sie werden nicht über Server verteilt und können nicht auf dem Server geplant werden.

Server-Scripts

Sie können allgemeine Verwaltungstasks mithilfe von Scripts, die in der Serverdatenbank gespeichert sind, automatisieren. Sie können die Verarbeitung eines Scripts mithilfe des Verwaltungsbefehlsschedulers auf dem Server planen.

IBM Spectrum Protect-Scripts weisen die folgende Funktionalität und Anweisungen auf:

- Befehlsparametersubstitution
- Befehle SELECT, die Sie bei der Verarbeitung des Scripts angeben
- Steuerung der Befehlsausführung, wie beispielsweise die Verarbeitungsoptionen PARALLEL und SERIAL
- Ablaufanweisungen mit bedingter Logik. Diese Logikablaufanweisungen umfassen die folgenden Anweisungen:
  - Die Klausel IF; diese Klausel legt fest, wie die Verarbeitung auf der Basis des aktuellen Rückkehrcodewerts fortgesetzt wird.
  - Die Anweisung EXIT; diese Anweisung beendet die Scriptverarbeitung.
  - Die Anweisungen GOTO und LABEL; diese Anweisungen steuern den Logikablauf so, dass die Verarbeitung bei der Zeile fortgesetzt wird, die mit der angegebenen Kennzeichnung beginnt
- Kommentarzeilen

Beispielscripts werden in der Datei scripts.smp bereitgestellt. Die Beispielscripts verfügen über eine beispielhafte Ausführungsreihenfolge zur Zeitplanung von Verwaltungsbefehlen.

Wenn einer der Befehle in dem Script nicht erfolgreich verarbeitet wird, werden die übrigen Befehle nicht verarbeitet.

- Server-Script definieren
  Sie können ein Server-Script zeilenweise definieren, eine Datei erstellen, die Befehlszeilen enthält, oder ein vorhandenes Script kopieren.
- Script aktualisieren
  Sie können ein Script aktualisieren, um eine Befehlszeile zu ändern oder einem Script eine Befehlszeile hinzuzufügen.
- Server-Script zum Erstellen eines anderen Server-Scripts abfragen
  Sie können weitere Server-Scripts durch Abfragen eines Scripts unter Angabe der Parameter FORMAT=RAW und OUTPUTFILE erstellen. Die Ausgabe der Abfrage kann als Eingabe für ein neues Script verwendet werden, so dass das neue Script nicht zeilenweise erstellt werden muss.
- Server-Script ausführen
  Um ein Script zu verarbeiten, verwenden Sie den Befehl RUN. Sie können ein Script, das Substitutionsvariablen enthält, ausführen, indem Sie die Substitutionsvariablen im Befehl RUN angeben.

Server-Script definieren

Sie können ein Server-Script zeilenweise definieren, eine Datei erstellen, die Befehlszeilen enthält, oder ein vorhandenes Script kopieren.

Informationen zu diesem Vorgang

Einschränkung: Sie können die Ausgabe eines Befehls in einem Server-Script nicht umleiten. Führen Sie stattdessen das Script aus und geben Sie dann die Befehlsumleitung an. Um beispielsweise die Ausgabe von script1 in das Verzeichnis c:\temp\test.out umzuleiten, führen Sie das Script aus und geben Sie die Befehlsumleitung wie in dem folgenden Beispiel gezeigt an:

```
run script1 > c:\temp\test.out
```

Vorgehensweise

1. Definieren Sie ein Script mit dem Befehl DEFINE SCRIPT. Anfänglich kann mit diesem Befehl die erste Zeile des Scripts definiert werden. Beispiel:

   ```
   define script qaixc "select node_name from nodes where platform='aix'"
   desc='AIX-Clients anzeigen'
   ```

   In diesem Beispiel wird das Script als QAIXC definiert. Wenn das Script ausgeführt wird, werden alle AIX-Clients angezeigt.
2. Definieren Sie mit dem Befehl UPDATE SCRIPT weitere Zeilen in dem Script. Wenn beispielsweise ein Befehl QUERY SESSION hinzugefügt werden soll, geben Sie Folgendes ein:

   ```
   update script qaixc "query session *"
   ```

3. Optional: Sie können einen Parameter WAIT im Befehl DEFINE CLIENTACTION angeben. Mithilfe dieses Parameters können Sie festlegen, dass die Clientaktion abgeschlossen sein muss, bevor der nächste Schritt im Befehlsscript oder Makro verarbeitet wird.
4. Optional: Mit dem Befehl ISSUE MESSAGE können Sie feststellen, wo innerhalb eines Befehls in einem Script ein Problem vorliegt.

- Befehle parallel oder seriell ausführen
  Sie können Befehle in einem Script seriell, parallel oder seriell und parallel ausführen. Geben Sie dazu den Scriptbefehl SERIAL oder PARALLEL im Parameter COMMAND_LINE der Befehle DEFINE und UPDATE SCRIPT an. Demzufolge ist es möglich, mehrere Befehle parallel auszuführen und zu warten, bis sie beendet sind, bevor der nächste Befehl ausgeführt wird.
- Befehle über mehrere Befehlszeilen fortsetzen
  Lange Befehle können über mehrere Befehlszeilen fortgesetzt werden, indem ein Fortsetzungszeichen (-) als letztes Zeichen in einer Zeile eines fortzusetzenden Befehls angegeben wird.
- Substitutionsvariablen in ein Script einschließen
  Sie können Substitutionsvariablen in ein Script einschließen. Substitutionsvariablen werden durch das Zeichen $ angegeben, gefolgt von einer Ziffer, die die Position des Parameters bei der Verarbeitung des Scripts angibt.
- Logikablaufanweisungen in ein Script einschließen
  Sie können Ablaufanweisungen mit bedingter Logik verwenden, die auf Rückkehrcodes basieren, die bei der vorherigen Befehlsverarbeitung ausgegeben wurden. Mithilfe dieser Logikanweisungen können Sie Ihre Scripts gemäß dem Ergebnis bestimmter Befehle verarbeiten. Die Anweisungen IF, EXIT und GOTO (LABEL) können verwendet werden.
- Befehle SELECT in einem Script verwenden
  Ein IBM Spectrum Protect-Script besteht aus mindestens einem Befehl und wird als Objekt in der Datenbank gespeichert. Sie können ein Script definieren, das einen oder mehrere Befehle SELECT enthält.

Befehle parallel oder seriell ausführen

Sie können Befehle in einem Script seriell, parallel oder seriell und parallel ausführen. Geben Sie dazu den Scriptbefehl SERIAL oder PARALLEL im Parameter COMMAND_LINE der Befehle DEFINE und UPDATE SCRIPT an. Demzufolge ist es möglich, mehrere Befehle parallel auszuführen und zu warten, bis sie beendet sind, bevor der nächste Befehl ausgeführt wird.

Informationen zu diesem Vorgang

Durch die serielle Ausführung von Befehlen in einem Script wird sichergestellt, dass alle vorhergehenden Befehle abgeschlossen sind, bevor der nächste Befehl ausgeführt wird, und dass alle nachfolgenden Befehle seriell ausgeführt werden. Wenn ein Script gestartet wird, werden alle Befehle so lange seriell ausgeführt, bis ein Befehl PARALLEL gefunden wird. Mehrere Befehle, die parallel ausgeführt werden und auf gemeinsame Ressourcen, wie beispielsweise Bandlaufwerke, zugreifen, können seriell ausgeführt werden.

Scriptrückkehrcodes vor und nach der Ausführung eines Befehls PARALLEL ändern sich nicht. Wenn ein Befehl SERIAL gefunden wird, wird der Scriptrückkehrcode auf den maximalen Rückkehrcode aller vorhergehenden Befehle gesetzt, die parallel ausgeführt wurden.

Wenn Sie Serverbefehle verwenden, die den Parameter WAIT im Anschluss an einen Befehl PARALLEL unterstützen, ist das Verhalten wie folgt:

- Wenn Sie den Standardwert WAIT=NO angeben oder verwenden, wartet das Script nicht auf den Abschluss des Befehls, wenn ein nachfolgender Befehl SERIAL gefunden wird. Der Rückkehrcode von diesem Befehl spiegelt die Verarbeitung nur bis zu dem Punkt wider, an dem der Befehl einen Hintergrundprozess startet. Der abschließende Rückkehrcode des Befehls ist für das Script nicht verfügbar.
- Wenn Sie WAIT=YES angeben, wartet das Script auf den Abschluss des Befehls, wenn ein nachfolgender Befehl SERIAL gefunden wird. Der Rückkehrcode von diesem Befehl spiegelt die Verarbeitung für den gesamten Befehl wider.

In den meisten Fällen können Sie WAIT=YES in Befehlen verwenden, die parallel ausgeführt werden.

Einschränkung: Wenn mit dem Befehl ein Hintergrundprozess gestartet wird, für den nicht der Parameter WAIT angegeben ist, wird der Befehl als abgeschlossen betrachtet, nachdem der Hintergrundthread gestartet wurde. Daher kann der Befehl nur in Parallelverarbeitung ausgeführt werden.

Das folgende Beispiel zeigt die Verwendung des Befehls PARALLEL zum Sichern, Umlagern und Wiederherstellen von Speicherpools.

```
/*mehrere Befehle parallel ausführen und auf deren Beendigung warten, bevor fortgefahren wird*/
PARALLEL
/*vier Speicherpools gleichzeitig sichern*/
BACKUP STGPOOL PRIMPOOL1 COPYPOOL1 WAIT=YES
BACKUP STGPOOL PRIMPOOL2 COPYPOOL2 WAIT=YES
BACKUP STGPOOL PRIMPOOL3 COPYPOOL3 WAIT=YES
BACKUP STGPOOL PRIMPOOL4 COPYPOOL4 WAIT=YES
/*warten, bis alle vorherigen Befehle beendet sind*/
SERIAL
/*nach Beendigung der Sicherungen die Speicherpools gleichzeitig umlagern*/
PARALLEL
MIGRATE STGPOOL PRIMPOOL1 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL2 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL3 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL4 DURATION=90 WAIT=YES
/*warten, bis alle vorherigen Befehle beendet sind*/
SERIAL
/*nach Beendigung der Umlagerung die Speicherpools gleichzeitig wiederherstellen*/
PARALLEL
RECLAIM STGPOOL PRIMPOOL1 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL2 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL3 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL4 DURATION=120 WAIT=YES
```

Zugehörige Verweise:
DEFINE SCRIPT (Server-Script definieren)
UPDATE SCRIPT (Server-Script aktualisieren)

Befehle über mehrere Befehlszeilen fortsetzen

Lange Befehle können über mehrere Befehlszeilen fortgesetzt werden, indem ein Fortsetzungszeichen (-) als letztes Zeichen in einer Zeile eines fortzusetzenden Befehls angegeben wird.

Informationen zu diesem Vorgang

Im folgenden Beispiel wird eine SQL-Anweisung über mehrere Befehlszeilen fortgesetzt:

```
/*-----------------------------*/
/* Beispiel einer Fortsetzung  */
SELECT-
* FROM-
NODE WHERE-
PLATFORM='win32'
```

Wenn dieser Befehl verarbeitet wird, wird der folgende Befehl ausgeführt:

```
select * from nodes where platform='win32'
```

Substitutionsvariablen in ein Script einschließen

Sie können Substitutionsvariablen in ein Script einschließen. Substitutionsvariablen werden durch das Zeichen $ angegeben, gefolgt von einer Ziffer, die die Position des Parameters bei der Verarbeitung des Scripts angibt.

Informationen zu diesem Vorgang

In dem folgenden Beispielscript SQLSAMPLE sind die Substitutionsvariablen $1 und $2 angegeben:

```
/*---------------------------------------------*/
/* Beispiel einer Substitution */
/* --------------------------------------------*/
SELECT-
$1 FROM-
NODES WHERE-
PLATFORM='$2'
```

Wenn Sie das Script ausführen, müssen Sie zwei Werte angeben, einen Wert für $1 und einen Wert für $2. Beispiel:

```
run sqlsample node_name aix
```

Der folgende Befehl wird verarbeitet, wenn das Script SQLSAMPLE ausgeführt wird:

```
select node_name from nodes where platform='aix'
```

Logikablaufanweisungen in ein Script einschließen

Sie können Ablaufanweisungen mit bedingter Logik verwenden, die auf Rückkehrcodes basieren, die bei der vorherigen Befehlsverarbeitung ausgegeben wurden. Mithilfe dieser Logikanweisungen können Sie Ihre Scripts gemäß dem Ergebnis bestimmter Befehle verarbeiten. Die Anweisungen IF, EXIT und GOTO (LABEL) können verwendet werden.

Bei der Verarbeitung der Befehle in einem Script wird der Rückkehrcode für eine mögliche Auswertung gesichert, bevor der nächste Befehl verarbeitet wird. Der Rückkehrcode kann eine der drei folgenden Bewertungsstufen haben: OK, WARNING oder ERROR. Eine Liste der gültigen Rückkehrcodes und Bewertungsstufen finden Sie in Rückkehrcodes für die Verwendung in Scripts.

- Klausel IF angeben
  Mit der Klausel IF am Anfang einer Befehlszeile kann bestimmt werden, wie die Verarbeitung des Scripts auf der Basis des aktuellen Rückkehrcodewertes fortgesetzt wird. In der Klausel IF wird ein symbolischer Wert oder eine Bewertung für einen Rückkehrcode angegeben.
- Anweisung EXIT angeben
  Verwenden Sie die Anweisung EXIT, um die Scriptverarbeitung zu beenden.
- Anweisung GOTO angeben
  Die Anweisung GOTO wird zusammen mit einer Kennzeichnungsanweisung verwendet. Die Kennzeichnungsanweisung ist das Ziel der Anweisung GOTO. Die Anweisung GOTO führt die Scriptverarbeitung zu der Zeile mit der Kennzeichnungsanweisung, damit die Verarbeitung an diesem Punkt wiederaufgenommen wird.

Klausel IF angeben

Mit der Klausel IF am Anfang einer Befehlszeile kann bestimmt werden, wie die Verarbeitung des Scripts auf der Basis des aktuellen Rückkehrcodewertes fortgesetzt wird. In der Klausel IF wird ein symbolischer Wert oder eine Bewertung für einen Rückkehrcode angegeben.

Informationen zu diesem Vorgang

Der Server setzt den Rückkehrcode am Anfang des Scripts anfänglich auf RC_OK. Der Rückkehrcode wird durch jeden verarbeiteten Befehl aktualisiert. Entspricht der aktuelle Rückkehrcode aus dem verarbeiteten Befehl einem der Rückkehrcodes oder einer der Bewertungen in der Klausel IF, wird der Rest der Zeile verarbeitet. Entspricht der aktuelle Rückkehrcode keinem der aufgelisteten Werte, wird die Zeile übersprungen.

Mit dem folgenden Beispielscript wird der Speicherpool BACKUPPOOL nur dann gesichert, wenn momentan keine Sitzungen auf den Server zugreifen. Die Sicherung wird nur dann fortgesetzt, wenn der Rückkehrcode RC_NOTFOUND empfangen wird:

```
/* Speicherpools sichern, wenn keine Clients auf den Server zugreifen */
select * from sessions
/* Keine Sitzungen vorhanden, wenn rc_notfound empfangen wird */
if(rc_notfound) backup stg backuppool copypool
```

Mit dem folgenden Beispielscript wird der Speicherpool BACKUPPOOL gesichert, wenn ein Rückkehrcode mit der Bewertung WARNING empfangen wird:

```
/* Speicherpools sichern, wenn keine Clients auf den Server zugreifen */
select * from sessions
/* Keine Sitzungen vorhanden, wenn rc_notfound empfangen wird */
if(warning) backup stg backuppool copypool
```

Anweisung EXIT angeben

Verwenden Sie die Anweisung EXIT, um die Scriptverarbeitung zu beenden.

Informationen zu diesem Vorgang

Im folgenden Beispiel wird mit der Klausel IF in Verbindung mit RC_OK festgestellt, ob Clients auf den Server zugreifen. Der Empfang des Rückkehrcodes RC_OK gibt an, dass Clientsitzungen auf den Server zugreifen. Das Script wird mit der Anweisung EXIT fortgesetzt und die Sicherung wird nicht gestartet.

```
/* Speicherpools sichern, wenn keine Clients auf den Server zugreifen */
select * from sessions
/* Sitzungen vorhanden, wenn rc_ok empfangen wird */
if(rc_ok) exit
backup stg backuppool copypool
```

Anweisung GOTO angeben

Die Anweisung GOTO wird zusammen mit einer Kennzeichnungsanweisung verwendet. Die Kennzeichnungsanweisung ist das Ziel der Anweisung GOTO. Die Anweisung GOTO führt die Scriptverarbeitung zu der Zeile mit der Kennzeichnungsanweisung, damit die Verarbeitung an diesem Punkt wiederaufgenommen wird.

Informationen zu diesem Vorgang

Hinter der Kennzeichnungsanweisung steht immer ein Doppelpunkt (:); hinter dem Doppelpunkt muss keine Angabe stehen. Das folgende Beispiel zeigt, wie mit der Anweisung GOTO ein Speicherpool nur dann gesichert wird, wenn momentan keine Sitzungen auf den Server zugreifen. In diesem Beispiel zeigt der Rückkehrcode RC_OK an, dass Clients auf den Server zugreifen. Die Anweisung GOTO überträgt die Verarbeitung an die Kennzeichnung `done:`, die die Anweisung EXIT enthält, mit der die Scriptverarbeitung beendet wird:

```
/* Speicherpools sichern, wenn keine Clients auf den Server zugreifen */
select * from sessions
/* Sitzungen vorhanden, wenn rc_ok empfangen wird */
if(rc_ok) goto done
backup stg backuppool copypool
done:exit
```

Befehle SELECT in einem Script verwenden

Ein IBM Spectrum Protect-Script besteht aus mindestens einem Befehl und wird als Objekt in der Datenbank gespeichert. Sie können ein Script definieren, das einen oder mehrere Befehle SELECT enthält.

Informationen zu diesem Vorgang

Ein Script kann über einen Verwaltungsclient oder über die Serverkonsole ausgeführt werden. Außerdem kann es einem Zeitplan für Verwaltungsbefehle hinzugefügt werden, damit es automatisch ausgeführt wird. Ausführliche Informationen befinden sich in Server-Scripts.

IBM Spectrum Protect wird mit einer Datei ausgeliefert, die eine Reihe von Beispielscripts enthält. Die Datei scripts.smp befindet sich im Serververzeichnis. Um die Scripts zu erstellen und als Objekte in Ihrer Serverdatenbank zu speichern, geben Sie den Befehl DSMSERV RUNFILE während der Installation aus:

```
> dsmserv runfile scripts.smp
```

Sie können die Datei auch als Makro über einen Verwaltungsbefehlszeilenclient ausführen:

```
macro scripts.smp
```

Die Datei mit den Beispielscripts enthält Befehle. Diese Befehle löschen zuerst alle Scripts mit denselben Namen wie die zu definierenden Scripts und definieren anschließend die Scripts. Die meisten Beispiele erstellen Befehle SELECT, andere sichern beispielsweise Speicherpools. Sie können die Datei mit den Beispielscripts auch kopieren und ändern, um eigene Scripts zu erstellen.

Nachfolgend sind einige Beispiele aus der Datei mit den Beispielscripts aufgeführt:

```
def script q_inactive_days '/* ------------------------------------------*/'
upd script q_inactive_days '/* Scriptname:   Q_INACTIVE                  */'
upd script q_inactive_days '/* Beschreibung: Knoten anzeigen, die für eine */'
upd script q_inactive_days '/*      bestimmte Anzahl Tage nicht auf den   */'
upd script q_inactive_days '/*      Sicherungsserver zugegriffen haben    */'
upd script q_inactive_days '/* Parameter 1: Tage                         */'
upd script q_inactive_days '/* Beispiel:    run q_inactive_days 5         */'
upd script q_inactive_days '/* ------------------------------------------*/'
upd script q_inactive_days "select node_name,lastacc_time from nodes where -"
upd script q_inactive_days "  cast((current_timestamp-lastacc_time)days as -"
upd script q_inactive_days " decimal) >= $1 "

/* Nachrichten mit Wertigkeit X oder Y im Aktivitätenprotokoll anzeigen   */

def script q_msg_sev desc='Nachr. mit Wertigk. X oder Y im Akt.-Prot. anz. '
upd script q_msg_sev '/* ------------------------------------------------*/'
upd script q_msg_sev '/* Scriptname:   Q_MSG_S EV                       */'
upd script q_msg_sev '/* Beschreibung: Nachrichten im Aktivitätenproto-  */'
upd script q_msg_sev '/*              koll mit einer der angegebenen    */'
upd script q_msg_sev '/*              Wertigkeiten anzeigen.            */'
upd script q_msg_sev '/* Parameter 1: Wertigkeit 1                      */'
upd script q_msg_sev '/* Parameter 2: Wertigkeit 2                      */'
upd script q_msg_sev '/*  Dabei ist Wertigkeit I, W, E, S oder D        */'
upd script q_msg_sev '/* Beispiel: run q_msg_sev S E                    */'
upd script q_msg_sev '/* ------------------------------------------------*/'
upd script q_msg_sev "select date_time,msgno,message from actlog -"
upd script q_msg_sev "  where severity=upper('$1') or severity=upper('$2')"
```

Script aktualisieren

Sie können ein Script aktualisieren, um eine Befehlszeile zu ändern oder einem Script eine Befehlszeile hinzuzufügen.

- Neuen Befehl anfügen
  Um einem vorhandenen Script eine Befehlszeile anzufügen, den Befehl UPDATE SCRIPT mit dem Parameter LINE= ausgeben. Der angefügten Befehlszeile wird eine um fünf größere Zeilennummer als der letzten Befehlszeile in der Befehlszeilenfolge zugeordnet. Wenn ein Script beispielsweise mit der Zeile 010 endet, wird der angefügten Befehlszeile die Zeilennummer 015 zugeordnet.
- Vorhandenen Befehl ersetzen
  Sie können eine vorhandene Befehlszeile ändern, indem Sie den Parameter LINE= angeben.
- Befehl und Zeilennummer hinzufügen
  Sie können ein vorhandenes Script ändern, indem Sie neue Zeilen hinzufügen.
- Befehl aus einem Server-Script löschen
  Aus einem Script kann eine einzelne Befehlszeile gelöscht werden. Wenn eine Zeilennummer angegeben wird, wird nur die entsprechende Befehlszeile aus dem Script gelöscht.

Neuen Befehl anfügen

Um einem vorhandenen Script eine Befehlszeile anzufügen, den Befehl UPDATE SCRIPT mit dem Parameter LINE= ausgeben. Der angefügten Befehlszeile wird eine um fünf größere Zeilennummer als der letzten Befehlszeile in der Befehlszeilenfolge zugeordnet. Wenn ein Script beispielsweise mit der Zeile 010 endet, wird der angefügten Befehlszeile die Zeilennummer 015 zugeordnet.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt das Script QSTATUS. Das Script hat die Zeilen 001, 005 und 010:

```
001 /* Dies ist das Script QSTATUS */
005  QUERY STATUS
010  QUERY PROCESS
```

Um den Befehl QUERY SESSION am Ende des Scripts anzufügen, geben Sie den folgenden Befehl aus:

```
update script qstatus "query session"
```

Dem Befehl QUERY SESSION wird die Befehlszeilennummer 015 zugeordnet; das aktualisierte Script sieht wie folgt aus:

```
001 /* Dies ist das Script QSTATUS */
005  QUERY STATUS
010  QUERY PROCESS
015  QUERY SESSION
```

Vorhandenen Befehl ersetzen

Sie können eine vorhandene Befehlszeile ändern, indem Sie den Parameter LINE= angeben.

Informationen zu diesem Vorgang

Zeilennummer 010 in dem Script QSTATUS enthält einen Befehl QUERY PROCESS. Um den Befehl QUERY PROCESS durch den Befehl QUERY STGPOOL zu ersetzen, geben Sie den Parameter LINE= wie folgt an:

```
update script qstatus "query stgpool" line=10
```

Das Script QSTATUS wird aktualisiert und enthält dann die folgenden Zeilen:

```
001 /* Dies ist das Script QSTATUS */
005  QUERY STATUS
010  QUERY STGPOOL
015  QUERY SESSION
```

Befehl und Zeilennummer hinzufügen

Sie können ein vorhandenes Script ändern, indem Sie neue Zeilen hinzufügen.

Informationen zu diesem Vorgang

Um dem Script QSTATUS den Befehl QUERY NODE OPEN als neue Zeile 007 hinzuzufügen, geben Sie den folgenden Befehl aus:

```
update script qstatus "query node" line=7
```

Das Script QSTATUS wird aktualisiert und enthält dann die folgenden Zeilen:

```
001 /* Dies ist das Script QSTATUS */
005 QUERY STATUS
007 QUERY NODE
010 QUERY STGPOOL
015 QUERY SESSION
```

Befehl aus einem Server-Script löschen

Aus einem Script kann eine einzelne Befehlszeile gelöscht werden. Wenn eine Zeilennummer angegeben wird, wird nur die entsprechende Befehlszeile aus dem Script gelöscht.

Informationen zu diesem Vorgang

Um beispielsweise die Befehlszeile 007 aus dem Script QSTATUS zu löschen, geben Sie den folgenden Befehl aus:

```
delete script qstatus line=7
```

Server-Script zum Erstellen eines anderen Server-Scripts abfragen

Sie können weitere Server-Scripts durch Abfragen eines Scripts unter Angabe der Parameter FORMAT=RAW und OUTPUTFILE erstellen. Die Ausgabe der Abfrage kann als Eingabe für ein neues Script verwendet werden, so dass das neue Script nicht zeilenweise erstellt werden muss.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt, wie das Script SRTL2 abgefragt und die Ausgabe in newscript.script übertragen wird:

```
query script srtl2 format=raw outputfile=newscript.script
```

Sie können die Datei newscript.script dann mit einem auf Ihrem System verfügbaren Editor editieren. Um ein neues Script mithilfe der editierten Ausgabe Ihrer Abfrage zu erstellen, geben Sie Folgendes aus:

```
define script srtnew file=newscript.script
```

Server-Script ausführen

Um ein Script zu verarbeiten, verwenden Sie den Befehl RUN. Sie können ein Script, das Substitutionsvariablen enthält, ausführen, indem Sie die Substitutionsvariablen im Befehl RUN angeben.

Informationen zu diesem Vorgang

Um ein Script zu stoppen, das gerade ausgeführt wird, muss ein Administrator den Server anhalten. Sie können ein Script nach seinem Start nicht mit einem IBM Spectrum Protect-Befehl abbrechen.

Vorgehensweise

- Rufen Sie eine Voranzeige der Befehle in einem Script auf, um das Script vor seiner Ausführung auszuwerten. Um die Voranzeige des Scripts aufzurufen, ohne die Befehle auszuführen, geben Sie den Befehl RUN mit dem Parameter PREVIEW=YES ein. Wenn das Script Substitutionsvariablen enthält, werden die Befehle mit den ersetzten Variablen angezeigt.
- Führen Sie ein Script, das keine Variablen enthält, durch Eingabe des folgenden Befehls aus: `run qaixc`; dabei ist `qaixc` der Name des Scripts.
- Führen Sie ein Script, das Substitutionsvariablen enthält, durch Angabe der Variablenwerte im Befehl aus. Inhalt des Scripts:

  ```
  /*---------------------------------------------*/
  /* Fortsetzungs- und Substitutionsbeispiel     */
  /* --------------------------------------------*/
  SELECT-
  $1 FROM-
  NODES WHERE-
  PLATFORM='$2'
  ```

  Um dieses Script auszuführen, geben Sie den folgenden Befehl ein:

  ```
  run qaixc Knotenname aix
  ```

  Dabei ist `Knotenname` der Wert für die Variable $1 und `aix` der Wert für die Variable $2.

Zugehörige Verweise:
RUN (Server-Script ausführen)

Makros des Verwaltungsclients

Ein Makro ist eine Datei, die mindestens einen Verwaltungsclientbefehl enthält. Sie können ein Makro vom Verwaltungsclient aus nur im Stapelmodus oder im interaktiven Modus ausführen. Makros werden als Datei auf dem Verwaltungsclient gespeichert. Sie werden nicht über Server verteilt und können nicht auf dem Server geplant werden.

Makros können die folgenden Elemente enthalten:

- Serververwaltungsbefehle
- Kommentare
- Fortsetzungszeichen
- Variablen

Der Name für ein Makro muss die Namenskonventionen des Verwaltungsclients erfüllen, der unter Ihrem Betriebssystem ausgeführt wird.

Verwenden Sie in einem Makro, das mehrere Befehle enthält, die Befehle COMMIT und ROLLBACK, um die Befehlsverarbeitung innerhalb des Makros zu steuern.

Sie können den Befehl MACRO in eine Makrodatei einschließen, um weitere Makros aufzurufen (bis zu 10 Ebenen sind möglich). Ein über die Befehlszeile des Verwaltungsclients aufgerufenes Makro wird als Makro höherer Ebene bezeichnet. Alle Makros, die innerhalb des Makros höherer Ebene aufgerufen werden, werden als *verschachtelte* Makros bezeichnet.

- Befehle in ein Makro schreiben
  Fügen sie einem Makro Verwaltungsbefehle hinzu. Der Verwaltungsclient ignoriert alle in Ihren Makros enthaltenen Leerzeilen. Ein Befehl, der (mit einem Fortsetzungszeichen) fortgesetzt wird, wird jedoch durch eine Leerzeile beendet.
- Kommentare in ein Makro schreiben
  Fügen Sie Ihrer Makrodatei Kommentare hinzu, um den Zweck oder die in der Datei enthaltenen Befehle zu beschreiben.
- Fortsetzungszeichen in ein Makro einschließen
  Sie können Fortsetzungszeichen in einer Makrodatei verwenden, wenn ein Befehl ausgeführt werden soll, der länger als die Anzeigen- oder Fensterbreite ist.

- Substitutionsvariablen in ein Makro einschließen
  Sie können Substitutionsvariablen in einem Makro verwenden, sodass Sie bei der Ausführung des Makros Werte für Elemente wie beispielsweise Befehlsparameter angeben können. Bei der Verwendung von Substitutionsvariablen kann ein Makro wiederholt zur Ausführung derselben Task für verschiedene Objekte oder mit unterschiedlichen Parameterwerten verwendet werden.
- Makro ausführen
  Verwenden Sie den Befehl MACRO, wenn ein Makro ausgeführt werden soll. Sie können den Befehl MACRO im Stapelmodus oder im interaktiven Modus eingeben.
- Befehlsverarbeitung in einem Makro
  Wenn Sie einen Befehl MACRO ausgeben, verarbeitet der Server nacheinander alle Befehle in der Makrodatei, einschließlich der Befehle, die in verschachtelten Makros enthalten sind. Der Server schreibt alle Befehle in einem Makro fest, nachdem die Verarbeitung der Makros höherer Ebene erfolgreich abgeschlossen wurde.

Befehle in ein Makro schreiben

Fügen sie einem Makro Verwaltungsbefehle hinzu. Der Verwaltungsclient ignoriert alle in Ihren Makros enthaltenen Leerzeilen. Ein Befehl, der (mit einem Fortsetzungszeichen) fortgesetzt wird, wird jedoch durch eine Leerzeile beendet.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt ein Makro mit dem Namen REG.MAC, das einen neuen Administrator registriert und ihm Berechtigungen erteilt:

```
register admin pease mypasswd -
  contact='david pease, x1234'
grant authority pease -
  classes=policy,storage -
  jdomains=domain1,domain2 -
  stgpools=stgpool1,stgpool2
```

Dieses Beispiel verwendet Fortsetzungszeichen in der Makrodatei. Weitere Informationen zu Fortsetzungszeichen befinden sich in Fortsetzungszeichen in ein Makro einschließen.

Nach der Erstellung einer Makrodatei können die darin enthaltenen Informationen aktualisiert werden, um sie erneut verwenden zu können. Sie können die Makrodatei auch kopieren. Nachdem Sie eine Kopie des Makros erstellt haben, können Sie die Kopie ändern und ausführen.

Kommentare in ein Makro schreiben

Fügen Sie Ihrer Makrodatei Kommentare hinzu, um den Zweck oder die in der Datei enthaltenen Befehle zu beschreiben.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um einen Kommentar zu schreiben:

- Schreiben Sie einen Schrägstrich und einen Stern (/*), um den Anfang des Kommentars anzugeben.
- Schreiben Sie den Kommentar.
- Schreiben Sie einen Stern und einen Schrägstrich (*/), um das Ende des Kommentars anzugeben.

Ein Kommentar kann auf einer eigenen Zeile oder auf einer Zeile stehen, die einen Befehl oder einen Teil eines Befehls enthält.

Um beispielsweise den Zweck eines Makros mithilfe eines Kommentars zu erläutern, geben Sie die folgende Zeile ein:

```
/* auth.mac - neue Knoten registrieren  */
```

Ein Kommentar kann auch verwendet werden, um einen Befehl oder einen Teil eines Befehls zu erläutern:

```
domain=domain1            /*Knoten domain1 zuordnen  */
```

Kommentare dürfen nicht verschachtelt werden und können sich nicht über mehrere Zeilen erstrecken. Jede Zeile eines Kommentars muss die Kommentarbegrenzer enthalten.

Fortsetzungszeichen in ein Makro einschließen

Sie können Fortsetzungszeichen in einer Makrodatei verwenden, wenn ein Befehl ausgeführt werden soll, der länger als die Anzeigen- oder Fensterbreite ist.

Informationen zu diesem Vorgang

Ohne Fortsetzungszeichen können bis zu 256 Zeichen eingegeben werden. Mit Fortsetzungszeichen können bis zu 1500 Zeichen eingegeben werden. Im Befehl MACRO werden Werte der Substitutionsvariablen bei der Anzahl Zeichen berücksichtigt.

Geben Sie als Fortsetzungszeichen einen Bindestrich oder einen umgekehrten Schrägstrich am Ende der fortzusetzenden Zeile ein. Mit Fortsetzungszeichen können Sie die folgenden Zeilen eines Makros fortsetzen.

Beispiele

- Befehl fortsetzen; Beispiel:

```
register admin pease mypasswd -
contact="david, ext1234"
```

- Eine Liste mit Werten durch einen Bindestrich oder einen umgekehrten Schrägstrich fortsetzen; dabei darf nach dem letzten Komma der Zeile, die auf der ersten Zeile begonnen wurde, kein Leerzeichen verwendet werden. Danach die restlichen Teile der Liste in die nächste Zeile eingeben, wobei die Zeile nicht mit Leerzeichen begonnen werden darf. In dem folgenden Beispiel wird eine Liste mit Speicherpoolnamen über mehrere Zeilen fortgesetzt:

```
stgpools=stg1,stg2,stg3,-
stg4,stg5,stg6
```

- Um eine Zeichenfolge aus Werten, die in Hochkommas oder Anführungszeichen eingeschlossen ist, fortzusetzen, schließen Sie den ersten Teil der Zeichenfolge in Hochkommas bzw. Anführungszeichen ein und geben Sie am Ende der Zeile einen Bindestrich oder einen umgekehrten Schrägstrich ein. Geben Sie dann den Rest der Zeichenfolge in die nächste Zeile ein. Schließen Sie den Rest der Zeichenfolge analog zum ersten Teil der Zeichenfolge in Hochkommas bzw. Anführungszeichen ein. Das folgende Beispiel zeigt eine Zeichenfolge, die über mehrere Zeilen fortgesetzt wird:

```
contact="david pease, bldg. 100, room 2b, san jose,"-
"ext. 1234, alternate contact-norm pass,ext 2345"
```

  Die beiden Zeichenfolgen werden ohne Zwischenleerschritte verkettet. Zum Fortsetzen einer in Hochkommas oder Anführungszeichen eingeschlossenen Zeichenfolge aus Werten über mehrere Zeilen darf nur diese Methode verwendet werden.

Substitutionsvariablen in ein Makro einschließen

Sie können Substitutionsvariablen in einem Makro verwenden, sodass Sie bei der Ausführung des Makros Werte für Elemente wie beispielsweise Befehlsparameter angeben können. Bei der Verwendung von Substitutionsvariablen kann ein Makro wiederholt zur Ausführung derselben Task für verschiedene Objekte oder mit unterschiedlichen Parameterwerten verwendet werden.

Informationen zu diesem Vorgang

Eine Substitutionsvariable besteht aus einem Prozentzeichen (%), gefolgt von einer eindeutigen Zahl, die die Substitutionsvariable angibt. Wenn Sie die Datei mit dem Befehl MACRO ausführen, müssen Sie für die Variablen Werte angeben.

Einschränkungen:

- Wenn Ihr System das Prozentzeichen als Platzhalterzeichen verwendet, interpretiert der Verwaltungsclient einen Mustererkennungsausdruck in einem Makro, bei dem auf das Prozentzeichen direkt eine Ziffer folgt, als Substitutionsvariable.
- Eine Substitutionsvariable kann nicht zwischen Anführungszeichen gesetzt werden. Ein Wert, den Sie als Substitution für die Variable angeben, kann jedoch eine Zeichenfolge in Anführungszeichen sein.

Beispiel

Erstellen Sie ein Makro mit dem Namen AUTH.MAC zum Registrieren neuer Knoten. Das Makro enthält vier Substitutionsvariablen für Parameter in dem Befehl:

```
/* neue Knoten registrieren */
register node %1 %2 -      /*  Benutzer-ID, Kennwort            */
  contact=%3 -             /* 'Name, Telefonnummer'             */
  domain=%4                /*  Maßnahmendomäne                  */
```

Wenn Sie das Makro ausführen, müssen Sie die Werte eingeben, die zur Verarbeitung des Befehls an den Server übergeben werden sollen.

Um beispielsweise das Makro zum Registrieren des Knotens mit dem Namen DAVID und dem Kennwort DAVIDPW zu verwenden, einen Namen und eine Telefonnummer als Kontaktinformationen einzuschließen und den Knoten der Maßnahmendomäne DOMAIN1 zuzuordnen, geben Sie den folgenden Befehl ein:

```
macro auth.mac david davidpw "david pease, x1234" domain1
```

Makro ausführen

Verwenden Sie den Befehl MACRO, wenn ein Makro ausgeführt werden soll. Sie können den Befehl MACRO im Stapelmodus oder im interaktiven Modus eingeben.

Informationen zu diesem Vorgang

Wenn das Makro keine Substitutionsvariablen enthält, führen Sie das Makro aus, indem Sie den Befehl MACRO zusammen mit dem Namen der Makrodatei eingeben. Beispiel:

```
macro reg.mac
```

Wenn das Makro Substitutionsvariablen enthält, geben Sie die bereitzustellenden Werte hinter dem Makronamen ein. Jeder Wert wird durch ein Leerzeichen begrenzt. Beispiel:

```
macro auth.mac pease mypasswd "david pease, x1234" domain1
```

Wenn weniger Werte eingegeben werden als Substitutionsvariablen im Makro vorhanden sind, ersetzt der Verwaltungsclient die restlichen Variablen durch Nullzeichenfolgen.

Wenn ein oder mehrere Werte zwischen Werten übergangen werden sollen, geben Sie für jeden übergangenen Wert eine Nullzeichenfolge ("") ein. Wenn beispielsweise die Kontaktinformationen aus dem vorhergehenden Beispiel übergangen werden sollen, folgendes eingeben:

```
macro auth.mac pease mypasswd "" domain1
```

Zugehörige Verweise:
MACRO (Makro aufrufen)

Befehlsverarbeitung in einem Makro

Wenn Sie einen Befehl MACRO ausgeben, verarbeitet der Server nacheinander alle Befehle in der Makrodatei, einschließlich der Befehle, die in verschachtelten Makros enthalten sind. Der Server schreibt alle Befehle in einem Makro fest, nachdem die Verarbeitung der Makros höherer Ebene erfolgreich abgeschlossen wurde.

Wenn in einem der Befehle in dem Makro oder in einem der verschachtelten Makros ein Fehler auftritt, stoppt der Server die Verarbeitung und macht alle Änderungen rückgängig, die durch alle vorhergehenden Befehle vorgenommen wurden.

Wenn Sie bei der Eingabe des Befehls DSMADMC die Option ITEMCOMMIT angeben, schreibt der Server jeden Befehl in einem Script oder einem Makro einzeln fest, nachdem die Verarbeitung für den jeweiligen Befehl erfolgreich abgeschlossen wurde. Wenn ein Fehler auftritt, setzt der Server die Verarbeitung fort und macht nur die Änderungen rückgängig, die durch den fehlgeschlagenen Befehl verursacht wurden.

Mit dem Befehl COMMIT können Sie präzise steuern, wann Befehle festgeschrieben werden. Wenn ein Fehler auftritt, während der Server die Befehle in einem Makro verarbeitet, beendet der Server die Verarbeitung des Makros und macht alle nicht festgeschriebenen Änderungen rückgängig. Nicht festgeschriebene Änderungen sind Befehle, die seit dem letzten Befehl COMMIT verarbeitet wurden. Stellen Sie sicher, dass Ihre Verwaltungsclientsitzung nicht mit der Option ITEMCOMMIT ausgeführt wird, wenn die Befehlsverarbeitung mit dem Befehl COMMIT gesteuert werden soll.

Sie können ein Makro vor seiner Implementierung mit dem Befehl ROLLBACK testen. Sie können die Befehle (mit Ausnahme des Befehls COMMIT), die ausgegeben werden sollen, in das Makro eingeben und ROLLBACK als letzten Befehl eingeben. Dann können Sie das Makro ausführen, um zu prüfen, ob alle Befehle erfolgreich verarbeitet werden. Alle Änderungen an der Datenbank, die durch die Befehle vorgenommen wurden, werden mit dem Befehl ROLLBACK rückgängig gemacht. Sie dürfen nicht vergessen, den Befehl ROLLBACK zu entfernen, bevor Sie das Makro zur Verwendung freigeben. Stellen Sie außerdem sicher, dass die Verwaltungsclientsitzung nicht mit der Option ITEMCOMMIT ausgeführt wird, wenn die Befehlsverarbeitung mit dem Befehl ROLLBACK gesteuert werden soll.

Tipp: Befehle, die Hintergrundprozesse starten, können nicht rückgängig gemacht werden.
Wenn eine Serie von Befehlen verwendet wird, die über die Befehlszeile erfolgreich ausgeführt werden, jedoch fehlschlagen, wenn sie in einem Makro ausgegeben werden, bestehen möglicherweise Abhängigkeiten zwischen den Befehlen. Es ist möglich, dass ein innerhalb eines Makros ausgegebener Befehl erst erfolgreich ausgeführt werden kann, wenn ein vorhergehender Befehl, der innerhalb desselben Makros ausgeführt wird, festgeschrieben wurde. Jede der beiden folgenden Aktionen ermöglicht die erfolgreiche Verarbeitung dieser Befehle innerhalb eines Makros:

- Fügen Sie einen Befehl COMMIT vor dem Befehl ein, der von einem vorherigen Befehl abhängig ist. Wenn beispielsweise COMMAND C von COMMAND B abhängig ist, würden Sie einen Befehl COMMIT vor COMMAND C einfügen.

  ```
  command a
  command b
  commit
  command c/
  ```

- Starten Sie die Verwaltungsclientsitzung unter Verwendung der Option ITEMCOMMIT. Diese Option hat zur Folge, dass jeder Befehl in einem Makro festgeschrieben wird, bevor der nächste Befehl verarbeitet wird.

Zugehörige Verweise:
COMMIT (Festschreiben von Befehlen in einem Makro steuern)
ROLLBACK (Nicht festgeschriebene Änderungen in einem Makro rückgängig machen)

Rückkehrcodes für die Verwendung in IBM Spectrum Protect-Scripts

Sie können IBM Spectrum Protect-Scripts schreiben, die Rückkehrcodes verwenden, um den Fortschritt der Scriptverarbeitung zu bestimmen. Die Rückkehrcodes können eine von drei Wertigkeiten haben: OK, WARNING, ERROR.

IBM Spectrum Protect-Scripts verwenden den symbolischen Rückkehrcode für die Verarbeitung, nicht den numerischen Wert. Der Verwaltungsclient zeigt die numerischen Werte an, wenn ein Befehl ausgeführt wird. Die Rückkehrcodes werden in der folgenden Tabelle angezeigt.

Tabelle 1. Rückkehrcodes

Rückkehrcode	**Wertigkeit**	**Numerischer Wert**	**Beschreibung**
RC_OK	OK	0	Der Befehl wurde erfolgreich ausgeführt.
RC_UNKNOWN	ERROR	2	Der Befehl wird nicht gefunden; kein bekannter Befehl.
RC_SYNTAX	ERROR	3	Der Befehl ist gültig, aber ein oder mehrere Parameter wurden nicht korrekt angegeben.
RC_ERROR	ERROR	4	Ein interner Serverfehler hat die erfolgreiche Ausführung des Befehls verhindert.
RC_NOMEMORY	ERROR	5	Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Speicher vorhanden ist.
RC_NOLOG	ERROR	6	Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Speicherbereich für das Wiederherstellungsprotokoll vorhanden ist.
RC_NODB	ERROR	7	Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Datenbankbereich vorhanden ist.
RC_NOSTORAGE	ERROR	8	Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Speicherbereich vorhanden ist.
RC_NOAUTH	ERROR	9	Der Befehl ist fehlgeschlagen, da der Administrator nicht berechtigt ist, den Befehl auszugeben.
RC_EXISTS	ERROR	10	Der Befehl ist fehlgeschlagen, da das angegebene Objekt bereits auf dem Server vorhanden ist.
RC_NOTFOUND	WARNING	11	Wird von einem Befehl QUERY oder SQL SELECT zurückgegeben, wenn keine Objekte gefunden werden, die den Spezifikationen entsprechen.
RC_INUSE	ERROR	12	Der Befehl ist fehlgeschlagen, da das Objekt, mit dem gearbeitet werden sollte, im Gebrauch war.
RC_ISREFERENCED	ERROR	13	Der Befehl ist fehlgeschlagen, da das Objekt, mit dem gearbeitet werden sollte, noch von einem anderen Serverkonstrukt referenziert wird.
RC_NOTAVAILABLE	ERROR	14	Der Befehl ist fehlgeschlagen, da das Objekt, mit dem gearbeitet werden sollte, nicht verfügbar ist.
RC_IOERROR	ERROR	15	Der Befehl ist fehlgeschlagen, da ein E/A-Fehler auf dem Server festgestellt wurde.
RC_NOTXN	ERROR	16	Der Befehl ist fehlgeschlagen, da eine Datenbanktransaktion auf dem Server fehlgeschlagen ist.
RC_NOLOCK	ERROR	17	Der Befehl ist fehlgeschlagen, da ein Sperrenkonflikt in der Serverdatenbank festgestellt wurde.
RC_NOTHREAD	ERROR	19	Der Befehl konnte nicht ausgeführt werden, da auf dem Server nicht genügend Speicher vorhanden ist.
RC_LICENSE	ERROR	20	Der Befehl ist fehlgeschlagen, da der Server die Lizenzierung nicht einhält.
RC_INVDEST	ERROR	21	Der Befehl ist fehlgeschlagen, da ein Zielwert ungültig war.
RC_IFILEOPEN	ERROR	22	Der Befehl ist fehlgeschlagen, da eine erforderliche Eingabedatei nicht geöffnet werden konnte.
RC_OFILEOPEN	ERROR	23	Der Befehl ist fehlgeschlagen, da er eine erforderliche Ausgabedatei nicht öffnen konnte.

Rückkehrcode	Wertigkeit	Numerischer Wert	Beschreibung
RC_OFILEWRITE	ERROR	24	Der Befehl ist fehlgeschlagen, da er nicht erfolgreich in eine erforderliche Ausgabedatei schreiben konnte.
RC_INVADMIN	ERROR	25	Der Befehl ist fehlgeschlagen, da der Administrator nicht definiert war.
RC_SQLERROR	ERROR	26	Ein SQL-Fehler wurde während der Abfrage einer Anweisung SELECT festgestellt.
RC_INVALIDUSE	ERROR	27	Der Befehl ist fehlgeschlagen, da er nicht korrekt verwendet wurde.
RC_NOTABLE	ERROR	28	Der Befehl ist aufgrund eines unbekannten SQL-Tabellennamens fehlgeschlagen.
RC_FS_NOTCAP	ERROR	29	Der Befehl ist aufgrund nicht kompatibler Typen des Dateibereichsnamens fehlgeschlagen.
RC_INVALIDADDR	ERROR	30	Der Befehl ist aufgrund einer falschen Adresse der höheren Ebene oder Adresse der unteren Ebene fehlgeschlagen.
RC_INVALIDCG	ERROR	31	Der Befehl ist fehlgeschlagen, da die Verwaltungsklasse keine Archivierungskopiengruppe hat.
RC_OVERSIZE_VOL	ERROR	32	Der Befehl ist fehlgeschlagen, da die Datenträgergröße den maximal zulässigen Wert überschreitet.
RC_DEFVOL_FAIL	ERROR	33	Der Befehl ist fehlgeschlagen, da Datenträger nicht in Speicherpools mit RECLAMATIONTYPE=SNAPLOCK definiert werden können.
RC_DELVOL_FAIL	ERROR	34	Der Befehl ist fehlgeschlagen, da Datenträger nicht in Speicherpools mit RECLAMATIONTYPE=SNAPLOCK gelöscht werden können.
RC_CANCELED	WARNING	35	Der Befehl wurde abgebrochen.
RC_INVPOLICY	ERROR	36	Der Befehl ist fehlgeschlagen, da die Maßnahmendomäne eine ungültige Definition enthält.
RC_INVALIDPW	ERROR	37	Der Befehl ist aufgrund eines ungültigen Kennworts fehlgeschlagen.
RC_UNSUPP_PARM	WARNING	38	Der Befehl ist fehlgeschlagen, da der Befehl oder der Parameter nicht unterstützt wird.

Zugehörige Verweise:
DEFINE SCRIPT (IBM Spectrum Protect-Prozedur definieren)
UPDATE SCRIPT (IBM Spectrum Protect-Prozedur aktualisieren)
RUN (IBM Spectrum Protect-Prozedur ausführen)

Serverdokumentation in PDF-Dateien

Vorgefertigte PDF-Dateien für die IBM Spectrum Protect-Dokumentation sind zum Herunterladen verfügbar.

Tipp: Ab Version 7.1.3 ist das *Administratorhandbuch* veraltet. Verwenden Sie die Handbücher für Speicherlösungen, um eine Plattenspeicherlösung für einen einzelnen Standort und eine Plattenspeicherlösung für mehrere Standorte zu implementieren und zu verwalten. Prozeduren für die Ausführung von Systemverwaltungstasks sind in den folgenden Abschnitten verfügbar:

- Speicherumgebung konfigurieren und verwalten
- IBM Spectrum Protect-Datenschutzlösungen

Verwenden Sie für die Ausführung der folgenden Tasks die PDF-Dateien in den folgenden Links.

Task	Komponenten	Links
Informationen zu Produktkonzepten und -lösungen lesen	• Server • Operations Center	Einführung in Datenschutzlösungen
Best-Practice-Lösung implementieren	• Server • Operations Center	• Plattenspeicherlösung für einen einzelnen Standort • Plattenspeicherlösung für mehrere Standorte • Bandspeicherlösung

Task	Komponenten	Links
Komponenten installieren	• Server • Operations Center	• AIX • Linux • Windows
Upgrade für Komponenten durchführen	• Server	• AIX • Linux • Windows
Befehle und Optionen verwenden	• Server	• AIX • Linux • Windows
Nachrichten und Fehlercodes verwenden	• Server	Alle Betriebssysteme

IBM Spectrum Protect-Clients für Sichern/Archivieren

Verwenden Sie den IBM Spectrum Protect-Client für Sichern/Archivieren, um Kopien von Dateien und Verzeichnissen auf Workstations zu sichern und die Daten auf dem IBM Spectrum Protect-Server zu speichern. Sie können diese Kopien bei einer Beschädigung oder einem Verlust der Originaldateien wiederherstellen. Je nach Zweck der Datenspeicherung können Sie die Daten entweder sichern oder archivieren.

- Neuerungen für IBM Spectrum Protect-Clients für Sichern/Archivieren
  Enthält Informationen zu neuen und geänderten Funktionen. Lesen Sie vor der Installation des Produkts die Releaseinformationen.
- Schutz für Workstations und Dateiserver
  IBM Spectrum Protect ist ein Client/Server-Lizenzprodukt, das Speicherverwaltungsservices in einer plattformübergreifenden Computerumgebung zur Verfügung stellt.
- IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
  Mit dem IBM Spectrum Protect-Client für Sichern/Archivieren können Sie die Informationen auf Ihren Workstations schützen.
- Clients für Sichern/Archivieren konfigurieren
  Sie können den Client für Sichern/Archivieren für die Verwendung zahlreicher verfügbarer Clientfunktionen konfigurieren. Informationen zur Konfiguration des Clients für Sichern/Archivieren werden bereitgestellt.
- Daten mit Clients für Sichern/Archivieren sichern und zurückschreiben
  Wenn Sie eine Kopie einer Datei von Ihrem Computer auf dem IBM Spectrum Protect-Server sichern wollen, verwenden Sie die Funktion *Sichern*. Falls die Originaldatei beschädigt wird oder verloren geht, können Sie die Sicherungsversion vom Server *zurückschreiben*.
- Daten mit Clients für Sichern/Archivieren archivieren und abrufen
  Wenn Sie eine Kopie einer Datei zur Langzeitspeicherung oder Archivierung auf dem IBM Spectrum Protect-Server speichern wollen, verwenden Sie die Funktion *Archivieren*.
- Operationen für Clients für Sichern/Archivieren planen
  Sie können Sicherungsoperationen zum Schützen von Clientdaten planen, um sicherzustellen, dass sie regelmäßig ausgeführt werden.
- Speicherverwaltungsmaßnahmen
  Speicherverwaltungsmaßnahmen sind vom Administrator definierte Regeln für die Verwaltung der Sicherungen und Archivierungen auf dem Server.
- Optionen und Befehle des Clients für Sichern/Archivieren
  Verwenden Sie die Clientoptionen, um die Verarbeitung des Clients für Sichern/Archivieren an Ihre Anforderungen anzupassen. Verwenden Sie die Befehlszeilenschnittstelle (CLI - Command-Line Interface) des Clients als Alternative zu der grafischen Benutzerschnittstelle (GUI - Graphical User-Interface). Referenzinformationen für die Clientoptionen und die Clientbefehle sowie ergänzende Informationen werden bereitgestellt.
- ANS-Nachrichten 0000-9999

Zugehörige Tasks:
Lösungen mit der Anwendungsprogrammierschnittstelle entwickeln
Zugehörige Verweise:
Druckbare PDF-Dateien

Neuerungen für IBM Spectrum Protect-Clients für Sichern/Archivieren

Enthält Informationen zu neuen und geänderten Funktionen. Lesen Sie vor der Installation des Produkts die Releaseinformationen.

- Aktualisierungen für den Client für Sichern/Archivieren
  Informieren Sie sich über neue Funktionen und Aktualisierungen für den Client für Sichern/Archivieren in IBM Spectrum Protect Version 8.1.
- Releaseinformationen für IBM Spectrum Protect Client für Sichern/Archivieren Version 8.1
  Der IBM Spectrum Protect Client für Sichern/Archivieren Version 8.1 ist verfügbar. Dieses Dokument enthält wichtige Installationsinformationen. Außerdem finden Sie in diesem Dokument Produktaktualisierungen, Kompatibilitätsanforderungen, Einschränkungen und bekannte Probleme.

- Readme-Dateien für Fixpacks des Clients für Sichern/Archivieren von IBM Spectrum Protect Version 8.1
  Readme-Dateien für die Fixpacks des Clients für Sichern/Archivieren von IBM Spectrum Protect Version 8.1 sind in IBM Support Knowledge Base verfügbar, wenn es ein Fixpack-Update gibt.
- Nachträgliche aktuelle Dokumentationsaktualisierungen
  Aktualisierungen der Dokumentation für den IBM Spectrum Protect-Client für Sichern/Archivieren können nach der Veröffentlichung der Dokumentation im IBM® Knowledge Center auftreten.

Aktualisierungen für den Client für Sichern/Archivieren

Informieren Sie sich über neue Funktionen und Aktualisierungen für den Client für Sichern/Archivieren in IBM Spectrum Protect Version 8.1.

Release	Neue Funktionen und Aktualisierungen
8.1.2	Client mit erweiterten Sicherheitseinstellungen schützen Ab IBM Spectrum Protect Version 8.1.2 werden im Client für Sichern/Archivieren mehrere Änderungen eingeführt, um eine Zusammenarbeit mit dem IBM Spectrum Protect-Server der Version 8.1.2 zu ermöglichen, der Erweiterungen zur Verbesserung der Sicherheit für die Kommunikation zwischen Client und Server bereitstellt. Nach dem Upgrade des IBM Spectrum Protect-Servers auf Version 8.1.2, der Konfiguration dieses Servers mit dem verbesserten Sicherheitsprotokoll und dem Upgrade des Clients für Sichern/Archivieren auf Version 8.1.2 müssen die Sicherheitseinstellungen für den Client so konfiguriert werden, dass eine Zusammenarbeit mit den Sicherheitserweiterungen auf dem Server möglich ist. Weitere Informationen zur Konfiguration des Clients für verschiedene Sicherheitsszenarios finden Sie in Clientsicherheitseinstellungen für eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 und höher konfigurieren. Die folgenden Änderungen sind in diesem Release verfügbar: Neue Option sslacceptcertfromserv, Änderungen an drei vorhandenen SSL-bezogenen Optionen Zur Vereinfachung des Verteilungsprozesses für Serverzertifikate verfügt IBM Spectrum Protect jetzt über eine neue Option sslacceptcertfromserv, die steuert, ob der Client für Sichern/Archivieren oder die API-Anwendung das öffentliche SSL-Zertifikat des IBM Spectrum Protect-Servers akzeptiert und als vertrauenswürdig anerkennt, wenn das erste Mal eine Verbindung zwischen ihnen hergestellt wird. Darüber hinaus haben sich drei SSL-bezogene Optionen, ssl, ssldisablelegacytls und sslarequired, geändert. Ihre Funktionsweise ist davon abhängig, ob die Ausführung mit dem IBM Spectrum Protect-Server der Version 8.1.2 oder mit dem IBM Spectrum Protect-Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Versionen erfolgt. Eine Beschreibung dieser Optionseinstellungen und wichtige Versionsinformationen finden Sie in Sslacceptcertfromserv, Ssl, Ssldisablelegacytls und Sslrequired. Änderung der Position des IBM Spectrum Protect-Kennworts Ab Version 8.1.2 werden alle IBM Spectrum Protect-Kennwörter in den Schlüsselspeichern von IBM® Global Security Kit (GSKit) gespeichert. Wenn Sie ein Upgrade des Clients für Sichern/Archivieren auf IBM Spectrum Protect Version 8.1.2 durchführen, werden die vorhandenen Kennwörter automatisch an neue Positionen auf dem Clientsystem migriert. Weitere Informationen zur neuen Kennwortposition und zugehörige Hinweise finden Sie in Sicherer Kennwortspeicher. Mit dem Dienstprogramm dsmcert steht eine neue Methode zum Importieren von Serverzertifikaten zur Verfügung. Informationen zum Importieren von Serverzertifikaten finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren. Wegen der Verwendung des neuen sicheren Kennwortspeichers stehen neue Prozeduren zur Erteilung der Kennwortzugriffsberechtigung für Benutzer ohne Verwaltungsaufgaben zur Verfügung. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeFür UNIX- und Linux-Clients: Benutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen. Windows-BetriebssystemeFür Windows-Clients: Operationen des Clients für Sichern/Archivieren und Sicherheitsberechtigungen. Aktualisierungen des Clients für Sichern/Archivieren automatisch implementieren Der Administrator des IBM Spectrum Protect-Servers kann Aktualisierungen für mindestens einen Client für Sichern/Archivieren mithilfe von Serverbefehlen planen. Die Aktualisierungen können Fixpacks oder neue Releases sein. Diese Funktion war bereits in früheren Releases von IBM Spectrum Protect verfügbar, in Version 8.1.2 steht jedoch eine verbesserte Prozedur zur Verfügung. Weitere Informationen finden Sie in Automatische Aktualisierungen für Clients für Sichern/Archivieren planen. Nicht weiter unterstützte Funktionen

Release	Neue Funktionen und Aktualisierungen
	Die folgenden Funktionen werden in diesem Release nicht weiter unterstützt: Optionen lanfreessl und replsslport Zwei SSL-bezogene Optionen, lanfreessl und replsslport, werden nicht mehr unterstützt und sind nicht verfügbar, wenn Sie die Verbindung zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen. Diese Optionen sind weiterhin gültig und verfügbar, wenn Sie die Verbindung zu einem IBM Spectrum Protect-Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Versionen herstellen. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeTrusted Communication Agent (TCA) AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeDer bisher von Benutzern ohne Rootberechtigung in Version 8.1.0 und 7.1.6 und älteren Clients verwendete Trusted Communication Agent (TCA) ist nicht mehr verfügbar. Rootbenutzer können Benutzern ohne Rootberechtigung die Verwaltung ihrer Dateien mit anderen Methoden ermöglichen. Weitere Informationen finden Sie in: • Trusted Communication Agent nicht mehr verfügbar • Benutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen IBM Spectrum Protect-Web-Client Sie können nicht mehr den Web-Client verwenden, um eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder einer höheren Version herzustellen. Sie können den Web-Client jedoch weiterhin verwenden, um eine Verbindung zu Servern mit IBM Spectrum Protect Version 8.1.1, Version 8.1.0, Version 7.1.7 oder früheren Versionen herzustellen. Weitere Informationen finden Sie in Web-Client in neuer Sicherheitsumgebung verwenden. AIX-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeNDMP-Befehlszeilen- und -Web-Client-Operationen AIX-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeWenn Sie eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder einer höheren Version herstellen, können nicht mehr die Clientbefehlszeilenschnittstelle oder den Web-Client verwenden, um NAS-Dateiserver unter Verwendung von NDMP (Network Data Management Protocol) zu sichern oder zurückzuschreiben. Um NDMP-Daten zurückzuschreiben, können Sie alternativ IBM Spectrum Protect-Serverbefehle mit dem Verwaltungsbefehlszeilenclient (dsmadmc) verwenden. Weitere Informationen zu NDMP finden Sie in Web-Client in neuer Sicherheitsumgebung verwenden. Offene Registrierung Die Funktion für offene Registrierung ist nicht mehr verfügbar, wenn der Client eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder einer höheren Version herstellt. Sie müssen die geschlossene Registrierung verwenden, um eine Verbindung zum IBM Spectrum Protect-Server herzustellen. Weitere Informationen finden Sie in Geschlossene Registrierung. Die offene Registrierung ist weiterhin verfügbar, wenn der Client eine Verbindung zu Servern mit IBM Spectrum Protect Version 8.1.1, 8.1.0, 7.1.7 oder früheren Versionen herstellt. Weitere Informationen zu Verbesserungen der Sicherheit finden Sie in Speicherumgebung mit einem verbesserten Sicherheitsprotokoll schützen. Windows-BetriebssystemeErweiterte Unterstützung für Data Protection for Microsoft Hyper-V bei der Ausführung unter Windows Server 2016 Windows-Betriebssysteme Sichern virtueller Maschinen mithilfe von Resilient Change Tracking (RCT) Um die Skalierbarkeit und Leistung bei der Sicherung virtueller Maschinen (VMs) zu verbessern, wird Resilient Change Tracking (RCT) für alle VM-Sicherungsoperationen von Hyper-V-Hosts verwendet, die unter dem Betriebssystem Microsoft Windows Server 2016 ausgeführt werden. Weitere Informationen finden Sie in Sicherungen virtueller Maschinen mit Resilient Change Tracking (RCT). Windows-Betriebssysteme Bessere Steuerung von Sicherungsoperationen auf virtuellen Maschinen (VMs) mit physischen Platten Sie können steuern, ob VM-Gesamtsicherungen mithilfe von Hyper-V RCT verarbeitet werden, wenn für die VM eine oder mehrere physische Platten (Durchgriffsplatten) bereitgestellt werden. Weitere Informationen liefern die folgenden Optionen: • Vmprocessvmwithphysdisks • Vmskipphysdisks Angabe der Anzahl Versuche zur Erstellung einer Momentaufnahme und Angabe der Datenkonsistenzebene für Sicherungsoperationen Um die Gesamtzahl Versuche zur Erstellung einer Momentaufnahme für eine virtuelle Maschine, die aufgrund eines Momentaufnahmefehlers während der Sicherungsverarbeitung fehlschlägt, zu bestimmen, verwenden Sie

Release	Neue Funktionen und Aktualisierungen
	die Option INCLUDE.VMSNAPSHOTATTEMPTS. Sie können wählen, ob anwendungskonsistente oder absturzkonsistente Momentaufnahmen erstellt werden sollen. Weitere Informationen finden Sie in INCLUDE.VMSNAPSHOTATTEMPTS. Ausschluss von VM-Platten aus Sicherungsoperationen oder Einschluss von VM-Platten in Sicherungsoperationen Mithilfe der Option exclude.vmdisk können Sie eine VM-Platte (VHDX) von VM-Sicherungsoperationen ausschließen; mithilfe der Option include.vmdisk können Sie eine VM-Platte in VM-Sicherungsoperationen einschließen. Weitere Informationen finden Sie in den folgenden Abschnitten: • Exclude.vmdisk • Include.vmdisk • Domain.vmfull • Backup VM  Windows-BetriebssystemeErweiterte Unterstützung für Data Protection for Microsoft Hyper-V bei der Ausführung unter Windows Server 2012 und 2012 R2  Windows-Betriebssysteme Verbesserte Skalierbarkeit und Zuverlässigkeit von VM-Sicherungen VMs werden logisch in eine einzige Momentaufnahme gruppiert, um Momentaufnahmekonflikte auf der Hyper-V-Host-Ebene zu reduzieren oder zu eliminieren. Die verbesserte Verarbeitung der Wiederholungsversuche für eine Momentaufnahmeoperation vereinfacht die Planung und verbessert die Zuverlässigkeit clusterknotenübergreifend. • Um steuern zu können, wie viele VMs in eine Momentaufnahme eingeschlossen werden sollen, verwenden Sie die Option vmmaxpersnapshot. Weitere Informationen finden Sie in Vmmaxpersnapshot. • Um steuern zu können, wie viele Wiederholungsversuche für eine Momentaufnahmeoperation ausgeführt werden, verwenden Sie die Option vmmaxsnapshotretry. Weitere Informationen finden Sie in Vmmaxsnapshotretry. Mithilfe dieser Verbesserungen zur Gruppierung und Wiederholung in Kombination mit der Option vmmaxparallel kann die Leistung verbessert werden. Informationen finden Sie in Geplante VM-Sicherungen für Windows Server 2012- und 2012 R2-Cluster optimieren.  Linux-Betriebssysteme  Windows-BetriebssystemeErweiterte Unterstützung für virtuelle Datenträger (VVOL)  Linux-Betriebssysteme  Windows-BetriebssystemeDie VVOL-Unterstützung wurde erweitert, um die Unterstützung für Momentaufnahmen, die Hardwarespeicher gespeichert sind, und Anwendungsschutz einzuschließen. Weitere Informationen zu neuen Features zur VVOL-Unterstützung finden Sie in Updates für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware. Um die erweiterten VVOL-Features verwenden zu können, verwenden Sie die in den folgenden Abschnitten beschriebenen Optionen: Geben Sie die Position für Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen an: LOCAL, SERVER oder BOTH. Für virtuelle Maschinen, die sich in VVOL-Datenspeichern befinden, können Sie jetzt eine der folgenden Sicherungspositionen für Sicherungs- und Zurückschreibungsoperationen angeben: LOCAL, SERVER oder BOTH. Eine lokale Sicherung ist eine im Hardwarespeicher gespeicherte Momentaufnahme. Geben Sie die Sicherungsposition für den Befehl Backup VM oder Restore VM mithilfe der Option vmbackuplocation an. Weitere Informationen finden Sie in Vmbackuplocation. Sie können die Sicherungsposition oder -positionen, die abgefragt werden sollen, auch bei der Ausführung des Befehls Query VM angeben. Weitere Informationen finden Sie in Query VM. Die Tags der Kategorie "Local Backup Management (IBM Spectrum Protect)" sind für lokale Sicherungen verfügbar. Weitere Informationen finden Sie in Unterstützte Datenschutztags. Erstellung einer Zeitplangruppe Sie können die Option schedgroup verwenden, um eine Gruppe zu erstellen, die mehrere Zeitpläne enthält. Mithilfe des IBM Spectrum Protect vSphere-Client-Plug-ins können Sie dann statt eines einzigen Zeitplans die Zeitplangruppe einem Objekt im VMware vSphere-Web-Client zuordnen. Ein Beispiel für die Verwendung dieser Option ist die Gruppierung mehrerer Zeitpläne zur täglichen lokalen Sicherung in einem einzigen Zeitplan zur Sicherung des IBM Spectrum Protect-Servers. Weitere Informationen finden Sie in Schedgroup.  Linux-Betriebssysteme  Windows-BetriebssystemeGleichzeitige Zurückschreibung mehrerer virtueller Platten  Linux-Betriebssysteme  Windows-BetriebssystemeMithilfe des IBM Spectrum Protect-Clients können Sie mehrere virtuellen Platten gleichzeitig unter den Microsoft Windows- und Linux-Betriebssystemen zurückschreiben, indem Sie

Release	Neue Funktionen und Aktualisierungen
	die Option vmmaxrestoreparalleldisks verwenden. Anweisungen zum Festlegen der Optionseinstellungen finden Sie in Vmmaxrestoreparalleldisks.  Linux-Betriebssysteme  Windows-BetriebssystemeHinzufügen der Clientoption snapdiffchangelogdir für Momentaufnahmedifferenzsicherungsoperationen  Linux-Betriebssysteme  Windows-BetriebssystemeMomentaufnahmedifferenzsicherungen verwenden nicht mehr die Option stagingdirectory zum Speichern von Änderungsprotokolldateien für Momentaufnahmedifferenzsicherungen. Verwenden Sie ab Version 8.1.2 die neue Option snapdiffchangelogdir zur Angabe der Position, an der der Client persistente Änderungsprotokolle für Momentaufnahmedifferenzsicherungen speichert. Eine Beschreibung der Optionseinstellungen und wichtige Informationen zur Migration von früheren Clientversionen finden Sie in Snapdiffchangelogdir.
8.1.0	IBM Tivoli Storage Manager ist jetzt IBM Spectrum Protect IBM Spectrum Protect Version 8.1 ist die nächste Generation von Tivoli Storage Manager. Dieses neue Release stellt mehr als eine Namensänderung in der Benutzerschnittstelle und der Dokumentation dar. Es ist die Weiterentwicklung zu einer höheren Ebene des Datenschutzes mit dem Ziel, die komplexen Anforderungen der heutigen Zeit zu erfüllen. Weitere Informationen finden Sie in Lernen Sie IBM Spectrum Protect kennen. Eine Benutzer-ID mit Administratorberechtigung wird mit dem Serverbefehl REGISTER NODE nicht mehr standardmäßig erstellt Ab IBM Spectrum Protect Version 8.1 wird mit dem Serverbefehl REGISTER NODE nicht automatisch eine Benutzer-ID mit Administratorberechtigung erstellt, die mit dem Knotennamen übereinstimmt. Diese Produktaktualisierung dient zur Optimierung der Benutzerauthentifizierung bei einem Lightweight Directory Access Protocol-Server (LDAP-Server). Diese Produktaktualisierung hat keine Auswirkungen auf vorhandene Clientknoten, kann sich jedoch auf den Prozess der Registrierung neuer Clientknoten, einschließlich Knoten für IBM Spectrum Protect-Clients für Sichern/Archivieren, auswirken. In einigen Fällen müssen Sie unter Umständen eine Benutzer-ID mit Administratorberechtigung erstellen, wenn Sie einen Knoten registrieren. Sie können die Benutzer-ID mit Administratorberechtigung erstellen, indem Sie den Befehl REGISTER NODE unter Angabe des Parameters USERID ausgeben. Informationen zu den betroffenen Clienttypen finden Sie in Technote 7048963. Wenn Sie planen, den Web-Client zu verwenden, müssen Sie manuell eine Benutzer-ID mit Administratorberechtigung erstellen, wenn Sie einen neuen Knoten registrieren. Weitere Informationen finden Sie in Workstation bei einem Server registrieren. Ausführung des Web-Clients unabhängig vom Web-Browser Anstatt den IBM Spectrum Protect-Web-Client als Java™-Applet auszuführen, wird der Web-Client als Java Web Start-Anwendung bereitgestellt, die unabhängig vom Web-Browser gestartet und verwaltet werden kann. Weitere Informationen zum Starten des Web-Clients finden Sie in Web-Client-Sitzung starten.  Linux-Betriebssysteme  Windows-BetriebssystemeErweiterungen des Sicherungsmanagements, einschließlich neuer Datenschutztags, die für die Tagging-Unterstützung verfügbar sind  Linux-Betriebssysteme  Windows-Betriebssysteme Neue Datenschutztags sind für die Tagging-Unterstützung verfügbar Es wurden neue Datenschutztags hinzugefügt, um Sie bei der Verwaltung von Sicherungsoperationen für virtuelle Maschinen mit dem IBM Spectrum Protect vSphere-Client-Plug-in im VMware vSphere-Web-Client zu unterstützen. Zusätzlich zur Verwendung von Tags zum Ausschließen virtueller Maschinen von geplanten Sicherungsoperationen und zum Zuordnen von Aufbewahrung oder Verwaltungsklassen, die in Version 7.1.6 eingeführt wurden, können Sie die neuen Tags vSphere-Bestandsobjekten zuordnen, um die folgenden Tasks auszuführen: • Einschließen virtueller Maschinen in geplante Sicherungsoperationen • Zuordnen einer Einheit zum Versetzen von Daten zu einer virtuellen Maschine • Angabe einer Liste zu sichernder virtueller Platten • Zuordnen eines Sicherungszeitplans zu virtuellen Maschinen in einem Container • Angabe der Datenkonsistenz, die für Versuche zur Erstellung von Momentaufnahmen während Sicherungsoperationen für virtuelle Maschinen erzielt werden soll • Bereitstellung von Anwendungsschutz für virtuelle Maschinen, auf denen Microsoft SQL Server- oder Microsoft Exchange Server-Software ausgeführt wird Weitere Informationen finden Sie in Unterstützte Datenschutztags. Festlegen einer Standardeinheit zum Versetzen von Daten für das Tagging Sie können eine Standardeinheit zum Versetzen von Daten festlegen, um virtuelle Maschinen in vSphere-Bestandsobjekten, die mit Datenschutztags versehen sind, zu schützen. Neue virtuelle Maschinen, die dem mit

Release	Neue Funktionen und Aktualisierungen
	Tags versehenen Container hinzugefügt werden und mithilfe eines Zeitplans geschützt werden, aber über keinen Tag für Einheiten zum Versetzen von Daten verfügen, werden mit der Standardeinheit zum Versetzen von Daten gesichert. Weitere Informationen finden Sie in Vmtagdefaultdatamover. Erben von Datenschutztags von vSphere-Bestandsobjekten höherer Ebene Mithilfe der Tagvererbung können Sie den Datenschutz für virtuelle Maschinen im vSphere-Bestand verwalten. Weitere Informationen finden Sie in Vererbung von Datenschutzeinstellungen. Virtuelle Maschinen können einem Sicherungszeitplan mithilfe des IBM Spectrum Protect vSphere-Client-Plug-ins hinzugefügt werden Sie können einen Sicherungszeitplan für virtuelle Maschinen aus dem IBM Spectrum Protect vSphere-Client-Plug-in im VMware vSphere-Web-Client auswählen. Der Sicherungszeitplan gibt an, wie oft und wann die virtuellen Maschinen in einem vSphere-Bestandsobjekt automatisch gesichert werden sollen. Weitere Informationen finden Sie in Zeitplan zum Sichern virtueller Maschinen auswählen. Es ist auch möglich, Sicherungszeitpläne über das IBM Spectrum Protect vSphere-Client-Plug-in anzuzeigen und zu verwalten. Weitere Informationen finden Sie in Sicherungszeitpläne in vCenter verwalten. Linux-BetriebssystemeWindows-BetriebssystemeKeine weitere Unterstützung von Momentaufnahmedifferenzsicherungen unter AIX Linux-BetriebssystemeWindows-BetriebssystemeEs ist nicht mehr möglich, Momentaufnahmedifferenzsicherungen von NetApp-Dateiserverdatenträgern auf dem Client für Sichern/Archivieren unter dem Betriebssystem IBM AIX auszuführen. Die Ausführung von Momentaufnahmedifferenzsicherungen ist nur auf Linux- und Microsoft Windows-Clients möglich. Nicht weiterverwendete Funktionen Die folgenden Funktionen werden in diesem Release nicht weiterverwendet: Linux-BetriebssystemeWindows-BetriebssystemeOperationen für virtuelle Maschinen auf dem Client für Sichern/Archivieren Linux-BetriebssystemeWindows-BetriebssystemeOperationen für virtuelle Maschinen sind nur verfügbar, wenn Sie den Client als Einheit zum Versetzen von Daten für die IBM Spectrum Protect for Virtual Environments-Produkte (Data Protection for VMware oder Data Protection for Microsoft Hyper-V) verwenden. Es ist nicht mehr möglich, Operationen für virtuelle Maschinen auszuführen, ohne IBM Spectrum Protect for Virtual Environments zu installieren. Linux-BetriebssystemeWindows-BetriebssystemeVMware vStorage-API ist nicht mehr Teil der Clientinstallation Linux-BetriebssystemeWindows-BetriebssystemeDie Komponente 'VMware vStorage-API-Laufzeitdateien', die für VMware-Operationen verwendet wird, ist nicht mehr Teil der Installation des Clients für Sichern/Archivieren. Sie wird als Teil des Data Protection for VMware-Installationspakets installiert. Linux-BetriebssystemeWindows-BetriebssystemeOperationen für virtuelle Maschinen, die für die Einheit zum Versetzen von Daten nicht weiterverwendet werden Linux-BetriebssystemeWindows-Betriebssysteme Sicherungen virtueller Maschinen auf Dateiebene Es ist nicht mehr möglich, Sicherungen virtueller VMware-Maschinen auf Dateiebene auf der Einheit zum Versetzen von Daten auszuführen. Verwenden Sie stattdessen immer inkrementelle Gesamtsicherungs- oder immer inkrementelle Teilsicherungsoperationen. Regelmäßige Gesamtsicherungen und Teilsicherungen Es ist nicht mehr möglich, regelmäßige Gesamtsicherungen und Teilsicherungen virtueller Maschinen auf der Einheit zum Versetzen von Daten auszuführen. Verwenden Sie stattdessen immer inkrementelle Gesamtsicherungs- oder immer inkrementelle Teilsicherungsoperationen. Unterstützung für VMware vCloud Director Es ist nicht mehr möglich, vCloud vApps mit der Einheit zum Versetzen von Daten zu sichern oder zurückzuschreiben. Um vApps zu sichern oder zurückzuschreiben, müssen Sie Data Protection for VMware Version 7.1 verwenden. Windows-BetriebssystemeOnlinezurückschreibungen des Systemstatus Windows-BetriebssystemeEs ist nicht mehr möglich, den Systemstatus auf ein System zurückzuschreiben, das online ist. Verwenden Sie stattdessen die ASR-basierte Wiederherstellungsmethode zum Zurückschreiben des Systemstatus im Offlinemodus von Windows Preinstallation Environment (PE). Weitere Informationen finden Sie in: • Windows-Betriebssystem mit der automatischen Systemwiederherstellung zurückschreiben • Restore Systemstate Windows-BetriebssystemeAdaptive Subdateisicherung

Release	Neue Funktionen und Aktualisierungen
	Windows-BetriebssystemeAdaptive Subdateisicherungsoperationen werden nicht weiterverwendet; Sie können jedoch weiterhin vorhandene Subdateisicherungsdaten zurückschreiben. Data Encryption Standard (DES) mit 56-Bit-Datenverschlüsselung Verwenden Sie zur Verbesserung der Sicherheit Advanced Encryption Standard (AES) mit 128-Bit- oder 256-Bit-Datenverschlüsselung für Sicherungs- und Archivierungsoperationen. Weitere Informationen finden Sie in Encryptiontype. Windows-BetriebssystemeGPFS-Unterstützung für den Windows-Client Windows-BetriebssystemeEs ist nicht mehr möglich, mit dem Windows-Client für Sichern/Archivieren Dateien in einem reinen Windows-GPFS-Cluster zu sichern oder in ihn zurückzuschreiben. Es ist jedoch weiterhin möglich, den AIX- oder Linux-Client für Sichern/Archivieren zu verwenden, um Daten in GPFS-Clustern zu schützen, die gemischte Knoten enthalten, die AIX, Linux und Windows umfassen können. Data Protection for IBM Domino-Plug-in Das Data Protection for IBM Domino-Plug-in wurde für Version 7.1.0 festgeschrieben und wird vom Client für Sichern/Archivieren nicht mehr unterstützt. Wenn das Data Protection for IBM Domino-Plug-in auf demselben Server wie der IBM Domino-Server und der Client für Sichern/Archivieren der Version 8.1 installiert und konfiguriert wird, ist es nicht mehr möglich, IBM Domino-Datenbanken und -Transaktionsprotokolldateien mit dem Web-Client zu sichern und zurückzuschreiben. Option guitreeviewafterbackup Die Option guitreeviewafterbackup wird in diesem Release nicht mehr unterstützt und wurde aus dem Profileditor entfernt. Wenn diese Option bei der Ausführung des Clients in der Clientoptionsdatei vorhanden ist, wird die Option ignoriert und es werden keine Clientfehlernachrichten angezeigt. Eingestellte Unterstützung für Clientbetriebssysteme Um die Vorteile der neuen Produktfunktionen nutzen zu können, installieren Sie den Client für Sichern/Archivieren der Version 8.1 unter einem der unterstützten Betriebssysteme. Die aktuelle Liste der unterstützten Betriebssysteme finden Sie in Technote 1243309. Die folgenden Betriebssysteme werden vom Client für Sichern/Archivieren nicht mehr unterstützt: • 32-Bit-Windows-Betriebssysteme (Client und API) • Betriebssysteme Windows Server 2008, Windows Server 2008 R2, Windows 7 und Windows 8 • HP-UX-Betriebssysteme. Sie können weiterhin die IBM Spectrum Protect-API unter einem HP-UX-Betriebssystem verwenden. • Linux on Power Systems (Big Endian). Sie können weiterhin die IBM Spectrum Protect-API unter Linux on Power Systems (Big Endian) verwenden. • Solaris SPARC-Betriebssysteme. Sie können weiterhin die IBM Spectrum Protect-API unter Solaris SPARC-Betriebssystemen verwenden.

Zugehörige Informationen:
Schutz für Workstations und Dateiserver

Releaseinformationen für IBM Spectrum Protect Client für Sichern/Archivieren Version 8.1

Der IBM Spectrum Protect Client für Sichern/Archivieren Version 8.1 ist verfügbar. Dieses Dokument enthält wichtige Installationsinformationen. Außerdem finden Sie in diesem Dokument Produktaktualisierungen, Kompatibilitätsanforderungen, Einschränkungen und bekannte Probleme.

Inhalt

Beschreibung

IBM Spectrum Protect ist ein Client/Server-Lizenzprodukt, das Speicherverwaltungsservices in einer plattformübergreifenden Computerumgebung zur Verfügung stellt. Mit dem Client für Sichern/Archivieren können Sie Dateien von Workstations oder Dateiservern im Speicher sichern und archivieren sowie Sicherungsversionen und Archivierungskopien von Dateien auf lokalen Workstations zurückschreiben und abrufen.

Eine Liste der APARs, die in diesem Release behoben wurden, finden Sie in Technote 1993247.

Ankündigung

Die Ankündigung für die Produktfamilie von IBM Spectrum Protect Version 8.1 umfasst die folgenden Informationen:

- Detaillierte Produktbeschreibung, einschließlich einer Beschreibung der neuen Funktionen
- Produktpositionierungsanweisung
- Details zu Produktauswahl und Bestellung
- Internationale Kompatibilitätsinformationen

Führen Sie die folgenden Schritte aus, um nach der Produktankündigung zu suchen:

1. Rufen Sie die Website für Produktankündigungen auf.
2. Geben Sie in das Feld Search for die Produkt-ID (PID) für Ihr Produkt ein. Die Produkt-ID (PID) für IBM Spectrum Protect ist 5725-W98.
3. Wählen Sie im Feld Information Type den Eintrag Announcement letters aus und klicken Sie auf Search.
4. Wählen Sie in der Liste Search in den Eintrag Product Number aus.
5. Optional: Wählen Sie im Teilfenster Refine Your Search auf der linken Seite des Fensters das Land aus, in dem Sie sich befinden.
6. Wählen Sie im Bereich Sort by den Eintrag Newest first aus.

Kompatibilität mit früheren Versionen

Informationen zur Kompatibilität mit früheren Versionen finden Sie in IBM Spectrum Protect Server/Client Compatibility and Upgrade Considerations.

Systemvoraussetzungen

Informationen zur Hardware- und Softwarekompatibilität finden Sie in dem detaillierten Dokument zu den Systemvoraussetzungen auf den folgenden Websites:

Apple Macintosh Client Requirements
: Technote 1053584

IBM® AIX Client Requirements
: Technote 1052226

Linux on Power Systems Client Requirements
: Technote 1169963

Linux x86_64 Client Requirements
: Technote 1052223

Linux on z Systems Client Requirements
: Technote 1066436

Microsoft Windows Client Requirements
: Technote 1197133

Oracle Solaris x86_64 Client Requirements
: Technote 1232956

Client für Sichern/Archivieren installieren

Wenn Sie das Produkt über IBM Passport Advantage herunterladen, befolgen Sie die Anweisungen in dem Downloaddokument in Technote 4042940.

Installationsanweisungen finden Sie in IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows).

Aktualisierungen, Einschränkungen und bekannte Probleme

Dokumentationsaktualisierungen, Einschränkungen und bekannte Probleme sind als Technotes in der Knowledge Base des IBM Support im IBM Support Portal for IBM Spectrum Protect dokumentiert. Sobald Probleme erkannt und gelöst werden, wird die Knowledge Base vom IBM Software Support aktualisiert. Durchsuchen Sie die Knowledge Base, um Fehlerumgehungen oder Lösungen für Probleme zu finden.

Einschränkungen und bekannte Probleme
: Zum Zeitpunkt der Veröffentlichung sind die Einschränkungen und bekannten Probleme in den folgenden Technotes dokumentiert:

  - Für AIX-, Linux-, Mac OS X- und Oracle Solaris-Betriebssysteme: Technote 1993251.
  - Für Windows-Betriebssysteme: Technote 1993250.

Dokumentationsaktualisierungen
: Für Informationen, die zum Zeitpunkt der Veröffentlichung nicht zur Verfügung standen, sind Dokumentationsaktualisierungen in den folgenden Technotes verfügbar:

  - Für AIX-, Linux-, Mac OS X- und Oracle Solaris-Betriebssysteme: Technote 7048955.
  - Für Windows-Betriebssysteme: Technote 7048956.

Readme-Dateien für Fixpacks des Clients für Sichern/Archivieren von IBM Spectrum Protect Version 8.1

Readme-Dateien für die Fixpacks des Clients für Sichern/Archivieren von IBM Spectrum Protect Version 8.1 sind in IBM Support Knowledge Base verfügbar, wenn es ein Fixpack-Update gibt.

Readme-Dateien für Fixpacks des Clients für Sichern/Archivieren von IBM Spectrum Protect Version 8.1 anzeigen

Nachträgliche aktuelle Dokumentationsaktualisierungen

Aktualisierungen der Dokumentation für den IBM Spectrum Protect-Client für Sichern/Archivieren können nach der Veröffentlichung der Dokumentation im IBM® Knowledge Center auftreten.

Nachträgliche aktuelle Dokumentationsaktualisierungen stehen im IBM Support-Portal in den folgenden Dokumenten zur Verfügung:

- Für AIX-, Linux-, Mac OS X- und Oracle Solaris-Clients: Technote 7048955
- Für Windows-Clients: Technote 7048956

Schutz für Workstations und Dateiserver

IBM Spectrum Protect ist ein Client/Server-Lizenzprodukt, das Speicherverwaltungsservices in einer plattformübergreifenden Computerumgebung zur Verfügung stellt.

Mit dem Client für Sichern/Archivieren können Benutzer Dateien aus ihren Workstations oder Dateiservern im Speicher sichern oder archivieren und Sicherungsversionen und Archivierungskopien der Dateien auf ihre lokalen Workstations zurückschreiben und abrufen.

Neben dem Client für Sichern/Archivieren umfasst IBM Spectrum Protect die folgenden Komponenten:

- Ein Serverprogramm, das als Sicherungs- und Archivierungsserver für verteilte Workstations und Dateiserver ausgeführt werden kann.

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDas Serverprogramm stellt außerdem Services für hierarchische Speicherverwaltung (HSM) bereit und gestattet die Ausführung von Systemen als Umlagerungsserver.

- Ein Verwaltungsclientprogramm, auf das von einem Web-Browser oder von der Befehlszeile aus zugegriffen werden kann. Mit dem Programm kann der IBM Spectrum Protect-Administrator Serveraktivitäten steuern und überwachen, Speicherverwaltungsmaßnahmen für Sicherungs-, Archivierungs- und Speicherverwaltungsservices definieren sowie Zeitpläne erstellen, um diese Services in regelmäßigen Intervallen auszuführen.
- Eine Anwendungsprogrammierschnittstelle (API), mit der Sie eine vorhandene Anwendung durch Speicherverwaltungsservices erweitern können. Wenn eine Anwendung in einem Server als Clientknoten registriert ist, kann sie Objekte im Speicher sichern, zurückschreiben, archivieren und abrufen.
- Ein Web-Client für Sichern/Archivieren, mit dem ein berechtigter Administrator, ein Help-Desk-Benutzer oder ein anderer Benutzer Sicherungen, Zurückschreibungen, Archivierungen und Abrufe mithilfe eines Web-Browsers auf einem fernen System ausführen kann.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeErgänzungen zu IBM Spectrum Protect, die jedoch separat verkauft werden, sind die Clientprogramme IBM Spectrum Protect for Space Management und IBM Spectrum Protect HSM for Windows. Diese Programme lagern auswählbare Dateien automatisch in den Speicher um, um einen bestimmten Stand freien Speicherbereichs in lokalen Dateisystemen aufrechtzuerhalten, und rufen umgelagerte Dateien automatisch zurück, wenn auf sie zugegriffen wird. Außerdem können Benutzer mit ihnen bestimmte Dateien umlagern und zurückrufen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDie Begriffe *Hierarchische Speicherverwaltung* und *Speicherverwaltung* haben in dieser Veröffentlichung dieselbe Bedeutung.

Zugehörige Konzepte:
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeSicherungen planen
Windows-BetriebssystemeSicherungen planen (Windows)
Aktualisierungen für den Client für Sichern/Archivieren
IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Zugehörige Tasks:
Clients für Sichern/Archivieren konfigurieren
Daten mit Clients für Sichern/Archivieren sichern und zurückschreiben
Daten mit Clients für Sichern/Archivieren archivieren und abrufen
AIX-BetriebssystemeMac OS X-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)

Mit dem IBM Spectrum Protect-Client für Sichern/Archivieren können Sie die Informationen auf Ihren Workstations schützen.

Sie können Sicherungsversionen Ihrer Dateien verwalten, die Sie zurückschreiben können, wenn die Originaldateien beschädigt werden oder verloren gehen. Sie können auch selten verwendete Dateien archivieren. Die Dateien bleiben dann in ihrem aktuellen Status, und Sie können sie bei Bedarf abrufen.

Der Client für Sichern/Archivieren arbeitet zusammen mit dem IBM Spectrum Protect-Server. Bitten Sie Ihren IBM Spectrum Protect-Serveradministrator um Sicherungs- oder Archivierungszugriff auf den Server oder entnehmen Sie den Serververöffentlichungen Informationen zum Installieren und Konfigurieren des IBM Spectrum Protect-Servers.

- Upgrade des Clients für Sichern/Archivieren durchführen
  In den folgenden Abschnitten wird erläutert, wie Sie von einer vorherigen Version ein Upgrade auf Version 8.1.2 des Clients für Sichern/Archivieren von IBM Spectrum Protect durchführen.
- Clientumgebungsvoraussetzungen
  Für jeden der IBM Spectrum Protect-Clients bestehen Hardware- und Softwarevoraussetzungen.
- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeVoraussetzungen für NDMP-Unterstützung (nur Extended Edition)
  Sie können NDMP (Network Data Management Protocol) verwenden, um NAS-Dateisysteme (Network Attached Storage) auf Bandlaufwerke oder Speicherarchive, die lokal an die NAS-Dateiserver von Network Appliance und EMC Celerra angeschlossen sind, zu sichern und von dort zurückzuschreiben.
- Linux-BetriebssystemeWindows-BetriebssystemeInstallationsvoraussetzungen für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Clientdaten
  Bevor Sie Ihre FastBack-Clientdaten sichern oder archivieren können, müssen Sie die erforderliche Software installieren.
- Windows-BetriebssystemeClientkonfigurationsassistent für Tivoli Storage Manager FastBack
  Der Client für Sichern/Archivieren stellt einen Assistenten bereit, der Sie bei der Konfiguration des Clients für Sichern/Archivieren für Tivoli Storage Manager FastBack unterstützt.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeUNIX- und Linux-Clients für Sichern/Archivieren installieren
  Dieser Abschnitt enthält Anweisungen zum Installieren und Konfigurieren der UNIX- und Linux-Clients von IBM Spectrum Protect.
- Windows-BetriebssystemeInstallationsübersicht für den Windows-Client für Sichern/Archivieren
  Sie können den IBM Spectrum Protect Windows-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.
- Linux-BetriebssystemeWindows-BetriebssystemeClientverwaltungsservice zur Erfassung von Diagnoseinformationen installieren
  Sie können die IBM Spectrum Protect-Clientverwaltungsservices installieren, um Diagnoseinformationen zum Client für Sichern/Archivieren zu erfassen. Der Clientverwaltungsservice macht IBM Spectrum Protect Operations Center die Informationen für grundlegende Überwachungsfunktionen verfügbar.

Zugehörige Konzepte:
Aktualisierungen für den Client für Sichern/Archivieren
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeSicherungen planen
Windows-BetriebssystemeSicherungen planen (Windows)
Zugehörige Tasks:
Clients für Sichern/Archivieren konfigurieren
Daten mit Clients für Sichern/Archivieren sichern und zurückschreiben
Daten mit Clients für Sichern/Archivieren archivieren und abrufen

Upgrade des Clients für Sichern/Archivieren durchführen

In den folgenden Abschnitten wird erläutert, wie Sie von einer vorherigen Version ein Upgrade auf Version 8.1.2 des Clients für Sichern/Archivieren von IBM Spectrum Protect durchführen.

- Upgradepfad für Clients und Server
  Das Upgrade der IBM Spectrum Protect-Clients kann zu einem anderen Zeitpunkt durchgeführt werden als das der IBM Spectrum Protect-Server. Die kombinierten Server und Clients, die Sie implementieren, müssen untereinander kompatibel sein.
- Zusätzliche Informationen zum Upgrade
  Wenn Sie ein Upgrade des Clients für Sichern/Archivieren durchführen, müssen Sie vor der Verwendung der neuen Client-Software zusätzliche Informationen beachten.
- Automatische Implementierung des Clients für Sichern/Archivieren
  Der IBM Spectrum Protect-Serveradministrator kann einen Client für Sichern/Archivieren automatisch implementieren, um Workstations zu aktualisieren, auf denen der Client für Sichern/Archivieren bereits installiert ist.

Upgradepfad für Clients und Server

Das Upgrade der IBM Spectrum Protect-Clients kann zu einem anderen Zeitpunkt durchgeführt werden als das der IBM Spectrum Protect-Server. Die kombinierten Server und Clients, die Sie implementieren, müssen untereinander kompatibel sein.

Um eine Unterbrechung Ihrer Sicherungs- und Archivierungsaktivitäten während eines Upgrades von einem Release auf ein anderes zu verhindern, befolgen Sie die Kompatibilitätsrichtlinien für IBM Spectrum Protect-Clients und -Server in Technote 1053218.

AIX-BetriebssystemeInformationen zum Upgrade Ihrer aktuellen IBM® PowerHA SystemMirror-Konfigurationen unter AIX finden Sie in Traditionelle AIXIBM PowerHA SystemMirror-Konfigurationen migrieren.

Zusätzliche Informationen zum Upgrade

Wenn Sie ein Upgrade des Clients für Sichern/Archivieren durchführen, müssen Sie vor der Verwendung der neuen Client-Software zusätzliche Informationen beachten.

Bei einem Upgrade eines Clients für Sichern/Archivieren müssen Sie die folgenden Informationen berücksichtigen:

-  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeWenn Sie ein Upgrade für den IBM® Tivoli Storage Manager-Client für Sichern/Archivieren der Version 7.1.2 oder früher unter dem Betriebssystem Oracle Solaris durchführen, müssen Sie alle zuvor installierten Sprachenpakete deinstallieren, bevor Sie mit dem Upgrade fortfahren.
-  Mac OS X-BetriebssystemeMac-Benutzer müssen bei Aktualisierungen für den Mac OS X-Client in IBM Spectrum Protect Version 6.3 oder höher Folgendes berücksichtigen:
  - Wenn Sie den in diesem Release bereitgestellte Mac OS X-Client verwenden, müssen die Dateien dsm.sys und dsm.opt unter Verwendung von Unicode (UTF-8) codiert werden. Die UTF-8-Codierung gestattet die Verwendung von Zeichen aus beliebigen Sprachen in den Optionsdateien. Falls Ihre Dateien dsm.sys und dsm.opt zuvor mit dem Format MacRoman (oder einem beliebigen anderen Format als UTF-8) codiert waren, öffnen Sie diese Dateien in einem Editor (z. B. TextEdit) und speichern Sie die Dateien mit der UTF-8-Codierung und ohne die Erweiterung .txt. Ihre Einschluss-/Ausschlusslisten können entweder mit UTF-8 oder mit UTF-16 codiert werden. Weitere Informationen zu Unicode finden Sie in Hinweise für Clients, die für Unicode aktiviert wurden.
  - IBM Spectrum Protect-Serverdateibereiche, die von Mac OS 9-Clients erstellt wurden, können nicht durch den in IBM Spectrum Protect Version 6.3 bereitgestellten Mac OS X-Client verwaltet werden. Verwenden Sie den Befehl `q file Knoten f=d` auf dem Server, um die für einen Knoten gesicherten Dateien aufzulisten. Alle Dateien der Mac-Plattform, die nicht mit einem Schrägstrich (/) beginnen, wurden wahrscheinlich durch einen älteren Mac-Client erstellt. Diese Dateien können mit dem in diesem Release bereitgestellten Mac OS X-Client weder zurückgeschrieben noch anderweitig verwaltet werden. Die Verwaltung dieser Dateien ist zwar möglich, muss jedoch mit einem Mac-Client erfolgen werden, der auf einem Clientknoten der Version 6.2.2 oder älter installiert ist.
-  Windows-BetriebssystemeDie Puffergröße für die Aufzeichnung von Änderungsbenachrichtigungen für ein bestimmtes Journaled File System (DirNotifyBufferSize) hat sich geändert. Der Standardwert ist 16 KB.
- Eine Liste der Nachrichten, die seit dem vorherigen IBM Spectrum Protect-Release hinzugefügt oder geändert wurden, finden Sie in der Datei client_message.chg im Clientpaket.

Automatische Implementierung des Clients für Sichern/Archivieren

Der IBM Spectrum Protect-Serveradministrator kann einen Client für Sichern/Archivieren automatisch implementieren, um Workstations zu aktualisieren, auf denen der Client für Sichern/Archivieren bereits installiert ist.

Der IBM Spectrum Protect-Server kann so konfiguriert werden, dass für Clients für Sichern/Archivieren auf Client-Workstations ein Upgrade automatisch durchgeführt wird. Die vorhandenen Clients für Sichern/Archivieren müssen Version 6.4.3 oder höher verwenden.

Weitere Informationen zur automatischen Implementierung von Clientaktualisierungen finden Sie in den folgenden Dokumenten:

- Technote 2004596 für Server mit IBM Spectrum Protect Version 8.1.2 oder höher.
- Technote 1673299 für Server mit IBM® Tivoli Storage Manager Version 7.1 und Server mit IBM Spectrum Protect Version 8.1.0 und Version 8.1.1.

Einschränkungen: Für die automatische Clientimplementierung gelten die folgenden Einschränkungen:

- Die Windows-Clusterserviceumgebung wird nicht unterstützt.
- Nur der Client für Sichern/Archivieren kann vom IBM Spectrum Protect-Server aus implementiert werden. Andere zugehörige Produkte wie z. B. IBM Spectrum Protect for Space Management, IBM Spectrum Protect HSM for Windows, IBM Spectrum Protect for Virtual Environments und andere Data Protection-Produkte werden nicht unterstützt. Wenn Sie versuchen, ein nicht unterstütztes Produkt zu implementieren, wird die Implementierung gestoppt und eine Fehlernachricht angezeigt.
- Für Workstations, auf denen die Anwendung IBM Spectrum Protect for ERP bereits installiert ist, dürfen Sie keine automatischen Clientimplementierungen planen.

  Wenn der Serveradministrator automatische Implementierungen des Clients für Sichern/Archivieren plant, werden die aktualisierten Clientpakete (die die Clientkomponenten und die API-Bibliothek enthalten) auf den Workstations installiert, auf denen sie empfangen werden. Das Clientinstallationsprogramm führt eine Abhängigkeitsprüfung durch, um sicherzustellen, dass kein Konflikt zwischen der API-Bibliothek und dem bereits installierten Clientpaket besteht.

  Anwendungen von IBM Spectrum Protect for ERP verwenden ein anderes Installationsverfahren als das Clientinstallationsprogramm. Daher kann bei der Abhängigkeitsprüfung der Clientinstallation nicht festgestellt werden, ob die von den Anwendungen von IBM Spectrum Protect for ERP verwendete API-Bibliothek mit der API-Bibliothek kompatibel ist, die bei den automatischen Clientimplementierungen installiert wird. Wenn ein Clientpaket auf einer Workstation automatisch implementiert und installiert wird, könnte die installierte API-Bibliothek mit der API-Bibliothek, die von den Anwendungen von IBM Spectrum Protect for ERP installiert wurde, inkompatibel sein. Die neu implementierte API-Bibliothek kann Fehler in den Anwendungen von IBM Spectrum Protect for ERP verursachen.

Auswirkung der Clientoption autodeploy auf die Clientimplementierung

Mit der Option autodeploy können Sie eine automatische Clientimplementierung unter der Bedingung aktivieren, dass kein Neustart der Client-Workstation für die Implementierung notwendig ist.

Standardmäßig ist die Option autodeploy aktiviert und die Client-Workstation wird bei Bedarf erneut gestartet.

Soll die automatische Implementierung ohne einen Neustart des Systems verwendet werden, geben Sie die Option autodeploy noreboot an.

Um die automatische Clientimplementierung zu inaktivieren, fügen Sie autodeploy no zur Clientoptionsdatei hinzu.

Sie können die Option autodeploy an folgenden Positionen festlegen:

- In einer Zeitplandefinition auf dem IBM Spectrum Protect-Server. Zeitplandefinitionen, die Client-Software-Aktualisierungen implementieren, verfügen über eine Anweisung `action=deploy`. In diesen Zeitplänen können Sie die Option autodeploy in den Befehl einfügen, den Sie in der Anweisung –postnschedulecmd angeben.
- Auf dem Clientknoten in einer Optionsdatei, die dem Client-Scheduler oder dem Clientakzeptor zugeordnet ist. Der Deployment Manager erkennt Optionsdateien, die dem Client-Scheduler oder dem Clientakzeptor zugeordnet sind. Falls auf einem Computer mehrere Scheduler- oder Clientakzeptorprozesse gleichzeitig ausgeführt werden und diese Prozesse unterschiedliche Optionsdateien verwenden, verwendet der Deployment Manager den in einer der Optionsdateien definierten Wert der Option autodeploy.
- Auf dem Client in der Clientoptionsdatei (dsm.opt). Die in der Clientoptionsdatei definierte Option autodeploy überschreibt alle anderen autodeploy-Einstellungen.

Zugehörige Verweise:
Autodeploy

Clientumgebungsvoraussetzungen

Für jeden der IBM Spectrum Protect-Clients bestehen Hardware- und Softwarevoraussetzungen.

Die folgende Liste enthält die Position der Umgebungsvoraussetzungen für jede unterstützte Plattform.

Aktuelle Informationen zu den Clientumgebungsvoraussetzungen für alle unterstützten Plattformen des Clients für Sichern/Archivieren finden Sie in Technote 1243309.

- AIX-BetriebssystemeAIX-Clientumgebung
  Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die AIX-Plattform.
- HP-UX Itanium 2-API-Umgebung
  Lesen Sie die Informationen zur API-Umgebung, zu installierbaren Komponenten sowie zu Hardware- und Softwarevoraussetzungen für die HP-UX Itanium 2-Plattform.
- Linux-BetriebssystemeLinux on Power Systems-Clientumgebung
  Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die Linux on Power Systems-Clientplattform.
- Linux-BetriebssystemeLinux x86_64-Clientumgebung
  Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die Linux on Intel-Plattform (Linux x86_64-Plattform).
- Linux-BetriebssystemeLinux on System z-Clientumgebung
  Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die Linux on System z-Plattform.
- Mac OS X-BetriebssystemeMac OS X-Clientumgebung
  Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für den Mac OS X-Client.
- Oracle Solaris-BetriebssystemeOracle Solaris-Clientumgebung
  Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Clientkomponenten und zu den Hardware- und Softwarevoraussetzungen für die Oracle Solaris-Plattform.
- Windows-BetriebssystemeVoraussetzungen für die Windows-Clientumgebung
  Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die unterstützten Windows-Plattformen.

Zugehörige Konzepte:
AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeVoraussetzungen für NDMP-Unterstützung (nur Extended Edition)
AIX-Betriebssysteme

AIX-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die AIX-Plattform.

- AIX-BetriebssystemeInstallierbare Komponenten des AIX-Clients
  Der Client für Sichern/Archivieren besteht aus mehreren installierbaren Komponenten.

- AIX-BetriebssystemeSystemvoraussetzungen für den AIX-Client
  Für den AIX-Client von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.
- AIX-BetriebssystemeÜbertragungsmethoden des AIX-Clients
  Für den AIX-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.
- AIX-BetriebssystemeUnter AIX verfügbare Features des Clients für Sichern/Archivieren
  In diesem Abschnitt sind die Features aufgelistet, die unter AIX unterstützt werden.

AIX-Betriebssysteme

Installierbare Komponenten des AIX-Clients

Der Client für Sichern/Archivieren besteht aus mehreren installierbaren Komponenten.

Installierbare Komponenten für den AIX-Client:

- Befehlszeilenclient für Sichern/Archivieren
- Verwaltungsclient
- Grafische Benutzerschnittstelle des Clients für Sichern/Archivieren, die Oracle Java™-Technologie verwendet
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-64-Bit-API

Die API kann separat installiert werden. Alle anderen Komponenten werden bei der Installation des AIX-Pakets (tivoli.tsm.client.api.64bit) installiert.

AIX-Betriebssysteme

Systemvoraussetzungen für den AIX-Client

Für den AIX-Client von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der AIX-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1052226.

AIX-Betriebssysteme

Übertragungsmethoden des AIX-Clients

Für den AIX-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Sie können die folgenden Übertragungsmethoden für den AIX-Client von IBM Spectrum Protect Version 8.1.2 verwenden:

Tabelle 1. Übertragungsmethoden des AIX-Clients

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei unterstützten AIX-Plattformen)	AIX, Linux, Windows
Shared Memory	TCP/IP (Standard bei unterstützten AIX-Plattformen)	AIX

AIX-Betriebssysteme

Unter AIX verfügbare Features des Clients für Sichern/Archivieren

In diesem Abschnitt sind die Features aufgelistet, die unter AIX unterstützt werden.

Tabelle 1. Unterstützte Features unter AIX

Features	Unter AIX unterstützt?
Befehlszeile und GUI für Sichern/Archivieren	yes
Journalbasierte Sicherung	Ja
LAN-unabhängige Operationen	yes
Online-Imagesicherung	yes
Offline-Imagesicherung	yes

HP-UX Itanium 2-API-Umgebung

Lesen Sie die Informationen zur API-Umgebung, zu installierbaren Komponenten sowie zu Hardware- und Softwarevoraussetzungen für die HP-UX Itanium 2-Plattform.

- Installierbare Komponente der Itanium 2-API
  In IBM Spectrum Protect Version 8.1.2 kann nur die HP-UX Itanium 2-API installiert werden.
- Systemvoraussetzungen für die HP-UX Itanium 2-API
  Für die HP-UX Itanium 2-API von IBM Spectrum Protect gelten Mindestanforderungen in Bezug auf die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.
- Übertragungsmethoden für die HP-UX Itanium 2-API
  Für die HP-UX Itanium 2-API sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Installierbare Komponente der Itanium 2-API

In IBM Spectrum Protect Version 8.1.2 kann nur die HP-UX Itanium 2-API installiert werden.

Systemvoraussetzungen für die HP-UX Itanium 2-API

Für die HP-UX Itanium 2-API von IBM Spectrum Protect gelten Mindestanforderungen in Bezug auf die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der HP-UX Itanium 2-API, einschließlich der neuesten Fixpacks, finden Sie in Technote 1197146.

Übertragungsmethoden für die HP-UX Itanium 2-API

Für die HP-UX Itanium 2-API sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Tabelle 1. Übertragungsmethoden für die HP-UX Itanium 2-API

Zur Verwendung dieser Übertragungsmethode:	**Diese Software installieren:**	**Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:**
TCP/IP	TCP/IP (Standard bei HP-UX)	AIX, Linux, Windows

Linux-Betriebssysteme

Linux on Power Systems-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die Linux on Power Systems-Clientplattform.

- LinuxBetriebssystemeInstallierbare Komponenten des Linux on Power Systems-Clients
  Die installierbaren Komponenten des Linux on Power Systems-Clients für Sichern/Archivieren umfassen die Befehlszeile des Clients für Sichern/Archivieren, die Java™-GUI, den Web-Client für Sichern/Archivieren und die API.
- LinuxBetriebssystemeSystemvoraussetzungen für Linux on Power Systems-Clients
  Für die Linux on Power Systems-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.
- LinuxBetriebssystemeÜbertragungsmethoden des Linux on Power Systems-Clients
  Clients für Sichern/Archivieren unter Linux on Power Systems können TCP/IP oder Shared Memory als Übertragungsmethode für die Client/Server-Kommunikation verwenden.

Linux-Betriebssysteme

Installierbare Komponenten des Linux on Power Systems-Clients

Die installierbaren Komponenten des Linux on Power Systems-Clients für Sichern/Archivieren umfassen die Befehlszeile des Clients für Sichern/Archivieren, die Java™-GUI, den Web-Client für Sichern/Archivieren und die API.

Sie können die folgenden Komponenten mit IBM Spectrum Protect Version 8.1.2 installieren:

- Client für Sichern/Archivieren
- Verwaltungsclient
- Grafische Java-Benutzerschnittstelle (Java-GUI) für Sichern/Archivieren
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API (64-Bit)

Linux-Betriebssysteme

Systemvoraussetzungen für Linux on Power Systems-Clients

Für die Linux on Power Systems-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Linux on Power Systems-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1169963.

Linux-Betriebssysteme

Übertragungsmethoden des Linux on Power Systems-Clients

Clients für Sichern/Archivieren unter Linux on Power Systems können TCP/IP oder Shared Memory als Übertragungsmethode für die Client/Server-Kommunikation verwenden.

In Tabelle 1 sind die verfügbaren Übertragungsmethoden für Linux on Power Systems-Clients sowie die Betriebssysteme des IBM Spectrum Protect-Servers, für die Sie sie verwenden können, aufgelistet.

Tabelle 1. Übertragungsmethoden des Linux on Power Systems-Clients

Zur Verwendung dieser Übertragungsmethode:	**Diese Software installieren:**	**Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:**
TCP/IP	TCP/IP (Standard bei Linux)	AIX, Linux, Windows
Shared Memory	TCP/IP (Standard bei Linux)	Linux on Power Systems

Linux-Betriebssysteme

Linux x86_64-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die Linux on Intel-Plattform (Linux x86_64-Plattform).

- Linux-Betriebssysteme**Installierbare Komponenten des Linux x86_64-Clients**
  Die installierbaren Komponenten des Linux on Intel-Clients für Sichern/Archivieren (Linux x86_64-Clients für Sichern/Archivieren) umfassen die Befehlszeile des Clients für Sichern/Archivieren, die Java™-GUI, den Web-Client für Sichern/Archivieren, den Verwaltungsclient und die API.
- Linux-Betriebssysteme**Systemvoraussetzungen für Linux x86_64-Clients**
  Für die Linux x86_64-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.
- Linux-Betriebssysteme**Übertragungsmethoden des Linux x86_64-Clients**
  Für den Linux on Intel-Client für Sichern/Archivieren (Linux x86_64-Client für Sichern/Archivieren) sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Linux-Betriebssysteme

Installierbare Komponenten des Linux x86_64-Clients

Die installierbaren Komponenten des Linux on Intel-Clients für Sichern/Archivieren (Linux x86_64-Clients für Sichern/Archivieren) umfassen die Befehlszeile des Clients für Sichern/Archivieren, die Java™-GUI, den Web-Client für Sichern/Archivieren, den Verwaltungsclient und die API.

Sie können die folgenden Komponenten mit IBM Spectrum Protect Version 8.1.2 installieren:

- Client für Sichern/Archivieren
- Verwaltungsclient
- Grafische Java-Benutzerschnittstelle (Java-GUI) für Sichern/Archivieren
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API

Linux-Betriebssysteme

Systemvoraussetzungen für Linux x86_64-Clients

Für die Linux x86_64-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Linux x86_64-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1052223.

Linux-Betriebssysteme

Übertragungsmethoden des Linux x86_64-Clients

Für den Linux on Intel-Client für Sichern/Archivieren (Linux x86_64-Client für Sichern/Archivieren) sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Sie können die folgenden Übertragungsmethoden für den Linux on Intel-Client (Linux x86_64-Client) von IBM Spectrum Protect Version 8.1.2 verwenden:

Tabelle 1. Übertragungsmethoden des Linux on Intel x86_64-Clients

Zur Verwendung dieser Übertragungsmethode:	**Diese Software installieren:**	**Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:**
TCP/IP	TCP/IP (Standard bei Linux)	AIX, Linux, Windows
Shared Memory	TCP/IP (Standard bei Linux)	Linux x86_64

Linux-Betriebssysteme

Linux on System z-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die Linux on System z-Plattform.

- LinuxBetriebssystemeInstallierbare Komponenten des Linux on System z-Clients
  Die installierbaren Komponenten des Linux on System z-Clients für Sichern/Archivieren umfassen die Befehlszeile des Clients für Sichern/Archivieren, den Verwaltungsclient, den Web-Client für Sichern/Archivieren und die API.
- LinuxBetriebssystemeSystemvoraussetzungen für Linux on System z-Clients
  Für die Linux System z-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.
- LinuxBetriebssystemeÜbertragungsmethoden des Linux on System z-Clients
  Für den Linux on System z-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Linux-Betriebssysteme

Installierbare Komponenten des Linux on System z-Clients

Die installierbaren Komponenten des Linux on System z-Clients für Sichern/Archivieren umfassen die Befehlszeile des Clients für Sichern/Archivieren, den Verwaltungsclient, den Web-Client für Sichern/Archivieren und die API.

Sie können die folgenden Komponenten mit IBM Spectrum Protect Version 8.1.2 installieren:

- Client für Sichern/Archivieren
- Verwaltungsclient
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API

Linux-Betriebssysteme

Systemvoraussetzungen für Linux on System z-Clients

Für die Linux System z-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Linux System z-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1066436.

Linux-Betriebssysteme

Übertragungsmethoden des Linux on System z-Clients

Für den Linux on System z-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Sie können die folgenden Übertragungsmethoden für den Linux on System z-Client von IBM Spectrum Protect Version 8.1.2 verwenden:

Tabelle 1. Übertragungsmethoden des Linux on System z-Clients

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei Linux)	AIX, Linux, Windows
Shared Memory	TCP/IP (Standard bei Linux)	Linux on System z


Mac OS X-Betriebssysteme

Mac OS X-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für den Mac OS X-Client.

- 
Mac OS X-BetriebssystemeInstallierbare Komponenten des Mac OS X-Clients
Die installierbaren Komponenten des Mac OS X-Clients für Sichern/Archivieren umfassen die Befehlszeile des Clients für Sichern/Archivieren, die Java™-GUI, den Web-Client für Sichern/Archivieren und die API.
- 
Mac OS X-BetriebssystemeSystemvoraussetzungen für Mac OS X-Clients
Für die Mac OS X-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.
- 
Mac OS X-BetriebssystemeÜbertragungsmethoden des Mac OS X-Clients
Für den Mac OS X-Client für Sichern/Archivieren sind die TCP/IP-Übertragungsmethoden verfügbar.


Mac OS X-Betriebssysteme

Installierbare Komponenten des Mac OS X-Clients

Die installierbaren Komponenten des Mac OS X-Clients für Sichern/Archivieren umfassen die Befehlszeile des Clients für Sichern/Archivieren, die Java™-GUI, den Web-Client für Sichern/Archivieren und die API.

Die folgenden Komponenten werden mit IBM Spectrum Protect Version 8.1.2 installiert:

- Client für Sichern/Archivieren
- Verwaltungsclient
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API
- Grafische Java-Benutzerschnittstelle (Java-GUI) für Sichern/Archivieren

Tipp: Die Shell-Script-Datei `dsmj` für die Java-GUI wird an der folgenden Position installiert:

```
/Library/Application Support/tivoli/tsm/client/ba/bin
```


Mac OS X-Betriebssysteme

Systemvoraussetzungen für Mac OS X-Clients

Für die Mac OS X-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Mac OS X-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1053584.


Mac OS X-Betriebssysteme

Übertragungsmethoden des Mac OS X-Clients

Für den Mac OS X-Client für Sichern/Archivieren sind die TCP/IP-Übertragungsmethoden verfügbar.

Sie können die folgenden Übertragungsmethoden mit dem Mac OS X-Client von IBM Spectrum Protect Version 8.1.2 verwenden:

Tabelle 1. Übertragungsmethoden des Mac OS X-Clients

Zur Verwendung dieser Übertragungsmethode:	Diese Software installieren:	Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:
TCP/IP	TCP/IP (Standard bei Mac OS X)	AIX, Linux, Windows


Oracle Solaris-Betriebssysteme

Oracle Solaris-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Clientkomponenten und zu den Hardware- und Softwarevoraussetzungen für die Oracle Solaris-Plattform.

Ab IBM Spectrum Protect Version 8.1.0 ist der Oracle Solaris-Client für Sichern/Archivieren nur auf der Oracle Solaris x86_64-Plattform verfügbar. Die Oracle Solaris-API ist auf den Oracle Solaris x86_64- und Oracle Solaris SPARC-Plattformen verfügbar.

- Oracle Solaris-BetriebssystemeInstallierbare Komponenten des Oracle Solaris-Clients
  Die installierbaren Komponenten des Oracle Solaris-Clients für Sichern/Archivieren umfassen die IBM Spectrum Protect-Befehlszeile, die Java™-GUI, den Web-Client für Sichern/Archivieren und die API.
- Oracle Solaris-BetriebssystemeSystemvoraussetzungen für Oracle Solaris-Clients
  Für die Oracle Solaris-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.
- Oracle Solaris-BetriebssystemeÜbertragungsmethoden des Oracle Solaris-Clients
  Für den Oracle Solaris-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Oracle Solaris-Betriebssysteme

Installierbare Komponenten des Oracle Solaris-Clients

Die installierbaren Komponenten des Oracle Solaris-Clients für Sichern/Archivieren umfassen die IBM Spectrum Protect-Befehlszeile, die Java™-GUI, den Web-Client für Sichern/Archivieren und die API.

Unter Oracle Solaris x86_64 können Sie die folgenden Clientkomponenten installieren:

- Client für Sichern/Archivieren
- Verwaltungsclient
- Grafische Java-Benutzerschnittstelle (Java-GUI) für Sichern/Archivieren
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API

Sie können die IBM Spectrum Protect-API unter Oracle Solaris SPARC installieren.

Oracle Solaris-Betriebssysteme

Systemvoraussetzungen für Oracle Solaris-Clients

Für die Oracle Solaris-Clients von IBM Spectrum Protect gelten Mindestanforderungen an die Hardware, den Plattenspeicherplatz, den Hauptspeicher und die Software.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Oracle Solaris-Clients von IBM Spectrum Protect, einschließlich der neuesten Fixpacks, finden Sie auf den folgenden IBM® Support-Seiten:

- Für Oracle Solaris x86_64-Clientvoraussetzungen siehe Technote 1232956.
- Für Oracle Solaris SPARC-API-Voraussetzungen siehe Technote 1052211.

Oracle Solaris-Betriebssysteme

Übertragungsmethoden des Oracle Solaris-Clients

Für den Oracle Solaris-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Sie können die folgenden Übertragungsmethoden mit dem Oracle Solaris-Client verwenden:

Tabelle 1. Übertragungsmethoden des Oracle Solaris-Clients

Zur Verwendung dieser Übertragungsmethode:	**Diese Software installieren:**	**Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:**
TCP/IP	TCP/IP (Standard bei Solaris)	AIX, Linux, Windows

Windows-Betriebssysteme

Voraussetzungen für die Windows-Clientumgebung

Dieser Abschnitt enthält Informationen zur Clientumgebung, zu Komponenten des Clients für Sichern/Archivieren und zu den Hardware- und Softwarevoraussetzungen für die unterstützten Windows-Plattformen.

- Windows-BetriebssystemeInstallierbare Komponenten des Windows-Clients
  Der Client für Sichern/Archivieren besteht aus mehreren installierbaren Komponenten.
- Windows-BetriebssystemeSystemvoraussetzungen für Windows-Clients
  Der Client für Sichern/Archivieren unter Windows erfordert einen Mindestumfang an Plattenspeicherplatz für die Installation und ein unterstütztes Betriebssystem.
- Windows-BetriebssystemeÜbertragungsmethoden des Windows-Clients
  Für den Windows-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.
- Windows-BetriebssystemeAuf Windows-Plattformen verfügbare Features des Clients für Sichern/Archivieren
  In diesem Abschnitt sind die Features aufgelistet, die auf den verschiedenen Windows-Plattformen unterstützt oder nicht unterstützt werden.
- Windows-BetriebssystemeUnterstützte Windows-Dateisysteme
  Der IBM Spectrum Protect-Client für Sichern/Archivieren unter Windows wird auf bestimmten Dateisystemen unterstützt.

Windows-Betriebssysteme

Installierbare Komponenten des Windows-Clients

Der Client für Sichern/Archivieren besteht aus mehreren installierbaren Komponenten.

Die installierbaren Komponenten für den Windows-Client für Sichern/Archivieren sind wie folgt:

- Befehlszeilenclient für Sichern/Archivieren
- Verwaltungsclient
- Grafische Benutzerschnittstelle des Clients für Sichern/Archivieren, die Oracle Java™-Technologie verwendet
- Web-Client für Sichern/Archivieren
- IBM Spectrum Protect-API (64-Bit)

Windows-Betriebssysteme

Systemvoraussetzungen für Windows-Clients

Der Client für Sichern/Archivieren unter Windows erfordert einen Mindestumfang an Plattenspeicherplatz für die Installation und ein unterstütztes Betriebssystem.

Informationen zu den Hardware- und Softwarevoraussetzungen für alle unterstützten Versionen der Windows-Clients, einschließlich der neuesten Fixpacks, finden Sie in Technote 1197133.

Windows-Betriebssysteme

Übertragungsmethoden des Windows-Clients

Für den Windows-Client für Sichern/Archivieren sind die Übertragungsmethoden TCP/IP und Shared Memory verfügbar.

Sie können die folgenden Übertragungsmethoden mit dem Windows-Client für Sichern/Archivieren verwenden:

Tabelle 1. Übertragungsmethoden des Windows-Clients

Zur Verwendung dieser Übertragungsmethode:	**Diese Software installieren:**	**Um Verbindung zu diesen IBM Spectrum Protect-Servern herzustellen:**
TCP/IP	TCP/IP (Standard bei allen unterstützten Windows-Plattformen)	AIX, Linux, Windows
Benannte Pipes	Benannte Pipes (Standard bei allen unterstützten Windows-Plattformen)	Windows
Shared Memory	TCP/IP (Standard bei allen unterstützten Windows-Plattformen)	Windows

Windows-Betriebssysteme

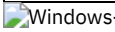
Auf Windows-Plattformen verfügbare Features des Clients für Sichern/Archivieren

In diesem Abschnitt sind die Features aufgelistet, die auf den verschiedenen Windows-Plattformen unterstützt oder nicht unterstützt werden.

Tabelle 1 zeigt die unterstützten und nicht unterstützten Features auf den verschiedenen Windows-Plattformen.

Tabelle 1. Unterstützte Features auf Windows-Plattformen

Features	Windows 10	Windows Server 2012 Windows Server 2012 R2 Windows Server 2016
Journalbasierte Sicherung	Ja	Ja
Online-Imagesicherung	Ja	Ja
Offline-Imagesicherung	Ja	Ja
Systemstatusunterstützung mit Volume Shadowcopy Services (VSS)	Ja	Ja
LAN-unabhängige Operationen	Ja	Ja
Automatische Systemwiederherstellung (ASR)	Ja	BIOS: Ja UEFI: Ja
Unterstützung offener Dateien (OFS)	Ja	Ja

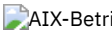


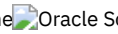
Unterstützte Windows-Dateisysteme

Der IBM Spectrum Protect-Client für Sichern/Archivieren unter Windows wird auf bestimmten Dateisystemen unterstützt.

Der Windows-Client für Sichern/Archivieren unterstützt die folgenden Dateisystemtypen:

- FAT und FAT32 (File Allocation Table)
- Microsoft NTFS (New Technology File System)
- Microsoft ReFS (Resilient File System). ReFS wurde auf Windows Server 2012-Systemen eingeführt.





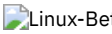
Voraussetzungen für NDMP-Unterstützung (nur Extended Edition)

Sie können NDMP (Network Data Management Protocol) verwenden, um NAS-Dateisysteme (Network Attached Storage) auf Bandlaufwerke oder Speicherarchive, die lokal an die NAS-Dateiserver von Network Appliance und EMC Celerra angeschlossen sind, zu sichern und von dort zurückzuschreiben.

NDMP-Unterstützung ist nur für IBM Spectrum Protect Extended Edition verfügbar.

NDMP-Unterstützung erfordert die folgende Hardware und Software:

- IBM Spectrum Protect Extended Edition
- Bandlaufwerk und Bandarchiv. Unterstützte Kombinationen finden Sie unter: Produktinformation.



Installationsvoraussetzungen für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Clientdaten

Bevor Sie Ihre FastBack-Clientdaten sichern oder archivieren können, müssen Sie die erforderliche Software installieren.

Sie müssen die folgende Software installieren:

- Tivoli Storage Manager FastBack Version 6.1
- Tivoli Storage Manager-Client Version 6.1.3.x (x ist 1 oder höher) oder Version 6.2 oder höher
- Tivoli Storage Manager-Server Version 6.1.3 oder höher
- Tivoli Storage Manager Administration Center Version 6.1.3
  - Nur erforderlich, wenn die integrierte Tivoli Storage Manager FastBack-Verwaltung verwendet werden soll.

    Ab Version 7.1 ist die Komponente 'Administration Center' nicht mehr in Tivoli Storage Manager- oder IBM Spectrum Protect-Verteilungen enthalten. FastBack-Benutzer, die über ein Administration Center aus einem früheren Server-Release verfügen, können damit weiterhin FastBack-Zeitpläne erstellen und ändern. Wenn noch kein Administration Center installiert ist, können Sie die Vorgängerversion von ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/admincenter/v6r3/ herunterladen. Wenn noch kein Administration Center installiert ist, müssen Sie FastBack-Zeitpläne auf dem IBM Spectrum Protect-Server erstellen und ändern. Informationen zur Erstellung von Zeitplänen auf dem Server finden Sie in der Dokumentation für den IBM Spectrum Protect-Server.

Die Tivoli Storage Manager FastBack-Umgebung muss aktiv sein. Informationen zur Installation und Konfiguration von Tivoli Storage Manager FastBack finden Sie in der Produktinformation für Tivoli Storage Manager FastBack.

Informationen zur Integration von IBM Spectrum Protect und Tivoli Storage Manager FastBack finden Sie in Tivoli Storage Manager FastBack und IBM Spectrum Protect integrieren.

Sie können den IBM Spectrum Protect-Client mit einem der folgenden Verfahren installieren:

- Windows-BetriebssystemeInstallieren Sie den Client für Sichern/Archivieren auf einer Workstation, auf der der FastBack-Server installiert ist. In diesem Fall sind die Voraussetzungen: FastBack-Server, FastBack Shell und FastBack Mount.
- Linux-BetriebssystemeInstallieren Sie den Client für Sichern/Archivieren auf einer Workstation, auf der der FastBack Disaster Recovery Hub installiert ist. In diesem Fall sind die Voraussetzungen: FastBack Disaster Recovery Hub-Konfiguration und FastBack Shell.
- Windows-BetriebssystemeInstallieren Sie den Client für Sichern/Archivieren auf einer Workstation, auf der der FastBack Disaster Recovery Hub installiert ist. In diesem Fall sind die Voraussetzungen: FastBack Disaster Recovery Hub-Konfiguration, FastBack Shell und FastBack Mount.
- Linux-BetriebssystemeInstallieren Sie den Client für Sichern/Archivieren auf einer Workstation, auf der weder der FastBack-Server noch der FastBack Disaster Recovery Hub installiert ist. In diesem Fall ist FastBack Shell weiterhin erforderlich.
- Windows-BetriebssystemeInstallieren Sie den Client für Sichern/Archivieren auf einer Workstation, auf der weder der FastBack-Server noch der FastBack Disaster Recovery Hub installiert ist. Stellen Sie in diesem Fall sicher, dass FastBack Shell und FastBack Mount installiert sind.

Zugehörige Konzepte:
Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren
Windows-Betriebssysteme

Clientkonfigurationsassistent für Tivoli Storage Manager FastBack

Der Client für Sichern/Archivieren stellt einen Assistenten bereit, der Sie bei der Konfiguration des Clients für Sichern/Archivieren für Tivoli Storage Manager FastBack unterstützt.

Der Assistent ist in einer fernen Anwendung (im Web-Client) und in einer lokalen Anwendung (in der Java™-GUI) verfügbar. Der Assistent unterstützt Sie beim Definieren der Optionen, über die Sie FastBack-Clientdaten wie geplant an den IBM Spectrum Protect-Server senden können.

Zugehörige Konzepte:
Client für Sichern/Archivieren für den Schutz von FastBack-Clientdaten konfigurieren
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

UNIX- und Linux-Clients für Sichern/Archivieren installieren

Dieser Abschnitt enthält Anweisungen zum Installieren und Konfigurieren der UNIX- und Linux-Clients von IBM Spectrum Protect.

Anmerkung: Sie müssen sich als Rootbenutzer anmelden, um den Client für Sichern/Archivieren auf einer UNIX- oder Linux-Workstation zu installieren.

Die unterstützten UNIX- und Linux-Clients sowie die Position der Installationsanweisungen für jeden Client sind hier aufgelistet.

- AIX-BetriebssystemeAIX-Client installieren
  Sie können den AIX-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.
- AIX-BetriebssystemeAIX-Client deinstallieren
  Sie können die folgenden Prozeduren verwenden, um den IBM Spectrum Protect AIX-Client für Sichern/Archivieren zu deinstallieren.
- HP-UX Itanium 2-API installieren
  Sie können die HP-UX Itanium 2-API von den Produktinstallationsmedien installieren.
- HP-UX Itanium 2-API deinstallieren
  Sie können die folgenden Prozeduren verwenden, um die IBM Spectrum Protect HP-UX Itanium 2-API zu deinstallieren.
- Linux-BetriebssystemeClient für Sichern/Archivieren unter Linux on Power Systems (Little Endian) installieren
  Sie können den Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.
- Linux-BetriebssystemeClient für Sichern/Archivieren unter Linux on Power Systems (Little Endian) deinstallieren
  Sie können den IBM Spectrum Protect-Client unter Linux on Power Systems (Little Endian) deinstallieren.
- Linux-BetriebssystemeClient für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) installieren
  Sie können den Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.
- Linux-BetriebssystemeClient unter Ubuntu Linux on Power Systems (Little Endian) deinstallieren
  Sie können den IBM Spectrum Protect-Client für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) deinstallieren.
- Linux-BetriebssystemeAPI unter Linux on Power Systems (Big Endian) installieren
  Sie können die IBM Spectrum Protect-API von den Produktinstallationsmedien installieren.
- Linux-BetriebssystemeAPI unter Linux on Power Systems (Big Endian) deinstallieren
  Sie können die IBM Spectrum Protect-API unter IBM Spectrum Protect Linux on Power Systems (Big Endian) deinstallieren.
- Linux-BetriebssystemeLinux x86_64-Client installieren
  Sie können den Linux x86_64-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.
- Linux-BetriebssystemeLinux x86_64-Client deinstallieren
  Sie können die folgende Prozedur verwenden, um den IBM Spectrum Protect Linux x86_64-Client zu deinstallieren.

- Linux-BetriebssystemeUbuntu Linux x86_64-Client installieren
  Sie können den Ubuntu Linux 64-Bit-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.
- Linux-BetriebssystemeUbuntu Linux x86_64-Client deinstallieren
  Verwenden Sie die folgende Prozedur, um den IBM Spectrum Protect Ubuntu Linux x86_64-Client zu deinstallieren.
- Linux-BetriebssystemeLinux on System z-Client installieren
  Sie können den Linux on System z-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.
- Linux-BetriebssystemeLinux on System z-Client deinstallieren
  Sie können die folgenden Prozeduren verwenden, um den IBM Spectrum Protect Linux on System z-Client zu deinstallieren.
- Mac OS X-BetriebssystemeMac OS X-Client installieren
  Sie können den IBM Spectrum Protect Mac OS X-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.
- Mac OS X-BetriebssystemeMac OS X-Client deinstallieren
  Sie können den IBM Spectrum Protect Mac OS X-Client deinstallieren, wenn er nicht mehr benötigt wird.
- Oracle Solaris-BetriebssystemeOracle Solaris x86_64-Client installieren
  Sie können den IBM Spectrum Protect Oracle Solaris x86_64-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.
- Oracle Solaris-BetriebssystemeOracle Solaris x86_64-Client deinstallieren
  Sie können alle Pakete deinstallieren, die zum IBM Spectrum Protect Oracle Solaris x86_64-Client gehören, einschließlich der Komponenten Befehlszeilenclient, GUI, Web-GUI und Verwaltungsclient.
- Oracle Solaris-BetriebssystemeOracle Solaris SPARC-API installieren
  Sie können die IBM Spectrum Protect Oracle Solaris SPARC-API von den Produktinstallationsmedien installieren.
- Oracle Solaris-BetriebssystemeOracle Solaris SPARC-API deinstallieren
  Sie können alle Pakete deinstallieren, die zur IBM Spectrum Protect Oracle Solaris SPARC-API gehören.
- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme
  Softwareaktualisierungen
  IBM® kann Softwareaktualisierungen regelmäßig für den Download bereitstellen.

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
AIX-Betriebssysteme

AIX-Client installieren

Sie können den AIX-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Informationen zu diesem Vorgang

In IBM Spectrum Protect Version 8.1.2 wird in den Verteilungsbibliotheken eine 64-Bit-Version des AIX-Clients bereitgestellt. Es ist nicht möglich, ein Upgrade für einen zuvor installierten 32-Bit-AIX-Client auf den neuen 64-Bit-AIX-Client durchzuführen. Falls bereits ein 32-Bit-Client einer früheren Version von IBM Spectrum Protect installiert ist, führen Sie die folgenden Schritte mit SMIT aus:

1. Deinstallieren Sie den 32-Bit-Client (tivoli.tsm.client.ba).
2. Deinstallieren Sie alle landessprachlichen Dateien, die zuvor installiert waren.
3. Deinstallieren Sie die API (tivoli.tsm.client.api.32bit).

Verwenden Sie anschließend SMIT, um die folgenden Pakete in den Verteilungsbibliotheken von IBM Spectrum Protect Version 8.1.2 in der folgenden Reihenfolge zu installieren:

1. Installieren Sie die 64-Bit-API (tivoli.tsm.client.api.64bit).
2. Installieren Sie den 64-Bit-Client (tivoli.tsm.client.ba.64bit).

Falls bereits ein 64-Bit-Client von IBM Spectrum Protect Version 6.3 (oder höher) installiert ist, können Sie ein Upgrade des Clients durchführen, statt den Client zu deinstallieren und anschließend erneut zu installieren.

Falls ein 64-Bit-Client einer früheren Version von IBM Spectrum Protect installiert ist (z. B. Version 6.1 oder 6.2), müssen Sie den Client, die Sprachenpakete und die API deinstallieren. Anschließend installieren Sie die neue API und den neuen Client von IBM Spectrum Protect.

Alle zur Installation des Clients benötigten Pakete befinden sich im AIX-Clientpaket; sie überschreiben während der Installation alle älteren ausführbaren Anwendungen auf Ihrem System. Die Laufzeitbibliothek LibC (C Set ++) ist erforderlich.

Wenn Sie für die Installation dieses Clients den Befehl installp verwenden, ändern Sie nicht die Standardfeldwerte für die folgenden beiden Auswahlmöglichkeiten:

- Erforderliche Software AUTOMATISCH installieren?
- Dieselbe Version oder neuere Versionen ÜBERSCHREIBEN?

Werden die Werte inaktiviert oder geändert, kann eine Clientkomponente mit einer niedrigeren Version über eine derzeit installierte Komponente mit einer höheren Version installiert werden. Unter derartigen Umständen könnten Funktionsaufrufe zwischen Komponenten mit unterschiedlichen Versionen nicht mehr gültig sein.

Installieren Sie die folgenden Pakete. Alle diese Pakete sind auf den Installationsmedien verfügbar. Sie benötigen eine Extended Edition-Lizenz für die Verwendung des NAS-Clients.

Die folgenden Dateien sind in der Reihenfolge der Abhängigkeit aufgelistet. Beispielsweise ist die API von Global Security Kit (GSKit) abhängig. Wenn Sie zur Installation aller Dateien SMIT verwenden, können Sie sie in beliebiger Reihenfolge auswählen (F7).

GSKit8.gskcrypt64.ppc.rte und GSKit8.gskssl64.ppc.rte
: IBM® GSKit 64-Bit (wird von der 64-Bit-Client-API benötigt).

tivoli.tsm.client.api.64bit
: Installiert die 64-Bit-API.

tivoli.tsm.client.ba.64bit
: Installiert die folgenden 64-Bit-Clientdateien:

  - Java™-Client für Sichern/Archivieren (GUI)
  - Web-Client für Sichern/Archivieren
  - NAS-Sicherungsclient

tivoli.tsm.filepath_aix
: Installiert die für die journalbasierte Sicherung erforderliche Kernelerweiterung des Dateipfads.

tivoli.tsm.client.jbb.64bit
: Installiert die Komponente für die journalbasierte Sicherung.

Jedes Paket wird in dem folgenden Standardinstallationsverzeichnis installiert:

- Die 64-Bit-Dateien des Clients für Sichern/Archivieren, des Web-Clients und des Verwaltungsclients (dsmadmc) werden im Verzeichnis `/usr/tivoli/tsm/client/ba/bin64` installiert.
- Die 64-Bit-Dateien der IBM Spectrum Protect-API werden im Verzeichnis `/usr/tivoli/tsm/client/api/bin64` installiert.
- Das Beispiel für die Systemoptionsdatei, dsm.sys.smp, wird in das Installationsverzeichnis gestellt.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Wenn Sie die Clientdateien zunächst in ein lokales Verzeichnis kopieren, erstellt der Befehl installp automatisch eine .toc-Datei. Sie können eine .toc-Datei manuell erstellen, indem Sie in dem lokalen Verzeichnis, in das Sie das IBM Spectrum Protect-Image kopiert haben, /usr/sbin/inutoc ausführen. Geben Sie in der AIX-Befehlszeile Folgendes ein:

```
/usr/sbin/inutoc /usr/sys/inst.images
```

Daraufhin wird eine .toc-Datei in dem betreffenden Verzeichnis erstellt.

Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
3. Geben Sie in der AIX-Befehlszeile `smitty install` ein und drücken Sie die Eingabetaste.
4. Wählen Sie Software installieren und aktualisieren aus und drücken Sie die Eingabetaste.
5. Wählen Sie Neueste verfügbare Software installieren und aktualisieren und drücken Sie die Eingabetaste.
6. Drücken Sie bei der Eingabeaufforderung `Eingabeeinheit/-verzeichnis für Software` die Taste F4, geben Sie das Verzeichnis an, das die Installationsimages enthält, und drücken Sie die Eingabetaste.
7. Bei der Eingabeaufforderung `Zu installierende Software` drücken Sie die Taste F4. Wählen Sie die gewünschten IBM Spectrum Protect-Dateigruppen für die Installation aus, indem Sie die Taste F7 drücken. Drücken Sie anschließend die Eingabetaste.
8. Drücken Sie in der Anzeige Von verfügbarer Software installieren und aktualisieren die Taste F4, um Eingabefelder zu ändern, oder verwenden Sie die Standardfelder. Drücken Sie zweimal die Eingabetaste, um mit der Installation zu beginnen.
9. Drücken Sie nach Abschluss der Installation zum Beenden die Taste F10.

Ergebnisse

Wenn Dateigruppen installiert werden, werden sie automatisch im System festgeschrieben. Die vorherige Version der Software des Clients für Sichern/Archivieren wird durch die neu installierte Version ersetzt.

Die Dateien des Clients für Sichern/Archivieren werden im Verzeichnis /usr/tivoli/tsm/client/ba/bin64 installiert. Wenn Sie die Clientdateien in ein anderes Verzeichnis versetzen, müssen Sie die folgenden Schritte ausführen:

1. Stellen Sie sicher, dass sich die Berechtigungen der installierten Dateien nicht geändert haben.
2. Aktualisieren Sie die symbolischen Verbindungen für die installierten Dateien in den folgenden Verzeichnissen:
   - Im Verzeichnis /usr/bin

- Im Verzeichnis /usr/lib für die IBM Spectrum Protect-Bibliotheken

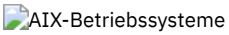
3. Stellen Sie sicher, dass jeder Benutzer des Clients für Sichern/Archivieren die Umgebungsvariable DSM_DIR auf das neu installierte Verzeichnis setzt.

Nächste Schritte

Nach dem Abschluss der Installation sind die in IBM Spectrum Protect-Client konfigurieren beschriebenen erforderlichen und optionalen Tasks auszuführen, bevor der Client für Sichern/Archivieren verwendet werden kann.

Anmerkung:

- AIX-Workloadpartitionen (WPAR) werden folgendermaßen unterstützt:
  - Unterstützung in globalen Umgebungen
  - Unterstützung mit nicht gemeinsam genutzten System-WPARs
  - Unterstützung mit gemeinsam genutzten System-WPARs (für Protokolle und Konfigurationsdateien des Clients für Sichern/Archivieren müssen andere Positionen als die Standardpositionen definiert sein)
  - Keine Unterstützung für Anwendungs-WPARs
  - Keine Unterstützung für Imagesicherung
  - Keine Unterstützung für Zurückschreibung einer Sicherungsgruppe von Band
- Wenn Sie unter AIX Version 6.1 EFS (Encrypted File System) mit dem Client für Sichern/Archivieren verwenden und das Schlüsselspeicherkennwort des EFS-Benutzers nicht mit dem Anmeldekennwort des Benutzers übereinstimmt, wird der EFS-Schlüsselspeicher bei Ihrer Anmeldung nicht automatisch geöffnet. Wenn der EFS-Schlüsselspeicher bei Ihrer Anmeldung nicht geöffnet ist, schreibt der Client eine Nicht-EFS-Datei möglicherweise nicht in ein EFS-Dateisystem zurück. Sie können das Problem beim Zurückschreiben eines EFS-Dateisystems durch eine der folgenden Maßnahmen verhindern:
  - Starten Sie den Client für Sichern/Archivieren mit dem Befehl efskeymgr -o. Zum Beispiel: efskeymgr -o ./dsmj
  - Synchronisieren Sie mit dem Befehl efskeymgr -n das Schlüsselspeicherkennwort mit dem Anmeldekennwort des Benutzers. Zum Beispiel: efskeymgr -n


AIX-Betriebssysteme

AIX-Client deinstallieren

Sie können die folgenden Prozeduren verwenden, um den IBM Spectrum Protect AIX-Client für Sichern/Archivieren zu deinstallieren.

Vorbereitende Schritte

Die IBM Spectrum Protect-Clientmodule und -komponenten sind nahtlos integriert und die installierten Dateigruppen werden automatisch festgeschrieben. Es gibt keine Option für ROLLBACK-Operationen deinstallierter Komponenten.

Vorgehensweise

1. Geben Sie den folgenden AIX-Befehl ein: smitty remove.
2. Drücken Sie die Eingabetaste.
3. Drücken Sie im Namensfeld SOFTWARE die Taste F4, um die IBM Spectrum Protect-Dateigruppen aufzulisten, die Sie deinstallieren wollen; drücken Sie die Eingabetaste.
4. Wählen Sie die IBM Spectrum Protect-Dateigruppen aus, die Sie deinstallieren wollen; drücken Sie die Eingabetaste.
   Anmerkung: Das Feature für die journalbasierte Sicherung befindet sich in zwei Dateigruppen. Wählen Sie sowohl tivoli.tsm.client.jbb.64bit als auch tivoli.tsm.filepath_aix aus. Falls Sie die Dateigruppen nacheinander deinstallieren, deinstallieren Sie zuerst die Dateigruppe tivoli.tsm.client.jbb.64bit.
5. Im Feld Nur Voranzeige? (es findet keine Löschoperation statt) wählen Sie Nein aus; drücken Sie die Eingabetaste.

HP-UX Itanium 2-API installieren

Sie können die HP-UX Itanium 2-API von den Produktinstallationsmedien installieren.

Informationen zu diesem Vorgang

Die folgenden Quellenpakete sind auf den Installationsdatenträgern verfügbar:

`tsmcli/hp11ia64/gskcrypt64-8.x.x.x.hpux.ia64.tar.Z` und `tsmcli/hp11ia64/gskssl64-8.x.x.x.hpux.ia64.tar.Z`
Enthält das GSKit. Wenn Sie eine vorherige Version des GSKit installiert haben, deinstallieren Sie diese, bevor Sie die neue Version installieren.

`tsmcli/hp11ia64/TIVsmCapi64`
In diesem Paket ist `TIVsm64` der Softwareauswahlname, der von swlist für den Produktnamen der höchsten Ebene verwendet wird. Die Komponente unter `TIVsm64` ist `TIVsm.CLIENT_API64`.

Standardinstallationsverzeichnisse

Während der Clientinstallation werden einige Dateien in den folgenden Standardverzeichnissen gespeichert:

- Die Dateien der IBM Spectrum Protect-API werden im Verzeichnis `/opt/tivoli/tsm/client/api/bin64` installiert.
- Die Beispielsystemoptionsdatei `dsm.sys.smp` wird in das Installationsverzeichnis gestellt.

Um frühere Versionen des Clients für Sichern/Archivieren zu entfernen, melden Sie sich als der Rootbenutzer an und geben Sie den folgenden Befehl ein:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64
```

Wenn Sie in einem Client der Version 7.1.2 oder früher zusätzliche Sprachen installiert haben, müssen Sie folgenden Befehl ausführen, um diese zu entfernen:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64.CLIENT_msg_Sprache
```

Ersetzen Sie dabei *Sprache* durch den entsprechenden Sprachencode aus Tabelle 1.

Tabelle 1. HP-UX Itanium 2-Client: Sprachencodes für Installationspakete

Sprache	Sprachencode
Vereinfachtes Chinesisch	ZH_CN
Traditionelles Chinesisch	ZH_TW
Tschechisch	CS_CZ
Französisch	FR_FR
Deutsch	DE_DE
Ungarisch	HU_HU
Italienisch	IT_IT
Japanisch	JA_JP
Koreanisch	KO_KR
Polnisch	PL_PL
Brasilianisches Portugiesisch	PT_BR
Russisch	RU_RU
Spanisch	ES_ES

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
3. Für die Installation des GSKit: Wenn Sie eine vorherige Version von GSKit installiert haben, entfernen Sie diese, bevor Sie die neue Version installieren. Extrahieren Sie den Inhalt der Dateien gskcrypt64-8.x.x.x.hpux.ia64.tar.Z und gskssl64-8.x.x.x.hpux.ia64.tar.Z in ein Verzeichnis auf Ihrer Festplatte. Geben Sie die folgenden Befehle ein, um die Pakete zu installieren:

   ```
   /usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`
     /gskcrypt64 gskcrypt64
   /usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`
     /gskssl64 gskssl64
   ```

4. Wenn Sie von FTP heruntergeladen haben, wechseln Sie in das Verzeichnis, in dem sich das installierbare Image befindet. Geben Sie den folgenden Befehl ein:

   ```
   /usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`/TIVsmCapi64 TIVsm64
   ```

   `` `pwd` `` kann anstelle des absoluten Namens des aktuellen Verzeichnisses verwendet werden.

- Standardbegrenzung für Datensegmentgröße erhöhen
  Die Standardbegrenzung für die Datensegmentgröße eines Prozesses in HP-UX 11i v2 beträgt 64 MB. Wenn große Dateisysteme gesichert werden, wird dieser Grenzwert möglicherweise von der API überschritten und es kann eine abnormale Speicherbedingung auftreten.

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren

HP-UX Itanium 2-API deinstallieren

Sie können die folgenden Prozeduren verwenden, um die IBM Spectrum Protect HP-UX Itanium 2-API zu deinstallieren.

Vorbereitende Schritte

Wichtig: Sie müssen die Pakete in der angegebenen Reihenfolge deinstallieren.

Vorgehensweise

1. Geben Sie den folgenden Befehl ein, um die Dateigruppe CLIENT_API zu entfernen:

   ```
   /usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64
   ```

2. Geben Sie die folgenden Befehle ein, um Global Security Kit (GSKit) zu entfernen:

   ```
   /usr/sbin/swremove -x mount_all_filesystems=false gskssl64
   /usr/sbin/swremoveswremove -x mount_all_filesystems=false gskcrypt64
   ```

Nächste Schritte

Nach der Deinstallation der HP-UX-API verbleiben mehrere leere Verzeichnisse in dem Dateisystem, wie beispielsweise die folgenden Verzeichnisse:

- Das Lizenzverzeichnis (/opt/tivoli/tsm/license)
- Ein oder mehrere Sprachenverzeichnisse (/opt/tivoli/tsm/client/ba/bin/xx_XX); hierbei ist xx_XX einer der folgenden Sprachencodes: `cs_CZ, de_DE, es_ES, it_IT, fr_FR, hu_HU, ja_JP, ko_KR, pl_PL, pt_BR, ru_RU, zh_CN und zh_TW`
- /opt/tivoli/tsm/client/ba/bin/cit
- /opt/tivoli/tsm/client/ba/bin/images
- /opt/tivoli/tsm/client/ba/bin/plugin

Sollen diese leeren Verzeichnisse entfernt werden, können Sie sie manuell entfernen.

Linux-Betriebssysteme

Client für Sichern/Archivieren unter Linux on Power Systems (Little Endian) installieren

Sie können den Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Informationen zu diesem Vorgang

Die folgenden Installationsoptionen sind in nicht komprimierten Paketen auf den Installationsmedien verfügbar.

Tabelle 1. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64-8.x.x.x.linux.ppcle.rpm gskssl64-8.x.x.x.linux.ppcle.rpm	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8

Paketname	Inhalt	Standardverzeichnis
TIVsm-API64.ppc64le.rpm	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64
TIVsm-BA.ppc64le.rpm	Client für Sichern/Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadmc) und Web-Client	/opt/tivoli/tsm/client/ba/bin Dieses Verzeichnis ist normalerweise das Standardinstallationsverzeichnis für viele Dateien des Clients für Sichern/Archivieren. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Wenn Sie die Umgebungsvariable DSM_DIR nicht definieren, werden die ausführbare Datei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis gespeichert. Wenn Sie die Umgebungsvariable DSM_CONFIG nicht definieren, muss sich die Clientbenutzeroptionsdatei in diesem Verzeichnis befinden. Wenn Sie die Umgebungsvariable DSM_LOG nicht definieren, schreibt der Client für Sichern/Archivieren Nachrichten in die Dateien dsmerror.log und dsmsched.log des aktuellen Arbeitsverzeichnisses.
TIVsm-APIcit.ppc64le.rpm TIVsm-BAcit.ppc64le.rpm	Diese Dateien stellen die Common Inventory Technology-Komponenten bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Diese Dateien sind optional. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Dokumentation zum IBM Spectrum Protect-Server.	APIcit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit installiert. BAcit wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin/cit installiert.
TIVsm-filepath-source.tar.gz TIVsm-JBB.ppc64le.rpm	Für journalbasierte Sicherungen benötigte Dateien.	Die Pakete filepath und TIVsm-JBB sind nur erforderlich, wenn Sie journalbasierte Sicherungen verwenden wollen. Filepath wird in /opt/filepath installiert. Das Paket TIVsm-JBB.ppc64le.rpm wird in /opt/tivoli/tsm/client/ba/bin installiert.

Vorgehensweise

1. Stellen Sie den Datenträger bereit, von dem die Pakete installiert werden.
2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In dem folgenden Befehlsbeispiel stehen die Zeichen "8.x.x.x" für die GSKit-Version:

   ```
   rpm -U gskcrypt64-8.x.x.x.linux.ppcle.rpm gskssl64-8.x.x.x.linux.ppcle.rpm
   ```

4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
   a. Erforderlich: Installieren Sie die API:

      ```
      rpm -ivh TIVsm-API64.ppc64le.rpm
      ```

   b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

      ```
      rpm -ivh TIVsm-APIcit.ppc64le.rpm
      ```

   Tipp: Wenn Sie für die API ein Upgrade durchführen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl für das API-Paket als auch für das Common Inventory Technology-Paket ein Upgrade durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

```
rpm -U TIVsm-API64.ppc64le.rpm TIVsm-APIcit.ppc64le.rpm
```

Falls Sie lediglich eine Installation der API benötigen, können Sie die Prozedur an dieser Stelle beenden. Die nachfolgenden Schritte in dieser Prozedur beschreiben, wie die Komponenten für den Client für Sichern/Archivieren und ein optionales Clientpaket installiert werden, das nur dann benötigt wird, wenn der Client PVU-Messwerte an den Server senden soll. In den nachfolgenden Schritten ist außerdem die Installation der Pakete beschrieben, die Sie benötigen, wenn Sie journalbasierte Sicherungen ausführen wollen.

5. Installieren Sie den Client für Sichern/Archivieren und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
   a. Installieren Sie die Komponenten des Clients für Sichern/Archivieren.

      ```
      rpm -ivh TIVsm-BA.ppc64le.rpm
      ```

   b. Optional: Installieren Sie das Common Inventory Technology-Paket, das vom Client verwendet wird, um PVU-Messwerte an den Server zu senden. Dieses Paket ist vom Clientpaket abhängig und muss daher nach der Installation des Clientpakets installiert werden.

      ```
      rpm -ivh TIVsm-BAcit.ppc64le.rpm
      ```

6. Optional: Falls Sie journalbasierte Sicherungen verwenden wollen, installieren Sie die Pakete, die für die Dateipfadkomponente und die journalbasierten Sicherungen erforderlich sind.
   a. Extrahieren Sie TIVsm-filepath-source.tar.gz und lesen Sie die Kompilier- und Installationsanweisungen in der README-Datei. Das Kernelmodul für den Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.
   b. Installieren Sie das Paket für die journalbasierte Sicherung:

      ```
      rpm -ivh TIVsm-JBB.ppc64le.rpm
      ```

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
Linux-Betriebssysteme

Client für Sichern/Archivieren unter Linux on Power Systems (Little Endian) deinstallieren

Sie können den IBM Spectrum Protect-Client unter Linux on Power Systems (Little Endian) deinstallieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt deinstallieren zu können. Sie müssen die Pakete in der angezeigten Reihenfolge deinstallieren, andernfalls schlägt die Deinstallation fehl.

Vorgehensweise

Um den Client für Sichern/Archivieren zu deinstallieren, geben Sie die folgenden Befehle ein. Mit diesen Befehlen werden die Pakete für die journalbasierte Sicherung, die Dateipfadkomponente, den Client für Sichern/Archivieren, die API und IBM Global Security Kit (GSKit) entfernt.

Tipp: Die Versionsnummer der Pakete ist nicht erforderlich.

1. Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie beide Pakete (journalbasierte Sicherung und Dateipfad). Das Paket TIVsm-JBB ist vom Dateipfadpaket abhängig. Wenn Sie zwei separate Befehle rpm -e verwenden, um die Komponenten nacheinander zu deinstallieren, deinstallieren Sie zuerst das Paket TIVsm-JBB.

   ```
   rpm -e TIVsm-JBB TIVsm-filepath
   ```

2. Deinstallieren Sie das Paket für den Client für Sichern/Archivieren:

   ```
   rpm -e TIVsm-BA
   ```

3. Deinstallieren Sie die Pakete für den Client für Sichern/Archivieren:
   a. Wenn das Common Inventory Technology-Paket für den Client (TIVsmBAcit) installiert wurde, deinstallieren Sie es:

      ```
      rpm -e TIVsm-BAcit
      ```

   b. Deinstallieren Sie das Paket für den Client für Sichern/Archivieren:

      ```
      rpm -e TIVsm-BA
      ```

4. Deinstallieren Sie Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail. Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Befolgen Sie die Anweisungen in den von der API abhängigen Produkten, um zu bestimmen, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.

5. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

```
rpm -e TIVsm-API64
```

6. Deinstallieren Sie die API-Pakete:
   a. Wenn das Common Inventory Technology-Paket für die API (TIVsm-APIcit installiert wurde, deinstallieren Sie es:

```
rpm -e TIVsm-APIcit
```

   b. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

```
rpm -e TIVsm-API64
```

7. Deinstallieren Sie GSKit, indem Sie den folgenden Befehl eingeben:

```
rpm -e gskcrypt64 gskssl64
```

Zugehörige Tasks:
Client für Sichern/Archivieren unter Linux on Power Systems (Little Endian) installieren
Linux-Betriebssysteme

Client für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) installieren

Sie können den Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen als der Rootbenutzer angemeldet sein, um das Produkt installieren zu können.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Informationen zu diesem Vorgang

Die folgenden Installationspakete sind auf den Installationsmedien verfügbar.

Tabelle 1. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64_8.x.x.x.ppc64el.deb gskssl64_8.x.x.x.ppc64el.deb	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8
tivsm-api64.ppc64el.deb	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzte Bibliothek und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64

Paketname	Inhalt	Standardverzeichnis
tivsm-ba.ppc64el.deb	Client für Sichern/Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadmc) und Web-Client	/opt/tivoli/tsm/client/ba/bin Dieses Verzeichnis ist normalerweise das Standardinstallationsverzeichnis für viele Dateien des Clients für Sichern/Archivieren. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Wenn Sie die Umgebungsvariable DSM_DIR nicht definieren, werden die ausführbare Datei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis gespeichert. Wenn Sie die Umgebungsvariable DSM_CONFIG nicht definieren, muss sich die Clientbenutzeroptionsdatei in diesem Verzeichnis befinden. Wenn Sie die Umgebungsvariable DSM_LOG nicht definieren, schreibt der Client für Sichern/Archivieren Nachrichten in die Dateien dsmerror.log und dsmsched.log des aktuellen Arbeitsverzeichnisses.
TIVsm-filepath-source.tar.gz tivsm-jbb.ppc64el.deb	Dateien, die für journalbasierte Sicherungen erforderlich sind	Das Paket TIVsm-filepath-source.tar.gz wird im Verzeichnis /opt/filepath installiert. Das Paket tivsm-jbb.ppc64el.rpm wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin installiert.

Vorgehensweise

1. Stellen Sie den Datenträger bereit, von dem die Pakete installiert werden.
2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In dem folgenden Befehlsbeispiel stehen die Zeichen "8.x.x.x" für die GSKit-Version:

   ```
   dpkg -i gskcrypt64_8.x.x.x.ppc64el.deb gskssl64_8.x.x.x.ppc64el.deb
   ```

4. Installieren Sie die IBM Spectrum Protect-API:

   ```
   dpkg -i tivsm-api64.ppc64el.deb
   ```

   Wenn nur die API installiert werden muss, können Sie die Prozedur an dieser Stelle stoppen. Führen Sie die folgenden Schritte aus, um den Client für Sichern/Archivieren und die für die Ausführung journalbasierter Sicherungen erforderlichen Pakete zu installieren.

5. Installieren Sie den Client für Sichern/Archivieren:

   ```
   dpkg -i tivsm-ba.ppc64el.deb
   ```

6. Optional: Wenn journalbasierte Sicherungen verwendet werden sollen, installieren Sie die folgenden Pakete:
   a. Extrahieren Sie TIVsm-filepath-source.tar.gz und prüfen Sie die README-Datei auf Anweisungen zur Vorgehensweise beim Kompilieren und Installieren der Software. Das Kernelmodul für den Linux-Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.
   b. Installieren Sie das Paket für die journalbasierte Sicherung:

      ```
      dpkg -i tivsm-jbb.ppc64el.deb
      ```

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
Linux-Betriebssysteme

Client unter Ubuntu Linux on Power Systems (Little Endian) deinstallieren

Sie können den IBM Spectrum Protect-Client für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) deinstallieren.

Vorbereitende Schritte

Sie müssen als der Rootbenutzer angemeldet sein, um das Produkt deinstallieren zu können.
Voraussetzung: Sie müssen die Pakete in der angezeigten Reihenfolge deinstallieren, andernfalls schlägt die Deinstallation fehl.

Vorgehensweise

Um den Client für Sichern/Archivieren zu deinstallieren, geben Sie die folgenden Befehle ein. Mit diesen Befehlen werden die Pakete für die journalbasierte Sicherung, den Client für Sichern/Archivieren, die API und IBM Global Security Kit (GSKit) entfernt. Anweisungen zur Deinstallation der Dateipfadkomponente werden mit dem Quellcode für den Dateipfad zusammen mit der Software von IBM® bereitgestellt.

Tipp: Die Versionsnummer der Pakete ist nicht erforderlich.

1. Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie das Paket tivsm-jbb und das Dateipfadpaket. Das Paket tivsm-jbb ist vom Dateipfadpaket abhängig. Deinstallieren Sie das Paket tivsm-jbb zuerst.
   a. `dpkg -r tivsm-jbb`
   b. `dpkg -r TIVsm-filepath`
2. Deinstallieren Sie das Paket für den Client für Sichern/Archivieren:

   ```
   dpkg -r tivsm-ba
   ```

3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail.

   Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Befolgen Sie die Anweisungen in den von der API abhängigen Produkten, um zu bestimmen, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.

4. Deinstallieren Sie das API-Paket, indem Sie den folgenden Befehl ausgeben:

   ```
   dpkg -r tivsm-api64
   ```

5. Entfernen Sie die GSKit-Pakete:

   ```
   dpkg -r gskcrypt64 gskssl64
   ```

Zugehörige Tasks:
Client für Sichern/Archivieren unter Ubuntu Linux on Power Systems (Little Endian) installieren
Linux-Betriebssysteme

API unter Linux on Power Systems (Big Endian) installieren

Sie können die IBM Spectrum Protect-API von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können.

Informationen zu diesem Vorgang

Falls IBM Spectrum Protect Version 6.2 (oder eine frühere Version) installiert ist, entfernen Sie diese Version (rpm -e) und alle anderen abhängigen Softwareprogramme, bevor Sie eine höhere Version installieren.

Falls IBM Spectrum Protect Version 6.3 (oder höher) installiert ist, können Sie die Upgradeoption von rpm (rpm -U) oder die Aktualisierungsoption von rpm (rpm -F) verwenden, um für die vorhandene Software ein Upgrade auf eine höhere Version durchzuführen. Mit dem Befehl rpm -U können Sie neue Pakete installieren oder für vorhandene Pakete ein Upgrade durchführen; rpm -F kann lediglich zum Aktualisieren von bereits installierten Paketen verwendet werden.

Stoppen Sie alle aktiven Clientprozesse, bevor Sie eine Deinstallation oder ein Upgrade der API oder des Clients für Sichern/Archivieren von IBM Spectrum Protect durchführen. Wenn Sie einen Client der Version 7.1.2 oder früher verwenden, müssen Sie alle Sprachenpakete deinstallieren, bevor Sie mit dem Upgrade fortfahren.

Tabelle 1 zeigt die Installationsoptionen, die in nicht komprimierten Paketen auf den Installationsmedien verfügbar sind.

Tabelle 1. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64-8.x.x.x.linux.ppc.rpm gskssl64-8.x.x.x.linux.ppc.rpm	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8
TIVsm-API64.ppc64.rpm	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64

Paketname	Inhalt	Standardverzeichnis
TIVsm-APIcit.ppc64.rpm	Optional. Diese Dateien stellen die Common Inventory Technology-Komponenten bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Dokumentation zum IBM Spectrum Protect-Server.	APIcit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit installiert.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

1. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In diesem Beispiel stehen die Zeichen "8.x.x.x" für die GSKit-Version:

   ```
   rpm -U gskcrypt64-8.x.x.x.linux.ppc.rpm gskssl64-8.x.x.x.linux.ppc.rpm
   ```

4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
   a. Erforderlich: Installieren Sie die API:

      ```
      rpm -i TIVsm-API64.ppc64.rpm
      ```

   b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

      ```
      rpm -i TIVsm-APIcit.ppc64.rpm
      ```

   Tipp: Wenn Sie für die API ein Upgrade durchführen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl für das API-Paket als auch für das Common Inventory Technology-Paket ein Upgrade durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

   ```
   rpm -U TIVsm-API64.ppc64.rpm TIVsm-APIcit.ppc64.rpm
   ```

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
Linux-Betriebssysteme

API unter Linux on Power Systems (Big Endian) deinstallieren

Sie können die IBM Spectrum Protect-API unter IBM Spectrum Protect Linux on Power Systems (Big Endian) deinstallieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt deinstallieren zu können. Deinstallieren Sie die Pakete in der angezeigten Reihenfolge.

Vorgehensweise

Um ein zuvor installiertes IBM Spectrum Protect-Paket zu deinstallieren, geben Sie die folgenden Befehle ein, um die Pakete für die journalbasierte Sicherung, die Dateipfadkomponente, den Client für Sichern/Archivieren (falls zutreffend), die API und IBM Global Security Kit (GSKit) zu entfernen.

Tipp: Die Versionsnummer der Pakete wird für die Deinstallation nicht benötigt.

1. Führen Sie diesen Schritt aus, wenn zuvor ein Client der Version 7.1 oder früher installiert wurde.

Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie beide Pakete (journalbasierte Sicherung und Dateipfad). Das Paket TIVsm-JBB ist vom Dateipfadpaket abhängig. Wenn Sie zwei separate Befehle rpm -e verwenden, um die Komponenten nacheinander zu deinstallieren, deinstallieren Sie zuerst das Paket TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Wenn zuvor ein Client der Version 7.1 oder früher installiert wurde, deinstallieren Sie die Pakete für den Clients für Sichern/Archivieren.
   a. Wenn das optionale Paket TIVsmBAcit installiert wurde, deinstallieren Sie es mithilfe des folgenden Befehls:

      ```
      rpm -e TIVsm-BAcit
      ```

   b. Deinstallieren Sie das Paket für den Client für Sichern/Archivieren:

      ```
      rpm -e TIVsm-BA
      ```

   Anmerkung: Wenn Sprachenpakete in einem Client der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl ein und ersetzen Sie hierbei *xx_xx* jeweils durch den Sprachencode jeder zusätzlichen Sprache, die installiert wurde. Eine Liste der Sprachencodekennungen finden Sie in Tabelle 1.

   ```
   rpm -e TIVsm-BA.msg.xx_xx
   ```

   Tabelle 1. Kennungen der Sprachenpakete

Sprache	**Sprachenkennung**
Tschechisch	CS_CZ
Französisch	FR_FR
Deutsch	DE_DE
Ungarisch	HU_HU
Italienisch	IT_IT
Japanisch	JA_JP
Koreanisch	KO_KR
Polnisch	PL_PL
Portugiesisch	PT_BR
Russisch	RU_RU
Spanisch	ES_ES
Traditionelles Chinesisch (erweiterter UNIX-Code)	ZH_CN
Traditionelles Chinesisch (Big-5; die fünf wichtigsten DBCS-Sprachen)	ZH_TW

3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail. Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Wenn Sie ein API-abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version des API-Pakets erneut installieren. Anhand der Dokumentation des abhängigen Produkts können Sie ermitteln, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.
4. Wenn das optionale Common Inventory Technology-Paket für die API (TIVsm-APIcit) installiert wurde, deinstallieren Sie dieses Paket mithilfe des folgenden Befehls:

   ```
   rpm -e TIVsm-APIcit
   ```

5. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

   ```
   rpm -e TIVsm-API64
   ```

6. Deinstallieren Sie GSKit mithilfe des folgenden Befehls:

   ```
   rpm -e gskcrypt64 gskssl64
   ```

Zugehörige Tasks:
API unter Linux on Power Systems (Big Endian) installieren
Linux-Betriebssysteme

Linux x86_64-Client installieren

Sie können den Linux x86_64-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

- Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können.

- Falls IBM Spectrum Protect Version 6.2 (oder eine frühere Version) installiert ist, entfernen Sie diese Version (rpm -e) und alle anderen abhängigen Softwareprogramme, bevor Sie eine höhere Version installieren.
- Falls IBM Spectrum Protect Version 6.3 (oder höher) installiert ist, können Sie die Upgradeoption von rpm (rpm -U) oder die Aktualisierungsoption von rpm (rpm -F) verwenden, um für die vorhandene Software ein Upgrade auf eine höhere Version durchzuführen. Mit dem Befehl rpm -U können Sie nur dann neue Pakete installieren oder für vorhandene Pakete ein Upgrade durchführen, wenn Sie zuvor keine Sprachenpakete installiert haben. Mit dem Befehl rpm -F können nur bereits installierte Pakete aktualisiert werden.
- Stoppen Sie alle aktiven Clientprozesse, bevor Sie eine Deinstallation oder ein Upgrade der API oder des Clients für Sichern/Archivieren von IBM Spectrum Protect durchführen.
- Wenn Sprachenpakete installiert sind, müssen Sie diese Pakete vor der Installation oder einem Upgrade der API oder des Clients für Sichern/Archivieren von IBM Spectrum Protect deinstallieren.

Informationen zu diesem Vorgang

Die folgenden Installationsoptionen sind in nicht komprimierten Paketen auf den Installationsmedien verfügbar.

Tabelle 1. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64-8.x.x.x.linux.x86_64.rpm gskssl64-8.x.x.x.linux.x86_64.rpm	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8
TIVsm-API64.x86_64.rpm	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64
TIVsm-BA.x86_64.rpm	Client für Sichern/Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadmc) und Web-Client	/opt/tivoli/tsm/client/ba/bin Dieses Verzeichnis wird für viele Dateien des Clients für Sichern/Archivieren als Standardinstallationsverzeichnis verwendet. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Falls die Umgebungsvariable DSM_DIR nicht definiert ist, werden die ausführbare Datei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis abgelegt. Falls die Umgebungsvariable DSM_CONFIG nicht definiert ist, muss sich die Clientbenutzeroptionsdatei in diesem Verzeichnis befinden. Wenn Sie DSM_LOG nicht definieren, werden Nachrichten in die Dateien dsmerror.log und dsmsched.log im aktuellen Arbeitsverzeichnis geschrieben.
TIVsm-APIcit.x86_64.rpm TIVsm-BAcit.x86_64.rpm	Optional. Diese Dateien stellen die Common Inventory Technology-Komponenten bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Dokumentation zum IBM Spectrum Protect-Server.	APIcit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit/ installiert. BAcit wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin/cit/ installiert.
TIVsm-filepath-source.tar.gz TIVsm-JBB.x86_64.rpm	Für die Unterstützung journalbasierter Sicherungen benötigte Dateien.	Filepath wird in /opt/filepath installiert. JBB wird in /opt/tivoli/tsm/client/ba/bin installiert.

Paketname	Inhalt	Standardverzeichnis
TIVsm_BAhdw.x86_64.rpm	Stellt die Unterstützung von Momentaufnahmeteilsicherungen für NetAPP- und N-Series-Dateiserver bereit.	/opt/tivoli/tsm/client/ba/bin/plugins

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Linux x86_64-Client für Sichern/Archivieren zu installieren:

1. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In diesem Beispiel stehen die Zeichen "8.x.x.x" für die GSKit-Version:

   ```
   rpm -U gskcrypt64-8.x.x.x.linux.x86_64.rpm gskssl64-8.x.x.x.linux.x86_64.rpm
   ```

4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
   a. Erforderlich: Installieren Sie die API:

      ```
      rpm -i TIVsm-API64.x86_64.rpm
      ```

   b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

      ```
      rpm -i TIVsm-APIcit.x86_64.rpm
      ```

   Tipp: Wenn Sie für die API ein Upgrade durchführen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl für das API-Paket als auch für das Common Inventory Technology-Paket ein Upgrade durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

   ```
   rpm -U TIVsm-API64.x86_64.rpm TIVsm-APIcit.x86_64.rpm
   ```

   Falls Sie lediglich eine Installation der API benötigen, können Sie die Prozedur an dieser Stelle beenden. Die nachfolgenden Schritte in dieser Prozedur beschreiben, wie die Komponenten für den Client für Sichern/Archivieren und ein optionales Clientpaket installiert werden, das nur dann benötigt wird, wenn der Client PVU-Messwerte an den Server senden soll. In den nachfolgenden Schritten ist außerdem die Installation der Pakete beschrieben, die Sie benötigen, wenn Sie journalbasierte Sicherungen ausführen wollen.

5. Installieren Sie den Client für Sichern/Archivieren und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
   a. Installieren Sie die Komponenten des Clients für Sichern/Archivieren.

      ```
      rpm -i TIVsm-BA.x86_64.rpm
      ```

   b. Optional: Installieren Sie das Common Inventory Technology-Paket, das vom Client verwendet wird, um PVU-Messwerte an den Server zu senden. Dieses Paket ist vom Clientpaket abhängig und muss daher nach der Installation des Clientpakets installiert werden.

      ```
      rpm -i TIVsm-BAcit.x86_64.rpm
      ```

6. Optional: Sollen journalbasierte Sicherungen verwendet werden, müssen Sie die Dateipfadkomponente kompilieren und installieren, die dem Linux-Kernel auf Ihrem Client-Computer entspricht. Extrahieren Sie TIVsm-filepath-source.tar.gz und lesen Sie die Kompilier- und Installationsanweisungen in der README-Datei. Das Kernelmodul für den Linux-Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.
7. Installieren Sie die Unterstützung für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz für NetApp- und N-Series-Dateiserver, indem Sie den folgenden Befehl eingeben:

   ```
   rpm -i TIVsm-BAhdw.x86_64.rpm
   ```

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
Linux-Betriebssysteme

Linux x86_64-Client deinstallieren

Sie können die folgende Prozedur verwenden, um den IBM Spectrum Protect Linux x86_64-Client zu deinstallieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt deinstallieren zu können. Deinstallieren Sie die Pakete in der angezeigten Reihenfolge.

Vorgehensweise

Um ein zuvor installiertes IBM Spectrum Protect-Clientpaket zu deinstallieren, geben Sie die folgenden Befehle ein. Mit diesen Befehlen werden die Pakete für die journalbasierte Sicherung, die Dateipfadkomponente, den Client für Sichern/Archivieren, die API und IBM Global Security Kit (GSKit) entfernt.

Tipp: Die Versionsnummer der Pakete wird für die Deinstallation nicht benötigt.

1. Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie beide Pakete (journalbasierte Sicherung und Dateipfad). Das Paket TIVsm-JBB ist vom Dateipfadpaket abhängig. Wenn Sie zwei separate Befehle rpm -e verwenden, um die Komponenten nacheinander zu deinstallieren, deinstallieren Sie zuerst das Paket TIVsm-JBB.

   ```
   rpm -e TIVsm-JBB TIVsm-filepath
   ```

2. Deinstallieren Sie die Pakete für den Client für Sichern/Archivieren:
   a. Falls das optionale Paket TIVsm-BAcit installiert wurde, deinstallieren Sie es, bevor Sie den Client deinstallieren:

      ```
      rpm -e TIVsm-BAcit
      ```

   b. Deinstallieren Sie den Client für Sichern/Archivieren.

      ```
      rpm -e TIVsm-BA
      ```

   Anmerkung: Wenn Sprachenpakete in einem Client der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl ein und ersetzen Sie hierbei *xx_xx* jeweils durch den Sprachencode jeder zusätzlichen Sprache, die installiert wurde. Eine Liste der Sprachencodekennungen finden Sie in Tabelle 1.

   ```
   rpm -e TIVsm-msg.xx_xx
   ```

   Tabelle 1. Kennungen der Sprachenpakete

Sprache	Sprachenkennung
Tschechisch	CS_CZ
Französisch	FR_FR
Deutsch	DE_DE
Ungarisch	HU_HU
Italienisch	IT_IT
Japanisch	JA_JP
Koreanisch	KO_KR
Polnisch	PL_PL
Portugiesisch	PT_BR
Russisch	RU_RU
Spanisch	ES_ES
Traditionelles Chinesisch (erweiterter UNIX-Code)	ZH_CN
Traditionelles Chinesisch (Big-5; die fünf wichtigsten DBCS-Sprachen)	ZH_TW

3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail. Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Anhand der Dokumentation des abhängigen Produkts können Sie ermitteln, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.
   a. Falls das optionale Common Inventory Technology-Paket für die API (TIVsm-APIcit) installiert wurde, deinstallieren Sie dieses Paket, bevor Sie das API-Paket deinstallieren. Verwenden Sie zum Deinstallieren des Pakets den folgenden Befehl:

      ```
      rpm -e TIVsm-APIcit
      ```

   b. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

```
rpm -e TIVsm-API64
```

4. Geben Sie den folgenden Befehl ein, um das 64-Bit-Paket von GSKit zu entfernen:

```
rpm -e gskcrypt64 gskssl64
```

Zugehörige Tasks:
Linux x86_64-Client installieren
Linux-Betriebssysteme

Ubuntu Linux x86_64-Client installieren

Sie können den Ubuntu Linux 64-Bit-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Informationen zu diesem Vorgang

Die folgenden Installationsoptionen sind in nicht komprimierten Paketen auf den Installationsmedien verfügbar.

Tabelle 1. Paketnamen, Inhalt und Standardverzeichnis

Paketname	Inhalt	Standardverzeichnis
gskcrypt64_8.0-50.40.linux.x86_64.deb gskssl64_8.0-50.40.linux.x86_64.deb	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8
tivsm-api64.amd64.deb	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64
tivsm-ba.amd64.deb	Client für Sichern/Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadmc) und Web-Client	/opt/tivoli/tsm/client/ba/bin Dieses Verzeichnis wird für viele Dateien des Clients für Sichern/Archivieren als Standardinstallationsverzeichnis verwendet. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Falls die Umgebungsvariable DSM_DIR nicht definiert ist, werden die ausführbare Datei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis abgelegt. Falls die Umgebungsvariable DSM_CONFIG nicht definiert ist, muss sich die Clientbenutzeroptionsdatei in diesem Verzeichnis befinden. Wenn Sie DSM_LOG nicht definieren, werden Nachrichten in die Dateien dsmerror.log und dsmsched.log im aktuellen Arbeitsverzeichnis geschrieben.
tivsm-apicit.amd64.deb tivsm-bacit.amd64.deb	Optional. Diese Dateien stellen die Common Inventory Technology-Komponenten bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Dokumentation zum IBM Spectrum Protect-Server.	APIcit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit installiert. BAcit wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin/cit installiert.

Paketname	Inhalt	Standardverzeichnis
tivsm-filepath-source.tar.gz tivsm-jbb.amd64.deb	Für die Unterstützung journalbasierter Sicherungen benötigte Dateien.	Die Pakete filepath und tivsm-jbb sind nur erforderlich, wenn Sie journalbasierte Sicherungen verwenden wollen. Das Paket tivsm-jbb.x86_64.deb wird in /opt/tivoli/tsm/client/ba/bin installiert.
tivsm-bahdw.amd64.deb	Stellt die Unterstützung von Momentaufnahmeteilsicherungen für NetAPP- und N-Series-Dateiserver bereit.	/opt/tivoli/tsm/client/ba/bin/plugins

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Ubuntu Linux x86_64-Client für Sichern/Archivieren zu installieren.

1. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
2. Wechseln Sie in das Verzeichnis, in dem die Installationspakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete.

   ```
   sudo dpkg -i gskcrypt64_8.0-50.40.linux.x86_64.deb gskssl64_8.0-50.40.linux.x86_64.deb
   ```

4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
   a. Erforderlich: Installieren Sie die API:

      ```
      sudo dpkg -i tivsm-api64.amd64.deb
      ```

   b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

      ```
      sudo dpkg -i tivsm-apicit.amd64.deb
      ```

   Falls Sie lediglich eine Installation der API benötigen, können Sie die Prozedur an dieser Stelle beenden. Die nachfolgenden Schritte in dieser Prozedur beschreiben, wie die Komponenten für den Client für Sichern/Archivieren und ein optionales Clientpaket installiert werden, das nur dann benötigt wird, wenn der Client PVU-Messwerte an den Server senden soll. In den nachfolgenden Schritten ist außerdem die Installation der Pakete beschrieben, die Sie benötigen, wenn Sie journalbasierte Sicherungen ausführen wollen.

5. Installieren Sie den Client für Sichern/Archivieren und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
   a. Installieren Sie die Komponenten des Clients für Sichern/Archivieren.

      ```
      sudo dpkg -i tivsm-ba.amd64.deb
      ```

   b. Optional: Installieren Sie das Common Inventory Technology-Paket, das vom Client verwendet wird, um PVU-Messwerte an den Server zu senden. Dieses Paket ist vom Clientpaket abhängig und muss daher nach der Installation des Clientpakets installiert werden.

      ```
      sudo dpkg -i tivsm-bacit.amd64.deb
      ```

6. Optional: Führen Sie diesen Schritt nur aus, wenn Sie journalbasierte Sicherungen verwenden wollen.
   a. Extrahieren Sie tivsm-filepath-source.tar.gz und lesen Sie die Kompilier- und Installationsanweisungen in der README-Datei. Das Kernelmodul für den Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.
   b. Installieren Sie das Paket für die journalbasierte Sicherung: `dpkg -i tivsm-jbb.amd64.deb`.
7. Installieren Sie die Unterstützung für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz für NetApp- und N-Series-Dateiserver, indem Sie den folgenden Befehl eingeben:

   ```
   sudo dpkg -i tivsm-bahdw.amd64.deb
   ```

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
Linux-Betriebssysteme

Ubuntu Linux x86_64-Client deinstallieren

Verwenden Sie die folgende Prozedur, um den IBM Spectrum Protect Ubuntu Linux x86_64-Client zu deinstallieren.

Vorgehensweise

Um ein zuvor installiertes IBM Spectrum Protect-Clientpaket zu deinstallieren, geben Sie die folgenden Befehle ein, um die Pakete für die journalbasierte Sicherung, den Client für Sichern/Archivieren, die API und IBM Global Security Kit (GSKit) zu entfernen. Anweisungen zur Deinstallation der Dateipfadkomponente erhalten Sie mit dem Quellcode für den Dateipfad zusammen mit der Software von IBM®.

1. Wenn Sie lediglich die Komponenten für die journalbasierte Sicherung deinstallieren wollen, entfernen Sie tivsm-jbb und die Dateipfadkomponente. Das Paket tivsm-jbb ist vom Dateipfadpaket abhängig. Deinstallieren Sie das Paket tivsm-jbb zuerst.
   a. `sudo dpkg -r tivsm-jbb`
   b. `sudo dpkg -r tivsm-filepath`
2. Deinstallieren Sie die Pakete für den Client für Sichern/Archivieren:
   a. Falls das optionale Paket tivsm-bacit installiert wurde, deinstallieren Sie es, bevor Sie den Client deinstallieren:

      ```
      sudo dpkg -r tivsm-bacit
      ```

   b. Deinstallieren Sie den Client für Sichern/Archivieren.

      ```
      sudo dpkg -r tivsm-ba
      ```

   Anmerkung: Wenn Sprachenpakete in einem Client der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl ein und ersetzen Sie hierbei *xx-xx* jeweils durch den Sprachencode jeder zusätzlichen Sprache, die installiert wurde. Eine Liste der Sprachencodekennungen finden Sie in Tabelle 1.

   ```
   dpkg -r tivsm-msg.xx-xx
   ```

   Tabelle 1. Kennungen der Sprachenpakete

Sprache	Sprachenkennung
Tschechisch	cs-cz
Französisch	fr-fr
Deutsch	de-de
Ungarisch	hu-hu
Italienisch	it-it
Japanisch	ja-jp
Koreanisch	ko-kr
Polnisch	pl-pl
Portugiesisch	pt-br
Russisch	ru-ru
Spanisch	es-es
Traditionelles Chinesisch (erweiterter UNIX-Code)	zh-cn
Traditionelles Chinesisch (Big-5; die fünf wichtigsten DBCS-Sprachen)	zh-tw

3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, z. B. IBM Spectrum Protect Data Protection-Produkte. Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Anhand der Dokumentation des abhängigen Produkts können Sie ermitteln, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.
   a. Falls das optionale Common Inventory Technology-Paket für die API (tivsm-apicit) installiert wurde, deinstallieren Sie dieses Paket, bevor Sie das API-Paket deinstallieren. Verwenden Sie zum Deinstallieren des Pakets den folgenden Befehl:

      ```
      sudo dpkg -r tivsm-apicit
      ```

   b. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

      ```
      sudo dpkg -r tivsm-api64
      ```

4. Geben Sie den folgenden Befehl ein, um die 64-Bit-Pakete von GSKit zu entfernen:

   ```
   sudo dpkg -r gskcrypt64 gskssl64
   ```

Zugehörige Tasks:
Ubuntu Linux x86_64-Client installieren
Linux-Betriebssysteme

Linux on System z-Client installieren

Sie können den Linux on System z-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können.

Informationen zu diesem Vorgang

Falls IBM Spectrum Protect Version 6.2 (oder eine frühere Version) installiert ist, entfernen Sie diese Version (rpm -e) und alle anderen abhängigen Softwareprogramme, bevor Sie eine höhere Version installieren.

Falls IBM Spectrum Protect Version 6.3 (oder höher) installiert ist, können Sie die Upgradeoption von rpm (rpm -U) oder die Aktualisierungsoption von rpm (rpm -F) verwenden, um für die vorhandene Software ein Upgrade auf eine höhere Version durchzuführen. Mit dem Befehl rpm -U können Sie neue Pakete installieren oder für vorhandene Pakete ein Upgrade durchführen; rpm -F kann lediglich zum Aktualisieren von bereits installierten Paketen verwendet werden.

Stoppen Sie alle aktiven Clientprozesse, bevor Sie eine Deinstallation oder ein Upgrade der API oder des Clients für Sichern/Archivieren von IBM Spectrum Protect durchführen. Wenn Sie einen Client der Version 7.1.2 oder früher verwenden, müssen Sie alle Sprachenpakete deinstallieren, bevor Sie mit dem Upgrade fortfahren.

Die folgenden Installationsoptionen sind in nicht komprimierten Paketen auf den Installationsmedien verfügbar.

Tabelle 1. Paketnamen, Inhalt und Standardverzeichnis

Paketname	**Inhalt**	**Standardverzeichnis**
gskcrypt64-8.x.x.x.linux.s390x.rpm gskssl64-8.x.x.x.linux.s390x.rpm	64-Bit-Version der Global Security Kit-Pakete (GSKit)	/usr/local/ibm/gsk8
TIVsm-API64.s390x.rpm	Anwendungsprogrammierschnittstelle (API), die die gemeinsam genutzten Bibliotheken und Beispiele für die IBM Spectrum Protect-API enthält.	/opt/tivoli/tsm/client/api/bin64
TIVsm-BA.s390x.rpm	Client für Sichern/Archivieren (Befehlszeile und GUI), Verwaltungsclient (dsmadmc) und Web-Client	/opt/tivoli/tsm/client/ba Dieses Verzeichnis wird für viele Dateien des Clients für Sichern/Archivieren als Standardinstallationsverzeichnis verwendet. Die Beispielsystemoptionsdatei (dsm.sys.smp) wird in dieses Verzeichnis geschrieben. Falls die Umgebungsvariable DSM_DIR nicht definiert ist, werden die ausführbare Datei dsmc, die Ressourcendateien und die Datei dsm.sys in diesem Verzeichnis abgelegt. Falls die Umgebungsvariable DSM_CONFIG nicht definiert ist, muss sich die Clientbenutzeroptionsdatei in diesem Verzeichnis befinden. Wenn Sie DSM_LOG nicht definieren, schreibt der Client für Sichern/Archivieren Nachrichten in die Dateien dsmerror.log und dsmsched.log im aktuellen Arbeitsverzeichnis.
TIVsm-APIcit.s390x.rpm TIVsm-BAcit.s390x.rpm	Optional. Diese Dateien stellen die Common Inventory Technology-Komponenten bereit, mit denen Sie Informationen zur Anzahl der Client- und Servereinheiten, die mit dem System verbunden sind, sowie zur Nutzung der Prozessor-Value-Units (PVUs) durch Servereinheiten abrufen können. Weitere Informationen zu PVUs finden Sie in Prozessor-Value-Units schätzen in der Dokumentation zum IBM Spectrum Protect-Server.	APIcit wird im Verzeichnis /opt/tivoli/tsm/client/api/bin64/cit installiert. BAcit wird im Verzeichnis /opt/tivoli/tsm/client/ba/bin/cit installiert.

Paketname	Inhalt	Standardverzeichnis
TIVsm-filepath-source.tar.gz TIVsm-JBB.s390x.rpm	Für die Unterstützung journalbasierter Sicherungen benötigte Dateien.	Filepath wird in /opt/filepath installiert. JBB wird in /opt/tivoli/tsm/client/ba/bin installiert.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Vorgehensweise

1. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
2. Wechseln Sie in das Verzeichnis, in dem die Pakete gespeichert sind.
3. Installieren Sie die 64-Bit-Version der GSKit-Pakete. In diesem Beispiel stehen die Zeichen "8.x.x.x" für die GSKit-Version:

   ```
   rpm -U gskcrypt64-8.x.x.x.linux.s390x.rpm gskssl64-8.x.x.x.linux.s390x.rpm
   ```

4. Installieren Sie die IBM Spectrum Protect-API und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
   a. Erforderlich: Installieren Sie die API:

      ```
      rpm -i TIVsm-API64.s390x.rpm
      ```

   b. Optional: Installieren Sie das durch die API verwendete Common Inventory Technology-Paket. Dieses Paket ist von der API abhängig und muss daher nach der Installation des API-Pakets installiert werden.

      ```
      rpm -i TIVsm-APIcit.s390x.rpm
      ```

   Tipp: Wenn Sie für die API ein Upgrade durchführen und das Common Inventory Technology-Paket zuvor installiert wurde, müssen Sie sowohl für das API-Paket als auch für das Common Inventory Technology-Paket ein Upgrade durchführen. Sie können beispielsweise den folgenden Befehl ausführen:

   ```
   rpm -U TIVsm-API64.s390x.rpm TIVsm-APIcit.s390x.rpm
   ```

   Falls Sie lediglich eine Installation der API benötigen, können Sie die Prozedur an dieser Stelle beenden. Die nachfolgenden Schritte in dieser Prozedur beschreiben, wie die Komponenten für den Client für Sichern/Archivieren und ein optionales Clientpaket installiert werden, das nur dann benötigt wird, wenn der Client PVU-Messwerte an den Server senden soll. In den nachfolgenden Schritten ist außerdem die Installation der Pakete beschrieben, die Sie benötigen, wenn Sie journalbasierte Sicherungen ausführen wollen.

5. Installieren Sie den Client für Sichern/Archivieren und wahlweise das Common Inventory Technology-Paket, das für die Unterstützung von PVU-Berechnungen benötigt wird.
   a. Installieren Sie die Komponenten des Clients für Sichern/Archivieren.

      ```
      rpm -i TIVsm-BA.s390x.rpm
      ```

   b. Optional: Installieren Sie das Common Inventory Technology-Paket, das vom Client verwendet wird, um PVU-Messwerte an den Server zu senden. Dieses Paket ist vom Clientpaket abhängig und muss daher nach der Installation des Clientpakets installiert werden.

      ```
      rpm -i TIVsm-BAcit.s390x.rpm
      ```

6. Optional: Sollen journalbasierte Sicherungen verwendet werden, müssen Sie die Dateipfadkomponente kompilieren und installieren, die dem Linux-Kernel auf Ihrem Client-Computer entspricht. Extrahieren Sie TIVsm-filepath-source.tar.gz und lesen Sie die Kompilier- und Installationsanweisungen in der README-Datei. Das Kernelmodul für den Linux-Dateipfad wird gemäß den Bedingungen von 'GNU General Public License' (GPL) lizenziert.

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
Linux-Betriebssysteme

Linux on System z-Client deinstallieren

Sie können die folgenden Prozeduren verwenden, um den IBM Spectrum Protect Linux on System z-Client zu deinstallieren.

Vorbereitende Schritte

Sie müssen als Rootbenutzer angemeldet sein, um das Produkt installieren zu können. Deinstallieren Sie die Pakete in der angezeigten Reihenfolge.

Informationen zu diesem Vorgang

Um ein zuvor installiertes IBM Spectrum Protect-Clientpaket zu deinstallieren, geben Sie die folgenden Befehle ein. Mit diesen Befehlen werden die Pakete für die journalbasierte Sicherung, die Dateipfadkomponente, den Client für Sichern/Archivieren, die API und IBM® Global Security Kit (GSKit) entfernt.

Tipp: Die Versionsnummer der Pakete wird für die Deinstallation nicht benötigt.

Vorgehensweise

1. Sollen nur die Komponenten für die journalbasierte Sicherung deinstalliert werden, entfernen Sie beide Pakete (journalbasierte Sicherung und Dateipfad). Das Paket TIVsm-JBB ist vom Dateipfadpaket abhängig. Wenn Sie zwei separate Befehle rpm -e verwenden, um die Komponenten nacheinander zu deinstallieren, deinstallieren Sie zuerst das Paket TIVsm-JBB.

   ```
   rpm -e TIVsm-JBB TIVsm-filepath
   ```

2. Deinstallieren Sie die Pakete für den Client für Sichern/Archivieren:
   a. Falls das optionale Paket TIVsm-BAcit installiert wurde, deinstallieren Sie es, bevor Sie den Client deinstallieren:

      ```
      rpm -e TIVsm-BAcit
      ```

   b. Deinstallieren Sie den Client für Sichern/Archivieren.

      ```
      rpm -e TIVsm-BA
      ```

   Anmerkung: Wenn Sprachenpakete in einem Client der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl ein und ersetzen Sie hierbei *xx_xx* jeweils durch den Sprachencode jeder zusätzlichen Sprache, die installiert wurde. Eine Liste der Sprachencodekennungen finden Sie in Tabelle 1.

   ```
   rpm -e TIVsm-msg.xx_xx
   ```

   Tabelle 1. Kennungen der Sprachenpakete

Sprache	**Sprachenkennung**
Tschechisch	CS_CZ
Französisch	FR_FR
Deutsch	DE_DE
Ungarisch	HU_HU
Italienisch	IT_IT
Japanisch	JA_JP
Koreanisch	KO_KR
Polnisch	PL_PL
Portugiesisch	PT_BR
Russisch	RU_RU
Spanisch	ES_ES
Traditionelles Chinesisch (erweiterter UNIX-Code)	ZH_CN
Traditionelles Chinesisch (Big-5; die fünf wichtigsten DBCS-Sprachen)	ZH_TW

3. Deinstallieren Sie alle Produkte, die von der API abhängig sind, wie beispielsweise IBM Spectrum Protect for Databases und IBM Spectrum Protect for Mail. Alle von der API abhängigen Produkte müssen vor der Deinstallation des API-Pakets deinstalliert werden. Falls Sie ein von der API abhängiges Produkt deinstallieren, müssen Sie es nach der Installation einer neueren Version der Pakete für die API und den Client für Sichern/Archivieren erneut installieren. Anhand der Dokumentation des abhängigen Produkts können Sie ermitteln, welche Maßnahmen erforderlich sind, um einen Datenverlust beim Deinstallieren und erneuten Installieren der Produkte zu verhindern.
   a. Falls das optionale Common Inventory Technology-Paket für die API (TIVsm-APIcit) installiert wurde, deinstallieren Sie dieses Paket, bevor Sie das API-Paket deinstallieren. Verwenden Sie zum Deinstallieren des Pakets den folgenden Befehl:

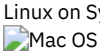
      ```
      rpm -e TIVsm-APIcit
      ```

   b. Deinstallieren Sie das API-Paket mit dem folgenden Befehl:

      ```
      rpm -e TIVsm-API64
      ```

4. Geben Sie den folgenden Befehl ein, um das 64-Bit-Paket von GSKit zu entfernen:

   ```
   rpm -e gskcryp64 gskssl64
   ```

Zugehörige Tasks:
Linux on System z-Client installieren
 Mac OS X-Betriebssysteme

Mac OS X-Client installieren

Sie können den IBM Spectrum Protect Mac OS X-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Sie müssen ein Systemadministrator sein, um den Client für Sichern/Archivieren installieren zu können.

Informationen zu diesem Vorgang

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Für MAC OS X-Clients können Sie einen Installationsassistenten verwenden, der die Eingabe von Informationen während der Installation des Produkts anfordert, oder Sie können den Client über die Befehlszeile installieren. Wenn Sie den Client mit dem Installationsverfahren über die Befehlszeile installieren, wird die Installation ohne Benutzerinteraktion ausgeführt. Die Installation über die Befehlszeile ist nützlich, wenn Sie ein Installationsscript erstellen und auf vielen Knoten ausführen wollen oder wenn Sie die Software auf einem System ohne Monitor installieren müssen.

Vorgehensweise

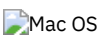
Wählen Sie eine Installationsmethode aus und installieren Sie den Client. Verwenden Sie entweder den Installationsassistenten oder installieren Sie den Client über die Befehlszeile.

Installationsmethode	Prozedur
Installationsassistent	a. Doppelklicken Sie auf die Datei 8.1.2.0.0-TIV-TSMBAC-Mac.dmg, um das Plattenimage anzuhängen. b. Doppelklicken Sie auf das Symbol für das IBM Spectrum Protect-Installationspaket und befolgen Sie die Bedienerführungen, um die Installation durchzuführen.
Befehlszeile:	a. Wechseln Sie in das Verzeichnis, in dem sich das IBM Spectrum Protect-Installationsprogramm befindet. b. Installieren Sie das Paket für die angepasste Installation mit dem folgenden Befehl: `/usr/sbin/installer -pkg "/Volumes/IBM Spectrum Protect/ IBM Spectrum Protect.pkg" -target /`

Nächste Schritte

Im Installationsverzeichnis wird ein Muster der Clientsystemoptionsdatei, `dsm.sys.smp`, erstellt. Sie können diese Musterdatei kopieren und ändern, um die Clientsystemoptionsdatei für Ihren Knoten zu erstellen. Der Standardname der Clientsystemoptionsdatei lautet dsm.sys.

Nach der Installation des Clients müssen Sie u. U. Umgebungsvariablen definieren, bevor Sie den Client verwenden. Weitere Informationen zum Definieren von Umgebungsvariablen finden Sie in Umgebungsvariablen für die Verarbeitung definieren.

 Mac OS X-Betriebssysteme

Mac OS X-Client deinstallieren

Sie können den IBM Spectrum Protect Mac OS X-Client deinstallieren, wenn er nicht mehr benötigt wird.

Vorbereitende Schritte

Wenn der IBM Spectrum Protect-Scheduler als Starteintrag konfiguriert ist, verwenden Sie die Funktion 'IBM Spectrum Protect-Tools für Administratoren' oder das Shell-Script StopCad.sh, um den Scheduler zu stoppen und zu deinstallieren, bevor Sie mit dieser Prozedur beginnen.

Informationen zu diesem Vorgang

Sie können den Client für Sichern/Archivieren mit einem Shell-Script deinstallieren. Der Name des Shell-Scripts lautet uninstall.sh und es befindet sich im Standardinstallationsverzeichnis /Library/Application Support/tivoli/tsm/client/ba/bin. Verwenden Sie den Befehl sudo, um das Script auszuführen.

Anstatt das Script zu verwenden, können Sie die folgenden Schritte ausführen:

Vorgehensweise

1. Versetzen Sie die folgenden Ordner in den Papierkorb:
   - /Applications/IBM Spectrum Protect
   - /Library/Application Support/tivoli
2. Entfernen Sie die folgenden symbolischen Verbindungen:
   - /usr/bin/dsmc
   - /usr/bin/dsmcad
   - /usr/bin/dsmadmc
   - /usr/bin/dsmtrace
   - /usr/bin/dsmagent
   - /usr/lib/libxmlutil-6.2.0.dylib
   - /usr/lib/libtsm620xerces-c1_6_0.dylib
3. Optional: Entfernen Sie die Protokolldateien und Optionsdateien, wenn Sie sie nicht aufbewahren wollen. Während des Deinstallationsprozesses bleiben sie auf der Platte, damit Ihre Einstellungen für den Fall erhalten bleiben, dass Sie das Produkt später erneut installieren.

   Vom Client für Sichern/Archivieren wurden möglicherweise Protokolldateien an den folgenden Positionen erstellt:

   a. /Library/Logs/tivoli
   b. ~/Library/Logs/tivoli

   Die Clientoptionsdateien (dsm.opt und dsm.sys) werden normalerweise an den folgenden Positionen gespeichert:

   a. /Library/Preferences/Tivoli Storage Manager
   b. ~/Library/Preferences/Tivoli Storage Manager

 Oracle Solaris-Betriebssysteme

Oracle Solaris x86_64-Client installieren

Sie können den IBM Spectrum Protect Oracle Solaris x86_64-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Ab IBM Spectrum Protect Version 8.1.0 ist der Oracle Solaris-Client für Sichern/Archivieren nur auf der Oracle Solaris x86_64-Plattform verfügbar. Auf der Oracle Solaris SPARC-Plattform ist der Client für Sichern/Archivieren nicht mehr verfügbar. Unter Oracle Solaris SPARC ist nur die IBM Spectrum Protect-API verfügbar. Informationen zur Installation der Solaris SPARC-API finden Sie in Oracle Solaris SPARC-API installieren.

Informationen zu diesem Vorgang

Wenn eine vorherige Version des Clients für Sichern/Archivieren installiert ist, müssen Sie diese entfernen, bevor Sie eine neue Version installieren. Informationen zum Entfernen vorheriger Solaris-Clientpakete finden Sie in Oracle Solaris x86_64-Client deinstallieren.

Die IBM Spectrum Protect-Installationsverwaltungsdatei (tsmadmin) wird anstelle der Standardverwaltungsdatei (/var/sadm/install/admin) verwendet, damit Sie während der Installation nicht nach der Berechtigung für `setuid`, `setgid` oder superuser gefragt werden. Wenn die Standardverwaltungsdatei verwendet werden soll, entfernen Sie die Option -a ./tsmadmin aus den angezeigten Befehlen und beantworten Sie die Fragen zur die Berechtigung für `setuid`, `setgid` oder superuser bei der Installation mit `Y`.

Tabelle 1. Namen und Beschreibungen der Installationspakete

Paket	Paketname	Paketbeschreibung
IBM® Global Security Kit (GSKit) 64 Bit	gsk8cry64.pkg und gsk8ssl64.pkg	Enthält IBM GSKit, das SSL-Datenverschlüsselung (SSL = Secure Sockets Layer) mit 64-Bit für die Kommunikation zwischen dem IBM Spectrum Protect-Client und -Server bereitstellt.
IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API)	TIVsmCapi.pkg	Enthält die gemeinsam genutzten Bibliotheken und Beispiele der 64-Bit-API von IBM Spectrum Protect.

Paket	Paketname	Paketbeschreibung
Client für Sichern/Archivieren	TIVsmCba.pkg	Enthält die folgenden 64-Bit-Komponenten: • Client für Sichern/Archivieren (Befehlszeile und GUI) • Verwaltungsclient (Befehlszeile) • Web-Client für Sichern/Archivieren Anmerkung: 1. TCP/IP und gemeinsam genutzter Speicher werden als Übertragungsmethodeen unterstützt. 2. Der Web-Client ist eine Komponente des Pakets des Clients für Sichern/Archivieren und kann nicht ohne dieses installiert werden.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Installieren Sie die Pakete in der angezeigten Reihenfolge; einige Pakete sind vom Vorhandensein anderer Pakete abhängig. Beispielsweise ist GSKit eine Voraussetzung für die API und die API ist eine Voraussetzung für das Paket des Clients für Sichern/Archivieren.

Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
3. Wechseln Sie in das Verzeichnis, in dem die Pakete gespeichert sind.
4. IBM GSKit ist eine Voraussetzung des Pakets für die IBM Spectrum Protect-API. Installieren Sie GSKit mit den folgenden Befehlen:

   ```
   pkgadd -n -a ./tsmadmin -d ./gsk8cry64.pkg gsk8cry64
   pkgadd -n -a ./tsmadmin -d ./gsk8ssl64.pkg gsk8ssl64
   ```

   Anmerkung: Unter Solaris 10 wird mit diesen Befehlen die 64-Bit-Version von GSKit in der globalen Zone und in allen aktiven nicht globalen Zonen installiert. Um den Client nur in einer nicht globalen Sparse-Root-Zone zu installieren, muss GSKit zunächst in der globalen Zone installiert werden. Unter Solaris 11 werden die Pakete nur in der Zone installiert, in der diese Befehle ausgeführt werden.
5. Installieren Sie die IBM Spectrum Protect-API mit dem folgenden Befehl:

   ```
   pkgadd -n -a ./tsmadmin -d ./TIVsmCapi.pkg TIVsmCapi
   ```

   Anmerkung: Unter Solaris 10 installiert dieser Befehl die 64-Bit-API von IBM Spectrum Protect in der globalen Zone und in allen aktiven nicht globalen Zonen. Falls Sie die API nur in der globalen Zone installieren wollen, verwenden Sie den Parameter -G des Befehls pkgadd. Unter Solaris 11 wird die API nur in der Zone installiert, in der dieser Befehl ausgeführt wird.
6. Verwenden Sie den folgenden Befehl, um den Client für Sichern/Archivieren zu installieren:

   ```
   pkgadd -n -a ./tsmadmin -d ./TIVsmCba.pkg TIVsmCba
   ```

   Anmerkung: Unter Solaris 10 installiert dieser Befehl die Komponenten des Clients für Sichern/Archivieren in der globalen Zone und in allen aktiven nicht globalen Zonen. Falls diese nur in der globalen Zone installiert werden sollen, verwenden Sie den Parameter -G des Befehls pkgadd. Unter Solaris 11 werden die Clientkomponenten nur in der Zone installiert, in der dieser Befehl ausgeführt wird.

Ergebnisse

Wichtig: Für eine nicht globale Sparse-Root-Zone unter Solaris 10 wird das Dateisystem `/usr` normalerweise in der globalen Zone als schreibgeschützt (LOFS) bereitgestellt und es gelten die folgenden Bedingungen:

- Wenn der Client nicht in der globalen Zone installiert wird, wird am Ende der Installation eine Warnung angezeigt. In der Nachricht wird der globale Administrator zum Erstellen der erforderlichen Verknüpfungen aufgefordert, die in den Warnungen angegeben sind.
- Wenn der Client bereits in der globalen Zone installiert ist, ist die Erstellung dieser Verknüpfungen nicht erforderlich. Die Verknüpfungen sind bereits vorhanden und verweisen auf die korrekten ausführbaren Dateien und Bibliotheken.

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
Oracle Solaris-Betriebssysteme

Oracle Solaris x86_64-Client deinstallieren

Sie können alle Pakete deinstallieren, die zum IBM Spectrum Protect Oracle Solaris x86_64-Client gehören, einschließlich der Komponenten Befehlszeilenclient, GUI, Web-GUI und Verwaltungsclient.

Informationen zu diesem Vorgang

Wichtig: Stellen Sie sicher, dass Sie die Pakete in der angegebenen Reihenfolge deinstallieren.

Die IBM Spectrum Protect-Installationsverwaltungsdatei (`tsmadmin`) wird anstelle der Standardverwaltungsdatei (`/var/sadm/install/admin`) verwendet, damit Sie während der Installation nicht nach der Berechtigung für `setuid`, `setgid` oder superuser gefragt werden. Wenn die Standardverwaltungsdatei verwendet werden soll, entfernen Sie die Option `-a ./tsmadmin` aus den folgenden Befehlen und beantworten Sie die Fragen zur Berechtigung für `setuid`, `setgid` oder superuser bei der Installation mit `y`.

Vorgehensweise

1. Geben Sie den folgenden Befehl ein, um den Client für Sichern/Archivieren zu deinstallieren:

   ```
   pkgrm -n -a ./tsmadmin TIVsmCba
   ```

   Dieser Befehl deinstalliert alle Komponenten des Clients für Sichern/Archivieren (Befehlszeile, GUI, Web-GUI und Verwaltungsclient). Die Deinstallation einzelner Komponenten dieses Pakets (z. B. des Befehlszeilenclients) ist nicht möglich.

   Anmerkung: Wenn landessprachliche Nachrichtenpakete in Clients der Version 7.1.2 oder früher installiert wurden, müssen Sie diese Pakete vor dem Entfernen des API-Pakets entfernen. Geben Sie den folgenden Befehl als Rootbenutzer ein:

   ```
   pkgrm -n -a ./tsmadmin TIVsmClCs TIVsmClDe TIVsmClEs TIVsmClFr \
                          TIVsmClHu TIVsmClIt TIVsmClJa TIVsmClKo \
                          TIVsmClPl TIVsmClPt TIVsmClRu TIVsmClSc TIVsmClTc
   ```

2. Geben Sie den folgenden Befehl ein, um die IBM Spectrum Protect-API zu deinstallieren:

   ```
   pkgrm -n -a ./tsmadmin TIVsmCapi
   ```

   Die API kann nicht entfernt werden, wenn der Client für Sichern/Archivieren installiert ist. Der Client für Sichern/Archivieren muss zuerst entfernt werden.

3. Geben Sie die folgenden Befehle ein, um GSKit zu deinstallieren:

   ```
   pkgrm -n -a ./tsmadmin gsk8ssl64
   pkgrm -n -a ./tsmadmin gsk8cry64
   ```

 Oracle Solaris-Betriebssysteme

Oracle Solaris SPARC-API installieren

Sie können die IBM Spectrum Protect Oracle Solaris SPARC-API von den Produktinstallationsmedien installieren.

Informationen zu diesem Vorgang

Wenn eine vorherige Version der API installiert ist, müssen Sie diese entfernen, bevor Sie eine neue Version installieren. Informationen zum Entfernen vorheriger Solaris-API-Pakete finden Sie in Oracle Solaris SPARC-API deinstallieren.

Die IBM Spectrum Protect-Installationsverwaltungsdatei (tsmadmin) wird anstelle der Standardverwaltungsdatei (/var/sadm/install/admin) verwendet, damit Sie während der Installation nicht nach der Berechtigung für `setuid`, `setgid` oder superuser gefragt werden. Wenn die Standardverwaltungsdatei verwendet werden soll, entfernen Sie die Option -a ./tsmadmin aus den angezeigten Befehlen und beantworten Sie die Fragen zur die Berechtigung für `setuid`, `setgid` oder superuser bei der Installation mit `Y`.

Tabelle 1. Namen und Beschreibungen der Installationspakete

Paket	Paketname	Paketbeschreibung
IBM® Global Security Kit (GSKit) 64 Bit	gsk8cry64.pkg und gsk8ssl64.pkg	Enthält IBM GSKit, das SSL-Datenverschlüsselung (SSL = Secure Sockets Layer) mit 64-Bit für die Kommunikation zwischen der IBM Spectrum Protect-API und dem Server bereitstellt.
IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API)	TIVsmCapi.pkg	Enthält die gemeinsam genutzten Bibliotheken und Beispiele der 64-Bit-API von IBM Spectrum Protect.

Mit diesem Installationsverfahren können neue Verteilungen oder Aktualisierungen von heruntergeladenen Installationsmedien installiert werden. Die heruntergeladenen Dateien, die Sie zum Installieren des Clients verwenden, können gegebenenfalls komprimiert sein. Kopieren oder extrahieren Sie die Dateien abhängig vom Format der Paketdatei auf Platte und installieren Sie die Komponenten gemäß diesen Anweisungen.

Sie können die entsprechende Paketdatei von einer der folgenden Websites herunterladen:

- Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.

Installieren Sie die Pakete in der angezeigten Reihenfolge.

Vorgehensweise

1. Melden Sie sich als Rootbenutzer an.
2. Stellen Sie den Datenträger bereit, von dem die Installation erfolgt.
3. Wechseln Sie in das Verzeichnis, in dem die Pakete gespeichert sind.
4. IBM GSKit ist eine Voraussetzung des Pakets für die IBM Spectrum Protect-API. Installieren Sie GSKit mit den folgenden Befehlen:

   ```
   pkgadd -n -a ./tsmadmin -d ./gsk8cry64.pkg gsk8cry64
   pkgadd -n -a ./tsmadmin -d ./gsk8ssl64.pkg gsk8ssl64
   ```

   Anmerkung: Unter Solaris 10 wird mit diesen Befehlen die 64-Bit-Version von GSKit in der globalen Zone und in allen aktiven nicht globalen Zonen installiert. Um die API nur in einer nicht globalen Sparse-Root-Zone zu installieren, muss GSKit zunächst in der globalen Zone installiert werden. Unter Solaris 11 werden die Pakete nur in der Zone installiert, in der diese Befehle ausgeführt werden.
5. Installieren Sie die IBM Spectrum Protect-API mit dem folgenden Befehl:

   ```
   pkgadd -n -a ./tsmadmin -d ./TIVsmCapi.pkg TIVsmCapi
   ```

   Anmerkung: Unter Solaris 10 installiert dieser Befehl die 64-Bit-API von IBM Spectrum Protect in der globalen Zone und in allen aktiven nicht globalen Zonen. Falls Sie die API nur in der globalen Zone installieren wollen, verwenden Sie den Parameter -G des Befehls pkgadd. Unter Solaris 11 wird die API nur in der Zone installiert, in der dieser Befehl ausgeführt wird.

Ergebnisse

Wichtig: Für eine nicht globale Sparse-Root-Zone unter Solaris 10 wird das Dateisystem `/usr` normalerweise in der globalen Zone als schreibgeschützt (LOFS) bereitgestellt und es gelten die folgenden Bedingungen:

- Wenn die API nicht in der globalen Zone installiert wird, wird am Ende der Installation eine Warnung angezeigt. In der Nachricht wird der globale Administrator zum Erstellen der erforderlichen Verknüpfungen aufgefordert, die in den Warnungen angegeben sind.
- Wenn die API bereits in der globalen Zone installiert ist, ist die Erstellung dieser Verknüpfungen nicht erforderlich. Die Verknüpfungen sind bereits vorhanden und verweisen auf die korrekten ausführbaren Dateien und Bibliotheken.

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
Oracle Solaris-Betriebssysteme

Oracle Solaris SPARC-API deinstallieren

Sie können alle Pakete deinstallieren, die zur IBM Spectrum Protect Oracle Solaris SPARC-API gehören.

Informationen zu diesem Vorgang

Wichtig: Stellen Sie sicher, dass Sie die Pakete in der angegebenen Reihenfolge deinstallieren.

Die IBM Spectrum Protect-Installationsverwaltungsdatei (`tsmadmin`) wird anstelle der Standardverwaltungsdatei (`/var/sadm/install/admin`) verwendet, damit Sie während der Installation nicht nach der Berechtigung für `setuid`, `setgid` oder superuser gefragt werden. Wenn die Standardverwaltungsdatei verwendet werden soll, entfernen Sie die Option `-a ./tsmadmin` aus den folgenden Befehlen und beantworten Sie die Fragen zur Berechtigung für `setuid`, `setgid` oder superuser bei der Installation mit `y`.

Vorgehensweise

1. Geben Sie den folgenden Befehl ein, um die IBM Spectrum Protect-API zu deinstallieren:

   ```
   pkgrm -n -a ./tsmadmin TIVsmCapi
   ```

2. Geben Sie die folgenden Befehle ein, um GSKit zu deinstallieren:

   ```
   pkgrm -n -a ./tsmadmin gsk8ssl64
   pkgrm -n -a ./tsmadmin gsk8cry64
   ```

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme

Softwareaktualisierungen

IBM® kann Softwareaktualisierungen regelmäßig für den Download bereitstellen.

Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal for IBM Spectrum Protect.

 Windows-Betriebssysteme

Installationsübersicht für den Windows-Client für Sichern/Archivieren

Sie können den IBM Spectrum Protect Windows-Client für Sichern/Archivieren von den Produktinstallationsmedien installieren.

Vorbereitende Schritte

Bevor Sie mit der Installation des Windows-Clients beginnen, müssen Sie sicherstellen, dass das System, auf dem Sie den Client installieren wollen, die Clientvoraussetzungen erfüllt. Anschließend bestimmen Sie den erforderlichen Installationstyp und führen die Schritte der entsprechenden Prozedur aus.

Informationen zu den Hardware- und Softwarevoraussetzungen für den Windows-Client finden Sie in Technote 1197133.

-  WindowsBetriebssystemeMöglicher Warmstart bei Windows-Clientinstallation
  Während des Windows-Clientinstallationsprozesses wird mindestens ein weiterverteilbares Paket von Microsoft C++ installiert, falls auf der Windows-Workstation noch nicht installiert. Diese Pakete können auch automatisch vom Windows-Aktualisierungsdienst aktualisiert werden. Wenn die Pakete aktualisiert werden, kann es beim Starten des Windows-Clientinstallationsprogramms zu einem Warmstart des Systems kommen.
-  WindowsBetriebssystemeInstallationsverfahren
  Die Vorgehensweise bei der Installation des IBM Spectrum Protect-Clients für Sichern/Archivieren unter Windows ist vom gewünschten Installationstyp abhängig.
-  WindowsBetriebssystemeFehlerbehebung bei der Installation (Windows)
  Wenn Sie ein Upgrade von einer vorherigen Version des Clients für Sichern/Archivieren durchführen und Client-Services (beispielsweise Clientakzeptor oder Scheduler) aktiv sind, wird während der Installation möglicherweise ein Fehler angezeigt.
-  WindowsBetriebssystemeSoftwareaktualisierungen
  IBM® kann Softwareaktualisierungen regelmäßig für den Download bereitstellen.

Zugehörige Konzepte:
 WindowsBetriebssystemeAutomatische Implementierung des Clients für Sichern/Archivieren
Zugehörige Tasks:
 WindowsBetriebssystemeClientoptionsdatei erstellen und ändern
Web-Client-Sitzung starten
 Windows-Betriebssysteme

Möglicher Warmstart bei Windows-Clientinstallation

Während des Windows-Clientinstallationsprozesses wird mindestens ein weiterverteilbares Paket von Microsoft C++ installiert, falls auf der Windows-Workstation noch nicht installiert. Diese Pakete können auch automatisch vom Windows-Aktualisierungsdienst aktualisiert werden. Wenn die Pakete aktualisiert werden, kann es beim Starten des Windows-Clientinstallationsprogramms zu einem Warmstart des Systems kommen.

Der Warmstart, der durch eine Aktualisierung der weiterverteilbaren Pakete von C++ ausgelöst wird, kann selbst unter den folgenden Bedingungen auftreten:

- Bei einer automatischen Clientimplementierung wird ein Client-Upgrade mit Push an einen Knoten übertragen und der Client oder der Scheduler setzt die Option AUTODEPLOY=NOREBOOT.
- Eine manuelle Installation oder ein manuelles Upgrade des Clients wird gestartet.
- Eine unbeaufsichtigte Clientinstallation wird ausgeführt, auch wenn die Optionen für die Unterdrückung von Warmstartanforderungen und des Clientwarmstarts selbst definiert sind.

Da das weiterverteilbare Paket für Microsoft Visual Studio C++ eine gemeinsam genutzte (freigegebene) Windows-Komponente ist, können darüber hinaus andere Anwendungen, bei denen Abhängigkeiten zu dem Paket bestehen, von Windows im Rahmen der Installation bzw. des Upgrades des weiterverteilbaren C++-Pakets gestoppt oder neu gestartet werden. Planen Sie die Clientinstallationen und -Upgrades in einem Wartungszeitfenster, in dem andere Anwendungen nicht beeinträchtigt werden, wenn sie während der Installation des weiterverteilbaren C++-Pakets gestoppt oder neu gestartet werden. Überwachen Sie andere Anwendungen nach der Installation des Clients, um festzustellen, ob Anwendungen gestoppt und nicht erneut gestartet wurden.
 Windows-Betriebssysteme

Installationsverfahren

Die Vorgehensweise bei der Installation des IBM Spectrum Protect-Clients für Sichern/Archivieren unter Windows ist vom gewünschten Installationstyp abhängig.

Prozeduren gibt es für jeden der folgenden Installationstypen:

Installationstyp	Installationsbeschreibung
Erstinstallation des Windows-Clients	Beschreibt, wie der Windows-Client für Sichern/Archivieren zum ersten Mal installiert wird. Voraussetzung für diese Prozedur ist, dass auf dem Windows-Computer, auf dem Sie den Client installieren wollen, noch nie eine Vorgängerversion des Clients installiert war.
Upgrade des Windows-Clients durchführen	Beschreibt, wie ein Upgrade einer früheren Version des Windows-Clients für Sichern/Archivieren auf die neueste Version durchgeführt wird.
Windows-Client erneut installieren	Beschreibt, wie der Windows-Client für Sichern/Archivieren erneut installiert wird, wenn Sie ihn deinstalliert haben.
Unbeaufsichtigte Installation	Beschreibt, wie eine unbeaufsichtigte Installation des Windows-Clients für Sichern/Archivieren ohne Benutzerinteraktion während der Installation durchgeführt wird.
Windows-Client ändern, reparieren oder deinstallieren	Beschreibt, wie Komponenten auf einem installierten Client für Sichern/Archivieren hinzugefügt oder entfernt werden (ändern), wie beschädigte Dateien oder fehlende Registrierungsschlüssel ersetzt werden (reparieren) und wie der Windows-Client für Sichern/Archivieren deinstalliert wird.

- Windows-BetriebssystemeErstinstallation des Windows-Clients
  Führen Sie diese Prozedur aus, um den Windows-Client für Sichern/Archivieren zum ersten Mal zu installieren.
- Windows-BetriebssystemeUpgrade des Windows-Clients durchführen
  Sie können ein Upgrade einer früheren Version des IBM Spectrum Protect-Clients für Sichern/Archivieren unter Windows auf Version 8.1.2 durchführen. Ihre bisherigen Konfigurationseinstellungen werden nach Möglichkeit beibehalten. Durch funktionale Erweiterungen in der aktuellen Version des Clients kann es jedoch möglich sein, dass die Verwendung von Optionen, die in älteren Versionen des Clients verfügbar waren, nicht mehr unterstützt oder verhindert wird.
- Windows-BetriebssystemeWindows-Client erneut installieren
  Wenn Sie den Windows-Client der Version 8.1.2 deinstallieren, können Sie ihn im Bedarfsfall erneut installieren.
- Windows-BetriebssystemeUnbeaufsichtigte Installation
  Das Installationsprogramm des Clients für Sichern/Archivieren unterstützt unbeaufsichtigte Installationen.
- Windows-BetriebssystemeWindows-Client ändern, reparieren oder deinstallieren
  Sie können einen vorhandenen Windows-Client ändern, reparieren oder deinstallieren.

Windows-Betriebssysteme

Erstinstallation des Windows-Clients

Führen Sie diese Prozedur aus, um den Windows-Client für Sichern/Archivieren zum ersten Mal zu installieren.

Vorbereitende Schritte

Wenn eine frühere Version des Windows-Clients für Sichern/Archivieren bereits auf einem Knoten installiert ist und ein Upgrade von dieser Version auf Version 8.1.2 durchgeführt werden soll, lesen Sie die Informationen in Upgrade des Windows-Clients durchführen.

Wichtig: Sie müssen den Hostnamen oder die IP-Adresse des IBM Spectrum Protect-Servers, die Anschlussnummer des Servers für den Empfang der Clientkommunikation und die für die Kommunikation zwischen Client und Server zu verwendende Übertragungsmethode kennen. Fragen Sie Ihren IBM Spectrum Protect-Serveradministrator nach diesen Informationen, bevor Sie mit dieser Prozedur beginnen.

Vorgehensweise

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter.
   - Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
   - Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.
2. Installieren Sie das Produkt mithilfe der komprimierten Installationsdatei, die Sie über Passport Advantage herunterladen.
   a. Kopieren Sie das heruntergeladene komprimierte Installationspaket auf eine lokale Platte oder in eine Netzfreigabe. Stellen Sie sicher, dass die Installationsdateien in ein leeres Verzeichnis extrahiert werden.
   b. Um die Installationsdateien in dasselbe Verzeichnis zu extrahieren, doppelklicken Sie auf das komprimierte Installationspaket.
   c. Standardmäßig werden die dekomprimierten Dateien im aktuellen Plattenlaufwerk im Verzeichnis *Downloadverzeichnis*\TSMClient gespeichert. Wenn das Installationsprogramm Dateien eines anderen Clientinstallationsversuchs in diesem Verzeichnis findet, werden Sie aufgefordert anzugeben, ob die alten Dateien überschrieben werden sollen. Wenn diese Eingabeaufforderung angezeigt wird, geben Sie `A` ein, um die vorhandenen Dateien zu überschreiben; mit dieser Auswahl wird sichergestellt, dass nur die Dateien der aktuellen Installation verwendet werden.
   d. Doppelklicken Sie auf die Datei spinstall.exe, um das Installationsprogramm für den Client zu starten.
3. Wählen Sie eine Sprache für diese Installation aus und klicken Sie auf OK.

4. Wenn der Installationsassistent anzeigt, dass weiterverteilbare Microsoft C++-Dateien installiert werden müssen, klicken Sie auf Installieren. Diese Dateien werden für die Ausführung des Windows-Clients benötigt.
5. Klicken Sie in der Eingangsanzeige des IBM Spectrum Protect-Clients auf Weiter, um die Installation der Client-Software zu starten.
6. Übernehmen Sie das Standardinstallationsverzeichnis, indem Sie auf Weiter klicken, oder geben Sie ein anderes Installationsverzeichnis an. Das Standardinstallationsverzeichnis ist C:\Programme\Tivoli\TSM.
7. Wählen Sie den Installationstyp aus: Standard oder Angepasst.

Option	Bezeichnung
Standard	Bei einer Standardinstallation werden die folgenden Komponenten installiert: ○ Die Dateien der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren (erforderlich für die Verwendung der Java™-GUI) ○ Die Webdateien des Clients für Sichern/Archivieren (erforderlich für die Verwendung des Web-Clients) ○ Die Client-API-Dateien (nach Bedarf Ihres Clients und Ihres Betriebssystems)
Angepasst	Bei einer angepassten Installation werden die gleichen Dateien wie bei einer Standardinstallation installiert. Sie haben jedoch die Wahl, die folgenden optionalen Komponenten zu installieren: ○ Die SDK-Dateien der API (nur erforderlich, wenn Sie Anwendungen entwickeln, die zusammen mit dem Client für Sichern/Archivieren eingesetzt werden) ○ Die Dateien für die Befehlszeile des Verwaltungsclients (erforderlich für die Ausführung von Administratorfunktionen auf dem IBM Spectrum Protect-Server über Fernzugriff)

8. Klicken Sie auf Weiter und dann auf Installieren.
9. Wenn das Installationsprogramm die Installation beendet hat, klicken Sie auf Fertigstellen.
10. Überprüfen Sie die Installation. Klicken Sie auf Start > Alle Programme > IBM Spectrum Protect. Die von Ihnen installierten Clientkomponenten werden in der Liste der startfähigen IBM Spectrum Protect-Programme angezeigt. In dieser Liste werden nur die folgenden Komponenten angezeigt: Verwaltungsbefehlszeilenclient, Befehlszeilenclient für Sichern/Archivieren und GUI für Sichern/Archivieren. Der Verwaltungsbefehlszeilenclient wird nur angezeigt, wenn Sie eine angepasste Installation ausführen und den Verwaltungsbefehlszeilenclient auswählen. Wenn Sie andere Komponenten installiert hatten, wie beispielsweise die API-Laufzeit und das SDK, werden diese Komponenten in dieser Liste nicht angezeigt.
11. Klicken Sie auf GUI für Sichern/Archivieren, um die Client-GUI zu starten. Der Konfigurationsassistent für Clientoptionsdatei wird gestartet. Klicken Sie auf Weiter, um den Assistenten zu starten.
12. Wählen Sie in der Optionsdateianzeige die Erstellung einer neuen Optionsdatei aus und klicken Sie auf Weiter.
13. Geben Sie in der Anzeige Clientknotenname einen Knotennamen an. Mit einem Knotennamen wird Ihr Knoten für den IBM Spectrum Protect-Server eindeutig identifiziert. Der Standardknotenname ist der kurze Hostname des Windows-Computers, auf dem Sie den Client installieren. Übernehmen Sie den Standardknotennamen oder geben Sie einen neuen Knotennamen an. Klicken Sie auf Weiter.
14. Geben Sie in der Anzeige IBM Spectrum Protect-Client/Server-Übertragung die Übertragungsmethode an, die verwendet werden soll, wenn der Client mit dem Server kommuniziert, und klicken Sie auf Weiter. Diese Informationen müssen Ihnen von Ihrem IBM Spectrum Protect-Serveradministrator zur Verfügung gestellt werden. Wenn Sie nicht sicher sind, übernehmen Sie die Standardeinstellung (TCP/IP). Funktioniert die Standardeinstellung nicht, wenn der Client versucht, die Verbindung zum Server herzustellen, wenden Sie sich zur Bestimmung der anzugebenden Übertragungsmethode an den Serveradministrator.
15. Geben Sie in der Anzeige TCP/IP-Optionen die Serveradresse und die Anschlussinformationen an, die Sie von Ihrem IBM Spectrum Protect-Administrator erhalten haben. Geben Sie im Feld Serveradresse die IP-Adresse oder den vollständig qualifizierten Domänennamen des IBM Spectrum Protect-Servers an. Geben Sie im Feld Anschlussnummer die Anschlussnummer des Servers für den Empfang der Clientkommunikation an. Die Standardanschlussnummer ist 1500. Klicken Sie auf Weiter.
16. Die Anzeige Empfohlene Einschluss-/Ausschlussliste enthält eine Liste der Systemdateien und Verzeichnisse, die bei Clientoperationen normalerweise berücksichtigt bzw. ausgeschlossen werden. Die ausgeschlossenen Dateien sind normalerweise für die Wiederherstellung Ihres Systems nicht erforderlich. Sie können alle Standardauswahlmöglichkeiten auswählen oder abwählen. Sie können auch mithilfe der Umschalttaste und der Steuertaste (Strg) Objekte selektiv einschließen. Klicken Sie auf Alles auswählen, um den Installationsprozess zu vereinfachen. Sie können später Dateien zu dieser Liste hinzufügen oder aus dieser Liste entfernen. Klicken Sie auf Weiter.
17. Die Anzeige Allgemeine Dateiausschlussauswahl enthält eine Standardliste der Dateierweiterungen, die Sie von Clientoperationen ausschließen können. Bei den Dateierweiterungen in dieser Liste handelt es sich in der Regel um Erweiterungen großer Dateien, z. B. Grafik- oder Multimediadateien. Diese Dateien beanspruchen Serverplattenspeicher, sind jedoch zum Zurückschreiben kritischer Daten möglicherweise nicht erforderlich. Klicken Sie auf Alles auswählen, um alle Standarddateierweiterungen auszuschließen. Sie können auch mithilfe der Umschalttaste und der Steuertaste (Strg) die Erweiterungen auswählen, die von den Clientoperationen ausgeschlossen werden sollen. Klicken Sie auf Alles löschen, um alle ausgewählten Erweiterungen zu löschen. Sie können diese Erweiterungen im Bedarfsfall später ändern. Klicken Sie auf Weiter.
18. In der Anzeige Domäne für Sicherung sind die Standarddateisysteme und -objekte aufgeführt, die bei Teil- und Imagesicherungen in Clientoperationen berücksichtigt werden sollen.
    a. Wählen Sie Teilsicherung im Feld Sicherungstyp aus, um die Standarddateisysteme für Teilsicherungen zu konfigurieren. Standardmäßig ist Alle lokalen Dateisysteme sichern ausgewählt. Sollen während der Teilsicherungen nicht standardmäßig alle lokalen Dateisysteme gesichert werden, wählen Sie diese Option ab und wählen Sie die einzuschließenden Dateisysteme einzeln aus. Sie können die Standardauswahl überschreiben, wenn Sie eine Teilsicherung einleiten.
    b. Wählen Sie Imagesicherung im Feld Sicherungstyp aus, um die Standarddateisysteme für Imagesicherungen zu konfigurieren. Standardmäßig ist Alle lokalen Dateisysteme sichern ausgewählt. Sollen während der Imagesicherungen nicht standardmäßig alle lokalen Dateisysteme gesichert werden, wählen Sie diese Option ab und wählen Sie die einzuschließenden Dateisysteme einzeln aus. Sie können die Standardauswahl überschreiben, wenn Sie eine Imagesicherung einleiten.
    c. Klicken Sie auf Weiter.
19. Klicken Sie in der Anzeige Konfiguration bestätigen und anwenden auf Anwenden. Gegebenenfalls werden Sie zur Eingabe einer Benutzer-ID und eines Kennworts für die Anmeldung beim IBM Spectrum Protect-Server aufgefordert. Der Standardwert der Benutzer-ID ist der

Knotenname, den Sie in Schritt 13 angegeben haben.

20. Sie können die Standard-Benutzer-ID übernehmen oder eine andere Benutzer-ID angeben. Geben Sie das Kennwort an, das Sie für die Anmeldung beim Server verwenden wollen. Klicken Sie auf Anmelden. Was als Nächstes passiert, ist davon abhängig, ob der IBM Spectrum Protect-Server für die offene oder für die geschlossene Registrierung konfiguriert ist.

Option	Bezeichnung
Server ist für offene Registrierung konfiguriert (IBM Spectrum Protect-Server der Version 8.1.1, Version 8.1.0, Version 7.1.7 oder einer früheren Version)	In der Registrierungsanzeige für neue Knoten müssen Sie Kontaktinformationen eingeben und die Kennworteingabe wiederholen. Die Angabe im Feld Kontaktinformationen ist optional, wird aber empfohlen. Geben Sie Ihren Namen an. Geben Sie Ihr Kennwort zweimal in die Felder für das Kennwort ein. Wenn das in diesen Feldern für das Kennwort eingegebene Kennwort und Bestätigungskennwort nicht mit der vorherigen Angabe in der Anzeige für die Anmeldung bei einem IBM Spectrum Protect-Server übereinstimmt, wird das hier angegebene und bestätigte Kennwort zu dem Kennwort, das für die Anmeldung beim Server erforderlich ist. Klicken Sie auf Registrieren, um diesen Knoten auf dem Server zu registrieren. Klicken Sie auf Fertig stellen. Die grafische Benutzerschnittstelle wird geöffnet und ist für die Verwendung bereit. Sie können über das Menü Start auch alle anderen installierten Clientkomponenten starten.
Server verwendet geschlossene Registrierung	Klicken Sie auf Fertig stellen. Stellen Sie Ihrem IBM Spectrum Protect-Serveradministrator die Informationen zur Verfügung, die Sie im Clientkonfigurationsassistenten angegeben haben. Stellen Sie dem Administrator die folgenden Informationen zur Verfügung: ◦ Den angegebenen Knotennamen. ◦ Die eingegebene Benutzer-ID und das eingegebene Kennwort. ◦ Ihre Kontaktinformationen, beispielsweise Ihr Name, Ihre E-Mail-Adresse und Ihre Telefonnummer, sodass der Administrator Kontakt mit Ihnen aufnehmen kann, nachdem Ihr Knoten und Ihre Benutzerdaten auf dem Server registriert wurden. Nachdem Ihr Knoten vom Administrator registriert wurde, können Sie alle installierten Clientkomponenten über das Menü Start starten.

Zugehörige Konzepte:
Fehlerbehebung bei der Installation (Windows)
 Windows-Betriebssysteme

Upgrade des Windows-Clients durchführen

Sie können ein Upgrade einer früheren Version des IBM Spectrum Protect-Clients für Sichern/Archivieren unter Windows auf Version 8.1.2 durchführen. Ihre bisherigen Konfigurationseinstellungen werden nach Möglichkeit beibehalten. Durch funktionale Erweiterungen in der aktuellen Version des Clients kann es jedoch möglich sein, dass die Verwendung von Optionen, die in älteren Versionen des Clients verfügbar waren, nicht mehr unterstützt oder verhindert wird.

Vorbereitende Schritte

Warten Sie, bis alle laufenden Tasks des Clients für Sichern/Archivieren (Sicherung, Zurückschreibung, Archivierung, Abruf) beendet sind, bevor Sie ein Upgrade für einen Clientknoten durchführen.

Informationen zu diesem Vorgang

Um ein Upgrade auf den Windows-Client der Version 8.1.2 durchzuführen, installieren Sie den Windows-Client der Version 8.1.2; es ist nicht erforderlich, zunächst die zuvor installierte Client-Software zu deinstallieren. Das Installationsprogramm für den Client der Version 8.1.2 behält Ihre aktuellen Clientoptionen und Einstellungen bei (in dsm.opt). Außerdem werden die Dateien dsmerror.log, dsmsched.log und dsmwebcl.log nicht überschrieben oder gelöscht, wenn Sie den neuen Client in demselben Verzeichnis wie die vorherige Installation installieren.

Der Logical Volume Snapshot Agent (LVSA, Agent für die Momentaufnahme des logischen Datenträgers) wird ab IBM Spectrum Protect Version 6.4 nicht weiter unterstützt. War LVSA bisher als Momentaufnahmeprovider konfiguriert, installieren Sie den Client der Version 8.1.2 und geben Sie dann in seiner Konfiguration die Verwendung von Microsoft Volume Shadow Copy Service (VSS, Volumeschattenkopie-Dienst) als Momentaufnahmeprovider in der neuen Installation an. Wenn LVSA installiert war, führt Ihr Client nach Beendigung der Upgradeinstallation einen Warmstart durch, damit LVSA-Einträge aus der Registrierung entfernt werden können.

Das Installationsprogramm stoppt alle aktiven Client-Services (Dienste), bevor es das Upgrade der Client-Software durchführt. Sie können die Dienste auch über die Systemsteuerung oder die Befehlszeile manuell stoppen. Tabelle 1 enthält die Dienste, die gestoppt werden können, sowie die Namen, die Sie nach Auswahl von Systemsteuerung > Verwaltung > Dienste in der Liste suchen müssen, damit die entsprechenden Dienste über die Systemsteuerung gestoppt werden können. Die Tabelle enthält außerdem die Befehle, mit denen sie über eine Befehlseingabeaufforderung oder ein Script gestoppt werden können.

Anmerkung: Die in der Tabelle aufgeführten Dienstnamen sind die vom Installationsprogramm festgelegten Standardnamen. Sie können einige dieser Dienstnamen ändern, wenn Sie die Dienste mit einem der Konfigurationsassistenten in den Menüs Dienstprogramme > Setup-Assistent konfigurieren. Wenn Sie den Dienstnamen ändern, notieren Sie den geänderten Namen und verwenden Sie diesen zum Stoppen der Dienste.

Tabelle 1. Stoppfähige Dienste

Anzeigename in der Systemsteuerung	Befehlszeilenprozedur
TSM-Journalservice	`net stop "TSM-Journalservice"`
TSM-Clientakzeptor	`net stop "TSM-Clientakzeptor"`
TSM-Client-Scheduler	`net stop "TSM-Client-Scheduler"`
Ferner Clientagent	`net stop "ferner TSM-Clientagent"`

Führen Sie die folgenden Schritte aus, um ein Upgrade von einer früheren Version des Windows-Clients für Sichern/Archivieren auf Version 8.1.2 durchzuführen:

Vorgehensweise

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter.
   - Laden Sie das Clientpaket über Passport Advantage oder Fix Central herunter.
   - Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal.
2. Installieren Sie das Produkt mithilfe der komprimierten Installationsdatei, die Sie über Passport Advantage herunterladen.
   a. Kopieren Sie das heruntergeladene komprimierte Installationspaket auf eine lokale Platte oder in eine Netzfreigabe. Stellen Sie sicher, dass die Installationsdateien in ein leeres Verzeichnis extrahiert werden.
   b. Um die Installationsdateien in dasselbe Verzeichnis zu extrahieren, doppelklicken Sie auf das komprimierte Installationspaket.
   c. Standardmäßig werden die dekomprimierten Dateien im aktuellen Plattenlaufwerk im Verzeichnis *Downloadverzeichnis*\TSMClient gespeichert. Wenn das Installationsprogramm Dateien eines anderen Clientinstallationsversuchs in diesem Verzeichnis findet, werden Sie aufgefordert anzugeben, ob die alten Dateien überschrieben werden sollen. Wenn diese Eingabeaufforderung angezeigt wird, geben Sie `A` ein, um die vorhandenen Dateien zu überschreiben; mit dieser Auswahl wird sichergestellt, dass nur die Dateien der aktuellen Installation verwendet werden.
   d. Doppelklicken Sie auf die Datei spinstall.exe, um das Installationsprogramm für den Client zu starten.
3. Wählen Sie eine Sprache für diese Installation aus und klicken Sie auf OK.
4. Wenn Sie zur Installation von mindestens einer weiterverteilbaren Microsoft C++-Datei aufgefordert werden, bedeutet dies, dass auf Ihrem Knoten die vom Windows-Client für Sichern/Archivieren benötigten C++-Dateien nicht vorhanden sind. Klicken Sie auf Installieren, um die Dateien zu installieren und die Clientinstallation fortzusetzen. Oder klicken Sie auf Abbrechen, um den Installationsprozess zu beenden.
5. Das Installationsprogramm für den Client für Sichern/Archivieren wird gestartet. Klicken Sie in der Eingangsanzeige auf Weiter, um die Installation der neuen Client-Software zu starten.
6. Übernehmen oder ändern Sie das Standardinstallationsverzeichnis.
7. Wählen Sie den Installationstyp aus: Standard oder Angepasst.

Option	Bezeichnung
Standard	Bei einer Standardinstallation werden die folgenden Komponenten installiert: - Die Dateien der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren (erforderlich für die Verwendung der Java™-GUI) - Die Webdateien des Clients für Sichern/Archivieren (erforderlich für die Verwendung des Web-Clients) - Die Client-API-Dateien (nach Bedarf Ihres Clients und Ihres Betriebssystems)
Angepasst	Bei einer angepassten Installation werden die gleichen Dateien wie bei einer Standardinstallation installiert. Sie haben jedoch die Wahl, die folgenden optionalen Komponenten zu installieren: - Die SDK-Dateien der API. Diese Dateien sind nur erforderlich, wenn Sie Anwendungen entwickeln, die zusammen mit dem Client für Sichern/Archivieren eingesetzt werden. - Die Dateien für die Befehlszeile des Verwaltungsclients. Diese Dateien sind für die Ausführung von Administratorfunktionen auf dem IBM Spectrum Protect-Server erforderlich.

8. Klicken Sie auf Weiter und dann auf Installieren.
9. Wenn das Installationsprogramm die Installation beendet hat, klicken Sie auf Fertigstellen.
10. Überprüfen Sie die Installation. Klicken Sie auf Start > Alle Programme > IBM Spectrum Protect. Die von Ihnen installierten Clientkomponenten werden in der Liste der startfähigen IBM Spectrum Protect-Programme angezeigt. Diese Liste enthält nur die folgenden Komponenten: Verwaltungsbefehlszeilenclient, Befehlszeilenclient für Sichern/Archivieren und GUI für Sichern/Archivieren. Die anderen installierbaren Komponenten (die API-Laufzeit und die SDK-Dateien) werden in dieser Liste nicht angezeigt.
11. Klicken Sie auf den Eintrag GUI für Sichern/Archivieren in der Liste der startfähigen Programme.
    a. Bei der entsprechenden Aufforderung geben Sie Ihre Benutzer-ID und Ihr Kennwort ein und klicken Sie auf Anmelden.
    b. Klicken Sie nach dem Start der GUI auf Hilfe > Produktinformation zu IBM Spectrum Protect. Überprüfen Sie, ob Version 8.1.2 angezeigt wird.

Nächste Schritte

Ihre bisherigen Konfigurationseinstellungen bleiben in der Datei dsm.opt erhalten. Wenn Sie bisher LVSA als Momentaufnahmeprovider verwendet haben, werden beim Starten des Befehlszeilenclients Warnungen angezeigt. Die Warnungen enthalten Anweisungen zur Bearbeitung der Datei dsm.opt und zum Entfernen der LVSA-Optionen. Das Entfernen der nicht verwendeten Optionen ist nicht erforderlich. Wirkungslose oder nicht verwendete Optionen sollten jedoch entfernt werden, um die Fehlerbehebung zu erleichtern. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, werden die Nachrichten nicht angezeigt, sondern in der Datei dsmerror.log im Verzeichnis baclient des Clientinstallationsverzeichnisses protokolliert. Nachrichten werden ausgegeben, wenn die Datei dsm.opt eine der folgenden Optionen enthält. Einige dieser Optionen sind für VSS gültig. In diesem Fall werden die Nachrichten nur dann angezeigt und protokolliert, wenn Sie LVSA-spezifische Parameter enthalten.

- snapshotcachelocation
- snapshotfsidleretries
- snapshotproviderimage
- snapshotproviderfs
- snapshotcachesize

Sie können VSS-Optionen auf der Registerkarte Momentaufnahme im Profileditor definieren. Sie können auch mithilfe der Konfigurationsassistenten für die Online-Imageunterstützung und für die Unterstützung offener Dateien definiert werden. Zur Verwendung der Assistenten starten Sie die grafische Benutzerschnittstelle (GUI) und klicken Sie auf Dienstprogramme > Setup-Assistent. Wählen Sie die gewünschten Assistenten aus und klicken Sie auf Weiter. Treffen Sie dann Ihre Auswahl gemäß den Eingabeaufforderungen.
Zugehörige Konzepte:
Fehlerbehebung bei der Installation (Windows)
Windows-Betriebssysteme

Windows-Client erneut installieren

Wenn Sie den Windows-Client der Version 8.1.2 deinstallieren, können Sie ihn im Bedarfsfall erneut installieren.

Informationen zu diesem Vorgang

Wenn Sie den Windows-Client in dem Verzeichnis erneut installieren, in dem er vorher bereits installiert war, werden die vorherigen Konfigurationsdaten vom Installationsprogramm erkannt. Da die vorherigen Konfigurationsdaten erkannt werden, ist der Installationsprozess mit einer Upgradeinstallation identisch. Führen Sie die Schritte in Upgrade des Windows-Clients durchführen aus, um den Windows-Client erneut zu installieren.

Wenn die alten Konfigurationsdaten nicht beibehalten werden sollen, können Sie diese entfernen. Informationen zum vollständigen Entfernen von Clienteinstellungen und -dateien finden Sie im IBM® developerWorks-Artikel How to completely remove the Backup-Archive client from Microsoft Windows.

Wenn Sie alle Konfigurationseinstellungen vollständig entfernen und später den Windows-Client neu installieren wollen, führen Sie die Schritte in Erstinstallation des Windows-Clients aus. Dieses Installationsverfahren ist geeignet, wenn Sie die Software in einem anderen Verzeichnis oder auf einem System, auf dem sich keine alten Konfigurationsdaten befinden, erneut installieren.

Windows-Betriebssysteme

Unbeaufsichtigte Installation

Das Installationsprogramm des Clients für Sichern/Archivieren unterstützt unbeaufsichtigte Installationen.

Anmerkung: Die weiterverteilbaren Pakete von Microsoft Visual C++ 2010 und 2012 sind für die Verwendung des Clients für Sichern/Archivieren erforderlich. Das grafisch orientierte Installationsprogramm installiert diese Pakete für Sie. Bei einer unbeaufsichtigten Installation des Clients unter Verwendung von MSIEXEC müssen Sie die weiterverteilbaren Pakete von Microsoft Visual C++ 2010 und 2012 separat installieren. Die Pakete können vor oder nach der unbeaufsichtigten Installation des Clients installiert werden. Ihre Installation muss jedoch vor der Verwendung des Clients für Sichern/Archivieren erfolgen.
Verwenden Sie die folgenden ausführbaren Dateien, um die weiterverteilbaren Pakete von C++ 2010 und 2012 zu installieren. In den gezeigten Pfadangaben steht die Zeichenfolge *Verzeichnis* für das Laufwerk und das Verzeichnis, in denen die Dateien beim Extrahieren aus dem Installationspaket gespeichert wurden.

Ausführbare Windows-Dateien für die Installation von weiterverteilbaren C++-Paketen
Verzeichnis\ISSetupPrerequisites\{270b0954-35ca-4324-bbc6-ba5db9072dad} (enthält MS 2010 x86 C++ Runtime - vcredist_x86.exe)
Verzeichnis\ISSetupPrerequisites\{BF2F04CD-3D1F-444e-8960-D08EBD285C3F} (enthält MS 2012 x86 C++ Runtime - vcredist_x86.exe)
Verzeichnis\ISSetupPrerequisites\{7f66a156-bc3b-479d-9703-65db354235cc} (enthält MS 2010 x64 C++ Runtime - vcredist_x64.exe)
Verzeichnis\ISSetupPrerequisites\{3A3AF437-A9CD-472f-9BC9-8EEDD7505A02} (enthält MS 2012 x64 C++ Runtime - vcredist_x64.exe)

Bevor Sie mit der unbeaufsichtigten Installation beginnen, installieren Sie anhand der folgenden Anweisungen eine vordefinierte (angepasste) Datei dsm.opt:

- Stellen Sie die angepasste Kopie der Datei dsm.opt in das Verzeichnis ...\CONFIG, das sich im Installationsimage befindet, beispielsweise:
  - `C:\tsm_images\TSMClient\Programme 64\Tivoli\TSM\config`

  Die Datei muss den Namen *dsm.opt* haben.

- Das Installationsprogramm kopiert die vordefinierte Datei dsm.opt in das Verzeichnis ..\BACLIENT, wenn BEIDE der folgenden Bedingungen erfüllt sind:
  - Die Datei dsm.opt ist NICHT im Verzeichnis ..\BACLIENT vorhanden. Das Installationsprogramm überschreibt keine vorhandene Datei dsm.opt.
  - Die Datei dsm.opt ist, wie oben beschrieben, im Verzeichnis ..\CONFIG des Installationsimage vorhanden.

Um die weiterverteilbaren C++-Pakete oder den Client für Sichern/Archivieren unbeaufsichtigt zu installieren, müssen Sie die Benutzerkontensteuerung inaktivieren.

Um die Benutzerkontensteuerung zu inaktivieren, verwenden Sie entweder die Windows-Systemsteuerung oder das Dienstprogramm MSCONFIG.

- Um die Benutzerkontensteuerung über die Systemsteuerung zu inaktivieren, rufen Sie die Systemsteuerung auf, lokalisieren Sie die Einstellungen der Benutzerkontensteuerung und setzen Sie dann die Benachrichtigungsstufe auf Nie benachrichtigen.
- Um die Benutzerkontensteuerung mit dem Dienstprogramm MSCONFIG zu inaktivieren, öffnen Sie ein Fenster mit Eingabeaufforderung und geben Sie msconfig ein. Wählen Sie das Tool für die Einstellungen der Benutzerkontensteuerung aus und setzen Sie die Benachrichtigungsstufe auf Nie benachrichtigen.

Denken Sie daran, nach der Installation der weiterverteilbaren C++-Pakete und des Windows-Clients die Benutzerkontensteuerung wieder zu aktivieren.

Zur Installation der weiterverteilbaren C++-Pakete sind erhöhte Berechtigungen erforderlich. Öffnen Sie wie folgt ein Fenster mit Eingabeaufforderung:

1. Klicken Sie auf Start > Alle Programme > Zubehör > Eingabeaufforderung.
2. Klicken Sie mit der rechten Maustaste auf auf das Symbol Eingabeaufforderung, um die Eigenschaften anzuzeigen.
3. Klicken Sie auf Als Administrator ausführen.
4. Klicken Sie im Berechtigungsfenster auf Weiter.
5. Starten Sie die Produktinstallation über das Fenster mit Eingabeaufforderung.

Unbeaufsichtigte Installation der weiterverteilbaren C++-Pakete

Führen Sie den folgenden Befehl zweimal aus. Führen Sie ihn zunächst in dem Verzeichnis aus, in dem die C++ 2010-Datei vcredist_x86.exe gespeichert ist. Führen Sie ihn dann erneut in dem Verzeichnis aus, in dem die C++ 2012-Datei vcredist_x86.exe gespeichert ist.

```
vcredist_x86.exe /install /quiet /norestart /log Protokolldateiname
```

Um weitere Informationen zum Befehl vcredist_x86.exe aufzurufen, führen Sie den folgenden Befehl aus:

```
vcredist_x86.exe /?
```

Führen Sie den folgenden Befehl zweimal aus. Führen Sie ihn zunächst in dem Verzeichnis aus, in dem die C++ 2010-Datei vcredist_x64.exe gespeichert ist. Führen Sie ihn dann erneut in dem Verzeichnis aus, in dem die C++ 2012-Datei vcredist_x64.exe gespeichert ist.

```
vcredist_x64.exe /install /quiet /norestart /log Protokolldateiname
```

Um weitere Informationen zu dem Befehl vcredist_x86.exe aufzurufen, führen Sie den folgenden Befehl aus:

```
vcredist_x64.exe /?
```

Installieren Sie den Windows-Client für Sichern/Archivieren. Die Benutzerkontensteuerung muss weiterhin inaktiviert sein. Ist dies nicht der Fall, inaktivieren Sie die Benutzerkontensteuerung jetzt. Öffnen Sie eine Eingabeaufforderung mit erhöhten Berechtigungen.

1. Klicken Sie auf Start > Alle Programme > Zubehör > Eingabeaufforderung.
2. Klicken Sie mit der rechten Maustaste auf auf das Symbol Eingabeaufforderung, um die Eigenschaften anzuzeigen.
3. Klicken Sie auf Als Administrator ausführen.
4. Klicken Sie im Berechtigungsfenster auf Weiter.
5. Starten Sie die unbeaufsichtigte Installation des Windows-Clients für Sichern/Archivieren über das Fenster mit Eingabeaufforderung. Führen Sie anhand der folgenden Anweisungen eine unbeaufsichtigte Installation des Windows-Clients und der Windows-API aus.

Unbeaufsichtigte Installation des Windows-Clients

Wenn Sie eine angepasste Version des Befehls msiexec (dieser ruft den Microsoft Software Installer auf) in eine Script- oder Stapeldatei einfügen, können Sie Installationen auf mehreren Windows-Systemen ausführen. Mit dem folgenden Beispielbefehl werden der Befehlszeilenclient für Sichern/Archivieren, die Client-GUI, der Web-Client, die API und der Verwaltungsbefehlszeilenclient installiert. Sie müssen dieses Beispiel unter Umständen anpassen, damit es auf Ihrem System korrekt ausgeführt wird. Der Befehl in dem folgenden Beispiel erstreckt sich zwar über mehrere Zeilen, Sie müssen ihn jedoch in einer einzigen Befehlszeile eingeben.

```
msiexec /i "Z:\tsm_images\TSMClient\IBM Tivoli Storage Manager Client.msi" RebootYesNo="No"
REBOOT="Suppress" ALLUSERS=1 INSTALLDIR="C:\Programme\Tivoli\Tsm"
ADDLOCAL="BackupArchiveGUI,BackupArchiveWeb,Api64Runtime, AdministrativeCmd" TRANSFORMS=1033.mst /qn /l*v
"C:\log.txt"
```

Beschreibung der Parameter für die unbeaufsichtigte Installation:

msiexec
: Startet das Programm Microsoft Software Installer (MSI).

/i
: Installiert das angegebene Quellenpaket (wird /i durch /x ersetzt, wird das Paket deinstalliert).

"*Z:*\tsm_images\TSMClient\IBM Tivoli Storage Manager Client.msi"
: Gibt den vollständigen Pfad zu dem Quellenpaket an. In diesem Beispiel wird das Laufwerk Z verwendet. Geben Sie den Laufwerkbuchstaben des Plattenlaufwerks in Ihrer Konfiguration an, in dem sich das Installationsimage befindet.

RebootYesNo="No" REBOOT="Suppress"
: Unter bestimmten Bedingungen muss unter Umständen ein Systemwarmstart durchgeführt werden, damit die Installation erfolgreich abgeschlossen werden kann. Diese Option bewirkt, dass das Installationsprogramm einen Warmstart für das System unterdrückt, auch wenn unter Umständen Gründe vorliegen, die im Normalfall einen Warmstart verursachen würden. Diese Option ist zwar bequem, sollte aber mit Vorsicht verwendet werden, da die Unterdrückung des Warmstarts dazu führen könnte, dass das Programm unvorhersehbar reagiert. Die häufigste Ursache für einen Warmstart ist, wenn es sich bei der Installation um ein Upgrade eines bestehenden Clients für Sichern/Archivieren handeln würde und die Installation während der Ausführung der Clientprogramme erfolgen würde. Beenden Sie daher alle Programme und Services des Clients für Sichern/Archivieren, bevor Sie die Installation starten.

ALLUSERS=1
: Gibt an, dass das Paket für alle Benutzer vorgesehen ist. Diese Option ist erforderlich.

INSTALLDIR="C:\Programme\Tivoli\TSM"
: Gibt den Zielpfad an. Wenn dieses Produkt oder eine vorherige Version dieses Produkts bereits auf Ihrer Workstation installiert wurde, verwenden Sie das aktuelle Installationsverzeichnis als Zielpfad für dieses Paket.

ADDLOCAL="BackupArchiveGUI,BackupArchiveWeb,Api64Runtime"
: Gibt die zu installierenden Features an. Geben Sie alle Komponenten auf einer einzigen Zeile an, und zwar in Anführungszeichen eingeschlossen, durch Komma getrennt und ohne Leerzeichen vor oder nach dem Komma. Die installierbaren Client-Features sind in der folgenden Tabelle aufgelistet:

Windows-Client-Features	**Featurebeschreibung**
BackupArchiveGUI	Grafische Benutzerschnittstelle
BackupArchiveWeb	Web-Client für Sichern/Archivieren
Api64Runtime	API-Laufzeit
ApiSdk	API-SDK
AdministrativeCmd	Verwaltungsbefehlszeile

TRANSFORMS=1033.mst
: Gibt an, welche Sprachenumsetzungen verwendet werden sollen. Die folgenden Sprachenumsetzungen sind verfügbar:

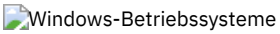
Umsetzung	**Sprache**
1028.mst	CHT Traditionelles Chinesisch
1029.mst	CSY Tschechisch
1031.mst	DEU Deutsch
1033.mst	ENG Englisch
1034.mst	ESP Spanisch
1036.mst	FRA Französisch
1038.mst	HUN Ungarisch
1040.mst	ITA Italienisch
1041.mst	JPN Japanisch
1042.mst	KOR Koreanisch
1045.mst	PLK Polnisch
1046.mst	PTB Portugiesisch
1049.mst	RUS Russisch
2052.mst	CHS Vereinfachtes Chinesisch

/qn
: Gibt an, dass das Produkt unbeaufsichtigt installiert werden soll.

/l*v "C:\log.txt"
: Gibt den Modus für ausführliches Protokollieren sowie den Namen und die Position der Protokolldatei an.

Der Installationsprozess erstellt den Ordner 'IBM Spectrum Protect' im Ordner 'Programme' im Windows-Menü Start. Sie können den Client für Sichern/Archivieren durch Klicken auf eines der Symbole in diesem Ordner starten.

Zugehörige Konzepte:
Fehlerbehebung bei der Installation (Windows)



Windows-Client ändern, reparieren oder deinstallieren

Sie können einen vorhandenen Windows-Client ändern, reparieren oder deinstallieren.

Informationen zu diesem Vorgang

Für eine Änderung, Reparatur oder Deinstallation des Windows-Clients verwenden Sie die Windows-Systemsteuerung.

Vorgehensweise

1. Klicken Sie auf Start > Systemsteuerung > Programm deinstallieren.
2. Wählen Sie IBM Spectrum Protect-Client in der Liste der installierten Programme aus.
3. Wählen Sie die gewünschte Funktion aus: Reparieren, Ändern oder Deinstallieren.

Option	Bezeichnung
Reparieren	Warten Sie, bis alle laufenden Tasks des Clients für Sichern/Archivieren beendet sind, bevor Sie den Windows-Client reparieren. Mit dieser Option kann eine vorhandene Windows-Clientinstallation repariert werden. Wenn Sie Reparieren auswählen, werden die vom Installationsprogramm installierten Dateien untersucht, um festzustellen, ob sie in irgendeiner Weise beschädigt wurden. Wenn festgestellt wird, dass eine Datei beschädigt ist, wird bei der Reparatur versucht, diese Datei durch eine Datei aus dem gespeicherten Installationsimage zu ersetzen. Bei der Reparatur werden auch fehlende Programmverknüpfungen und -symbole, fehlende Dateien und Registrierungsschlüssel repariert.
Ändern	Warten Sie, bis alle laufenden Tasks des Clients für Sichern/Archivieren beendet sind, bevor Sie den Windows-Client ändern. Mit dieser Option kann eine vorhandene Installation geändert werden. Wenn Sie Ändern auswählen, wird in der nächsten Anzeige Ändern als Option für die Änderung installierter Programme angezeigt. Wenn Sie den Client bereits installiert haben und Komponenten hinzufügen oder entfernen müssen, klicken Sie auf Ändern und wählen Sie Ändern aus. Wählen Sie das Symbol neben der Komponente, die installiert oder entfernt werden soll, und dann die entsprechende Aktion in der Dropdown-Liste aus. Wenn Sie den Client beispielsweise mit der Standardinstallation installiert haben, sind die Befehlszeilenschnittstellendateien des Verwaltungsclients nicht installiert. Wenn Sie zu dem Entschluss kommen, dass ein Knoten diese Schnittstelle benötigt, wählen Sie das Symbol neben Verwaltungsclient - Befehlszeilendateien aus und klicken Sie auf die Option Diese Funktion wird auf der lokalen Festplatte installiert. Anmerkung: Mit dieser Option erzielen Sie dasselbe Ergebnis wie bei einem Upgrade des Clients. Der Unterschied besteht darin, dass Sie die ersten Schritte umgehen, so dass der Installationsprozess mit dem zuletzt ausgewählten Installationstyp beginnt. Wenn der Installationstyp geändert werden soll, können Sie auf Zurück klicken und den neuen Installationstyp auswählen; geben Sie dann die angeforderten erforderlichen Informationen an. Wenn Sie Fragen zu einer Eingabeaufforderung haben, lesen Sie die Informationen in Upgrade des Windows-Clients durchführen (beginnen Sie mit Schritt 7).

Option	Bezeichnung
Deinstallieren	Warten Sie, bis alle laufenden Tasks des Clients für Sichern/Archivieren beendet sind, bevor Sie den Windows-Client deinstallieren. Mit dieser Option wird das Windows-Clientprogramm deinstalliert. Es werden keine Client-Services entfernt. Außerdem werden keine Protokolldateien und anderen Elemente, die bei der Konfiguration oder Verwendung des Clients erstellt wurden, entfernt. Die meisten dieser Artefakte verbleiben im Installationsverzeichnis (Programme\Tivoli\TSM), sie können sich jedoch - abhängig von Auswahl des Installationsverzeichnisses und anderer Optionen - an jeder beliebigen Position auf der Platte befinden. Mit dieser Option werden außerdem keine Dateien entfernt, die auf die lokale Platte kopiert wurden, wenn Sie die Installationsdateien aus einer komprimierten Verteilungsdatei extrahiert haben. Der Verbleib dieser Artefakte auf der Platte stellt kein Problem dar, wenn der Client später erneut installiert werden soll. Informationen zum vollständigen Entfernen des Clients sowie zugehöriger Dateien und Einstellungen finden Sie im Wiki-Artikel How to completely remove the Backup-Archive client from Microsoft Windows. Das Installationsprogramm stoppt alle aktiven Client-Services (Dienste), bevor es die Software deinstalliert. Wenn Sie die Services selbst stoppen möchten, geben Sie die folgenden Befehle in einem Fenster mit Eingabeaufforderung ein: ◦ `net stop "TSM-Journalservice"` ◦ `net stop "TSM-Clientakzeptor"` ◦ `net stop "TSM-Client-Scheduler"` ◦ `net stop "ferner TSM-Clientagent"` Sie können diese Dienste auch über die Systemsteuerung stoppen. Ihre Anzeigenamen entsprechen den in der Befehlszeile verwendeten Namen. Anmerkung: Die hier gezeigten Dienstnamen sind die vom Installationsprogramm festgelegten Standardnamen. Sie können einige dieser Dienstnamen ändern, wenn Sie die Dienste mit einem der Konfigurationsassistenten in den Menüs Dienstprogramme > Setup-Assistent konfigurieren. Wenn Sie den Dienstnamen ändern, notieren Sie den geänderten Namen und verwenden Sie diesen zum Stoppen der Dienste. Wenn einer dieser Dienste entfernt werden soll, ohne den Client zu deinstallieren, führen Sie die folgenden Schritte aus: a. Klicken Sie auf Start > Alle Programme > IBM Spectrum Protect > GUI für Sichern/Archivieren. b. Klicken Sie auf Dienstprogramme > Setup-Assistent. c. Wählen Sie den Assistenten aus und führen Sie ihn für jeden Dienst aus, der entfernt werden soll. Mit den Optionen des Setup-Assistenten können auch die Konfigurationsdaten für die Online-Image-Unterstützung und die Unterstützung offener Dateien entfernt werden.

 Windows-Betriebssysteme

Fehlerbehebung bei der Installation (Windows)

Wenn Sie ein Upgrade von einer vorherigen Version des Clients für Sichern/Archivieren durchführen und Client-Services (beispielsweise Clientakzeptor oder Scheduler) aktiv sind, wird während der Installation möglicherweise ein Fehler angezeigt.

Sind für ein beliebiges Konto IBM Spectrum Protect-Client-Services aktiv (z. B. Clientakzeptor oder Scheduler), wird während der Installation möglicherweise eine Anforderung für einen Warmstart des Systems angezeigt. Sie müssen alle Instanzen des IBM Spectrum Protect-Clients für alle Konten stoppen, bevor die Installation gestartet wird.

Bei der Installation wird möglicherweise der folgende Fehler angezeigt:

```
Fehler 1303. Das Installationsprogramm verfügt nicht über ausreichende
Berechtigungen für den Zugriff auf folgendes Verzeichnis:
(Installationslaufwerk):\Programme\Tivoli\TSM\baclient\plugins. Die Installation
kann nicht fortgesetzt werden. Melden Sie sich als Administrator an oder wenden
Sie sich an Ihren Systemadministrator.
```

Wenn dieser Fehler auftritt, müssen Sie die Installation stoppen. Nach dem Stoppen des Installationsprozesses ist die vorherige Version nicht mehr installiert. Stoppen Sie die Client-Services und wiederholen Sie den Installationsprozess.

 Windows-Betriebssysteme

Softwareaktualisierungen

IBM® kann Softwareaktualisierungen regelmäßig für den Download bereitstellen.

Die neuesten Informationen, Aktualisierungen und Wartungsfixes finden Sie im IBM Support Portal for IBM Spectrum Protect.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Clientverwaltungsservice zur Erfassung von Diagnoseinformationen installieren

Sie können die IBM Spectrum Protect-Clientverwaltungsservices installieren, um Diagnoseinformationen zum Client für Sichern/Archivieren zu erfassen. Der Clientverwaltungsservice macht IBM Spectrum Protect Operations Center die Informationen für grundlegende Überwachungsfunktionen verfügbar.

Informationen zu diesem Vorgang

Nachdem Sie den Client für Sichern/Archivieren installiert haben, installieren Sie den Clientverwaltungsservice auf demselben Computer, damit der IBM Spectrum Protect-Serveradministrator Diagnoseinformationen aus Operations Center anzeigen kann.

Installationsanweisungen und weitere Informationen zum Clientverwaltungsservice finden Sie in Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen.

Clients für Sichern/Archivieren konfigurieren

Sie können den Client für Sichern/Archivieren für die Verwendung zahlreicher verfügbarer Clientfunktionen konfigurieren. Informationen zur Konfiguration des Clients für Sichern/Archivieren werden bereitgestellt.

- IBM Spectrum Protect-Client konfigurieren
  Nachdem Sie den Client für Sichern/Archivieren installiert haben, müssen Sie ihn vor der Ausführung von Operationen konfigurieren.
- Erste Schritte
  Bevor Sie den IBM Spectrum Protect-Client für Sichern/Archivieren verwenden können, müssen Sie wissen, wie eine GUI- oder Befehlszeilensitzung gestartet und der Client-Scheduler automatisch gestartet wird. Sie lernen auch andere häufig verwendete Tasks kennen.

Zugehörige Konzepte:
IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Zugehörige Tasks:
Daten mit Clients für Sichern/Archivieren sichern und zurückschreiben
Daten mit Clients für Sichern/Archivieren archivieren und abrufen
Operationen für Clients für Sichern/Archivieren planen
Zugehörige Verweise:
Optionen und Befehle des Clients für Sichern/Archivieren

IBM Spectrum Protect-Client konfigurieren

Nachdem Sie den Client für Sichern/Archivieren installiert haben, müssen Sie ihn vor der Ausführung von Operationen konfigurieren.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWenn Sie ein Upgrade des Clients für Sichern/Archivieren durchführen, ist es nicht erforderlich, den Scheduler, den Web-Client oder andere Konfigurationseinstellungen zu rekonfigurieren. Wenn die von der vorherigen Clientinstallation verwendeten Dateien dsm.opt und dsm.sys im Standardinstallationsverzeichnis bzw. in dem Verzeichnis oder der Datei verfügbar sind, auf das/die die Umgebungsvariablen DSM_CONFIG und DSM_DIR verweisen, greift der Client auf diese Dateien zu, um Konfigurationsdaten abzurufen.

Windows-BetriebssystemeWenn Sie ein Upgrade des Clients für Sichern/Archivieren durchführen, ist es nicht erforderlich, den Scheduler, den Web-Client oder andere Konfigurationseinstellungen zu rekonfigurieren. Wenn die von der vorherigen Clientinstallation verwendete Datei dsm.opt im Standardinstallationsverzeichnis bzw. in dem Verzeichnis oder der Datei verfügbar ist, auf das/die die Umgebungsvariablen DSM_CONFIG und DSM_DIR verweisen, greift der Client auf diese Datei zu, um Konfigurationsdaten abzurufen.

Einige Konfigurationstasks sind erforderlich, andere sind optional. Die folgenden Konfigurationstasks sind erforderlich:

- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme
  Clientsystemoptionsdatei erstellen und ändern
- Windows-BetriebssystemeClientoptionsdatei erstellen und ändern
- Workstation bei einem Server registrieren

Die folgenden Konfigurationstasks sind optional:

- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeStandardclientbenutzeroptionsdatei erstellen
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeAngepasste Clientbenutzeroptionsdatei erstellen
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeUmgebungsvariablen
- Windows-BetriebssystemeOptionsdatei in gemeinsam genutztem Verzeichnis erstellen
- Windows-BetriebssystemeMehrere Clientoptionsdateien erstellen
- Windows-BetriebssystemeUmgebungsvariablen
- Windows-BetriebssystemeSprache für die Anzeige der Java-GUI konfigurieren
- Windows-BetriebssystemeWeb-Client auf Windows-Systemen konfigurieren

- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWeb-Client auf AIX-, Linux-, Mac- und Solaris-Systemen konfigurieren
- Scheduler konfigurieren
- Windows-BetriebssystemeJournalsteuerkomponentenservice konfigurieren
- Windows-BetriebssystemeUnterstützung für Online-Imagesicherung konfigurieren
- Windows-BetriebssystemeUnterstützung offener Dateien konfigurieren
- Einschluss-/Ausschlussliste erstellen
- Linux-BetriebssystemeWindows-BetriebssystemeParallele Sicherungen von virtuellen VMware-Maschinen konfigurieren. Siehe Parallele Sicherungen virtueller Maschinen.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTasks für Rootbenutzer und berechtigte Benutzer UNIX- und Linux-Clients
  Ein berechtigter Benutzer ist jeder Benutzer ohne Rootberechtigung, der über Lese- und Schreibzugriff auf das gespeicherte Kennwort (Datei TSM.sth) verfügt, oder eine beliebige Person, die das Kennwort kennt und interaktiv eingibt. Berechtigte Benutzer definieren das Verzeichnis, in dem ihre Kopie der Kennwortdatei gespeichert ist, mit der Option passworddir.
- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeBenutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen
  Damit Benutzer ohne Rootberechtigung eigene Daten mithilfe des Clients für Sichern/Archivieren verwalten können, muss der Systemadministrator zusätzlich zu den normalen Konfigurationsschritten weitere Schritte ausführen, mit denen berechtigte Erstbenutzer für Benutzer ohne Rootberechtigung konfiguriert werden.
- Übersicht über die Clientoptionsdatei
  In einer Clientoptionsdatei können Sie Clientoptionen und Werte festlegen (angeben). Clientoptionen können auch auf dem Server in einer *Clientoptionsgruppe* definiert werden. In einer Clientoptionsgruppe auf dem Server festgelegte Clientoptionen setzen die in der Clientoptionsdatei definierten Clientoptionen außer Kraft.
- Windows-BetriebssystemeUmgebungsvariablen
  Im Allgemeinen ist die Definition von Umgebungsvariablen eine optionale Task. Wenn Sie sie definieren, erleichtert dies die Verwendung der Befehlszeile.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeUmgebungsvariablen
  Im Allgemeinen ist die Definition von Umgebungsvariablen eine optionale Task. Wenn Sie diese Variablen definieren, erleichtert dies die Verwendung der Befehlszeile.
- Windows-BetriebssystemeSprache für die Anzeige der Java-GUI konfigurieren
  Sie können die Sprache für die Anzeige der Java-GUI des Clients für Sichern/Archivieren auswählen.
- Übersicht über die Konfiguration des Web-Clients
  Der IBM Spectrum Protect-Web-Client stellt die Fernverwaltung eines Clientknotens über einen Web-Browser zur Verfügung. Die Prozeduren für die Konfiguration des Web-Clients variieren abhängig davon, welches Betriebssystem auf dem Clientknoten verwendet wird.
- Scheduler konfigurieren
  Ihr IBM Spectrum Protect-Administrator kann den Client für die automatische Ausführung von Tasks konfigurieren. Damit geplante Ereignisse auf dem Client stattfinden können, müssen Sie den Client-Scheduler für die Kommunikation mit dem IBM Spectrum Protect-Server konfigurieren.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeClient-Scheduler starten
  Diese Task führt Sie durch die Schritte zum Planen von Ereignissen mithilfe der grafischen Benutzerschnittstelle und des Befehlszeilenclients.
- Windows-BetriebssystemeClient-Scheduler starten
  Um den Client-Scheduler zu starten, verwenden Sie die Systemsteuerung oder den Befehl **net start**.
- IBM Spectrum Protect-Client/Server-Übertragung über eine Firewall hinweg konfigurieren
  In den meisten Fällen können die IBM Spectrum Protect-Server und -Clients über eine Firewall hinweg zusammenarbeiten.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeIBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren
  Secure Sockets Layer (SSL) ermöglicht eine sichere Kommunikation auf SSL-Basis nach Industriestandard zwischen dem IBM Spectrum Protect-Client und -Server.
- AIX-BetriebssystemeWindows-BetriebssystemeLinux-BetriebssystemeSystem für die journalbasierte Sicherung konfigurieren
  Bevor Sie journalbasierte Sicherungen ausführen können, müssen Sie den Journaldämon (Linux) oder den Journalsteuerkomponentenservice (Windows) installieren und konfigurieren.
- Clientseitige Datendeduplizierung
  Die *Datendeduplizierung* ist eine Methode zur Reduzierung des Speicherbedarfs, indem redundante Daten entfernt werden.
- Konfiguration und Verwendung der automatisierten Clientübernahme
  Wenn der IBM Spectrum Protect-Server nicht verfügbar ist, kann eine automatische Übernahme des Clients für Sichern/Archivieren auf einem Sekundärserver zum Zweck der Datenwiederherstellung stattfinden. Sie können in der Konfiguration des Clients die automatisierte Übernahme angeben oder eine Übernahme des Clients unterbinden. Außerdem können Sie den Replikationsstatus Ihrer Daten auf dem Sekundärserver bestimmen, bevor Sie die replizierten Daten zurückschreiben oder abrufen.
- Linux-BetriebssystemeWindows-BetriebssystemeClient für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren
  Bevor Sie Tivoli Storage Manager FastBack-Clientdaten sichern oder archivieren können, müssen Sie Konfigurationstasks ausführen.
- Windows-BetriebssystemeClient für Sichern/Archivieren für den Schutz von FastBack-Clientdaten konfigurieren
  Sie können den Client für Sichern/Archivieren mithilfe des Clientkonfigurationsassistenten für den Schutz von FastBack-Clientdaten konfigurieren.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeKonfiguration und Verwendung der Clusterumgebung

Der Begriff *Cluster* hat in unterschiedlichen Umgebungen unterschiedliche Bedeutungen. Er kann Folgendes bedeuten: hoch verfügbar, hohe Leistung, Lastausgleich, Grid-Computing oder eine Kombination all dieser Begriffe.

- Windows-BetriebssystemeClient für Sichern/Archivieren in einer Cluster-Server-Umgebung konfigurieren
  Sie können die Software des Clients für Sichern/Archivieren lokal auf jedem Knoten eines Clusters in einer MSCS-Umgebung (Microsoft Cluster Server) oder VCS-Umgebung (Veritas Cluster Server) installieren.
- Windows-BetriebssystemeUnterstützung für Online-Imagesicherung konfigurieren
  Wenn die Online-Imagefunktion konfiguriert ist, führt der Client für Sichern/Archivieren eine momentaufnahmebasierte Imagesicherung aus, während der der reale Datenträger für andere Systemanwendungen verfügbar ist.
- Windows-BetriebssystemeUnterstützung offener Dateien konfigurieren
  Sie konfigurieren die Unterstützung offener Dateien (Open File Support, OFS) nach der Installation des Windows-Clients.
- AIX-BetriebssystemeHinweise zur AIX-Konfiguration vor Ausführung von momentaufnahmebasierten Dateisicherungen und -archivierungen
  Wenn Sie Ihren IBM Spectrum Protect-AIX-Client für die Ausführung von momentaufnahmebasierten Dateisicherungen und -archivierungen konfigurieren, sind einige Hinweise zu beachten.
- Linux-BetriebssystemeWindows-BetriebssystemeNetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren
  Sie müssen die Verbindungsinformationen für den NetApp-Dateiserver konfigurieren, damit der Befehl für eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz auf dem Client für Sichern/Archivieren ausgeführt werden kann. Außerdem müssen Sie mit dem Befehl set password den Hostnamen des Dateiservers sowie das Kennwort und den Benutzernamen für den Zugriff auf den Dateiserver angeben.
- Workstation bei einem Server registrieren
  Damit Sie IBM Spectrum Protect verwenden können, müssen Sie einen Knotennamen und ein Kennwort definieren und Ihren Knoten beim Server registrieren.
- Einschluss-/Ausschlussliste erstellen
  Wenn Sie keine Einschluss-/Ausschlussliste erstellen, berücksichtigt der Client für Sichern/Archivieren alle Dateien für Sicherungsservices und verwendet die Standardverwaltungsklasse für Sicherungs- und Archivierungsservices.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Tasks für Rootbenutzer und berechtigte Benutzer UNIX- und Linux-Clients

Ein berechtigter Benutzer ist jeder Benutzer ohne Rootberechtigung, der über Lese- und Schreibzugriff auf das gespeicherte Kennwort (Datei TSM.sth) verfügt, oder eine beliebige Person, die das Kennwort kennt und interaktiv eingibt. Berechtigte Benutzer definieren das Verzeichnis, in dem ihre Kopie der Kennwortdatei gespeichert ist, mit der Option passworddir.

In Tabelle 1 sind die Tasks aufgeführt, die ein Root, berechtigte Benutzer und andere Benutzer ausführen können bzw. nicht ausführen können.

Tabelle 1. Tasks für Roots und berechtigte Benutzer

Task	Root	Berechtigter Benutzer
Mit einem LDAP-Server zur Authentifizierung der Berechtigungsnachweise beim IBM Spectrum Protect-Server anmelden.	Ja	Ja
Neue Knoten auf dem IBM Spectrum Protect-Server registrieren (wenn die offene Registrierung auf dem Server angegeben ist).	Ja	Ja

Task	Root	Berechtigter Benutzer
IBM Spectrum Protect-Kennwort für Client-Workstations definieren oder erneut erstellen.	Ja	Ja
Sichern	Ja Anmerkung: Der IBM Spectrum Protect-Administrator kann entweder für den Befehl Register Node oder für den Befehl Update Node eine Option angeben, um zu definieren, wer zum Sichern von Daten für einen Knoten berechtigt sein soll. Wird für BACKUPINITiation die Einstellung root verwendet, schränkt dies Sicherungen dahingehend ein, dass nur Rootbenutzer oder berechtigte Benutzer die Dateien auf einem Knoten sichern dürfen. Wird für BACKUPINITiation die Einstellung all verwendet, kann jeder beliebige Benutzer Daten auf einem Knoten sichern. Informationen zu diesen Befehlen und Optionen finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.	Ja, wenn Sie über Lesezugriff verfügen, unabhängig vom Eigentumsrecht
Zurückschreibung	Ja; beim Zurückschreiben an eine neue Position oder an dieselbe Position werden Dateiberechtigung und Eigentumsrecht beibehalten	Ja; das Betriebssystem verhindert jedoch das Schreiben an dieselbe Position, wenn die Datei nur Lesezugriff hat. Beim Zurückschreiben an dieselbe Position werden Dateiberechtigungen und Eigentumsrecht beibehalten. Beim Zurückschreiben an eine andere Position werden die Berechtigungen der zurückgeschriebenen Datei beibehalten, das Eigentumsrecht geht jedoch auf den aktuellen Benutzer über.
Archivieren	Ja	Ja, wenn Sie über Lesezugriff verfügen, unabhängig vom Eigentumsrecht
Abruf	Ja. Beim Abrufen an eine neue Position oder an dieselbe Position werden Dateiberechtigungen und Eigentumsrecht beibehalten.	Ja. Das Betriebssystem verhindert jedoch das Schreiben an dieselbe Position, wenn die Datei nur Lesezugriff hat. Das Eigentumsrecht aller abgerufenen Objekte geht auf den aktuellen Benutzer über.
Client-Scheduler	Ja	Ja, wenn der Clientakzeptordämon nicht verwendet wird. Für die Verwaltung des Clientakzeptordämons müssen Sie Root sein. Ein berechtigter Benutzer ohne Rootberechtigung kann den Scheduler (dsmc sched) verwenden.
Benutzerzugriff auf Dateien auf dem IBM Spectrum Protect-Server erteilen	Ja	Ja
Dateibereiche auf dem IBM Spectrum Protect-Server löschen	Ja, wenn der IBM Spectrum Protect-Serveradministrator dem Knoten die Berechtigung zum Löschen von Sicherungen oder Archivierungen erteilt hat.	Ja, wenn der IBM Spectrum Protect-Serveradministrator dem Knoten die Berechtigung zum Löschen von Sicherungen oder Archivierungen erteilt hat.

Auf Mac OS X-Systemen ist ein Systemadministrator jeder Benutzer, der das System verwalten darf. Sie können Ihren Kontotyp mithilfe des Tools Systemvorgaben > Accounts überprüfen. Der Kontotyp von Systemadministratoren lautet Admin.

Mac OS X-BetriebssystemeEs ist Aufgabe des Systemadministrators, den Client für Sichern/Archivieren so zu konfigurieren, dass Benutzer ohne Administratorberechtigung eigene Daten verwalten können. Benutzer ohne Administratorberechtigung (oder nicht berechtigte Benutzer)

entsprechen den folgenden Kriterien:

Mac OS X-Betriebssysteme

- Sie haben nicht die Benutzer-ID 0 und sind nicht der Rootbenutzer.
- Sie haben ein Benutzerkonto, das nicht als Systemadministrator konfiguriert ist.

Mac OS X-BetriebssystemeWenn für die Ausführung einer Task zusätzliche Berechtigung erforderlich ist, müssen Sie zum Starten des Clients für Sichern/Archivieren die Berechtigungsanwendung verwenden. Dies ermöglicht die Ausführung des Clients mit ausreichenden Systemberechtigungen zur Ausführung der Task. In der folgenden Tabelle sind die zu verwendenden Berechtigungstools aufgelistet.

Tabelle 2. Mac OS X-Berechtigungstools und zugeordnete IBM Spectrum Protect-Anwendungen

Mac OS X-Berechtigungstool	Zugeordnete IBM Spectrum Protect-Anwendung
IBM Spectrum Protect For Administrators	IBM Spectrum Protect StartCad.sh StopCad.sh
sudo	dsmc

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

Benutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen

Damit Benutzer ohne Rootberechtigung eigene Daten mithilfe des Clients für Sichern/Archivieren verwalten können, muss der Systemadministrator zusätzlich zu den normalen Konfigurationsschritten weitere Schritte ausführen, mit denen berechtigte Erstbenutzer für Benutzer ohne Rootberechtigung konfiguriert werden.

Zusätzlich zu den normalen Konfigurationsschritten muss der Systemadministrator die folgenden Schritte ausführen, mit denen berechtigte Benutzer für Benutzer ohne Rootberechtigung konfiguriert werden:

1. Eine Zeilengruppe für den Benutzer ohne Rootberechtigung in der Clientsystemoptionsdatei, dsm.sys, hinzufügen.
2. In dieser Zeilengruppe mit der Option passworddir auf ein Verzeichnis zeigen, dessen Eigner der Benutzer ohne Rootberechtigung ist. Der Benutzer ohne Rootberechtigung kann dann eine Datei in diesem passworddir-Verzeichnis erstellen.
3. Dem Benutzer ohne Rootberechtigung einen eindeutigen TSM-Knotennamen zuordnen.
4. Sicherstellen, dass im passworddir-Verzeichnis keine vorherige Datei TSM.PWD, deren Eigner nicht der Benutzer ohne Rootberechtigung ist, vorhanden ist. Ist eine solche Datei vorhanden, das Eigentumsrecht dieser Datei dem Benutzer ohne Rootberechtigung übertragen oder die Datei entfernen.
5. Sicherstellen, dass im passworddir-Verzeichnis keine Datei TSM.KDB, TSM.IDX oder TSM.sth, deren Eigner nicht der Benutzer ohne Rootberechtigung ist, vorhanden ist. Sind diese Dateien vorhanden, müssen sie entfernt werden.

Nachdem der Systemadministrator diese Schritte ausgeführt hat, muss der Benutzer ohne Rootberechtigung die folgenden Schritte ausführen:

1. Eine Clientsystemoptionsdatei, dsm.opt, erstellen und mit der Option servername den Namen der Zeilengruppe angeben.
2. Sicherstellen, dass die Datei dsm.opt von der Umgebungsvariablen DSM_CONFIG standardmäßig gelesen werden kann. Eine Überprüfung kann durch Ausgabe des Befehls export DSM_CONFIG=<dsm.opt> in einem Shellbefehlsfenster erfolgen.
3. Den Befehl dsmc q f ausführen, um Kennwortdateien zu verwenden, auf die die Option passworddir zeigt. Sind keine Kennwortdateien vorhanden, erfolgt eine Benutzereingabeaufforderung.

- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeVerschlüsselung für Benutzer des Clients für Sichern/Archivieren aktivieren
  Wenn Sie in der Konfiguration des Clients für Sichern/Archivieren festlegen, dass Daten während Sicherungs- und Archivierungsoperationen verschlüsselt werden sollen, und wenn Sie die Option für die Speicherung des Kennworts für den Verschlüsselungsschlüssel (encryptkey save) angeben, können standardmäßig nur Rootbenutzer und berechtigte IBM Spectrum Protect-Benutzer das gespeicherte Kennwort zur Verschlüsselung oder Entschlüsselung von Dateien verwenden. Berechtigte Benutzer sind alle Benutzer ohne Rootberechtigung, die über Lese- und Schreibzugriff auf das gespeicherte Kennwort (Datei TSM.sth) verfügen, oder Benutzer, die das Kennwort kennen und interaktiv eingeben.

Übersicht über die Clientoptionsdatei

In einer Clientoptionsdatei können Sie Clientoptionen und Werte festlegen (angeben). Clientoptionen können auch auf dem Server in einer *Clientoptionsgruppe* definiert werden. In einer Clientoptionsgruppe auf dem Server festgelegte Clientoptionen setzen die in der Clientoptionsdatei definierten Clientoptionen außer Kraft.

Windows-BetriebssystemeAuf Windows-Systemen hat die Clientoptionsdatei standardmäßig den Namen dsm.opt.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeAuf AIX-, Linux-, Mac- und Solaris-Systemen hat die Clientoptionsdatei standardmäßig den Namen dsm.opt. Bei diesen Betriebssystemen enthalten zwei Dateien Optionen für den Client für Sichern/Archivieren:

- Die *Clientbenutzeroptionsdatei*. Der Standardname für diese Datei lautet dsm.opt. Häufig wird diese Datei kurz auch als *Clientoptionsdatei* bezeichnet.
- Die *Clientsystemoptionsdatei*. Der Standardname für diese Datei lautet dsm.sys. Die Clientsystemoptionsdatei ist eine editierbare Datei, die den Server und die Übertragungsmethode festlegt und die Konfiguration für die Sicherung, Archivierung, hierarchische Speicherverwaltung und Zeitplanung bereitstellt. Häufig wird diese Datei kurz auch als *Systemoptionsdatei* bezeichnet.

Sie können mehrere Clientoptionsdateien erstellen. Falls Ihre Clientoptionsdatei nicht dsm.opt heißt oder die Datei dsm.opt nicht im Standardverzeichnis vorhanden ist, teilen Sie dem Client für Sichern/Archivieren mit der Clientoption OPTFILE mit, aus welcher Datei die Optionen und Parameter beim Starten des Clients für Sichern/Archivieren gelesen werden sollen.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDer Name der Clientsystemoptionsdatei kann nicht geändert werden. Er muss dsm.sys lauten.

Mit einer Texteditoranwendung können Sie die Clientoptionsdatei direkt editieren. Zum Festlegen von Optionen können Sie auch die GUI des Clients für Sichern/Archivieren verwenden. Wählen Sie in der GUI die Optionen Editieren > Vorgaben aus und legen Sie die Clientoptionen im Profileditor fest. Optionen, die Sie im Profileditor festlegen, werden in der Clientoptionsdatei gespeichert. Im Profileditor können allerdings nicht alle Clientoptionen festgelegt werden.

Mac OS X-BetriebssystemeEinschränkung: Bei Mac OS X müssen die Clientbenutzeroptionsdatei und die Clientsystemoptionsdatei einfache, in Unicode (UTF-8) codierte Textdateien sein. Standardmäßig sichert TextEdit Dateien nicht als einfache Textdatei. Wählen Sie die Optionen Format > Make Plain Text aus, um die Dateien als einfache Textdateien zu speichern. Wählen Sie den Eintrag Unicode (UTF-8) in der Dropdown-Liste Plain Text Encoding aus. Fügen Sie beim Speichern der Datei nicht die Erweiterung .txt hinzu.

Sie können den Befehl query options verwenden, um alle oder einen Teil der Optionen und ihre aktuellen Einstellungen anzuzeigen. In diesem Befehl können Sie ein Argument eingeben, das eine Untergruppe von Optionen angibt. Standardmäßig werden alle Optionen angezeigt.

Einige Optionen bestehen nur aus dem Optionsnamen, z. B. verbose und quiet. Sie können den vollständigen Optionsnamen oder seine Abkürzung eingeben. Sie können beispielsweise die Option verbose wie folgt angeben:

```
verbose
ve
```

Richten Sie sich beim Hinzufügen von Optionen zu Optionsdateien nach den folgenden Regeln:

- Sie können Optionseinstellungen mit Anmerkungen versehen, indem Sie Kommentare zur Optionsdatei hinzufügen. Beginnen Sie jeden Kommentar mit einem Stern (*) als erstem Zeichen in der Zeile.
- Geben Sie Optionen nicht in einer Zeile an, die einen Kommentar enthält.
- Optional können Sie Optionen mit Leerzeichen oder Tabstopps einrücken, damit die in der Datei angegebenen Optionen und Werte besser zu erkennen sind.
- Geben Sie jede Option in einer separaten Zeile ein und geben Sie alle Parameter für eine Option in derselben Zeile ein. Dies ist in den folgenden Beispielen dargestellt:
  AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

  ```
  domain /home /mfg /planning /mrkting /mgmtdomain / /Volumes/fs2 /Volumes/fs2
  /Volumes/fs3 /Volumes/fs4
  ```

  Windows-Betriebssysteme

  ```
  domain="c: d:"
  domain="ALL-LOCAL -c: -systemstate"
  ```

- Um eine Option in dieser Datei zu definieren, geben Sie den Optionsnamen und eines oder mehrere Leerzeichen gefolgt vom Optionswert ein.
- Geben Sie eines oder mehrere Leerzeichen zwischen Parametern ein.
- Die Länge der Datei- und Pfadnamen in der Clientoptionsdatei darf die folgenden Grenzwerte nicht überschreiten:
  - AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeBei AIX, Mac OS und Solaris beträgt die maximale Länge für einen Dateinamen 255 Byte. Die maximale Länge der Kombination aus Dateiname und Pfadname ist 1024 Zeichen. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthalten könnte, variieren kann.
  - Linux-BetriebssystemeBei Linux beträgt die maximale Länge für einen Dateinamen 255 Byte. Die maximale Länge der Kombination aus Dateiname und Pfadname beträgt 4096 Byte. Dies entspricht dem vom Betriebssystem unterstützten Wert für PATH_MAX. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, aus denen ein Pfad- und Dateiname besteht, variieren kann. Die Begrenzung ist die Anzahl Byte in den Pfad- und Dateikomponenten, die einer gleichen Anzahl Zeichen entsprechen kann, aber nicht muss.
  - Windows-BetriebssystemeUnter Windows darf ein Dateiname 255 Byte nicht überschreiten. Verzeichnisnamen sind, einschließlich des Verzeichnisbegrenzers, ebenfalls auf 255 Byte begrenzt. Die maximale Länge der Kombination aus Dateiname und Pfadname beträgt 5192 Byte. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthalten könnte, variieren kann.

    Die Grenzwerte für Dateipfade und Dateinamen sind in Tabelle 1 aufgeführt.

  - Für Archivierungs- oder Abrufoperationen beträgt die maximale Länge, die Sie für eine Kombination aus Pfad- und Dateiname angeben können, 1024 Byte.

Windows-Betriebssysteme

Tabelle 1. Grenzwerte für Dateipfad und Namen

MBCS-Codierung	Längenbegrenzungen für Pfadnamen	Längenbegrenzungen für Dateinamen
1	5192 Byte	255 Byte
2	4092 Byte	127 Byte
3	2728 Byte	85 Byte

Windows-BetriebssystemeIn der Tabelle hat MBCS-Codierung die folgende Bedeutung:

Lateinischer Basiszeichensatz
: Standardzeichen in amerikanischem Englisch, Zahlen, Symbole und Steuerzeichen, die traditionell in 7-Bit-ASCII dargestellt werden, haben ein 1:1-Verhältnis von Byte zu Zeichen.

Erweiterter lateinischer Zeichensatz
: Lateinische Zeichen mit Tilden, Gravis- oder Akutakzenten usw. sowie griechische, koptische, kyrillische, armenische, hebräische und arabische Zeichen haben normalerweise ein 2:1-Verhältnis von Byte zu Zeichen.

Chinesisch, Japanisch, Koreanisch, Vietnamesisch
: Diese Zeichen und andere ostasiatische Sprachzeichen haben normalerweise ein 3:1-Verhältnis von Byte zu Zeichen.

Windows-BetriebssystemeWenn Sie die Clientoptionsdatei aktualisieren, während eine Sitzung aktiv ist, müssen Sie die Sitzung erneut starten, damit die Änderungen in Kraft treten. Wenn Sie den Setup-Assistenten der Client-GUI verwenden, um Änderungen vorzunehmen, werden die Änderungen sofort wirksam. Wenn Sie nicht den Clientakzeptor zur Verwaltung des Schedulers verwenden, müssen Sie auch den Scheduler erneut starten.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWenn Sie die Clientbenutzeroptionsdatei aktualisieren, während eine Sitzung aktiv ist, müssen Sie die Sitzung erneut starten, damit die Änderungen in Kraft treten.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme
  Clientsystemoptionsdatei erstellen und ändern
  Die Clientsystemoptionsdatei ist eine editierbare Datei, die den Server und die Übertragungsmethode festlegt und die Konfiguration für die Sicherung, Archivierung, hierarchische Speicherverwaltung und Zeitplanung bereitstellt.
- Windows-BetriebssystemeClientoptionsdatei erstellen und ändern
  Die Clientoptionsdatei ist eine editierbare Textdatei, die Konfigurationsdaten für den Client für Sichern/Archivieren enthält.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme
  Standardclientbenutzeroptionsdatei erstellen
  In einer Clientbenutzeroptionsdatei werden die Verarbeitungsoptionen des Clients für Sichern/Archivieren gespeichert. Bei der Installation des Clients für Sichern/Archivieren speichert das Installationsprogramm für die Sicherung/Archivierung ein Beispiel für die Clientbenutzeroptionsdatei auf der Platte. Ein Systemadministrator oder Root kann diese Datei editieren, um eine Standardclientoptionsdatei zu erstellen, und die Datei den Workstationbenutzern zugänglich machen, die den Client für Sichern/Archivieren verwenden. Einzelne Benutzer können eigene Clientoptionsdateien erstellen und verwenden.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAngepasste Clientbenutzeroptionsdatei erstellen
  Wenn Sie andere Optionen als die in der Standardclientbenutzeroptionsdatei (dsm.opt) angegebenen Optionen verwenden wollen, können Sie eine eigene Clientbenutzeroptionsdatei erstellen.
- Windows-BetriebssystemeOptionsdatei in gemeinsam genutztem Verzeichnis erstellen
  Der IBM Spectrum Protect-Serveradministrator kann Clientoptionsdateien in einem gemeinsam genutzten Verzeichnis generieren.
- Windows-BetriebssystemeMehrere Clientoptionsdateien erstellen
  Sie können mehrere Clientoptionsdateien erstellen, wenn Sie mit mehreren Servern arbeiten müssen oder falls für einige Sicherungs- und Archivierungstasks andere Parametergruppen verwendet werden sollen.

Zugehörige Verweise:
Optfile
Query Options
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Clientsystemoptionsdatei erstellen und ändern

Die Clientsystemoptionsdatei ist eine editierbare Datei, die den Server und die Übertragungsmethode festlegt und die Konfiguration für die Sicherung, Archivierung, hierarchische Speicherverwaltung und Zeitplanung bereitstellt.

Informationen zu diesem Vorgang

Die Erstellung und Änderung der Clientsystemoptionsdatei (dsm.sys) ist eine erforderliche Task.

Die GUI des Clients für Sichern/Archivieren stellt einen Konfigurationsassistenten bereit, mit dem Sie Basiskonfigurationsdateien erstellen und die Verbindung zum IBM Spectrum Protect-Server testen können. Der Konfigurationsassistent wird automatisch gestartet, wenn die Konfigurationsdateien beim Starten der GUI nicht gefunden werden. Wenn Sie die Konfigurationsdateien zu einem Zeitpunkt nach der Erstellung ändern wollen, klicken Sie auf Setup-Assistent im Menü Dienstprogramme der GUI.

Wenn Sie den Konfigurationsassistenten nicht verwenden, können Sie die Clientoptionsdatei manuell erstellen und ändern.

Für Mac OS X: Kopieren Sie die Datei dsm.sys.smp an einer der folgenden Positionen in dsm.sys. Die Standardpositionen sind in der Reihenfolge aufgelistet, in der sie durchsucht werden.

1. Eine Position, die durch die Umgebungsvariable DSM_DIR angegeben wird
2. `/Library/Application Support/tivoli/tsm/client/ba/bin/`
3. `/Library/Preferences/Tivoli Storage Manager/`

   Der Client verwendet die erste Optionsdatei, die gefunden wird. Sie müssen für diese Datei den Namen dsm.sys verwenden. Die Datei dsm.sys wird vom Systemadministrator gesteuert.

Bei Oracle Solaris-Systemen ist das Kopieren der Datei dsm.sys.smp in dsm.sys nicht erforderlich. Die Clientoptionsdateien (dsm.opt und dsm.sys) werden automatisch im Verzeichnis /usr/bin erstellt, wenn sie noch nicht vorhanden sind, und bei der Installation des Clients mit dem Clientinstallationsverzeichnis verbunden. Beachten Sie, dass die Dateien beim Deinstallieren des Clients nicht entfernt werden und Sie Ihre Einstellungen daher bei einem Upgrade oder einer Neuinstallation des Clients wiederverwenden können.

Kopieren Sie bei den anderen Plattformen die Datei dsm.sys.smp als Rootbenutzer in dsm.sys und editieren Sie anschließend diese Datei, um Ihre Einstellungen zu konfigurieren. Der Client sucht nach der Datei dsm.sys in dem Verzeichnis, das durch die Umgebungsvariable DSM_DIR angegeben wird (sofern festgelegt und exportiert). Anschließend wird im Installationsverzeichnis nach der Datei gesucht.

Wichtig: Wenn Sie eine erneute Installation ausführen und die vorhandene Datei dsm.sys unverändert beibehalten wollen, kopieren Sie die Datei dsm.sys.smp nicht in dsm.sys.

Verwenden Sie die Datei dsm.sys, um einen oder mehrere Server anzugeben, die für Services kontaktiert werden sollen, sowie um die Übertragungsoptionen für jeden Server anzugeben. Diese Datei kann außerdem Berechtigungsoptionen, Verarbeitungsoptionen für Sichern und Archivieren sowie Planungsoptionen enthalten.

Editieren Sie dsm.sys und fügen Sie den Server oder die Server hinzu, zu dem oder denen eine Verbindung hergestellt werden soll. Das folgende Beispiel zeigt eine Zeilengruppe einer Clientsystemoptionsdatei, die die erforderlichen Optionen für einen Server enthält, zu dem die Benutzer eine Verbindung herstellen sollen. Sie können Optionen für mehrere Server angeben:

```
Servername              server_a
COMMMethod              TCPip
TCPPort                 1500
TCPServeraddress        node.domain.company.com
```

Wichtig: Wenn Sie den Web-Client verwenden wollen, müssen Sie auch die Option passwordaccess=generate angeben und sich mit dem Client anmelden, um das Kennwort zu speichern.

Standardmäßig kontaktiert Ihr Clientknoten den ersten Server, der in der Datei dsm.sys angegeben ist. Sie können einen anderen Server angeben, zu dem eine Verbindung hergestellt werden soll, indem Sie die Option servername in Ihrer Clientbenutzeroptionsdatei (dsm.opt) angeben oder mit einem Befehl eingeben.

Sie können auch einen Standardserver und einen Umlagerungsserver (falls auf Ihrer Workstation der HSM-Client installiert ist) in Ihrer Datei dsm.sys angeben.

Die Datei dsm.sys kann außerdem die folgenden Optionskategorien enthalten:

- Optionen für die Datenübertragung
- Verarbeitungsoptionen für Sichern und Archivieren
- Verarbeitungsoptionen für Zurückschreiben und Abrufen
- Planungsoptionen
- Berechtigungsoptionen
- Fehlerverarbeitungsoptionen
- Transaktionsverarbeitungsoptionen
- Web-Client-Optionen

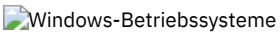
Sie können Ihre Datei dsm.sys über eine der folgenden Methoden ändern:

- Wählen Sie im Hauptfenster der Java™-GUI des Clients die Optionen Editieren > Clientvorgaben aus.
- Verwenden Sie Ihren bevorzugten Texteditor.

Wichtig: Für Mac OS X: Die Systemoptionsdatei muss eine einfache in Unicode (UTF-8) codierte Textdatei sein. Standardmäßig sichert TextEdit Dateien nicht als unverschlüsselte Textdatei. Wählen Sie Format > Make PlainText (Als einfachen Text speichern) aus, um die Benutzeroptionsdatei als unverschlüsselte Textdatei zu speichern. Legen Sie für Plain Text Encoding (Codierung für unverschlüsselten Text) den Wert `Unicode (UTF-8)` fest. Fügen Sie nicht die Erweiterung .txt hinzu.

Wenn Sie die Datei dsm.sys aktualisieren, während der Client aktiv ist, müssen Sie den Prozess erneut starten, um die Änderungen in Kraft zu setzen.

Zugehörige Konzepte:
Übersicht über die Clientoptionsdatei

Verarbeitungsoptionen
Zugehörige Verweise:
Defaultserver
Passwordaccess


Clientoptionsdatei erstellen und ändern

Die Clientoptionsdatei ist eine editierbare Textdatei, die Konfigurationsdaten für den Client für Sichern/Archivieren enthält.

Informationen zu diesem Vorgang

Beim ersten Start der grafischen Benutzerschnittstelle (GUI) des Windows-Clients für Sichern/Archivieren sucht das Installationsprogramm eine vorhandene Clientoptionsdatei mit dem Namen dsm.opt. Wenn diese Datei nicht gefunden wird, startet ein Konfigurationsassistent für Clientoptionsdateien und Sie werden zur Angabe von Anfangswerten für die Clientkonfiguration aufgefordert. Am Ende der Assistentenausführung werden die von Ihnen angegebenen Informationen in der Datei dsm.opt gespeichert. Die Datei dsm.opt wird standardmäßig in C:\Programme\Tivoli\TSM\baclient gespeichert.

Für die Kommunikation mit dem Server muss die Optionsdatei die folgenden Informationen enthalten:

- Hostname oder IP-Adresse des IBM Spectrum Protect-Servers.
- Portnummer, an der der Server die Clientkommunikation empfängt. Der Konfigurationsassistent für die Clientoptionsdatei konfiguriert eine Standardportnummer. Sie müssen diese Standardportnummer nur ändern, wenn auf Ihrem Server ein anderer Empfangsport konfiguriert ist.
- Name Ihres Clientknotens. Mit dem Knotennamen wird Ihr Clientknoten eindeutig identifiziert. Standardeinstellung für den Knotennamen ist der kurze Hostname des Computers, auf dem der Client installiert ist.

Weitere Clientoptionen können nach Bedarf angegeben werden.
Anmerkung: Clientoptionen können auch auf dem Server in einer *Clientoptionsgruppe* definiert werden. In einer Clientoptionsgruppe auf dem Server definierte Clientoptionen überschreiben die in der Clientoptionsdatei definierten Clientoptionen.

Eine Beispieloptionsdatei wird bei der Installation des Clients für Sichern/Archivieren auf Ihre Platte kopiert. Diese Datei heißtdsm.smp. Die Datei dsm.smp wird standardmäßig in C:\Programme\Tivoli\TSM\config\ kopiert. Sie können den Inhalt dieser Datei anzeigen, um Beispiele verschiedener Optionen zu sehen und wie diese angegeben werden. Die Datei enthält auch Kommentare, die Syntaxkonventionen für Einschluss- und Ausschlusslisten sowie die Verwendung von Platzhalterzeichen erläutern. Sie können diese Datei auch als Vorlage für Ihre Clientoptionsdatei verwenden. Hierfür bearbeiten Sie die Datei und speichern sie unter dem Namen dsm.opt im Verzeichnis C:\Programme\Tivoli\TSM\baclient.

Nach der Erstellung der Anfangsclientoptionsdatei können Sie die Clientoptionen durch Hinzufügen oder Ändern nach Bedarf anpassen. Für die Änderung der Datei dsm.opt haben Sie folgende Möglichkeiten:

- Ausführung des Konfigurationssetupassistenten für die Clientoptionsdatei
- Verwendung des Profileditors des Clients
- Bearbeitung der Datei dsm.opt mit einem Texteditor, z. B. Notepad

Gehen Sie wie folgt vor, um die Clientoptionen zu ändern:

Vorgehensweise

1. Wählen Sie eine Methode für die Änderung der Datei aus.

Option	Bezeichnung
Setup-Assistent	a. Klicken Sie auf Start > Alle Programme > IBM Spectrum Protect > GUI für Sichern/Archivieren. b. Wählen Sie Dienstprogramme > Setup-Assistent > Hilfe zum Konfigurieren der Clientoptionsdatei aus. Für die Assistentenanzeigen stehen Text auf dem Bildschirm und Onlinehilfe als Anleitung zur Verfügung. Die Auswahlmöglichkeiten in diesem Konfigurationsassistenten für die Clientoptionsdatei sind begrenzt, es werden nur die grundlegendsten Optionen konfiguriert.
Profileditor	a. Klicken Sie auf Start > Alle Programme > IBM Spectrum Protect > GUI für Sichern/Archivieren. b. Wählen Sie Editieren > Clientvorgaben aus. Wählen Sie die Registerkarten im Profileditor aus, um Clientoptionen zu definieren. Geben Sie die Optionen in den Dialogfeldern, Dropdown-Listen und anderen Steuerelementen an. Onlinehilfe steht zur Verfügung. Wenn Sie auf das Fragezeichen (?) klicken, werden die Hilfethemen der Onlinehilfe für die gerade bearbeitete Registerkarte angezeigt. Im Profileditor können Sie mehr Optionen definieren als im Setup-Assistenten.
Datei dsm.opt bearbeiten	a. Die Datei dsm.opt bearbeiten Sie mit einem einfachen Texteditor. Die einzelnen Optionen werden in der Dokumentation in Clientoptionsreferenz ausführlich beschrieben. Dies ist die vielseitigste Möglichkeit zur Definition von Clientoptionen, weil im Konfigurationsassistenten für die Clientoptionsdatei und im Profileditor nicht alle Optionen definiert werden können. b. Soll eine Einstellung auf Kommentar gesetzt werden, fügen Sie einen Stern (*) als erstes Zeichen in der entsprechenden Zeile ein. Wenn Sie den Stern entfernen, wird die entsprechende Option aktiviert.

2. Speichern Sie die Änderungen.

a. Die im Konfigurationsassistenten für die Clientoptionsdatei und im Profileditor vorgenommenen Änderungen erkennt der Client bei Beendigung des Assistenten bzw. beim Verlassen des Profileditors.
b. Wenn Sie die Clientoptionsdatei mit einem Texteditor bearbeiten, während der Client aktiv ist, müssen Sie die Datei speichern und den Client erneut starten, damit die Änderungen erkannt werden.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Standardclientbenutzeroptionsdatei erstellen

In einer Clientbenutzeroptionsdatei werden die Verarbeitungsoptionen des Clients für Sichern/Archivieren gespeichert. Bei der Installation des Clients für Sichern/Archivieren speichert das Installationsprogramm für die Sicherung/Archivierung ein Beispiel für die Clientbenutzeroptionsdatei auf der Platte. Ein Systemadministrator oder Root kann diese Datei editieren, um eine Standardclientoptionsdatei zu erstellen, und die Datei den Workstationbenutzern zugänglich machen, die den Client für Sichern/Archivieren verwenden. Einzelne Benutzer können eigene Clientoptionsdateien erstellen und verwenden.

Vorbereitende Schritte

Sie müssen ein Root oder ein Systemadministrator sein, um diese Prozedur ausführen zu können.

Informationen zu diesem Vorgang

Die Erstellung einer Standardclientbenutzeroptionsdatei ist eine optionale Task.

Die Clientbenutzeroptionsdatei heißt standardmäßig dsm.opt und enthält die folgenden Typen von Clientoptionen:

- Verarbeitungsoptionen für Sichern und Archivieren
- Verarbeitungsoptionen für Zurückschreiben und Abrufen
- Planungsoptionen
- Formatoptionen
- Befehlsverarbeitungsoptionen
- Berechtigungsoptionen
- Fehlerverarbeitungsoptionen
- Transaktionsverarbeitungsoptionen
- Web-Client-Optionen

Bei Mac-Clients speichert das Clientinstallationsprogramm ein Beispiel für die Clientbenutzeroptionsdatei namens dsm.opt.smp an der Position /Libraries/Preferences/Tivoli Storage Manager/. In diesem Verzeichnis speichert das Installationsprogramm auch ein Beispiel für die Clientsystemoptionsdatei (dsm.sys.smp).

Bei AIX- und Linux-Clients speichert das Clientinstallationsprogramm ein Beispiel für die Clientbenutzeroptionsdatei mit dem Namen dsm.opt.smp im standardmäßigen Clientinstallationsverzeichnis. In diesem Verzeichnis speichert das Installationsprogramm auch ein Beispiel für die Clientsystemoptionsdatei (dsm.sys.smp).

Bei Oracle Solaris-Clients speichert das Installationsprogramm eine anfängliche Clientbenutzeroptionsdatei namens dsm.opt im Verzeichnis /usr/bin. In diesem Verzeichnis speichert das Installationsprogramm auch ein Beispiel für die Clientsystemoptionsdatei (dsm.sys).

Bei allen Clientbetriebssystemen werden Sie in der folgenden Prozedur angewiesen, das Beispiel für die Clientbenutzeroptionsdatei zu editieren und unter dem Standardnamen dsm.opt zu speichern. Sie können die Datei auf Wunsch auch unter einem anderen Namen oder Pfad speichern. Falls Sie jedoch den Dateinamen ändern oder die Datei aus dem Standardinstallationsverzeichnis versetzen, müssen Sie den Pfad und den Namen der Clientbenutzeroptionsdatei mit einem der folgenden Verfahren angeben:

- Legen Sie die Umgebungsvariable DSM_CONFIG so fest, dass sie den Pfad und Dateinamen der Clientbenutzeroptionsdatei (dsm.opt) angibt. Legen Sie die Umgebungsvariable DSM_DIR so fest, dass sie den Pfad und Dateinamen der Clientsystemptionsdatei (dsm.sys) angibt. Weitere Informationen zu den Umgebungsvariablen finden Sie in Umgebungsvariablen für die Verarbeitung definieren.
- Geben Sie mit der Option optfile des Clients für Sichern/Archivieren den Pfad und Dateinamen der Clientbenutzeroptionsdatei an. Anmerkung: Alle Knotenbenutzer müssen Lesezugriff auf die Plattenposition besitzen, an der Sie die Clientbenutzeroptionsdatei speichern.

Vorgehensweise

1. Wechseln Sie in das Verzeichnis, in dem sich das Beispiel für die Clientbenutzeroptionsdatei befindet.
2. Kopieren Sie die Datei nach dsm.opt.
3. Fügen Sie Optionen für Ihren Knoten zur Datei dsm.opt hinzu. Verwenden Sie zum Festlegen der Clientbenutzeroptionen eines der folgenden Verfahren:
    - Editieren Sie die Datei dsm.opt in einem Texteditor und fügen Sie die für den Knoten benötigten Optionen zur Datei hinzu. Anmerkung: Unter Mac OS X muss die Datei dsm.opt als einfache Textdatei gespeichert und Unicode (UTF-8) als Schema für die Codeumsetzung verwendet werden. Standardmäßig sichert TextEdit Dateien nicht als einfache Textdatei. Um die Datei dsm.opt in TextEdit zu speichern, wählen Sie die Optionen Format > Make Plain Text aus. Wählen Sie in der Dropdown-Liste Plain Text Encoding den Eintrag Unicode (UTF-8) aus. Fügen Sie nicht die Erweiterung .txt zum Dateinamen hinzu.

- Legen Sie Clientoptionen mit dem Profileditor fest. Wählen Sie in der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren die Optionen Editieren > Clientvorgaben und dann die Optionen aus, die Sie konfigurieren wollen. Der Profileditor aktualisiert die Clientkonfigurationsdateien dsm.opt und dsm.sys, falls Sie Optionen hinzufügen, ändern oder entfernen. Wenn Sie die Datei dsm.opt aktualisieren, während der Client für Sichern/Archivieren ausgeführt wird, müssen Sie den Client für Sichern/Archivieren erneut starten, damit die Aktualisierungen erkannt werden.

  Der Profileditor ermittelt anhand der Umgebungsvariablen DSM_DIR die Clientsystemoptionsdatei (dsm.sys) sowie anhand der Umgebungsvariablen DSM_CONFIG die Clientbenutzeroptionsdatei (dsm.opt). Falls sich die Datei dsm.opt an einer anderen als der Standardposition befinden soll, legen Sie die Umgebungsvariable DSM_CONFIG fest, bevor Sie den Client für Sichern/Archivieren starten, und verwenden Sie anschließend den Profileditor, um die Optionen festzulegen. Der Profileditor fragt den Server nach Optionen auf dem Server ab, kann aber die Serveroptionsdatei nicht ändern.

Zugehörige Konzepte:
Verarbeitungsoptionen
Umgebungsvariablen für die Verarbeitung definieren
Zugehörige Tasks:
Clientsystemoptionsdatei erstellen und ändern
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Angepasste Clientbenutzeroptionsdatei erstellen

Wenn Sie andere Optionen als die in der Standardclientbenutzeroptionsdatei (dsm.opt) angegebenen Optionen verwenden wollen, können Sie eine eigene Clientbenutzeroptionsdatei erstellen.

Informationen zu diesem Vorgang

Sie können alle Optionen definieren, die in der Standardbenutzeroptionsdatei angegeben werden können. Die Erstellung einer angepassten Clientbenutzeroptionsdatei (dsm.opt) ist eine optionale Task. Verwenden Sie die folgende Methode, um eine Clientbenutzeroptionsdatei zu erstellen oder zu ändern:

Vorgehensweise

1. Fragen Sie den IBM Spectrum Protect-Administrator für Ihre Workstation nach der Position der Muster-Clientbenutzeroptionsdatei dsm.opt.smp, nach der TCP/IP-Adresse des Sicherungsservers, zu dem Sie eine Verbindung herstellen, und nach dem Anschluss, an dem er empfangsbereit ist.
2. Kopieren Sie dsm.opt.smp in Ihr Ausgangsverzeichnis als dsm.opt oder mit einem neuen Dateinamen Ihrer Wahl. Sie können Ihre Clientbenutzeroptionsdatei in jedem Verzeichnis speichern, auf das Sie Schreibzugriff haben.
3. Definieren Sie die Umgebungsvariable DSM_CONFIG so, dass sie auf Ihre neue Clientbenutzeroptionsdatei zeigt.
4. Editieren Sie die Datei dsm.opt gemäß Ihrem System oder verwenden Sie den Profileditor, indem Sie Editieren > Clientvorgaben in der GUI des Clients für Sichern/Archivieren auswählen.

Ergebnisse

Nachdem Sie eine Optionsdatei erstellt haben, können Sie sie mit den folgenden Schritten über die grafische Benutzerschnittstelle editieren:

1. Öffnen Sie das Menü Editieren und wählen Sie Clientvorgaben aus.
2. Nehmen Sie die erforderlichen Änderungen vor und klicken Sie anschließend auf OK, um diese Änderungen zu speichern.

Mac OS X-BetriebssystemeWichtig: Für Mac OS X: Die Systemoptionsdatei muss eine einfache in Unicode (UTF-8) codierte Textdatei sein. Standardmäßig sichert TextEdit Dateien nicht als unverschlüsselte Textdatei. Wählen Sie Format > Make PlainText (Als einfachen Text speichern) aus, um die Benutzeroptionsdatei als unverschlüsselte Textdatei zu speichern. Legen Sie die Auswahl in der Dropdown-Liste Plain Text Encoding (Codierung für unverschlüsselten Text) mit `Unicode (UTF-8)` fest. Fügen Sie nicht die Erweiterung .txt hinzu.
Zugehörige Konzepte:
Umgebungsvariablen
Übersicht über die Clientoptionsdatei
Windows-Betriebssysteme

Optionsdatei in gemeinsam genutztem Verzeichnis erstellen

Der IBM Spectrum Protect-Serveradministrator kann Clientoptionsdateien in einem gemeinsam genutzten Verzeichnis generieren.

Windows-Clients können auf das gemeinsam genutzte Verzeichnis zugreifen und die darin gespeicherten Dateien verwenden, um eine eigene Clientoptionsdatei zu erstellen.

Die Erstellung einer Optionsdatei in einem gemeinsam genutzten Verzeichnis ist eine optionale Task für den Root oder berechtigten Benutzer.

Windows-Betriebssysteme

Mehrere Clientoptionsdateien erstellen

Sie können mehrere Clientoptionsdateien erstellen, wenn Sie mit mehreren Servern arbeiten müssen oder falls für einige Sicherungs- und Archivierungstasks andere Parametergruppen verwendet werden sollen.

Informationen zu diesem Vorgang

Angenommen, die Dateien sollen auf einem Server (`Server a`) gesichert und auf einem anderen Server (`server b`) archiviert werden. Statt die Datei dsm.opt jedesmal zu editieren, wenn auf einen anderen Server zugegriffen werden soll, können Sie zwei Optionsdateien erstellen. Erstellen Sie beispielsweise die Optionsdatei a.opt für `Server a` und b.opt für `Server b`.

Vorgehensweise

Verwenden Sie eine der folgenden Methoden, um eine andere Clientoptionsdatei anzugeben oder zu verwenden:

- Ersetzen Sie die Datei dsm.opt durch die entsprechende Optionsdatei, bevor Sie den Client für Sichern/Archivieren starten.
  Geben Sie beispielsweise die folgenden Befehle aus, um die Datei a.opt in dsm.opt zu kopieren, und starten Sie anschließend die grafische Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren:

  ```
  copy a.opt dsm.opt
  dsm
  ```

- Starten Sie den Client für Sichern/Archivieren über die Befehlszeile und geben Sie die Optionsdatei, die Sie verwenden wollen, mit der Option optfile an.
  Zum Beispiel:

  ```
  dsm -optfile=b.opt
  ```

- Definieren Sie die Umgebungsvariable DSM_CONFIG, um die zu verwendende Optionsdatei anzugeben, bevor Sie eine Sitzung des Clients für Sichern/Archivieren starten.
  Zum Beispiel:

  ```
  SET DSM_CONFIG=C:\Programme\Tivoli\TSM\baclient\b.opt
  ```

Nächste Schritte

Wenn Sie den Client für Sichern/Archivieren über die Befehlszeile ausführen, müssen die Umgebungsvariablen DSM_DIR und DSM_LOG möglicherweise außerdem wie folgt konfiguriert werden:

- Definieren Sie die Umgebungsvariable DSM_DIR so, dass sie auf das Verzeichnis zeigt, das alle übrigen ausführbaren Dateien enthält:

  ```
  SET DSM_DIR=C:\Programme\Tivoli\TSM\baclient
  ```

- Definieren Sie die Umgebungsvariable DSM_LOG so, dass sie auf das Verzeichnis zeigt, in dem sich die Datei `dsmerror.log` befindet:

  ```
  SET DSM_LOG=C:\Programme\Tivoli\TSM\baclient
  ```

Anmerkung: Der Verzeichnispfad, in dem sich die ausführbaren Clientdateien befinden, muss in der Umgebungsvariable PATH angegeben werden. Andernfalls ist ein vollständig qualifizierter Pfad anzugeben.
 Windows-Betriebssysteme

Umgebungsvariablen

Im Allgemeinen ist die Definition von Umgebungsvariablen eine optionale Task. Wenn Sie sie definieren, erleichtert dies die Verwendung der Befehlszeile.

Informationen zu diesem Vorgang

Die Definition der Umgebungsvariablen ist jedoch erforderlich, wenn Sie das Programm in einer der folgenden Umgebungen ausführen müssen:

- Der Client für Sichern/Archivieren soll von einem anderen Verzeichnis als dem Installationsverzeichnis des Clients für Sichern/Archivieren aufgerufen werden.
- Es soll eine andere Optionsdatei für den Client für Sichern/Archivieren und/oder den Verwaltungsclient angegeben werden.

Anmerkung: Sie können auch eine andere Clientoptionsdatei für den Befehlszeilenclient (nicht den Verwaltungsclient) angeben, wenn Sie die Option ***optfile*** verwenden.
Vier Umgebungsvariablen müssen definiert werden:

PATH
: Dies ist der Standardsuchpfad, den das Betriebssystem zum Suchen von ausführbaren Dateien verwendet. Geben Sie in dieser Variable den vollständig qualifizierten Pfad der Clientinstallationsverzeichnisse an.

DSM_CONFIG
: Geben Sie in dieser Umgebungsvariablen den vollständig qualifizierten Pfad und Dateinamen der Clientoptionsdatei an.

DSM_DIR
: Geben Sie in dieser Umgebungsvariablen das Verzeichnis an, in dem sich die Clientnachrichtendatei dsc*.txt befindet.

DSM_LOG
: Geben Sie in dieser Umgebungsvariablen das Verzeichnis an, in dem sich die Protokolldateien befinden sollen.

Stellen Sie sicher, dass die Umgebungsvariablen folgenden Richtlinien entsprechen:

- Geben Sie in der aktuellen Umgebungsvariable PATH das Verzeichnis an, in dem sich die ausführbaren Dateien (z. B. dsm.exe) befinden. Wenn Sie das Standardinstallationsverzeichnis akzeptiert und Laufwerk C: verwendet haben, können Sie Folgendes bei einer Eingabeaufforderung eingeben:

  ```
  SET PATH=C:\Programme\Tivoli\TSM\baclient
  ```

- Geben Sie den vollständigen Pfadnamen Ihrer Clientoptionsdatei (dsm.opt) in der Umgebungsvariable DSM_CONFIG an:

  ```
  SET DSM_CONFIG=C:\Programme\Tivoli\TSM\baclient\dsm.opt
  ```

- Definieren Sie die Umgebungsvariable DSM_DIR so, dass sie auf das Verzeichnis verweist, in dem sich die Clientnachrichtendatei dsc*.txt befindet:

  ```
  SET DSM_DIR=C:\Programme\Tivoli\TSM\baclient
  ```

Zugehörige Verweise:
Optfile
AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme

Umgebungsvariablen

Im Allgemeinen ist die Definition von Umgebungsvariablen eine optionale Task. Wenn Sie diese Variablen definieren, erleichtert dies die Verwendung der Befehlszeile.

- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme
  Sprachumgebungsvariablen definieren
  Der Client für Sichern/Archivieren erkennt automatisch die Sprache der Systemländereinstellung und wird dieser Sprache angezeigt.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeUmgebungsvariablen für die Verarbeitung definieren
  Unter bestimmten Umständen ist es erforderlich, Umgebungsvariablen zu definieren, um sicherzustellen, dass IBM Spectrum Protect-Anwendungen die Dateien finden können, die für die Ausführung von Clientoperationen benötigt werden, und dass Anwendungen Protokolldateien erstellen können, in denen Ereignisse und Fehler aufgezeichnet werden, die während Clientoperationen auftreten.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeBourne- und Korn-Shell-Variablen definieren
  Geben Sie die Umgebungsvariablen in die Datei `.profile` (Korn-Shell) oder in die Datei `.bash_profile` (Bourne-Shell) im Verzeichnis `$HOME` ein.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeC-Shell-Variablen definieren
  Für die C-Shell fügen Sie die Variablen DSM_CONFIG, DSM_LOG und DSM_DIR der Datei `.cshrc` im Verzeichnis `$HOME` hinzu.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeAPI-Umgebungsvariablen definieren
  Wenn Sie die IBM Spectrum Protect-API installiert haben, definieren Sie die folgenden Umgebungsvariablen.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Sprachumgebungsvariablen definieren

Der Client für Sichern/Archivieren erkennt automatisch die Sprache der Systemländereinstellung und wird dieser Sprache angezeigt.

Beispielsweise zeigt ein französisches Betriebssystem den Client für Sichern/Archivieren standardmäßig in Französisch an. Wenn der Client für Sichern/Archivieren den französischen Nachrichtenkatalog nicht laden kann, wird standardmäßig amerikanisches Englisch verwendet. Wenn der Client beispielsweise mit einer nicht unterstützten Kombination aus Sprache und Ländereinstellung wie Französisch/Kanada oder Spanisch/Mexiko ausgeführt wird, wird für den Client standardmäßig amerikanisches Englisch angenommen.

Sie können die Umgebungsvariable LANG verwenden, um die Sprache für die UNIX- und Linux-Clients anzugeben.

Anmerkung: Die Ländereinstellung des Betriebssystems, der Zeichensatz der Datenstation und die Zeichensatzcodierung für Dateinamen müssen übereinstimmen, damit Dateinamen ordnungsgemäß angezeigt oder eingegeben werden können.
Soll die Umgebungsvariable LANG für Französisch definiert werden, geben Sie die folgende Anweisung ein:

```
export LANG=fr_FR
```

Anmerkung:

- Diese Task gilt nicht für Mac OS X.
- Wenn die IBM Spectrum Protect-Hilfemenüs in der Sprache der aktuellen Ländereinstellung angezeigt werden sollen, muss sichergestellt werden, dass in der Umgebungsvariablen NLSPATH in der Datei `/etc/profile` folgende Pfadangabe enthalten ist:

  ```
  NLSPATH=/usr/dt/lib/nls/msg/%L/%N.cat:$NLSPATH
  export NLSPATH
  ```

Wenn die Ländereinstellung des Clients für Sichern/Archivieren mit der Zeichencodierung der Dateinamen übereinstimmt, werden alle diese Dateien korrekt gesichert oder zurückgeschrieben. Wenn Sie mit einem beliebigen Einzelbytezeichensatz (SBCS) arbeiten, sind alle Dateinamen gültig und werden vom Client für Sichern/Archivieren gesichert oder zurückgeschrieben.

Wenn Sie mit einer DBCS- oder UTF-8-Ländereinstellung arbeiten, können Dateinamen mit Zeichen, die in der DBCS- oder UTF-8-Ländereinstellung nicht gültig sind, nicht in der Befehlszeile des Clients für Sichern/Archivieren eingegeben werden. Die Dateien werden möglicherweise übersprungen, wenn Sie eine Sicherung mit Platzhalterzeichen ("*") für Dateinamenspezifikationen ausführen. Werden Dateien übersprungen, wird eine Fehlernachricht wie im folgenden Beispiel ausgegeben:

```
ANS4042E Objektname '/testData/en_US_files/file3?'
enthält ein oder mehrere unbekannte Zeichen und ist nicht gültig.
```

Wurden Ihre Verzeichnisse und Dateien mit verschiedenen Ländereinstellungen erstellt, führen Sie geplante Sicherungen mit einer Ländereinstellung für Einzelbytezeichensatz aus. Damit ist sichergestellt, dass Dateien nicht übersprungen werden, weil der Dateiname Zeichen enthält, die nicht in der aktuellen Ländereinstellung definiert sind. Die Zurückschreibung von Dateien führen Sie in der Ländereinstellung durch, die der Codierung der Dateinamen entspricht.

Beispiel: Aus japanischen Zeichen bestehende Dateinamen enthalten möglicherweise ungültige Mehrbytezeichen, wenn sie in einer chinesischen Ländereinstellung angezeigt werden. Diese Dateien werden weder gesichert noch in der grafischen Benutzerschnittstelle angezeigt. Werden solche Dateien während der Sicherung festgestellt, werden die übersprungenen Dateien in der Datei dsmerror.log aufgelistet.

Tipp: Wenn Sie den Planungsmodus des Clients für Sichern/Archivieren für die Sicherung eines gesamten Systems verwenden, setzen Sie die Umgebungsvariable LANG auf `en_US` (oder eine andere SBCS-Sprache), um übersprungene Dateien zu vermeiden.
 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Umgebungsvariablen für die Verarbeitung definieren

Unter bestimmten Umständen ist es erforderlich, Umgebungsvariablen zu definieren, um sicherzustellen, dass IBM Spectrum Protect-Anwendungen die Dateien finden können, die für die Ausführung von Clientoperationen benötigt werden, und dass Anwendungen Protokolldateien erstellen können, in denen Ereignisse und Fehler aufgezeichnet werden, die während Clientoperationen auftreten.

Sie müssen die Umgebungsvariablen in jeder der folgenden Situationen definieren:

- Der Client für Sichern/Archivieren soll von einem anderen Verzeichnis als dem Installationsverzeichnis des Clients für Sichern/Archivieren aufgerufen werden.
- Es soll eine andere Optionsdatei für den Client für Sichern/Archivieren und/oder den Verwaltungsclient angegeben werden.
- Protokolldateien sollen nicht im Standardinstallationsverzeichnis gespeichert werden.

Tipp: Sie können auch eine andere Clientoptionsdatei für den Befehlszeilenclient (nicht den Verwaltungsclient) angeben, wenn Sie die Option optfile verwenden.

Es können vier Umgebungsvariablen definiert werden, die sich auf die Verarbeitung durch den Client für Sichern/Archivieren auswirken:

PATH
: Schließt das Verzeichnis ein, in dem sich die ausführbare Datei für die ausführbaren Dateien des Clients (dsmc, dsmadmc, dsmj) befindet.

DSM_DIR
: Gibt das Verzeichnis an, in dem sich die ausführbare Datei für die ausführbaren Dateien des Clients (`dsmc`, dsmadmc, dsmj), die Ressourcendateien und die Datei dsm.sys befinden. Das Stammverzeichnis (/) kann für DSM_DIR nicht angegeben werden.

  Informationen zum Standardinstallationsverzeichnis finden Sie im Installationsabschnitt für Ihr Betriebssystem.

   Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeWenn Sie eine Imagesicherung, eine Imagezurückschreibung, eine momentaufnahmebasierte Dateisicherung, eine NAS-Sicherung oder eine NAS-Zurückschreibung anfordern, lokalisiert der Client die entsprechende Plug-In-Bibliothek mithilfe der Umgebungsvariablen DSM_DIR. Wenn für DSM_DIR kein Wert festgelegt wurde, sucht der Client in folgenden Verzeichnissen nach den Plug-in-Bibliotheken:

  AIX
  : /usr/tivoli/tsm/client/ba/bin/plugins

  Oracle Solaris- und alle Linux-Clients
  : /opt/tivoli/tsm/client/ba/bin/plugins

DSM_CONFIG
: Gibt den vollständig qualifizierten Pfad und Dateinamen der Clientbenutzeroptionsdatei für Benutzer an, die ihre persönliche Optionsdatei erstellen. Ist DSM_CONFIG nicht definiert oder wird die Clientoption optfile nicht verwendet, muss die Clientbenutzeroptionsdatei die folgenden Anforderungen erfüllen:

1. Die Optionsdatei muss den Namen `dsm.opt` haben.
2. Für andere UNIX-Clients als Mac OS X: Ist DSM_DIR *nicht* definiert, muss die Datei sich im Standardinstallationsverzeichnis befinden. Ist DSM_DIR *definiert*, muss die Datei sich in dem Verzeichnis befinden, das von DSM_DIR angegeben ist.
3.  Für Mac OS X: Die Datei kann sich an einer der folgenden Positionen befinden. Diese Verzeichnisse werden in der angegebenen Reihenfolge durchsucht und die erste gefundene Optionsdatei wird verwendet. `~/Library Preferences/Tivoli Storage Manager`, `/Library Preferences/Tivoli Storage Manager` oder `/Library/Application Support/tivoli/tsm/client/ba/bin`.

Informationen zum Standardinstallationsverzeichnis finden Sie im Installationsabschnitt für Ihr Betriebssystem.

DSM_LOG
: Verweist auf das Verzeichnis, in dem die IBM Spectrum Protect-Protokolldateien gespeichert werden sollen. Das Stammverzeichnis (/) kann für DSM_LOG nicht angegeben werden. Die Protokolldateien enthalten Informationen zu Fehlern und Ereignissen, die während der Verarbeitung auftreten. Der Client erstellt die Protokolle, um den Mitarbeitern der technischen Unterstützung die Diagnose schwerwiegender Fehler zu erleichtern.

  Informationen zum Standardinstallationsverzeichnis finden Sie im Installationsabschnitt für Ihr Betriebssystem.

  Wichtig: Geben Sie für die Umgebungsvariable DSM_LOG ein Verzeichnis an, in dem die Schreib-/Leseberechtigungen dem Benutzer den erforderlichen Schreibzugriff ermöglichen, um die Protokolldatei erstellen und Daten in sie schreiben zu können. Dadurch werden Fehler beim Schreiben in das Protokoll und Prozessbeendigungen verhindert. Erteilen Sie mit den Befehlen chmod oder setacl die Berechtigungen für die Dateien, die allen Clientbenutzer-IDs das Lesen der Dateien und das Schreiben in die Dateien gestatten. Wenn die Protokollnamen die Standardnamen sind, setzen Sie einfach die Umgebungsvariable DSM_LOG, sodass sie auf das Verzeichnis zeigt, in dem sich die Protokolle befinden. Wenn der Client keine Daten in die Protokolldatei schreiben kann, wird eine Fehlernachricht in stderror und in den syslog-Dämon geschrieben. Der syslog-Dämon muss aktiv und so konfiguriert sein, dass Nachrichten mit der Priorität LOG_ERR verarbeitet werden, damit die Fehlernachricht im Systemprotokoll angezeigt wird. Das Starten und Konfigurieren des syslog-Dämons erfolgt systemspezifisch. Mit dem Befehl man syslogd können Sie Informationen zum Starten des syslog-Dämons abrufen. Verwenden Sie man syslog.conf, um Informationen zum Konfigurieren des syslog-Dämons abzurufen.
  Anmerkung:

  1. Die Optionen errorlogname und schedlogname überschreiben DSM_LOG. Wenn Sie die Clientoption errorlogname angeben, wird die Datei nicht an der durch DSM_LOG angegebenen Position, sondern in dem durch die Option errorlogname angegebenen Verzeichnis gespeichert. Wenn Sie die Clientoption schedlogname angeben, wird sie nicht an die durch DSM_LOG angegebene Position, sondern in das durch die Option schedlogname angegebene Verzeichnis geschrieben.
  2. Die Protokolldateien dürfen keine symbolischen Verbindungen sein. Der Client erkennt derartige Verbindungen, löscht die Verbindungen und beendet die Operation. Mit dieser Aktion wird verhindert, dass der Client geschützte Daten überschreibt. Die betroffenen Protokolle werden in einer nachfolgenden Operation als Dateien erstellt.

Damit die Java™-GUI des Clients für Sichern/Archivieren verwendet werden kann, müssen Sie das Verzeichnis, in dem die Java-Binärdatei installiert ist, exportieren. Geben Sie z. B. den folgenden Befehl ein:

```
export PATH=$PATH:Verzeichnis_für_Java-Binärdatei
```

Dabei ist *Verzeichnis_für_Java-Binärdatei* der Pfad zu der ausführbaren Java-Binärdatei in Ihrem Dateisystem.

Zugehörige Verweise:
Optfile
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Bourne- und Korn-Shell-Variablen definieren

Geben Sie die Umgebungsvariablen in die Datei `.profile` (Korn-Shell) oder in die Datei `.bash_profile` (Bourne-Shell) im Verzeichnis `$HOME` ein.

Im folgenden Beispiel ist `/home/davehil/dsm.opt` der Pfad und Dateiname für Ihre Clientbenutzeroptionsdatei und `/home/davehil` ist das Verzeichnis, in dem Sie die Datei `dsmerror.log`, die ausführbaren Dateien, die Ressourcendateien und die Datei dsm.sys speichern wollen.

```
DSM_DIR=/home/davehil
   DSM_CONFIG=/home/davehil/dsm.opt
   DSM_LOG=/home/davehil
   export DSM_DIR DSM_CONFIG DSM_LOG
```

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

C-Shell-Variablen definieren

Für die C-Shell fügen Sie die Variablen DSM_CONFIG, DSM_LOG und DSM_DIR der Datei `.cshrc` im Verzeichnis `$HOME` hinzu.

Im folgenden Beispiel ist `/home/davehil/dsm.opt` der Pfad und Dateiname für Ihre Clientbenutzeroptionsdatei und `/home/davehil` ist das Verzeichnis, in dem Sie die Datei `dsmerror.log`, die ausführbaren Dateien, die Ressourcendateien und die Datei dsm.sys speichern wollen.

```
setenv DSM_DIR /home/davehil
   setenv DSM_CONFIG /home/davehil/dsm.opt
   setenv DSM_LOG /home/davehil
```

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

API-Umgebungsvariablen definieren

Wenn Sie die IBM Spectrum Protect-API installiert haben, definieren Sie die folgenden Umgebungsvariablen.

DSMI_DIR
: Zeigt auf das Installationsverzeichnis. Die Datei dsm.sys muss sich in dem Verzeichnis befinden, auf das DSMI_DIR zeigt. Diese Umgebungsvariable muss vorhanden sein.

DSMI_CONFIG
: Vollständiger Pfadname Ihrer eigenen Clientbenutzeroptionsdatei (dsm.opt).

DSMI_LOG
: Pfad für dsierror.log (dieser Pfad kann keine symbolische Verbindung sein).

Anmerkung: Endbenutzer von Anwendungen, die mit der API entwickelt wurden, können anhand der Installationsanweisungen für diese Anwendung feststellen, ob bestimmte Pfadnamen oder Richtlinien für Optionen einzuhalten sind.

Weitere Informationen zu den Umgebungsvariablen finden Sie in Umgebungsvariablen für die Verarbeitung definieren.

Weitere Informationen zur IBM Spectrum Protect-API finden Sie in Lösungen mit der Anwendungsprogrammierschnittstelle entwickeln.

 Windows-Betriebssysteme

Sprache für die Anzeige der Java-GUI konfigurieren

Sie können die Sprache für die Anzeige der Java™-GUI des Clients für Sichern/Archivieren auswählen.

Informationen zu diesem Vorgang

Die Sprache, die von der Java-GUI des Clients für Sichern/Archivieren angezeigt wird, wird über die Windows-Anzeigeländereinstellung und nicht über die Windows-Systemländereinstellung definiert. Wenn beispielsweise für die System- und Eingabeländereinstellung unter Windows Französisch festgelegt ist, für die Anzeigeländereinstellung jedoch Russisch definiert ist, wird von der Java-GUI als Sprache standardmäßig Russisch angezeigt, sofern die Option language nicht verwendet wird.

Wenn die Java-GUI in amerikanischem Englisch oder einer anderen Sprache angezeigt werden soll, können Sie die Standardanzeigesprache überschreiben, indem Sie die Option language angeben.

Tipp: Die Option language wirkt sich nicht auf den Web-Client aus. Der Web-Client wird in der Sprache angezeigt, die der Ländereinstellung des Browsers zugeordnet ist. Ist im Browser eine Ländereinstellung aktiv, die der Client nicht unterstützt, wird der Web-Client in amerikanischem Englisch angezeigt.

Vorgehensweise

Verwenden Sie eine der folgenden Methoden, um die Sprache für die Anzeige der Java-GUI zu konfigurieren:

- Fügen Sie der Clientoptionsdatei (dsm.opt) die Option `language` *`Sprache`* hinzu. Um beispielsweise die Anzeigesprache auf amerikanisches Englisch zu setzen, fügen Sie die folgende Anweisung hinzu:

  ```
  language enu
  ```

- Führen Sie in der Java-GUI des Clients für Sichern/Archivieren die folgenden Schritte aus:
  1. Klicken Sie im Hauptfenster der Java-GUI auf Editieren > Clientvorgaben.
  2. Klicken Sie auf die Registerkarte Regionale Einstellungen.
  3. Klicken Sie auf die Dropdown-Liste Sprache und wählen Sie eine Sprache aus.
  4. Klicken Sie auf OK.

Zugehörige Verweise:
Language

Übersicht über die Konfiguration des Web-Clients

Der IBM Spectrum Protect-Web-Client stellt die Fernverwaltung eines Clientknotens über einen Web-Browser zur Verfügung. Die Prozeduren für die Konfiguration des Web-Clients variieren abhängig davon, welches Betriebssystem auf dem Clientknoten verwendet wird.

Ab IBM Spectrum Protect Version 8.1.2 können Sie nicht mehr den Web-Client verwenden, um eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder höher herzustellen. Sie können den Web-Client jedoch weiterhin verwenden, um eine Verbindung zu Servern mit

IBM Spectrum Protect Version 8.1.1, Version 8.1.0, Version 7.1.7 und früheren Versionen herzustellen. Weitere Informationen finden Sie in Web-Client in neuer Sicherheitsumgebung verwenden.

Zum Konfigurieren der Web-Client-Einstellungen werden Optionen des Clients für Sichern/Archivieren verwendet. Hierzu gehören die Optionen httpport, managedservices, webports und revokeremoteaccess.

 Auf Windows-Client-Knoten steht in der GUI des Clients für Sichern/Archivieren ein Setup-Assistent zur Verfügung. Mit dem Setup-Assistenten können Sie den Web-Client konfigurieren. Die Optionen, die Sie im Assistenten auswählen, werden in die Clientbenutzeroptionsdatei (dsm.opt) kopiert. Sie können die Optionen auch direkt zur Datei dsm.opt hinzufügen, indem Sie die Datei editieren und die Web-Client-Optionen hinzufügen.

    Auf AIX-, Linux-, Mac- und Solaris-Clientknoten fügen Sie die Web-Client-Optionen zur Clientsystemoptionsdatei (dsm.sys) hinzu.

Um den Web-Client über die Schnittstelle des IBM Spectrum Protect Operations Center zu verwenden, geben Sie die Web-Client-Adresse im Parameter URL des Befehls REGISTER NODE oder UPDATE NODE an. Die Webadresse muss den DNS-Namen oder die IP-Adresse des Knotens sowie die Anschlussnummer enthalten, die der Web-Client verwendet. Beispiel: `http://node.example.com:1581`. Ersetzen Sie in diesem Beispiel den Hostnamen durch die IP-Adresse oder den Hostnamen Ihres Clientknotens. Wenn Sie mithilfe eines Web-Browsers auf den Web-Client zugreifen, geben Sie dieselbe Syntax in der Adressleiste des Browsers ein.

Alle Web-Client-Nachrichten werden in die Protokolldatei des Web-Clients geschrieben. Diese Datei heißt dsmwebcl.log. Die Datei dsmwebcl.log und die Fehlerprotokolldatei des Clients für Sichern/Archivieren (dsmerror.log) werden standardmäßig im Clientinstallationsverzeichnis erstellt. Mit der Umgebungsvariablen DSM_LOG können Sie die Standardpositionen für die Fehlerprotokolle überschreiben. Falls Sie die Umgebungsvariable DSM_LOG festlegen, geben Sie als Position für die Fehlerprotokolle nicht das Stammverzeichnis an. Die Position der Fehlerprotokolldateien können Sie auch mit der Option errorlogname des Clients für Sichern/Archivieren ändern. Falls Sie diese Option angeben, setzt sie die Einstellung der Umgebungsvariablen DSM_LOG außer Kraft.

-     Web-Client auf AIX-, Linux-, Mac- und Solaris-Systemen konfigurieren
  Zur Konfiguration des Web-Clients müssen Sie die Clientsystemoptionsdatei (dsm.sys) editieren und die erforderlichen Optionen angeben. Anschließend starten Sie den Clientakzeptordämon.
-  Web-Client auf Windows-Systemen konfigurieren
  Auf Windows-Systemen können Sie zum Konfigurieren und Starten des Web-Clients einen Assistenten, der in der GUI des Clients für Sichern/Archivieren verfügbar ist, oder IBM Spectrum Protect- und Windows-Befehle verwenden.

Zugehörige Konzepte:
Web-Client-Optionen
Zugehörige Tasks:
    Web-Client auf AIX-, Linux-, Mac- und Solaris-Systemen konfigurieren
 Web-Client auf Windows-Systemen konfigurieren
   

Web-Client auf AIX-, Linux-, Mac- und Solaris-Systemen konfigurieren

Zur Konfiguration des Web-Clients müssen Sie die Clientsystemoptionsdatei (dsm.sys) editieren und die erforderlichen Optionen angeben. Anschließend starten Sie den Clientakzeptordämon.

Vorgehensweise

1. Legen Sie die folgenden Optionen in der Datei dsm.sys fest: managedservices webclient schedule und passwordaccess generate.
2. Generieren Sie das IBM Spectrum Protect-Kennwort. Geben Sie `dsmc query session` ein. Sobald die Berechtigungsnachweise von Ihnen angefordert werden, geben Sie den Benutzernamen und das Kennwort für IBM Spectrum Protect ein.

    Auf Mac OS X-Systemen können Sie zum Generieren des Kennworts auch die Anwendung 'IBM Spectrum Protect-Tools für Administratoren' verwenden. Wählen Sie in der Anwendung IBM Spectrum Protect aus, um den Client zu starten.

3. Starten Sie den Clientakzeptordämon. Geben Sie `dsmcad` ein.

    Unter Mac OS X können Sie zum Starten des Clientakzeptordämons auch die Anwendung 'IBM Spectrum Protect-Tools für Administratoren' verwenden. Wählen Sie in der Anwendung die Option zum Starten des Clientakzeptordämons aus.

4. Um aus einem Browser auf den Web-Client zuzugreifen, geben Sie in der Adressleiste des Browsers den Hostnamen oder die IP-Adresse des Clientknotens gefolgt von der Anschlussnummer des Web-Clients an. Die Standardanschlussnummer ist 1581. Um beispielsweise auf den Web-Client auf dem Knoten namens 'myserver.example.com' zuzugreifen, geben Sie `http://myserver.example.com:1581` an.

   Falls Sie die Standardanschlussnummer des Web-Clients ändern müssen, verwenden Sie die Option httpport des Clients für Sichern/Archivieren, um eine andere Anschlussnummer zuzuordnen.

Nächste Schritte

Nachdem Sie den Web-Client konfiguriert haben, können Sie Daten auf einem Knoten mit dem IBM Spectrum Protect Operations Center oder einem Browser sichern oder zurückschreiben bzw. archivieren oder abrufen.

Zugehörige Konzepte:
Planungsoptionen
Web-Client-Optionen

Zugehörige Tasks:
Web-Client-Sitzung starten

Zugehörige Verweise:
Httpport
Passwordaccess

 Windows-Betriebssysteme

Web-Client auf Windows-Systemen konfigurieren

Auf Windows-Systemen können Sie zum Konfigurieren und Starten des Web-Clients einen Assistenten, der in der GUI des Clients für Sichern/Archivieren verfügbar ist, oder IBM Spectrum Protect- und Windows-Befehle verwenden.

Vorgehensweise

Für die Konfiguration des Windows-Web-Clients stehen die folgenden Verfahren zur Auswahl:

Konfigurationsmethode	Prozedur
Setup-Assistent	a. Starten Sie die grafische Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren. b. Klicken Sie auf Dienstprogramme > Setup-Assistent. c. Wählen Sie das Kontrollkästchen Hilfe zum Konfigurieren des Web-Clients aus. d. Klicken Sie auf Weiter und konfigurieren Sie die Optionen für den Web-Client nach den Anweisungen des Assistenten.

Eingabeaufforderung	a. Legen Sie die folgenden Optionen in der Datei dsm.opt fest: managedservices webclient schedule und passwordaccess generate.
	b. Installieren Sie den Clientakzeptorservice, indem Sie den folgenden Befehl eingeben:
	`dsmcutil install cad /name:"`*`TSM-CAD`*`" /node:`*`Knotenname`*
	`/password:`*`Kennwort`*` /autostart:yes`
	Hierbei gilt Folgendes:
	TSM-CAD ist ein Name für den Service. Der Standardname ist 'TSM-Clientakzeptor'.
	Knotenname ist der Name des Clientknotens.
	Kennwort ist das IBM Spectrum Protect-Kennwort.
	`/autostart:yes` gibt an, dass der Clientakzeptorservice beim Start des Betriebssystems gestartet wird.
	Starten Sie den Service mit dem Windows-Befehl net start.
	c. Installieren Sie den IBM Spectrum Protect-Service 'Ferner Clientagent', indem Sie den folgenden Befehl eingeben:
	`dsmcutil install remoteagent /name:"`*`TSM-AGENT`*`" /node:`*`Knotenname`*
	`/password:`*`Kennwort`*` /partnername:"`*`TSM-CAD`*`"`
	Hierbei gilt Folgendes:
	○ *TSM-AGENT* ist ein Name für den Service 'Ferner Clientagent'. Der Standardservicename lautet 'Ferner TSM-Clientagent'.
	○ *Knotenname* ist der Name des Clientknotens.
	○ *Kennwort* ist das IBM Spectrum Protect-Kennwort.
	○ *TSM-CAD* ist der Name des Servicepartners. Dieser Name muss mit dem Servicenamen identisch sein, den Sie bei der Installation des Clientakzeptorservice angegeben haben. Der Standardname ist 'TSM-Clientakzeptor'.
	Starten Sie den Service 'Ferner TSM-Clientagent' nicht über die Sicht Systemsteuerung > Verwaltung > Dienste oder mit dem Befehl net start. Der Clientakzeptorservice startet den fernen Clientagenten, sobald er benötigt wird.

Nächste Schritte

Nachdem Sie den Web-Client konfiguriert haben, können Sie Daten auf einem Knoten mit dem IBM Spectrum Protect Operations Center oder einem Browser sichern oder zurückschreiben bzw. archivieren oder abrufen.
Zugehörige Konzepte:
Planungsoptionen
Web-Client-Optionen
Zugehörige Tasks:
Web-Client-Sitzung starten
Zugehörige Verweise:
Httpport
Passwordaccess

Scheduler konfigurieren

Ihr IBM Spectrum Protect-Administrator kann den Client für die automatische Ausführung von Tasks konfigurieren. Damit geplante Ereignisse auf dem Client stattfinden können, müssen Sie den Client-Scheduler für die Kommunikation mit dem IBM Spectrum Protect-Server konfigurieren.

Informationen zu diesem Vorgang

So können Sie beispielsweise Dateien jeden Abend automatisch sichern oder einige Dateien jeden Freitag archivieren. Bei dieser Prozedur, die als zentrale Zeitplanung bezeichnet wird, arbeiten der Server und Ihr Clientknoten zusammen. Der Administrator ordnet Clients einem oder mehreren Zeitplänen zu, die zu der Maßnahmendomäne gehören, die in der Serverdatenbank verwaltet wird. Der IBM Spectrum Protect-Administrator definiert die zentrale Zeitplanung auf dem Server und Sie starten den Client-Scheduler auf Ihrer Workstation. Nach dem Starten des Client-Schedulers ist kein weiterer Eingriff erforderlich.

Mithilfe der Clientzeitplanung können Sie folgende Tasks ausführen:

- Informationen zu verfügbaren Zeitplänen anzeigen.
- Informationen zu geplanter Arbeit, die beendet ist, anzeigen.
- Windows-BetriebssystemePlanungsoptionen in der Clientoptionsdatei (dsm.opt) ändern.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemePlanungsoptionen in der Datei dsm.sys ändern.

Die effektivste Möglichkeit zur Verwaltung des Client-Schedulers besteht in der Verwendung des Clientakzeptorservice. Sie können Informationen zu einem Vergleich zwischen der Verwendung des Clientakzeptors und traditioneller Scheduler-Services für die Verwaltung des Schedulers lesen. Außerdem erfahren Sie, wie der Client für die Verwaltung des Schedulers durch den Clientakzeptor konfiguriert wird.

- Vergleich zwischen vom Clientakzeptor verwalteten Services und traditionellen Scheduler-Services
  Sie können den IBM Spectrum Protect-Scheduler mit dem Clientakzeptorservice oder mit dem traditionellen Scheduler-Service verwalten. Dieser Abschnitt enthält einen Vergleich dieser Methoden.
- Client für die Verwaltung des Schedulers durch den Clientakzeptorservice konfigurieren
  Eine der effektivsten Möglichkeiten zur Verwaltung des Client-Schedulers besteht in der Verwendung des Clientakzeptorservice. Sie müssen den Client für die Verwaltung des Schedulers durch den Clientakzeptor konfigurieren.

Vergleich zwischen vom Clientakzeptor verwalteten Services und traditionellen Scheduler-Services

Sie können den IBM Spectrum Protect-Scheduler mit dem Clientakzeptorservice oder mit dem traditionellen Scheduler-Service verwalten. Dieser Abschnitt enthält einen Vergleich dieser Methoden.

Die folgende Tabelle zeigt die Unterschiede zwischen den vom Clientakzeptor verwalteten Services und den standardmäßigen traditionellen Scheduler-Services.

Tabelle 1. Vergleich zwischen vom Clientakzeptor verwalteten Services und traditionellen Scheduler-Services

Vom Clientakzeptor verwaltete Services	**Traditionelle IBM Spectrum Protect-Scheduler-Services**
Werden mithilfe der Option `managedservices schedule` definiert und mit Clientakzeptorservices gestartet. AIX-BetriebssystemeLinux-Betriebssysteme Mac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDer Clientakzeptordämon wird mit dem Befehl dsmcad gestartet. Windows-BetriebssystemeDer Clientakzeptorservice wird als Windows-Dienst gestartet.	Werden mit dem Befehl dsmc sched gestartet.
Der Clientakzeptorservice startet und stoppt den Schedulerprozess für jede geplante Aktion nach Bedarf.	Bleiben aktiv, selbst wenn die geplante Sicherung beendet ist.

Vom Clientakzeptor verwaltete Services	Traditionelle IBM Spectrum Protect-Scheduler-Services
Erfordern weniger Systemressourcen bei Inaktivität.	Erfordern einen höheren Verbrauch an Systemressourcen bei Inaktivität.
Clientoptionen und Überschreibungsoptionen auf dem IBM Spectrum Protect-Server werden jedes Mal aktualisiert, wenn die Clientakzeptorservices eine geplante Sicherung starten.	Clientoptionen und Überschreibungsoptionen auf dem IBM Spectrum Protect-Server werden erst nach dem Start von dsmc sched verarbeitet.
Können nicht bei Sicherungen mit `SESSIONINITiation=SERVEROnly` verwendet werden.	Sie müssen den Schedulerprozess erneut starten, damit aktualisierte Clientoptionen wirksam werden. Wichtig: Wenn Sie den Client-Scheduler über die Befehlszeile ausführen, wird der Scheduler nicht als Hintergrundservice ausgeführt. Tipp: Starten Sie den traditionellen Scheduler regelmäßig, um Systemressourcen freizugeben, die zuvor von Systemaufrufen verwendet wurden.

Client für die Verwaltung des Schedulers durch den Clientakzeptorservice konfigurieren

Eine der effektivsten Möglichkeiten zur Verwaltung des Client-Schedulers besteht in der Verwendung des Clientakzeptorservice. Sie müssen den Client für die Verwaltung des Schedulers durch den Clientakzeptor konfigurieren.

Vorbereitende Schritte

- Wenn Sie Dateien für die Verschlüsselung einschließen, stellen Sie sicher, dass die Option encryptkey in der Optionsdatei auf save gesetzt ist. Diese Option wird durch Auswahl von Kennwort für Verschlüsselungsschlüssel lokal speichern auf der Registerkarte Berechtigung des Profileditors definiert. Wenn diese Option definiert ist, können unbeaufsichtigte geplante Services ausgeführt werden. Wenn der Verschlüsselungsschlüssel noch nicht gespeichert wurde, müssen Sie eine überwachte Sicherung von mindestens einer Datei ausführen, damit die Eingabeaufforderung für die Verschlüsselung angezeigt wird und Sie den Schlüssel speichern können.
- Sie können den Clientakzeptor nicht für die Planung verwenden, wenn die Option sessioninitiation auf serveronly gesetzt ist.

Informationen zu diesem Vorgang

Der Clientakzeptor dient als externer Zeitgeber für den Scheduler. Wenn der Scheduler gestartet wird, fragt er den Server nach dem nächsten geplanten Ereignis. Das Ereignis wird entweder sofort ausgeführt oder der Scheduler wird beendet. Der Clientakzeptor startet den Scheduler erneut, wenn der Zeitpunkt für die Ausführung des geplanten Ereignisses erreicht wird. Mit dieser Aktion wird die Anzahl Hintergrundprozesse auf Ihrer Workstation reduziert und Probleme in Bezug auf die Speicheraufbewahrungsdauer, die auftreten können, wenn der Scheduler ohne Verwaltung durch den Clientakzeptor ausgeführt wird, werden vermieden.

Der Clientakzeptorservice wird als auch Clientakzeptordämon (CAD) bezeichnet.

Vorgehensweise

- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeFühren Sie die folgenden Schritte aus, um den Clientakzeptor für die Verwaltung des Client-Schedulers zu verwenden:
  1. Wählen Sie in der GUI des Clients für Sichern/Archivieren Editieren > Vorgaben aus.
  2. Klicken Sie auf die Registerkarte Web-Client.
  3. Klicken Sie im Feld für die Optionen verwalteter Services auf Zeitplan. Wenn der Clientakzeptor auch den Web-Client verwalten soll, klicken Sie auf die Option Beide.
  4. Starten Sie den Clientakzeptordämon mit dem folgenden Befehl in der Befehlszeile:

     ```
     dsmcad
     ```

  Tipp:
  - Sie können auch die Option managedservices in der Clientsystemoptionsdatei (dsm.sys) verwenden, um anzugeben, ob der Clientakzeptor den Scheduler verwaltet.
  - Wenn der Clientakzeptor den Scheduler im Abfragemodus verwalten soll, ohne einen Empfangsport zu öffnen, verwenden Sie die Option cadlistenonport in der Datei dsm.sys.
- Windows-BetriebssystemeFühren Sie die folgenden Schritte aus, um den Clientakzeptor für die Verwaltung des Schedulers auf dem Windows-Client zu verwenden:
  1. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Dienstprogramme > Setup-Assistent > Hilfe zum Konfigurieren des Client-Schedulers und dann auf Weiter.
  2. Lesen Sie die Informationen auf der Seite Schedulerassistent und klicken Sie auf Weiter.
  3. Wählen Sie auf der Seite Scheduler-Task Neuen oder zusätzlichen Scheduler installieren aus und klicken Sie auf Weiter.
  4. Geben Sie auf der Seite Schedulername und -position einen Namen für den Clientakzeptorservice an, der den Scheduler verwalten soll. Wählen Sie dann Scheduler mit Clientakzeptor verwalten aus und klicken Sie auf Weiter.

5. Wenn der Clientakzeptor bereits für die Verwendung durch den Web-Client installiert ist, wählen Sie diesen Namen des Clientakzeptors aus der Dropdown-Liste auf der Seite Web-Service-Name aus. Geben Sie andernfalls den Namen ein, der diesem Clientakzeptor zugeordnet werden soll. Der Standardname ist TSM-Clientakzeptor. Klicken Sie auf Weiter.
6. Befolgen Sie die Anweisungen in den übrigen Anzeigen, um die Konfiguration abzuschließen.

   Füllen Sie die Assistentenseiten mithilfe der folgenden Informationen aus:

   - Wenn die Option sessioninitiation in der Clientoptionsdatei (dsm.opt) auf serveronly gesetzt ist, können der Clientkonfigurationsassistent und der Scheduler-Service die Authentifizierung mit dem IBM Spectrum Protect-Server möglicherweise nicht einleiten. Zur Vermeidung dieses Problems müssen Sie sicherstellen, dass das Kontrollkästchen IBM Spectrum Protect-Server zwecks Kennwortprüfung kontaktieren auf der Seite 'IBM Spectrum Protect-Authentifizierung' nicht ausgewählt ist.
   - Wählen Sie für den vom Clientakzeptor verwalteten Scheduler Manuell beim expliziten Start des Service auf der Seite Serviceanmeldeoptionen aus.
7. Starten Sie den Clientakzeptorservice über die Servicesystemsteuerung, starten Sie aber nicht den Scheduler-Service. Der Scheduler-Service wird nach Bedarf automatisch vom Clientakzeptorservice gestartet und gestoppt.

Tipp:

- Sie können auch die Option managedservices in der Clientoptionsdatei (dsm.opt) verwenden, um anzugeben, ob der Clientakzeptor den Scheduler verwaltet.
- Wenn der Clientakzeptor den Scheduler im Abfragemodus verwalten soll, ohne einen Empfangsport zu öffnen, verwenden Sie die Option cadlistenonport in der Datei dsm.opt.
- Wenn Sie den Scheduler nicht mithilfe des Clientakzeptors verwalten, wählen Sie Automatisch beim Booten von Windows im Fenster Serviceanmeldeoptionen aus. Mit dieser Einstellung wird der Service beim Windows-Start automatisch gestartet, damit Ihre Zeitpläne automatisch ausgeführt werden. Sie können den Scheduler-Service auch über die Servicesystemsteuerung oder den Befehl net start starten.
- Sie können den Scheduler auch mit dem Konfigurationsdienstprogramm für den Scheduler-Service (dsmcutil.exe) konfigurieren. Das Konfigurationsdienstprogramm für den Scheduler-Service muss von einem Konto ausgeführt werden, das zur Gruppe 'Administratoren/Domänen-Admins' gehört. Es können mehrere Client-Scheduler-Services auf dem System gestartet werden.

Zugehörige Konzepte:
Übersicht über die Konfiguration des Web-Clients
Geplante Befehle aktivieren oder inaktivieren
Planungsoptionen
Zugehörige Tasks:
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren
Zugehörige Verweise:
Cadlistenonport
Managedservices
Sessioninitiation
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

Client-Scheduler starten

Diese Task führt Sie durch die Schritte zum Planen von Ereignissen mithilfe der grafischen Benutzerschnittstelle und des Befehlszeilenclients.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeEreignisse mit dem Befehlszeilenclient planen
  Diese Task führt Sie durch die Schritte zum Planen von Ereignissen über den Befehlszeilenclient.

Windows-Betriebssysteme

Client-Scheduler starten

Um den Client-Scheduler zu starten, verwenden Sie die Systemsteuerung oder den Befehl **net start**.

Informationen zu diesem Vorgang

Führen Sie den Client-Scheduler nicht über die Befehlszeile aus, um Probleme zu vermeiden. Über die Befehlszeile wird der Scheduler nicht als Hintergrundservice ausgeführt.

Nach dem Start des Client-Schedulers bleibt dieser solange aktiv, bis das Fenster geschlossen, das System heruntergefahren oder eine Abmeldung vom System durchgeführt wird. Wenn der Scheduler-Service ausgeführt wird, ist der Scheduler so lange aktiv, bis ein Systemabschluss ausgeführt wird oder bis der Scheduler mit der Funktion "Dienste" in der "Systemsteuerung" explizit gestoppt wird.

- Windows-BetriebssystemeEreignisse mithilfe der GUI planen
  Diese Task führt Sie durch die Schritte zum Planen von Ereignissen über die GUI.

Zugehörige Konzepte:
Verarbeitungsoptionen

IBM Spectrum Protect-Client/Server-Übertragung über eine Firewall hinweg konfigurieren

In den meisten Fällen können die IBM Spectrum Protect-Server und -Clients über eine Firewall hinweg zusammenarbeiten.

Informationen zu diesem Vorgang

Alle Firewalls sind unterschiedlich; daher muss der Firewall-Administrator möglicherweise die Anweisungen für die verwendete Firewall-Software oder -Hardware konsultieren.

Es gibt zwei Methoden, um Client- und Serveroperationen durch eine Firewall zu aktivieren:

Methode 1:

Damit Clients über eine Firewall hinweg mit einem Server kommunizieren können, müssen folgende Anschlüsse in der Firewall durch den Firewall-Administrator geöffnet werden:

TCP/IP-Anschluss

Sollen der Client für Sichern/Archivieren, der Befehlszeilenverwaltungsclient und der Scheduler außerhalb einer Firewall ausgeführt werden, muss der Anschluss, der von der Serveroption ***tcpport*** angegeben wird (Standardwert 1500), vom Firewall-Administrator geöffnet werden. Dieser Anschluss wird mit der Option ***tcpport*** auf dem Client und Server definiert. Die Einstellung muss auf dem Client und Server dieselbe sein. Dies ermöglicht IBM Spectrum Protect-Schedulerkommunikation sowohl im Modus *Ausführung bei Sendeaufruf* als auch im Modus *gesteuerte Ausführung*, vom Clientakzeptor verwaltete Scheduler und regelmäßige Operationen des Clients für Sichern/Archivieren.

Anmerkung: Der Client kann den Anschluss, der durch die Option ***tcpadminport*** (auf dem Server) angegeben ist, nicht für eine Clientsitzung verwenden. Dieser Anschluss kann nur für Verwaltungssitzungen verwendet werden.

HTTP-Anschluss

Damit der Web-Client mit den fernen Workstations über eine Firewall hinweg kommunizieren kann, muss der HTTP-Anschluss für die ferne Workstation geöffnet werden. Verwenden Sie die Option ***httpport*** in der Clientoptionsdatei der fernen Workstation, um diesen Anschluss anzugeben. Der standardmäßige HTTP-Anschluss ist 1581.

TCP/IP-Anschlüsse für die ferne Workstation

Die beiden TCP/IP-Anschlüsse für den fernen Workstation-Client müssen geöffnet werden. Verwenden Sie die Option ***webports*** in der Clientoptionsdatei der fernen Workstation, um diese Anschlüsse anzugeben. Werden keine Werte für die Option ***webports*** angegeben, bewirkt der Standardwert null (0), dass TCP/IP willkürlich zwei freie Anschlussnummern zuweist.

TCP/IP-Anschluss für Verwaltungssitzungen

Gibt eine separate TCP/IP-Anschlussnummer an, an der der Server Anforderungen für Verwaltungsclientsitzungen erwartet. Dies ermöglicht sichere Verwaltungssitzungen innerhalb eines privaten Netzes.

Methode 2:

Es ist unnötig, für den Client-Scheduler im Modus mit Bedienerführung *irgendwelche* Anschlüsse auf der Firewall zu öffnen. Wenn Sie die Option ***sessioninitiation*** auf *serveronly* setzen, versucht der Client nicht, Kontakt zum Server aufzunehmen. *Alle Sitzungen werden durch die Zeitplanung über Serversystemanfrage* an dem mit der Option ***tcpclientport*** auf dem Client definierten Anschluss eingeleitet. Die Option ***sessioninitiation*** beeinflusst nur das Verhalten des Client-Schedulers, der im Modus mit Bedienerführung ausgeführt wird.

Der IBM Spectrum Protect-Server muss für jeden Knoten den Parameter "SESSIONINITiation" in den Befehlen **register node** und **update node** definieren. Wenn der Server SESSIONINITiation=*clientorserver*, den Standardwert, angibt, kann der Client entscheiden, welche Methode verwendet werden soll. Wenn der Server SESSIONINITiation=*serveronly* angibt, werden alle Sitzungen vom Server eingeleitet.

Anmerkung:

1. Wird ***sessioninitiation*** auf *serveronly* gesetzt, muss der Wert für die Clientoption ***tcpclientaddress*** mit dem Wert für die Option ***HLAddress*** im Serverbefehl **update node** oder **register node** übereinstimmen. Der Wert für die Clientoption ***tcpclientport*** muss mit dem Wert für die Option ***LLAddress*** im Serverbefehl **update node** oder **register node** übereinstimmen.
2. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWenn Sie die Option ***sessioninitiation*** auf *serveronly* setzen, versuchen der Befehlszeilenclient, die Java™-GUI des Clients für Sichern/Archivieren und die Web-Client-GUI mit Ausnahme der vom Clientakzeptor verwalteten Scheduler weiterhin, Sitzungen einzuleiten; sie werden jedoch vom IBM Spectrum Protect-Server für Knoten blockiert, für die die Option ***sessioninitiation*** auf *serveronly* gesetzt ist.
3. Windows-BetriebssystemeWenn Sie die Option ***sessioninitiation*** auf *serveronly* setzen, versuchen der Befehlszeilenclient, die GUI des Clients für Sichern/Archivieren und die Web-Client-GUI mit Ausnahme der vom Clientakzeptor verwalteten Scheduler weiterhin, Sitzungen einzuleiten; sie werden jedoch vom IBM Spectrum Protect-Server für Knoten blockiert, für die die Option ***sessioninitiation*** auf *serveronly* gesetzt ist.
4. Windows-BetriebssystemeWenn der Scheduler mithilfe des Setup-Assistenten oder mithilfe von dsmcutil installiert wird und sich der IBM Spectrum Protect-Server hinter einer Firewall befindet, wird das Knotenkennwort nicht auf der Client-Workstation gespeichert. Als Ergebnis kann sich der Scheduler-Service unter Umständen nicht beim Server authentifizieren, wenn der Server Kontakt mit dem Client aufnimmt, um einen Zeitplan auszuführen. In diesen Fall können Sie den Scheduler über die Befehlszeile ausführen (dsmc schedule), auf den Start einer geplanten Operation warten und das Kennwort für Ihren Knoten eingeben, wenn Sie dazu aufgefordert werden. Nachdem Sie das Kennwort für Ihren Knoten eingegeben haben, müssen Sie den Scheduler-Service erneut starten. Sie können auch den folgenden **dsmcutil**-Befehl verwenden, um das Kennwort zu speichern:

```
dsmcutil updatepw /node:nnn /password:ppp /validate:no
```

Wenn die Option ***sessioninitiation*** in Ihrer Clientoptionsdatei (dsm.opt) auf *serveronly* gesetzt ist, können der Client-Setup-Assistent und der Scheduler-Service nicht die Authentifizierung mit dem IBM Spectrum Protect-Server einleiten. Zur Vermeidung dieses Problems müssen Sie beim Konfigurieren des Client-Schedulers mit dem Setup-Assistenten sicherstellen, dass das Kontrollkästchen IBM Spectrum Protect-Server zwecks Kennwortprüfung kontaktieren auf der Seite 'IBM Spectrum Protect-Authentifizierung' nicht ausgewählt ist.

Ein ähnliches Problem kann auftreten, wenn ein Verschlüsselungsschlüssel für Sicherungsoperationen erforderlich ist. In diesem Fall können Sie den Scheduler über die Befehlszeile ausführen (dsmc schedule), warten, bis eine geplante Sicherung gestartet wird, und den Verschlüsselungsschlüssel eingeben, wenn Sie dazu aufgefordert werden. Nachdem das Kennwort und der Verschlüsselungsschlüssel aktualisiert wurden, müssen Sie den Scheduler erneut starten.

5. Wenn der Scheduler zum ersten Mal auf einer Client-Workstation konfiguriert wird, kann sich der Scheduler-Service unter Umständen nicht beim Server authentifizieren, wenn der Server den Client-Scheduler kontaktiert, um einen Zeitplan auszuführen. Dies kann geschehen, wenn ***passwordaccess*** auf generate gesetzt ist, der IBM Spectrum Protect-Server sich hinter einer Firewall befindet und das verschlüsselte Kennwort nicht lokal gespeichert werden kann, bevor der Scheduler gestartet wird. Um dieses Problem zu beheben, müssen Sie den Scheduler von der Befehlszeile aus ausführen (dsmc schedule), warten, bis eine geplante Operation gestartet wird, und das Kennwort für Ihren Knoten eingeben, wenn Sie dazu aufgefordert werden.
6. Der Client kann keine Eingabeaufforderung für das Kennwort für den Verschlüsselungsschlüssel im Schedulermodus anzeigen. Wenn Sie die IBM Spectrum Protect-Datenverschlüsselung verwenden, müssen Sie einmal eine interaktive Erstsicherung ausführen, um den Verschlüsselungsschlüssel zu definieren, indem Sie die TCP/IP-Verbindung von der Client-Workstation zur Server-Workstation öffnen. Weitere Informationen zum Einrichten dieser Übertragung finden Sie unter **Methode 1**. Nachdem der Verschlüsselungsschlüssel definiert wurde, können Sie vom Server eingeleitete Sitzungen verwenden, um die Dateien mithilfe der Verschlüsselung zu sichern.

Wenn Sie die Option ***sessioninitiation*** auf *client* setzen, leitet der Client Sitzungen mit dem Server ein (**Methode 1**), indem er über den TCP/IP-Anschluss kommuniziert, der durch die *Server*option ***tcpport*** definiert ist. Dies ist der Standardwert. Mit der Zeitplanung über Serversystemanfrage kann der Client dazu aufgefordert werden, eine Verbindung zum Server herzustellen.

Bei Verwendung von IBM Spectrum Protect über eine Firewall hinweg im *Modus mit Bedienerführung* muss der IBM Spectrum Protect-Server den Kontakt zum Client herstellen. Dazu muss unter Umständen Software auf dem IBM Spectrum Protect-Server installiert werden, damit die Anforderung über die Firewall geleitet werden kann. Diese Software leitet die Serveranforderung über einen Socks-Anschluss auf der Firewall. Diese Methode wird als *Socksifizierung eines Systems* bezeichnet. Proxys werden nicht unterstützt, da sie nur bestimmte Arten von Übertragungsprotokollen (HTTP, FTP, GOPHER) weiterleiten. IBM Spectrum Protect-Übertragungen werden nicht durch Proxys weitergeleitet. Es ist wichtig zu wissen, dass der Client nach entsprechender Aufforderung eine neue Verbindung zum IBM Spectrum Protect-Server herstellt. Dies bedeutet, dass die oben beschriebene Firewall-Konfiguration die geeigneten Einstellungen aufweisen muss.

Zugehörige Tasks:
Scheduler konfigurieren
Zugehörige Verweise:
Sessioninitiation
Tcpadminport
Tcpport
Webports

IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren

Secure Sockets Layer (SSL) ermöglicht eine sichere Kommunikation auf SSL-Basis nach Industriestandard zwischen dem IBM Spectrum Protect-Client und -Server.

Informationen zu diesem Vorgang

Die folgenden Clientkomponenten unterstützen SSL:

- Befehlszeilenclient
- Verwaltungsbefehlszeilenclient
- Client-GUI
- Client-API

Nur abgehende Client/Server-Verbindungen unterstützen SSL. Ein Client der Version 8.1.2, der mit einer Server einer früheren Version kommuniziert, unterstützt SSL. Ein Client der Version 8.1.2, der mit einem Server der Version 8.1.2 kommuniziert, muss SSL verwenden. Eingehende Verbindungen (beispielsweise Clientakzeptor, vom Server eingeleitete Zeitplanverbindungen) unterstützen SSL nicht. Die Kommunikation zwischen Clients unterstützt SSL. Die Web-GUI unterstützt SSL nicht. Die Web-GUI wird bei der Kommunikation mit einem Server der Version 8.1.2 nicht mehr unterstützt.

Jeder IBM Spectrum Protect-Server, der für SSL aktiviert ist, muss über ein eindeutiges Zertifikat verfügen. Das Zertifikat kann einen der folgenden Typen aufweisen:

- Ein von IBM Spectrum Protect selbst signiertes Zertifikat.
- Ein von einer Zertifizierungsstelle (Certificate Authority - CA) ausgestelltes Zertifikat. Die Zertifizierungsstelle kann ein Unternehmen wie VeriSign oder Thawte oder eine interne Zertifizierungsstelle innerhalb Ihres Unternehmens sein.

Führen Sie die folgenden Schritte aus, um die SSL-Übertragung mit einem selbst signierten Zertifikat zu aktivieren:

1. Besorgen Sie sich das selbst signierte Zertifikat des IBM Spectrum Protect-Servers (cert256.arm). Verwenden Sie die Zertifikatsdatei cert.arm, wenn der Server nicht für die Verwendung von Transport Layer Security (TLS) 1.2 konfiguriert ist. Verwenden Sie andernfalls die Datei cert256.arm. Die Clientzertifikatsdatei muss mit der vom Server verwendeten Zertifikatsdatei identisch sein.
2. Konfigurieren Sie die Clients. Damit SSL verwendet werden kann, muss jeder Client das selbst signierte Serverzertifikat importieren.

   Importieren Sie das Zertifikat mithilfe des Dienstprogramms dsmcert.

3. Geht bei einem Ausfall des IBM Spectrum Protect-Servers das Zertifikat verloren, wird automatisch ein neues Zertifikat vom Server generiert. Jeder Client muss das neue Zertifikat abrufen und importieren.

Für Schnellzugriffspfaddetails für die Kommunikation zwischen einem Client der Version 8.1.2 und einem Server der Version 8.1.2 können Sie die Option SSLACCEPTCERTFROMSERV verwenden, um ein selbst signiertes Zertifikat automatisch zu akzeptieren. Ausführliche Informationen finden Sie in Standardsicherheitseinstellungen für den Client (Schnellzugriffspfad).

Führen Sie die folgenden Schritte aus, um die SSL-Übertragung mit einem von einer Zertifizierungsstelle signierten Zertifikat zu aktivieren:

1. Besorgen Sie sich das CA-Stammzertifikat.
2. Konfigurieren Sie die Clients. Damit SSL verwendet werden kann, muss jeder Client das selbst signierte Serverzertifikat importieren.

   Importieren Sie das Zertifikat mithilfe des Dienstprogramms dsmcert.

   Tipp: Nachdem Sie diesen Schritt ausgeführt haben, muss der Client das Stammzertifikat nicht erneut importieren, wenn der Server ein neues Zertifikat erhält, das von derselben CA signiert ist.
3. Wenn Sie den Client für Sichern/Archivieren im Rahmen der Wiederherstellung nach einem Katastrophenfall wiederherstellen, müssen Sie das SSL-Zertifikat erneut auf dem Server installieren. Wenn das Zertifikat nicht mehr vorhanden ist, müssen Sie ein neues Zertifikat anfordern. Sie müssen den Client nicht rekonfigurieren, wenn das neue Zertifikat von einer CA signiert wurde.

Windows-BetriebssystemeDas Dienstprogramm dsmcert wird vom Client für Sichern/Archivieren bereitgestellt und automatisch in `C:\Program Files\Tivoli\TSM\baclient` installiert.

Windows-BetriebssystemeFühren Sie die folgenden Schritte aus, bevor Sie das Serverzertifikat auf dem Client einrichten:

1. Öffnen Sie eine Eingabeaufforderung und wechseln Sie in das Verzeichnis des Clients für Sichern/Archivieren, beispielsweise: cd `"C:\Programme\Tivoli\TSM\baclient"`
2. Fügen Sie den Pfad für Binärprogramme und den Bibliothekspfad des GSKit der Umgebungsvariablen `PATH` hinzu. Beispiel:

   ```
   set PATH=C:\Programme\Common Files\Tivoli\TSM\api64\gsk8\bin\;
    C:\Programme\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
   ```

   Ausführliche Informationen zu GSkit-Bibliotheken finden Sie in Symbolischen Link für den Zugriff auf die neueste GSKit-Bibliothek erstellen und IBM Global Security Kit-Rückkehrcodes.

Als Nächstes müssen Sie das Serverzertifikat oder das CA-Stammzertifikat importieren.

Bei Verwendung eines selbst signierten Zertifikats

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeJeder IBM Spectrum Protect-Server generiert ein eigenes Zertifikat. Der festgelegte Dateiname des Zertifikats ist entweder cert.arm oder cert256.arm. Die Zertifikatsdatei wird auf der Server-Workstation im Serverinstanzverzeichnis gespeichert (z. B. /opt/tivoli/tsm/server/bin/cert256.arm). Falls die Zertifikatsdatei nicht vorhanden ist und Sie die Serveroption SSLTCPPORT oder SSLTCPADMINPORT angeben, wird die Zertifikatsdatei erstellt, wenn Sie den Server mit diesen Optionen erneut starten. IBM Spectrum Protect-Server der Version 6.3 (und höher) generieren Dateien namens cert256.arm und cert.arm. IBM Spectrum Protect-Server mit einer älteren Version als 6.3 generieren ausschließlich Zertifikatsdateien namens cert.arm. Sie müssen das Zertifikat auswählen, das als Standardwert auf dem Server festgelegt ist.

Windows-BetriebssystemeJeder IBM Spectrum Protect-Server generiert ein eigenes Zertifikat. Der festgelegte Dateiname des Zertifikats ist entweder cert.arm oder cert256.arm. Die Zertifikatsdatei wird auf der Server-Workstation im Serverinstanzverzeichnis gespeichert (z. B. C:\Programme\tivoli\tsm\server1\cert256.arm). Falls die Zertifikatsdatei nicht vorhanden ist und Sie die Serveroption SSLTCPPORT oder SSLTCPADMINPORT angeben, wird die Zertifikatsdatei erstellt, wenn Sie den Server mit diesen Optionen erneut starten. IBM Spectrum Protect-Server der Version 6.3 (und höher) generieren Dateien namens cert256.arm und cert.arm. IBM Spectrum Protect-Server mit einer älteren Version als 6.3 generieren ausschließlich Zertifikatsdateien namens cert.arm. Sie müssen das Zertifikat auswählen, das als Standardwert auf dem Server festgelegt ist.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

Windows-BetriebssystemeFühren Sie die folgenden Schritte aus, um die SSL-Verbindung zu einem Server einzurichten:

1. Besorgen Sie sich das Zertifikat beim Serveradministrator.
2. Importieren Sie das Zertifikat mit dem folgenden Befehl in die Schlüsseldatenbank des Clients:

   ```
   dsmcert -add -server <Servername> -file <Pfad_zu_cert256.arm>
   ```

Bei Verwendung eines Zertifikats von einer Zertifizierungsstelle

Wenn das Zertifikat von einer Zertifizierungsstelle (Certificate Authority - CA) wie VeriSign oder Thawte ausgestellt wurde, ist der Client für SSL bereit und Sie können die folgenden Schritte überspringen.
Die Liste der vorinstallierten Stammzertifikate externer Zertifizierungsstellen finden Sie in Stammzertifikate von Zertifizierungsstellen.
Wenn das Zertifikat nicht von einer der anerkannten Zertifizierungsstellen ausgestellt wurde, führen Sie die folgenden Schritte aus:

1. Besorgen Sie sich das Stammzertifikat der Zertifizierungsstelle, die das Zertifikat signiert hat.
2. Importieren Sie das Zertifikat mit dem folgenden Befehl in die Schlüsseldatenbank des Clients:

```
dsmcert -add -server <Servername> -file <Pfad_zu_cert256.arm>
```

Wichtig:

1. Die Schlüsseldatenbank wird mit einem automatisch generierten Pseudokennwort verschlüsselt. Das Kennwort wird automatisch in der Stashdatei (`dsmcert.sth`) gespeichert. Die Stashdatei wird vom Client für Sichern/Archivieren verwendet, um das Kennwort für die Schlüsseldatenbank abzurufen.
2. Der Schlüsseldatenbankdatei des Clients können mehrere Serverzertifikate hinzugefügt werden, sodass der Client eine Verbindung zu verschiedenen Servern herstellen kann. Ebenso können der Schlüsseldatenbank des Clients mehrere CA-Stammzertifikate hinzugefügt werden.
3. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWenn Sie die vorhergehenden Befehle nicht im Verzeichnis des Clients für Sichern/Archivieren ausführen, müssen Sie `dsmcert.kdb` und `dsmcert.sth` in dieses Verzeichnis kopieren.
4. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeStandardmäßig ist der Root Eigner der lokalen Schlüsseldatenbankdateien und nur er verfügt über Berechtigungen. Andere Benutzer können diese Dateien nicht lesen. Wenn Sie planen, den Client als Benutzer ohne Rootberechtigung auszuführen, müssen Sie die Berechtigungen aktualisieren. Führen Sie beispielsweise den folgenden Befehl aus, um allen Benutzern und Gruppen Lesezugriff zu erteilen:

   ```
   # chmod go+r dsmcert.*
   ```

5. Windows-BetriebssystemeWenn Sie die vorhergehenden Befehle nicht im Verzeichnis des Clients für Sichern/Archivieren ausführen, müssen Sie `dsmcert.kdb` und `dsmcert.sth` in dieses Verzeichnis kopieren.
6. Aus Leistungsgründen sollten Sie SSL nur bei Bedarf für Sitzungen verwenden. Ein Client der Version 8.1.2, der mit einem Server der Version 8.1.2 kommuniziert, muss SSL verwenden. SSL No (der Standardwert) gibt an, dass keine Verschlüsselung verwendet wird, wenn Daten zwischen dem Client und einem Server einer Version vor Version 8.1.2 übertragen werden. Wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, gibt der Standardwert No an, dass Objektdaten nicht verschlüsselt werden. Alle anderen Informationen werden verschlüsselt, wenn der Client mit dem Server kommuniziert. Wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, gibt der Wert Yes an, dass SSL zum Verschlüsseln aller Informationen, einschließlich Objektdaten, verwendet wird, wenn der Client mit dem Server kommuniziert. Sie könnten dem IBM Spectrum Protect-Serversystem für die höheren Anforderungen zusätzliche Prozessorressourcen hinzufügen.
7. Damit ein Client eine Verbindung zu einem Server herstellen kann, der Transport Layer Security (TLS) Version 1.2 verwendet, muss das Zertifikat den Signaturalgorithmus SHA-1 oder einen strengeren Algorithmus aufweisen. Falls Sie ein selbst signiertes Zertifikat verwenden, müssen Sie das Zertifikat cert256.arm verwenden. Ihr IBM Spectrum Protect-Administrator muss möglicherweise das Standardzertifikat auf dem IBM Spectrum Protect-Server ändern.

Weitere ausführliche Informationen für einen Client der Version 8.1.2, der mit einem Server der Version 8.1.1 oder früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Versionen kommuniziert

Nachdem das Serverzertifikat der Clientschlüsseldatenbank hinzugefügt wurde, fügen Sie die Option SSL Yes der Clientoptionsdatei hinzu und aktualisieren den Wert der Option TCPPORT. Es ist wichtig zu verstehen, dass der Server normalerweise auf einem anderen Anschluss für SSL-Verbindungen eingerichtet wird. In anderen Worten: Auf dem Server werden zwei Anschlüsse geöffnet:

1. Ein Anschluss akzeptiert normale Clientverbindungen ohne SSL.
2. Ein anderer Anschluss akzeptiert nur SSL-Verbindungen.

Sie können mit einem SSL-fähigen Client keine Verbindung zu einem Nicht-SSL-Anschluss herstellen, und umgekehrt gilt dies ebenso.

Ist der Wert von tcpport falsch, kann der Client keine Verbindung zum Server herstellen. Geben Sie in der Option tcpport die richtige Anschlussnummer an.

Wenn Sicherheitsprotokolle inaktiviert werden sollen, die nicht so sicher wie TLS 1.2 sind, fügen Sie der Clientoptionsdatei die Option SSLDISABLELEGACYtls yes hinzu oder wählen Sie in der Java™-GUI das Kontrollkästchen TLS 1.2 oder höher erforderlich auf der Registerkarte Übertragung des Profileditors aus. Wenn TLS 1.2 oder höher als erforderlich angegeben wird, können Attacken durch Schadprogramme besser verhindert werden.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeSymbolischen Link für den Zugriff auf die neueste GSKit-Bibliothek erstellen
  Sie können einen symbolischen Link erstellen, um von dem Verzeichnis, in dem die frühere Version von GSKit installiert ist, auf die Position zu verweisen, an der sich die neuesten GSKit-Bibliotheken auf dem System befinden.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeStammzertifikate von Zertifizierungsstellen
  Der Client für Sichern/Archivieren verfügt über eine Liste von Stammzertifikaten für eine Reihe bekannter Zertifizierungsstellen.

Zugehörige Verweise:

Ssl
Sslfipsmode

Symbolischen Link für den Zugriff auf die neueste GSKit-Bibliothek erstellen

Sie können einen symbolischen Link erstellen, um von dem Verzeichnis, in dem die frühere Version von GSKit installiert ist, auf die Position zu verweisen, an der sich die neuesten GSKit-Bibliotheken auf dem System befinden.

Informationen zu diesem Vorgang

Wenn Sie DB2 for Linux, UNIX, and Windows unter UNIX und Linux installieren, werden auch lokale GSKit-Bibliotheken installiert. Diese Bibliotheken sind in <DB2-Installationspfad>/lib64/gskit_db2 oder <DB2-Installationspfad>/lib32/gskit_db2 gespeichert. Unter Windows ist die Standardposition C:\Programme\ibm\gsk8.

Während der Installation anderer IBM Produkte, wie beispielsweise IBM Spectrum Protect, wird unter Umständen eine weitere Kopie der GSKit-Bibliotheken installiert. Abhängig von dem Produkt kann es sich bei diesen Bibliotheken um lokale GSKit-Bibliotheken oder globale GSKit-Bibliotheken handeln. Wenn DB2 for Linux, UNIX, and Windows und ein anderes IBM Produkt, das GSKit-Bibliotheken umfasst, auf demselben System installiert werden, kann es zu Interoperabilitätsproblemen kommen. Diese Interoperabilitätsprobleme können auftreten, da GSKit nur Bibliotheken aus einer einzigen GSKit-Quelle in einem einzelnen Prozess zulässt. Die Interoperabilitätsprobleme können zu unvorhersehbarem Verhalten und Laufzeitfehlern führen.

Um sicherzustellen, das eine einzige Quelle für GSKit-Bibliotheken verwendet wird, kann das Konzept symbolischer Links verwendet werden. Im Rahmen einer Erstinstallation von DB2 for Linux, UNIX, and Windows erstellt das Installationsprogramm einen symbolischen Link <DB2-Installationspfad>/lib64/gskit oder <DB2-Installationspfad>/lib32/gskit zu <DB2-Installationspfad>/lib64/gskit_db2 oder <DB2-Installationspfad>/lib32/gskit_db2. Diese symbolischen Links sind die Standardpositionen, aus denen die GSKit-Bibliotheken geladen werden. Für Produkte, die im Produktpaket von DB2 for Linux, UNIX, and Windows vorhanden sind, und den symbolischen Link vom Standardverzeichnis in das Bibliotheksverzeichnis einer anderen Kopie von GSKit ändern, muss sichergestellt werden, dass das neu installierte GSKit dieselbe oder eine höhere Version hat. Diese Einschränkung gilt unabhängig davon, ob es sich um globale oder lokale Bibliotheken handelt. Während eines Upgrades oder Updates von DB2 for Linux, UNIX, and Windows wird der symbolische Link beibehalten. Wenn die neu installierte Kopie über einen symbolischen Link zur Standardposition verfügt, wird der symbolische Link, der der älteren Installationskopie zugeordnet ist, beibehalten. Wenn die neu installierte Kopie über keinen symbolischen Link zur Standardposition verfügt, wird der symbolische Link, der der neueren Installationskopie zugeordnet ist, beibehalten.

Es bestehen bestimmte Einschränkungen, da sich der symbolische Link <DB2-Installationspfad>/lib64/gskit oder <DB2-Installationspfad>/lib32/gskit in dem Pfad der Installationskopie von DB2 for Linux, UNIX, and Windows befindet. Wenn beispielsweise zwei oder mehr Instanzen für eine DB2-Kopie erstellt werden, haben Änderungen an dem symbolischen Link Auswirkungen auf alle Instanzen.

Sie können auch ein Domino-Server-GSKit auf ähnliche Weise ändern. Ein Domino-Server verfügt über nicht über einen GSKit-Ordner, aber über die Ordner C und N sowie eine Bibliothek libgsk8iccs_64.so. Sie können zunächst Softlinks für diese Ordner und Dateien erstellen, um auf die entsprechenden Ordner im GSKit-Paket zu verweisen, in denen der IBM Spectrum Protect-Client für Sichern/Archivieren der Version 8.1.2 installiert ist; gehen Sie dazu wie folgt vor:

- ln -s /usr/local/ibm/gsk8_64/lib64/C /opt/ibm/lotus/notes/90010/zlinux
- ln -s /usr/local/ibm/gsk8_64/lib64/N /opt/ibm/lotus/notes/90010/zlinux
- ln -s /usr/local/ibm/gsk8_64/lib64/libgsk8iccs_64.so /opt/ibm/lotus/notes/90010/zlinux

Ändern Sie im nächsten Schritt das Kennwort des DPD-Knotens in domdsmc CHANGEADSMPwd tvt1054_domnote2 tvt1054_domnote2 tvt1054_domnote2. Führen Sie abschließend domdsmc query adsm aus.

Vorgehensweise

1. Erstellen Sie einen symbolischen Link unter Windows, wenn Sie über Administratorberechtigungen verfügen. Benennen Sie die DB2-Kopie von GSKit im Verzeichnis lib64, das sich an der Standardposition C:\Programme\ibm\gsk8 befindet, um. Starten Sie eine DOS-Shell, navigieren Sie zu der Position von DB2-GSKit und benennen Sie das Verzeichnis wie folgt um:

   ```
   cd C:\Programme\ibm\gsk8

   rename lib64 lib64-db2
   ```

2. Erstellen Sie einen symbolischen Link an der Position der DB2-Kopie von GSKit und verweisen Sie auf die Position der TSM-Kopie von GSKit, indem Sie in der DOS-Shell die folgenden Befehle ausführen. Navigieren Sie zu der Position der DB2-Kopie von GSKit und erstellen Sie dann wie folgt den symbolischen Link:

   ```
   cd C:\Programme\ibm\gsk8

   mklink /d lib64 "c:\Programme\Common Files\Tivoli\TSM\api64\gsk8\lib64"
   ```

3. Starten Sie DB2 erneut, damit die Änderungen wirksam werden. Beim Start lädt DB2 GSKit aus der neuen Position, die auf die IBM Spectrum Protect-Kopie von GSKit verweist. Geben Sie in der DB2-Eingabeaufforderung die folgenden Befehle ein:

   ```
   db2stop
   ```

```
db2start
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Stammzertifikate von Zertifizierungsstellen

Der Client für Sichern/Archivieren verfügt über eine Liste von Stammzertifikaten für eine Reihe bekannter Zertifizierungsstellen.

Die folgende Liste enthält die Stammzertifikate für eine Reihe bekannter Zertifizierungsstellen, die mit dem Client geliefert werden:

- Entrust.net Global Secure Server Certification Authority
- Entrust.net Global Client Certification Authority
- Entrust.net Client Certification Authority
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 2 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 1 Public Primary Certification Authority - G3
- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA
- RSA Secure Server Certification Authority

Wenn Sie Zertifikate verwenden wollen, die von einer anderen Zertifizierungsstelle ausgegeben wurden, müssen Sie das Stammzertifikat dieser Zertifizierungsstelle im Rahmen der Clientkonfiguration auf allen Clients installieren.

AIX-BetriebssystemeWindows-BetriebssystemeLinux-Betriebssysteme

System für die journalbasierte Sicherung konfigurieren

Bevor Sie journalbasierte Sicherungen ausführen können, müssen Sie den Journaldämon (Linux) oder den Journalsteuerkomponentenservice (Windows) installieren und konfigurieren.

- Windows-BetriebssystemeJournalsteuerkomponentenservice konfigurieren
  Die journalbasierte Sicherung kann für alle Windows-Clients verwendet werden. Wenn der Journalsteuerkomponentenservice installiert und aktiv ist, führt der Befehl incremental automatisch eine journalbasierte Sicherung der ausgewählten Dateisysteme aus, die vom Journalsteuerkomponentenservice überwacht werden.
- AIX-BetriebssystemeLinux-BetriebssystemeKonfiguration des Journaldämons
  Die journalbasierte Sicherung wird durch die Installation und Konfiguration des IBM Spectrum Protect-Journaldämons ermöglicht.

Windows-Betriebssysteme

Journalsteuerkomponentenservice konfigurieren

Die journalbasierte Sicherung kann für alle Windows-Clients verwendet werden. Wenn der Journalsteuerkomponentenservice installiert und aktiv ist, führt der Befehl incremental automatisch eine journalbasierte Sicherung der ausgewählten Dateisysteme aus, die vom Journalsteuerkomponentenservice überwacht werden.

Informationen zu diesem Vorgang

Die journalbasierte Sicherung wird durch die Installation und Konfiguration des IBM Spectrum Protect-Journalservice ermöglicht. Sie können den Journalservice mit dem Setup-Assistenten der GUI oder mit dem Befehl dsmcutil installieren. Die Basiskonfiguration des Journalservice kann mit dem Setup-Assistenten der GUI erfolgen, die erweiterte Konfiguration kann durch Editieren der Konfigurationsdatei für den Journalservice, tsmjbbd.ini, ausgeführt werden.
Tipp: Die Standardposition für die Konfigurationsdatei für den Journalservice ist C:\Programme\Tivoli\TSM\baclient\tsmjbbd.ini. Wenn Sie den Journalsteuerkomponentenservice zum ersten Mal konfigurieren und noch keine Kopie von tsmjbbd.ini vorhanden ist, kopieren Sie die Musterdatei C:\Programme\Tivoli\TSM\config\tsmjbbd.ini.smp nach C:\Programme\Tivoli\TSM\baclient\tsmjbbd.ini.

Soll dieser Service mit dem Setup-Assistenten der Client-Java™GUI installiert und konfiguriert werden, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Öffnen Sie im Hauptfenster das Menü Dienstprogramme und wählen Sie Setup-Assistent aus.
2. Wählen Sie das Kontrollkästchen Hilfe zum Konfigurieren der Journalsteuerkomponente aus.
3. Wählen Sie die Task aus, die die ausgeführt werden soll. Sie können eine neue Journalsteuerkomponente installieren, eine zuvor installierte Journalsteuerkomponente aktualisieren oder eine zuvor installierte Journalsteuerkomponente aus dem System entfernen.
4. Füllen Sie jede Anzeige im Assistenten aus und klicken Sie zur Fortsetzung auf die Schaltfläche Weiter. Um zu einer vorherigen Anzeige zurückzugehen, klicken Sie auf die Schaltfläche Zurück. Um Hilfetext für die Anzeige aufzurufen, klicken Sie auf die Schaltfläche Hilfe.

Ergebnisse

Die Konfigurationseinstellungen für den Journalservice sind in der Journalkonfigurationsdatei tsmjbbd.ini gespeichert. Diese Datei kann mithilfe des Setup-Assistenten der GUI installiert und konfiguriert oder manuell editiert werden.

Führen Sie die folgenden Schritte aus, um Mehrfachjournalservices zu definieren:

1. Erstellen und definieren Sie für jeden Journalservice, der installiert werden soll, eine separate Journalkonfigurationsdatei (tsmjbbd.ini). Jede Konfigurationsdatei muss einen anderen Wert für JournalPipe angeben und muss zusätzlich verschiedene Laufwerke für die Journalführung angeben, damit sich die beiden Services nicht gegenseitig stören. Mehrere Journalservices, die eine Journalführung für dasselbe Laufwerk ausführen, verursachen Probleme. Die unterschiedlichen Services versuchen, in dieselbe Journaldatenbank zu schreiben, sofern dies nicht durch Angabe unterschiedlicher Journalverzeichnisse in den verschiedenen Konfigurationsdateien speziell überschrieben wird.
2. Installieren Sie die Mehrfachjournalservices mit dem Tool dsmcutil.exe. Verwenden Sie für jeden Service unverkennbare Namen und geben Sie die Option /JBBCONFIGFILE an, um die Datei tsmjbbd.ini zu identifizieren, die für diese bestimmte Journalinstanz verwendet werden soll. Zum Beispiel:

   ```
   dsmcutil install journal /name:"TSM-Journalservice 1" /JBBCONFIGFILE:c:\journalconfig\tsmjbbd1.ini

   dsmcutil install journal /name:"TSM-Journalservice 2" /JBBCONFIGFILE:d:\journalconfig\tsmjbbd2.ini
   ```

   Anmerkung: Im UNC-Format muss der jbbconfigfile-Pfad einen Laufwerkbuchstaben enthalten (UNC - Universal Naming Convention, allgemeine Namenskonvention). In dem folgenden Beispiel im UNC-Format enthält der Pfad den Laufwerkbuchstaben D$: \\computer7\D$\journalconfig\tsmjbbd1.ini
3. Jetzt können unterschiedliche Sicherungsclients (basierend auf der jeweils verwendeten Datei dsm.opt) zu dem gewünschten Journalservice eine Verbindung herstellen, indem sie die korrekte Option JournalPipe in der entsprechenden Datei dsm.opt angeben, die der Journalserviceeinstellung JournalPipe entspricht.

Anmerkung:

1. Jede Journalserviceinstanz ist nur einem einzigen Knotennamen des Clients für Sichern/Archivieren zugeordnet. Eine Änderung der Zuordnung erfordert einen Neustart des Journalservice, damit die neue Zuordnung erkannt wird.
2. Sie können keine Netzdateisysteme und entfernbaren Dateisysteme verwenden.

Konfigurationseinstellungen, die Sie anwenden, wenn der Journalservice gestartet wird, und alle Änderungen, die während der Ausführung des Journalservice vorgenommen werden, werden angewendet, ohne dass der Service erneut gestartet werden muss. Dies gilt auch für die Journalausschlussliste. Einige Einstellungen für Journaled File Systems werden jedoch erst wirksam, wenn das Dateisystem in den Status "offline" und anschließend wieder in den Status "online" versetzt wird.

Dateisysteme können in den Status 'online' (hinzugefügt) oder 'offline' (entfernt) versetzt werden, ohne dass der Journalservice gestoppt und erneut gestartet werden muss. Sie können ein Dateisystem in den Status 'offline' bringen, indem Sie es aus der Liste der Journaled File Systems in der Journalkonfigurationsdatei `tsmjbbd.ini` entfernen oder indem Sie den Journalservice herunterfahren. Sie können ein Dateisystem wieder in den Status 'online' bringen, indem Sie es zur Liste der Journaled File Systems in der Journalkonfigurationsdatei `tsmjbbd.ini` hinzufügen oder indem Sie den Journalservice starten (erneut starten).

Achtung: Wenn Sie ein Dateisystem in den Status 'offline' versetzen, ohne den Wert für PreserveDbOnExit auf 1 zu setzen, wird die Journaldatenbank des Journaled File System gelöscht. PreserveDbOnExit=1 gibt an, dass die Datenbank des Journaled File System nicht gelöscht wird, wenn das Journaled File System in den Status 'offline' versetzt wird. Die Datenbank hat immer noch Gültigkeit, wenn das Journaled File System wieder in den Status 'online' versetzt wird.
Nachfolgend steht die Syntax für Zeilengruppen und Zeilengruppeneinstellungen:

Syntax für Zeilengruppen:
    [*Zeilengruppenname*]
Syntax für Zeilengruppeneinstellungen:
    Zeilengruppeneinstellung=Wert

Anmerkung:

1. Sie können Kommentare in der Datei angeben, indem Sie die Zeile mit einem Semikolon beginnen.
2. Bei Namen von Zeilengruppen und Werten muss die Groß-/Kleinschreibung nicht beachtet werden muss.

3. Numerische Werte können hexadezimal angegeben werden, indem dem Wert die Zeichen `0x` vorangestellt werden; andernfalls wird er als Dezimalwert interpretiert.
4. Es besteht keine Korrelation zwischen diesen Einstellungen und den Einstellungen in der Optionsdatei für den Client für Sichern/Archivieren. Beim Journalservice handelt es sich um einen vollständig unabhängigen Prozess, der keine Optionen für den Client für Sichern/Archivieren verarbeitet.

- Windows-BetriebssystemeZeilengruppe 'JournalSettings' (Windows)
  Einstellungen unter dieser Zeilengruppe sind global und gelten für den gesamten Journalservice.
- Windows-BetriebssystemeZeilengruppe JournalExcludeList
  Die Liste der Exclude-Anweisungen filtert Änderungen und verhindert, dass manche Änderungen in der Journaldatenbank aufgezeichnet werden. Änderungen an Objekten, die mit den Anweisungen in dieser Zeilengruppe übereinstimmen, werden ignoriert und nicht in der Journaldatenbank aufgezeichnet.
- Windows-BetriebssystemeZeilengruppe JournaledFileSystemSettings
  Einstellungen unter dieser Zeilengruppe gelten für jedes angegebene Journaled File System, sofern sie nicht für einzelne Dateisysteme in einer Überschreibungszeilengruppe überschrieben sind.
- Windows-BetriebssystemeZeilengruppen überschreiben
  Jede beliebige Einstellung in der Zeilengruppe ***JournaledFileSystemSettings*** kann für ein bestimmtes Journaled File System überschrieben werden, indem eine Überschreibungszeilengruppe erstellt wird.

Zugehörige Konzepte:
Journalbasierte Sicherung
Windows-Betriebssysteme

Zeilengruppe 'JournalSettings' (Windows)

Einstellungen unter dieser Zeilengruppe sind global und gelten für den gesamten Journalservice.

Die Zeilengruppe `JournalSettings` hat folgende Syntax:

Syntax für die Zeilengruppe `JournalSettings`:
```
[JournalSettings]
```
Syntax für Zeilengruppeneinstellungen:
JournalSettings=*Wert*

Sie können folgende Werte für `JournalSettings` angeben:

JournalPipe=*Pipename*
Gibt den Namen der Pipe des Sitzungsmanagers des Journalservice an, zu dem die Sicherungsclients anfänglich eine Verbindung aufbauen, wenn sie eine journalbasierte Sicherungssitzung herstellen. Diese Einstellung wird in Zusammenhang mit der Sicherungsclientoption desselben Namens verwendet. Der Standardpipename ist `\\.\pipe\jnlSessionMgr1`. Beispielsweise in dsm.opt:

```
JournalPipe \\.\pipe\jnlSessionMgr1
```

In `tsmjbbd.ini` unter der Zeilengruppe [JournalSettings]:

```
JournalPipe=\\.\pipe\jnlSessionMgr1
```

Anmerkung: Derselbe Pipename muss vom Client mithilfe der Option `JournalPipe` angegeben werden.

`NlsRepos`
Gibt das Repository für die Landessprachenunterstützung an, das der Journalservice für das Generieren von Nachrichten verwendet. Da der Journalservice nicht interaktiv ist, gilt dies nur für Nachrichten, die in das Journalfehlerprotokoll geschrieben werden. Der Standardwert ist `dscameng.txt`. Beispiel:

```
NlsRepos=dscenu.txt
```

`ErrorLog`
Gibt die Protokolldatei an, in die die vom Journalservice generierten, ausführlichen Nachrichten geschrieben werden. Beachten Sie, dass weniger ausführliche Fehlernachrichten und Informationsnachrichten außerdem auch in das Windows-Anwendungsereignisprotokoll geschrieben werden. Der Standardwert ist `jbberror.log`. Zum Beispiel:

```
ErrorLog=jbberror.log
```

Im UNC-Format (Universal Naming Convention) muss der Pfad einen Laufwerkbuchstaben enthalten. In dem folgenden Beispiel im UNC-Format enthält der Pfad den Laufwerkbuchstaben D$: \\computer7\D$\temp\jbberror.log.

`JournalDir`
Gibt das Verzeichnis an, in das Journaldatenbankdateien geschrieben werden und in dem sie gespeichert sind. Das Standardverzeichnis ist das Installationsverzeichnis des Journalservice. Sie können für jedes Dateisystem, das aufgezeichnet wird, eine andere Journalposition angeben. Dies ist bei einer Clusterumgebung hilfreich, da die Position des Journals für jede Workstation im Cluster, die den Journalservice ausführt, im Zugriff sein muss. In der Regel befindet sich das Journal für lokale Ressourcen, die aufgezeichnet werden, an derselben Position und das Journal für gemeinsame Clusterressourcen (die von Workstation zu Workstation verschoben werden können) befindet sich auf der gemeinsamen Ressource, um sicherzustellen, dass es für beide Workstations im Zugriff ist.

Standardmäßig gilt diese Einstellung für alle Journaled File Systems; sie kann jedoch durch eine Überschreibungszeilengruppe für jedes Journaled File System überschrieben werden. Wenn der Standardwert ein vollständig qualifizierter Pfad ist (zum Beispiel c:\tsmjournal), werden alle Journaldatenbankdateien in das angegebene Verzeichnis geschrieben. Wenn der Standardwert keinen Laufwerkbuchstaben angibt (zum Beispiel \tsmjournal), werden die Journaldatenbankdateien für jedes Journaled File System in das angegebene Verzeichnis in jedem Journaled File System geschrieben.

Im UNC-Format (Universal Naming Convention) muss der Pfad einen Laufwerkbuchstaben enthalten. In dem folgenden Beispiel im UNC-Format enthält der Pfad den Laufwerkbuchstaben D$: \\computer7\D$\temp\tsmjournal.

Es folgt ein Beispiel für die Konfiguration der Zeilengruppe:

```
[JournalSettings]
;
; Alle Ressourcen an einer Position speichern, wenn nicht
; durch eine Überschreibungszeilengruppe überschrieben
;
JournalDir=c:\tsmjournal
;
;
[JournaledFileSystemSettings.D:\]
;
; Journal für d: befindet sich nur an folgender Position
;
  JournalDir=d:\tsmjournal
```

Anmerkung: Änderungen an dieser Einstellung werden erst wirksam, wenn die Journaled File Systems in den Status 'online' versetzt werden.

 Windows-Betriebssysteme

Zeilengruppe JournalExcludeList

Die Liste der Exclude-Anweisungen filtert Änderungen und verhindert, dass manche Änderungen in der Journaldatenbank aufgezeichnet werden. Änderungen an Objekten, die mit den Anweisungen in dieser Zeilengruppe übereinstimmen, werden ignoriert und nicht in der Journaldatenbank aufgezeichnet.

Anmerkung:

1. Das Ausschließen von Dateien aus dem Journal hat keine Bedeutung für diejenigen Dateien, die vom Sicherungsclient ausgeschlossen werden, außer dass verhindert wird, dass während einer journalbasierten Sicherung die Dateien zur Verarbeitung an den Sicherungsclient gesendet werden. Eine Datei, die nicht aus dem Journal ausgeschlossen ist, sollte dennoch vom Client für Sichern/Archivieren ausgeschlossen werden, wenn es eine übereinstimmende Exclude-Anweisung in der Clientoptionsdatei gibt.
2. Der Journalservice bietet nur eine Teilmenge der Funktion INCLUDE/EXCLUDE, die vom Client für Sichern/Archivieren zur Verfügung gestellt wird. Der Journalservice unterstützt keine Anweisungen INCLUDE und auch nicht die Option *exclude.dir*.

Es besteht keine Korrelation zwischen der Ausschlussliste des Journals und der Ausschlussliste des Clients für Sichern/Archivieren.

Die folgenden Beispiele zeigen äquivalente Journal-Exclude-Anweisungen:

```
dsm.opt: tsmjbbd.ini

EXCLUDE c:\testdir\...\* c:\testdir\*
EXCLUDE.DIR c:\testdir\test* c:\testdir\test*\*
```

Die folgenden Metazeichen für die Mustererkennung werden unterstützt:

%
: Stimmt mit genau einem einzigen Zeichen überein.

*
: Entspricht null oder mehr Zeichen.

%EnvVar%
: Erweitert die Umgebungsvariable.

Nachfolgend steht ein Beispiel für die Syntax einer Exclude-Anweisung:

```
  [JournalExcludeList]
    %SystemRoot%\System32\Config\*
  C:\Programme\Tivoli\TSM\baclient\adsm.sys\*
    %TEMP%\*
    %TMP%\*
    c:\excludedir\*
    c:\dir1\excludefile
    *.:\*.tmp
```

Anmerkung: Die Anweisung `c:\excludedir\*` stimmt mit der gesamten Baumstruktur überein, einschließlich Unterverzeichnissen und Dateien.

 Windows-Betriebssysteme

Zeilengruppe JournaledFileSystemSettings

Einstellungen unter dieser Zeilengruppe gelten für jedes angegebene Journaled File System, sofern sie nicht für einzelne Dateisysteme in einer Überschreibungszeilengruppe überschrieben sind.

Nachfolgend wird die Syntax für die Zeilengruppe JournaledFileSystemSettings gezeigt:

Syntax für die Zeilengruppe ***JournaledFileSystemSettings***:
[*JournaledFileSystemSettings*]
Syntax für Zeilengruppeneinstellungen:
JournaledFileSystemSetting=*Wert*

Sie können folgende Werte für ***JournaledFileSystemSettings*** angeben:

DirNotifyBufferSize
Gibt die Größe des Puffers zum Aufzeichnen von Änderungsbenachrichtigungen für ein bestimmtes Journaled File System an. Sie müssen diesen Wert für Journaled File Systems, die Änderungsaktivitäten in großem Umfang generieren, unter Umständen vergrößern. Die Puffergröße wird durch die Speicherkapazität begrenzt. Der Standardwert ist 16 KB.
JournaledFileSystems
Gibt eine Liste der aufzuzeichnenden Dateisysteme an (die einzelnen Einträge werden durch Leerzeichen voneinander getrennt). Es werden vollständige Dateisystemspezifikationen und virtuelle Windows-Zusammenführungen unterstützt. Es gibt keinen Standardwert. Sie müssen mindestens ein Journaled File System angeben, damit der Service ausgeführt wird. Journaled File Systems können online hinzugefügt oder entfernt werden, ohne dass der Service erneut gestartet werden muss. Zum Beispiel:

```
JournaledFileSystems=c: d:
```

JournalDbSize
Gibt die maximale Größe der Journaldatenbank an. Die Größe der Journaldatenbank wird in Byte angegeben. Der Wert Null (0) gibt an, dass die Datenbankgröße nur von der Kapazität des Dateisystems, das die Journaldatenbank enthält, begrenzt wird. Der Standardwert ist `0` (unbegrenzt). Zum Beispiel:

```
JournalDBSize=0x10000000
```

NotifyBufferSize
Gibt die Größe des Speicherpuffers an, der Änderungsbenachrichtigungen des Dateisystems für ein bestimmtes Journaled File System empfängt. Sie müssen diesen Wert für Journaled File Systems, die Änderungsaktivitäten in großem Umfang generieren, unter Umständen vergrößern. Die Puffergröße wird durch die Speicherkapazität begrenzt. Der Standardwert ist 32 KB. Zum Beispiel:

```
NotifyBufferSize=0x00008000
```

NotifyFilter
Gibt an, welche Aktionen bei der Dateisystemänderung Benachrichtigungen für den Journalservice generieren. ***NotifyFilter*** gilt für Datei- und Verzeichnisänderungen. Änderungen von Verzeichnisnamen, z. B. Löschungen und Erstellungen, werden unabhängig vom Filterwert immer aufgezeichnet. Es können mehrere Aktionen überwacht werden, indem Werte kombinieret werden. Der Standardwert ist `0x11F` (Änderungen für Datei- und Verzeichnisname, Attribute, Größe, letzte Schreiboperation und Sicherheit). Sie können auch den Assistenten für die IBM Spectrum Protect-Journalsteuerkomponente verwenden, um eine oder alle dieser Aktionen überwachen zu lassen.
Unterstützte Werte sind:

Werttyp	Dezimal	Hexadezimal
Dateiname	1	0x001
Verzeichnisname	2	0x002
Attribut	4	0x004
Dateigröße*	8	0x008
Datum/Uhrzeit der letzten Schreiboperation*	16	0x010
Datum/Uhrzeit des letzten Zugriffs	32	0x020
Erstellungszeitpunkt	64	0x040
Sicherheit (ACL)	256	0x100

Der Stern (*) gibt an, dass Benachrichtigungen so lange verzögert werden, bis der Plattenschreib-Cache abgebrochen wird. Unter Namensänderungen versteht man das Erstellen, Löschen oder Umbenennen von Objekten.

Beispiel:

```
NotifyFilter=0x107
```

Einstellung PreserveDbOnExit
Diese Einstellung ermöglicht, dass ein Journal gültig bleibt, wenn ein Journaled File System in den Status 'offline' und danach wieder in den Status 'online' versetzt wird. Dies ist hilfreich, um das Journal beim Systemwarmstart, bei Clusterübernahmen und bei der

Ressourcenversetzung beizubehalten.

Dateisysteme werden in den Status 'offline' versetzt, wenn der Journalservice gestoppt wird oder wenn das Dateisystem aus der Konfigurationsdatei entfernt wird. Dateisysteme werden wieder in den Staus 'online' versetzt, wenn der Journalservice gestartet wird oder wenn das Dateisystem der Konfigurationsdatei hinzugefügt wird.

Diese Einstellung ermöglicht, dass bei einer journalbasierten Sicherung die Verarbeitung fortgesetzt wird, wenn der Service erneut gestartet wird (oder das Dateisystem wieder in den Status 'online' versetzt wird), ohne eine vollständige Teilsicherung ausführen zu müssen.

Anmerkung: Jede Änderungsaktivität, die auftritt, während der Journalservice nicht aktiv ist (oder während das Dateisystem offline ist), wird nicht im Journal aufgezeichnet.

In einer Clusterumgebung können gemeinsame Ressourcen in andere Workstations im Cluster versetzt werden. Beim Journalservice, der auf jeder Workstation im Cluster ausgeführt wird, müssen diese gemeinsamen Ressourcen in der Liste mit Journaled File Systems aufgeführt sein. Der Journalservice auf der Workstation, die derzeit Eigner der Ressource ist, zeichnet die gemeinsame Ressource aktiv auf, während die anderen Journalservices auf den Workstations im Cluster, die nicht Eigner der Ressource sind, die Aufzeichnung so lange verzögern müssen, bis die Ressource wieder verfügbar ist (oder auf die betreffende Workstation versetzt wird). Die Konfigurationseinstellungen *deferFSMonStart*, *deferRetryInterval* und *logFSErrors* ermöglichen die Verzögerung für ein Dateisystem, bis das Dateisystem verfügbar und im Zugriff ist.

Der Wert 1 gibt an, dass die Datenbank des Journaled File System nicht gelöscht wird, wenn das Journaled File System in den Status 'offline' versetzt wird. Die Datenbank hat immer noch Gültigkeit, wenn das Journaled File System wieder in den Status 'online' versetzt wird. Dieser Wert sollte mit Vorsicht verwendet werden, da jede Änderungsaktivität für das Dateisystem, die auftritt, während das Journaled File System offline ist, nicht in der Journaldatenbank widergespiegelt wird. Mit der Standardeinstellung 0 wird die Journaldatenbank des Journaled File System gelöscht.

Anmerkung: Das Journal bleibt nur erhalten, wenn ein Journaled File System normal 'offline' gesetzt wird oder 'offline' gesetzt wird, wenn die Ressource nicht mehr verfügbar ist und Sie die Einstellung deferFsMonStart angeben. Wird ein Dateisystem aufgrund eines Fehlers wie beispielsweise eines Benachrichtigungspufferüberlaufs 'offline' gesetzt, wird das Journal gelöscht.
Nachfolgend steht ein Beispiel, bei dem die Journaldatenbank beim Verlassen nicht gelöscht wird:

```
[JournaledFileSystemSettings.D:\]
;
; Journal nicht löschen, wenn D:\ in den Status 'offline' versetzt wird
;
PreserveDbOnExit=1
```

Einstellung deferFSMonStart
Diese Einstellung verzögert in folgenden Fällen den Versuch, mit der Überwachung eines Dateisystems zu beginnen:

- Wenn das angegebene Journaled File System nicht gültig oder nicht verfügbar ist.
- Das Journalverzeichnis für das angegebene Journaled File System ist nicht im Zugriff oder kann nicht erstellt werden.

Die Überprüfung der Ressourcen findet in den Intervallen statt, die Sie über die Einstellung *deferRetryInterval* angeben.

Die Einstellung *deferFSMonStart* wird meistens in einer Clusterumgebung verwendet, in der gemeinsam genutzte Ressourcen von verschiedenen Workstations im Cluster verwendet werden können.

Der Wert 1 gibt an, dass die Einstellung aktiviert ist. Der Wert 0 gibt an, dass die Einstellung inaktiviert ist. Standardwert ist 0.

Einstellung deferRetryInterval
Diese Einstellung gibt das Zeitintervall in Sekunden an, nach dem ein verzögertes Dateisystem mit aktivierter Einstellung *deferRetryInterval* auf seine Verfügbarkeit geprüft und in den Status 'online' versetzt wird. Der Standardwert ist 1 Sekunde.

Einstellung logFSErrors
Diese Einstellung gibt an, ob Fehler, die beim Zugriff auf ein Journaled File System oder ein Journalverzeichnis erkannt werden, in der Datei `jbberror.log` und dem Ereignisprotokoll protokolliert werden.

Verwenden Sie die Einstellung *logFSErrors* zusammen mit der Einstellung *deferFSMonStart*, um zu verhindern, dass sehr viele Nachrichten *Dateisystem nicht verfügbar* protokolliert werden, wenn ein Journaled File System verzögert in den Status 'online' versetzt wird. Nur der erste Fehler, der zur Verzögerung des Dateisystems führt, wird protokolliert. Nachfolgende Fehler werden nicht protokolliert. Der Wert 1 gibt an, dass die Einstellung aktiviert ist. Der Wert 0 gibt an, dass die Einstellung inaktiviert ist.

Nachfolgend steht ein Beispiel, bei dem die Journalführung verzögert wird, bis die Dateisystemjournalverzeichnisse gültig sind:

```
[JournalSettings]
;
; Journaldateien in Verzeichnis auf jedem Journaled File System stellen
;
journalDir=\tsmjournal

[JournaledFileSystemSettings]
;
;Journal c:, d: und f:
;
```

```
JournaledFileSystems=c: d: d:\mountpoint f:
;
; Überschreibungszeilengruppe, um die Journalführung für f:\
; zu verzögern, bis es ein gültiges Dateisystem ist

[JournalFileSystemSettings.f:\]
;
; Datenbank bleibt gültig, wenn das Dateisystem in den Status 'offline' versetzt wird.
;
PreserveDBOnExit=1
;
; Journalführung verzögern, bis Dateisystem und Journalverzeichnis
; Gültigkeit haben
;
deferFSMonStart=1
;
; Versuchen, Journalführung bei Verzögerung alle 120 Sekunden zu starten
;
deferRetryInterval=120;
; Keine mehrfachen Nachrichten über Nichtverfügbarkeit der Ressource protokollieren
;
logFsErrors=0
```

Zugehörige Konzepte:
Zeilengruppen überschreiben
 Windows-Betriebssysteme

Zeilengruppen überschreiben

Jede beliebige Einstellung in der Zeilengruppe ***JournaledFileSystemSettings*** kann für ein bestimmtes Journaled File System überschrieben werden, indem eine Überschreibungszeilengruppe erstellt wird.

Nachfolgend steht die Syntax für die Zeilengruppe ***JournaledFileSystemSettings***:

Syntax für die Zeilengruppe JournaledFileSystemSettings:
[***JournaledFileSystemSettings***.*fs*]
Syntax für Zeilengruppeneinstellungen:
JournaledFileSystemSetting=*neuer Wert*

Beispiel:

```
[JournalFileSystemSettings.C:\]
  NotifyBuffer=0x0020000
  NotifyFilter=0x107
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

Konfiguration des Journaldämons

Die journalbasierte Sicherung wird durch die Installation und Konfiguration des IBM Spectrum Protect-Journaldämons ermöglicht.

Konfigurieren Sie den Journaldämon, indem Sie die Konfigurationsmusterdatei für den Journaldämon (tsmjbbd.ini.smp) editieren und unter dem Namen tsmjbbd.ini speichern. Beide Dateien sollten sich im Standardinstallationsverzeichnis befinden.

Starten Sie nach der Konfiguration der Datei tsmjbbd.ini den Journaldämon, indem Sie die ausführbare Datei tsmjbbd starten.

 AIX-BetriebssystemeFühren Sie die Scriptdatei jbbinittab aus, um der Datei /etc/inittab einen Eintrag hinzuzufügen, damit unter AIX der Journaldämon nach dem Neustart Ihres Systems gestartet wird. Die ausführbare Datei tsmjbbd und die Scriptdatei jbbinittab sollten sich im Standardinstallationsverzeichnis befinden.

 AIX-BetriebssystemeDamit der Journaldämon unter AIX gestoppt wird, geben Sie den Befehl `kill nnnn` aus (*nnnn* ist die Prozess-ID von tsmjbbd). Bevor der Journaldämonprozess (tsmjbbd) beendet wird, wird die Dateipfadkernelerweiterung benachrichtigt, das Puffern von Dateiänderungen zu stoppen.
Wichtig: Verwenden Sie nicht den Befehl `kill -9 nnnn`, weil der Befehl `kill -9` den Prozess sofort und ohne eine Benachrichtigung, dass das Puffern von Dateiänderungen gestoppt werden soll, beendet.
 Linux-BetriebssystemeUnter Linux erstellt das Installationsprogramm den Service tsmjbbd an der Position /etc/init.d. Führen Sie zum Steuern des Service den folgenden Befehl als Root aus. Mit diesem Befehl können Sie den Service stoppen, starten, erneut starten oder seinen Status überprüfen:

```
>>-service tsmjbbd--+-start---+--------------------------------><
                    +-stop----+
                    +-restart-+
                    '-status--'
```

Wenn das Betriebssystem Linux den Initialisierungsservice `systemd` ausführt, führen Sie die folgenden Schritte aus, um den Journaldämon zu starten:

1. Kopieren Sie die bereitgestellte `systemd`-Einheitendatei /opt/tivoli/tsm/client/ba/bin/tsmjbbd.service in das Verzeichnis /etc/systemd/system/.
2. Führen Sie den folgenden Befehl aus, um die `systemd`-Einheitenliste zu aktualisieren:

   ```
   systemctl daemon-reload
   ```

3. Führen Sie den folgenden Befehl aus, um den Journaldämon zur Systembootzeit zu starten:

   ```
   systemctl enable tsmjbbd.service
   ```

4. Führen Sie den folgenden Befehl aus, um den Journaldämon zu starten:

   ```
   systemctl start tsmjbbd.service
   ```

Anmerkung:

1. Netzdateisysteme und auslagerbare Dateisysteme werden nicht unterstützt.
2. Tägliche journalbasierte Sicherungen sollten durch regelmäßige vollständige Teilsicherungen ergänzt werden. Die Ausführung progressiver vollständiger Teilsicherungen kann mehr Zeit in Anspruch nehmen als eine journalbasierte Sicherung. Berücksichtigen Sie dies bei der Terminierung dieser Sicherungen, indem Sie die Teilsicherungen beispielsweise für Zeiten mit geringer Systemauslastung planen. Setzen Sie diese Sicherungsverfahren in einem ausgewogenen Verhältnis ein, das sich an Ihren Geschäftsanforderungen orientiert. Beispielsweise könnten Sie für jede Nacht eine journalbasierte Sicherung sowie zusätzlich eine vollständige progressive Teilsicherung pro Woche planen.
3. Bei der journalbasierten Sicherung wird die Dateipfadkernelerweiterung für die Überwachung der Dateisystemänderungen verwendet. Um die Leistung der journalbasierten Sicherungen zu verbessern, werden Verzeichnisse, die keine Benutzerdateien enthalten, nicht auf Änderungen überwacht und nicht in journalbasierte Sicherungen einbezogen. Die folgende Liste enthält die Verzeichnisse, die auf AIX- und Linux-Systemen bei journalbasierten Sicherungen nicht berücksichtigt werden. Änderungen an diesen Verzeichnissen werden verarbeitet, wenn Sie unter Verwendung des Befehls incremental mit der Option -nojournal regelmäßige vollständige Teilsicherungen ausführen.

AIX	**Linux**
/bin /dev /etc /lib /usr/bin /usr/lib /usr/share	/bin /boot /dev /etc /lib /proc /sbin /sys /usr/bin /usr/lib /usr/share /var

Die Konfigurationsdatei des Journaldämons wird regelmäßig auf Aktualisierungen der Liste der Journaled File Systems überprüft. Dateisysteme können zur Liste der überwachten Dateisysteme hinzugefügt oder daraus entfernt werden, ohne dass der Journaldämon gestoppt werden muss.

Achtung: Wenn Sie ein vom Journaldämon überwachtes Dateisystem abhängen, wird die Journaldatenbank für dieses Dateisystem gelöscht. Damit die Datenbank erhalten bleibt, legen Sie `PreserveDbOnExit=1` in der Zeilengruppe mit den Einstellungen für Dateisysteme mit Journalaufzeichnung an. Diese Einstellung hat zur Folge, dass die Journaldatenbank erhalten bleibt, wenn das Dateisystem abgehängt wird; außerdem wird sichergestellt, dass die Journaldatenbank gültig ist, wenn das Dateisystem wieder angehängt wird. Weitere Informationen finden Sie in Zeilengruppe JournaledFileSystemSettings.
Die Syntax für Zeilengruppen und Zeilengruppeneinstellungen ist wie folgt:

Syntax für Zeilengruppen:
    [*Zeilengruppenname*]
Syntax für Zeilengruppeneinstellungen:
    Zeilengruppeneinstellung=`Wert`

Anmerkung:

1. Sie können Kommentare in der Datei angeben, indem Sie die Zeile mit einem Semikolon beginnen.
2. Bei Namen von Zeilengruppen und Werten muss die Groß-/Kleinschreibung nicht beachtet werden muss.
3. Numerische Werte können als Hexadezimalwerte angegeben werden, indem dem Wert die Zeichen `0x` vorangestellt werden; andernfalls wird der Wert als Dezimalwert interpretiert.
4. Es besteht keine Korrelation zwischen diesen Einstellungen für Dateisysteme mit Journalaufzeichnung und Einstellungen in der Clientoptionsdatei. Beim Journaldämon handelt es sich um einen unabhängigen Prozess, der keine Optionen in der Clientoptionsdatei verarbeitet.

- AIX-BetriebssystemeLinux-BetriebssystemeZeilengruppe JournalSettings
  Einstellungen unter dieser Zeilengruppe sind global und gelten für den gesamten Journaldämon.
- AIX-BetriebssystemeLinux-BetriebssystemeZeilengruppe JournalExcludeList
  Die Liste der Exclude-Anweisungen filtert Änderungen und verhindert, dass manche Änderungen in der Journaldatenbank aufgezeichnet werden.

- AIX-BetriebssystemeLinux-BetriebssystemeZeilengruppe JournaledFileSystemSettings
  Einstellungen unter dieser Zeilengruppe gelten für jedes angegebene Journaled File System, sofern sie nicht für einzelne Dateisysteme in einer Überschreibungszeilengruppe überschrieben sind.
- AIX-BetriebssystemeLinux-BetriebssystemeZeilengruppen überschreiben
  Jede beliebige Einstellung in der Zeilengruppe JournaledFileSystemSettings kann für ein bestimmtes Journaled File System überschrieben werden, indem eine Überschreibungszeilengruppe erstellt wird.

AIX-BetriebssystemeLinux-Betriebssysteme

Zeilengruppe JournalSettings

Einstellungen unter dieser Zeilengruppe sind global und gelten für den gesamten Journaldämon.

Die Zeilengruppe `JournalSettings` hat folgende Syntax:

Syntax für die Zeilengruppe `JournalSettings`:
```
[JournalSettings]
```
Syntax für Zeilengruppeneinstellungen:
JournalSettings=*Wert*

Sie können folgende Werte für `JournalSettings` angeben:

ErrorLog
: Gibt die Protokolldatei an, in die die vom Journaldämon generierten, ausführlichen Nachrichten geschrieben werden. Der Standardwert ist `jbberror.log` im Verzeichnis der ausführbare Datei des Dämons. Zum Beispiel:

```
ErrorLog=/logs/jbberror.log
```

JournalDir
: Verzeichnis, in das Journaldatenbankdateien geschrieben werden und in dem sie gespeichert sind.

  Ist der angegebene Pfad ein absoluter `Pfadname` (wenn er z. B. mit einem Begrenzer `dir` beginnt), ist dies das verwendete Verzeichnis. Ist der angegebene Pfad ein relativer Verzeichnisname, wird dieser Pfad an jeden Dateisystemnamen angehängt, und es wird der daraus resultierende Pfadname verwendet.

  Standardwert ist ein Verzeichnis mit dem Namen `.tSm_JoUrNaL` (wird innerhalb jedes Dateisystems verwendet, für das eine Journalführung erfolgt).

  Der Vorteil des Ansiedelns der Journaldatenbank auf dem Dateisystem, das überwacht wird, ist das Verbleiben der Datenbank beim Dateisystem. Der Nachteil liegt darin, dass die Aktualisierungen für die Datenbank verarbeitet und gelöscht werden müssen.
  Wichtig: Übertragen Sie die Datenbank in ein Dateisystem, das kein Journaled File System ist, sofern dieses Dateisystem nicht in einer Clusterumgebung gemeinsam genutzt wird.

  Diese Einstellung gilt für alle Journaled File Systems; sie kann jedoch durch eine Überschreibungszeilengruppe für jedes Journaled File System überschrieben werden.

AIX-Betriebssysteme

Zeilengruppe JournalExcludeList

Die Liste der Exclude-Anweisungen filtert Änderungen und verhindert, dass manche Änderungen in der Journaldatenbank aufgezeichnet werden.

Änderungen an Objekten, die mit den Anweisungen in dieser Zeilengruppe übereinstimmen, werden ignoriert und nicht in der Journaldatenbank aufgezeichnet.

Anmerkung:

1. Das Ausschließen von Dateien aus dem Journal hat keine Bedeutung für diejenigen Dateien, die vom Sicherungsclient ausgeschlossen werden, außer dass verhindert wird, dass während einer journalbasierten Sicherung die Dateinamen zur Verarbeitung an den Sicherungsclient gesendet werden. Eine Datei, die nicht aus dem Journal ausgeschlossen ist, sollte dennoch vom Client für Sichern/Archivieren ausgeschlossen werden, wenn es eine übereinstimmende Exclude-Anweisung in der Clientoptionsdatei gibt.
2. Der Journaldämon bietet nur eine Teilmenge der Funktion INCLUDE/EXCLUDE, die vom Client für Sichern/Archivieren zur Verfügung gestellt wird. Der Journaldämon unterstützt keine Anweisungen INCLUDE und auch nicht die Option *exclude.dir*.

Es besteht keine Korrelation zwischen der Ausschlussliste des Journals und der Ausschlussliste des Clients für Sichern/Archivieren.

Die folgenden Metazeichen für die Mustererkennung werden unterstützt:

%
: Stimmt mit genau einem einzigen Zeichen überein.

*
: Entspricht null oder mehr Zeichen.

%EnvVar%
Erweitert die Umgebungsvariable.

Nachfolgend steht ein Beispiel für die Syntax einer Exclude-Anweisung:

```
[JournalExcludeList]
*.jbb.jbbdb
*.jbbInc.jbbdb
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

Zeilengruppe JournaledFileSystemSettings

Einstellungen unter dieser Zeilengruppe gelten für jedes angegebene Journaled File System, sofern sie nicht für einzelne Dateisysteme in einer Überschreibungszeilengruppe überschrieben sind.

Dateisysteme, die Sie in der Zeilengruppe 'JournalFileSystems.Extended' angeben, überschreiben alle Dateisysteme, die Sie möglicherweise zuvor in der der Zeilengruppe 'JournaledFileSystemSettings' in der Liste der Journaled File Systems angegeben haben. Alle anderen Optionen, die Sie in der Zeilengruppe 'JournaledFileSystemsSettings' angegeben haben, bleiben erhalten.

Die Syntax für die Zeilengruppe 'JournaledFileSystemSettings' ist nachfolgend dargestellt:

Syntax für die Zeilengruppe ***JournaledFileSystemSettings***:
[*JournaledFileSystemSettings*]
Syntax für Zeilengruppeneinstellungen:
JournaledFileSystemSetting=*Wert*

Sie können folgende Werte für ***JournaledFileSystemSettings*** angeben:

JournaledFileSystems
Gibt eine Liste der aufzuzeichnenden Dateisysteme an (die einzelnen Einträge werden durch Leerzeichen voneinander getrennt). Es werden vollständige Dateisystemspezifikationen und virtuelle Windows-Zusammenführungen unterstützt. Es gibt keinen Standardwert. Sie müssen mindestens ein Journaled File System angeben, damit der Journaldämon ausgeführt wird. Journaled File Systems können online hinzugefügt oder entfernt werden, ohne dass der Dämon erneut gestartet werden muss. Zum Beispiel:

```
JournaledFileSystems=/home /other
```

Wichtig: Das Journal wählt Objektnamen streng auf der Basis einer Zeichenfolgeübereinstimmung aus. Die Auswirkungen auf den Benutzer liegen darin, dass er größte Sorgfalt walten lassen muss, wenn er Dateisysteme für die Journalführung auswählt. Beispiel: Angenommen, Sie haben ein Dateisystem `/jbb` und ein anderes Dateisystem namens `/jbb/mnt1`. Wenn Sie das Journal anweisen, nur `/jbb` zu überwachen, entsprechen auch alle Änderungen für `/jbb/mnt1` dieser Zeichenfolge und werden in die Datenbank eingegeben. Wenn Sie jedoch eine Sicherung auf dem Client durchführen, wird dieser den Namen auf der Basis der Dateisysteme syntaktisch analysieren, erkennen, dass das Journal dieses Dateisystem nicht überwacht und anschließend dem Journal mitteilen, die Dateien `/jbb/mnt1` aus der Datenbank zu entfernen. Die Lösung ist, entweder beide zu überwachen oder die Liste JournalExcludeList zu verwenden. Dasselbe gilt für die Optionen der virtuellen Mountpunkte. Sie müssen mit dieser Liste konsistent sein. Wenn Sie beispielsweise `/home/student1` als virtuellen Mountpunkt in Ihrer Optionsdatei dsm.sys angeben und `/home` unter Journalführung stellen wollen, müssen Sie `JournaledFileSystems=/home /home/student1` angeben. In diesem Fall werden zwei separate Datenbanken erstellt.

JournalDbSize
Gibt die maximale Größe der Journaldatenbank an. Die Größe der Journaldatenbank wird in Byte angegeben. Der Wert Null (0) gibt an, dass die Datenbankgröße nur von der Kapazität des Dateisystems, das die Journaldatenbank enthält, begrenzt wird. Der Standardwert ist `0` (unbegrenzt). Zum Beispiel:

```
JournalDBSize=0x10000000
```

NotifyBufferSize, *DirNotifyBufferSize*
Geben Sie Benachrichtigung über Änderungen der Puffergrößen für ein Journaled File System an. Ein großer Unfang an Änderungsaktivitäten auf einem Journaled File System erfordert unter Umständen, dass diese vergrößert werden. Der Standardwert ist `0x00020000` (128 k) für Dateien und `0x00010000` (64 k) fü Verzeichnisse.

```
NotifyBufferSize=0x00200000
```

Einstellung PreserveDbOnExit
Diese Einstellung ermöglicht, dass ein Journal gültig bleibt, wenn ein Journaled File System in den Status 'offline' und danach wieder in den Status 'online' versetzt wird. Dies ist hilfreich, um das Journal beim Systemwarmstart und bei der Ressourcenversetzung beizubehalten.

Diese Einstellung ermöglicht, dass bei einer journalbasierten Sicherung die Verarbeitung fortgesetzt wird, wenn der Dämon erneut gestartet wird (oder das Dateisystem wieder in den Status 'online' versetzt wird), ohne eine vollständige Teilsicherung ausführen zu müssen.

Anmerkung: Jede Änderungsaktivität, die auftritt, während der Journaldämon nicht aktiv ist (oder während das Dateisystem offline ist), wird nicht im Journal aufgezeichnet.

Der Wert 1 gibt an, dass die Datenbank des Journaled File System nicht gelöscht wird, wenn das Journaled File System in den Status 'offline' versetzt wird. Die Datenbank hat immer noch Gültigkeit, wenn das Journaled File System wieder in den Status 'online' versetzt wird. Dieser Wert sollte mit Vorsicht verwendet werden, da jede Änderungsaktivität für das Dateisystem, die auftritt, während das Journaled File System offline ist, nicht in der Journaldatenbank widergespiegelt wird. Mit der Standardeinstellung 0 wird die Journaldatenbank des Journaled File System gelöscht.

Anmerkung: Das Journal bleibt nur erhalten, wenn ein Journaled File System normal 'offline' gesetzt wird oder 'offline' gesetzt wird, wenn die Ressource nicht mehr verfügbar ist und Sie die Einstellung deferFsMonStart angeben. Wird ein Dateisystem aufgrund eines Fehlers wie beispielsweise eines Benachrichtigungspufferüberlaufs 'offline' gesetzt, wird das Journal gelöscht.
Anmerkung: Setzen Sie PreserveDBonExit nur, wenn Sie sicherzustellen können, dass der Journalservice kontrolliert beendet wird. Unter eine "kontrollierte Beendigung" fällt auch das Stoppen des Journalservice, um das System erneut zu starten, die Übernahme einer Clusterressource oder das Versetzen einer Clusterressource. Die Journaldatenbank kann beschädigt werden, wenn die Beendigung nicht kontrolliert erfolgt. Führen Sie daher die folgenden Schritte aus, wenn der Journalservice nicht kontrolliert beendet wurde oder wenn die Journaldatenbank durch andere Ursachen nicht kontrolliert offline gesetzt wurde.

1. Stoppen Sie den Journalservice (falls er aktiv ist).
2. Löschen Sie die beschädigte Journaldatenbank.
3. Starten Sie den Journalservice erneut.
4. Führen Sie eine Teilsicherung aus.

Nachfolgend steht ein Beispiel, bei dem die Journaldatenbank beim Verlassen nicht gelöscht wird:

```
preserveDBOnExit=1
```

Einstellung deferFSMonStart
Diese Einstellung verzögert in folgenden Fällen den Versuch, mit der Überwachung eines Dateisystems zu beginnen:

- Wenn das angegebene Journaled File System nicht gültig oder nicht verfügbar ist.
- Das Journalverzeichnis für das angegebene Journaled File System ist nicht im Zugriff oder kann nicht erstellt werden.

Die Überprüfung der Ressourcen findet in den Intervallen statt, die Sie über die Einstellung *deferRetryInterval* angeben.

Der Wert 1 gibt an, dass die Einstellung aktiviert ist. Der Wert 0 gibt an, dass die Einstellung inaktiviert ist. Standardwert ist 0.

Einstellung deferRetryInterval
Diese Einstellung gibt das Zeitintervall in Sekunden an, nach dem verzögerte Dateisysteme mit aktivierter Einstellung *deferRetryInterval* auf ihre Verfügbarkeit geprüft und in den Status 'online' versetzt werden. Der Standardwert ist 5 Sekunden.
Einstellung logFSErrors
Der Wert 1 besagt, dass alle Fehler protokolliert werden sollen, die beim Zugriff auf ein Journaled File System oder Journalverzeichnis festgestellt wurden. Der Wert Null besagt, dass das Protokollieren von Fehlern, die beim Überprüfen verzögerter Dateisysteme und Journalverzeichnisse festgestellt wurden, unterdrückt wird. Dies wird normalerweise zusammen mit der Einstellung *deferFSMonStart* verwendet, um zu verhindern, dass sehr viele Nachrichten `Dateisystem nicht verfügbar` in die Protokolle geschrieben werden, wenn ein Journaled File System verzögert in den Status 'online' versetzt wird. Der Standardwert ist 1 (alle Fehler protokollieren).

- Linux-BetriebssystemeAIX-BetriebssystemeZeilengruppe 'JournaledFileSystems.Extended'
  Die Zeilengruppe 'JournaledFileSystems.Extended' überschreibt alle Dateisysteme, die in der Zeilengruppe 'JournaledFileSystems' enthalten sind. Außerdem hebt sie die von der Zeilengruppe 'JournaledFileSystems' auferlegte Begrenzung auf 1023 Zeichen auf.

Zugehörige Konzepte:
Zeilengruppen überschreiben
Zeilengruppe 'JournaledFileSystems.Extended'
AIX-BetriebssystemeLinux-Betriebssysteme

Zeilengruppen überschreiben

Jede beliebige Einstellung in der Zeilengruppe JournaledFileSystemSettings kann für ein bestimmtes Journaled File System überschrieben werden, indem eine Überschreibungszeilengruppe erstellt wird.

HookFileName
Damit das Journal mit der Überwachung eines Dateisystems beginnt, muss es den Namen einer vorhandenen Datei in diesem Dateisystem kennen. Diese Einstellung gibt eine vorhandene Datei an. Der Zugriff auf diese Datei wird dann als Test verwendet, um zu sehen, ob dieses Dateisystem online ist. (Die Systemdefinition 'angehängt' kann nicht verwendet werden, da wir die Verwendung virtueller Mountpunkte im Client für Sichern/Archivieren zulassen. Dies bedeutet, dass das System des Clients für Sichern/Archivieren ein Verzeichnis als (virtuelles) Dateisystem behandeln kann).

Deshalb muss, wenn dieses Dateisystem angehängt und abgehängt werden kann, ein Eintrag für HookFileName zur Verfügung gestellt werden.

Wird kein Eintrag für HookFileName eingegeben, versucht der Journaldämon, eine temporäre Datei im höchsten Verzeichnis zu erstellen, sie für den Beginn der Überwachung zu verwenden und sie anschließend zu löschen.

Nachfolgend steht die Syntax für die Zeilengruppe JournaledFileSystemSettings:

Syntax für die Zeilengruppe JournaledFileSystemSettings:
[*JournaledFileSystemSettings*.*fs*]
Syntax für Zeilengruppeneinstellungen:
JournaledFileSystemSetting=*neuer Wert*

Der Name der Überschreibungszeilengruppe für `/home` wäre beispielsweise:

```
JournaledFileSystemSettings./home
  HookFileName=/home/doNotDeleteThisFile
```

Clientseitige Datendeduplizierung

Die *Datendeduplizierung* ist eine Methode zur Reduzierung des Speicherbedarfs, indem redundante Daten entfernt werden.

Übersicht

Zwei Datendeduplizierungstypen sind verfügbar: *clientseitige Datendeduplizierung* und *serverseitige Datendeduplizierung*.

Als *clientseitige Datendeduplizierung* wird ein Datendeduplizierungsverfahren bezeichnet, das der Client für Sichern/Archivieren verwendet, um bei der Sicherungs- und Archivierungsverarbeitung redundante Daten zu entfernen, bevor die Daten an den IBM Spectrum Protect-Server übertragen werden. Durch die clientseitige Datendeduplizierung kann das Datenvolumen reduziert werden, das über ein lokales Netz gesendet wird.

Unter *serverseitiger Datendeduplizierung* versteht man ein Datendeduplizierungsverfahren, das der Server durchführt. Der IBM Spectrum Protect-Administrator kann die zu verwendende Position für die Datendeduplizierung (Client oder Server) mit dem Parameter DEDUP im Serverbefehl REGISTER NODE oder UPDATE NODE angeben.

Erweiterungen

Mit der clientseitigen Datendeduplizierung haben Sie folgende Möglichkeiten:

- Bestimmte Dateien auf einem Client von der Datendeduplizierung ausschließen.
- Einen Cache für die Datendeduplizierung aktivieren, der den Datenaustausch im Netz zwischen dem Client und dem Server reduziert. Der Cache enthält Bereiche, die in vorherigen Teilsicherungsoperationen an den Server gesendet wurden. Anstatt den Server nach dem Vorhandensein eines Bereichs abzufragen, fragt der Client seinen Cache ab.

  Eine Größe und Position für einen Client-Cache angeben. Wird eine Inkonsistenz zwischen dem Server und dem lokalen Cache festgestellt, wird der lokale Cache entfernt und erneut gefüllt.

  Anmerkung: Für Anwendungen, die die IBM Spectrum Protect-API verwenden, darf der Datendeduplizierungscache wegen möglicher Sicherungsfehler nicht verwendet werden, die verursacht werden, wenn der Cache nicht mit dem IBM Spectrum Protect-Server synchron ist. Wenn mehrere, gleichzeitig ablaufende Sitzungen des Clients für Sichern/Archivieren konfiguriert sind, muss für jede Sitzung ein separater Cache konfiguriert werden.
- Sowohl die clientseitige Datendeduplizierung als auch die Komprimierung aktivieren, um das vom Server gespeicherte Datenvolumen zu reduzieren. Jeder Bereich wird komprimiert, bevor er an den Server gesendet wird. Der Kompromiss liegt zwischen Speichereinsparungen und der Verarbeitungsleistung, die zum Komprimieren der Clientdaten erforderlich ist. Im Allgemeinen gilt: Wenn Sie Daten auf dem Clientsystem komprimieren und deduplizieren, ist etwa zweimal so viel Verarbeitungsleistung wie für die Datendeduplizierung allein erforderlich.

  Der Server kann mit deduplizierten, komprimierten Daten arbeiten. Außerdem können Clients für Sichern/Archivieren vor Version 6.2 deduplizierte, komprimierte Daten zurückschreiben.

Bei der clientseitigen Datendeduplizierung wird der folgende Prozess verwendet:

- Der Client erstellt Bereiche. *Bereiche* sind Abschnitte von Dateien, die mit anderen Dateibereichen verglichen werden, um Duplikate festzustellen.
- Der Client und der Server arbeiten zusammen, um doppelte Bereiche zu identifizieren. Der Client sendet Bereiche, die nicht doppelt sind, an den Server.
- Nachfolgende Deduplizierungsoperationen für Clientdaten erstellen neue Bereiche. Einige oder alle dieser Bereiche können mit den Bereichen übereinstimmen, die in vorherigen Deduplizierungsoperationen für Daten erstellt und an den Server gesendet wurden. Übereinstimmende Bereiche werden nicht erneut an den Server gesendet.

Vorteile

Die clientseitige Datendeduplizierung bietet mehrere Vorteile:

- Sie kann das über das lokale Netz (LAN) gesendete Datenvolumen reduzieren.
- Die zum Identifizieren doppelter Daten erforderliche Verarbeitungsleistung wird vom Server auf Clientknoten verlagert. Die serverseitige Datendeduplizierung ist für Speicherpools, die für die Deduplizierung aktiviert sind, immer aktiviert. Dateien, die sich in den Speicherpools befinden, die für die Deduplizierung aktiviert sind, und die vom Client dedupliziert wurden, erfordern jedoch keine zusätzliche Verarbeitung.

- Die zum Entfernen doppelter Daten auf dem Server erforderliche Verarbeitungsleistung wird eliminiert. Dadurch werden Speichereinsparungen auf dem Server sofort wirksam.

Die clientseitige Datendeduplizierung hat einen möglichen Nachteil. Der Server verfügt erst dann über vollständige Kopien von Clientdateien, *wenn* Sie die primären Speicherpools, die die clientseitigen Bereiche enthalten, in einem nicht deduplizierten Kopienspeicherpool sichern. (*Bereiche* sind Teile einer Datei, die während des Prozesses für die Datendeduplizierung erstellt werden.) Während der Speicherpoolsicherung in einem nicht deduplizierten Speicherpool werden clientseitige Bereiche in aneinandergrenzenden Dateien neu erstellt.

Standardmäßig müssen primäre Speicherpools mit sequenziellem Zugriff, die für die Datendeduplizierung definiert sind, in nicht deduplizierten Kopienspeicherpools gesichert werden, bevor sie zurückgefordert und doppelte Daten entfernt werden können. Mit dem Standardwert wird sichergestellt, dass der Server immer über Kopien vollständiger Dateien in einem primären Speicherpool oder einem Kopienspeicherpool verfügt.

Wichtig: Um das Datenvolumen noch weiter zu reduzieren, können Sie gleichzeitig die clientseitige Datendeduplizierung und die Komprimierung aktivieren. Jeder Bereich wird komprimiert, bevor er an den Server gesendet wird. Durch Komprimierung wird Speicherbereich eingespart, jedoch die Verarbeitungszeit auf der Client-Workstation verlängert.

In einem für die Datendeduplizierung aktivierten Speicherpool (Dateipool) wird nur eine einzige Instanz eines Datenbereichs aufbewahrt. Andere Instanzen desselben Datenbereichs werden durch einen Zeiger auf die aufbewahrte Instanz ersetzt.

Ist die clientseitige Datendeduplizierung aktiviert und verfügt der Server über keinen weiteren Speicherbereich im Zielpool, wobei ein nächster Pool definiert ist, stoppt der Server die Transaktion. Der Client für Sichern/Archivieren wiederholt die Transaktion ohne clientseitige Datendeduplizierung. Zur Behebung des Problems muss der IBM Spectrum Protect-Administrator dem ursprünglichen Dateipool weitere Arbeitsdatenträger hinzufügen oder die Operation ohne Aktivierung der Deduplizierung wiederholen.

Zur Verwendung der clientseitigen Datendeduplizierung muss der IBM Spectrum Protect-Server Version 6.2 oder höher haben.

Voraussetzungen

Bei der Konfiguration der clientseitigen Datendeduplizierung müssen die folgenden Voraussetzungen erfüllt sein:

- Der Client und Server müssen die Version 6.2.0 oder eine höhere Version haben. Es sollte immer die letzte Wartungsversion verwendet werden.
- Wenn ein Client eine Datei sichert oder archiviert, werden die Daten in den primären Speicherpool geschrieben, der durch die Kopiengruppe der Verwaltungsklasse angegeben wird, die an die Daten gebunden ist. Um die Clientdaten zu deduplizieren, muss der primäre Speicherpool ein Plattenspeicherpool (FILE) mit sequenziellem Zugriff sein, der für die Datendeduplizierung aktiviert ist.
- Für die Option DEDUPLICATION auf dem Client muss YES definiert sein. Sie können die Option DEDUPLICATION in der Clientoptionsdatei, im Profileditor der GUI des Clients für Sichern/Archivieren oder in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definieren. Verwenden Sie den Befehl DEFINE CLIENTOPT, um die Option DEDUPLICATION in einer Clientoptionsgruppe zu definieren. Um zu verhindern, dass der Client den Wert in der Clientoptionsgruppe überschreibt, geben Sie FORCE=YES an.
- Die clientseitige Datendeduplizierung muss auf dem Server aktiviert sein. Um die clientseitige Datendeduplizierung zu aktivieren, verwenden Sie den Parameter DEDUPLICATION im Serverbefehl REGISTER NODE oder UPDATE NODE. Setzen Sie den Wert des Parameters auf CLIENTORSERVER.
- Stellen Sie sicher, dass Dateien auf dem Client nicht von der clientseitigen Datendeduplizierung ausgeschlossen sind. Standardmäßig sind alle Dateien eingeschlossen. Sie können wahlweise bestimmte Dateien mit der Clientoption exclude.dedup von der clientseitigen Datendeduplizierung ausschließen.
- Dateien auf dem Client dürfen nicht verschlüsselt sein. Verschlüsselte Dateien und Dateien aus verschlüsselten Dateisystemen können nicht dedupliziert werden.
- Dateien müssen größer als 2 KB und Transaktionen unter dem mit der Option CLIENTDEDUPTXNLIMIT angegebenen Wert liegen. Dateien mit einer Größe von 2 KB oder weniger werden nicht dedupliziert.

Der Server kann die maximale Transaktionsgröße für die Datendeduplizierung durch Definieren der Option CLIENTDEDUPTXNLIMIT auf dem Server begrenzen. Weitere Informationen zu dieser Option finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Die folgenden Operationen haben Vorrang vor der clientseitigen Datendeduplizierung:

- LAN-unabhängige Datenversetzung
- Simultane Schreiboperationen
- Datenverschlüsselung

Wichtig: Planen oder aktivieren Sie keine dieser Operationen während der clientseitigen Datendeduplizierung. Wird eine dieser Operationen während der clientseitigen Datendeduplizierung ausgeführt, wird die clientseitige Datendeduplizierung inaktiviert und es wird eine Nachricht in das Fehlerprotokoll geschrieben.

Die Einstellung auf dem Server legt letztendlich fest, ob die clientseitige Datendeduplizierung aktiviert ist. Siehe Tabelle 1.

Tabelle 1. Datendeduplizierungseinstellungen: Client und Server

Wert der Clientoption DEDUPLICATION	**Einstellung auf dem Server**	**Position für die Datendeduplizierung**
Yes	Entweder auf dem Server oder auf dem Client	Client
Yes	Nur auf dem Server	Server

Wert der Clientoption DEDUPLICATION	Einstellung auf dem Server	Position für die Datendeduplizierung
No	Entweder auf dem Server oder auf dem Client	Server
No	Nur auf dem Server	Server

Verschlüsselte Dateien

Der IBM Spectrum Protect-Server und der Client für Sichern/Archivieren können keine verschlüsselten Dateien deduplizieren. Wird während der Datendeduplizierungsverarbeitung eine verschlüsselte Datei entdeckt, wird die Datei nicht dedupliziert und eine Nachricht wird protokolliert.
Tipp: Sie müssen verschlüsselte Dateien und Dateien, die für die clientseitige Datendeduplizierung ausgewählt werden können, nicht separat verarbeiten. Beide Typen von Dateien können in derselben Operation verarbeitet werden. Sie werden jedoch in verschiedenen Transaktionen an den Server gesendet.
Als Sicherheitsvorkehrung können Sie einen oder mehrere der folgenden Schritte ausführen:

- Aktivieren Sie die Speichereinheitenverschlüsselung zusammen mit der clientseitigen Datendeduplizierung.
- Verwenden Sie die clientseitige Datendeduplizierung nur für Knoten, die sicher sind.
- Sind Sie sich bezüglich der Netzsicherheit nicht sicher, aktivieren Sie Secure Sockets Layer (SSL).
- Sollen bestimmte Objekte (beispielsweise Imageobjekte) nicht von der clientseitigen Datendeduplizierung verarbeitet werden, können Sie sie auf dem Client ausschließen. Wird ein Objekt von der clientseitigen Datendeduplizierung ausgeschlossen und an einen Speicherpool gesendet, der für die Datendeduplizierung definiert ist, wird das Objekt auf dem Server dedupliziert.
- Verwenden Sie den Befehl SET DEDUPVERIFICATIONLEVEL, um mögliche Sicherheitsattacken auf den Server während der clientseitigen Datendeduplizierung festzustellen. Mit diesem Befehl können Sie einen Prozentsatz von Clientbereichen angeben, die vom Server geprüft werden sollen. Wenn der Server eine mögliche Sicherheitsattacke feststellt, wird eine Nachricht angezeigt.

- Client für die Datendeduplizierung konfigurieren
  Konfigurieren Sie den Client so, dass Sie die Datendeduplizierung beim Sichern und Archivieren Ihrer Dateien verwenden können.
- Dateien bei der Datendeduplizierung ausschließen
  Sie können eine Datei bei der Datendeduplizierung während der Sicherungs- oder Archivierungsverarbeitung ausschließen.

Zugehörige Tasks:
Client für die Datendeduplizierung konfigurieren
Zugehörige Verweise:
Deduplication
Ausschlussoptionen
Dedupcachepath
Dedupcachesize
Enablededupcache
Ieobjtype

Client für die Datendeduplizierung konfigurieren

Konfigurieren Sie den Client so, dass Sie die Datendeduplizierung beim Sichern und Archivieren Ihrer Dateien verwenden können.

Vorbereitende Schritte

Stellen Sie vor dem Konfigurieren des Clients für die Datendeduplizierung sicher, dass die Voraussetzungen erfüllt sind, die in Clientseitige Datendeduplizierung aufgelistet sind:

- Der Server muss den Client mit dem Parameter DEDUP=CLIENTORSERVER im Befehl REGISTER NODE oder UPDATE NODE für die clientseitige Datendeduplizierung aktivieren.
- Der Zielspeicherpool für die Daten muss ein Speicherpool sein, der für die Datendeduplizierung aktiviert ist.
- Stellen Sie sicher, dass Ihre Dateien an die korrekte Verwaltungsklasse gebunden sind.
- Die Dateien müssen größer als 2 KB sein.

Eine Datei kann von der Verarbeitung für die clientseitige Datendeduplizierung ausgeschlossen sein. Standardmäßig sind alle Dateien eingeschlossen. Weitere Informationen finden Sie in der Beschreibung der Option exclude.dedup.

Der Server kann die maximale Transaktionsgröße für die Datendeduplizierung durch Definieren der Option CLIENTDEDUPTXNLIMIT auf dem Server begrenzen.

Vorgehensweise

Verwenden Sie zur Aktivierung der Datendeduplizierung auf dem Client eine der folgenden Methoden:

Option	Bezeichnung

Option	Bezeichnung
Clientoptionsdatei bearbeiten	• AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme Fügen Sie die Option `deduplication yes` der Datei dsm.sys hinzu. • Windows-BetriebssystemeFügen Sie die Option `deduplication yes` der Datei dsm.opt hinzu.
Profileditor	a. Klicken Sie im IBM Spectrum Protect-Fenster auf Editieren > Clientvorgaben. b. Klicken Sie auf Deduplizierung. c. Wählen Sie das Kontrollkästchen Deduplizierung aktivieren aus. d. Klicken Sie auf OK, um Ihre ausgewählten Einträge zu sichern und den Profileditor zu schließen.

Ergebnisse

Nachdem Sie den Client für die Datendeduplizierung konfiguriert haben, starten Sie eine Sicherungs- oder Archivierungsoperation. Wenn die Operation beendet ist, zeigt der Sicherungs- oder Archivierungsbericht das Datenvolumen an, das in dieser Operation dedupliziert wurde, sowie die Anzahl der von der clientseitigen Datendeduplizierung verarbeiteten Dateien.

Wenn nicht genügend Plattenspeicherplatz für die Sicherungs- oder Archivierungsoperation zur Verfügung steht, können Sie die clientseitige Datendeduplizierung ohne lokalen Datendeduplizierungscache aktivieren. Gehen Sie dabei wie folgt vor:

1. Fügen Sie die Option `deduplication yes` der Clientoptionsdatei hinzu.
   - AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeFügen Sie die Option `deduplication yes` der Datei dsm.sys hinzu. Sie können diese Option auch in der GUI definieren.
   - Windows-BetriebssystemeFügen Sie die Option `deduplication yes` der Datei dsm.opt hinzu. Sie können diese Option auch in der GUI definieren.
2. Inaktivieren Sie den lokalen Datendeduplizierungscache. Führen Sie hierfür einen der folgenden Schritte aus:
   - AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeFügen Sie die Option `ENABLEDEDUPCACHE NO` der Datei dsm.sys hinzu.
   - Windows-BetriebssystemeFügen Sie die Option `ENABLEDEDUPCACHE NO` der Datei dsm.opt hinzu.

   Sie können diese Option auch im Profileditor des Clients für Sichern/Archivieren definieren, indem Sie das Kontrollkästchen Deduplizierungscache aktivieren abwählen.

Beispiel

Im folgenden Beispiel wird der Befehl 'query session' verwendet, um die Datentypen anzuzeigen, die für die Datendeduplizierung verarbeitet wurden.

```
Protect> q sess
IBM Spectrum Protect-Serververbindungsinformationen

Servername...................: SERVER1
Servertyp....................: Windows
Schutz der Archivaufbewahrung: "Nein"
Serverversion................: Ver. 6, Rel. 2, Stu. 0.0
Datum des letzten Zugriffs...: 25.08.2009 13:38:18
Sicherungsdateien löschen....: "Nein"
Archivierungsdateien löschen.: "Ja"
Deduplizierung...............: "Client oder Server"

Knotenname...................: AVI
Benutzername.................:
```

Im folgenden Beispiel wird der Befehl 'query management class' verwendet, um die Datentypen anzuzeigen, die für die Datendeduplizierung verarbeitet wurden.

```
Protect> q mgmt -det
Domänenname : DEDUP
Aktivierte Maßnahmengruppe : DEDUP
Aktivierungsdatum/-zeit : 24.08.2009 07:26:09
Standardverwaltungsklasse : DEDUP
Aufbewahrungszeitraum für Sicherung : 30 Tag(e)
Aufbewahrungszeitraum für Archivierung: 365 Tag(e)


Verw.-Klasse: DEDUP
Beschreibung: dedup - Standardwerte
Speicherverwaltungsverfahren: Keine
Auto-Umlagerung bei Nichtbenutzung: 0
Sicherung vor Umlagerung erforderlich: JA
Ziel für umgelagerte Dateien: SPACEMGPOOL
Kopiengruppe
Kopiengruppenname......: STANDARD
Kopienart..............: Sichern
```

```
Kopienhäufigkeit.......: 0 Tag(e)
Versionen bestehender Daten: 2 Version(en)
Versionen gelöschter Daten: 1 Version(en)
Extraversionen aufbewahren: 30 Tag(e)
Einzige Version aufbewahren: 60 Tag(e)
Kopiennummerierung.....: Gemeinsam statisch
Kopienmodus............: Geändert
Kopienziel.............: AVIFILEPOOL
LAN-unabhängiges Ziel..: NEIN
Daten deduplizieren....: JA

Kopiengruppenname......: STANDARD
Kopienart..............: Archivieren
Kopienhäufigkeit.......: Cmd
Version aufbewahren....: 365 Tag(e)
Kopiennummerierung.....: Gemeinsam statisch
Kopienmodus............: Absolut
Aufbewahrungsstart.....: Erstellen
Mindestaufbewahrung....: 65534 Tag(e)
Kopienziel.............: FILEPOOL
LAN-unabhängiges Ziel..: NEIN
Daten deduplizieren....: JA

ANS1900I Rückkehrcode ist 0.
```

Zugehörige Konzepte:
Clientseitige Datendeduplizierung
Zugehörige Verweise:
Option CLIENTDEDUPTXNLIMIT
Befehl REGISTER NODE
Befehl UPDATE NODE
Deduplication
Enablededupcache
Ausschlussoptionen

Dateien bei der Datendeduplizierung ausschließen

Sie können eine Datei bei der Datendeduplizierung während der Sicherungs- oder Archivierungsverarbeitung ausschließen.

Informationen zu diesem Vorgang

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeSie können nur Dateien bei der Deduplizierung von Archivierungsdaten ausschließen. Sie können Dateien und Images (soweit zutreffend) bei der Deduplizierung von Sicherungsdaten ausschließen.

Windows-BetriebssystemeSie können nur Dateien bei der Deduplizierung von Archivierungsdaten ausschließen. Sie können Dateien, Images, Systemstatusobjekte und ASR bei der Deduplizierung von Sicherungsdaten ausschließen.

Vorgehensweise

Sollen bestimmte Dateien bei der clientseitigen Datendeduplizierung nicht verarbeitet werden, können Sie diese über die GUI bei der Datendeduplizierungsverarbeitung ausschließen:

1. Klicken Sie auf Editieren > Clientvorgaben.
2. Klicken Sie auf die Registerkarte Einschluss/Ausschluss.
3. Klicken Sie auf Hinzufügen, um das Fenster Include/Exclude-Optionen definieren zu öffnen.
4. Wählen Sie eine Kategorie für die Verarbeitung aus.
   - Um eine Datei bei der Datendeduplizierung während der Archivierungsverarbeitung auszuschließen, wählen Sie Archivieren in der Liste Kategorie aus.
   - Um eine Datei bei der Datendeduplizierung während der Sicherungsverarbeitung auszuschließen, wählen Sie Sichern in der Liste Kategorie aus.
5. Wählen Sie Exclude.Dedup in der Liste Typ aus.
6. Wählen Sie einen Eintrag in der Liste Objekttyp aus.
   - Für die Archivierungsverarbeitung ist nur der Objekttyp Datei verfügbar.
   - Für die Sicherungsverarbeitung wählen Sie einen der folgenden Objekttypen aus:
     - Datei
     - Image
     - Windows-BetriebssystemeSystemstatus
     - Windows-BetriebssystemeASR
7. Geben Sie eine Datei oder ein Muster im Feld Datei oder Muster an. Sie können Platzhalterzeichen verwenden. Wenn Sie die Datei oder das Muster nicht eingeben wollen, klicken Sie auf Durchsuchen, um ein Auswahlfenster zu öffnen und eine Datei auszuwählen. Für angehängte Dateibereiche können Sie den Verzeichnismountpunkt im Auswahlfenster auswählen.

Windows-BetriebssystemeFür ASR und Systemstatus wird dieses Feld automatisch ausgefüllt. Wenn Sie den Objekttyp Image angeben, muss auf den Laufwerkbuchstaben die Zeichenfolge ':**' folgen. Beispiel: Zum Ausschließen von Laufwerk E: geben Sie das folgende Muster ein:

```
E:\*\*
```

8. Klicken Sie auf OK, um das Fenster 'Include/Exclude-Optionen definieren' zu schließen. Die Ausschlussoptionen, die Sie definiert haben, befinden sich in einer Exclude-Anweisung unten im Listenfeld für Anweisungen auf der Registerkarte Vorgaben für Einschluss/Ausschluss.
9. Klicken Sie auf OK, um Ihre ausgewählten Einträge zu sichern und den Profileditor zu schließen.

Nächste Schritte

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeSie können auch Dateien von der Datendeduplizierungsverarbeitung ausschließen, indem Sie die Datei dsm.sys editieren:

1. Fügen Sie die Option `deduplication yes` hinzu.
2. Die Dateien in einem Verzeichnis von der Datendeduplizierung ausschließen. Sollen beispielsweise die Dateien im Verzeichnis /Users/Administrator/Documents/Taxes/ ausgeschlossen werden, fügen Sie die folgende Anweisung hinzu: `EXCLUDE.dedup /Users/Administrator/Documents/Taxes/.../*`
3. Clientseitige Datendeduplizierung für die Imagesicherung eines Dateisystems ausschließen. Soll beispielsweise das Dateisystem /home ausgeschlossen werden, fügen Sie die folgende Anweisung hinzu: `EXCLUDE.DEDUP /home/*/* IEOBJTYPE=Image`

Windows-BetriebssystemeSie können auch Dateien von der Datendeduplizierungsverarbeitung ausschließen, indem Sie die Datei dsm.opt editieren:

1. Fügen Sie die Option `deduplication yes` hinzu.
2. Clientseitige Datendeduplizierung für die Imagesicherung eines Laufwerks ausschließen. Soll beispielsweise das Laufwerk E: ausgeschlossen werden, fügen Sie die Anweisung `EXCLUDE.DEDUP E:\*\* IEOBJTYPE=Image` der Datei dsm.opt hinzu.

Wichtig: Wird ein Objekt an einen Datendeduplizierungspool gesendet, wird die Datendeduplizierung auf dem Server ausgeführt, selbst wenn das Objekt von der clientseitigen Datendeduplizierung ausgeschlossen ist.
Zugehörige Konzepte:
Clientseitige Datendeduplizierung
Zugehörige Verweise:
Deduplication
Enablededupcache
Ausschlussoptionen

Konfiguration und Verwendung der automatisierten Clientübernahme

Wenn der IBM Spectrum Protect-Server nicht verfügbar ist, kann eine automatische Übernahme des Clients für Sichern/Archivieren auf einem Sekundärserver zum Zweck der Datenwiederherstellung stattfinden. Sie können in der Konfiguration des Clients die automatisierte Übernahme angeben oder eine Übernahme des Clients unterbinden. Außerdem können Sie den Replikationsstatus Ihrer Daten auf dem Sekundärserver bestimmen, bevor Sie die replizierten Daten zurückschreiben oder abrufen.

- Automatisierte Clientübernahme - Übersicht
  Bei einem Ausfall auf dem IBM Spectrum Protect-Server kann eine automatische Übernahme des Clients für Sichern/Archivieren auf einem Sekundärserver zum Zweck der Datenwiederherstellung stattfinden.
- Client für automatisierte Übernahme konfigurieren
  Sie können durch eine manuelle Konfiguration festlegen, dass eine automatische Übernahme des Clients auf dem Sekundärserver stattfindet.
- Status replizierter Clientdaten bestimmen
  Bevor Sie Clientdaten vom Sekundärserver zurückschreiben oder abrufen, können Sie prüfen, ob die neueste Sicherung des Clients auf dem Sekundärserver repliziert wurde.
- Automatisierte Clientübernahme verhindern
  Sie können in der Konfiguration des Clients festlegen, dass die automatisierte Clientübernahme auf dem Sekundärserver verhindert werden soll.
- Clientübernahme erzwingen
  Es kann eine sofortige Übernahme des Clients auf dem Sekundärserver stattfinden, auch wenn der Primärserver betriebsbereit ist. Sie können mit diesem Verfahren beispielsweise prüfen, ob eine Übernahme des Clients auf dem erwarteten Sekundärserver stattfindet.

Zugehörige Tasks:
Daten während einer Übernahme zurückschreiben oder abrufen

Automatisierte Clientübernahme - Übersicht

Bei einem Ausfall auf dem IBM Spectrum Protect-Server kann eine automatische Übernahme des Clients für Sichern/Archivieren auf einem Sekundärserver zum Zweck der Datenwiederherstellung stattfinden.

Der IBM Spectrum Protect-Server, zu dem der Client während der normalen Produktionsprozesse eine Verbindung herstellt, wird als *Primärserver* bezeichnet. Wenn der Primärserver und die Clientknoten für die Knotenreplikation konfiguriert sind, wird dieser Server auch als *Quellenreplikationsserver* bezeichnet. Die Clientdaten auf dem Quellenreplikationsserver können auf einem anderen IBM Spectrum Protect-Server, dem *Zielreplikationsserver*, repliziert werden. Dieser Server wird auch als *Sekundärserver* bezeichnet, auf dem eine automatische Übernahme des Clients stattfindet, wenn der Primärserver ausfällt.

Damit eine automatische Übernahme des Clients auf dem Sekundärserver stattfinden kann, müssen dem Client die Verbindungsinformationen für den Sekundärserver zur Verfügung gestellt werden. Während des Normalbetriebs werden die Verbindungsinformationen für den Sekundärserver im Verlauf des Anmeldeprozesses automatisch vom Primärserver an den Client gesendet. Die Daten des Sekundärservers werden automatisch in der Clientoptionsdatei gespeichert. Es ist kein manueller Eingriff des Benutzers erforderlich, um die Daten für den Sekundärserver hinzuzufügen.

Der Client versucht bei jeder Anmeldung am IBM Spectrum Protect-Server eine Verbindung zum Primärserver herzustellen. Wenn der Primärserver nicht verfügbar ist, findet automatisch eine Übernahme des Clients auf dem Sekundärserver statt und zwar gemäß den Informationen zum Sekundärserver in der Clientoptionsdatei. In diesem Übernahmemodus können Sie alle replizierten Clientdaten zurückschreiben oder abrufen. Wenn der Primärserver wieder online ist, wird der Client bei seinem nächsten Start automatisch wieder auf den Primärserver zurückgesetzt.

 Windows-BetriebssystemeDer folgende Beispieltext zeigt die Verbindungsinformationen des Sekundärservers, die an den Client gesendet und in der Clientoptionsdatei (dsm.opt) gespeichert werden:

```
*** Diese Optionen sollten nicht manuell geändert werden
REPLSERVERNAME          TARGET
   REPLTCPSERVERADDRESS 192.0.2.9
   REPLTCPPORT          1501
   REPLSSLPORT          1502
   REPLSERVERGUID       60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

MYREPLICATIONServer TARGET
MYPRIMARYServer SERVER1
*** Ende der automatisch aktualisierten Optionen
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeDer folgende Beispieltext zeigt die Verbindungsinformationen des Sekundärservers, die an den Client gesendet und in der Clientsystemoptionsdatei (dsm.sys) gespeichert werden:

```
*** Diese Optionen sollten nicht manuell geändert werden
REPLSERVERNAME          TARGET
   REPLTCPSERVERADDRESS 192.0.2.9
   REPLTCPPORT          1501
   REPLSSLPORT          1502
   REPLSERVERGUID       60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

MYREPLICATIONServer TARGET
*** Ende der automatisch aktualisierten Optionen
```

- Voraussetzungen für die automatisierte Clientübernahme
  Bevor Sie den Client für die automatisierte Clientübernahme konfigurieren oder verwenden, müssen der Client für Sichern/Archivieren und der IBM Spectrum Protect-Server mehrere Voraussetzungen erfüllen.
- Einschränkungen für die automatisierte Clientübernahme
  Der folgende Abschnitt enthält Informationen, die den Prozess der automatisierten Clientübernahme und die damit verbundenen Einschränkungen erläutern.
- Übernahmefunktionalität der IBM Spectrum Protect-Komponenten
  IBM Spectrum Protect-Komponenten und -Produkte verwenden den Client für Sichern/Archivieren oder die API für die Sicherung von Daten auf dem IBM Spectrum Protect-Primärserver. Wenn der Primärserver ausfällt, kann eine Übernahme einiger dieser Produkte und Komponenten auf dem Sekundärserver erfolgen, während andere Komponenten nicht übernahmefähig sind.

Voraussetzungen für die automatisierte Clientübernahme

Bevor Sie den Client für die automatisierte Clientübernahme konfigurieren oder verwenden, müssen der Client für Sichern/Archivieren und der IBM Spectrum Protect-Server mehrere Voraussetzungen erfüllen.

Stellen Sie sicher, dass der Client die folgenden Voraussetzungen für die automatisierte Clientübernahme erfüllt:

- Auf dem Primärserver, dem Sekundärserver und dem Client für Sichern/Archivieren muss IBM Spectrum Protect Version 7.1 oder eine höhere Version ausgeführt werden.
- Der Primärserver und der Sekundärserver müssen für die Knotenreplikation konfiguriert sein.
- Der Clientknoten muss mithilfe des Serverbefehls `REGISTER NODE REPLSTATE=ENABLED` oder `UPDATE NODE REPLSTATE=ENABLED` für die Knotenreplikation auf dem Quellenreplikationsserver konfiguriert sein.
- Die automatisierte Clientübernahme ist auf dem Client standardmäßig aktiviert. Ist jedoch die Option `usereplicationfailover no` in der Clientoptionsdatei angegeben, geben Sie entweder hier den Wert yes an oder entfernen Sie die Option.
- Die Clientoptionsdatei muss gültige Verbindungsinformationen für den Sekundärserver enthalten. Während des Normalbetriebs werden diese Informationen automatisch vom Primärserver an den Client gesendet.

- Um die vom Primärserver gesendeten Verbindungsinformationen des Sekundärservers speichern zu können, benötigt der Client Schreibzugriff auf die Datei dsm.opt (Windows-Clients) bzw. die Datei dsm.sys (AIX-, Linux-, Mac OS X- und Oracle Solaris-Clients). Wenn der Client keinen Schreibzugriff auf diese Dateien hat, werden die Informationen des Sekundärservers nicht in der Clientoptionsdatei gespeichert und ein Fehler wird im Fehlerprotokoll hinzugefügt.
- Benutzer ohne Rootberechtigung können die Standardposition für die Knotenreplikationstabelle nicht verwenden. Sie müssen die Option nrtablepath in die Datei dsm.sys einfügen, um eine andere Position anzugeben. Weitere Informationen finden Sie in Nrtablepath.
- Bevor die Verbindungsinformationen des Sekundärservers an die Optionsdatei gesendet werden, müssen die folgenden Prozesse stattfinden:
  - Der Client muss mindestens einmal auf dem Quellenreplikationsserver gesichert werden.
  - Der Clientknoten muss mindestens einmal auf dem Zielreplikationsserver repliziert werden.
- Die Übernahme erfolgt für Clientknoten, die mit der Unterstützung für den Clientknoten-Proxy gesichert werden, wenn sowohl der Ziel- als auch der Agentenknoten für die Replikation auf dem Zielreplikationsserver konfiguriert ist. Wenn der Zielknoten explizit repliziert wird, wird auch der Agentenknoten zusammen mit der Proxy-Beziehung implizit auf dem Zielreplikationsserver repliziert.
  Beispiel: Node_B wird mit dem folgenden Befehl die Berechtigung zur Ausführung von Clientoperationen im Namen von Node_A erteilt:

  ```
  grant proxynode target=Node_A agent=Node_B
  ```

  Ist für beide Knoten die Replikation mit der Option `replstate=enabled` in der Knotendefinition konfiguriert, werden auch Node_B und die Proxy-Beziehung repliziert, wenn Node_A repliziert wird.

Einschränkungen für die automatisierte Clientübernahme

Der folgende Abschnitt enthält Informationen, die den Prozess der automatisierten Clientübernahme und die damit verbundenen Einschränkungen erläutern.

Für die automatisierte Clientübernahme gelten die folgenden Einschränkungen:

- Wenn sich der Client im Übernahmemodus befindet, können Sie keine Funktionen verwenden, für die eine Datenspeicherung auf dem Sekundärserver erforderlich ist (z. B. Sicherungs- oder Archivierungsoperationen). Sie können lediglich Datenwiederherstellungsfunktionen verwenden, z. B. Zurückschreibungs-, Abruf- oder Abfrageoperationen. Sie können auch Clientoptionen bearbeiten und das Kennwort des IBM Spectrum Protect-Clients ändern.
- Zeitpläne werden nicht auf dem Sekundärserver repliziert. Daher werden keine Zeitpläne ausgeführt, während der Primärserver nicht verfügbar ist.
- Nachdem der Client eine Verbindung zum Sekundärserver im Übernahmemodus hergestellt hat, versucht er erst wieder bei der nächsten Erstanmeldung am Server eine Verbindung zum Primärserver herzustellen. Der Client unternimmt nur dann einen Übernahmeversuch auf dem Sekundärserver, wenn die einleitende Verbindung zum Primärserver fehlschlägt. Die einleitende Verbindung ist die erste Verbindung, die der Client zum Server herstellt.

  Wenn der Primärserver während einer Clientoperation ausfällt, findet keine Übernahme des Clients auf dem Sekundärserver statt und die Operation schlägt fehl. Sie müssen den Client erneut starten, damit eine Übernahme auf dem Sekundärserver stattfinden kann, und dann die Clientoperation wiederholen.

  Zurückschreibungsoperationen, die unterbrochen werden, wenn der Primärserver ausfällt, können nach der Übernahme des Clients nicht erneut gestartet werden. Sie müssen nach der Übernahme des Clients auf dem Sekundärserver die gesamte Zurückschreibungsoperation erneut ausführen.

- Wird das IBM Spectrum Protect-Kennwort vor der Replikation des Clientknotens geändert, wird es zwischen dem Primärserver und dem Sekundärserver nicht synchronisiert. Wenn während dieser Zeit eine Übernahme stattfindet, müssen Sie das Kennwort auf dem Sekundärserver und auf dem Client manuell zurücksetzen. Wenn der Primärserver wieder online ist, muss das Kennwort zurückgesetzt werden, damit der Client eine Verbindung zum Primärserver herstellen kann.

  Wird das Kennwort zurückgesetzt, während eine Verbindung des Clients zum Sekundärserver besteht, muss das Kennwort auf dem Primärserver zurückgesetzt werden, bevor sich der Client am Primärserver anmelden kann. Diese Einschränkung gilt, wenn für die Option passwordaccess der Wert generate definiert ist oder wenn das Kennwort manuell zurückgesetzt wird.

- Wenn Sie Clientdaten gesichert oder archiviert haben, der Primärserver jedoch ausfällt, bevor er den Clientknoten repliziert, werden die neuesten Sicherungs- bzw. Archivierungsdaten nicht auf dem Sekundärserver repliziert. Der Replikationsstatus des Dateibereichs ist nicht aktuell. Wenn Sie versuchen, die Daten im Übernahmemodus zurückzuschreiben oder abzurufen, während der Replikationsstatus nicht aktuell ist, wird in einer Nachricht angezeigt, dass die Daten, die Sie wiederherstellen wollen, nicht auf dem neuesten Stand sind. Sie können mit der Wiederherstellung fortfahren oder warten, bis der Primärserver wieder online ist.
- Wenn auf dem Quellenreplikationsserver eine Benutzer-ID mit Administrator- und Clienteignerberechtigung vorhanden ist und der Name der Benutzer-ID mit dem Namen des Clientknotens identisch ist, wird die Benutzer-ID mit Administratorberechtigung während des Knotenreplikationsprozesses auf dem Server repliziert. Ist eine solche Benutzer-ID auf dem Quellenreplikationsserver nicht vorhanden, wird während des Replikationsprozesses diese Administratordefinition auf dem Zielreplikationsserver nicht erstellt.

  Sind dem Knoten andere Benutzer-IDs mit Administratorberechtigung zugeordnet, muss der IBM Spectrum Protect-Administrator die Benutzer-IDs mit Administratorberechtigung auf dem Zielreplikationsserver manuell konfigurieren. Andernfalls kann der Benutzer mit Verwaltungsaufgaben keine Verbindung zum Zielreplikationsserver (Sekundärserver) mit dem IBM Spectrum Protect-Web-Client herstellen.

- Wenn Sie eine Datei von IBM Spectrum Protect zurückschreiben und das Dateisystem von IBM Spectrum Protect for Space Management verwaltet wird, dürfen Sie die Datei nicht als Stubdatei zurückschreiben. Sie müssen die vollständige Datei zurückschreiben. Verwenden Sie die Option `restoremigstate=no`, um die vollständige Datei zurückzuschreiben. Wenn Sie die Datei als Stubdatei vom Zielserver zurückschreiben, kann dies folgende Konsequenzen haben:
  - Sie können die Datei nicht mithilfe des IBM Spectrum Protect for Space Management-Clients vom IBM Spectrum Protect-Quellenserver zurückrufen.
  - Die Datei verfällt durch den für den IBM Spectrum Protect-Quellenserver ausgeführten IBM Spectrum Protect for Space Management-Abgleichsprozess. Wenn die Datei durch einen Abgleichsprozess verfällt, können Sie die vollständige Datei mithilfe des Clients für Sichern/Archivieren und der Option `restoremigstate=no` zurückschreiben.

Übernahmefunktionalität der IBM Spectrum Protect-Komponenten

IBM Spectrum Protect-Komponenten und -Produkte verwenden den Client für Sichern/Archivieren oder die API für die Sicherung von Daten auf dem IBM Spectrum Protect-Primärserver. Wenn der Primärserver ausfällt, kann eine Übernahme einiger dieser Produkte und Komponenten auf dem Sekundärserver erfolgen, während andere Komponenten nicht übernahmefähig sind.

Weitere Informationen zur Übernahmefunktionalität der IBM Spectrum Protect-Komponenten und -Produkte finden Sie in Technote 1649484.

Zugehörige Tasks:
Status replizierter Clientdaten bestimmen

Client für automatisierte Übernahme konfigurieren

Sie können durch eine manuelle Konfiguration festlegen, dass eine automatische Übernahme des Clients auf dem Sekundärserver stattfindet.

Vorbereitende Schritte

Vor der Konfiguration:

- Stellen Sie sicher, dass der Clientknoten an der Knotenreplikation auf dem Primärserver beteiligt ist.
- Stellen Sie sicher, dass der Client die Voraussetzungen für die automatisierte Clientübernahme erfüllt.
- Verwenden Sie diese Prozedur nur, wenn die Verbindungsinformationen für den Sekundärserver nicht aktuell oder in der Clientoptionsdatei nicht vorhanden sind.

Informationen zu diesem Vorgang

Eine manuelle Konfiguration des Clients für die automatisierte Übernahme ist in folgenden Situationen denkbar:

- Die Konfiguration des Sekundärservers wurde geändert und der Primärserver fällt aus, bevor sich der Client beim Server anmeldet. Wenn Sie die Verbindungsinformationen manuell hinzufügen, ist eine Übernahme des Clients auf dem Sekundärserver möglich.
- Die Verbindungsinformationen des Sekundärservers in der Clientoptionsdatei wurden versehentlich ganz oder teilweise gelöscht.
  Tipp: Anstelle einer manuellen Konfiguration der Clientoptionsdatei können Sie den Befehl dsmc q session ausführen, wobei Sie zur Anmeldung beim Primärserver aufgefordert werden. Die Verbindungsinformationen für den Sekundärserver werden automatisch an die Clientoptionsdatei gesendet.

Vorgehensweise

Gehen Sie wie folgt vor, um den Client manuell für die automatisierte Übernahme zu konfigurieren:

1. Stellen Sie sicher, dass die automatisierte Clientübernahme für den Client aktiviert ist, indem Sie dafür sorgen, dass die Option `usereplicationfailover` entweder in der Clientoptionsdatei nicht vorhanden oder auf `yes` gesetzt ist. Die automatisierte Clientübernahme ist auf dem Client standardmäßig aktiviert, daher ist die Option `usereplicationfailover` in der Clientoptionsdatei nicht erforderlich.
2. Bitten Sie den Administrator des IBM Spectrum Protect-Servers um Auskunft über die Verbindungsinformationen des Sekundärservers und fügen Sie diese Informationen am Anfang der Clientoptionsdatei ein. Gruppieren Sie die Anweisungen in einer Zeilengruppe unter der Anweisung replservername.
    AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeFügen Sie beispielsweise die folgenden Anweisungen in die Datei dsm.sys ein:

```
REPLSERVERNAME          TARGET
   REPLTCPSERVERADDRESS 192.0.2.9
   REPLTCPPORT          1501
   REPLSSLPORT          1502
   REPLSERVERGUID       60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

SErvername     server_a
       COMMMethod              TCPip
   TCPPort                  1500
       TCPServeraddress         server_hostname1.example.com
```

```
   PASSWORDAccess            prompt
   MYREPLICATIONServer       TARGET
```

Windows-BetriebssystemeFügen Sie beispielsweise die folgenden Anweisungen in die Datei dsm.opt ein:

```
REPLSERVERNAME          TARGET
   REPLTCPSERVERADDRESS 192.0.2.9
   REPLTCPPORT          1501
   REPLSSLPORT          1502
   REPLSERVERGUID       60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

MYREPLICATIONServer TARGET
MYPRIMARYSERVERNAME SERVER1
```

3. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeBenutzer ohne Rootberechtigung müssen eine Position für die Knotenreplikationstabelle angeben, indem die Option nrtablepath zur Datei dsm.sys hinzugefügt wird. Der Client für Sichern/Archivieren verwendet diese Tabelle für die Speicherung von Informationen zu jeder Sicherungs- oder Archivierungsoperation auf dem IBM Spectrum Protect-Server.
   Sie müssen eine Position angeben, für die Ihre Benutzer-ID Schreibzugriff hat. Beispiel:

   ```
   nrtablepath /Volumes/nrtbl
   ```

   Einschränkung: Geben Sie nicht das Stammverzeichnis (/) als Position der Knotenreplikationstabelle an.
4. Speichern und schließen Sie die Clientoptionsdatei.
5. Starten Sie die GUI des Clients für Sichern/Archivieren erneut oder melden Sie sich über die Befehlszeilenschnittstelle beim IBM Spectrum Protect-Server an. Der Client ist mit dem Sekundärserver verbunden.

Beispiel

Nachdem Sie die automatisierte Clientübernahme auf dem Client konfiguriert haben und der Client versucht, sich beim Server anzumelden, wird die folgende Beispielbefehlsausgabe angezeigt:

```
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
  Clientversion 8, Release 1, Stufe 0.0
  Clientdatum/-zeit: 16.12.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016. Alle Rechte vorbehalten.

Knotenname: MY_NODE_NAME
ANS2106I Verbindung zum primären IBM Spectrum Protect-Server 192.0.2.1 ist
fehlgeschlagen.

ANS2107I Es wird versucht, eine Verbindung zum sekundären Server TARGET
unter 192.0.2.9 : 1501 herzustellen.

Knotenname: MY_NODE_NAME
Sitzung hergestellt mit Server TARGET: Windows
  Serverversion 8, Release 1, Stufe 0.0
  Serverdatum/-zeit: 16.12.2016 12:05:35  Letzter Zugriff: 15.12.2016 09:55:56

  Sitzung im Übernahmemodus auf dem sekundären Server aufgebaut
ANS2108I Verbindung zum sekundären Server TARGET hergestellt.
```

Nächste Schritte

Sie können alle replizierten Daten im Übernahmemodus zurückschreiben oder abrufen.

Zugehörige Konzepte:
Automatisierte Clientübernahme - Übersicht
Zugehörige Tasks:
Daten während einer Übernahme zurückschreiben oder abrufen
Zugehörige Verweise:
Forcefailover
Windows-BetriebssystemeMyprimaryserver
Myreplicationserver
Nrtablepath
Replserverguid
Replservername
Replsslport
Repltcpport
Repltcpseveraddress
Usereplicationfailover

Status replizierter Clientdaten bestimmen

Bevor Sie Clientdaten vom Sekundärserver zurückschreiben oder abrufen, können Sie prüfen, ob die neueste Sicherung des Clients auf dem Sekundärserver repliziert wurde.

Informationen zu diesem Vorgang

Sie können den Status replizierter Clientdaten abrufen, um festzustellen, ob die neueste Clientsicherung auf dem Sekundärserver repliziert wurde.

Wenn die Zeitmarke der neuesten Sicherungsoperation auf dem Client mit der Zeitmarke der Sicherung auf dem Sekundärserver übereinstimmt, ist der Replikationsstatus aktuell.

Wenn die Zeitmarke der neuesten Sicherungsoperation von der Zeitmarke der Sicherung auf dem Sekundärserver abweicht, ist der Replikationsstatus nicht aktuell. Diese Situation kann eintreten, wenn Sie den Client zwar gesichert haben, der Primärserver aber vor dem Replizieren des Clientknotens ausfällt.

Vorgehensweise

Geben Sie den folgenden Befehl in die Eingabeaufforderung ein, um den Status der replizierten Clientdaten zu bestimmen:

```
dsmc query filespace -detail
```

Die folgende Beispielausgabe zeigt, dass die Zeitmarken auf dem Server und auf dem Client übereinstimmen und dass daher der Replikationsstatus aktuell ist:

```
Nr.  Datum ltzt Teilsich. Typ    FSID  Unicode  Replikation  Dateibereichsname
---  --------------       -------     ----  -------  -----------  ----------------
  1    00.00.0000 00:00:00   HFS            9  Yes      Current         /

        Letztes
        Speicherdatum       Server                 Lokal
        ---------------     ------                 -----
                  Sicherungsdaten:    22.04.2013 19:39:17     22.04.2013 19:39:17
             Archivierungsdaten:    Kein Datum verfügbar    Kein Datum verfügbar
```

Die folgende Beispielausgabe zeigt, dass die Zeitmarken auf dem Server und auf dem Client nicht übereinstimmen und dass daher der Replikationsstatus nicht aktuell ist:

```
Nr.  Datum ltzt Teilsich. Typ    FSID  Unicode  Replikation  Dateibereichsname
---  --------------       -------     ----  -------  -----------  ----------------
  1    00.00.0000 00:00:00   HFS            9  Yes      Not Current  /

        Letztes
        Speicherdatum       Server                 Lokal
        ---------------     ------                 -----
                  Sicherungsdaten:    22.04.2013 19:39:17     24.04.2013 19:35:41
             Archivierungsdaten:    Kein Datum verfügbar    Kein Datum verfügbar
```

Nächste Schritte

Wenn Sie versuchen, die Daten im Übernahmemodus zurückzuschreiben, während der Replikationsstatus nicht aktuell ist, wird in einer Nachricht angezeigt, dass die Daten, die Sie zurückschreiben wollen, nicht auf dem neuesten Stand sind. Sie können mit der Zurückschreibung fortfahren oder warten, bis der Primärserver wieder online ist.

Zugehörige Tasks:
Daten während einer Übernahme zurückschreiben oder abrufen
Zugehörige Verweise:
Nrtablepath

Automatisierte Clientübernahme verhindern

Sie können in der Konfiguration des Clients festlegen, dass die automatisierte Clientübernahme auf dem Sekundärserver verhindert werden soll.

Informationen zu diesem Vorgang

Sie können die automatisierte Clientübernahme verhindern, z. B., wenn Sie wissen, dass die Daten auf dem Clientknoten vor dem Ausfall des Primärservers nicht auf dem Sekundärserver repliziert wurden. In diesem Fall wollen Sie verhindern, dass replizierte Daten vom Sekundärserver wiederhergestellt werden, die möglicherweise veraltet sind.

Vorgehensweise

Um eine Übernahme des Clientknotens auf dem Sekundärserver zu verhindern, fügen Sie die folgende Anweisung in die Clientoptionsdatei ein:

```
usereplicationfailover no
```

Diese Einstellung setzt die Konfiguration außer Kraft, die der IBM Spectrum Protect-Serveradministrator auf dem Primärserver angibt.

Ergebnisse

Es findet keine automatische Übernahme des Clientknotens auf dem Sekundärserver statt, wenn er den nächsten Versuch unternimmt, eine Verbindung zum inaktiven Primärserver herzustellen.

Zugehörige Tasks:
Status replizierter Clientdaten bestimmen
Zugehörige Verweise:
Usereplicationfailover

Clientübernahme erzwingen

Es kann eine sofortige Übernahme des Clients auf dem Sekundärserver stattfinden, auch wenn der Primärserver betriebsbereit ist. Sie können mit diesem Verfahren beispielsweise prüfen, ob eine Übernahme des Clients auf dem erwarteten Sekundärserver stattfindet.

Vorgehensweise

Gehen Sie wie folgt vor, um eine sofortige Übernahme des Clients auf dem Sekundärserver zu erzwingen:

1. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie die Option forcefailover yes in die Clientsystemoptionsdatei (dsm.sys) ein.
2. Windows-BetriebssystemeFügen Sie die Option forcefailover yes in die Clientoptionsdatei (dsm.opt) ein.
3. Stellen Sie ein Verbindung zum Sekundärserver her, indem Sie die GUI des Clients für Sichern/Archivieren erneut starten oder indem Sie eine Befehlssitzung mit dem Befehl dsmc starten.
4. Optional: Sie können eine Verbindung zum Sekundärserver auch herstellen, indem Sie die Option `-forcefailover=yes` in einem Befehl angeben, anstatt die Optionsdatei zu aktualisieren. Beispiel:

   ```
   dsmc q sess -forcefailover=yes
   ```

Nächste Schritte

Sie können mit einer der folgenden Methoden überprüfen, ob eine Verbindung zum Sekundärserver besteht:

- Überprüfen Sie das Feld Informationen zum sekundären Server im Fenster Verbindungsinformationen in der GUI des Clients für Sichern/Archivieren.
- Überprüfen Sie die Befehlsausgabe, wenn Sie eine Befehlssitzung starten. Der Status des Sekundärservers wird in der Ausgabe angezeigt.

Linux-BetriebssystemeWindows-Betriebssysteme

Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren

Bevor Sie Tivoli Storage Manager FastBack-Clientdaten sichern oder archivieren können, müssen Sie Konfigurationstasks ausführen.

Stellen Sie zunächst sicher, dass der Client für Sichern/Archivieren konfiguriert und der Tivoli Storage Manager FastBack-Client installiert wurde.

Installieren Sie den FastBack-Client anhand der Informationen in Tivoli Storage Manager FastBack.

Linux-BetriebssystemeFühren Sie nach der Installation des FastBack-Clients die folgenden Tasks aus:

Windows-BetriebssystemeFühren Sie nach der Installation des FastBack-Clients die folgenden Tasks aus. Sie können auch den Clientkonfigurationsassistenten für Tivoli Storage Manager FastBack verwenden.

1. Registrieren Sie einen Knoten für jeden FastBack-Client, auf dem Daten gesichert und archiviert werden. Der Knotenname muss der kurze Hostname des FastBack-Clients sein.

   Dies ist eine einmalige Konfiguration, die für jeden FastBack-Client, dessen Datenträger gesichert oder archiviert werden müssen, einmal ausgeführt wird.

   Dieser Registrierungsschritt muss nur dann manuell ausgeführt werden, wenn der Client für Sichern/Archivieren als eigenständige Anwendung verwendet wird.

   Das Administration Center führt diese Knotenregistrierung automatisch aus, wenn der Benutzer über das Administration Center Zeitpläne für die Archivierung oder Sicherung von FastBack-Daten erstellt. Ab Version 7.1 ist die Komponente 'Administration Center' nicht mehr in Tivoli Storage Manager- oder IBM Spectrum Protect-Verteilungen enthalten. FastBack-Benutzer, die über ein Administration Center aus einem früheren Server-Release verfügen, können damit weiterhin FastBack-Zeitpläne erstellen und ändern. Wenn noch kein Administration Center installiert ist, können Sie die Vorgängerversion von ftp://public.dhe.ibm.com/storage/tivoli-storage-

management/maintenance/admincenter/v6r3/ herunterladen. Wenn kein Administration Center installiert ist, müssen Sie FastBack-Zeitpläne auf dem IBM Spectrum Protect-Server erstellen und ändern. Informationen zur Erstellung von Zeitplänen auf dem Server finden Sie in der Dokumentation für den IBM Spectrum Protect-Server.

2. Erteilen Sie mit dem Serverbefehl GRANT PROXY Ihrem aktuellen Knoten des Clients für Sichern/Archivieren Proxy-Berechtigung auf jedem Knoten, der den in Schritt 1 erstellten FastBack-Client darstellt. Der FastBack-Knoten muss das Ziel und der aktuelle Clientknoten der Proxy sein.

   Dies ist eine einmalige Konfiguration, die vom Administration Center ausgeführt wird, wenn die Sicherung oder Archivierung vom Administration Center eingeleitet wird.

3. Führen Sie den Befehl set password aus, um die Berechtigungsnachweise der FastBack-Repositorys zu speichern, zu denen der Client für Sichern/Archivieren eine Verbindung herstellt. Führen Sie den Befehl `set password -type=fastback` einmal für jedes Repository aus, zu dem der Client für Sichern/Archivieren voraussichtlich eine Verbindung herstellt.
   Die gespeicherten Berechtigungsnachweise sind von den folgenden Konfigurationen abhängig:
   - Client für Sichern/Archivieren auf dem FastBack-Server
   - Client für Sichern/Archivieren auf dem FastBack Disaster Recovery Hub
   - Client für Sichern/Archivieren auf einer dedizierten Proxy-Workstation

Informationen zur Integration von IBM Spectrum Protect und Tivoli Storage Manager FastBack finden Sie in Tivoli Storage Manager FastBack und IBM Spectrum Protect integrieren.

Zugehörige Konzepte:
Installationsvoraussetzungen für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Clientdaten
Windows-BetriebssystemeClientkonfigurationsassistent für Tivoli Storage Manager FastBack
Windows-BetriebssystemeClient für Sichern/Archivieren für den Schutz von FastBack-Clientdaten konfigurieren
Zugehörige Verweise:
Set Password
Windows-Betriebssysteme

Client für Sichern/Archivieren für den Schutz von FastBack-Clientdaten konfigurieren

Sie können den Client für Sichern/Archivieren mithilfe des Clientkonfigurationsassistenten für den Schutz von FastBack-Clientdaten konfigurieren.

Bevor Sie den IBM Spectrum Protect-Clientkonfigurationsassistenten für FastBack verwenden können, müssen Sie die folgenden Tasks ausführen:

- Stellen Sie sicher, dass entweder der FastBack-Server oder der FastBack Disaster Recovery Hub installiert und für die kurzfristige Datenaufbewahrung konfiguriert ist.
- Stellen Sie außerdem sicher, dass mindestens eine Momentaufnahme erstellt wurde.
- Stellen Sie sicher, dass der Client für Sichern/Archivieren ordnungsgemäß für den IBM Spectrum Protect-Server konfiguriert ist. Stellen Sie außerdem sicher, dass der Clientakzeptorservice (dsmcad.exe) aktiv ist. Sie können den IBM Spectrum Protect-Clientkonfigurationsassistenten in der GUI des Clients für Sichern/Archivieren verwenden, nachdem Sie den Client für Sichern/Archivieren installiert haben.
- Führen Sie für die folgenden Zwecke eine einmalige Einrichtung nach der Installation aus:
  - Angabe des FastBack-Benutzernamens und -Kennworts, den bzw. das der Assistent verwenden soll, um Datenträger im FastBack-Repository abzufragen und bereitzustellen
  - Ausführung von IBM Spectrum Protect-Scheduler-Scripts
- Definition der Datei für FastBack-Berechtigungsnachweise. Die Benutzer-ID, die Sie angeben, muss Tivoli Storage Manager FastBack-Administratorberechtigung haben.
  1. Konfiguration der Benutzer-ID und des Kennworts. Führen Sie den folgenden Befehl auf der Workstation aus, auf der der Client für Sichern/Archivieren und der FastBack-Server oder Disaster Recovery Hub installiert sind:

     ```
     cd <TSM_FastBack-Installationsposition>\FastBack\shell
     ```

     Dabei ist <TSM_FastBack-Installationsposition> die Verzeichnisposition, an der der Tivoli Storage Manager FastBack-Client installiert ist.

  2. Falls nicht vorhanden, erstellen Sie einen Ordner mit dem Namen FastbackTSMScripts auf dem Systemlaufwerk der Workstation. Verwenden Sie dazu den folgenden Befehl:

     ```
     mkdir <Systemlaufwerk der Maschine>:\FastbackTSMScripts
     ```

  3. Führen Sie den Befehl fastbackshell aus:

     ```
     FastBackShell -c encrypt -u Benutzername -d Domäne -p Kennwort -f
     <Systemlaufwerk der Maschine>:\FastbackTSMScripts\credential.txt
     ```

     In diesem Befehlsbeispiel werden die folgenden Optionen verwendet:

- -u gibt den Tivoli Storage Manager FastBack-Administratornamen an.
- -p gibt das Tivoli Storage Manager FastBack-Administratorkennwort an.
- -d gibt die Tivoli Storage Manager FastBack-Domäne für den Benutzernamen an.
- -f gibt die Ausgabedatei an, in die die verschlüsselten Berechtigungsnachweise geschrieben werden sollen.

Wichtig: Die Datei für Berechtigungsnachweise muss mit dem Namen "credential.txt" generiert werden. Damit der Assistent ordnungsgemäß funktioniert, muss die Datei für Berechtigungsnachweise sich außerdem im Verzeichnis FastbackTSMScripts im Systemlaufwerk der Workstation befinden.

Sie können den Clientkonfigurationsassistenten in der Java™-GUI des Clients für Sichern/Archivieren oder im Web-Client für Sichern/Archivieren verwenden.

Führen Sie die folgenden Schritte aus, um den Clientkonfigurationsassistenten in der Java-GUI zu verwenden:

1. Stellen Sie sicher, dass der Client für Sichern/Archivieren ordnungsgemäß für den IBM Spectrum Protect-Server konfiguriert ist.
2. Der Konfigurationsassistent wird automatisch gestartet, um die Konfigurationsdatei zu erstellen.
3. Befolgen Sie die angezeigten Anweisungen, um den Assistenten auszuführen.
4. Wählen Sie im Hauptfenster der GUI des Clients für Sichern/Archivieren Dienstprogramme > Setup-Assistent aus.
5. Wählen Sie auf der Begrüßungsseite Hilfe zum Konfigurieren des Clients zum Schützen der FastBack-Clientdaten aus und klicken Sie auf Weiter.
6. Führen Sie den Konfigurationsprozess mit dem Assistenten aus.

Führen Sie die folgenden Schritte aus, um den Clientkonfigurationsassistenten im Web-Client zu starten:

1. Stellen Sie sicher, dass der Web-Client ordnungsgemäß für den IBM Spectrum Protect-Server konfiguriert ist und dass der IBM Spectrum Protect-Clientakzeptorservice aktiv ist.

   Gehen Sie wie folgt vor, um den Web-Client zu konfigurieren:

   a. Klicken Sie im Hauptfenster der GUI des Clients für Sichern/Archivieren in der Java-GUI auf Dienstprogramme > Setup-Assistent.
   b. Wählen Sie auf der Begrüßungsseite Hilfe zum Konfigurieren des Web-Clients aus und klicken Sie auf Weiter. Befolgen Sie die angezeigten Anweisungen, um den Assistenten auszuführen.
2. Starten Sie den Web-Client. Geben Sie in Ihrem Web-Browser den Clientknotennamen und die Nummer des Anschlusses an, an dem der Clientakzeptorservice ausgeführt wird.

   Beispiel: `http://<Maschinenname_oder_IP-Adresse>:1585`

3. Klicken Sie im Hauptfenster der GUI des Clients für Sichern/Archivieren auf Dienstprogramme > Setup-Assistent.
4. Wählen Sie auf der Begrüßungsseite Hilfe zum Konfigurieren des Clients zum Schützen der FastBack-Clientdaten aus und klicken Sie auf Weiter.
5. Führen Sie den Konfigurationsprozess mit dem Assistenten aus.

Zugehörige Konzepte:
Clientkonfigurationsassistent für Tivoli Storage Manager FastBack
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

Konfiguration und Verwendung der Clusterumgebung

Der Begriff *Cluster* hat in unterschiedlichen Umgebungen unterschiedliche Bedeutungen. Er kann Folgendes bedeuten: hoch verfügbar, hohe Leistung, Lastausgleich, Grid-Computing oder eine Kombination all dieser Begriffe.

Es sind derzeit mehrere Clusteringprodukte für UNIX und Linux verfügbar, und in diesem Abschnitt werden diejenigen Aspekte einer Clusteringumgebung definiert, die vorhanden sein müssen, damit diese Sicherungsmethodik korrekt funktioniert. Ein Basisverständnis über die Funktionsweise Ihrer Clustersoftware wird benötigt. Aktivitäten in Bezug auf Clustersoftware wie z. B. die Entwicklung von Anwendungsstart- und -stoppscripts werden in diesem Abschnitt nicht beschrieben.

Eine Clusterumgebung bezieht sich auf eine UNIX- oder Linux-Umgebung, die folgende Merkmale aufweist:

- Platten werden von physischen Workstations gemeinsam genutzt, entweder auf exklusive Weise (zu jedem Zeitpunkt hat nur ein Host Zugriff auf die logische Platte) oder gleichzeitig.
- Platten werden dem Host als lokale Festplatten und nicht als Netzressourcen angezeigt.
  Wichtig: Hängen Sie die Dateisysteme lokal an das System an und nicht über ein LAN-gestütztes Dateifreigabeprotokoll wie z. B. Network File System (NFS).
- Mountpunkte lokaler Festplatten sind auf jedem physischen Host in der Umgebung identisch (wenn das Dateisystem `/group1_disk1` von `NodeA zu NodeB` fehlschlägt, wird es auf `NodeB` als `/group1_disk1` angehängt).

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeÜbersicht über Clusterumgebungen
  Clusterumgebungen können in vielen unterschiedlichen Konfigurationen definiert werden. In diesem Abschnitt werden die gängigsten Clusterkonfigurationen beschrieben.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeClient für Sichern/Archivieren in einer Clusterumgebung konfigurieren

Der Client für Sichern/Archivieren ist so konzipiert, dass er die Sicherung von Clusterlaufwerken verwaltet, indem er den Client für Sichern/Archivieren in den Kontext der Ressourcengruppen des Clusters stellt.

- Mac OS X-BetriebssysemeAIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeWeb-Client-Zugriff in einer Clusterumgebung aktivieren
  Wenn während einer Übernahmebedingung IBM Spectrum Protect-Web-Client-Zugriff erforderlich ist, müssen Sie den Web-Clientakzeptordämon, der dem Cluster zugeordnet ist, so konfigurieren, dass für ihn zusammen mit der Clusterressource eine Übernahme erfolgt.
- AIX-BetriebssysemeTraditionelle AIXIBM PowerHA SystemMirror-Konfigurationen migrieren
  Wenn Sie den Client für Sichern/Archivieren gegenwärtig in einer IBM® PowerHA SystemMirror-Umgebung mit der Option clusternode verwenden, müssen Sie Ihre aktuellen Konfigurationen aktualisieren. Die Option clusternode wird nicht mehr unterstützt.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-Betriebssysteme

Übersicht über Clusterumgebungen

Clusterumgebungen können in vielen unterschiedlichen Konfigurationen definiert werden. In diesem Abschnitt werden die gängigsten Clusterkonfigurationen beschrieben.

- Mac OS X-BetriebssysemeAIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeAktiv/Aktiv: Pool-Clusterressourcen
  In einer Konfiguration Aktiv/Aktiv verwaltet jeder Knoten aktiv mindestens eine Ressource und wird als Sicherung für eine oder mehrere Ressourcen im Cluster konfiguriert. Aktiv/Aktiv ist die häufigste Form einer Clusterumgebung.
- Mac OS X-BetriebssysemeAIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeAktiv/Passiv: Fehlertolerant
  In einer Konfiguration Aktiv/Passiv verwaltet ein Knoten aktiv die Ressource.
- Mac OS X-BetriebssysemeAIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeGleichzeitiger Zugriff
  In einer gleichzeitig ablaufenden Konfiguration verwalten mehrere Knoten eine Ressource. Wenn ein Fehler auftritt, wird die Ressource von den anderen Knoten weiter verwaltet.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-Betriebssysteme

Aktiv/Aktiv: Pool-Clusterressourcen

In einer Konfiguration Aktiv/Aktiv verwaltet jeder Knoten aktiv mindestens eine Ressource und wird als Sicherung für eine oder mehrere Ressourcen im Cluster konfiguriert. Aktiv/Aktiv ist die häufigste Form einer Clusterumgebung.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-Betriebssysteme

Aktiv/Passiv: Fehlertolerant

In einer Konfiguration Aktiv/Passiv verwaltet ein Knoten aktiv die Ressource.

Der andere Knoten wird nur verwendet, wenn es beim Primärknoten zu einem Fehler kommt und die Ressource eine Übernahme benötigt. Ein Cluster Aktiv/Passiv ist ein Subtyp eines Clusters Aktiv/Aktiv.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-Betriebssysteme

Gleichzeitiger Zugriff

In einer gleichzeitig ablaufenden Konfiguration verwalten mehrere Knoten eine Ressource. Wenn ein Fehler auftritt, wird die Ressource von den anderen Knoten weiter verwaltet.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-Betriebssysteme

Client für Sichern/Archivieren in einer Clusterumgebung konfigurieren

Der Client für Sichern/Archivieren ist so konzipiert, dass er die Sicherung von Clusterlaufwerken verwaltet, indem er den Client für Sichern/Archivieren in den Kontext der Ressourcengruppen des Clusters stellt.

Informationen zu diesem Vorgang

Dies hat den Vorteil, dass Daten von lokalen Ressourcen gesichert werden können (im Gegensatz zum Zugriff auf die Daten über das Netz), um die Leistung der Sicherungsoperation zu maximieren und die Sicherungsdaten in Bezug auf die Ressourcengruppe zu verwalten. Deshalb kann der Client für Sichern/Archivieren Daten immer auf Clusterressourcen sichern, als ob die Daten lokale Daten wären, und die Leistung beim Sichern maximieren. Dadurch wird sichergestellt, dass kritische Daten über Systemausfälle hinweg gesichert werden.

Beispiel: Eine Clusterumgebung Aktiv/Aktiv hat drei physische Hosts im Cluster mit den Namen `NodeA`, `NodeB` und `NodeC`.

Die Knoten verfügen über folgende Qualitäten:

- `NodeA` ist Eigner der Clusterressource mit den Dateisystemen `/A1` und `/A2`
- `NodeB` ist Eigner der Clusterressource mit den Dateisystemen `/B1` und `/B2`
- `NodeC` ist Eigner der Clusterressource mit den Dateisystemen `/C1` und `/C2`

Anmerkung: `NodeA` hat möglicherweise noch zwei Datenträger, `/fs1` und `/fs2`, die keine Clusterdatenträger sind und gesichert werden müssen.

Um die beste Sicherungsleistung zu erzielen, möchten Sie unter Umständen, dass alle Knoten im Cluster die Sicherungen der in ihrem Besitz befindlichen gemeinsam genutzten Dateisysteme ausführen. Wenn eine Knotenübernahme auftritt, werden die Sicherungstasks des fehlgeschlagenen Knotens auf den Knoten verschoben, auf dem die Übernahme auftrat. Beispiel: Wenn `NodeA` fehlschlägt und von `NodeB` übernommen wird, wird die Sicherung von `/A1` und `/A2` auf `NodeB` verschoben.

Nachfolgend die Voraussetzungen, die erfüllt sein müssen, bevor der Client für Sichern/Archivieren für das Sichern von Cluster- und Nicht-Clusterdatenträgern konfiguriert werden kann:

- Für jede Ressourcengruppe, die geschützt werden soll, muss ein separater Schedulerprozess des Clients für Sichern/Archivieren ausgeführt werden. Unter normalen Bedingungen hätte jeder Knoten zwei Schedulerprozesse: einen für die Clusterressourcen und einen für die lokalen Dateisysteme. Nach einer Störung werden zusätzliche Schedulerprozesse auf einem Knoten gestartet, damit die Ressourcen, die von einem anderen Knoten verschoben wurden, geschützt werden.
- Die Kennwortdateien des Clients für Sichern/Archivieren müssen auf Clusterplatten gespeichert werden, damit das generierte Kennwort des Clients für Sichern/Archivieren dem Übernahmeknoten nach einer Störung zur Verfügung steht.
- Die Dateisysteme, die als Teil einer Ressourcengruppe geschützt werden sollen, werden mithilfe der Option domain des Clients für Sichern/Archivieren definiert. Die Option domain wird in der Datei `dsm.sys` angegeben, die ebenfalls auf einer Clusterplatte gespeichert werden sollte, damit der Übernahmeknoten auf sie zugreifen kann.

Führen Sie die folgenden Schritte aus, um den Client für Sichern/Archivieren in einer Clusterumgebung zu konfigurieren.

Vorgehensweise

1. Registrieren Sie die Knotendefinitionen des Clients für Sichern/Archivieren beim IBM Spectrum Protect-Server. Alle Knoten im Cluster müssen auf dem IBM Spectrum Protect-Server definiert sein. Wenn Sie mehrere Clusterressourcen in einer Clusterumgebung definieren, für die die Übernahme unabhängig voneinander erfolgt, muss für jede Ressourcengruppe ein eindeutiger Knotenname definiert werden. Für das oben stehende Beispiel einer Drei-Wege-Clusterkonfiguration Aktiv/Aktiv müssen Sie wie folgt drei Knoten (einen pro Ressource) definieren: (1) `Protect: IBM>register node nodeA nodeApw domain=standard`, (2) `Protect: IBM>register node nodeB nodeBpw domain=standard`, (3) `Protect: IBM>register node nodeC nodeCpw domain=standard`.
2. Konfigurieren Sie die Systemoptionsdatei des Clients für Sichern/Archivieren. Jeder Knoten im Cluster muss für jede Clusterressourcengruppe separate Serverzeilengruppen haben, damit er in jeder entsprechenden Datei `dsm.sys` gesichert werden kann. Sie müssen sicherstellen, dass die Serverzeilengruppen in den Systemoptionsdateien auf jedem Knoten identisch sind. Als Alternative können Sie die Datei `dsm.sys` auf eine gemeinsam genutzte Clusterlokation stellen. Die Serverzeilengruppe, die für die Sicherung von Datenträgern mit Clustern definiert werden, müssen folgende speziellen Merkmale aufweisen:
   - Die Option nodename muss sich auf den Namen des Clientknotens beziehen, der auf dem IBM Spectrum Protect-Server registriert ist. Ist der Clientknotenname nicht definiert, nimmt der Knotenname standardmäßig den Wert des Hostnamens des Knoten an, was möglicherweise zu einem Konflikt mit anderen Knotennamen führt, die für dasselbe Clientsystem verwendet werden.
     Wichtig: Verwenden Sie die Option nodename, um den Clientknoten explizit zu definieren.
   - Für die Option tcpclientaddress muss die Service-IP-Adresse des Clusterknotens angegeben werden.
   - Für die Option passworddir muss ein Verzeichnis auf den gemeinsam genutzten Datenträgern angegeben werden, die Bestandteil der Clusterressourcengruppe sind.
   - Die Optionen errorlogname und schedlogname müssen sich auf Dateien auf den gemeinsam genutzten Datenträgern beziehen, die Bestandteil der Clusterressourcengruppe sind, um eine einzelne, kontinuierliche Protokolldatei aufrecht zu erhalten.
   - Alle Include/Exclude-Anweisungen müssen sich auf Dateien auf den gemeinsam genutzten Datenträgern beziehen, die Bestandteil der Clusterressourcengruppe sind.
   - Wenn Sie die Option inclexcl verwenden, muss sich diese auf einen Dateipfad auf den gemeinsam genutzten Datenträgern beziehen, die Bestandteil der Clusterressourcengruppe sind.
   - Die Zeilengruppennamen, die mit der Option servername identifiziert werden, müssen auf allen Systemen identisch sein.
3. Andere Optionen des Clients für Sichern/Archivieren können nach Bedarf definiert werden. Im folgenden Beispiel müssen alle drei Knoten, `NodeA`, `NodeB` und `NodeC`, die folgenden drei Serverzeilengruppen in ihrer Datei `dsm.sys` aufweisen:

```
Servername        server1_nodeA
nodename          NodeA
commmethod        tcpip
tcpport           1500
tcpserveraddress  server1.example.com
tcpclientaddres   nodeA.example.com
passwordaccess    generate
passworddir       /A1/tsm/pwd
managedservices   schedule
schedlogname      /A1/tsm/dsmsched.log
errorlogname      /A1/tsm/errorlog.log

Servername        server1_nodeB
nodename          NodeB
commmethod        tcpip
```

```
tcpport           1500
tcpserveraddress  server1.example.com
tcpclientaddres   nodeB.example.com
passwordaccess    generate
passworddir       /B1/tsm/pwd
managedservices   schedule
schedlogname      /B1/tsm/dsmsched.log
errorlogname      /B1/tsm/errorlog.log

Servername        server1_nodeC
nodename          NodeC
commmethod        tcpip
tcpport           1500
tcpserveraddress  server1.example.com
tcpclientaddres   nodeC.example.com
passwordaccess    generate
passworddir       /C1/tsm/pwd
managedservices   schedule
schedlogname      /C1/tsm/dsmsched.log
errorlogname      /C1/tsm/errorlog.log
```

4. Konfigurieren Sie die Benutzeroptionsdatei des Clients für Sichern/Archivieren. Die Optionsdatei (`dsm.opt`) muss auf den gemeinsam genutzten Datenträgern in der Clusterressourcengruppe stehen. Definieren Sie die Umgebungsvariable `DSM_CONFIG` so, dass sie sich auf diese Datei bezieht. Stellen Sie sicher, dass die Datei `dsm.opt` folgende Einstellungen enthält:
   - Der Wert für die Option servername muss der Serverzeilengruppe in der Datei `dsm.sys` entsprechen, die Parameter für die Sicherung von Clusterdatenträgern enthält.
   - Definieren Sie die Clusterdateisysteme so, dass sie mit der Option domain gesichert werden.
     Anmerkung: Stellen Sie sicher, dass Sie die Option 'domain' in der Datei `dsm.opt` definieren oder geben Sie die Option im Zeitplan oder in der Befehlszeile des Clients für Sichern/Archivieren an. Dadurch werden Clusteroperationen auf Clusterressourcen und Nicht-Clusteroperationen auf Nicht-Clusterressourcen beschränkt.

   Im Beispiel definieren die Knoten `NodeA`, `NodeB` und `NodeC` ihre entsprechende Datei `dsm.opt` und die Umgebungsvariable `DSM_CONFIG` wie folgt:

   NodeA:

   ```
   1) Die Datei /A1/tsm/dsm.opt definieren:

   servername server1_nodeA
   domain     /A1 /A2

   2) Folgenden Befehl ausgeben oder in Ihr Benutzerprofil einschließen:

   export DSM_CONFIG=/A1/tsm/dsm.opt
   ```

   NodeB:

   ```
   1) Die Datei /B1/tsm/dsm.opt definieren:

   servername server1_nodeB
   domain     /B1 /B2

   2) Folgenden Befehl ausgeben oder in Ihr Benutzerprofil einschließen:

   export DSM_CONFIG=/B1/tsm/dsm.opt
   ```

   NodeC:

   ```
   1) Die Datei /C1/tsm/dsm.opt definieren:

   servername server1_nodeC
   domain     /C1 /C2

   2) Folgenden Befehl ausgeben oder in Ihr Benutzerprofil einschließen:

   export DSM_CONFIG=/C1/tsm/dsm.opt
   ```

5. Definieren Sie die Zeitplandefinitionen für jede Clusterressourcengruppe. Nachdem die Basiseinrichtung abgeschlossen ist, definieren Sie die automatischen Zeitpläne für das Sichern von Clusterressourcen, um die Sicherungsanforderungen zu erfüllen. Die Prozedur illustriert die Zeitplaneinrichtung durch Verwendung des integrierten IBM Spectrum Protect-Scheduler. Wenn Sie einen von einem Lieferanten erworbenen Scheduler verwenden, schlagen Sie in der vom Schedulerlieferanten zur Verfügung gestellten Dokumentation nach.
   - Definieren Sie einen Zeitplan in der Maßnahmendomäne, in der Clusterknoten definiert sind. Stellen Sie sicher, dass das Startfenster des Zeitplans groß genug ist, um im Fall einer Störung und eines Zurücksetzungsereignisses den Zeitplan auf dem Übernahmeknoten erneut starten zu können. Dies bedeutet, dass die Dauer des Zeitplans so definiert werden muss, dass sie länger ist als die Zeit, die benötigt wird, um die Sicherung der Clusterdaten für diesen Knoten unter normalen Bedingungen zu beenden.

     Wenn der erneute Verbindungsaufbau innerhalb des Startfensters für das betreffende Ereignis gelingt, wird der geplante Befehl erneut gestartet. Die geplante Teilsicherung prüft dann erneut die Dateien, die vor der Übernahme an den Server gesendet wurden.

Die Sicherung wird an der Stelle fortgesetzt, an der sie vor der Übernahme gestoppt wurde.

Im folgenden Beispiel wird der Zeitplan `clus_backup` in der Standarddomäne so definiert, dass die Sicherung um 00:30 Uhr täglich gestartet wird, wobei die Dauer auf zwei Stunden festgesetzt ist (dies ist die normale Sicherungszeit für die Daten eines einzelnen Knotens).

```
Protect: IBM>define schedule standard clus_backup action=incr
starttime=00:30 startdate=TODAY  Duration=2
```

- Ordnen Sie den Zeitplan wie folgt allen Knoten des Clients für Sichern/Archivieren zu, die für das Sichern von Clusterressourcen definiert sind: `(1) Protect: IBM>define association standard clus_backup nodeA`, (2) `Protect: IBM>define association standard clus_backup nodeB`, (3) `Protect: IBM>define association standard clus_backup nodeC`.

6. Definieren Sie den Scheduler-Service für Sichern. Auf jedem Clientknoten muss für jede Ressource, für deren Sicherung der Knoten unter normalen Bedingungen verantwortlich ist, ein Scheduler-Service konfiguriert werden. Die Umgebungsvariable `DSM_CONFIG` für jeden Ressourcenscheduler-Service muss so definiert werden, dass sie auf die entsprechende Datei `dsm.opt` für diese Ressource verweist. Für die Beispielkonfiguration müssen folgende Shell-Scripts erstellt werden, damit die `dsmcad`-Prozesse nach Bedarf von jedem beliebigen Knoten im Cluster gestartet werden können.

```
NodeA: /A1/tsm/startsched
#!/bin/ksh
export DSM_CONFIG=/A1/tsm/dsm.opt
dsmcad
NodeB: /B1/tsm/startsched
#!/bin/ksh
export DSM_CONFIG=/B1/tsm/dsm.opt
dsmcad
NodeC: /C1/tsm/startsched
#!/bin/ksh
export DSM_CONFIG=/C1/tsm/dsm.opt
dsmcad
```

7. Definieren Sie den Client für Sichern/Archivieren für die Clusteranwendung. Damit die Sicherung der fehlgeschlagenen Ressource nach einer Übernahmebedingung fortgesetzt werden kann, muss der IBM Spectrum Protect-Scheduler-Service (für jeden Cluster-Clientknoten) als Ressource für die Clusteranwendung definiert werden, um an der Übernahmeverarbeitung teilzuhaben. Dies ist erforderlich, damit die Sicherung der fehlgeschlagenen Ressourcen von dem Knoten, der die Ressource übernimmt, fortgesetzt werden kann. Eine gegenteilige Aktion würde zu einer unvollständigen Sicherung der fehlgeschlagenen Ressource führen. Die Beispielscripts in Schritt 5 können den Clusterressourcen zugeordnet werden, um sicherzustellen, dass sie auf Knoten im Cluster gestartet werden, während die Plattenressourcen, die geschützt werden, von einem Knoten zum anderen verschoben werden. Die tatsächlichen Schritte, die erforderlich sind, um den Scheduler-Service als Clusterressource zu installieren, hängen von der spezifischen Cluster-Software ab. Die Dokumentation zu Ihrer Clusteranwendung enthält weitere Informationen.
8. Stellen Sie sicher, dass das Kennwort für jeden Knoten korrekt generiert und an der mit der Option passworddir angegebenen Position in den Cache gestellt wurde. Dies können Sie prüfen, indem Sie folgende Schritte ausführen:
   a. Prüfen Sie, ob jeder Knoten ohne Aufforderung zur Kennworteingabe eine Verbindung zum IBM Spectrum Protect-Server herstellen kann. Hierfür führen Sie die Befehlszeilenschnittstelle des Clients für Sichern/Archivieren aus und geben auf jedem Knoten den folgenden Befehl ein:

      ```
      #dsmc query session
      ```

      Wenn Sie zur Eingabe Ihres Kennworts aufgefordert werden, geben Sie das Kennwort ein, um den Befehl erfolgreich auszuführen, und wiederholen den Befehl. Das zweite Mal sollte der Befehl ohne Eingabeaufforderung für das Kennwort ausgeführt werden. Wenn Sie zur Kennworteingabe aufgefordert werden, überprüfen Sie Ihre Konfiguration.

   b. Prüfen Sie, ob die anderen Knoten im Cluster Sitzungen mit dem IBM Spectrum Protect-Server wegen des in einer Übernahmeverarbeitung befindlichen Knotens starten können. Dies kann durchgeführt werden, indem dieselben Befehle, wie im Schritt oben beschrieben, auf den Sicherungsknoten ausgeführt werden. Beispiel: Um zu prüfen, ob `NodeB` und `NodeC` bei einem Übernahmeereignis eine Sitzung als `NodeA` starten können, ohne dass zur Eingabe des Kennworts aufgefordert wird, führen Sie folgende Befehle auf `NodeB` und `NodeC` aus.

      ```
      #export DSM_CONFIG=/A1/tsm/dsm.opt
      #dsmc query session
      ```

      Die Eingabeaufforderung für das Kennwort wird jetzt möglicherweise angezeigt, aber dies ist unwahrscheinlich. Wenn Sie zur Eingabe aufgefordert werden, war das Kennwort in der gemeinsam genutzten Lokation nicht richtig gespeichert. Überprüfen Sie die Einstellung der Option passworddir, die für `NodeA` verwendet wird, und folgen Sie den Konfigurationsschritten erneut.

   c. Stellen Sie sicher, dass die Zeitpläne von jedem Knoten korrekt ausgeführt werden. Sie können einen Zeitplan auslösen, indem Sie die Startzeit des Zeitplans auf `Jetzt` setzen. Denken Sie daran, die Startzeit nach Abschluss des Tests wieder zurückzusetzen.

      ```
      Protect: IBM>update sched standard clus_backup starttime=now
      ```

   d. Die Übernahme und Rückübertragung zwischen `nodeA` und `nodeB` ist immer noch gültig, während `nodeA` die Sicherung ausführt und sich im Startfenster des Zeitplans befindet. Überprüfen Sie, ob die Teilsicherung nach Übernahme und Rückübertragung weiterhin ausgeführt und erfolgreich beendet wird.
   e. Geben Sie den folgenden Befehl aus, damit das Kennwort eines Knotens (`nodeA`) abläuft. Stellen Sie sicher, dass die Sicherung unter normalen Clusteroperationen ebenso wie die Übernahme und Rückübertragung normal weiterläuft:

```
Protect: IBM>update node nodeA forcep=yes
```

9. Konfigurieren Sie den Client für Sichern/Archivieren, sodass lokale Ressourcen gesichert werden.
   a. Definieren Sie Clientknoten auf dem IBM Spectrum Protect-Server. Lokale Ressourcen sollten nie mit Knotennamen gesichert oder archiviert werden, die für das Sichern von Clusterdaten definiert sind. Werden lokale Datenträger gesichert, die nicht als Clusterressourcen definiert sind, müssen für die Datenträger im Cluster und die Datenträger, die nicht zum Cluster gehören, separate Knotennamen (und separate Clientinstanzen) verwendet werden.

      Im folgenden Beispiel setzen wir voraus, dass nur `NodeA` über die zu sichernden lokalen Dateisysteme `/fs1` und `/fs2` verfügt. Zum Verwalten der lokalen Ressourcen registrieren Sie den Knoten `NodeA_local` auf dem IBM Spectrum Protect-Server: `Protect: IBM>register node nodeA_local nodeA_localpw domain=standard`.

   b. Fügen Sie in der Systemoptionsdatei `dsm.sys` auf jedem Knoten eine separate Zeilengruppe hinzu, die lokale Ressourcen mit den folgenden besonderen Merkmalen sichern muss:
      - Der Wert der Option tcpclientaddress muss der Name oder die IP-Adresse des lokalen Hosts sein. Dabei handelt es sich um die IP-Adresse, die für den primären Datenverkehr zu und von einem Knoten verwendet wird.
      - Wenn der Client nicht zu einem Cluster gehörende Datenträger sichert und zurückschreibt, ohne mit dem Cluster verbunden zu sein, muss der Wert der Option tcpclientaddress die Boot-IP-Adresse sein. Diese IP-Adresse wird zum Starten des Systems (Knoten) verwendet, bevor die Verbindung zum Cluster hergestellt wird:

        ```
        Beispielzeilengruppe für NodeA_local:

        Servername        server1_nodeA_local
        nodename          nodeA_local
        commmethod        tcpip
        tcpport           1500
        tcpserveraddress  server1.example.com
        tcpclientaddres   nodeA_host.example.com
        passwordaccess    generate
        managedservices   schedule
        ```

   c. Definieren Sie die Benutzeroptionsdatei `dsm.opt` in einem Pfad, der sich auf einer Ressource ohne Cluster befindet.
      - Der Wert für die Option servername muss der Serverzeilengruppe in der Datei dsm.sys entsprechen, die Parameter für die Sicherung von Datenträgern ohne Cluster definiert.
      - Verwenden Sie die Option domain, um die zu sichernden Dateisysteme ohne Cluster zu definieren.

      Anmerkung: Stellen Sie sicher, dass Sie die Option 'domain' in der Datei `dsm.opt` definieren oder geben Sie die Option im Zeitplan oder in der Befehlszeile des Clients für Sichern/Archivieren an, um die Sicherungs-/Archivierungsoperationen auf Datenträger ohne Clustering zu beschränken.

      Im folgenden Beispiel verwendet `nodeA` die folgende Datei `/home/admin/dsm.opt` und richtet die Umgebung `DSM_CONFIG` so ein, dass sie auf `/home/admin/A1.dsm.opt` verweist.

      Inhalt von `/home/admin/A1.dsm.opt`

      ```
      servername ibm_nodeA_local
      domain     /fs1 /fs2


      export DSM_CONFIG=/home/admin/A1.dsm.opt
      ```

   d. Definieren Sie einen Zeitplan und richten Sie ihn so ein, dass er die Teilsicherung für Dateisysteme außerhalb des Clusters ausführt.

      ```
      Protect: IBM>define schedule standard local_backup action=incr
      starttime=00:30 startdate=TODAY  Duration=2
      ```

      Ordnen Sie den Zeitplan allen Knoten des Clients für Sichern/Archivieren zu, die für das Sichern von Ressourcen außerhalb des Clusters definiert sind.

      ```
      Protect: IBM>define association standard nodeA_local
      ```

10. Schreiben Sie die Gruppendateisystemdaten zurück. Alle Datenträger in einer Clusterressource werden unter dem Zielknoten gesichert, der für diese Clusterressource definiert ist. Wenn Sie die Daten, die auf einem Clusterdatenträger resident sind, zurückschreiben müssen, können Sie sie von dem Clientknoten zurückschreiben, der zum Zeitpunkt der Zurückschreibung Eigner der Clusterressource ist. Der Client für Sichern/Archivieren muss dieselbe Benutzeroptionsdatei (`dsm.opt`) verwenden, die während der Sicherung verwendet wurde, um die Daten zurückzuschreiben. Es sind keine zusätzlichen Installationsvoraussetzungen erforderlich, um Daten auf Clusterdatenträgern zurückzuschreiben.
11. Schreiben Sie die Daten des lokalen Dateisystems zurück. Die Datenträger ohne Cluster werden unter der separaten Knotennamenkonfiguration für Operationen ohne Cluster gesichert. Zum Zurückschreiben dieser Daten muss der Client für Sichern/Archivieren dieselbe Benutzeroptionsdatei (`dsm.opt`) verwenden, die während der Sicherung verwendet wurde. Definieren Sie in dem Beispiel die Umgebungsvariable `DSM_CONFIG` so, dass sie auf `/home/admin/A1.dsm.opt` verweist, bevor Sie eine Clientzurückschreibung für den lokalen Knoten `nodeA_local` ausführen.

Zugehörige Konzepte:
Daten zurückschreiben
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

Web-Client-Zugriff in einer Clusterumgebung aktivieren

Wenn während einer Übernahmebedingung IBM Spectrum Protect-Web-Client-Zugriff erforderlich ist, müssen Sie den Web-Clientakzeptordämon, der dem Cluster zugeordnet ist, so konfigurieren, dass für ihn zusammen mit der Clusterressource eine Übernahme erfolgt.

Vorbereitende Schritte

Ab IBM Spectrum Protect Version 8.1.2 können Sie nicht mehr den Web-Client verwenden, um eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder höher herzustellen. Sie können den Web-Client jedoch weiterhin verwenden, um eine Verbindung zu Servern mit IBM Spectrum Protect Version 8.1.1, Version 8.1.0, Version 7.1.7 und früheren Versionen herzustellen. Weitere Informationen finden Sie in Web-Client in neuer Sicherheitsumgebung verwenden.

Informationen zu diesem Vorgang

Nachdem Sie die im Abschnitt *Client für Sichern/Archivieren in einer Clusterumgebung konfigurieren* beschriebenen Konfigurationsschritte ausgeführt haben, müssen Sie die nachfolgend beschriebenen zusätzlichen Schritte ausführen, um die Konfiguration des Web-Client-Zugriffs abzuschließen:

Vorgehensweise

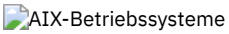
1. Konfigurieren Sie den Clientakzeptordämon so, dass er den Web-Client und den Scheduler verwaltet. In der Konfiguration des Clientakzeptordämons sollte festgelegt werden, dass er sowohl Scheduler als auch den Web-Client-Zugriff verwaltet. Auf diese Weise wird die Anzahl Dämonen verkleinert, die als Clusteranwendungen konfiguriert werden müssen, und die Konfiguration und Verwaltung dadurch vereinfacht. Wenn eine Übernahme erfolgt, startet der Clientakzeptor auf dem Knoten, der die Übernahme handhabt.
2. Aktualisieren Sie die Option managedservices in der Systemoptionsdatei `dsm.sys` auf jedem Knoten für jede Serverzeilengruppe, wie unten für `NodeA` gezeigt:

```
Servername          server1_NodeA
nodename            NodeA
commmethod          tcpip
tcpp                1500
tcps                server1.example.com
tcpclientaddres     nodeA.example.com
passwordaccess      generate
passworddir         /A1/tsm/pwd
schedlogn           /A1/tsm/dsmsched.log
errorlogname        /A1/tsm/errorlog.log
managedservices     webclient schedule
```

3. Konfigurieren Sie den Clientakzeptordämon für die Verwendung eines bekannten HTTP-Anschlusses. Standardmäßig verwendet der Clientakzeptordämon für den Web-Client-Zugriff HTTP-Anschluss 1581, sofern verfügbar. Wenn dieser Anschluss nicht verfügbar ist, sucht der Clientakzeptor den ersten verfügbaren Anschluss ab 1581. Bei einer Übernahmebedingung einer Clusterkonfiguration Aktiv/Aktiv führt das Hostsystem eines Übernahmeclusters wahrscheinlich mehrere Instanzen des Clientakzeptors aus. Wenn die Standardeinstellungen für den HTTP-Anschluss verwendet werden, verwendet der Übernahmeknoten einen beliebigen verfügbaren Anschluss für den Clientakzeptor, für den eine Übernahme erfolgt, da der Standardanschluss wahrscheinlich durch die aktuellen Clientakzeptorprozesse des Übernahmehosts belegt ist. Dies führt zu Problemen für den Web-Client, der dem Clientakzeptor, für den die Übernahme erfolgt ist, zugeordnet ist, da der neue HTTP-Anschluss den Web-Client-Benutzern nicht bekannt ist. Sie können gegebenenfalls die Option httpport verwenden, um für jede Ressource die Anschlüsse für den Web-Client-Zugriff anzugeben. Dadurch ist es möglich, dass Sie stets denselben Anschluss verwenden, wenn Sie eine Verbindung von einem Web-Browser aus herstellen, unabhängig vom Knoten, der die Clusterressource bedient. Fügen Sie wie folgt auf jedem Knoten für jede Serverzeilengruppe die Option httpport in der Systemoptionsdatei (`dsm.sys`) hinzu und stellen Sie dabei sicher, dass in jeder Zeilengruppe ein eindeutiger Wert verwendet wird:

```
Servername          server1_NodeA
nodename            NodeA
commmethod          tcpip
tcpp                1500
tcps                server1.example.com
tcpclientaddres     nodeA.example.com
passwordaccess      generate
passworddir         /A1/tsm/pwd
managedservices     webclient schedule
schedlogn           /A1/tsm/dsmsched.log
errorlogname        /A1/tsm/errorlog.log
httpport            1510


Servername          server1_NodeB
nodename            NodeB
commmethod          tcpip
tcpp                1500
tcps                server1.example.com
tcpclientaddres     nodeB.example.com
passwordaccess      generate
passworddir         /B1/tsm/pwd
```

```
managedservices   webclient schedule
schedlogn         /B1/tsm/dsmsched.log
errorlogname      /B1/tsm/errorlog.log
httpport          1511


Servername        server1_NodeC
nodename          NodeC
commmethod        tcpip
tcpp              1500
tcps              server1.example.com
tcpclientaddres   nodeC.example.com
passwordaccess    generate
passworddir       /C1/tsm/pwd
managedservices   webclient schedule
schedlogn         /C1/tsm/dsmsched.log
errorlogname      /C1/tsm/errorlog.log
httpport          1512
```



Traditionelle AIXIBM PowerHA SystemMirror-Konfigurationen migrieren

Wenn Sie den Client für Sichern/Archivieren gegenwärtig in einer IBM® PowerHA SystemMirror-Umgebung mit der Option clusternode verwenden, müssen Sie Ihre aktuellen Konfigurationen aktualisieren. Die Option clusternode wird nicht mehr unterstützt.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um Ihre aktuellen Konfigurationen zu aktualisieren:

Vorgehensweise

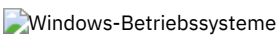
1. Aktualisieren Sie die Systemoptionsdatei des Clients für Sichern/Archivieren. Wie bei der Option clusternode muss jeder Knoten im Cluster auch weiterhin für jede Clusterressourcengruppe separate Serverzeilengruppen haben, damit er in jeder entsprechenden Datei `dsm.sys` gesichert werden kann. Die bestehende Datei `dsm.sys` für `NodeA` wird möglicherweise wie folgt angezeigt:

   ```
   Servername        server1_nodeA
   commmethod        tcpip
   tcpp              1500
   tcps              server1.example.com
   tcpclientaddres   nodeA.example.com
   passwordaccess    generate
   passworddir       /A1
   clusternode       yes
   managedservices   schedule
   schedlogn         /A1/dsmsched.log
   errorlogname      /A1/errorlog.log
   ```

2. Beachten Sie, dass in diesem Beispiel keine Option nodename verwendet wird. Nehmen Sie die folgenden Änderungen an der bestehenden Datei `dsm.sys` für `NodeA` vor.
   - Entfernen Sie die Option clusternode.
   - Geben Sie, falls nicht bereits geschehen, eine Option nodename an.
3. Die neue Datei `dsm.sys` für `NodeA` sollte wie folgt erscheinen:

   ```
   Servername        server1_nodeA
   commmethod        tcpip
   nodename          myclus (myclus ist der vorhandene Clustername)
   tcpp              1500
   tcps              server1.example.com
   tcpclientaddres   nodeA.example.com
   passwordaccess    generate
   passworddir       /A1
   managedservices   schedule
   schedlogn         /A1/dsmsched.log
   errorlogname      /A1/errorlog.log
   ```

4. Registrieren Sie die Knoten des Clients für Sichern/Archivieren beim IBM Spectrum Protect-Server. Wenn die neuen Knoten des Clients für Sichern/Archivieren im ersten Schritt hinzugefügt werden, um den aktuellen Standardwert des Clusterknotennamens zu ersetzen, registrieren Sie diese Knoten auf dem IBM Spectrum Protect-Server.
5. Aktualisieren Sie die Zeitplandefinitionen. Wenn im vorherigen Schritt neue Knoten des Clients für Sichern/Archivieren hinzugefügt wurden, stellen Sie sicher, dass die Sicherungszeitplandefinitionen, die vorher zum Sichern der Daten dieses Knotens verwendet wurden, jetzt den neuen Clientknotennamen zugeordnet werden.
6. Prüfen Sie die Konfiguration. Weitere Informationen finden Sie in Client für Sichern/Archivieren in einer Clusterumgebung konfigurieren.



Client für Sichern/Archivieren in einer Cluster-Server-Umgebung konfigurieren

Sie können die Software des Clients für Sichern/Archivieren lokal auf jedem Knoten eines Clusters in einer MSCS-Umgebung (Microsoft Cluster Server) oder VCS-Umgebung (Veritas Cluster Server) installieren.

Sie können den Client für Sichern/Archivieren in einer VCS-Umgebung auf den unterstützten Plattformen von Windows Server verwenden.

Außerdem können Sie den Scheduler-Service für jeden Clusterknoten installieren und konfigurieren, um alle lokalen Platten und jede Clustergruppe, die physische Plattenressourcen enthält, verwalten zu können.

Beispiel: Der MSCS-Cluster mscs-cluster enthält zwei Knoten, node-1 und node-2, sowie zwei Clustergruppen, group-a und group-b, die physische Plattenressourcen enthalten. In diesem Fall sollte eine Instanz des IBM Spectrum Protect-Scheduler-Service für Sichern/Archivieren für node-1, node-2, group-a und group-b installiert werden. So wird sichergestellt, dass die geeigneten Ressourcen für den Client für Sichern/Archivieren verfügbar sind, wenn Platten zwischen den Clusterknoten verschoben werden (oder fehlschlagen).

Mit der Option clusternode wird sichergestellt, dass der Client Sicherungsdaten, unabhängig davon, welcher Clusterknoten eine Clusterplattenressource sichert, logisch verwaltet. Verwenden Sie diese Option für Clientknoten, die Clusterplattenressourcen und keine lokalen Ressourcen verarbeiten.

Anmerkung: Sie müssen die Option clusternode: für alle von IBM Spectrum Protect verwalteten Clusteroperationen auf `yes` setzen. Wird die Option clusternode für einen bestimmten IBM Spectrum Protect-Clusterknotennamen nicht konsistent verwendet, wird das verschlüsselte Kennwort für den Clusterknotennamen möglicherweise ungültig und der Client fordert den Benutzer beim nächsten Aufruf des Programms 'Client für Sichern/Archivieren' zur erneuten Eingabe des Kennworts auf.

Verwenden Sie die Option optfile, um die korrekte (Cluster-)Datei dsm.opt für alle Clientprogramme aufzurufen, um für clusterbezogene Operationen die korrekte Funktionalität zu gewährleisten.

Auf welche Weise der Client für Sichern/Archivieren in einer Clusterumgebung installiert und konfiguriert wird, ist von der verwendeten Cluster-Server-Technologie (MSCS oder VCS) und von dem Betriebssystem abhängig, das von den Knoten im Cluster verwendet wird.

- Windows-BetriebssystemeDaten in MSCS-Clustern schützen (Windows Server-Clients)
  Auf Knoten in einer MSCS-Clusterumgebung wird ein Clientkonfigurationsassistent verwendet, um die Konfiguration des Clients für Sichern/Archivieren für den Schutz von Clusterplattengruppen zu automatisieren und zu vereinfachen. Der Assistent kann nur auf Knoten verwendet werden, auf denen unterstützte Windows Server-Clients als Betriebssystem ausgeführt werden.
- Windows-BetriebssystemeWeb-Client in einer Clusterumgebung konfigurieren
  Soll der Web-Client in einer Clusterumgebung verwendet werden, müssen Sie die GUI des Clients für Sichern/Archivieren für die Ausführung in einer Clusterumgebung konfigurieren.
- Windows-BetriebssystemeHäufig gestellte Fragen
  Dieser Abschnitt enthält einige häufig gestellte Fragen und die zugehörigen Antworten zur Verwendung von Cluster-Services.

Zugehörige Verweise:
Optfile
Windows-Betriebssysteme

Daten in MSCS-Clustern schützen (Windows Server-Clients)

Auf Knoten in einer MSCS-Clusterumgebung wird ein Clientkonfigurationsassistent verwendet, um die Konfiguration des Clients für Sichern/Archivieren für den Schutz von Clusterplattengruppen zu automatisieren und zu vereinfachen. Der Assistent kann nur auf Knoten verwendet werden, auf denen unterstützte Windows Server-Clients als Betriebssystem ausgeführt werden.

- Windows-BetriebssystemeClusterschutz konfigurieren (Windows Server-Clients)
  Mit demIBM Spectrum Protect-Clusterassistenten können Sie den Client für Sichern/Archivieren für den Schutz von Clusterressourcen konfigurieren. Der Assistent stellt die Informationen zusammen, die benötigt werden, damit der Client für Sichern/Archivieren Clusterressourcen schützen und sich beim Server anmelden kann.

Windows-Betriebssysteme

Web-Client in einer Clusterumgebung konfigurieren

Soll der Web-Client in einer Clusterumgebung verwendet werden, müssen Sie die GUI des Clients für Sichern/Archivieren für die Ausführung in einer Clusterumgebung konfigurieren.

Ab IBM Spectrum Protect Version 8.1.2 können Sie nicht mehr den Web-Client verwenden, um eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder höher herzustellen. Sie können den Web-Client jedoch weiterhin verwenden, um eine Verbindung zu Servern mit IBM Spectrum Protect Version 8.1.1, Version 8.1.0, Version 7.1.7 und früheren Versionen herzustellen. Weitere Informationen finden Sie in Web-Client in neuer Sicherheitsumgebung verwenden.

Siehe Windows-BetriebssystemeClusterschutz konfigurieren (Windows Server-Clients) für ausführliche Informationen zur Installation und Konfiguration des Clients für Sichern/Archivieren in einer MSCS- oder VCS-Umgebung.

- Windows-BetriebssystemeWeb-Client für die Verarbeitung von Clusterplattenressourcen konfigurieren
  Nach der Installation und Konfiguration des Clients für Sichern/Archivieren in einer MSCS- oder VCS-Umgebung müssen Sie einige Schritte ausführen, um Clusterplattenressourcen zu verarbeiten.

Windows-Betriebssysteme

Häufig gestellte Fragen

Dieser Abschnitt enthält einige häufig gestellte Fragen und die zugehörigen Antworten zur Verwendung von Cluster-Services.

Informationen zu diesem Vorgang

F: Wie wird eine Verknüpfung für die GUI des Clients für Sichern/Archivieren in einer Clusterumgebung konfiguriert?
A: Um ein Symbol für die GUI des Clients für Sichern/Archivieren (beispielsweise auf dem Windows-Desktop) zu konfigurieren, das Sie für die Verwaltung von Operationen für eine Clusterressourcengruppe in einem Windows-Cluster verwenden können, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Klicken Sie mit der rechten Maustaste auf den Desktop und wählen Sie die Optionen Neu > Verknüpfung aus.
2. Suchen Sie in dem Fenster, das angezeigt wird, den Pfad zu der ausführbaren Datei dsm.exe (sie befindet sich standardmäßig im Verzeichnis `C:\Programme\tivoli\tsm\baclient\`). Wenn Sie den Pfad eingeben, anstatt die Schaltfläche Durchsuchen zu verwenden, müssen Sie den Pfad in Anführungszeichen einschließen. Beispiel: "C:\Programme\tivoli\tsm\baclient\dsm.exe"
3. Nachdem Sie den Pfad und den Namen der ausführbaren Datei in das Textfeld eingegeben haben, fügen Sie nach dem abschließenden Anführungszeichen folgende Informationen hinzu (fügen Sie auch ein Leerzeichen zwischen dem Anführungszeichen und dem Folgenden hinzu): `-optfile="x:\path\to\cluster\dsm.opt"`. Dadurch wird die richtige IBM Spectrum Protect-Clusteroptionsdatei, die Sie verwenden wollen, identifiziert. In diesem Beispiel wird angenommen, dass die Clusteroptionsdatei sich im Ordner "x:\path\to\cluster\" befindet und den Dateinamen dsm.opt hat.
4. Die vollständige Zeile im Textfeld sollte jetzt ähnlich wie die folgende Zeile aussehen:
   `"C:\Programme\tivoli\tsm\baclient\dsm.exe" -optfile="x:\path\to\cluster\ dsm.opt"`.
5. Klicken Sie auf Weiter und geben Sie dieser Verknüpfung einen aussagekräftigen Namen, wie z. B. Sichern/Archivieren - GUI: Clustergruppe X.
6. Klicken Sie auf Fertig stellen. Jetzt sollte ein Desktopsymbol verfügbar sein. In den Merkmalen dieses Symbols wird das folgende korrekte Ziel angezeigt, wie in Schritt 4 angegeben: `"C:\Programme\tivoli\tsm\baclient\dsm.exe" -optfile="x:\path\to\cluster\ dsm.opt"`.

Ergebnisse

F: Wie wird überprüft, ob eine Scheduler-Service-Installation in einer Clusterumgebung funktioniert?
A: Das Definieren eines Scheduler-Service für eine Microsoft-Clusterressourcengruppe kann zeitaufwendig sein und durch Syntaxfehler in den Befehlen, mit denen er erstellt wird, in die Länge gezogen werden. Durch sorgfältiges Eingeben der Befehle und das Aufzeichnen wichtiger Informationen über die Clusterinstallation kann die Konfigurationszeit verringert werden. Führen Sie folgende Schritte aus, um erfolgreich einen Scheduler-Service für Microsoft-Clusterumgebungen zu installieren:

1. Lesen Sie die Informationen in diesem Anhang sorgfältig durch, um die korrekte Syntax beim Definieren eines Scheduler-Service für eine Clustergruppe zu erhalten.
2. Stellen Sie sicher, dass die richtige(n) Datei(en) dsm.opt für den Cluster verwendet werden. Auf einer typischen normalen Workstation wird nur eine Datei dsm.opt verwendet. In einer Clusterumgebung sind zusätzliche Dateien dsm.opt erforderlich. Jede Clustergruppe, die gesichert wird, muss ihre eigene Datei dsm.opt haben. Eine Clustergruppe ist jede Gruppe, die unter dem Ordner GRUPPE der Clusterbaumstruktur innerhalb des Dienstprogramms Microsoft Cluster Administrator oder des VCS-Konfigurationseditors aufgelistet ist.
3. Machen Sie sich bewusst, was die folgenden Optionen in dsmcutil.exe bedeuten, und wann sie zu verwenden sind. (1) /clustername:*Clustername* - Gibt den Namen des Microsoft-Clusters an, wobei *Clustername* für den Namen auf der höchsten Ebene der Baumstruktur innerhalb des Dienstprogramms Microsoft Cluster Administrator oder des VCS-Konfigurationseditors steht. Verwenden Sie diese Option mit dsmcutil.exe nur, wenn Sie einen Scheduler-Service für eine Clustergruppe installieren. Geben Sie keinen Clusternamen mit mehr als 64 Zeichen an. Wenn Sie mehr als 256 Zeichen angeben und Veritas Storage Foundation mit hoher Verfügbarkeit oder eine Microsoft Cluster Server-Konfiguration verwenden, können Sie den Scheduler-Service von IBM Spectrum Protect möglicherweise nicht installieren oder starten. (2) /clusternode:yes - Gibt an, dass Sie Unterstützung für Clusterressourcen aktivieren wollen. Verwenden Sie diese Option in der Datei dsm.opt für jede Clustergruppe und zusammen mit dsmcutil.exe, wenn Sie einen Scheduler-Service für eine Clustergruppe installieren.
4. Häufig anzutreffende Fehler werden beim Eingeben der Syntax des Befehls dsmcutil.exe gemacht. Ein einfacher Weg, um diese Syntaxprobleme zu verhindern, ist das Erstellen einer temporären Textdatei, die für die Clustergruppe zugänglich ist (stellen Sie sie z. B. auf ein Clusterlaufwerk, das zu dieser Clustergruppe gehört), und das Eingeben der Syntax in diese Datei. Falls notwendig, schneiden Sie diese Syntax aus der Datei aus, fügen Sie sie bei der DOS-Eingabeaufforderung ein und drücken Sie die Eingabetaste. Dadurch wird die Konsistenz der Befehlssyntax garantiert, unabhängig davon, auf welchem Computer sie eingegeben wird.
5. Wenn der Neustart des Scheduler-Service fehlschlägt, nachdem eine Übernahme der Clustergruppen auftritt (z. B. mit der Option MOVE GROUP im Cluster Administrator), liegen möglicherweise Kennwortsynchronisationsprobleme zwischen den beiden Cluster-Workstations vor. Sie können überprüfen, ob die Kennwörter übereinstimmen, indem Sie den folgenden Registrierungsschlüssel auf

jeder Workstation anzeigen und den verschlüsselten Kennwortwert vergleichen: HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ADSM\CurrentVersion\Nodes\ *Knotenname**Servername*.

Wenn die verschlüsselten Schlüssel für diesen Knoten auf den beiden Cluster-Workstations nicht übereinstimmen, liegt eine Kennwortdiskrepanz auf einer der beiden oder auf beiden Workstations vor. Zum Korrigieren dieses Fehlers verwenden Sie das Programm dsmc.exe, um das Kennwort auf beiden Workstations manuell zu aktualisieren.

Beispiel: Angenommen, Laufwerk Y: ist Teil der Clustergruppe, die Probleme hat, mit einem Scheduler-Service gesichert zu werden. Das Verzeichnis Y:\tsm enthält die Datei dsm.opt für diese Clustergruppe. Geben Sie den folgenden Befehl auf beiden Workstations ein, um das Kennwort manuell zu aktualisieren: `dsmc -optfile=Y:\tsm\dsm.opt -clusternode=yes`. Geben Sie außerdem den folgenden Befehl ein, damit die Eingabeaufforderung für den Knotennamen und das Kennwort angezeigt wird: dsmc q se -optfile=Y:\tsm\dsm.opt -clusternode=yes.

Überprüfen Sie, ob die Kennwörter synchronisiert sind, und starten Sie den Scheduler-Service erneut, um zu prüfen, ob die Kennwörter konsistent bleiben. Wenn die Kennwortdiskrepanz weiterhin besteht, kann die Ursache ein Syntaxfehler im ursprünglichen Befehl dsmcutil.exe sein, der für die Installation des Scheduler-Service verwendet wurde. In diesem Fall deinstallieren Sie den Scheduler-Service (mit dem Befehl `dsmcutil remove /name:`*`Zeitplanname`*) und installieren den Scheduler-Service erneut (mithilfe der oben beschriebenen Syntax in der gemeinsam genutzten Textdatei).

F: Wie wird ein Clusterlaufwerk einer vorhandenen Cluster-Scheduler-Service-Ressource für die Sicherung hinzugefügt?

A: Um einem vorhandenen Cluster-Scheduler-Service des Clients für Sichern/Archivieren eine weitere Clusterlaufwerkressource hinzuzufügen, müssen die folgenden Komponenten geändert oder aktualisiert werden, um diese Änderung korrekt widerzuspiegeln:

1. Die Clusterlaufwerkressource und alle zugehörigen gemeinsamen Ressourcenzugriffe müssen vorhanden und innerhalb der angegebenen Clustergruppe resident sein, wie im Dienstprogramm Microsoft Cluster Administrator oder im VCS-Konfigurationseditor definiert ist. Die angegebene Clustergruppe muss bereits die Cluster-Scheduler-Serviceressource enthalten, für die dieses neue Laufwerk hinzugefügt wird.
2. Die Datei dsm.opt, die von der angegebenen Cluster-Scheduler-Serviceressource verwendet wird, muss geändert werden, sodass die zusätzliche Clusterlaufwerkressource in der Optionsanweisung domain einbezogen wird. Beispiel: Wenn Sie das Laufwerk `R:\` hinzufügen wollen und in der Anweisung domain zurzeit die Clusterlaufwerke `Q:` und `S:` angegeben sind, aktualisieren Sie wie folgt die Anweisung domain in Ihrer Datei dsm.opt: `domain Q: S: R:`.
3. Sie müssen die Eigenschaften der Cluster-Scheduler-Serviceressource so ändern, dass diese Datei in die Liste der abhängigen Ressourcen einbezogen wird, die benötigt werden, um diese Ressource online zu schalten. Dadurch wird sichergestellt, dass die Clusterlaufwerkressource, die hinzugefügt wird, in die neuen Sicherungen und in die Sicherungen, die nach dem Auftreten einer Übernahme ausgeführt werden, eingeschlossen wird.

Nachdem die oben aufgeführten Änderungen ausgeführt sind, müssen Sie die Cluster-Scheduler-Serviceressource offline und wieder online schalten. Der Zeitplan sollte nun diese zusätzliche Ressource für Sicherungen verarbeiten.

F: Der Clientakzeptorservice wurde entfernt und jetzt schlägt die Ressource "Allgemeiner Dienst" für die Clustergruppe fehl. Wie kann dies korrigiert werden?

A: Der Clientakzeptor kann verwendet werden, um den Scheduler und/oder den Web-Client für eine Clusterumgebung zu steuern. Wenn der Clientakzeptor entfernt wird, ohne dass die generische Clusterressource aktualisiert wird, schlägt die Ressource fehl. Führen Sie folgende Schritte aus, um dies zu korrigieren:

1. Prüfen Sie, welcher Scheduler-Service vom Clientakzeptor gesteuert wurde.
2. Rufen Sie mithilfe des Dienstprogramms Microsoft Cluster Administrator oder des VCS-Konfigurationseditors das Fenster Eigenschaften der Serviceressource auf, wählen Sie die Registerkarte Parameter aus und geben Sie den Namen des korrekten Scheduler-Service ein, der verwendet werden soll.
3. Wiederholen Sie die Schritte 1 und 2 für jede Clustergruppe, die von dem spezifischen Clientakzeptor verwaltet wurde.
4. Zum Testen der aktualisierten Serviceressource leiten Sie einen Fehler der Ressource ein. Wenn die Ressource ohne Fehler wieder online geschaltet wird, hat die Aktualisierung richtig funktioniert.

Anmerkung: Um den Clientakzeptorservice vollständig zu inaktivieren, müssen Sie die Option managedservices in der Datei dsm.opt für die Clustergruppe entfernen oder auf Kommentar setzen.

Windows-Betriebssysteme

Unterstützung für Online-Imagesicherung konfigurieren

Wenn die Online-Imagefunktion konfiguriert ist, führt der Client für Sichern/Archivieren eine momentaufnahmebasierte Imagesicherung aus, während der der reale Datenträger für andere Systemanwendungen verfügbar ist.

Informationen zu diesem Vorgang

Während der Online-Imagesicherung wird ein konsistentes Image des Datenträgers aufrecht erhalten.

Führen Sie folgende Schritte aus, um eine Online-Imagesicherung zu konfigurieren:

Vorgehensweise

1. Wählen Sie Dienstprogramme > Setup-Assistent im Hauptfenster der GUI des Clients für Sichern/Archivieren aus. Die Anzeige für den Clientkonfigurationsassistenten wird aufgerufen.
2. Wählen Sie Hilfe zum Konfigurieren der Online-Imageunterstützung aus und klicken Sie auf Weiter. Die Anzeige 'Assistent für Online-Imageunterstützung' wird aufgerufen.
3. Klicken Sie auf Volume Shadowcopy Services (VSS) und dann auf Weiter. Um die Online-Imageunterstützung zu inaktivieren, klicken Sie auf Keine (Online-Imageunterstützung inaktivieren).
4. Klicken Sie auf die Schaltfläche Fertigstellen, um die Konfiguration zu beenden.
5. Füllen Sie jede Anzeige im Assistenten aus und klicken Sie zur Fortsetzung auf Weiter. Um zu einer vorherigen Anzeige zurückzugehen, klicken Sie auf Zurück. Um Hilfetext für die Anzeige aufzurufen, klicken Sie auf das Hilfesymbol.

Ergebnisse

Um die Vorgaben für die Unterstützung offener Dateien zu definieren, verwenden Sie die Registerkarte 'Einschluss/Ausschluss' im IBM Spectrum Protect-Profileditor. Sie können die folgenden Optionen für alle Datenträger oder für einzelne Datenträger zusammen mit der Option include.fs definieren: snapshotproviderfs, presnapshotcmd, postsnapshotcmd.

Zugehörige Konzepte:
Clientoptionsreferenz
Imagesicherung
Windows-Betriebssysteme

Unterstützung offener Dateien konfigurieren

Sie konfigurieren die Unterstützung offener Dateien (Open File Support, OFS) nach der Installation des Windows-Clients.

Informationen zu diesem Vorgang

Wenn die Funktion zur Unterstützung offener Dateien (OFS) konfiguriert ist, führt der Client für Sichern/Archivieren eine momentaufnahmebasierte Operation auf Dateiebene aus, während der der reale Datenträger für andere Systemanwendungen verfügbar ist. Während der Operation wird ein konsistentes Image des Datenträgers aufrecht erhalten.

Führen Sie folgende Schritte aus, um OFS zu konfigurieren:

Vorgehensweise

1. Starten Sie die Java-GUI des Windows-Clients (führen Sie dsm.exe aus).
2. Wählen Sie Dienstprogramme > Setup-Assistent aus.
3. Wählen Sie Hilfe zum Konfigurieren der Online-Imageunterstützung aus und klicken Sie auf Weiter.
4. Klicken Sie erneut auf Weiter.
5. Wählen Sie den Momentaufnahmeprovider VSS aus, um die Unterstützung offener Dateien (Open File Support, OFS) zu aktivieren, oder wählen Sie Keine aus, um normale Sicherungen (ohne Momentaufnahme) der Dateien auf Ihrem Datenträger durchzuführen. Klicken Sie anschließend auf Weiter.
6. Klicken Sie auf Anwenden und dann auf Fertigstellen.

Ergebnisse

Um Vorgaben für die Unterstützung offener Dateien zu definieren, verwenden Sie die Registerkarte 'Einschluss/Ausschluss' im Profileditor. Sie können die folgenden Optionen für alle Datenträger oder für einzelne Datenträger zusammen mit der Option include.fs definieren: snapshotproviderfs, presnapshotcmd, postsnapshotcmd.

Zugehörige Konzepte:
Clientoptionsreferenz
 AIX-Betriebssysteme

Hinweise zur AIX-Konfiguration vor Ausführung von momentaufnahmebasierten Dateisicherungen und -archivierungen

Wenn Sie Ihren IBM Spectrum Protect-AIX-Client für die Ausführung von momentaufnahmebasierten Dateisicherungen und -archivierungen konfigurieren, sind einige Hinweise zu beachten.

- Stellen Sie sicher, dass die Datenträgergruppe, die das Dateisystem enthält, von dem eine Momentaufnahme erstellt werden soll, ausreichenden Plattenspeicherplatz aufweist, damit externe JFS2-Momentaufnahmen für das Dateisystem erstellt werden können.
- Der Client verwendet eine Standardgröße von 100 Prozent der Dateisystemgröße für die Momentaufnahmegröße. Dieser Wert wurde als geeignetster Wert für Dateisysteme mit ruhiger mittlerer Dateisystemaktivität gefunden. Wenn Sie auf der Grundlage Ihrer Erfahrung mit Ihrer eigenen Dateisystemaktivität glauben, diesen Wert verringern zu müssen, können Sie mit der Option snapshotcachesize diesen Wert durch Feinabstimmung optimieren.

- Aktivieren Sie keine internen Momentaufnahmen, wenn Sie neue JFS2-Dateisysteme unter AIX 6.1 oder höher für alle Dateisysteme erstellen, die von IBM Spectrum Protect verwaltet werden. Der Client verwendet externe Momentaufnahmen und JFS2 ermöglicht nicht die gleichzeitige Erstellung externer und interner Momentaufnahmen für dasselbe Dateisystem.

Zugehörige Verweise:
Snapshotcachesize
Linux-BetriebssystemeWindows-Betriebssysteme

NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren

Sie müssen die Verbindungsinformationen für den NetApp-Dateiserver konfigurieren, damit der Befehl für eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz auf dem Client für Sichern/Archivieren ausgeführt werden kann. Außerdem müssen Sie mit dem Befehl set password den Hostnamen des Dateiservers sowie das Kennwort und den Benutzernamen für den Zugriff auf den Dateiserver angeben.

Vorgehensweise

1. Gehen Sie wie folgt vor, um eine Konsolsitzung auf dem NetApp-Dateiserver aufzubauen und einen neuen Benutzer auf dem Dateiserver zu definieren:
   a. Fügen Sie die Benutzer-ID einer Gruppe hinzu, die eine Benutzeranmeldung auf dem Dateiserver mit HTTP und die Ausführung von API-Befehlen gestattet.
   b. Geben Sie auf dem Dateiserver den folgenden Befehl ein, um die Benutzer-ID aufzulisten und die Einstellungen zu überprüfen und ob die Ausgabe ähnlich ist:

      ```
      useradmin user list snapdiff-Benutzer

      Name: snapdiff-Benutzer
      Info:
      Rid: 131077
      Groups: snapdiff-Gruppe
      Full Name:
      ```

      Für 7-Mode-NetApp-Dateiserver:

      ```
      Allowed Capabilities: login-http-admin,api-*
      ```

      Bei Clustered Data ONTAP-NetApp-Dateiservern ist als einzige Berechtigung `ontapapi` mit der Rolle `admin` erforderlich.

   c. Ist für die Option security.passwd.firstlogin.enable für die Benutzer-ID auf dem NetApp-Server on definiert, stellen Sie sicher, dass alle Gruppen über die Leistungsmerkmale login-telnet und cli–passwd* verfügen.
   Tipp: Wenn die Option security.passwd.firstlogin.enable aktiviert ist, wird die Benutzer-ID bei der Erstellung auf expired gesetzt. Der Benutzer kann keine Befehle ausführen (auch keine Momentaufnahmedifferenzteilsicherung), bis sein Kennwort geändert wird. Benutzer in Gruppen, die nicht über diese Funktionalität verfügen, können sich nicht beim Speichersystem anmelden. Informationen zur Definition einer Benutzer-ID und eines Kennworts auf dem NetApp-Dateiserver finden Sie in der NetApp-Dokumentation.
2. Konfigurieren Sie den integrierten NetApp Data ONTAP-HTTP-Server, um Verwaltungssitzungen über Fernzugriff für den NetApp-Dateiserver zu ermöglichen.
   a. Wenn eine normale HTTP-Verbindung für Momentaufnahmedifferenzsicherungen verwendet werden soll, aktivieren Sie die Option httpd.admin.enable auf dem NetApp-Dateiserver.
   b. Wenn eine sichere HTTPS-Verbindung für Momentaufnahmedifferenzsicherungen verwendet werden soll (durch Angabe der Option -snapdiffhttps), aktivieren Sie die Option httpd.admin.ssl.enable auf dem NetApp-Dateiserver.
   c. Testen Sie auf dem IBM Spectrum Protect-Clientknoten die Verbindung zwischen dem IBM Spectrum Protect-Client-Computer und dem NetApp ONTAP-Server, um sicherzustellen, dass die Verbindung zum NetApp-Server nicht durch Firewalls oder andere NetApp-Konfigurationsoptionen verhindert wird.
   Tipp: Informationen zum Testen der Verbindung finden Sie in der NetApp ONTAP-Dokumentation.
3. Windows-BetriebssystemeExportieren Sie die NetApp-Datenträger und ziehen Sie die folgenden Einstellungen in Betracht:
   Tipp: Ausführliche Informationen zum Exportieren der NetApp-Datenträger für die Verwendung in Windows finden Sie in der NetApp-Dokumentation.
   - Ordnen Sie die NetApp-Datenträger mit CIFS zu.
   - Stellen Sie sicher, dass die NetApp-Datenträger über die NTFS-Sicherheitseinstellung verfügen.
4. Linux-BetriebssystemeExportieren Sie die NetApp-Datenträger und ziehen Sie die folgenden Einstellungen in Betracht:
   Tipp: Ausführliche Informationen zum Exportieren der NetApp-Datenträger für die Verwendung in Linux-Hosts finden Sie in der NetApp-Dokumentation.
   - Ordnen Sie die NetApp-Datenträger mit einem NFS-Mount zu.
   - Stellen Sie sicher, dass die NetApp-Datenträger über die UNIX-Sicherheitseinstellung verfügen.
5. Definieren Sie die Benutzer-ID und das Kennwort auf dem Client für Sichern/Archivieren für die in Schritt 1 erstellte Benutzer-ID, indem Sie die folgenden Schritte ausführen:
   a. Linux-BetriebssystemeMelden Sie sich mit der Rootbenutzer-ID an.
   b. Windows-BetriebssystemeMelden Sie sich als Benutzer mit Schreib-/Lesezugriff auf die CIFS-Freigabe an.
   c. Geben Sie den folgenden Befehl in die Befehlszeile des Clients für Sichern/Archivieren ein:

```
dsmc set password -type=filer eigener_Dateiserver snapdiff-Benutzer neues_Kennwort
```

Ersetzen Sie folgende Werte:

eigener_Dateiserver
: Dieser Wert ist der vollständig qualifizierte Hostname Ihres NetApp-Dateiservers.

snapdiff-Benutzer
: Dieser Wert ist die in Schritt 1 erstellte Benutzer-ID.

neues_Kennwort
: Dieser Wert ist das Kennwort für die in Schritt 1 erstellte Benutzer-ID.

- Linux-BetriebssysemeWindows-BetriebssystemeClustered Data ONTAP NetApp-Dateiserverdatenträger schützen
  Sie können eine Momentaufnahmedifferenzteilsicherung eines Datenträgers auf einem NetApp-Dateiserver erstellen, der zu einer Clustered Data ONTAP-Konfiguration gehört (C-Mode-Dateiserver).
- Linux-BetriebssysemeWindows-BetriebssystemeSnapMirror-Unterstützung für momentaufnahmegestützte progressive Teilsicherung von NetApp (snapdiff)
  Sie können die SnapDiff-Sicherungsverarbeitung von NetApp in Verbindung mit der SnapMirror-Replikation von NetApp verwenden, um Datenträger des NetApp-Quellen- oder -Ziel-Dateiservers zu sichern.

Zugehörige Tasks:
Clustered Data ONTAP NetApp-Dateiserverdatenträger schützen
Zugehörige Verweise:
Snapdiff
Snapdiffhttps
Createnewbase
Linux-BetriebssysemeWindows-Betriebssysteme

Clustered Data ONTAP NetApp-Dateiserverdatenträger schützen

Sie können eine Momentaufnahmedifferenzteilsicherung eines Datenträgers auf einem NetApp-Dateiserver erstellen, der zu einer Clustered Data ONTAP-Konfiguration gehört (C-Mode-Dateiserver).

Vorbereitende Schritte

- Führen Sie die Prozedur in NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren aus.
- Stellen Sie sicher, dass die Clustered Data ONTAP-Umgebung korrekt vom Administrator der NetApp Storage Virtual Machine konfiguriert wurde.

Einschränkung: Die IBM Spectrum Protect-Unterstützung für Momentaufnahmedifferenzteilsicherungen von Clustered Data ONTAP-Datenträgern gilt nur bei NetApp ONTAP 8.2.1 und höheren Versionen.

Informationen zu diesem Vorgang

In einer Clustered Data ONTAP-Umgebung enthalten Storage Virtual Machines (die auch als Daten-vServer bezeichnet werden) Datenträger, die vom Client für Sichern/Archivieren geschützt werden können.

Eine Storage Virtual Machine besteht aus einem einzelnen infiniten Datenträger (Infinite Volume) oder einem oder mehreren flexiblen Datenträgern (FlexVol Volumes). Der Zugriff auf Datenträger erfolgt über Fernzugriff mithilfe der Dateifreigabe (CIFS unter Windows-Betriebssystemen, NFS unter Linux-Betriebssystemen).

Die Storage Virtual Machines werden vom Cluster-Management-Dateiserver verwaltet, dem physischen Dateiserver (C-Mode-Dateiserver), auf dem sich die Storage Virtual Machines befinden. Der Sicherungsclient ist auf der fernen Maschine installiert, die auf die Datenträger zugreift.

Der Client für Sichern/Archivieren muss mit Berechtigungsnachweisen für die NetApp-C-Mode-Dateiserver konfiguriert werden, auf die für Sicherungsoperationen zugegriffen wird.

Voraussetzungen:

- Für diese Prozedur sind die folgenden Informationen erforderlich:
  - Der Hostname oder die IP-Adresse des Cluster-Management-Dateiservers.
  - Der Hostname oder die IP-Adresse der Storage Virtual Machine.
  - Der Name der Storage Virtual Machine.
  - Die Berechtigungsnachweise des Cluster-Management-Dateiservers (Benutzername und Kennwort).
- Dem Benutzer des Cluster-Management-Dateiservers, der vom Client konfiguriert wird, muss die Berechtigung `ontapapi` mit der Rolle `admin` zugeordnet sein.

  Die Berechtigung `ontapapi` ermöglicht keinen interaktiven Zugriff auf den Dateiserver mithilfe von Methoden wie `telnet`, `ssh` oder `http/https`. Für die Ausführung von Momentaufnahmedifferenzteilsicherungen sind keine weiteren Benutzerberechtigungen erforderlich.

Vorgehensweise

Führen Sie die folgenden Schritte auf der fernen Maschine aus, auf der der Client für Sichern/Archivieren installiert ist:

1. Konfigurieren Sie den Client für Sichern/Archivieren mit den Berechtigungsnachweisen des Cluster-Management-Dateiservers. Verwenden Sie den Befehl dsmc set password, um die Berechtigungsnachweise des Management-Dateiservers, der der Storage Virtual Machine zugeordnet ist, zu speichern. Geben Sie beispielsweise den folgenden Befehl ein:

   ```
   dsmc set password -type=filer Hostname_des_Management-Dateiservers
      Name_des_Benutzers_des_Management-Dateiservers Kennwort_des_Management-Dateiservers
   ```

   Dabei gilt:

   Hostname_des_Management-Dateiservers
   : Der Hostname oder die IP-Adresse des Cluster-Management-Dateiservers.

   Name_des_Benutzers_des_Management-Dateiservers
   : Der Name des Benutzers des Cluster-Management-Dateiservers.

   Kennwort_des_Management-Dateiservers
   : Das Kennwort für den Benutzer des Management-Dateiservers.

   Tipp: Das Kennwort des Cluster-Management-Dateiservers wird verschlüsselt, wenn es vom Client für Sichern/Archivieren gespeichert wird.
2. Ordnen Sie jede Storage Virtual Machine mithilfe des Befehls dsmc set netappsvm dem Management-Dateiserver zu. Geben Sie z. B. den folgenden Befehl ein:

   ```
   dsmc set netappsvm Hostname_der_Storage_Virtual_Machine
   Hostname_des_Management-Dateiservers Name_der_Storage_Virtual_Machine
   ```

   Dabei gilt:

   Hostname_der_Storage_Virtual_Machine
   : Der Hostname oder die IP-Adresse der Storage Virtual Machine, die zur Bereitstellung von Datenträgern verwendet wird, die gesichert werden sollen.

   Hostname_des_Management-Dateiservers
   : Der Hostname oder die IP-Adresse des Cluster-Management-Dateiservers.

   Name_der_Storage_Virtual_Machine
   : Der Name der Storage Virtual Machine.

   Anmerkung: Der Hostname oder die IP-Adresse der Storage Virtual Machine, die zur Bereitstellung von Datenträgern verwendet wird, muss mit der Angabe in den Befehlen dsmc set konsistent sein. Wenn beispielsweise die Datenträger über die IP-Adresse einer Storage Virtual Machine bereitgestellt werden, muss die IP-Adresse (nicht der Hostname) in den Befehlen dsmc set verwendet werden. Andernfalls schlägt die Clientauthentifizierung mit dem Cluster-Management-Dateiserver fehl.

   Sie müssen den Befehl dsmc set netappsvm nur einmal für jede Storage Virtual Machine angeben. Wenn die Storage Virtual Machine auf einen anderen Cluster-Management-Dateiserver versetzt wird, müssen Sie den Hostnamen des zugehörigen Cluster-Management-Dateiservers mithilfe des Befehls aktualisieren.
3.  Windows-BetriebssystemeOrdnen Sie die Datenträger Laufwerkbuchstaben zu. Geben Sie beispielsweise den folgenden Befehl für jede Storage Virtual Machine ein:

   ```
   net use y: \\Hostname_der_Storage_Virtual_Machine Domänenname\Name_der_CIFS-Freigabe
   ```

   Dabei gilt:

   `y:`
   : Das Laufwerk, dem der Datenträger zugeordnet werden soll.

   Hostname_der_Storage_Virtual_Machine
   : Der Hostname oder die IP-Adresse der Storage Virtual Machine.

   Domänenname\Name_der_CIFS-Freigabe
   : Die CIFS-Freigabe, die auf dem Dateiserver auf dem Datenträger definiert ist, der gesichert wird.
4.  Linux-BetriebssystemeStellen Sie die ferne Storage Virtual Machine auf einem lokalen Dateisystem bereit. Geben Sie beispielsweise den folgenden Befehl für jede Storage Virtual Machine ein:

   ```
   mount Hostname_der_Storage_Virtual_Machine/tmp/fs1
   ```

   Dabei gilt:

   Hostname_der_Storage_Virtual_Machine
   : Der Hostname oder die IP-Adresse der Storage Virtual Machine.

   /tmp/fs1
   : Ein Beispiel eines Dateisystems, in dem der Datenträger der Storage Virtual Machine bereitgestellt werden soll.
5. Starten Sie eine progressive vollständige Teilsicherung eines flexiblen oder infiniten Datenträgers.

Der HTTP-Zugriff auf den NetApp-Dateiserver ist standardmäßig nicht aktiviert. Wenn Sie Ihren Dateiserver nicht so konfiguriert haben, dass der Zugriff unter Verwendung von HTTP zulässig ist, verwenden Sie die Option snapdiffhttps des Clients für Sichern/Archivieren, um den Zugriff auf den Cluster-Management-Server mit dem Protokoll HTTPS zu ermöglichen.

 Windows-BetriebssystemeGeben Sie beispielsweise auf Windows-Clients den folgenden Befehl ein:

```
dsmc incr y: -snapdiff -snapdiffhttps
```

 Linux-BetriebssystemeGeben Sie beispielsweise auf Linux-Clients den folgenden Befehl ein:

```
dsmc incr /tmp/fs1 -snapdiff -snapdiffhttps
```

Tipp: Sie müssen die progressive vollständige Teilsicherung nur einmal ausführen. Nachdem diese Sicherung erfolgreich abgeschlossen wurde, führen in zukünftigen Sicherungsoperationen Differenzsicherungen aus.

6. Starten Sie eine Momentaufnahmedifferenzsicherung des flexiblen oder infiniten Datenträgers.
 Windows-BetriebssystemeGeben Sie beispielsweise auf Windows-Clients den folgenden Befehl ein:

```
dsmc incr y: -snapdiff -snapdiffhttps
```

 Linux-BetriebssystemeGeben Sie beispielsweise auf Linux-Clients den folgenden Befehl ein:

```
dsmc incr /tmp/fs1 -snapdiff -snapdiffhttps
```

Beispiel

Ein Benutzer des Clients für Sichern/Archivieren möchte eine Momentaufnahmedifferenzteilsicherung der Datenträger auf einem C-Mode-Dateiserver ausführen. Der Benutzer verwendet für die Ausführung der Sicherung einen Windows-Client für Sichern/Archivieren und die Datenträger werden als CIFS-Freigaben bereitgestellt. Die Konfiguration des C-Mode-Dateiservers ist wie folgt:

ONTAP 8.31-Management-Dateiserver

```
Hostname: netapp1mgmt.example.com
Benutzer: netapp1mgmt_user
Kennwort: pass4netapp1mgmt
CIFS-Domänencontroller: WINDC
Domänenbenutzer: domainuser
```

Storage Virtual Machine mit flexiblem Datenträger

```
Hostname: netapp1-v1.example.com
Name der Storage Virtual Machine: netapp1-client1
CIFS-Freigabe: demovol
Datenträgername: demovol
```

Storage Virtual Machine mit infinitem Datenträger

```
Hostname: netapp1-v4.example.com
Name der Storage Virtual Machine: netapp1-infiniteVolume1
CIFS-Freigabe: InfiniteVol
```

Der Benutzer führt auf dem Client für Sichern/Archivieren die folgenden Schritte aus:

1. Konfigurieren des Clients mit Berechtigungsnachweisen des Management-Dateiservers durch Ausgabe des folgenden Befehls:

   ```
   dsmc set password -type=filer netapp1mgmt.example.com netapp1mgmt_user pass4netapp1mgmt
   ```

2. Definieren der Storage Virtual Machine-Zuordnungen für jede Storage Virtual Machine mit den folgenden Befehlen:

   ```
   dsmc set netappsvm netapp1-v1.example.com netapp1mgmt.example.com netapp1-client1

   dsmc set netappsvm netapp1-v4.example.com netapp1mgmt.example.com netapp1-infiniteVolume1
   ```

3. Zuordnen ferner Datenträger zu Laufwerkbuchstaben für jede Storage Virtual Machine:

   ```
   net use y: \\netapp1-v1.example.com\demovol WINDC\domainuser

   net use z: \\netapp1-v4.example.com\InfiniteVol WINDC\domainuser
   ```

4. Ausführen einer progressiven vollständigen Teilsicherung des flexiblen Datenträgers und des infiniten Datenträgers:

   ```
   dsmc incr y: -snapdiff -snapdiffhttps

   dsmc incr z: -snapdiff -snapdiffhttps
   ```

   Sie müssen die progressive vollständige Teilsicherung nur einmal ausführen. Nachdem diese Sicherung erfolgreich abgeschlossen wurde, führen Sie in zukünftigen Sicherungsoperationen Differenzsicherungen aus.

5. Ausführen einer Momentaufnahmedifferenzsicherung des flexiblen Datenträgers und des infiniten Datenträgers:

   ```
   dsmc incr y: -snapdiff -snapdiffhttps
   ```

```
dsmc incr z: -snapdiff -snapdiffhttps
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

SnapMirror-Unterstützung für momentaufnahmegestützte progressive Teilsicherung von NetApp (snapdiff)

Sie können die SnapDiff-Sicherungsverarbeitung von NetApp in Verbindung mit der SnapMirror-Replikation von NetApp verwenden, um Datenträger des NetApp-Quellen- oder -Ziel-Dateiservers zu sichern.

In einer NetApp-SnapMirror-Umgebung werden Daten auf Datenträgern, die dem primären Datencenter zugeordnet sind, auf Datenträger gespiegelt, die einem fernen Server an einem Standort zur Wiederherstellung nach einem Katastrophenfall zugeordnet sind. Der NetApp-Dateiserver im primären Datencenter wird als Quellen-Dateiserver bezeichnet und der NetApp-Dateiserver am Standort zur Wiederherstellung nach einem Katastrophenfall als Ziel-Dateiserver. Mithilfe des Clients für Sichern/Archivieren können Sie Momentaufnahmedifferenzsicherungen der Datenträger auf dem Quellen- und Ziel-Dateiserver erstellen.

Szenario: Daten auf einem Datenträger des Quellen-Dateiservers sichern

 Linux-BetriebssystemeSie können in der Konfiguration des Clients für Sichern/Archivieren angeben, dass Daten von den Datenträgern des Quellen-Dateiservers gesichert werden sollen. Für dieses Szenario müssen Sie einen Knoten des Clients für Sichern/Archivieren so konfigurieren, dass er Zugriff auf die Datenträger des NetApp-Quellen-Dateiservers hat; dabei werden mit NFS exportierte Freigaben zum Anhängen der Dateiserverdatenträger verwendet.

 WindowsBetriebssystemeIn der Konfiguration des Clients für Sichern/Archivieren können Sie angeben, dass Daten von den Datenträgern des Quellen-Dateiservers gesichert werden sollen. Für dieses Szenario müssen Sie einen Knoten des Clients für Sichern/Archivieren so konfigurieren, dass er Zugriff auf die Datenträger des NetApp-Quellen-Dateiservers hat; dabei werden CIFS-Freigaben zum Anhängen der Dateiserverdatenträger verwendet.

 LinuxBetriebssystemeAngenommen, es wird eine Konfiguration verwendet, in der der Quellen-Dateiserver den Namen ProdFiler hat. Außerdem wird angenommen, dass auf dem Dateiserver ProdFiler ein Datenträger mit dem Namen UserDataVol vorhanden ist und dass mithilfe von NFS über einen Clientknoten für Sichern/Archivieren auf den Datenträger zugegriffen werden kann. Es wird angenommen, dass die Freigabe als UserDataVol_Share angehängt ist.

 WindowsBetriebssystemeAngenommen, es wird eine Konfiguration verwendet, in der der Quellen-Dateiserver den Namen ProdFiler hat. Außerdem wird angenommen, dass auf dem Dateiserver ProdFiler ein Datenträger mit dem Namen UserDataVol vorhanden ist und dass mithilfe von CIFS über einen Clientknoten für Sichern/Archivieren auf den Datenträger zugegriffen werden kann. Es wird angenommen, dass die Freigabe als UserDataVol_Share angehängt ist.

Wenn Sie eine Momentaufnahmedifferenzsicherung einleiten, erstellt der NetApp-Dateiserver eine neue Differenzmomentaufnahme auf dem Datenträger, der gerade gesichert wird. Diese Differenzmomentaufnahme wird mit der Basismomentaufnahme (die vorherige Momentaufnahme) verglichen. Der Name der Basismomentaufnahme wurde bei Beendigung der vorherigen Sicherung auf dem IBM Spectrum Protect-Server registriert. Der Inhalt dieser Basismomentaufnahme wird mit der Differenzmomentaufnahme verglichen, die auf dem Datenträger des Quellen-Dateiservers erstellt wird. Unterschiede zwischen den beiden Momentaufnahmen werden auf dem Server gesichert.

Die Momentaufnahmedifferenzsicherung wird mit dem folgenden Befehl eingeleitet. Der Befehl wird an der Konsole eines Clientknotens eingegeben, der für den Zugriff auf die Datenträger auf dem Quellen-Dateiserver sowie für den Schutz dieser Datenträger konfiguriert ist. Da dieser Befehl für die Sicherung von Datenträgern auf einem Quellen-Dateiserver ausgegeben wird, wird eine neue Momentaufnahme (die Differenzmomentaufnahme) erstellt und die auf dem IBM Spectrum Protect-Server registrierte Momentaufnahme wird als Basismomentaufnahme verwendet. Die Erstellung sowohl der Differenzmomentaufnahme als auch der Basismomentaufnahme ist das Standardverhalten. Die Option `-diffsnapshot=create` ist ein Standardwert und muss in diesem Befehl nicht explizit angegeben werden.

```
dsmc incr \\ProdFiler\UserDataVol_Share -snapdiff -diffsnapshot=create
```

Daten auf einem Ziel-Dateiserver sichern

Eine typischere Konfiguration besteht darin, die Sicherungen vom Quellen-Dateiserver auszulagern. Hierbei werden Sicherungen der Quellendatenträger mithilfe der replizierten Datenträgermomentaufnahmen, die auf dem Ziel-Dateiserver gespeichert sind, erstellt. Gewöhnlich stellt die Sicherung eines Ziel-Dateiservers ein Problem dar, weil für die Erstellung einer Momentaufnahmedifferenzsicherung eine neue Momentaufnahme auf dem Datenträger, den Sie gerade sichern, erstellt werden muss. Die Datenträger des Ziel-Dateiservers, in denen der Inhalt der Quellendatenträger gespiegelt ist, sind schreibgeschützte Datenträger. Daher können auf ihnen keine Momentaufnahmen erstellt werden.

Um diese Einschränkung, die aufgrund des Schreibschutzes besteht, zu umgehen, werden Clientkonfigurationsoptionen zur Verfügung gestellt, mit denen Sie die vorhandenen Basis- und Differenzmomentaufnahmen auf dem schreibgeschützten Zieldatenträger verwenden können, um Änderungen auf dem IBM Spectrum Protect-Server zu sichern.

 AIX-Betriebssysteme  LinuxBetriebssystemeWie in dem Szenario für den Quellen-Dateiserver erfolgt der Zugriff auf die Datenträger des Ziel-Dateiservers mithilfe von mit NFS exportierten Freigaben.

 WindowsBetriebssystemeWie in dem Szenario für den Quellen-Dateiserver erfolgt der Zugriff auf die Datenträger des Ziel-Dateiservers mithilfe von CIFS-Freigaben.

Zusammenfassung der Momentaufnahmedifferenzoptionen

Die Option useexistingbase bewirkt, dass die jüngste Momentaufnahme auf dem Datenträger als Basismomentaufnahme verwendet wird, wenn eine Basismomentaufnahme erstellt werden muss. Eine neue Basismomentaufnahme wird erstellt, wenn eine der folgenden Bedingungen erfüllt ist:

- Wenn diese Sicherung die Erstsicherung ist.
- Wenn `createnewbase=yes` angegeben ist.
- Wenn die Basismomentaufnahme, die durch eine vorherige Differenzmomentaufnahme registriert wurde, nicht mehr vorhanden ist und keine Momentaufnahme vorhanden ist, die älter als die fehlende Basismomentaufnahme ist.

Wenn diese Option nicht angegeben wird, wird eine neue Momentaufnahme auf dem Datenträger erstellt, der gesichert wird. Da Datenträger des Ziel-Dateiservers schreibgeschützt sind, muss useexistingbase bei der Erstellung von Momentaufnahmedifferenzsicherungen von Datenträgern des Ziel-Dateiservers angegeben werden. Wenn useexistingbase nicht angegeben wird, schlagen Momentaufnahmedifferenzsicherungen eines Datenträgers des Ziel-Dateiservers fehl, weil die neue Momentaufnahme auf dem schreibgeschützten Datenträger nicht erstellt werden kann.

Verwenden Sie bei der Sicherung von Datenträgern des Ziel-Dateiservers sowohl die Option useexistingbase als auch die Option diffsnapshot=latest, um sicherzustellen, dass während der Datenträgersicherung die neuesten Basis- und Differenzmomentaufnahmen verwendet werden.

Mit der Option basesnapshotname geben Sie an, welche Momentaufnahme auf dem Datenträger des Ziel-Dateiservers als Basismomentaufnahme verwendet werden soll. Wenn Sie diese Option nicht angeben, wird die jüngste Momentaufnahme auf dem Datenträger des Ziel-Dateiservers als Basismomentaufnahme verwendet. Den Namen der Basismomentaufnahme können Sie mithilfe von Platzhalterzeichen angeben.

Mit der Option diffsnapshotname können Sie angeben, welche Differenzmomentaufnahme auf dem Datenträger des Ziel-Dateiservers während einer Momentaufnahmedifferenzsicherung verwendet werden soll. Diese Option wird nur angegeben, wenn Sie auch diffsnapshot=latest angeben. Den Namen der Differenzmomentaufnahme können Sie mithilfe von Platzhalterzeichen angeben.

Die Option diffsnapshot=latest gibt an, dass Sie die neueste Momentaufnahme, die auf dem Dateiserver gefunden wird, als Quellenmomentaufnahme verwenden wollen.

Weitere Informationen zu diesen Optionen finden Sie in den Abschnitten der Clientoptionsreferenz.

Befehlsbeispiele für Momentaufnahmedifferenzsicherungen

In den nachfolgenden Beispielen wird davon ausgegangen, dass Datenträger auf einem Quellen-Dateiserver mithilfe der SnapMirror-Technologie von NetApp auf einem Dateiserver für die Wiederherstellung nach einem Katastrophenfall (Hostname DRFiler) repliziert werden. Da die Datenträger auf DRFiler schreibgeschützt sind, verwenden Sie die Optionen zur Angabe, welche der replizierten Momentaufnahmen als Basismomentaufnahme und welche der Momentaufnahmen als Differenzmomentaufnahme verwendet werden soll. Werden bei der Erstellung einer Momentaufnahmedifferenzsicherung eines Ziel-Dateiservers die zu verwendenden Momentaufnahmen angegeben, wird kein Versuch unternommen, eine Momentaufnahme auf den schreibgeschützten Datenträgern zu erstellen.

Die folgenden Befehle werden verwendet, um Momentaufnahmedifferenzsicherungen einzuleiten. Bei den meisten dieser Befehle werden Momentaufnahmedifferenzsicherungen mithilfe von Momentaufnahmen erstellt, die auf den Datenträgern des Ziel-Dateiservers gespeichert sind. Achten Sie bei der Sicherung von einem Datenträger des Ziel-Dateiserver darauf, dass die Option -useexistingbase angegeben wird, weil diese Option dafür sorgt, dass kein Versuch zur Erstellung einer neuen Momentaufnahme auf den schreibgeschützten Datenträgern des Ziel-Dateiservers unternommen wird.

Beispiel 1: Ziel-Dateiserversicherung in täglichen, durch den NetApp-Momentaufnahmescheduler erstellten Standardsicherungen durchführen

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase
  -diffsnappshot=latest -basesnapshotname="nightly.?"
```

Sie können ein Fragezeichen (?) als Entsprechung für ein einzelnes Zeichen verwenden. In diesem Beispiel wird durch die Angabe von -basesnapshotname=nightly.? die jüngste Basismomentaufnahme mit dem Teilnamen "nightly.", an den sich ein einzelnes Zeichen anschließt (z. B. nightly.0, nightly.1 etc.) verwendet.

Beispiel 2: Datenträger eines Ziel-Dateiservers mithilfe manuell (nicht durch den NetApp-Momentaufnahmescheduler) erstellter Momentaufnahmen sichern

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase
  -diffsnapshot=latest -basesnapshotname="share_vol_base?"
  -diffsnapshotname="share_vol_diff?"
```

Auch in diesem Beispiel wird das Fragezeichen (?) zur Veranschaulichung der Syntax verwendet, wenn die Namen der Basis- und der Differenzmomentaufnahme unterschiedliche Nummern enthalten.

Beispiel 3: Datenträger eines Ziel-Dateiservers sichern und die für die Basis- und Differenzmomentaufnahmen zu verwendenden Momentaufnahmen angeben

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase
  -diffsnapshot=latest -basesnapshotname="share_vol_base"
  -diffsnapshotname="share_vol_diff_snap"
```

Beispiel 4: Scriptgenerierte Momentaufnahmen sichern, die eine Namenskonvention verwenden

In diesem Beispiel fügt ein auf dem NetApp-Dateiserver ausgeführtes Script den Momentaufnahmenamen ein Datum und eine Zeitmarke hinzu. Eine am 3. November 2012 um 23:36:33 Uhr erstellte Momentaufnahme heißt beispielsweise UserDataVol_20121103233633_snapshot. Sie können Platzhalterzeichen in den Optionen verwenden, um die jüngsten Basis- und Differenzmomentaufnahmen auszuwählen. Beispiel:

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase
  -basesnapshotname="UserDataVol_Share_*_snapshot" -diffsnapshot=latest
  -diffnsnapshotname="UserDataVol_Share_*snapshot
```

-useexistingbase wählt die jüngste Basismomentaufnahme aus. Wird in -basesnapshotname ein Stern (*) als Platzhalterzeichen hinzugefügt, wird die jüngste Basismomentaufnahme ausgewählt, die der Scriptnamenskonvention entspricht. Die Option -diffsnapshot=latest verhindert die Erstellung einer neuen Differenzmomentaufnahme und -diffsnapshotname= wählt die jüngste vorhandene Differenzmomentaufnahme aus, die der Scriptnamenskonvention entspricht. (Das Platzhalterzeichen * entspricht einer beliebigen Zeichenfolge.)

Beispiel 5: Momentaufnahmedifferenzsicherung mithilfe einer auf dem Quellen-Dateiserver vorhandenen Differenzmomentaufnahme durchführen

Soll eine auf dem Quellen-Dateiserver vorhandene Differenzmomentaufnahme verwendet werden, geben Sie -diffsnapshot=latest an, um die Erstellung einer neuen Differenzmomentaufnahme zu verhindern. Geben Sie außerdem die Option -diffsnapshotname an, um festzulegen, welche vorhandene Differenzmomentaufnahme verwendet werden soll. Die von Ihnen angegebene Momentaufnahme wird mit der Basismomentaufnahme verglichen, die bei der Erstellung der letzten Sicherung in der IBM Spectrum Protect-Serverdatenbank registriert wurde. Beispiel:

```
dsmc incr \\ProdFiler\UserDataVol_Share -snapdiff -diffsnapshot=latest
  -diffsnapshotname="share_vol_diff_snap"
```

Workstation bei einem Server registrieren

Damit Sie IBM Spectrum Protect verwenden können, müssen Sie einen Knotennamen und ein Kennwort definieren und Ihren Knoten beim Server registrieren.

Der Prozess, bei dem ein Knotenname und ein Kennwort definiert werden, wird als *Registrierung* bezeichnet. Es sind zwei Registrierungstypen verfügbar: *offene* und *geschlossene* Registrierung.

Der Registrierungstyp für Ihren Standort wird von Ihrem IBM Spectrum Protect-Serveradministrator ausgewählt.

Einschränkung: Ab IBM Spectrum Protect-Server der Version 8.1.2 ist die offene Registrierung nicht mehr verfügbar. Sie müssen die geschlossene Registrierung verwenden. Die offene Registrierung ist nur für IBM Spectrum Protect-Server der Version 8.1.1, Version 8.1.0, Version 7.1.7 oder einer früheren Version verfügbar.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeSie müssen ein Root oder ein berechtigter Benutzer sein, um diese erforderliche Task auszuführen.

Wenn Sie planen, den Web-Client zu verwenden, benötigen Sie eine Benutzer-ID mit Administratorberechtigung, die über Systemberechtigung, Maßnahmenberechtigung, Clientzugriffsberechtigung oder Clienteignerberechtigung verfügt. Wenn ein neuer Knoten registriert wird, muss der Serveradministrator eine Benutzer-ID mit Administratorberechtigung erstellen, die mit dem Knotennamen übereinstimmt. Standardmäßig hat dieser Knoten Clienteignerberechtigung.

Der IBM Spectrum Protect-Serveradministrator muss den Parameter userid im Serverbefehl REGISTER NODE angeben:

```
REGISTER NODE Knotenname Kennwort userid=Benutzer-ID
```

Dabei müssen der Knotenname und die Benutzer-ID mit Administratorberechtigung übereinstimmen. Beispiel:

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

- Geschlossene Registrierung
  Bei der geschlossenen Registrierung muss der IBM Spectrum Protect-Administrator Ihre Workstation als Clientknoten beim Server registrieren. Verwendet Ihr Unternehmen die geschlossene Registrierung, müssen Sie Ihrem IBM Spectrum Protect-Administrator einige Informationen zur Verfügung stellen.
- Offene Registrierung
  Bei der offenen Registrierung kann ein Systemadministrator Ihre Workstation als Clientknoten beim IBM Spectrum Protect-Server der Version 8.1.1, Version 8.1.0, Version 7.1.7 oder einer früheren Version registrieren.

Geschlossene Registrierung

Bei der geschlossenen Registrierung muss der IBM Spectrum Protect-Administrator Ihre Workstation als Clientknoten beim Server registrieren. Verwendet Ihr Unternehmen die geschlossene Registrierung, müssen Sie Ihrem IBM Spectrum Protect-Administrator einige Informationen zur Verfügung stellen.

Informationen zu diesem Vorgang

Die folgenden Informationen müssen Sie Ihrem IBM Spectrum Protect-Administrator bereitstellen:

- Ihren Knotennamen (dies ist der vom Befehl **hostname** zurückgegebene Wert, der Name Ihrer Workstation oder der mit der Option ***nodename*** angegebene Knotenname). Wenn Sie keinen Knotennamen mit der Option ***nodename*** angeben, ist die Standardanmelde-ID der Name, den der Befehl **hostname** zurückgibt.
- Das gewünschte Anfangskennwort, falls erforderlich.
- Kontaktinformationen, wie z. B. Benutzername, Benutzer-ID und Rufnummer.

Ihr IBM Spectrum Protect-Administrator definiert Folgendes für Sie:

- Die Maßnahmendomäne, zu der der Clientknoten des Benutzers gehört. Eine Maßnahmendomäne enthält die Maßnahmengruppen und Verwaltungsklassen, die steuern, wie IBM Spectrum Protect die von Ihnen gesicherten und archivierten Dateien verwaltet.
- Ob Dateien komprimiert werden können, bevor sie an den Server gesendet werden.
- Ob der Benutzer Sicherungs- und Archivierungsdaten aus dem Serverspeicher löschen darf.

Offene Registrierung

Bei der offenen Registrierung kann ein Systemadministrator Ihre Workstation als Clientknoten beim IBM Spectrum Protect-Server der Version 8.1.1, Version 8.1.0, Version 7.1.7 oder einer früheren Version registrieren.

Informationen zu diesem Vorgang

Beim ersten Start einer Sitzung werden Sie zur Eingabe von Informationen aufgefordert, die für die Registrierung Ihrer Workstation bei dem in Ihrer Clientoptionsdatei angegebenen IBM Spectrum Protect-Server erforderlich sind. Sie müssen den Knotennamen, ein Kennwort und Kontaktinformationen angeben.

Bei Verwendung der offenen Registrierung:

- Wird der Clientknoten des Benutzers der Maßnahmendomäne **Standard** zugeordnet.
- Können Archivierungskopien, jedoch keine Sicherungsversionen von Dateien aus dem Serverspeicher gelöscht werden.

Falls erforderlich, kann Ihr IBM Spectrum Protect-Administrator diese Standardwerte später ändern.

Einschluss-/Ausschlussliste erstellen

Wenn Sie keine Einschluss-/Ausschlussliste erstellen, berücksichtigt der Client für Sichern/Archivieren alle Dateien für Sicherungsservices und verwendet die Standardverwaltungsklasse für Sicherungs- und Archivierungsservices.

Informationen zu diesem Vorgang

Hierbei handelt es sich um eine optionale Task, die aber sehr wichtig ist.

Mithilfe einer Einschluss-/Ausschlussliste können bestimmte Dateien oder Dateigruppen von den Sicherungsservices ausgeschlossen und Dateien bestimmte Verwaltungsklassen zugeordnet werden. Der Client sichert jede Datei, die nicht explizit ausgeschlossen wurde. Sie sollten die IBM Spectrum Protect-Clientverzeichnisse von den Sicherungsservices ausschließen. Mit dem Befehl query inclexcl können Sie eine Liste der Einschluss- und Ausschlussanweisungen in der Reihenfolge anzeigen, in der sie bei der Bestimmung, ob ein Objekt eingeschlossen werden soll, geprüft werden.

Windows-BetriebssystemeGeben Sie die Einschluss-/Ausschlussliste in Ihrer Clientoptionsdatei (dsm.opt) an. Die Einschluss-/Ausschlussliste kann auch in einer separaten Datei stehen, auf die die Option inclexcl verweist. Bei den Include/Exclude-Anweisungen muss Groß-/Kleinschreibung nicht berücksichtigt werden.

Windows-BetriebssystemeDie Clientoptionsdatei dsm.opt muss ein Nicht-Unicode-Format haben. Wenn Sie jedoch mit einer separaten Einschluss-/Ausschlussdatei arbeiten, kann sie Unicode- oder Nicht-Unicode-Format haben.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeGeben Sie die Einschluss-/Ausschlussliste in Ihrer Datei dsm.sys an. Wenn mehrere Server in der Datei dsm.sys definiert sind, muss für jeden Server eine eigene Einschluss-/Ausschlussliste angegeben werden. In dieser Liste können auch Include/Exclude-Anweisungen aus Einschluss-/Ausschlussdateien enthalten sein, die Sie mit der Option inclexcl angeben.

Windows-BetriebssystemeWenn der Client Include/Exclude-Anweisungen verarbeitet, werden die Include/Exclude-Anweisungen innerhalb der Einschluss-/Ausschlussdatei in derselben Reihenfolge an die Position in dsm.opt gestellt, die durch die Option inclexcl belegt ist, und entsprechend verarbeitet.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWenn der Client Include/Exclude-Anweisungen verarbeitet, werden die Include/Exclude-Anweisungen innerhalb der Einschluss-/Ausschlussdatei in derselben Reihenfolge an die Position in dsm.sys gestellt, die durch die Option inclexcl belegt ist, und entsprechend verarbeitet.

Vorgehensweise

Für das Erstellen einer Einschluss-/Ausschlussliste bzw. für die Angabe einer Einschluss-/Ausschlussdatei können Sie mit folgenden Methoden arbeiten:

- Sie können Einschluss-/Ausschlussanweisungen in der Verzeichnisstruktur der GUI des Clients für Sichern/Archivieren oder des Web-Clients hinzufügen. Die Onlinehilfe bietet detaillierte Anweisungen.
  1. Öffnen Sie das Menü Editieren und wählen Sie Clientvorgaben aus. Wählen Sie im Dialog 'Vorgaben' die Registerkarte Einschluss/Ausschluss aus. Sie können eine INCLEXCL-Datei über den Profileditor angeben. Über den Profileditor können Sie die INCLEXCL-Datei jedoch nicht erstellen.
  2. Erstellen Sie anhand der aufgelisteten Schritte die Einschluss-/Ausschlussliste manuell.
- Sie können eine Einschluss-/Ausschlussliste manuell erstellen, indem Sie die folgenden Schritte ausführen:
  1. Legen Sie Ihre Einschluss- und Ausschlussanforderungen fest.
  2. Windows-BetriebssystemeLokalisieren Sie die Clientoptionsdatei.
  3. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeLokalisieren Sie die Serverzeilengruppe in Ihrer Datei dsm.sys. Jede Serverzeilengruppe muss über eine eigene Einschluss-/Ausschlussliste verfügen.
  4. Windows-Betriebssysteme**Wichtig:** Ordnen Sie Ihre Include/Exclude-Optionen zusammen in Ihrer Clientoptionsdatei an.
  5. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeGeben Sie Ihre include- und exclude-Anweisungen ein. Der Client wertet *zuerst* alle Anweisungen exclude.fs und exclude.dir aus (unabhängig von ihrer Position in der Einschluss-/Ausschlussliste) und entfernt die ausgeschlossenen Dateibereiche, Verzeichnisse und Dateien aus der Liste der Objekte, die für die Verarbeitung verfügbar sind. Alle anderen Include/Exclude-Anweisungen werden vom Ende der Liste aufwärts zum Anfang verarbeitet. Deshalb ist es wichtig, alle Include/Exclude-Anweisungen in der richtigen Reihenfolge einzugeben. Mit der folgenden Einschluss-/Ausschlussliste wird die Datei `includefile.cpp` beispielsweise *nicht gesichert*:

     ```
     include /Users/user01/Documents/includefile.cpp
     exclude /Users/user01/Documents/.../*
     ```

     Mit der folgenden Einschluss-/Ausschlussliste wird die Datei `includefile.cpp` jedoch gesichert:

     ```
     exclude /Users/user01/Documents/.../*
     include /Users/user01/Documents/includefile.cpp
     ```

  6. Windows-BetriebssystemeGeben Sie Ihre include- und exclude-Anweisungen ein. Der Client wertet *zuerst* alle Anweisungen exclude.dir aus (unabhängig von ihrer Position in der Einschluss-/Ausschlussliste) und entfernt die ausgeschlossenen Verzeichnisse und Dateien aus der Liste der Objekte, die für die Verarbeitung verfügbar sind. Alle anderen Include/Exclude-Anweisungen werden vom Ende der Liste aufwärts zum Anfang verarbeitet. Deshalb ist es wichtig, alle Include/Exclude-Anweisungen in der richtigen Reihenfolge einzugeben. Mit der folgenden Einschluss-/Ausschlussliste wird die Datei `includefile.txt` beispielsweise *nicht gesichert*:

     ```
     include c:\test\includefile.txt
     exclude c:\test\...\*
     ```

     Mit der folgenden Einschluss-/Ausschlussliste wird die Datei `includefile.txt` jedoch *gesichert*:

     ```
     exclude c:\test\...\*
     include c:\test\includefile.txt
     ```

  7. Die Datei sichern und schließen.

     Mac OS X-BetriebssystemeFür Mac OS X: Stellen Sie sicher, dass Sie die Datei als einfache, in Unicode (UTF-8 oder UTF-16) codierte Textdatei sichern. Fügen Sie nicht die Erweiterung `.txt` hinzu.

  8. Windows-BetriebssystemeStarten Sie den Client sowie den Scheduler-Service und den Clientakzeptorservice erneut, um Ihre Einschluss-/Ausschlussliste zu aktivieren.
  9. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeStarten Sie den Client erneut, um Ihre Einschluss-/Ausschlussliste zu aktivieren.

- Einschluss-/Ausschlussoptionen
  Dieser Abschnitt enthält kurze Beschreibungen der Optionen include und exclude, die Sie in Ihrer Clientoptionsdatei angeben können, eine minimale Einschluss-/Ausschlussliste für den Ausschluss von Systemdateien, eine Liste der unterstützten Platzhalterzeichen und Beispiele für die Verwendung von Platzhalterzeichen in include- und exclude-Mustern.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeVerarbeitung von symbolischen Verbindungen und Aliasnamen
  Der Client für Sichern/Archivieren wertet alle Anweisungen exclude.fs und exclude.dir aus und entfernt die ausgeschlossenen Dateibereiche und Verzeichnisse.
- Komprimierungs- und Verschlüsselungsverarbeitung festlegen
  Der Client für Sichern/Archivieren wertet die Option exclude.dir und andere Einschluss-/Ausschlussoptionen, die die Sicherungs- und Archivierungsverarbeitung steuern, aus und legt dann fest, für welche Dateien die Komprimierungs- und Verschlüsselungsverarbeitung ausgeführt wird.
- Dateien in der Einschluss-/Ausschlussliste voranzeigen
  Sie können die Liste der Objekte, die gemäß der Einschluss-/Ausschlussliste gesichert oder archiviert werden sollen, vor dem Senden von Daten an den Server in einer Voranzeige aufrufen.
- Verarbeitung von Einschluss- und Ausschlussoptionen
  Der IBM Spectrum Protect-Server kann Include/Exclude-Optionen mithilfe des Parameters inclexcl in einer Clientoptionsgruppe

definieren.
- Windows-BetriebssystemeVerarbeitungsregeln bei Verwendung von UNC-Namen
  Bei der Verarbeitung von Dateien mit Namen, die der allgemeinen Namenskonvention entsprechen, müssen Regeln eingehalten werden.

Zugehörige Konzepte:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeHinweise für Clients, die für Unicode aktiviert wurden
Auszuschließende Systemdateien
Speicherverwaltungsmaßnahmen
Zugehörige Verweise:
Inclexcl

Einschluss-/Ausschlussoptionen

Dieser Abschnitt enthält kurze Beschreibungen der Optionen include und exclude, die Sie in Ihrer Clientoptionsdatei angeben können, eine minimale Einschluss-/Ausschlussliste für den Ausschluss von Systemdateien, eine Liste der unterstützten Platzhalterzeichen und Beispiele für die Verwendung von Platzhalterzeichen in include- und exclude-Mustern.

- Dateibereiche und Verzeichnisse ausschließen
  Verwenden Sie Anweisungen exclude.dir, um alle Dateien und Unterverzeichnisse im angegebenen Verzeichnis von der Verarbeitung auszuschließen.
- Windows-BetriebssystemeEinschluss-/Ausschlussanweisungen für vernetzte Dateisysteme
  Einschluss-/Ausschlussanweisungen, die vernetzte Dateisysteme (ferne Laufwerke) einbeziehen, müssen im UNC-Format geschrieben werden.
- AIX-BetriebssystemeWindows-BetriebssystemeDateien und Verzeichnisse von einer journalbasierten Sicherung ausschließen
  Es gibt zwei Methoden, Dateien und Verzeichnisse von einer journalbasierten Sicherung auszuschließen.
- Verarbeitung mit Ausschlussanweisungen steuern
  Nachdem der Client alle Ausschlussanweisungen ausgewertet hat, werden die folgenden Optionen mit der Liste der verbleibenden Objekte abgeglichen, die für die Verarbeitung verfügbar sind.
- Auszuschließende Systemdateien
  Einige Systemdateien sollten in die Clientoptionsdatei gestellt werden, sodass sie ausgeschlossen werden.
- Windows-BetriebssystemeDateien ausschließen, deren Namen der allgemeinen Namenskonvention entsprechen
  Sie können Dateien, auf die von fern zugegriffen wird, ausschließen, indem Sie in der Exclude-Anweisung UNC-Namen, d. h. Namen in der allgemeinen Namenskonvention (UNC = Universal Naming Convention) angeben.
- Dateien mit Platzhalterzeichen einschließen und ausschließen
  Sie müssen besondere Escapezeichen verwenden, wenn Sie Dateien und Verzeichnisse einschließen oder ausschließen, deren Namen Platzhalterzeichen enthalten.
- Dateigruppen mit Platzhalterzeichen einschließen und ausschließen
  Sie können Platzhalterzeichen verwenden, um Dateigruppen einzuschließen oder auszuschließen.
- Beispiele für Platzhalterzeichen in Einschluss- und Ausschlussmustern
  Der Client für Sichern/Archivieren akzeptiert die Option exclude.dir, mit der Verzeichniseinträge ausgeschlossen werden können. Die Optionen include und exclude.dir können jedoch nicht gemeinsam verwendet werden.

Dateibereiche und Verzeichnisse ausschließen

Verwenden Sie Anweisungen exclude.dir, um alle Dateien und Unterverzeichnisse im angegebenen Verzeichnis von der Verarbeitung auszuschließen.

Der Client für Sichern/Archivieren wertet *zuerst* alle Anweisungen exclude.dir aus (unabhängig von ihrer Position in der Einschluss-/Ausschlussliste) und entfernt die ausgeschlossenen Verzeichnisse und Dateien aus der Liste der Objekte, die für die Verarbeitung verfügbar sind. Die Anweisungen exclude.dirüberschreiben alle Include-Anweisungen, die mit dem Muster übereinstimmen.

In Tabelle 1 sind die Optionen aufgelistet, die Sie verwenden können, um Dateibereiche und Verzeichnisse von der Verarbeitung auszuschließen.

Tabelle 1. Optionen zum Ausschließen von Dateibereichen und Verzeichnissen

Option	Beschreibung
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme exclude.fs Ausschlussoptionen	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMit dem Muster übereinstimmende Dateibereiche werden ausgeschlossen. Vom Client wird der angegebene Dateibereich bei der Verarbeitung nicht berücksichtigt, und die gewöhnliche Verfallsverarbeitung gelöschter Dateien findet nicht statt. Wenn Sie einen Dateibereich ausschließen, der zuvor eingeschlossen war, bleiben bestehende Sicherungsversionen auf dem Server und unterliegen den Aufbewahrungszeitregeln, die in der zugeordneten Verwaltungsklassendefinition angegeben sind.

Option	Beschreibung

Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme exclude.dir Ausschlussoptionen	Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeSchließt ein Verzeichnis, seine Dateien sowie alle zugehörigen Unterverzeichnisse und ihre Dateien von der Sicherungsverarbeitung aus. Beispiel: Die Anweisung `exclude.dir /test/dan/data1` schließt das Verzeichnis `/test/dan/data1`, dessen Dateien und Unterverzeichnisse sowie die Dateien in den Unterverzeichnissen aus. Die Verwendung der Option exclude.dir ist der Standardoption exclude vorzuziehen, wenn große Verzeichnisse mit vielen Dateien, die Sie nicht sichern wollen, ausgeschlossen werden sollen. Sie können keine Include-Optionen verwenden, um eine Anweisung exclude.dir zu überschreiben. Verwenden Sie exclude.dir nur, wenn Sie einen gesamten Verzeichniszweig ausschließen wollen.
	
	• Verwenden Sie die folgenden Anweisungen, um die Datenträger `/Volumes/disk2` insgesamt von der Sicherungsverarbeitung auszuschließen. Beachten Sie, dass der Datenträger `(/Volumes/disk2)` trotzdem gesichert wird, aber alle anderen Verzeichnisse auf `/Volumes/disk2` ausgeschlossen werden.
	
	`exclude /Volumes/disk2/*`
	`exclude.dir /Volumes/disk2/*`
	
	• Ein Alternativverfahren zum Ausschließen eines vollständigen Datenträgers von der Domänenteilsicherung wäre die Verwendung einer Domänenanweisung, um den Datenträger auszuschließen. Zum Beispiel:
	
	`domain "-/Volumes/disk2"`
	
	Diese Alternative erlaubt dennoch eine selektive Sicherungsverarbeitung von Dateien auf `/Volumes/disk2`.

Option	Beschreibung

Windows-Betriebssysteme exclude.dir Ausschlussoptionen	Windows-BetriebssystemeSchließt ein Verzeichnis, seine Dateien sowie alle zugehörigen Unterverzeichnisse und ihre Dateien von der Sicherungsverarbeitung aus. Beispiel: Die Anweisung `exclude.dir c:\test\dan\data1` schließt das Verzeichnis `c:\test\dan\data1`, dessen Dateien und Unterverzeichnisse sowie die Dateien in den Unterverzeichnissen aus. Die Verwendung der Option exclude.dir ist der Standardoption exclude vorzuziehen, wenn große Verzeichnisse mit vielen Dateien, die Sie nicht sichern wollen, ausgeschlossen werden sollen. Sie können keine Include-Optionen verwenden, um eine Anweisung exclude.dir zu überschreiben. Verwenden Sie exclude.dir nur, wenn Sie einen gesamten Verzeichniszweig ausschließen wollen.
	
	Wenn Sie eine Exclude-Anweisung ohne Laufwerkbuchstaben definieren, beispielsweise `exclude.dir dirname`, wird jedes Verzeichnis mit dem Namen `dirname` auf allen Laufwerken von der Verarbeitung ausgeschlossen.
	
	• Die folgenden Beispiele illustrieren gültige Anweisungen `exclude.dir`:
	Verzeichnis `C:\MyPrograms\Traverse` und seine Dateien und Unterverzeichnisse ausschließen:
	
	`exclude.dir c:\MyPrograms\Traverse`
	
	Alle Verzeichnisse unter `c:\MyPrograms\Traverse` ausschließen. Beachten Sie, dass das Verzeichnis `C:\MyPrograms\Traverse` und die Dateien unmittelbar unter `C:\MyPrograms\Traverse` trotzdem für die Sicherung in Frage kommen.
	
	`exclude.dir c:\MyPrograms\Traverse\*`
	
	Alle Verzeichnisse ausschließen, deren Namen mit `temp` beginnen und die sich innerhalb des Verzeichnisses `x:\documents and settings` und seinen Unterverzeichnissen befinden, wobei *x:* für ein beliebiges Laufwerk steht.
	
	`exclude.dir "*:\Dokumente und Einstellungen\...\temp*"`
	
	Alle Verzeichnisse ausschließen, deren Namen mit `temp` beginnen, unabhängig vom Laufwerk oder Verzeichnis, in dem sie resident sind:
	
	`exclude.dir temp*`
	
	Das folgende Beispiel ist ungültig, weil es mit einem Verzeichnisbegrenzer endet:
	
	`exclude.dir c:\MyPrograms\Traverse\`
	
	• Verwenden Sie die folgenden Anweisungen, um das Laufwerk `x:` insgesamt von der Sicherungsverarbeitung auszuschließen. Beachten Sie, dass das Stammverzeichnis des Laufwerks `(x:\)` trotzdem gesichert wird, aber alle anderen Dateien und Verzeichnisse auf `x:` ausgeschlossen werden.
	
	`exclude x:\*`
	`exclude.dir x:\*`
	
	• Ein Alternativverfahren zum Ausschließen eines vollständigen Laufwerks von der Domänenteilsicherung wäre die Verwendung einer Domänenanweisung, um das Laufwerk auszuschließen. Zum Beispiel:
	
	`domain -x:`
	
	Diese Alternative erlaubt dennoch eine selektive und explizite Teilsicherungsverarbeitung von Dateien auf `x:`. Zum Beispiel:
	
	`dsmc s x:\ -subdir=yes`
	`dsmc i x:`
	`dsmc i x:\MyPrograms\ -subdir=yes`

Windows-Betriebssysteme

Einschluss-/Ausschlussanweisungen für vernetzte Dateisysteme

Einschluss-/Ausschlussanweisungen, die vernetzte Dateisysteme (ferne Laufwerke) einbeziehen, müssen im UNC-Format geschrieben werden.

Im folgenden Beispiel ist `Z:` ein zugeordnetes Laufwerk für ein fernes Dateisystem auf `vista.example.com`.

Das alte Format wäre, `\dir\dir2` auf dem fernen Dateisystem auszuschließen, wie im folgenden Beispiel gezeigt:

```
EXCLUDE.DIR "Z:\dir1\dir2"
```

Hier folgt ein Beispiel des neuen Formats mit UNC:

```
EXCLUDE.DIR "\\vista.example.com\d$\dir1\dir2"
```

Die im alten Format geschriebenen Einschluss-/Ausschlussanweisungen werden vom Client nicht erkannt.

AIX-BetriebssystemeWindows-BetriebssystemeLinux-Betriebssysteme

Dateien und Verzeichnisse von einer journalbasierten Sicherung ausschließen

Es gibt zwei Methoden, Dateien und Verzeichnisse von einer journalbasierten Sicherung auszuschließen.

AIX-BetriebssystemeLinux-Betriebssysteme

- Unter AIX und Linux werden bei der einen Methode der Clientoptionsdatei Exclude-Anweisungen hinzugefügt, um zu verhindern, dass die Dateien oder Verzeichnisse während der Sicherungsverarbeitung gesichert werden.
- Unter AIX und Linux werden bei der anderen Methode Exclude-Anweisungen zur Journalkonfigurationsdatei `tsmjbbd.ini` hinzugefügt, um zu verhindern, dass Journaleinträge für die Dateien oder Verzeichnisse hinzugefügt werden, die sie daran hindern, während einer journalbasierten Sicherung verarbeitet zu werden.

  AIX-BetriebssystemeWenn Sie AIX Version 6.1 oder später ausführen, fügen Sie die Anweisung `exclude .snapshot` zur Datei `tsmjbbd.ini` hinzu, um zu verhindern, dass interne JFS2-Momentaufnahmeverzeichnisse vom Dämon für die journalbasierte Sicherung überwacht werden.

Windows-Betriebssysteme

- Bei der einen Methode werden der Clientoptionsdatei Exclude-Anweisungen hinzugefügt, um zu verhindern, dass die Dateien oder Verzeichnisse während der Sicherungsverarbeitung gesichert werden.
- Bei der anderen Methode werden Exclude-Anweisungen zur Journalkonfigurationsdatei `tsmjbbd.ini` hinzugefügt, um zu verhindern, dass Journaleinträge für die Dateien oder Verzeichnisse hinzugefügt werden, die sie daran hindern, während einer journalbasierten Sicherung verarbeitet zu werden.

Anmerkung: Es besteht keine Korrelation zwischen den beiden Exclude-Anweisungen. Die bevorzugte Position für Exclude-Anweisungen ist die Datei `tsmjbbd.ini`. Dies verhindert, dass sie Eingang in die Journaldatenbank finden und während einer journalbasierten Sicherung verarbeitet werden.

Verarbeitung mit Ausschlussanweisungen steuern

Nachdem der Client alle Ausschlussanweisungen ausgewertet hat, werden die folgenden Optionen mit der Liste der verbleibenden Objekte abgeglichen, die für die Verarbeitung verfügbar sind.

In Tabelle 1 sind die Optionen aufgelistet, die Sie verwenden können, um die Verarbeitung mit Include- und Exclude-Anweisungen zu steuern.

Tabelle 1. Optionen zur Verarbeitungssteuerung mit Include- und Exclude-Anweisungen

Option	Beschreibung	Seite
Sicherungsverarbeitung		
exclude exclude.backup exclude.file exclude.file.backup	*Diese Optionen sind äquivalent.* Mit diesen Optionen können Sie eine Datei oder Dateigruppe von den Sicherungsservices und von den Speicherverwaltungsservices (wenn der HSM-Client installiert ist) ausschließen. Die Option exclude.backup schließt Dateien nur von der normalen Sicherung aus, nicht von HSM.	Ausschlussoptionen
include include.backup include.file	Mit diesen Optionen können Sie Dateien einschließen oder Verwaltungsklassen für die Sicherungsverarbeitung zuordnen.	Einschlussoptionen
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme include.fs	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSteuert, wie der Client Ihren Dateibereich für Teilsicherungen verarbeitet.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Einschlussoptionen
Windows-Betriebssysteme include.fs	Windows-BetriebssystemeMit dieser Option können Optionen auf der Basis Dateibereich nach Dateibereich definiert werden.	Windows-Betriebssysteme Einschlussoptionen
Archivierungsverarbeitung		
exclude.archive	Schließt eine Datei oder Dateigruppe von den Archivierungsservices aus.	Ausschlussoptionen

Option	Beschreibung	Seite
include include.archive	*Diese Optionen sind äquivalent*. Mit diesen Optionen können Dateien eingeschlossen oder Verwaltungsklassen für die Archivierungsverarbeitung zugeordnet werden.	Einschlussoptionen
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme **Imageverarbeitung**		
AIX-BetriebssystemeOracle Solaris-Betriebssysteme exclude.fs.nas	AIX-BetriebssystemeOracle Solaris-BetriebssystemeBei Verwendung im Befehl backup nas werden Dateisysteme auf dem NAS-Dateiserver von der Imagesicherung ausgeschlossen. Wenn Sie keinen NAS-Knotennamen angeben, gilt das angegebene Dateisystem für alle NAS-Dateiserver. Der Befehl backup nas ignoriert alle anderen Exclude-Anweisungen einschließlich der Anweisungen exclude.fs und exclude.dir. Diese Option ist *nur* für AIX- und Solaris-Clients gültig.	AIX-BetriebssystemeOracle Solaris-Betriebssysteme Ausschlussoptionen
Windows-Betriebssysteme exclude.fs.nas	Windows-BetriebssystemeBei Verwendung im Befehl backup nas werden Dateisysteme auf dem NAS-Dateiserver von der Imagesicherung ausgeschlossen. Wenn Sie keinen NAS-Knotennamen angeben, gilt das angegebene Dateisystem für alle NAS-Dateiserver. Der Befehl backup nas ignoriert alle anderen Exclude-Anweisungen einschließlich Anweisungen exclude.dir. Diese Option ist für alle Windows-Clients gültig.	Windows-Betriebssysteme Ausschlussoptionen
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme exclude.image	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSchließt angehängte Dateisysteme und unformatierte logische Datenträger, die dem angegebenen Muster entsprechen, von den Imagegesamtsicherungsoperationen aus. Imageteilsicherungsoperationen sind von exclude.image nicht betroffen. Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig.	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Ausschlussoptionen
Windows-Betriebssysteme exclude.image	Windows-BetriebssystemeSchließt angehängte Dateisysteme und unformatierte logische Datenträger, die dem angegebenen Muster entsprechen, von den Imagegesamtsicherungsoperationen aus. Imageteilsicherungsoperationen sind von exclude.image nicht betroffen. Diese Option ist für alle Windows-Clients gültig.	Windows-Betriebssysteme Ausschlussoptionen
AIX-BetriebssystemeOracle Solaris-Betriebssysteme include.fs.nas	AIX-BetriebssystemeOracle Solaris-BetriebssystemeVerwenden Sie die Option include.fs.nas, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Um anzugeben, ob der Client während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) spichert, verwenden Sie die Option toc mit der Option include.fs.nas in Ihrer Datei dsm.sys. Weitere Informationen finden Sie in Toc. Diese Option ist nur für AIX- und Solaris-Clients gültig.	AIX-BetriebssystemeOracle Solaris-Betriebssysteme Einschlussoptionen
Windows-Betriebssysteme include.fs.nas	Windows-BetriebssystemeVerwenden Sie die Option include.fs.nas, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Um anzugeben, ob der Client während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) speichert, verwenden Sie die Option toc mit der Option include.fs.nas in Ihrer Clientoptionsdatei (dsm.opt). Weitere Informationen finden Sie in Toc. Diese Option ist für alle Windows-Clients gültig.	Windows-Betriebssysteme Einschlussoptionen
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme include.image	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSchließt einen Dateibereich oder einen logischen Datenträger ein, ordnet eine Verwaltungsklasse zu oder ermöglicht es, einem bestimmten logischen Datenträger eine oder mehrere Optionen für die Imagesicherungsverarbeitung zuzuordnen, wenn die Option zusammen mit dem Befehl backup image verwendet wird. Der Befehl backup image ignoriert alle anderen Include-Optionen. Diese Option ist nur für AIX, Solaris, Linux x86_64 und Linux on POWER gültig.	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Einschlussoptionen
Windows-Betriebssysteme include.image	Windows-BetriebssystemeSchließt einen Dateibereich oder einen logischen Datenträger ein, ordnet eine Verwaltungsklasse zu oder ermöglicht es, einem bestimmten logischen Datenträger eine oder mehrere Optionen für die Imagesicherungsverarbeitung zuzuordnen, wenn die Option zusammen mit dem Befehl backup image verwendet wird. Der Befehl backup image ignoriert alle anderen Include-Optionen. Diese Option ist für alle Windows-Clients gültig.	Windows-Betriebssysteme Einschlussoptionen
Windows-Betriebssysteme**Systemstatusverarbeitung**		

Option	Beschreibung	Seite
Windows-Betriebssysteme include.systemstate	Windows-BetriebssystemeOrdnet Verwaltungsklassen für die Sicherung des Windows-Systemstatus zu. Der Standardwert ist, das Systemstatusobjekt an die Standardverwaltungsklasse zu binden.	Windows-Betriebssysteme Einschlussoptionen

Mac OS X-BetriebssystemeWindows-Betriebssysteme

Auszuschließende Systemdateien

Einige Systemdateien sollten in die Clientoptionsdatei gestellt werden, sodass sie ausgeschlossen werden.

Achtung: Diese Systemdateien sind entweder vom Betriebssystem gesperrt oder können beim Zurückschreiben Probleme verursachen. Hierbei handelt es sich um Systemdateien, die nicht wiederhergestellt werden können, ohne das Betriebssystem möglicherweise zu beschädigen, oder um temporäre Dateien mit Daten, die Sie problemlos erneut erstellen können.

Die implizit generierten Anweisungen können in den Ausgabezeilen des Befehls query inclexcl mit der Quelle "Betriebssystem" eingesehen werden.

Windows-BetriebssystemeVerwenden Sie das Beispiel für eine Einschluss-/Ausschlussliste in der Datei dsm.smp als Ausgangspunkt für Ihre Einschluss-/Ausschlussliste. Dies ist die Einschluss-/Ausschlussliste mit den mindestens empfohlenen Angaben. Die Datei dsm.smp befindet sich im Konfigurationsordner (config) im Installationsverzeichnis. Wenn Sie die Standardwerte akzeptiert haben, lautet der Pfad zu dieser Datei `C:\Programme\Tivoli\TSM\config\dsm.smp`.

Windows-BetriebssystemeEinige Exclude-Anweisungen werden aus einer Liste generiert, die das Windows-Betriebssystem in der Windows-Registrierung definiert. Diese implizit generierten Anweisungen können in den Ausgabezeilen des Befehls query inclexcl mit der Quelle "Betriebssystem" eingesehen werden.

Mac OS X-BetriebssystemeDer Client für Sichern/Archivieren fügt der Einschluss-/Ausschlussliste Ihrer Datei dsm.sys die folgenden Ausschlussanweisungen hinzu. Schließen Sie keine dieser Anweisungen in der Datei dsm.sys ein, sonst kommt es zu doppelten Einträgen.

```
EXCLUDE.ARCHIVE "/.../Desktop DB"
EXCLUDE.BACKUP "/.../Desktop DB"
EXCLUDE.ARCHIVE "/.../Desktop DF"
EXCLUDE.BACKUP "/.../Desktop DF"
EXCLUDE.ARCHIVE /.vol
EXCLUDE.BACKUP /.vol
EXCLUDE.ARCHIVE /automount
EXCLUDE.BACKUP /automount
EXCLUDE.ARCHIVE /Network
EXCLUDE.BACKUP /Network
EXCLUDE.ARCHIVE /dev
EXCLUDE.BACKUP /dev
EXCLUDE.BACKUP /.vol/.../*
EXCLUDE.ARCHIVE /.vol/.../*
EXCLUDE.BACKUP /automount/.../*
EXCLUDE.ARCHIVE /automount/.../*
EXCLUDE.BACKUP /Network/.../*
EXCLUDE.ARCHIVE /Network/.../*
EXCLUDE.BACKUP /dev/.../*
EXCLUDE.ARCHIVE /dev/.../*
EXCLUDE.DIR /.vol
EXCLUDE.DIR /automount
EXCLUDE.DIR /Network
EXCLUDE.DIR /dev
```

Mac OS X-BetriebssystemeAnmerkung:

1. Geben Sie keine Datenträger an, deren Name Punkte enthält (...). Der Client für Sichern/Archivieren verwendet die Punktesequenz als Teil der Einschluss-/Ausschlussverarbeitung. Der Client meldet eine ungültige Einschluss-/Ausschlussanweisung zurück, wenn ein Datenträgername eine Punktesequenz enthält. Der Datenträger *muss* umbenannt werden.
2. Objekte mit dem Typ 'rhap' und dem Ersteller 'lcmt' werden von der Verarbeitung ausgeschlossen. Im Allgemeinen sind dies spezielle Dateisystemobjekte, die auch mit dem Befehl mknod erstellt werden können, oder sind UNIX-Mountpunkte. Die Objekte oder Mountpunkte müssen als Teil einer vollständigen Systemzurückschreibung manuell erneut erstellt werden.

Mac OS X-BetriebssystemeIhre Einschluss-/Ausschlussoptionsdatei sollte mindestens die folgende Einschluss-/Ausschlussliste umfassen:

```
EXCLUDE   /.../dsmsched.log
EXCLUDE   /.../dsmprune.log
EXCLUDE   /.../dsmj.log
EXCLUDE   /.../dsmerror.log
EXCLUDE  /.../.hotfiles.bTree

EXCLUDE.DIR  /private/tmp
EXCLUDE.DIR  /private/var/vm
EXCLUDE.DIR  /private/var/tmp
EXCLUDE.DIR  /private/var/db/netinfo/local.nidb
```

```
EXCLUDE.DIR  /.../.Trashes
EXCLUDE.DIR  /.../.Spotlight-*
EXCLUDE.DIR  /.../Library/Caches
EXCLUDE.DIR  /.../.fseventsd
```

Windows-Betriebssysteme

Dateien ausschließen, deren Namen der allgemeinen Namenskonvention entsprechen

Sie können Dateien, auf die von fern zugegriffen wird, ausschließen, indem Sie in der Exclude-Anweisung UNC-Namen, d. h. Namen in der allgemeinen Namenskonvention (UNC = Universal Naming Convention) angeben.

Bei dem folgenden Beispiel wird angenommen, dass der lokale Laufwerkbuchstabe `g` dem folgenden fernen Freigabepunkt zugeordnet ist:

```
\\remote\books
```

Alle Dateien im Stammverzeichnis dieses Freigabepunkts, deren Erweiterung `.txt` lautet, sollen von der Sicherung ausgeschlossen werden. Hierfür kann einer der beiden folgenden Befehle verwendet werden:

```
exclude g:\*.txt
exclude \\remote\books\*.txt
```

Für Laufwerke mit Wechseldatenträgern, z. B. DVD-, Zip- oder Diskettenlaufwerke, können keine UNC-Namen angegeben werden. Der folgende Befehl ist beispielsweise *nicht gültig*:

```
exclude \\ocean\a$\winnt\system32\...\*
```

Dateien mit Platzhalterzeichen einschließen und ausschließen

Sie müssen besondere Escapezeichen verwenden, wenn Sie Dateien und Verzeichnisse einschließen oder ausschließen, deren Namen Platzhalterzeichen enthalten.

Der Client für Sichern/Archivieren behandelt Platzhalterzeichen auf verschiedenen Plattformen unterschiedlich.

Die Namen von Verzeichnissen und Dateien können verschiedene Symbole enthalten. Welche Typen von Symbolen zulässig sind, ist vom Betriebssystem abhängig.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeUnter AIX können die Namen von Verzeichnissen oder Dateien beispielsweise die folgenden Symbole enthalten:

```
* ? : [ ]
```

Windows-BetriebssystemeUnter Windows können die Namen von Verzeichnissen und Dateien nicht die folgenden Symbole enthalten:

```
? * < > " / \ : |
```

Windows-BetriebssystemeSie können jedoch die folgenden Symbole enthalten:

```
[ ]
```

Bei der Angabe von Dateien und Verzeichnissen in Include- und Exclude-Anweisungen müssen Sie das Escapezeichen "`\`" verwenden, um die Platzhalterzeichen anzugeben. Das Escapezeichen kann jedoch nur innerhalb der Zeichenklassen "`[]`" verwendet werden.

Die folgenden Beispiele zeigen, wie Dateien und Verzeichnisse, deren Namen Platzhalterzeichen enthalten, in Include/Exclude-Anweisungen mit dem Escapezeichen und Zeichenklassen anzugeben sind.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeZum Ausschließen des einzelnen Verzeichnisses /usr1/[dir2] von der Sicherungsverarbeitung geben Sie Folgendes in die Datei dsm.sys oder in die Einschluss-/Ausschlussdatei ein:

```
exclude.dir "/usr1/[\[]dir2[\]]"
```

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeZum Ausschließen der einzelnen Datei /usr1/fi*le1 von der Sicherungsverarbeitung geben Sie die folgende Anweisung in die Datei dsm.sys oder in die Einschluss-/Ausschlussdatei ein:

```
exclude "/usr1/fi[\*]le1"
```

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeTipp: Wenn Sie den Profileditor verwenden, um eine einzelne Datei oder ein einzelnes Verzeichnis einzuschließen, deren bzw. dessen Name Platzhalterzeichen enthält, müssen Sie die Include- oder Exclude-Anweisung manuell editieren, um das Escapezeichen für das Platzhalterzeichen einzufügen. Der Profileditor fügt

nicht automatisch Escapezeichen für Platzhalterzeichen ein. Orientieren Sie sich beim Editieren der Include- oder Exclude-Anweisungen in der Datei dsm.sys oder in der Einschluss-/Ausschlussdatei an den obigen Beispielen.
Zum Ausschließen des einzelnen Verzeichnisses `C:\[dir2]` von der Sicherungsverarbeitung geben Sie Folgendes in die Datei dsm.opt ein:

```
exclude.dir "C:\[\[]dir2[\]]"
```

Zum Ausschließen der einzelnen Datei `C:\file[.txt` von der Sicherungsverarbeitung geben Sie Folgendes in die Datei dsm.opt ein:

```
exclude.dir "C:\file[\[].txt"
```

Tipp: Wenn Sie den Profileditor verwenden, um eine einzelne Datei oder ein einzelnes Verzeichnis einzuschließen, deren bzw. dessen Name Platzhalterzeichen enthält, müssen Sie die Include- oder Exclude-Anweisung manuell editieren, um das Escapezeichen für das Platzhalterzeichen einzufügen. Der Profileditor fügt nicht automatisch Escapezeichen für Platzhalterzeichen ein. Orientieren Sie sich beim Editieren der Include- oder Exclude-Anweisungen in der Datei dsm.opt oder in der Einschluss-/Ausschlussdatei an den obigen Beispielen.
Zugehörige Konzepte:
Platzhalterzeichen

Dateigruppen mit Platzhalterzeichen einschließen und ausschließen

Sie können Platzhalterzeichen verwenden, um Dateigruppen einzuschließen oder auszuschließen.

Verwenden Sie die Platzhalterzeichen, die in der folgenden Tabelle aufgelistet sind, um Dateigruppen anzugeben, die Sie einschließen oder ausschließen wollen. Diese Tabelle gilt *nur* für Anweisungen include und exclude.

Eine sehr große Einschluss-/Ausschlussliste kann die Leistung bei der Sicherung beeinträchtigen. Verwenden Sie Platzhalterzeichen, um unnötige Include-Anweisungen zu vermeiden und den Umfang der Liste zu verringern.

Tabelle 1. Platzhalterzeichen und andere Sonderzeichen

Zeichen	Funktion
?	Das Platzhalterzeichen für ein Zeichen entspricht einem beliebigen Einzelzeichen, *mit Ausnahme* des Verzeichnistrennzeichens. Es entspricht nicht dem Ende der Zeichenfolge. Zum Beispiel: • Das **Muster** ab? **entspricht** abc, aber **entspricht nicht** ab, abab oder abzzz. • Das **Muster** ab?rs **entspricht** abfrs, aber **entspricht nicht** abrs oder abllrs. • Das **Muster** ab?ef?rs **entspricht** abdefjrs, aber **entspricht nicht** abefrs, abdefrs oder abefjrs. • Das **Muster** ab??rs **entspricht** abcdrs oder abzzrs, aber **entspricht nicht** abrs, abjrs oder abkkkrs.
*****	Das Platzhalterzeichen für alle Zeichen. Zum Beispiel: • Das **Muster** ab* **entspricht** ab, abb oder abxxx, aber **entspricht nicht** a, b, aa, bb. • Das **Muster** ab*rs **entspricht** abrs, abtrs oder abrsrs, aber **entspricht nicht** ars, aabrs oder abrss. • Das **Muster** ab*ef*rs **entspricht** abefrs oder abefghrs, aber **entspricht nicht** abefr, abers. • Das **Muster** abcd.* **entspricht** abcd.c oder abcd.txt, aber **entspricht nicht** abcd, abcdc oder abcdtxt.

Windows-Betriebssysteme **\...**	Das Platzhalterzeichen für n Zeichen entspricht null oder mehr Verzeichnissen.
	Das folgende Muster gibt alle Dateien im Stammverzeichnis des Laufwerks C an:
	`c:\*`
	Das folgende Muster gibt alle Dateien und alle Verzeichnisse auf dem Laufwerk C an:
	`c:\...\*`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme **/...**	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDas Platzhalterzeichen für n Zeichen entspricht null oder mehr Verzeichnissen.
[	Mit dem Anfangszeichen für die Zeichenklasse wird die Aufzählung einer Zeichenklasse begonnen. Beispiel: `xxx[abc] entspricht xxxa, xxxb oder xxxc.`

Zeichen	Funktion
–	Das Zeichen für den Zeichenklassenbereich umfasst die Zeichen vom ersten angegebenen Zeichen bis zum letzten angegebenen Zeichen. Beispiel: `xxx[a-z] entspricht xxxa, xxxb, xxxc, ... xxxz.` Windows-BetriebssystemeDieses Format sollte nicht für die Angabe ferner Laufwerke in einer ***exclude***-Anweisung verwendet werden.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme ****	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeDas Literal-Escapezeichen. Wird das Literal-Escapezeichen in einer Zeichenklasse verwendet, wird das nächste Zeichen wörtlich behandelt. Außerhalb einer Zeichenklasse wird es nicht auf diese Weise behandelt. Soll beispielsweise ']' in eine Zeichenklasse eingeschlossen werden, ist [...\]...] einzugeben. Das Escapezeichen löscht die normale Bedeutung von ']' als Zeichen zum Schließen der Zeichenklasse.
]	Mit dem Endzeichen für die Zeichenklasse wird die Aufzählung einer Zeichenklasse beendet.
Windows-Betriebssysteme **:**	Windows-BetriebssystemeDas Laufwerktrennzeichen trennt eine Dateispezifikation. Die Zeichen *vor* dem Doppelpunkt geben einen Laufwerkbuchstaben an. Die Zeichen *hinter* dem Doppelpunkt geben eine Dateispezifikation oder ein Dateimuster an. Beispiel: `d:\direct\file.nam`

Windows-BetriebssystemeAnmerkung: Da eine Laufwerkspezifikation nur aus einem einzelnen Buchstaben bestehen darf, sollten Sie nicht mehrere Platzhalterzeichen oder eine Kombination aus einem Platzhalterzeichen und einem Buchstaben verwenden, um eine Laufwerkspezifikation anzugeben. Die folgenden Muster sind nicht zulässig. Werden sie in der Clientoptionsdatei (dsm.opt) angegeben, bewirken sie, dass das Clientprogramm sofort nach dem Start gestoppt wird:
Windows-Betriebssysteme

- ?*:\test.txt
- *?:\...\pagefile.sys
- H*:\test.*
- *H:\test.txt
- myvolume*:\
- myvolume?*:\

Windows-BetriebssystemeWenn Sie UNC-Namen verwenden, zeigt Tabelle 2, wie gemeinsame Laufwerke richtig angegeben werden.

Tabelle 2. Laufwerkspezifikation mit Platzhalterzeichen angeben

Falsch	Richtig
\\remote*:\...*.*	\\remote*$\...*.*
\\remote\?:\...*.*	\\remote\?$\...*.*
\\remote*:\...\pagefile.sys	\\remote*$\...\pagefile.sys

Zugehörige Konzepte:
Platzhalterzeichen

Beispiele für Platzhalterzeichen in Einschluss- und Ausschlussmustern

Der Client für Sichern/Archivieren akzeptiert die Option exclude.dir, mit der Verzeichniseinträge ausgeschlossen werden können. Die Optionen include und exclude.dir können jedoch nicht gemeinsam verwendet werden.

Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Anmerkung: In der Datei dsm.sys funktionieren die Optionen include und exclude nicht mit symbolischen Verbindungen auf Verzeichnisse. Beispiel: Verwenden Sie in Ihren Include- oder Exclude-Anweisungen nicht `/u`, da `/u` eine symbolische Verbindung für das Verzeichnis `/home` darstellt. Anstelle von:

```
include /u/tmp/save.fil
```

Folgendes eingeben:

```
include /home/tmp/save.fil
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDie Option exclude funktioniert jedoch mit symbolischen Verbindungen zu Verzeichnissen, wenn Sie einen Sicherungsbefehl mit dem absoluten Pfad eingeben, der die

symbolische Verbindung enthält.

Tabelle 1 zeigt die Verwendung von Platzhalterzeichen zum Einschließen oder Ausschließen von Dateien.

Tabelle 1. Platzhalterzeichen in Include- und Exclude-Mustern verwenden

Task	Muster

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien ausschließen, die mit `.doc` enden, mit Ausnahme der Dateien im Verzeichnis `Documents` im Ausgangsverzeichnis von aleko.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme
	`EXCLUDE /.../*.doc`
	`INCLUDE "/home/aleko/Documents/ *.doc"`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien mit der Erweiterung *bak* während der Sicherung ausschließen, mit Ausnahme der Dateien, die sich im Dateisystem /usr im Verzeichnis `dev` befinden.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme
	`exclude /.../*.bak`
	`include /usr/dev/*.bak`

Windows-BetriebssystemeAlle Dateien mit der Erweiterung *bak* während der Sicherung ausschließen, mit Ausnahme der Dateien, die sich in Laufwerk `d:` im Verzeichnis `dev` befinden.	Windows-Betriebssysteme
	`exclude ?:\*.bak`
	`include d:\dev\*.bak`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien und Ordner unter allen vorhandenen Ordnern `Documents` ausschließen; die Datei `Current` des Benutzers `aleko` soll hiervon *ausgenommen* werden.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme
	`EXCLUDE /.../Documents/.../*`
	`INCLUDE "/home/aleko/Documents/ Current"`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien in allen Verzeichnissen mit dem Namen "tmp" und ihren Unterverzeichnissen ausschließen; die Datei `/home/tmp/save.fil` soll hiervon *ausgenommen* werden.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme
	`exclude /.../tmp/.../*`
	`include /home/tmp/save.fil`

Windows-BetriebssystemeAlle Dateien in allen Verzeichnissen mit dem Namen "tmp" und ihren Unterverzeichnissen ausschließen; die Datei `d:\tmp\save.fil` soll hiervon *ausgenommen* werden.	Windows-Betriebssysteme
	`exclude ?:\...\tmp\...\*`
	`include d:\tmp\save.fil`

Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien mit der Erweiterung `.cpp` in allen Verzeichnissen auf den Datenträgern `Vol1`, `Vol2`, `Vol3` und `Vol4` ausschließen.	Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `EXCLUDE /Volumes/Vol[1-4]/.../*.cpp`
Mac OS X-BetriebssystemeAlle Dateien mit der Erweiterung `.cpp` in allen Verzeichnissen auf den Datenträgern `Vol1`, `Vol2`, `Vol3` und `Vol4` ausschließen.	Mac OS X-Betriebssysteme `EXCLUDE /Volumes/Vol[1-4]/.../*.cpp`
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien mit der Erweiterung `.cpp` in allen Verzeichnissen in den Dateisystemen `/fs1`, `/fs2`, `/fs3` und `/fs4` ausschließen.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `EXCLUDE /fs[1-4]/.../*.cpp`
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDie Dateien mit der Erweiterung `.cpp` im Verzeichnis `/fs2/source` ausschließen.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `EXCLUDE /fs2/source/*.cpp`
Windows-BetriebssystemeAlle Dateien mit der Erweiterung `.obj` in allen Verzeichnissen der Laufwerke `c:`, `e:`, `f:` und `g:` von der Sicherung ausschließen.	Windows-Betriebssysteme `exclude [ce-g]:\...\*.obj` Die Laufwerke `c:`, `e:`, `f:` und `g:` sind lokale Laufwerke oder Wechsellaufwerke.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien mit der Erweiterung `.o` in allen Verzeichnissen in den Dateisystemen `/usr1`, `/usr2` und `/usr3` ausschließen.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `exclude /usr[1-3]/.../*.o`
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme*Nur* die Dateien mit der Erweiterung `.o` ausschließen, die sich im Stammverzeichnis des Dateisystems `usr2` befinden.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `exclude /usr2/*.o`

Task	Muster
Windows-Betriebssysteme*Nur* die Dateien mit der Erweiterung `.obj` ausschließen, die sich im Stammverzeichnis des Laufwerks `d:` befinden.	Windows-Betriebssysteme `exclude d:\*.obj`
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien ausschließen, die sich unter dem Verzeichnis `tmp` in einem beliebigen Dateisystem befinden.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `exclude /.../tmp/.../*`
Windows-BetriebssystemeAlle Dateien ausschließen, die sich unter dem Verzeichnis `tmp` in einem beliebigen Laufwerk befinden.	Windows-Betriebssysteme `exclude ?:\tmp\...\*`
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDie vollständige Verzeichnisstruktur `/var/spool` von der gesamten Verarbeitung ausschließen.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `exclude.dir /var/spool`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeEin einzelnes Dateisystem von der Sicherungsverarbeitung ausschließen.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme
	`exclude.fs /fs1`
	`exclude.fs home:`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateisysteme von der Sicherungsverarbeitung ausschließen, die an einer beliebigen Position in der Verzeichnisbaumstruktur `/test/myfs/fs01` und `/test/myfs/fs02` angehängt sind.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme
	`exclude.fs /test/myfs/fs01/.../*`
	`exclude.fs /test/myfs/fs02/*`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDas Verzeichnis `/home/mydir/test1` und alle Dateien und Unterverzeichnisse unter diesem Verzeichnis ausschließen.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `exclude.dir /home/mydir/test1`
Windows-BetriebssystemeDas Verzeichnis `c:\mydir\test1` und alle Dateien und Unterverzeichnisse unter diesem Verzeichnis ausschließen.	Windows-Betriebssysteme `exclude.dir c:\mydir\test1`
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Verzeichnisse unter dem Verzeichnis `/home/mydir` ausschließen, deren Name mit `test` beginnt.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `exclude.dir /home/mydir/test*`
Windows-BetriebssystemeAlle Verzeichnisse unter dem Verzeichnis `\mydir` ausschließen, deren Name mit `test` beginnt.	Windows-Betriebssysteme `exclude.dir c:\mydir\test*`
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeIn allen Dateisystemen alle Verzeichnisse direkt unter dem Verzeichnis `/mydir` ausschließen, deren Name mit `test` beginnt.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme `exclude.dir /.../mydir/test*`
Windows-BetriebssystemeIn allen Laufwerken alle Verzeichnisse direkt unter dem Verzeichnis `\mydir` ausschließen, deren Name mit `test` beginnt.	Windows-Betriebssysteme `exclude.dir ?:\mydir\test*`
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDen unformatierten logischen Datenträger von der Imagesicherung ausschließen.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme `exclude.image /dev/hd0`
Windows-BetriebssystemeDen unformatierten logischen Datenträger von der Imagesicherung ausschließen.	Windows-Betriebssysteme `exclude.image c:\*`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-BetriebssystemeAlle symbolischen Verbindungen oder Aliasnamen (Aliasnamen gelten für Mac OS X) von der Sicherungsverarbeitung ausschließen, außer dem Verzeichnis `Docs` für `user1`.	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-Betriebssysteme
	`EXCLUDE.ATTRIBUTE.SYMLINK /.../*`
	`INCLUDE.ATTRIBUTE.SYMLINK /Users/ user1/Docs/*`

Windows-BetriebssystemeAlle Verzeichnisse und Dateien auf den lokalen Laufwerken, ausgenommen Laufwerk **c:**, ausschließen.	Windows-Betriebssysteme
	`exclude [abd-z]:\...\*`
	`exclude.dir [abd-z]:\...\*`

Zugehörige Konzepte:
Beispiele für Platzhalterzeichen in Einschluss- und Ausschlussmustern
Zugehörige Verweise:
Ausschlussoptionen
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Verarbeitung von symbolischen Verbindungen und Aliasnamen

Der Client für Sichern/Archivieren wertet alle Anweisungen exclude.fs und exclude.dir aus und entfernt die ausgeschlossenen Dateibereiche und Verzeichnisse.

Nach diesem ersten Auswertungsschritt wertet der Client alle Einschluss-/Ausschlussanweisungen für die Steuerung der Verarbeitung von symbolischen Verbindungen und Aliasnamen (exclude.attribute.symlink und include.attribute.symlink) aus und gleicht sie mit der verbleibenden Liste der Objekte ab, die für die Verarbeitung verfügbar sind.

Die Verarbeitung von Aliasnamen gilt für Mac OS X.

Tabelle 1 definiert Optionen für die Steuerung der Verarbeitung von symbolischen Verbindungen und Aliasnamen.

Tabelle 1. Optionen für das Steuern der Verarbeitung von symbolischen Verbindungen und Aliasnamen

Option	Beschreibung	Seite
exclude.attribute.symlink	Schließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt, nur von der Sicherungsverarbeitung aus.	Ausschlussoptionen
include.attribute.symlink	Schließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt, innerhalb einer größeren Gruppe von ausgeschlossenen Dateien nur für die Sicherungsverarbeitung ein.	Einschlussoptionen

Komprimierungs- und Verschlüsselungsverarbeitung festlegen

Der Client für Sichern/Archivieren wertet die Option exclude.dir und andere Einschluss-/Ausschlussoptionen, die die Sicherungs- und Archivierungsverarbeitung steuern, aus und legt dann fest, für welche Dateien die Komprimierungs- und Verschlüsselungsverarbeitung ausgeführt wird.

Die folgenden Optionen bestimmen, für welche Dateien die Komprimierungs- und Verschlüsselungsverarbeitung ausgeführt wird.

Windows-Betriebssysteme

Tabelle 1. Optionen für die Steuerung der Komprimierungs- und Verschlüsselungsverarbeitung

Option	Beschreibung	Seite
Komprimierungsverarbeitung		
exclude.compression	Schließt Dateien von der Komprimierungsverarbeitung aus, wenn compression=*yes* angegeben ist. Diese Option gilt für Sicherungen und Archivierungen.	Ausschlussoptionen
include.compression	Schließt Dateien für die Komprimierungsverarbeitung ein, wenn compression=*yes* angegeben ist. Diese Option gilt für Sicherungen und Archivierungen.	Einschlussoptionen
Verschlüsselungsverarbeitung		
exclude.encrypt	Schließt Dateien von der Verschlüsselungsverarbeitung aus.	Ausschlussoptionen
include.encrypt	Schließt Dateien für die Verschlüsselungsverarbeitung ein. Die Daten, die Sie einschließen, werden in verschlüsselter Form gespeichert; die Verschlüsselung hat keine Auswirkungen auf das gesendete oder empfangene Datenvolumen. **Wichtig:** Die Option include.encrypt ist die einzige Möglichkeit, die Verschlüsselung auf dem Client für Sichern/Archivieren zu aktivieren. Werden keine Anweisungen include.encrypt verwendet, findet keine Verschlüsselung statt.	Einschlussoptionen

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Tabelle 2. Optionen für die Steuerung der Komprimierung und Verschlüsselung

Option	Beschreibung	Seite
Komprimierungsverarbeitung		
exclude.compression	Schließt Dateien von der Komprimierungsverarbeitung aus, wenn compression=*yes* angegeben ist. Diese Option gilt für Sicherungen und Archivierungen.	Ausschlussoptionen
include.compression	Schließt Dateien für die Komprimierungsverarbeitung ein, wenn compression=*yes* angegeben ist. Diese Option gilt für Sicherungen und Archivierungen.	Einschlussoptionen
Verschlüsselungsverarbeitung		
exclude.encrypt	Schließt Dateien von der Verschlüsselungsverarbeitung aus.	Ausschlussoptionen
include.encrypt	Schließt Dateien für die Verschlüsselungsverarbeitung ein. Die Daten, die Sie einschließen, werden in verschlüsselter Form gespeichert; die Verschlüsselung hat keine Auswirkungen auf das gesendete oder empfangene Datenvolumen. **Wichtig:** Die Option include.encrypt ist die einzige Möglichkeit, die Verschlüsselung auf dem Client für Sichern/Archivieren zu aktivieren. Werden keine Anweisungen include.encrypt verwendet, findet keine Verschlüsselung statt.	Einschlussoptionen

Dateien in der Einschluss-/Ausschlussliste voranzeigen

Sie können die Liste der Objekte, die gemäß der Einschluss-/Ausschlussliste gesichert oder archiviert werden sollen, vor dem Senden von Daten an den Server in einer Voranzeige aufrufen.

Die Verzeichnisstruktur in der GUI des Clients für Sichern/Archivieren zeigt detaillierte Informationen zu eingeschlossenen und ausgeschlossenen Objekten an. In den Verzeichnisstrukturfenstern der GUI des Clients für Sichern/Archivieren können Sie Dateien und Verzeichnisse auswählen, die eingeschlossen oder ausgeschlossen werden sollen. Sie sollten diesen Befehl preview verwenden, um sicherzustellen, dass Sie die richtigen Dateien einschließen und ausschließen. Im Folgenden wird ein Beispielszenario für die Verwendung der Funktion 'Voranzeige für Einschluss/Ausschluss' aufgeführt.

Beispiel: Führen Sie die folgenden Schritte aus, um die Dateien in Ihrem Dateibereich `/Users/home` zu sichern:

1. Starten Sie die GUI des Clients für Sichern/Archivieren und öffnen Sie die Baumstruktur für Sichern. Sie können alle Verzeichnisse und Dateien sehen, die von Ihrer Optionsdatei und anderen Quellen ausgeschlossen wurden.
2. Blättern Sie in der Baumstruktur abwärts. Sie stellen fest, dass alle `*.o`-Dateien in `/Volumes/home/mary/myobjdir` gesichert werden.
3. Sie wollen die `*.o`-Dateien nicht sichern. Also klicken Sie mit der rechten Maustaste auf eine `.o`-Datei und wählen "Dateiinformationen anzeigen" im Popup-Menü aus.
4. Der Dialog zeigt an, dass diese Dateien eingeschlossen sind. Daher klicken Sie auf die Schaltfläche "Erweitert" und erstellen eine Regel, um alle `.o`-Dateien im Dateibereich `DATA:\home` auszuschließen.
5. Am Ende Ihrer Optionsdatei wird eine Regel erstellt. Das aktuelle Verzeichnis wird in der Baumstruktur für Sichern aktualisiert und die Dateien `.o` werden mit einem roten `'X'` markiert; dies gibt an, dass die Dateien ausgeschlossen sind.
6. Wenn Sie andere Verzeichnisse ansehen, zeigen diese die von Ihnen hinzugefügten neuen Ausschließungen. Klicken Sie auf "Sichern" und sichern Sie die Dateien in Ihrem Dateibereich `/home`.

Zugehörige Verweise:
Preview Archive
Preview Backup

Verarbeitung von Einschluss- und Ausschlussoptionen

Der IBM Spectrum Protect-Server kann Include/Exclude-Optionen mithilfe des Parameters inclexcl in einer Clientoptionsgruppe definieren.

Die vom Server angegebenen Include/Exclude-Anweisungen werden zusammen mit den Include/Exclude-Anweisungen in der Clientoptionsdatei ausgewertet. Die Server-Include-Exclude-Anweisungen werden immer erzwungen und an das Ende der Einschluss-/Ausschlussliste gestellt und somit vor den Client-Include-Exclude-Anweisungen ausgewertet.

 Windows-BetriebssystemeWenn die Einschluss-/Ausschlussliste in der Clientoptionsdatei eine oder mehrere Optionen inclexcl enthält, die Einschluss-/Ausschlussdateien angeben, werden die Include/Exclude-Anweisungen in diesen Dateien an der Position in die Liste eingefügt, an der sich die zugehörige Option inclexcl befindet, und entsprechend verarbeitet.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWenn die Einschluss-/Ausschlussliste in der Datei dsm.sys eine oder mehrere Optionen inclexcl enthält, die Einschluss-/Ausschlussdateien angeben, werden die Include/Exclude-Anweisungen in diesen Dateien an der Position in die Liste eingefügt, an der sich die zugehörige Option inclexcl befindet, und entsprechend verarbeitet.

Eine sehr große Einschluss-/Ausschlussliste kann die Leistung bei der Sicherung beeinträchtigen. Verwenden Sie Platzhalterzeichen, um unnötige Include-Anweisungen zu vermeiden und den Umfang der Liste zu verringern.

Windows-BetriebssystemeBei einer Teilsicherung wertet der Client zuerst alle Anweisungen exclude.dir aus und entfernt die ausgeschlossenen Verzeichnisse und Dateien aus der Liste der Objekte, die für die Verarbeitung verfügbar sind.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBei einer Teilsicherung wertet der Client zuerst alle Anweisungen exclude.fs und exclude.dir aus und entfernt die ausgeschlossenen Dateibereiche, Verzeichnisse und Dateien aus der Liste der Objekte, die für die Verarbeitung verfügbar sind.

Windows-BetriebssystemeNach der Auswertung aller Anweisungen exclude.dir wertet der Client die Einschluss-/Ausschlussliste von unten nach oben aus und stoppt, wenn eine Einschluss- oder Ausschlussanweisung gefunden wird, die mit der Datei übereinstimmt, die gerade verarbeitet wird. Die Reihenfolge, in der die Einschluss- und Ausschlussoptionen eingegeben werden, hat daher Einfluss darauf, welche Dateien eingeschlossen und welche Dateien ausgeschlossen werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeNach der Auswertung aller Anweisungen exclude.fs und exclude.dir wertet der Client die Einschluss-/Ausschlussanweisungen zur Steuerung der Verarbeitung symbolischer Verbindungen oder Aliasnamen (exclude.attribute.symlink und include.attribute.symlink) von unten nach oben aus und stoppt, wenn eine Einschluss-/Ausschlussanweisung gefunden wird, die mit der Datei übereinstimmt, die gerade verarbeitet wird. Nach der Verarbeitung der Einschluss-/Ausschlussanweisungen zur Steuerung der Verarbeitung symbolischer Verbindungen oder Aliasnamen wertet der Client die verbleibende Einschluss-/Ausschlussliste von unten nach oben aus und stoppt, wenn eine Einschluss- oder Ausschlussanweisung gefunden wird, die mit der Datei übereinstimmt, die gerade verarbeitet wird. Die Reihenfolge, in der die Einschluss- und Ausschlussoptionen eingegeben werden, hat daher Einfluss darauf, welche Dateien eingeschlossen und welche Dateien ausgeschlossen werden.

Zum Anzeigen einer Liste, in der alle auf der Client-Workstation aktiven Include/Exclude-Anweisungen in der tatsächlichen Reihenfolge aufgeführt sind, in der sie verarbeitet werden, den Befehl query inclexcl verwenden.

Das Clientprogramm verarbeitet die Liste der Include/Exclude-Anweisungen anhand folgender Regeln:

1. Dateien werden überprüft; Verzeichnisse werden nur überprüft, wenn die Option exclude.dir angegeben ist.
2. Dateinamen werden von unten nach oben mit den Mustern in der Einschluss-/Ausschlussliste abgeglichen. Wird eine Übereinstimmung gefunden, stoppt die Verarbeitung, und es wird überprüft, ob die Option include oder exclude lautet. Lautet die Option include, wird die Datei gesichert. Lautet die Option exclude, wird die Datei nicht gesichert.
   Anmerkung: Wird keine Übereinstimmung gefunden, werden die Dateien implizit eingeschlossen und gesichert.
3. Wird eine Datei gesichert, wird sie an die Standardverwaltungsklasse gebunden, sofern sie nicht mit einer Anweisung include übereinstimmt, die einen anderen Verwaltungsklassennamen angegeben hat; in letzterem Fall wird sie an die angegebene Verwaltungsklasse gebunden.

Die folgenden Beispiele veranschaulichen die Verarbeitung von unten nach oben. Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme

Beispiel 1

Nehmen wir an, `La Pomme` ist nicht der Startdatenträger.

```
EXCLUDE /.../*.cpp
INCLUDE "/Volumes/La Pomme/Foo/.../*.cpp"
EXCLUDE "/Volumes/La Pomme/Foo/Junk/*.cpp"
```

Folgende Datei wird gerade verarbeitet: `/Volumes/La Pomme/Foo/Dev/test.cpp`. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 (die letzte definierte Anweisung include oder exclude) wird aufgrund der Verarbeitung von unten nach oben zuerst überprüft. Das Muster `/Volumes/La Pomme/Foo/Junk/*.cpp` stimmt nicht mit dem Namen der Datei überein, die gerade verarbeitet wird.
2. Die Verarbeitung und Überprüfung werden bei Regel 2 fortgesetzt. Dieses Mal stimmt das Muster `/Volumes/La Pomme/Foo/.../*.cpp` mit dem Namen der Datei überein, die gerade verarbeitet wird. Die Verarbeitung stoppt, die Option wird überprüft und das Objekt wird eingeschlossen.
3. Datei `/Volumes/La Pomme/Foo/Dev/test.cpp` wird gesichert.

Beispiel 2

Nehmen wir an, `La Pomme` ist nicht der Startdatenträger.

```
EXCLUDE /.../*.cpp
INCLUDE "/Volumes/La Pomme/Foo/.../*.cpp"
EXCLUDE "/Volumes/La Pomme/Foo/Junk/*.cpp"
```

Folgende Datei wird gerade verarbeitet: `/Volumes/La Pomme/Widget/Sample File`. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
2. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 1 wird überprüft, ohne eine Übereinstimmung zu finden.
4. Da keine Übereinstimmung gefunden wurde, wird `Volumes/La Pomme/Widget/Sample File` implizit eingeschlossen und gesichert.

Beispiel 3

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude *.o
   include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

Folgende Datei wird gerade verarbeitet: `/home/foo/dev/test.o`. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 (die letzte definierte Anweisung) wird wegen der Verarbeitung von unten nach oben zuerst überprüft. Das Muster `/home/foo/junk/*.o` stimmt nicht mit dem Namen der Datei überein, die gerade verarbeitet wird.
2. Die Verarbeitung und Überprüfung werden bei Regel 2 fortgesetzt. Dieses Mal stimmt das Muster `/home/foo/.../*.o` mit dem Namen der Datei überein, die gerade verarbeitet wird. Die Verarbeitung stoppt, die Option wird überprüft und lautet include.
3. Die Datei `/home/foo/dev/test.o` wird gesichert.

Beispiel 4

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude *.obj
   include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

Folgende Datei wird gerade verarbeitet: `/home/widg/copyit.txt` . Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
2. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 1 wird überprüft, ohne eine Übereinstimmung zu finden.
4. Da keine Übereinstimmung gefunden wurde, wird die Datei `/home/widg/copyit.txt` implizit eingeschlossen und gesichert.

Beispiel 5

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude /.../*.o
   include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

Zurzeit wird die folgende Datei verarbeitet: `/home/lib/objs/printf.o`. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
2. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 1 wird überprüft, und es wird eine Übereinstimmung gefunden.
4. Die Verarbeitung stoppt, die Option wird überprüft und das Objekt wird ausgeschlossen.
5. Die Datei `/home/lib/objs/printf.o` wird nicht gesichert.

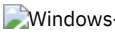
Beispiel 6

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude.attribute.symlink /.../*
exclude /.../*.o
   include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

Zurzeit wird die folgende Datei verarbeitet: /home/lib/objs/printf.o. Folgende Verarbeitungsschritte werden durchgeführt:

1. Die Anweisung exclude.attribute.symlink wird zuerst überprüft. Ist die Datei printf.o eine symbolische Verbindung, wird sie ausgeschlossen, andernfalls wird mit dem nächsten Schritt fortgefahren. Bitte beachten Sie, dass die Anweisungen exclude.attribute.symlink immer vor den anderen Include/Exclude-Anweisungen verarbeitet werden, unabhängig von Ihrer Position in der Einschluss-/Ausschlussliste.
2. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
4. Regel 1 wird überprüft, und es wird eine Übereinstimmung gefunden.
5. Die Verarbeitung stoppt, die Option wird überprüft und das Objekt wird ausgeschlossen.
6. Datei /home/lib/objs/printf.o wird nicht gesichert.


Windows-Betriebssysteme

Beispiel 1

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude ?:\*.obj
include c:\foo\...\*.obj
exclude c:\foo\junk\*.obj
```

Folgende Datei wird gerade verarbeitet: `c:\foo\dev\test.obj`. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 (die letzte definierte Anweisung) wird wegen der Verarbeitung von unten nach oben zuerst überprüft. Das Muster `c:\foo\junk\*.obj` stimmt nicht mit dem Namen der Datei überein, die gerade verarbeitet wird.
2. Die Verarbeitung und Überprüfung werden bei Regel 2 fortgesetzt. Dieses Mal stimmt das Muster `c:\foo\...\*.obj` mit dem Namen der Datei überein, die gerade verarbeitet wird. Die Verarbeitung stoppt, die Option wird überprüft und das Objekt wird eingeschlossen.
3. Die Datei `c:\foo\dev\test.obj` wird gesichert.

Beispiel 2

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude ?:\*.obj
include c:\foo\...\*.obj
exclude c:\foo\junk\*.obj
```

Folgende Datei wird gerade verarbeitet: `c:\widg\copyit.bat`. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
2. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 1 wird überprüft, ohne eine Übereinstimmung zu finden.
4. Da keine Übereinstimmung gefunden wurde, wird die Datei `c:\widg\copyit.bat` implizit eingeschlossen und gesichert.

Beispiel 3

Sie haben die folgenden Anweisungen für die Optionen include und exclude definiert:

```
exclude ?:\...\*.obj
include c:\foo\...\*.obj
exclude c:\foo\junk\*.obj
```

Zurzeit wird die folgende Datei verarbeitet: `c:\lib\objs\printf.obj`. Folgende Verarbeitungsschritte werden durchgeführt:

1. Regel 3 wird überprüft, ohne eine Übereinstimmung zu finden.
2. Regel 2 wird überprüft, ohne eine Übereinstimmung zu finden.
3. Regel 1 wird überprüft, und es wird eine Übereinstimmung gefunden.
4. Die Verarbeitung stoppt, die Option wird überprüft und das Objekt wird ausgeschlossen.
5. Die Datei `c:\lib\objs\printf.obj` wird nicht gesichert.

Zugehörige Konzepte:
Dateibereiche und Verzeichnisse ausschließen
Verarbeitungsoptionen
Zugehörige Verweise:
Ausschlussoptionen
Query Inclexcl
Windows-Betriebssysteme

Verarbeitungsregeln bei Verwendung von UNC-Namen

Bei der Verarbeitung von Dateien mit Namen, die der allgemeinen Namenskonvention entsprechen, müssen Regeln eingehalten werden.

Der Client für Sichern/Archivieren verwendet die in Verarbeitung von Einschluss- und Ausschlussoptionen beschriebenen Regeln. Außerdem gelten die Regeln in Explizite Verwendung von UNC-Namen für ferne Laufwerke.

- Windows-BetriebssystemeExplizite Verwendung von UNC-Namen für ferne Laufwerke
  Der Client für Sichern/Archivieren erkennt die explizite Verwendung von UNC-Namen für ferne Laufwerke.
- Windows-BetriebssystemeKonvertierung von DOS-Pfadnamen für Festplatten- und ferne Laufwerke
  Der Client für Sichern/Archivieren konvertiert DOS-Pfadnamen, die fernen Freigabepunkten zugeordnet sind.
- Windows-BetriebssystemeBeispiele für Übereinstimmungen bei Zeichenklassen
  Dieser Abschnitt enthält Beispiele für gültige Übereinstimmungen bei der Verwendung von Zeichenklassen.

Windows-Betriebssysteme

Explizite Verwendung von UNC-Namen für ferne Laufwerke

Der Client für Sichern/Archivieren erkennt die explizite Verwendung von UNC-Namen für ferne Laufwerke.

Wie in Tabelle 1 gezeigt, kann beispielsweise das DOS-Muster durch das Muster für UNC-Namen ersetzt werden.

Angenommen, der lokale Laufwerkbuchstabe `r:` ist dem fernen Freigabepunkt `\\remote\c$` zugeordnet, `s:` ist `\\remote\share4` zugeordnet und `t:` ist `\\remote\share2` zugeordnet.

Tabelle 1. Muster für UNC-Namen und DOS-Muster

Muster für UNC-Namen	DOS-Muster
`\\remote\c$\include\file.out`	`r:\include\file.out`
`\\remote\c$\...\file.out`	`r:\...\file.out`
`\\remote\share4\exclude\*`	`s:\exclude\*`
`\\remote\share2\...\?.out`	`t:\...\?.out`

 Windows-Betriebssysteme

Konvertierung von DOS-Pfadnamen für Festplatten- und ferne Laufwerke

Der Client für Sichern/Archivieren konvertiert DOS-Pfadnamen, die fernen Freigabepunkten zugeordnet sind.

Beispielsweise wird ein zugeordneter ferner Freigabepunkt von `r:\test\...\exclude.out` in `\\remote\share\test\...\exclude.out` konvertiert. Nicht zugeordnete ferne Freigabepunkte werden nicht konvertiert. Dateien auf austauschbaren Datenträgern werden nicht konvertiert.

 Windows-Betriebssysteme

Beispiele für Übereinstimmungen bei Zeichenklassen

Dieser Abschnitt enthält Beispiele für gültige Übereinstimmungen bei der Verwendung von Zeichenklassen.

```
\\remote[a-z]\share\file.txt
entspricht    \\remotea\share\file.txt
  \\remote\share[a-z]\file.txt
entspricht    \\remote\sharex\file.txt
  \\remote\share\file[a-z].txt
entspricht    \\remote\share\fileg.txt
```

Erste Schritte

Bevor Sie den IBM Spectrum Protect-Client für Sichern/Archivieren verwenden können, müssen Sie wissen, wie eine GUI- oder Befehlszeilensitzung gestartet und der Client-Scheduler automatisch gestartet wird. Sie lernen auch andere häufig verwendete Tasks kennen.

Führen Sie die folgenden Tasks aus, bevor Sie den Client für Sichern/Archivieren verwenden:

- Java-GUI-Sitzung starten
- Befehlszeilensitzung starten
- Web-Client-Sitzung starten
- Client-Scheduler automatisch starten
- Kennwort ändern

Sie können auch die folgenden Tasks ausführen:

- Dateilisten mithilfe der GUI des Clients für Sichern/Archivieren sortieren
- Onlinehilfe anzeigen
- Sitzung beenden

- Clientsicherheitseinstellungen für eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 und höher konfigurieren
  Wenn Sie die Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen, gibt es mehrere Konfigurationsoptionen, die zu den Sicherheitseinstellungen des IBM Spectrum Protect-Clients gehören. Wenn Sie die Standardwerte für diese Optionen akzeptieren, erfolgt die Konfiguration des Clients aus Gründen einer verbesserten Sicherheit transparent; dies wird für die meisten Anwendungsfälle empfohlen.
- Sicherer Kennwortspeicher
  In IBM Spectrum Protect Version 8.1.2 befindet sich das IBM Spectrum Protect-Kennwort an einer anderen Position.
-  Windows-BetriebssystemeOperationen des Clients für Sichern/Archivieren und Sicherheitsberechtigungen
  In diesem Abschnitt werden die Operationstypen des IBM Spectrum Protect-Clients für Sichern/Archivieren, die ausgeführt werden können, und die notwendigen Sicherheitsberechtigungen erklärt.
-  Windows-BetriebssystemeErforderliche Berechtigungen zum Zurückschreiben von Dateien, die mit adaptiver Subdateisicherung verarbeitet wurden
  Die adaptive Subdateisicherung ist veraltet; es ist jedoch weiterhin möglich, Subdateisicherungsdaten, die mit dem Client der Version 7.1 oder früher erstellt wurden, zurückzuschreiben. Zum Zurückschreiben von Dateien, die mithilfe der adaptiven Subdateisicherung verarbeitet wurden, muss der Benutzer der Eigner der Dateien sein oder über Lesezugriffsberechtigung verfügen.
-  Windows-BetriebssystemeErforderliche Berechtigungen zum Sichern, Archivieren, Zurückschreiben oder Abrufen von Dateien auf Clusterressourcen

Wenn auf Clusterressourcen von Microsoft Cluster Server (MSCS) oder Veritas Cluster Server gespeicherte Daten gesichert, zurückgeschrieben, archiviert oder abgerufen werden sollen, muss Ihr Windows-Konto zur Gruppe 'Administratoren' oder 'Domänen-Admins' oder zur Gruppe 'Sicherungsoperatoren' gehören.

- IBM Spectrum Protect-Clientauthentifizierung
  Wenn Sie die grafische Benutzerschnittstelle oder Befehlszeilenschnittstelle des IBM Spectrum Protect-Clients verwenden, können Sie sich mit einem Knotennamen und einem Kennwort *oder* mit einer Benutzer-ID mit Administratorberechtigung und dem zugehörigen Kennwort anmelden.
- Windows-BetriebssystemeBenutzerkontensteuerung
  Die Benutzerkontensteuerung ist eine Windows-Sicherheitsfunktion, die eine Beeinträchtigung des Betriebssystems durch Malware zu verhindern hilft. Die Benutzerkontensteuerung beschränkt Programme auf Standardbenutzerberechtigungen.
- Java-GUI-Sitzung starten
  Welche Schritte zum Starten der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren ausgeführt werden, ist vom Betriebssystem abhängig.
- Befehlszeilensitzung starten
  Sie können eine Befehlszeilensitzung starten, indem Sie den Befehl dsmc aufrufen.
- Eingabezeichenfolgen angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthalten
  Sie müssen bestimmte Regeln einhalten, wenn Sie eine Eingabezeichenfolge angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthält.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWeitere Hinweise zum Starten
  Optionen können als Argumente in den Befehlen **dsmj** und **dsmc** angegeben werden. Mithilfe von Optionen kann beispielsweise das für die Anzeige von Datum, Uhrzeit und Zahlen verwendete Format geändert werden oder das Kennwort eingeschlossen werden, sodass der Client für Sichern/Archivieren nicht zur Eingabe des Kennworts auffordert.
- Web-Client in neuer Sicherheitsumgebung verwenden
  Ab IBM Spectrum Protect Version 8.1.2 können Sie nicht mehr den Web-Client verwenden, um eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder höher herzustellen.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme
  Windows-BetriebssystemeClient-Scheduler automatisch starten
  Sie können den Client-Scheduler beim Start Ihrer Workstation automatisch starten.
- Kennwort ändern
  Der IBM Spectrum Protect-Administrator kann für die Verbindung zum Server die Eingabe eines Kennworts durch den Benutzer erforderlich machen.
- Dateilisten mithilfe der GUI des Clients für Sichern/Archivieren sortieren
  Mithilfe der GUI des Clients für Sichern/Archivieren können Sie Dateien anzeigen, sortieren oder auswählen.
- Onlinehilfe anzeigen
  Zum Anzeigen der Onlinehilfe stehen die folgenden Möglichkeiten zur Verfügung: in der GUI des Clients für Sichern/Archivieren, über den Web-Client oder über die dsmc-Befehlszeile.
- Sitzung beenden
  Sie können eine Clientsitzung über die GUI des Clients für Sichern/Archivieren oder die dsmc-Befehlszeile beenden.
- Onlineforen
  Um an Benutzerdiskussionen zu IBM Spectrum Protect-Produkten teilnehmen zu können, können Sie eine Subskription für den Listenserver ADSM-L beantragen.

Clientsicherheitseinstellungen für eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 und höher konfigurieren

Wenn Sie die Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen, gibt es mehrere Konfigurationsoptionen, die zu den Sicherheitseinstellungen des IBM Spectrum Protect-Clients gehören. Wenn Sie die Standardwerte für diese Optionen akzeptieren, erfolgt die Konfiguration des Clients aus Gründen einer verbesserten Sicherheit transparent; dies wird für die meisten Anwendungsfälle empfohlen.

- Standardsicherheitseinstellungen für den Client (Schnellzugriffspfad)
  Schnellzugriffspfaddetails sind die Konfigurationsoptionen, die Auswirkungen auf die Sicherheit der Clientverbindung zum Server und das Verhalten für verschiedene Anwendungsfälle haben, wenn Standardwerte akzeptiert werden. Dieses Szenario minimiert die Schritte im Konfigurationsprozess an Endpunkten. Es werden automatisch Zertifikate vom Server abgerufen, wenn der Client zum ersten Mal die Verbindung herstellt, vorausgesetzt der Parameter SESSIONSECURITY auf dem IBM Spectrum Protect-Server ist auf TRANSITIONAL gesetzt; TRANSITIONAL ist der Standardwert und der empfohlene Wert. Sie können diesem Szenario unabhängig davon folgen, ob Sie zuerst das Upgrade für den IBM Spectrum Protect-Server auf Version 8.1.2 ausführen und anschließend das Upgrade für den Client auf Version 8.1.2 ausführen oder umgekehrt.
- Client ohne automatische Verteilung von Zertifikaten konfigurieren
  Dieses Szenario erläutert die einzelnen Konfigurationsoptionen, die Auswirkungen auf die Sicherheit des Clients haben, wenn die automatische Verteilung von Zertifikaten vom Server nicht zulässig ist. Die automatische Verteilung von Zertifikaten vom Server ist nicht zulässig, wenn der Server für die Verwendung der LDAP-Authentifizierung konfiguriert ist oder wenn Zertifikate von einer Zertifizierungsstelle signiert werden müssen.

Standardsicherheitseinstellungen für den Client (Schnellzugriffspfad)

Schnellzugriffspfaddetails sind die Konfigurationsoptionen, die Auswirkungen auf die Sicherheit der Clientverbindung zum Server und das Verhalten für verschiedene Anwendungsfälle haben, wenn Standardwerte akzeptiert werden. Dieses Szenario minimiert die Schritte im Konfigurationsprozess an Endpunkten. Es werden automatisch Zertifikate vom Server abgerufen, wenn der Client zum ersten Mal die Verbindung herstellt, vorausgesetzt der Parameter SESSIONSECURITY auf dem IBM Spectrum Protect-Server ist auf TRANSITIONAL gesetzt; TRANSITIONAL ist der Standardwert und der empfohlene Wert. Sie können diesem Szenario unabhängig davon folgen, ob Sie zuerst das Upgrade für den IBM Spectrum Protect-Server auf Version 8.1.2 ausführen und anschließend das Upgrade für den Client auf Version 8.1.2 ausführen oder umgekehrt.

Achtung: Dieses Szenario kann nicht verwendet werden, wenn der IBM Spectrum Protect-Server für die LDAP-Authentifizierung konfiguriert ist. Wenn LDAP verwendet wird, können Sie die erforderlichen Zertifikate manuell mithilfe des Dienstprogramms dsmcert importieren. Ausführliche Informationen finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.

Clientoptionen mit Auswirkungen auf die Sitzungssicherheit

1. SSLREQUIRED. Mit dem Standardwert Default werden bestehende Verbindungen mit Sitzungssicherheit zu Servern einer Version vor Version 8.1.2 aktiviert und der Client automatisch zum Herstellen einer sicheren Verbindung zu einem Server der Version 8.1.2 oder höher unter Verwendung von TLS für die Authentifizierung konfiguriert.
2. SSLACCEPTCERTFROMSERV. Der Standardwert Yes ermöglicht es dem Client, automatisch ein selbst signiertes öffentliches Zertifikat vom Server zu akzeptieren und den Client automatisch für die Verwendung dieses Zertifikats zu konfigurieren, wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt.
3. SSL. Der Standardwert No gibt an, dass keine Verschlüsselung verwendet wird, wenn Daten zwischen dem Client und einem Server einer Version vor Version 8.1.2 übertragen werden. Wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, gibt der Standardwert No an, dass Objektdaten nicht verschlüsselt werden. Alle anderen Informationen werden verschlüsselt, wenn der Client mit dem Server kommuniziert. Wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, gibt der Wert Yes an, dass SSL zum Verschlüsseln aller Informationen, einschließlich Objektdaten, verwendet wird, wenn der Client mit dem Server kommuniziert.
4. SSLFIPSMODE. Der Standardwert No gibt an, dass keine mit FIPS zertifizierte SSL-Bibliothek erforderlich ist.

Darüber hinaus gelten die folgenden Optionen nur, wenn der Client SSL-Verbindungen zu einem Server einer Version vor Version 8.1.2 verwendet. Sie werden ignoriert, wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt.

1. SSLDISABLELEGACYTLS. Der Standardwert No gibt an, dass Verbindungen mit TLS 1.1 oder SSL-Protokollen früherer Versionen zulässig sind, wenn der Client mit einem Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Versionen kommuniziert.
2. LANFREESSL. Gibt an, ob der Client die SSL-Kommunikation mit dem Speicheragenten verwendet, wenn die LAN-unabhängige Datenübertragung konfiguriert ist.
3. REPLSSLPORT. Gibt an, ob die TCP/IP-Anschlussadresse für SSL aktiviert ist, wenn der Client mit dem Zielreplikationsserver kommuniziert.

Anwendungsfälle für Standardsicherheitseinstellungen für den Client (Schnellzugriffspfad)

1. Zuerst wird das Upgrade für den Server auf Version 8.1.2 durchgeführt. Anschließend wird das Upgrade für den Client durchgeführt. Der vorhandene Client verwendet keine SSL-Kommunikation:
   - An den Clientsicherheitsoptionen sind keine Änderungen erforderlich.
   - Für die Clientkonfiguration erfolgt ein automatisches Update für die Verwendung von TLS, wenn sich der Client beim Server authentifiziert.
2. Zuerst wird das Upgrade für den Server auf Version 8.1.2 durchgeführt. Anschließend wird das Upgrade für den Client durchgeführt. Der vorhandene Client verwendet die SSL-Kommunikation:
   - An den Clientsicherheitsoptionen sind keine Änderungen erforderlich.
   - Es wird weiterhin die SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat verwendet.
   - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die vom Server benötigt wird.
3. Zuerst wird das Upgrade für den Client auf Version 8.1.2 durchgeführt. Anschließend wird das Upgrade für den Server durchgeführt. Der vorhandene Client verwendet keine SSL-Kommunikation:
   - An den Clientsicherheitsoptionen sind keine Änderungen erforderlich.
   - Das vorhandene Authentifizierungsprotokoll wird weiterhin für Server einer Version vor Version 8.1.2 verwendet.
   - Für die Clientkonfiguration erfolgt ein automatisches Update für die Verwendung von TLS, wenn sich der Client beim Server authentifiziert, nachdem für den Server ein Update auf Version 8.1.2 oder höher durchgeführt wurde.
4. Zuerst wird das Upgrade für den Client auf Version 8.1.2 durchgeführt. Anschließend wird das Upgrade für den Server durchgeführt. Der vorhandene Client verwendet die SSL-Kommunikation:
   - An den Clientsicherheitsoptionen sind keine Änderungen erforderlich.
   - Es wird weiterhin die SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat mit Servern einer Version vor Version 8.1.2 verwendet.
   - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die vom Server benötigt wird, nachdem für den Server ein Update auf Version 8.1.2 oder höher durchgeführt wurde.
5. Zuerst wird das Upgrade für den Client auf Version 8.1.2 durchgeführt. Anschließend stellt der Client die Verbindung zu mehreren Servern her. Das Upgrade für die Server auf Version 8.1.2 erfolgt zu unterschiedlichen Zeiten:
   - An den Clientsicherheitsoptionen sind keine Änderungen erforderlich.
   - Der Client verwendet die vorhandene Authentifizierung und das vorhandene Sitzungssicherheitsprotokoll zum Herstellen der Verbindung zu Servern einer Version vor Version 8.1.2; für den Client erfolgt ein automatisches Upgrade für die Verwendung der

TLS-Authentifizierung, wenn der Client zum ersten Mal die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt. Die Sitzungssicherheit wird für jeden Server separat verwaltet.

6. Neue Clientinstallation mit einem Server der Version 8.1.2 oder höher:
    - Konfigurieren Sie den Client gemäß einer neuen Clientinstallation.
    - Mit den Standardwerten für die Clientsicherheitsoptionen wird der Client automatisch für die mit TLS verschlüsselte Sitzungsauthentifizierung konfiguriert.
    - Setzen Sie den Parameter SSL auf Yes, wenn die Verschlüsselung aller Datenübertragungen zwischen dem Client und dem Server erforderlich ist.
7. Neue Clientinstallation mit einem Server einer Version vor Version 8.1.2:
    - Konfigurieren Sie den Client gemäß einer neuen Clientinstallation.
    - Akzeptieren Sie die Standardwerte für die Parameter für die Clientsitzungssicherheit, wenn die SSL-Verschlüsselung aller Datenübertragungen nicht erforderlich ist.
        - Das Nicht-SSL-Authentifizierungsprotokoll wird so lange verwendet, bis für den Server ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird.
    - Setzen Sie den Parameter SSL auf Yes, wenn die Verschlüsselung aller Datenübertragungen zwischen dem Client und dem Server erforderlich ist, und fahren Sie mit der manuellen Clientkonfiguration für SSL fort.
        - Ausführliche Informationen finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
        - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die vom Server benötigt wird, nachdem für den Server ein Update auf Version 8.1.2 oder höher durchgeführt wurde.

Zugehörige Verweise:
Sslrequired
Sslacceptcertfromserv
Ssl
Sslfipsmode
Ssldisablelegacytls
Lanfreessl
Replsslport

Client ohne automatische Verteilung von Zertifikaten konfigurieren

Dieses Szenario erläutert die einzelnen Konfigurationsoptionen, die Auswirkungen auf die Sicherheit des Clients haben, wenn die automatische Verteilung von Zertifikaten vom Server nicht zulässig ist. Die automatische Verteilung von Zertifikaten vom Server ist nicht zulässig, wenn der Server für die Verwendung der LDAP-Authentifizierung konfiguriert ist oder wenn Zertifikate von einer Zertifizierungsstelle signiert werden müssen.

Anmerkung: In diesem Szenario können Sie die Standardwerte für die meisten Optionen für die Sitzungssicherheit akzeptieren; die einzige Ausnahme ist die Option SSLACCEPTCERTFROMSERV.

Clientoptionen mit Auswirkungen auf die Sitzungssicherheit

1. SSLREQUIRED. Mit dem Standardwert Default werden bestehende Verbindungen mit Sitzungssicherheit zu Servern einer Version vor Version 8.1.2 aktiviert und der Client automatisch zum Herstellen einer sicheren Verbindung zu einem Server der Version 8.1.2 oder höher unter Verwendung von TLS für die Authentifizierung konfiguriert.
2. SSLACCEPTCERTFROMSERV. Setzen Sie diesen Wert auf No, um sicherzustellen, dass der Client nicht automatisch ein selbst signiertes öffentliches Zertifikat vom Server akzeptiert, wenn der Client zum ersten Mal die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt.
3. SSL. Der Standardwert No gibt an, dass keine Verschlüsselung verwendet wird, wenn Daten zwischen dem Client und einem Server einer Version vor Version 8.1.2 übertragen werden. Wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, gibt der Standardwert No an, dass Objektdaten nicht verschlüsselt werden. Alle anderen Informationen werden verschlüsselt, wenn der Client mit dem Server kommuniziert. Wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, gibt der Wert Yes an, dass SSL zum Verschlüsseln aller Informationen, einschließlich Objektdaten, verwendet wird, wenn der Client mit dem Server kommuniziert.
4. SSLFIPSMODE. Der Standardwert No gibt an, dass keine mit FIPS zertifizierte SSL-Bibliothek erforderlich ist.

Darüber hinaus gelten die folgenden Optionen nur, wenn der Client SSL-Verbindungen zu einem Server einer Version vor Version 8.1.2 verwendet. Sie werden ignoriert, wenn der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt.

1. SSLDISABLELEGACYTLS. Der Standardwert No gibt an, dass Verbindungen mit TLS 1.1 oder SSL-Protokollen früherer Versionen zulässig sind, wenn der Client mit einem Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Versionen kommuniziert.
2. LANFREESSL. Gibt an, ob der Client die SSL-Kommunikation mit dem Speicheragenten verwendet, wenn die LAN-unabhängige Datenübertragung konfiguriert ist.
3. REPLSSLPORT. Gibt an, ob die TCP/IP-Anschlussadresse für SSL aktiviert ist, wenn der Client mit dem Zielreplikationsserver kommuniziert.

Anwendungsfälle für die Konfiguration des Clients ohne automatische Verteilung von Zertifikaten

1. Zuerst wird das Upgrade für den Server auf Version 8.1.2 durchgeführt. Anschließend wird das Upgrade für den Client durchgeführt. Der vorhandene Client verwendet keine SSL-Kommunikation:
    - Setzen Sie mithilfe des Clientkonfigurationsassistenten die Option SSLACCEPTCERTFROMSERV auf den Wert No.
    - Fordern Sie das erforderliche Zertifikat von einer vertrauenswürdigen Quelle an.
    - Importieren Sie das Zertifikat für die Verwendung durch den Client mithilfe des Dienstprogramms dsmcert. Ausführliche Informationen finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
2. Zuerst wird das Upgrade für den Server auf Version 8.1.2 durchgeführt. Anschließend wird das Upgrade für den Client durchgeführt. Der vorhandene Client verwendet die SSL-Kommunikation:
    - An den Clientsicherheitsoptionen sind keine Änderungen erforderlich. Wenn der Client bereits über ein Serverzertifikat für die SSL-Kommunikation verfügt, ist die Option SSLACCEPTCERTFROMSERV nicht zutreffend.
    - Es wird weiterhin die SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat verwendet.
    - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die vom Server benötigt wird.
3. Zuerst wird das Upgrade für den Client auf Version 8.1.2 durchgeführt. Anschließend wird das Upgrade für den Server durchgeführt. Der vorhandene Client verwendet keine SSL-Kommunikation:
    - Setzen Sie mithilfe des Clientkonfigurationsassistenten die Option SSLACCEPTCERTFROMSERV auf den Wert No.
    - Das vorhandene Authentifizierungsprotokoll wird weiterhin für Server einer Version vor Version 8.1.2 verwendet.
    - Bevor der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, müssen Sie folgende Schritte ausführen:
        - Fordern Sie das erforderliche Zertifikat von einer vertrauenswürdigen Quelle an.
        - Importieren Sie das Zertifikat für die Verwendung durch den Client mithilfe des Dienstprogramms dsmcert. Ausführliche Informationen finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
4. Zuerst wird das Upgrade für den Client auf Version 8.1.2 durchgeführt. Anschließend wird das Upgrade für den Server durchgeführt. Der vorhandene Client verwendet die SSL-Kommunikation:
    - An den Clientsicherheitsoptionen sind keine Änderungen erforderlich. Wenn der Client bereits über ein Serverzertifikat für die SSL-Kommunikation verfügt, ist die Option SSLACCEPTCERTFROMSERV nicht zutreffend.
    - Es wird weiterhin die SSL-Kommunikation mit dem vorhandenen öffentlichen Serverzertifikat mit Servern einer Version vor Version 8.1.2 verwendet.
    - Die SSL-Kommunikation wird automatisch für die Verwendung der TLS-Version erweitert, die vom Server benötigt wird, nachdem für den Server ein Update auf Version 8.1.2 oder höher durchgeführt wurde.
5. Zuerst wird das Upgrade für den Client auf Version 8.1.2 durchgeführt. Anschließend stellt der Client die Verbindung zu mehreren Servern her. Das Upgrade für die Server auf Version 8.1.2 erfolgt zu unterschiedlichen Zeiten:
    - Setzen Sie mithilfe des Clientkonfigurationsassistenten die Option SSLACCEPTCERTFROMSERV auf den Wert No.
    - Das vorhandene Authentifizierungsprotokoll wird weiterhin für Server einer Version vor Version 8.1.2 verwendet.
    - Bevor der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt oder wenn die SSL-Kommunikation für eine Version des Servers erforderlich ist, müssen Sie folgende Schritte ausführen:
        - Fordern Sie das erforderliche Zertifikat für den Zielserver von einer vertrauenswürdigen Quelle an.
        - Importieren Sie das Zertifikat für die Verwendung durch den Client mithilfe des Dienstprogramms dsmcert. Ausführliche Informationen finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
    - Der Client verwendet die vorhandene Authentifizierung und das vorhandene Sitzungssicherheitsprotokoll zum Herstellen der Verbindung zu Servern einer Version vor Version 8.1.2; für den Client erfolgt ein automatisches Upgrade für die Verwendung der TLS-Authentifizierung, wenn der Client zum ersten Mal die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt. Die Sitzungssicherheit wird für jeden Server separat verwaltet.
6. Neue Clientinstallation mit einem Server der Version 8.1.2 oder höher:
    - Konfigurieren Sie den Client gemäß einer neuen Clientinstallation.
    - Setzen Sie mithilfe des Clientkonfigurationsassistenten die Option SSLACCEPTCERTFROMSERV auf den Wert No.
    - Fordern Sie das erforderliche Zertifikat von einer vertrauenswürdigen Quelle an.
    - Importieren Sie das Zertifikat für die Verwendung durch den Client mithilfe des Dienstprogramms dsmcert. Ausführliche Informationen finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
    - Setzen Sie den Parameter SSL auf Yes, wenn die Verschlüsselung aller Datenübertragungen zwischen dem Client und dem Server erforderlich ist.
7. Neue Clientinstallation mit einem Server einer Version vor Version 8.1.2, wenn mit SSL verschlüsselte Sitzungen erforderlich sind:
    - Konfigurieren Sie den Client gemäß einer neuen Clientinstallation.
    - Setzen Sie den Parameter SSL auf den Wert Yes.
    - Fordern Sie das erforderliche Zertifikat von einer vertrauenswürdigen Quelle an.
    - Importieren Sie das Zertifikat für die Verwendung durch den Client mithilfe des Dienstprogramms dsmcert. Ausführliche Informationen finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.
8. Neue Clientinstallation mit einem Server einer Version vor Version 8.1.2, wenn keine mit SSL verschlüsselte Sitzungen erforderlich sind:
    - Konfigurieren Sie den Client gemäß einer neuen Clientinstallation.
    - Setzen Sie mithilfe des Clientkonfigurationsassistenten die Option SSLACCEPTCERTFROMSERV auf den Wert No.
        - Das Nicht-SSL-Authentifizierungsprotokoll wird so lange verwendet, bis für den Server ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird.
    - Bevor der Client die Verbindung zu einem Server der Version 8.1.2 oder höher herstellt, müssen Sie folgende Schritte ausführen:
        - Fordern Sie das erforderliche Zertifikat von einer vertrauenswürdigen Quelle an.
        - Importieren Sie das Zertifikat für die Verwendung durch den Client mithilfe des Dienstprogramms dsmcert. Ausführliche Informationen finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.

Zugehörige Verweise:
Sslrequired
Sslacceptcertfromserv
Ssl

Sslfipsmode
Ssldisablelegacytls
Lanfreessl
Replsslport

Sicherer Kennwortspeicher

In IBM Spectrum Protect Version 8.1.2 befindet sich das IBM Spectrum Protect-Kennwort an einer anderen Position.

In den Clients der Version 8.1.0, 7.1.6 und früherer Versionen wurde das IBM Spectrum Protect-Kennwort bei Windows-Clients in der Windows-Registrierungsdatenbank und bei UNIX- und Linux-Clients in der Datei TSM.PWD gespeichert.

Ab Version 8.1.2 werden alle IBM Spectrum Protect-Kennwörter in den Schlüsselspeichern von IBM® Global Security Kit (GSKit) gespeichert. Der Importprozess für Serverzertifikate ist vereinfacht. Informationen zum Importieren von Serverzertifikaten finden Sie in IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren.

Wenn Sie ein Upgrade des Clients für Sichern/Archivieren auf IBM Spectrum Protect Version 8.1.2 durchführen, werden die vorhandenen Kennwörter in die folgenden Dateien im neuen Kennwortspeicher migriert:

TSM.KDB
: In dieser Datei werden die verschlüsselten Kennwörters gespeichert.

TSM.sth
: In dieser Datei wird der Verschlüsselungszufallsschlüssel gespeichert, mit dem Kennwörter in der Datei TSM.KDB verschlüsselt werden. Diese Datei wird durch das Dateisystem geschützt. Diese Datei wird für automatisierte Operationen benötigt.

TSM.IDX
: Eine indexierte Datei zur Protokollierung der Kennwörter in der Datei TSM.KDB.

Linux-BetriebssysteWindows-BetriebssystemeBei Data Protection for VMware-Clients wird das Verwaltungskennwort des Data Protection for VMware-GUI-Servers in einen Schlüsselspeicher migriert.

Windows-Betriebssysteme

Kennwortpositionen auf Windows-Clients

Auf Windows-Clients werden die Kennwörter im Registrierungsschlüssel SOFTWARE\IBM\ADSM\CurrentVersion\BackupClient\Nodes und im Registrierungsschlüssel SOFTWARE\IBM\ADSM\CurrentVersion\Nodes in den neuen Kennwortspeicher umgelagert.

Die Kennworteinträge in diesen Registrierungsschlüsseln werden nach der Migration gelöscht.

Die migrierten Server- und Verschlüsselungskennwörter werden in den Kennwortspeichern in separaten Unterverzeichnissen des verborgenen Verzeichnisses C:\ProgramData\Tivoli\TSM\baclient gespeichert. Durch eine derartige Trennung der Serverkennwörter ist es möglich, dass ein Administrator einem Benutzer ohne Verwaltungsaufgaben den Zugriff auf einzelne Kennwörter gewährt, ohne dass dieser Benutzer Zugriff auf alle anderen Kennwörter erhält. Die folgenden Verzeichnisse sind Beispiele für Kennwortdateipositionen:

- C:\ProgramData\Tivoli\TSM\BAClient\NodeName\ServerName
- C:\ProgramData\Tivoli\TSM\BAClient\(VCB)\ServerName
- C:\ProgramData\Tivoli\TSM\BAClient\(DOMAIN)\ServerName
- C:\ProgramData\Tivoli\TSM\BAClient\(FILER)\ServerName

Der Zugriff auf die Kennwortstashdateien (TSM.sth) ist auf den Ersteller des Schlüsselspeichers, auf Administratoren und das System beschränkt. Für eine einfache Änderung von Zugriffssteuerungslisten für Kennwortdateien steht Windows-Benutzern ein Dienstprogramm (dsmcutil addace) zur Verfügung. Weitere Informationen finden Sie in ADDACE und in DELETEACE.

AIX-BetriebssysteLinux-BetriebssysteMac OS X-BetriebssysteOracle Solaris-Betriebssysteme

Kennwortpositionen auf UNIX- und Linux-Clients

Auf UNIX- und Linux-Clients werden die in den Dateien TSM.PWD vorhandenen Kennwörter in den neuen Kennwortspeicher an derselben Position migriert. Bei Rootbenutzern lautet die Standardposition für den Kennwortspeicher /etc/adsm. Bei Benutzern ohne Rootberechtigung wird die Position des Kennwortspeichers mit der Option passworddir angegeben.

Die Datei TSM.PWD wird nach der Migration gelöscht.

AIX-BetriebssysteLinux-BetriebssysteMac OS X-BetriebssysteOracle Solaris-Betriebssysteme

Trusted Communication Agent nicht mehr verfügbar

Der bisher von Benutzern ohne Rootberechtigung in Version 8.1.0 und 7.1.6 und älteren Clients verwendete Trusted Communication Agent (TCA) ist nicht mehr verfügbar. Rootbenutzer können Benutzern ohne Rootberechtigung die Verwaltung ihrer Dateien mit den folgenden Methoden ermöglichen:

Help-Desk
: Bei der Help-Desk-Methode führt der Rootbenutzer alle Sicherungs- und Zurückschreibungsoperationen aus. Der Benutzer ohne Rootberechtigung muss sich an den Rootbenutzer wenden, um die Sicherung oder Zurückschreibung bestimmter Dateien anzufordern.

Berechtigter Benutzer
: Bei der Methode mit einem berechtigten Benutzer erhält ein Benutzer ohne Rootberechtigung Schreib-/Lesezugriff auf den Kennwortspeicher. Hierbei wird die Option passworddir verwendet, um auf eine Kennwortposition zu zeigen, auf die der Benutzer ohne Rootberechtigung Schreib-/Lesezugriff hat. Mit dieser Methode können Benutzer ohne Rootberechtigung ihre eigenen Dateien sichern und zurückschreiben, die Verschlüsselung verwenden und ihre eigenen Kennwörter mit der Option passwordaccess generate verwalten.

  Weitere Informationen finden Sie in Benutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen.

Ist keine dieser Methoden zufriedenstellend, müssen Sie die früheren Clients verwenden, die über den Trusted Communication Agent (TCA) verfügen.

 Windows-Betriebssysteme

Kennwortpositionen in Clusterumgebungen

Wird der Client in einer Clusterumgebung ausgeführt (CLUSTERNODE YES in der Clientoptionsdatei), werden die Kennwortdateien in einem Unterverzeichnis des Verzeichnisses der Clientoptionsdatei gespeichert. Der Name des Unterverzeichnisses lautet:

`NODES\`*`Knotenname`*`\`*`Servername`*

In einer Clusterkonfiguration wird die Optionsdatei auf einer Clusterplatte gespeichert, damit der Übernahmeknoten auf sie zugreifen kann. Die Kennwortdateien müssen auch auf einer Clusterplatte gespeichert werden, damit das generierte Kennwort des Clients für Sichern/Archivieren dem Übernahmeknoten nach einer Störung zur Verfügung steht.
Wenn sich beispielsweise die Datei dsm.opt im Verzeichnis c:\ClusterStorage\Volume1\SPData befindet, der Knotenname `Cluster-B` und der Servername `Bigdata` lautet, ist die Position für Kennwortdateien

```
C:\ClusterStorage\Volume1\SPdata\Nodes\Cluster-B\Bigdata
```

 Windows-Betriebssysteme

Operationen des Clients für Sichern/Archivieren und Sicherheitsberechtigungen

In diesem Abschnitt werden die Operationstypen des IBM Spectrum Protect-Clients für Sichern/Archivieren, die ausgeführt werden können, und die notwendigen Sicherheitsberechtigungen erklärt.

Zum Installieren und Konfigurieren der Client-Services von IBM Spectrum Protect müssen Sie über die Berechtigungen eines lokalen Administrators oder eines Domänenadministrators verfügen.

Tabelle 1 fasst die Benutzersicherheitsberechtigungen zusammen, die für Sicherungs- und Zurückschreibungsoperationen benötigt werden. Bei den Informationen in der Tabelle wird vorausgesetzt, dass die Standardberechtigungen für die Microsoft Windows-Gruppen 'Administratoren', 'Sicherungsoperatoren' und 'Benutzer' nicht geändert wurden.

Tabelle 1. Erforderliche Benutzersicherheitsberechtigungen für Sicherungs- und Zurückschreibungsservices von IBM Spectrum Protect

Betriebssystem	Konto	Was kann ich sichern und zurückschreiben?
Windows-Clients	Mitglied der Gruppe 'Administratoren'	• Alle Datei- und Verzeichnisobjekte sichern und zurückschreiben • Den Systemstatus sichern und zurückschreiben • Systemstatusdaten (die Gruppe 'Sicherungsoperatoren' kann keine ASR-Ausgabeprogrammdaten sichern und keine Systemstatusdaten zurückschreiben)
Windows-Clients	Mitglied der Gruppe 'Sicherungsoperatoren'	• Alle Datei- und Verzeichnisobjekte sichern und zurückschreiben • Systemstatus sichern, außer für ASR-Ausgabeprogramm Anmerkung: Mitglieder der Gruppe 'Sicherungsoperatoren' können den Systemstatus nicht zurückschreiben.

Betriebssystem	Konto	Was kann ich sichern und zurückschreiben?
Windows-Clients	Mitglied der Gruppe 'Benutzer' oder einer anderen Gruppe	• Alle Datei- und Verzeichnisobjekte sichern und zurückschreiben Achtung: Benutzer benötigen die folgenden Microsoft Windows-Sicherheitsberechtigungen, um Dateien und Verzeichnisse sichern und zurückschreiben zu können: ◦ Dateien und Verzeichnisse sichern ◦ Dateien und Verzeichnisse zurückschreiben Diese Berechtigungen stellen ein potenzielles Sicherheitsrisiko dar, da sie die Sicherung bzw. Zurückschreibung jeder Datei gestatten, für die eine Sicherungskopie vorhanden ist. Diese Berechtigungen sollten nur vertrauenswürdigen Benutzern erteilt werden. Weitere Informationen zu diesen Berechtigungen finden Sie in der Microsoft Windows-Dokumentation. Anmerkung: Der Systemstatus kann nicht gesichert oder zurückgeschrieben werden.

Die IBM Spectrum Protect-Client-Services (Dienste) werden standardmäßig unter dem lokalen Systemkonto ausgeführt. Das lokale Systemkonto hat jedoch keinen Zugriff auf verbundene Netzlaufwerke und hat nicht dieselben Berechtigungen und Anmeldemerkmale wie ein Benutzer, der beim System angemeldet ist. Wenn bei Verwendung des lokalen Systemkontos Diskrepanzen zwischen einer vom Benutzer eingeleiteten Sicherung und einer terminierten Sicherung auftreten, sollten Sie erwägen, die Services unter Verwendung des Benutzerkontos auszuführen.

Tipp: Zusätzlich zu den entsprechenden Benutzersicherheitsberechtigungen erfordert der IBM Spectrum Protect-Client für Sichern/Archivieren, dass der Benutzer Leseberechtigung für das Stammverzeichnis aller Laufwerke hat, die gesichert oder zurückgeschrieben werden müssen. Wenn Sie das Systemkonto für die Anmeldung beim IBM Spectrum Protect-Scheduler-Service verwenden, müssen Sie sicherstellen, dass Sie dem Systemkonto (SYSTEM) Lesezugriff auf das Stammverzeichnis des Laufwerks erteilen. Es reicht nicht aus, jedem Lesezugriff auf das Stammverzeichnis des Laufwerks zu erteilen.

Auf Domänenressourcen (z. B. Netzlaufwerke) können nur Services zugreifen, deren Konfiguration eine Ausführung unter einem für Domänen berechtigten Konto mithilfe von dsmcutil oder Service Control Panel Application (Anwendung für Servicesteuerkonsole) zulässt.

Ab IBM Spectrum Protect Version 8.1.2 wird eine strengere Zugriffssteuerung für den IBM Spectrum Protect-Kennwortspeicher in Windows-Betriebssystemen durchgesetzt. Standardmäßig haben nur die Konten 'Administrator', 'SYSTEM' und 'Lokales System' Zugriff den Kennwortspeicher und die SSL-Zertifikate.

Sie können den Befehl dsmcutil addace verwenden, um die Zugriffssteuerungsliste zu ändern, damit weitere Benutzer (z. B. Benutzer ohne Verwaltungsaufgaben) oder Prozesse (z. B. die IBM Spectrum Protect Data Protection-Clientprozesse) auf den Kennwortspeicher und die SSL-Zertifikate zugreifen können.

Sie können den Befehl dsmcutil deleteace verwenden, um die Zugriffssteuerungsliste zu ändern und den Zugriff auf den Kennwortspeicher und die SSL-Zertifikate für Benutzer (z. B. Benutzer ohne Verwaltungsaufgaben) oder Prozesse (z. B. die IBM Spectrum Protect Data Protection-Clientprozesse) aufzuheben.

Weitere Informationen finden Sie in ADDACE und in DELETEACE.

- Windows-BetriebssystemeOperationen der Gruppe 'Sicherungsoperatoren'
  Die Gruppe 'Sicherungsoperatoren' ermöglicht Benutzern das Sichern und Zurückschreiben von Dateien unabhängig davon, ob sie über Lese- oder Schreibzugriff auf die Dateien verfügen.
- Windows-BetriebssystemeHinweise vor der Verwendung eines Kontos der Gruppe 'Sicherungsoperatoren'
  Beachten Sie die folgenden Hinweise, bevor Sie ein Konto der Gruppe 'Sicherungsoperatoren' verwenden, um Ihre Daten zu sichern, zu archivieren, zurückzuschreiben oder abzurufen.

Windows-Betriebssysteme

Operationen der Gruppe 'Sicherungsoperatoren'

Die Gruppe 'Sicherungsoperatoren' ermöglicht Benutzern das Sichern und Zurückschreiben von Dateien unabhängig davon, ob sie über Lese- oder Schreibzugriff auf die Dateien verfügen.

Diese Gruppe verfügt nur über begrenzte Benutzerberechtigungen, daher stehen den Mitgliedern der Gruppe 'Sicherungsoperatoren' einige Funktionen nicht zur Verfügung.

Die folgende Liste enthält die Operationen des Clients für Sichern/Archivieren, die ein Mitglied der Gruppe 'Sicherungsoperatoren' ausführen kann:

- Dateien sichern und zurückschreiben (siehe Tabelle 1).
- Den Systemstatus sichern.

  Sie müssen ein Mitglied der Gruppe 'Administratoren' sein, um ASR-Ausgabeprogrammdaten sichern zu können.

- Starten des Scheduler-Service

Die folgende Liste enthält die Operationen des Clients für Sichern/Archivieren, die ein Mitglied der Gruppe 'Sicherungsoperatoren' nicht ausführen kann:

- Starten anderer Services (Clientakzeptor, ferner Clientagent und Journalservice)
- Installieren und Konfigurieren von Client-Services
- Verwendung der Unterstützung offener Dateien (OFS)
- Sichern und Zurückschreiben von Images
- Sichern und Zurückschreiben von Windows-Dateifreigaben

 Windows-Betriebssysteme

Hinweise vor der Verwendung eines Kontos der Gruppe 'Sicherungsoperatoren'

Beachten Sie die folgenden Hinweise, bevor Sie ein Konto der Gruppe 'Sicherungsoperatoren' verwenden, um Ihre Daten zu sichern, zu archivieren, zurückzuschreiben oder abzurufen.

Beachten Sie die folgenden Hinweise, bevor Sie ein Konto der Gruppe 'Sicherungsoperatoren' verwenden, um Ihre Daten zu sichern, zu archivieren, zurückzuschreiben oder abzurufen:

- Wenn Sie den Client für Sichern/Archivieren bereits mit einem Konto der Gruppe 'Administratoren' verwendet haben, können Sie den Client unter Umständen nicht starten, da Sie die Protokolldateien (beispielsweise `dsmerror.log`) nicht öffnen können. Um dieses Problem zu lösen, können Sie der Gruppe 'Sicherungsoperatoren' Lese- und Schreibberechtigungen für die Protokolldateien oder die Verzeichnisse, die diese Protokolldateien enthalten, erteilen.
- Wenn Sie über vorhandene Sicherungen eines Clients für Sichern/Archivieren der Version 5.2 oder früher verfügen und versuchen, als Mitglied der Gruppe 'Sicherungsoperatoren' eine Teilsicherung eines vorhandenen Dateibereichs auszuführen, werden alle Daten als geändert betrachtet und erneut an den IBM Spectrum Protect-Server gesendet.
- Mitglieder der Gruppe 'Sicherungsoperatoren' sind möglicherweise nicht in der Lage, Dateidaten zu sichern oder zurückzuschreiben, die von einem Administratorkonto verschlüsselt wurden, das das Encrypted File System (EFS) von Windows verwendet.
- Mitglieder der Gruppe 'Sicherungsoperatoren' haben nicht die korrekte Berechtigung, um die letzte Zugriffszeit für Dateien zu aktualisieren, die mit dem Encrypted File System (EFS) von Windows verschlüsselt wurden. Wenn EFS-Dateien von einem Mitglied der Gruppe 'Sicherungsoperatoren' zurückgeschrieben werden, werden Datum und Uhrzeit des letzten Zugriffs nicht beibehalten.

 Windows-Betriebssysteme

Erforderliche Berechtigungen zum Zurückschreiben von Dateien, die mit adaptiver Subdateisicherung verarbeitet wurden

Die adaptive Subdateisicherung ist veraltet; es ist jedoch weiterhin möglich, Subdateisicherungsdaten, die mit dem Client der Version 7.1 oder früher erstellt wurden, zurückzuschreiben. Zum Zurückschreiben von Dateien, die mithilfe der adaptiven Subdateisicherung verarbeitet wurden, muss der Benutzer der Eigner der Dateien sein oder über Lesezugriffsberechtigung verfügen.

Diese Berechtigungen kommen zu den erforderlichen Berechtigungen für eine normale Zurückschreibung hinzu.

Informationen zur adaptiven Subdateisicherung finden Sie in Sicherungen mit eingeschränkter Bandbreite ausführen in der Dokumentation des Clients für Sichern/Archivieren der Version 7.1.

 Windows-Betriebssysteme

Erforderliche Berechtigungen zum Sichern, Archivieren, Zurückschreiben oder Abrufen von Dateien auf Clusterressourcen

Wenn auf Clusterressourcen von Microsoft Cluster Server (MSCS) oder Veritas Cluster Server gespeicherte Daten gesichert, zurückgeschrieben, archiviert oder abgerufen werden sollen, muss Ihr Windows-Konto zur Gruppe 'Administratoren' oder 'Domänen-Admins' oder zur Gruppe 'Sicherungsoperatoren' gehören.

Standardmäßig haben Sicherungsoperatoren nicht die Benutzerrechte, die erforderlich sind, um diese Tasks auf einem Clusterknoten auszuführen. Sicherungsoperatoren können diese Prozedur jedoch ausführen, wenn diese Gruppe dem Sicherheitsdeskriptor für den Clusterservice hinzugefügt wird. Sie können das mithilfe des Clusteradministrators oder mit cluster.exe tun.

IBM Spectrum Protect-Clientauthentifizierung

Wenn Sie die grafische Benutzerschnittstelle oder Befehlszeilenschnittstelle des IBM Spectrum Protect-Clients verwenden, können Sie sich mit einem Knotennamen und einem Kennwort *oder* mit einer Benutzer-ID mit Administratorberechtigung und dem zugehörigen Kennwort anmelden.

Der Client fordert Sie zur Eingabe Ihrer Benutzer-ID auf und vergleicht sie mit dem konfigurierten Knotennamen. Wenn sie übereinstimmen, versucht der Client, die Benutzer-ID als Knotenname zu authentifizieren. Wenn die Authentifizierung fehlschlägt oder wenn die Benutzer-ID nicht mit dem konfigurierten Knotennamen übereinstimmt, versucht der Client, die Benutzer-ID als Benutzer-ID mit Administratorberechtigung zu authentifizieren.

Damit eine Benutzer-ID für Verwaltungsaufgaben für die Clients für Sichern/Archivieren verwendet werden kann, muss die Benutzer-ID über eine der folgenden Berechtigungen verfügen:

Systemberechtigung
: Berechtigung über das gesamte System. Ein Administrator mit Systemberechtigung kann jede Verwaltungstask ausführen.

Maßnahmenberechtigung
: Berechtigung über die Maßnahmendomäne des Knotens. Ermöglicht einem Administrator, Maßnahmenobjekte zu verwalten, Clientknoten zu registrieren und Clientoperationen für Clientknoten zu planen.

Clienteigner
: Berechtigung über den registrierten IBM Spectrum Protect-Clientknoten. Sie können über den Web-Client oder den Client für Sichern/Archivieren auf den Client zugreifen. Sie sind Eigner der Daten und haben das Recht, über Remotezugriff physisch auf die Daten zuzugreifen. Sie können Dateien auf demselben System oder einem anderen System sichern und zurückschreiben und Sie können Dateibereiche oder Archivierungsdaten löschen.

Clientzugriff
: Um den Web-Client für die Sicherung und Zurückschreibung von Dateien auf einem fernen Clientsystem verwenden zu können, müssen Sie über eine Benutzer-ID mit Administratorberechtigung verfügen, die gleichzeitig Clientzugriffsberechtigung für den Knotennamen des fernen Clientsystems hat. Wenn IBM Spectrum Protect-Administratoren mit Clientzugriffsberechtigung für Ihren Knotennamen keine Dateien auf Ihrem System sichern und zurückschreiben können sollen, geben Sie die Option revokeremoteaccess in Ihrer Clientoptionsdatei an.

  Die Clientzugriffsberechtigung ermöglicht IBM Spectrum Protect-Administratoren nur, Dateien auf fernen Systemen zu sichern und zurückzuschreiben. Sie haben keinen physischen Zugriff auf die Daten. Das heißt, sie können die Daten, die zu dem fernen System gehören, nicht auf ihr eigenes System zurückschreiben. Um Daten, die zu einem fernen System gehören, auf Ihr eigenes System zurückschreiben zu können, müssen Sie mindestens über Clienteignerberechtigung verfügen.

Verwenden Sie eine der folgenden Methoden, um festzustellen, welche Berechtigung Sie haben:

- Wählen Sie im Hauptfenster der IBM Spectrum Protect-GUI **Datei** > **Verbindungsinformationen** aus.
- Verwenden Sie den IBM Spectrum Protect-Serverbefehl QUERY ADMIN vom Verwaltungsbefehlszeilenclient aus.

Zugehörige Verweise:
Revokeremoteaccess
Befehl QUERY ADMIN
Windows-Betriebssysteme

Benutzerkontensteuerung

Die Benutzerkontensteuerung ist eine Windows-Sicherheitsfunktion, die eine Beeinträchtigung des Betriebssystems durch Malware zu verhindern hilft. Die Benutzerkontensteuerung beschränkt Programme auf Standardbenutzerberechtigungen.

Wenn die Benutzerkontensteuerung aktiviert ist, können Programme, die erhöhte Berechtigungen benötigen, nicht ohne Ihre Genehmigung ausgeführt werden.

Für den Client für Sichern/Archivieren sind erhöhte Berechtigungen erforderlich. Ein Dialogfenster der Benutzerkontensteuerung wird angezeigt, wenn Sie den Client ausführen und die Benutzerkontensteuerung aktiviert ist. Das Dialogfenster zeigt die Frage an, ob Sie die Ausführung des Programms zulassen wollen. Wenn Sie nicht als Administrator angemeldet sind, müssen Sie in dem Dialogfenster außerdem die Berechtigungsnachweise für Ihr Konto ('Anmeldeinformationen' in Windows) angeben.

- Windows-BetriebssystemeClientzugriff auf Netzfreigaben bei aktiver Benutzerkontensteuerung aktivieren
  Wenn die Windows-Benutzerkontensteuerung (User Account Control, UAC) aktiviert ist, kann der Client für Sichern/Archivieren nicht auf vorhandene Netzfreigabezuordnungen zugreifen. Die Lösung besteht in der Zuordnung der Netzfreigaben über eine Eingabeaufforderung mit erhöhten Berechtigungen, bevor Sie den Client starten.

Java-GUI-Sitzung starten

Welche Schritte zum Starten der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren ausgeführt werden, ist vom Betriebssystem abhängig.

Vorgehensweise

Führen Sie die entsprechende Prozedur für Ihr Betriebssystem zum Starten der Java™-GUI aus.

Betriebssystem	Prozedur
Mac OS X-Betriebssysteme **Mac OS X**	Mac OS X-Betriebssysteme • Doppelklicken Sie auf die Anwendung 'IBM Spectrum Protect', um den Client für Sichern/Archivieren ohne Systemadministratorberechtigungen zu starten. Wenn Sie den Client ohne Systemadministratorberechtigungen ausführen, können Sie Dateien verwalten, deren Eigner der aktuelle Benutzer ist. • Doppelklicken Sie auf IBM Spectrum Protect-Tools für Administratoren und wählen Sie IBM Spectrum Protect aus. Nach der Eingabe eines Benutzernamens und eines Kennworts für den Systemadministrator wird der Client mit Systemadministratorberechtigungen gestartet. Wenn Sie den Client mit Systemadministratorberechtigungen ausführen, können Sie Dateien verwalten, deren Eigner alle Benutzer des Systems sind. • Sie können den Client für Sichern/Archivieren auch mit dem Befehl dsmj starten. Sie können den Client entweder als Vordergrund- oder als Hintergrundprozess ausführen. Das Script dsmj wird in /Library/Application Support/tivoli/tsm/client/ba/bin installiert.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme **AIX, Linux, Solaris**	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Auf anderen UNIX-Systemen als Mac OS X muss die GUI des Clients für Sichern/Archivieren vom X Window System ausgeführt werden. Wenn das Symbol für IBM Spectrum Protect auf dem Desktop angezeigt wird, ist der Client bereits aktiv. Doppelklicken Sie auf das Symbol, um das Fenster 'IBM Spectrum Protect' zu öffnen. Wenn das Symbol für IBM Spectrum Protect auf Ihrem Desktop nicht angezeigt, starten Sie die grafische Benutzerschnittstelle des Clients für Sichern/Archivieren mit dem Befehl dsmj. Sie können den Client entweder als Vordergrund- oder als Hintergrundprozess ausführen.
Windows-Betriebssysteme **Windows**	Windows-Betriebssysteme Um die GUI des Clients für Sichern/Archivieren auf einem Windows-System zu starten, verwenden Sie eine der folgenden Methoden: • Klicken Sie auf Start > Programme > IBM Spectrum Protect > GUI für Sichern/Archivieren. • Klicken Sie auf Start > Ausführen und geben Sie den vollständigen Pfad zur Datei dsm.exe des Sicherungsclients ein. • Wechseln Sie in der Befehlszeile in das Installationsverzeichnis des Clients für Sichern/Archivieren und geben Sie dsm ein. Unter Windows-Betriebssystemen mit aktivierter Benutzerkontensteuerung werden Sie möglicherweise aufgefordert, die Ausführung des Programms dsm.exe zu ermöglichen. Damit das Programm fortgesetzt und die GUI des Clients für Sichern/Archivieren gestartet werden kann, geben Sie Verwaltungsberechtigungsnachweise ein.

Windows-BetriebssystemeDer Client für Sichern/Archivieren lokalisiert und verwendet die Optionen, die in der Clientoptionsdatei (dsm.opt) angegeben sind.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeDer Client für Sichern/Archivieren lokalisiert und verwendet die Optionen, die in der Clientsystemoptionsdatei (dsm.sys) und in der Clientoptionsdatei (dsm.opt) angegeben sind.

- IBM Spectrum Protect-Kennwort
  Der IBM Spectrum Protect-Administrator kann für die Verbindung zum Server die Eingabe eines Kennworts durch den Benutzer erforderlich machen.
- Setup-Assistent
  Wenn die grafische Benutzerschnittstelle des Clients (Client-GUI) startet, wird geprüft, ob eine Clientoptionsdatei vorhanden ist.

Zugehörige Tasks:
Windows-BetriebssystemeSprache für die Anzeige der Java-GUI konfigurieren

IBM Spectrum Protect-Kennwort

Der IBM Spectrum Protect-Administrator kann für die Verbindung zum Server die Eingabe eines Kennworts durch den Benutzer erforderlich machen.

Der IBM Spectrum Protect-Client fordert Sie zur Eingabe des Kennworts auf, falls ein Kennwort erforderlich ist. Wenden Sie sich an den IBM Spectrum Protect-Administrator, wenn Ihnen das Kennwort nicht bekannt ist.

Zugehörige Tasks:
Kennwort ändern

Setup-Assistent

Wenn die grafische Benutzerschnittstelle des Clients (Client-GUI) startet, wird geprüft, ob eine Clientoptionsdatei vorhanden ist.

Ist die Clientoptionsdatei nicht vorhanden (dies ist normalerweise der Fall, wenn Sie den Client zum ersten Mal auf Ihrem System installiert haben), startet der Setup-Assistent automatisch und führt Sie durch den Konfigurationsprozess.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDie Clientoptionsdatei ist die Datei dsm.sys.

Windows-BetriebssystemeSie können den Setup-Assistenten jederzeit starten, um Ihre Clientoptionsdatei zu ändern.

Windows-BetriebssystemeDie Clientoptionsdatei ist die Datei dsm.opt.

Befehlszeilensitzung starten

Sie können eine Befehlszeilensitzung starten, indem Sie den Befehl dsmc aufrufen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAnmerkung: Wenn das Verzeichnis `/usr/bin` eine symbolische Verbindung zu der ausführbaren IBM Spectrum Protect-Datei enthält und alle DSM-Umgebungsvariablen definiert sind, können Sie den Befehl dsmc in jedem Verzeichnis eingeben. Andernfalls geben Sie den vollständig qualifizierten Pfad des Befehls ein.
Mac OS X-BetriebssystemeAnmerkung: Unter Mac OS X können Systemadministratoren mit dem Befehl sudo weitere Berechtigungen erhalten, sodass der Client für Sichern/Archivieren auf Dateien für alle Benutzer im System zugreifen kann.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeGeben Sie in der Befehlszeile dsmc gefolgt von dem Befehl ein *(Stapelmodus)*. Wenn das Verzeichnis `/usr/bin` oder `opt/bin` eine symbolische Verbindung zum IBM Spectrum Protect-Installationsverzeichnis enthält, können Sie den Befehl dsmc in jedem Verzeichnis eingeben. Andernfalls können Sie den vollständig qualifizierten Namen eingeben.

Windows-BetriebssystemeAnmerkung: Wenn die Umgebungsvariable PATH auf das Clientinstallationsverzeichnis gesetzt ist, können Sie den Befehl dsmc in jedem Verzeichnis eingeben; geben Sie andernfalls den vollständig qualifizierten Pfad ein.

Der Client kann nur mit dem Befehl "dsmc" gestartet werden, wenn die Umgebungsvariable PATH mit dem Pfad zu der Clientposition aktualisiert wurde.

Windows-BetriebssystemeSie können das Windows-Menü Start öffnen und Programme > IBM Spectrum Protect > Befehlszeile für Sichern/Archivieren auswählen.

Der IBM Spectrum Protect-Administrator kann für die Verbindung zum Server die Eingabe eines Kennworts durch den Benutzer erforderlich machen. Der Client fordert Sie zur Eingabe des Kennworts auf, falls ein Kennwort erforderlich ist. Wenden Sie sich an Ihren Administrator, wenn Ihnen das Kennwort nicht bekannt ist.

- Stapelmodus verwenden
  Verwenden Sie den *Stapelmodus*, um einen einzelnen Clientbefehl einzugeben. Bei Verwendung des Stapelmodus muss dem Befehl die Zeichenfolge **dsmc** vorausgehen.
- Folge von Befehlen im interaktiven Modus ausgeben
  Der *interaktive* Modus (Dialogmodus) wird verwendet, wenn eine Reihe von Befehlen ausgegeben werden soll.
- Windows-BetriebssystemeEuro-Zeichen bei einer Eingabeaufforderung anzeigen
  In diesem Abschnitt wird erläutert, wie das Euro-Zeichen bei der Windows-Eingabeaufforderung (im Konsolfenster) angezeigt wird.
- Windows-BetriebssystemeOptionen im Befehl DSMC verwenden
  Dieser Abschnitt enthält einige Beispiele für die Verwendung von Optionen im Befehl dsmc.

Zugehörige Konzepte:
Windows-BetriebssystemeOperationen des Clients für Sichern/Archivieren und Sicherheitsberechtigungen
Optionen im interaktiven Modus
Windows-BetriebssystemeClientbefehlssitzung starten und beenden
Mac OS X-BetriebssystemeTasks für Rootbenutzer und berechtigte Benutzer UNIX- und Linux-Clients
Befehle verwenden

Stapelmodus verwenden

Verwenden Sie den *Stapelmodus*, um einen einzelnen Clientbefehl einzugeben. Bei Verwendung des Stapelmodus muss dem Befehl die Zeichenfolge **dsmc** vorausgehen.

Informationen zu diesem Vorgang

Soll beispielsweise der Befehl incremental ausgegeben werden, geben Sie bei der Eingabeaufforderung Folgendes ein:

```
dsmc incremental
```

Einige Befehle erfordern ein Argument oder mehrere Argumente. Beispiel: Der Befehl zum Archivieren einer Datei:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc archive /home/proj1/file1.txt
```

Windows-Betriebssysteme

```
dsmc archive c:\myfiles\file1.dat
```

Abhängig von der aktuellen Einstellung der Option passwordaccess fordert der Client Sie möglicherweise zur Eingabe Ihres Kennworts auf, bevor der Befehl in einer Sitzung im Stapelmodus verarbeitet wird.

Wenn Sie Ihr Kennwort eingeben, wird das Kennwort nicht am Bildschirm angezeigt.

Zugehörige Verweise:
Passwordaccess

Folge von Befehlen im interaktiven Modus ausgeben

Der *interaktive* Modus (Dialogmodus) wird verwendet, wenn eine Reihe von Befehlen ausgegeben werden soll.

Informationen zu diesem Vorgang

Die Verbindung zum Server wird im interaktiven Modus nur einmal hergestellt, sodass eine Folge von Befehlen im interaktiven Modus schneller verarbeitet werden kann als im Stapelmodus.

Damit eine Clientbefehlssitzung im interaktiven Modus gestartet wird, muss einer der beiden folgenden Befehle eingegeben werden:

- `dsmc`
- `dsmc loop`

Die folgende Eingabeaufforderung wird auf Ihrem Bildschirm angezeigt:

```
Protect>
```

Windows-BetriebssystemeWenn Sie sich mit einer Administrator-ID anmelden, können Sie Tasks für Standardbenutzer ausführen. . Sind Sie nicht angemeldet, wenn Sie eine Task über ein Fenster mit Eingabeaufforderung starten, werden Sie zur Anmeldung aufgefordert. .

Im interaktiven Modus darf den Befehlen nicht die Zeichenfolge dsmc vorangestellt werden. Beispielsweise wird zum Archivieren einer Datei dann nicht dsmc archive, sondern nur **archive** eingegeben.

Soll beispielsweise eine Datei archiviert werden, geben Sie den Befehl mit der Dateispezifikation ein:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
archive /home/proj1/file1.txt
```

Windows-Betriebssysteme

```
archive c:\myfiles\file1.dat
```

Abhängig von der aktuellen Einstellung der Option passwordaccess fordert der Client Sie möglicherweise zur Eingabe Ihres Kennworts auf, bevor die Eingabe des Befehls in einer interaktiven Sitzung zulässig ist.

Wenn Sie Ihr Kennwort eingeben, wird das Kennwort nicht am Bildschirm angezeigt.

Windows-Betriebssysteme

Euro-Zeichen bei einer Eingabeaufforderung anzeigen

In diesem Abschnitt wird erläutert, wie das Euro-Zeichen bei der Windows-Eingabeaufforderung (im Konsolfenster) angezeigt wird.

Vorgehensweise

1. Wenden Sie sich an Ihren Ansprechpartner bei Microsoft und bitten Sie ihn um die Codepage 858 (Dateiname `c_858.nls`). Kopieren Sie die Datei in Ihr Windows-Verzeichnis system32 (beispielsweise `C:\WINNT\system32`).
2. Editieren Sie den Windows-Registrierungsschlüssel mit dem folgenden Befehl: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage\850`. Setzen Sie ihn auf den Wert `c_858.nls`. **Änderungen, die Sie mit dem Editor für die Windows-Registrierung vornehmen, können nicht rückgängig gemacht werden**. Fehler beim Editieren der Windows-Registrierung können dazu führen, dass das System nicht mehr funktioniert, und sogar bewirken, dass das System nicht mehr gestartet werden kann. **Gehen Sie sehr vorsichtig vor**, wenn Sie die Windows-Registrierung editieren. Wenn Sie mit dem Editor für die Windows-Registrierung nicht vertraut sind, sollten Sie jemanden um Hilfe bitten, der sich mit dem Editor für die Windows-Registrierung auskennt.
3. Wählen Sie in den regionalen Einstellungen ein westeuropäisches Land (Deutschland, Frankreich, Italien etc.) als Ländereinstellung aus.
4. Verlassen Sie die Datei und führen Sie einen Warmstart durch.

Ergebnisse

Stellen Sie sicher, dass die von Ihnen verwendete Konsolfensterschriftart das Euro-Symbol unterstützt (beispielsweise Lucida Console).

Windows-Betriebssysteme

Optionen im Befehl DSMC verwenden

Dieser Abschnitt enthält einige Beispiele für die Verwendung von Optionen im Befehl dsmc.

Informationen zu diesem Vorgang

Angenommen, Sie haben eine Workstation mit dem Knotennamen `galaxy1` und eine weitere Workstation mit dem Knotennamen `galaxy2`. Sie möchten die Daten von `galaxy1` auf das System `galaxy2` zurückschreiben. Um eine Datei von einer Workstation (`galaxy1`) wiederherstellen zu können, während Sie an der anderen Workstation (`galaxy2`) angemeldet sind, benötigen Sie Zugriff auf `galaxy1`. Verwenden Sie den Befehl set access, um Zugriff zu erhalten.

Beispiel: Der Name der Datei, die auf `galaxy1` wiederhergestellt werden soll, lautet `c:\universe\saturn.planet`. Der Eigner von `galaxy1` gibt folgenden Befehl ein:

```
dsmc set access archive c:\universe\saturn.planet galaxy2
```

Wenn die Zugriffsberechtigung erteilt wurde, können Sie die Datei abrufen, indem Sie den folgenden Befehl eingeben:

```
dsmc retrieve -fromnode=galaxy1 \\galaxy1\universe\saturn.planet c:\
```

Anmerkung: Der Zugriff auf die Dateien eines anderen Benutzers kann auch über die grafische Benutzerschnittstelle (GUI) ermöglicht werden. Wenn Sie in Ihrem Unternehmen über mehrere Sicherungsserver verfügen, können Sie problemlos zwischen den Servern hin- und herschalten, indem Sie mit einer Befehlszeilenoption arbeiten. Um den in dsm.opt angegebenen Server zu überschreiben, könnten Sie einen Befehl wie beispielsweise den folgenden verwenden:

```
dsmc -tcpserveraddress=myserver -node=mynode -tcpport=1599
```

Zugehörige Verweise:
Fromnode
Set Access

Eingabezeichenfolgen angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthalten

Sie müssen bestimmte Regeln einhalten, wenn Sie eine Eingabezeichenfolge angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthält.

Halten Sie die folgenden Regeln ein, wenn Sie eine Eingabezeichenfolge angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthält:

- Enthält die Eingabezeichenfolge mindestens ein Leerzeichen, schließen Sie die Zeichenfolge in Hochkommas oder Anführungszeichen ein. Sie können Hochkommas oder Anführungszeichen verwenden, sie müssen jedoch paarig angegeben werden.
- Enthält die Eingabezeichenfolge ein Hochkomma, schließen Sie die Zeichenfolge, wie im folgenden Beispiel gezeigt, in Anführungszeichen ein:

  ```
  -description="Annual backup of the accounting department's monthly reports"
  ```

- Enthält die Eingabezeichenfolge ein Anführungszeichen, schließen Sie die Zeichenfolge, wie im folgenden Beispiel gezeigt, in Hochkommas ein:

  ```
  -description='Neue Übersetzungen von "Odyssee" und "Ilias"'
  ```

- Enthält die Eingabezeichenfolge Leerzeichen und Hochkommas oder Anführungszeichen, schließen Sie die Zeichenfolge in Hochkommas bzw. Anführungszeichen ein. Dabei dürfen die Hochkommas oder Anführungszeichen am Anfang und am Ende der Zeichenfolge nicht identisch mit den Hochkommas oder Anführungszeichen innerhalb der Zeichenfolge sein.

Einschränkung: Eine Eingabezeichenfolge, die Hochkommas und Anführungszeichen enthält, ist keine gültige Eingabezeichenfolge.

Die folgenden Regeln gelten für diese Datentypen:

- Vollständig qualifizierte Namen.
- Die Beschreibung (description), die Sie im Befehl archive angeben.
- Einen beliebigen Wert für einen Optionswert, wobei die Zeichenfolge Leerzeichen oder Anführungszeichen enthalten kann.

Wichtig: In Eingabezeichenfolgen können Sie keine Escapezeichen verwenden. Escapezeichen werden ebenso wie alle anderen Zeichen behandelt. Im Folgenden finden Sie einige Beispiele, in denen Escapezeichen nicht erkannt werden:

- Wenn die Zeichenfolge sich in einer Optionsdatei befindet.
- Wenn die Zeichenfolge sich in einer Listendatei befindet.
- Wenn die Zeichenfolge im interaktiven Modus eingegeben wird.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Weitere Hinweise zum Starten

Optionen können als Argumente in den Befehlen **dsmj** und **dsmc** angegeben werden. Mithilfe von Optionen kann beispielsweise das für die Anzeige von Datum, Uhrzeit und Zahlen verwendete Format geändert werden oder das Kennwort eingeschlossen werden, sodass der Client für Sichern/Archivieren nicht zur Eingabe des Kennworts auffordert.

Informationen zu diesem Vorgang

Wenn Sie mehrere Server in dsm.sys definiert haben und auf einen anderen (als den in Ihrer Clientbenutzeroptionsdatei dsm.opt definierten) Server für Sicherungs-/Archivierungsservices zugreifen möchten, können Sie darüber hinaus mit der Option servername diesen Server angeben.

Beispiel:

```
dsmj -servername=server_b
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie Java™-GUI (dsmj) akzeptiert Befehlszeilenparameter wie die Java-X-Optionen. Daher ist es jetzt auch möglich, die Größe des Java-Heapspeichers zu ändern. Beispiel:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmj -Xmx512M
```

Web-Client in neuer Sicherheitsumgebung verwenden

Ab IBM Spectrum Protect Version 8.1.2 können Sie nicht mehr den Web-Client verwenden, um eine Verbindung zum IBM Spectrum Protect-Server der Version 8.1.2 oder höher herzustellen.

Sie können den Web-Client jedoch weiterhin verwenden, um eine Verbindung zu Servern mit IBM Spectrum Protect Version 8.1.1, Version 8.1.0, Version 7.1.7 oder früheren Versionen herzustellen.

Wenn eine Verbindung zu dem IBM Spectrum Protect-Server der Version 8.1.2 oder höher besteht, verwenden Sie die folgenden Alternativen für den Web-Client:

- Um Daten zurückzuschreiben, die mit dem Client für Sichern/Archivieren gesichert wurden, verwenden Sie die Java-GUI des Clients für Sichern/Archivieren (dsmj) oder den Befehlszeilenclient (dsmc).Weitere Informationen finden Sie in:
  - Daten sichern
  - Daten zurückschreiben
- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeSollen NAS-Dateiserver unter Verwendung von NDMP (Network Data Management Protocol) gesichert und zurückgeschrieben werden, verwenden Sie die IBM Spectrum Protect-Serverbefehle im Verwaltungsbefehlszeilenclient (dsmadmc).
  Weitere Informationen finden Sie in der folgenden Serverdokumentation:
  - NAS-Dateiserver schützen
  - NAS-Dateiserver mithilfe von NDMP sichern und zurückschreiben
  - Sicherung und Zurückschreibung auf Dateiebene für NDMP-Operationen
- Web-Client-Sitzung starten
  Der Web-Client ist eine Java™ Web Start-Anwendung, die unabhängig von der Web-Browser-Software gestartet und verwaltet werden kann. Nach der Installation und Konfiguration des Web-Clients auf Ihrer Workstation können Sie den Web-Client für den Fernzugriff verwenden, um Daten auf dem Clientknoten über Fernzugriff zu sichern, zurückzuschreiben, zu archivieren oder abzurufen. Der Web-Client erleichtert die Verwendung von Einheiten für behindertengerechte Bedienung für Benutzer mit Behinderungen und bietet eine verbesserte Navigation über die Tastatur.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Client-Scheduler automatisch starten

Sie können den Client-Scheduler beim Start Ihrer Workstation automatisch starten.

Hat der IBM Spectrum Protect-Administrator Zeitpläne für Ihren Knoten definiert, können Sie nach dem Starten des Client-Schedulers die Workstation automatisch sichern (oder andere geplante Aktionen ausführen).

Sie können auch den IBM Spectrum Protect-Clientakzeptorservice zum Verwalten des Schedulers verwenden.

Windows-BetriebssystemeIBM Spectrum Protect unterstützt ferne Netzverbindungen zum Server. Mit einer fernen Netzverbindung müssen mobile Benutzer sich nicht mehr für eine geplante Sicherung in ihr Firmennetz einwählen. IBM Spectrum Protect stellt vor dem Zeitpunkt der geplanten Sicherung automatisch eine Verbindung her. Wenn die Verbindung fehlschlägt, wird sie von IBM Spectrum Protect erneut hergestellt, bevor die Durchführung der Sicherung versucht wird.

Zugehörige Tasks:
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren

Kennwort ändern

Der IBM Spectrum Protect-Administrator kann für die Verbindung zum Server die Eingabe eines Kennworts durch den Benutzer erforderlich machen.

Informationen zu diesem Vorgang

Der Client für Sichern/Archivieren fordert Sie zur Eingabe des Kennworts auf, falls ein Kennwort erforderlich ist. Wenden Sie sich an den IBM Spectrum Protect-Administrator, wenn Ihnen das Kennwort nicht bekannt ist.

Wichtig: Das Kennwort, das Thema dieses Abschnitts ist, unterscheidet sich von dem Kennwort für die Verschlüsselung von Dateien.

Die Änderung des Kennworts über die grafische Benutzerschnittstelle wird wie folgt vorgenommen:

Vorgehensweise

1. Mac OS X-BetriebssystemeStarten Sie auf Mac OS X-Clients den Client für Sichern/Archivieren mit den IBM Spectrum Protect-Tools für Administratoren.
2. AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeÖffnen Sie im Hauptfenster das Menü **Dienstprogramme** und wählen Sie **Kennwort ändern** aus.
3. Geben Sie das aktuelle und das neue Kennwort ein und geben Sie danach im Feld **Kennwort bestätigen** das neue Kennwort nochmals ein.
4. Klicken Sie auf **Ändern**.

Ergebnisse

Zum Ändern des Kennworts über den Befehlszeilenclient geben Sie den folgenden Befehl ein:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Für UNIX-, Linux- und Windows-Clients:

```
dsmc set password
```

Mac OS X-BetriebssystemeFür Mac OS X-Clients geben Sie den folgenden Befehl ein, um Ihr Kennwort über den Befehlszeilenclient zu ändern:

```
sudo dsmc set password
```

Geben Sie dann nach entsprechender Aufforderung das alte und das neue Kennwort ein.

Die maximale Kennwortlänge beträgt 63 Zeichen. Kennwortbedingungen variieren, abhängig davon, wo die Kennwörter gespeichert und verwaltet werden, und abhängig von der Version des IBM Spectrum Protect-Servers, zu dem Ihr Client die Verbindung herstellt.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden

Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Bei den Kennwörtern muss die Groß-/Kleinschreibung beachtet werden. Außerdem können die Kennwörter weiteren Einschränkungen aufgrund von LDAP-Richtlinien unterliegen.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie keinen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden

Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Kennwörter werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

Wenn Ihr IBM Spectrum Protect-Server eine Version vor Version 6.3.3 aufweist
Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
_ - & + .
```

Kennwörter werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Hinweis:

Schließen Sie in der Befehlszeile alle Parameter, die mindestens ein Sonderzeichen enthalten, in Anführungszeichen ein. Ohne Anführungszeichen können die Sonderzeichen als Shell-Escapezeichen, als Dateiumleitungszeichen oder als andere Zeichen, die eine Bedeutung für das Betriebssystem haben, interpretiert werden.

Windows-Betriebssysteme

Auf Windows-Systemen:
Schließen Sie die Befehlsparameter in Anführungszeichen (") ein.

Beispiel für die Befehlszeile:

```
dsmc set password "t67@#$%^&" "pass2><w0rd"
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Auf AIX-, Linux- und Solaris-Systemen:
Schließen Sie die Befehlsparameter in Hochkommas (') ein.

Beispiel für die Befehlszeile:

```
dsmc set password -type=vmguest 'Win 2012 SQL' 'tsml2dag\administrator' '7@#$%^&7'
```

Anführungszeichen sind nicht erforderlich, wenn Sie ein Kennwort mit Sonderzeichen in einer Optionsdatei eingeben.

Zugehörige Konzepte:
Client-Scheduler automatisch starten
Zugehörige Tasks:
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWeitere Hinweise zum Starten
Zugehörige Verweise:
Password
Set Password

Dateilisten mithilfe der GUI des Clients für Sichern/Archivieren sortieren

Mithilfe der GUI des Clients für Sichern/Archivieren können Sie Dateien anzeigen, sortieren oder auswählen.

Informationen zu diesem Vorgang

Tabelle 1. Über die GUI des Clients für Sichern/Archivieren mit Ihren Dateien arbeiten

Task	Prozedur
Dateien anzeigen	Zum Anzeigen von Dateien in einem Verzeichnis klicken Sie auf das Ordnersymbol neben dem Verzeichnisnamen. Die Dateien werden im Fenster Dateiliste rechts angezeigt.
Dateiliste sortieren	• Klicken Sie auf die entsprechende Spaltenüberschrift im Fenster Dateiliste.
Aktive und inaktive Sicherungsversionen anzeigen	• Klicken Sie auf die Option Aktive/inaktive Dateien anzeigen im Menü Sicht. • Klicken Sie in der Funktionsleiste auf das Tool Aktive und inaktive Dateien anzeigen.
Nur aktive Sicherungsversionen anzeigen	Klicken Sie auf die Option Nur aktive Dateien anzeigen im Menü Sicht.
Dateien zum Zurückschreiben oder Abrufen auswählen	• Klicken Sie auf das Auswahlfeld neben dem Verzeichnis, das Sie zurückschreiben oder abrufen wollen. • Heben Sie die Dateien hervor, die Sie zurückschreiben oder abrufen wollen, und klicken Sie auf das Tool Einträge auswählen in der Funktionsleiste. • Heben Sie die Dateien hervor, die Sie zurückschreiben oder abrufen wollen, und klicken Sie auf die Option Einträge auswählen im Menü Editieren.

Task	Prozedur
Auswahl von Dateien zurücknehmen	• Klicken Sie auf das markierte Auswahlfeld neben dem Verzeichnis oder Dateinamen. • Heben Sie die Dateien hervor, deren Auswahl Sie zurücknehmen wollen, und klicken Sie auf das Tool Auswahl der Einträge zurücknehmen in der Funktionsleiste. • Heben Sie die Dateien hervor, deren Auswahl Sie zurücknehmen wollen, und klicken Sie auf die Option Auswahl der Einträge zurücknehmen im Menü Editieren.
Dateiinformationen anzeigen	• Heben Sie den Dateinamen hervor und klicken Sie auf die Schaltfläche Dateiinformationen anzeigen in der Funktionsleiste. • Heben Sie den Dateinamen hervor und klicken Sie auf Dateiinformationen im Menü Sicht.

Anmerkung:

1. Falls nicht anders angegeben, gelten die in der oben stehenden Tabelle enthaltenen Tasks und Prozeduren für alle Client-GUIs.
2. Mithilfe der Client-GUIs können Sie eine Liste der Dateien nach verschiedenen Attributen wie Name, Verzeichnis, Größe oder Änderungsdatum sortieren. Das Sortieren von Dateien nach dem Datum der letzten Sicherung kann sehr nützlich zum Bestimmen des Datums und der Uhrzeit für das Zurückschreiben nach Zeitpunkt sein.
3. Eine *aktive* Datei ist die letzte (jüngste) Sicherungsversion einer Datei, die bei der letzten Sicherung auf der Workstation des Benutzers vorhanden war. Alle anderen Sicherungsversionen dieser Datei sind *inaktiv*. Es werden nur aktive Sicherungsversionen von Dateien angezeigt, sofern Sie nicht die Menüoption Aktive/inaktive Dateien anzeigen ausgewählt haben. Wird die Datei aus der Workstation gelöscht, wird die aktive Version bei der nächsten Teilsicherung inaktiv.

   Im Befehlszeilenclient können Sie query-Befehle mit der Option inactive verwenden, um sowohl aktive als auch inaktive Objekte anzuzeigen. Sie können restore-Befehle mit den Optionen 'pick' und 'inactive' verwenden, um eine Liste der aktiven und inaktiven Sicherungen anzuzeigen, aus denen Sie auswählen können.

Zugehörige Verweise:
Inactive
Pick

Onlinehilfe anzeigen

Zum Anzeigen der Onlinehilfe stehen die folgenden Möglichkeiten zur Verfügung: in der GUI des Clients für Sichern/Archivieren, über den Web-Client oder über die dsmc-Befehlszeile.

Informationen zu diesem Vorgang

- In der GUI des Clients für Sichern/Archivieren:
  - Öffnen Sie das Hilfemenü. Klicken Sie auf Hilfe oder drücken Sie die Taste F1.
  - Klicken Sie auf die Schaltfläche Hilfe im aktuellen Fenster.
  - Mac OS X-BetriebssystemeKlicken Sie auf Mac-Systemen auf das Fragezeichen (?) in der GUI. Daraufhin werden Onlineinformationen zur aktuellen Operation angezeigt.
- Über die dsmc-Befehlszeile: Geben Sie den Befehl help ein. Das vollständige Inhaltsverzeichnis für den verfügbaren Hilfetext wird angezeigt.

Zugehörige Verweise:
Help

Sitzung beenden

Sie können eine Clientsitzung über die GUI des Clients für Sichern/Archivieren oder die dsmc-Befehlszeile beenden.

Informationen zu diesem Vorgang

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

- Über die GUI des Clients für Sichern/Archivieren:
  - Mac OS X-BetriebssystemeÖffnen Sie das Menü Datei und wählen Sie Beenden aus.
  - Mac OS X-BetriebssystemeDrücken Sie Befehl+Q.
  - AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeÖffnen Sie das Menü Datei und wählen Sie Ende aus.
  - Windows-BetriebssystemeKlicken Sie auf das Symbol X in der oberen rechten Ecke.
  - AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeÖffnen Sie das Menü System und wählen Sie Schließen aus.
  - Windows-BetriebssystemeDrücken Sie die Tasten `Alt+F4`.
  - AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeFür den Web-Client: Öffnen Sie eine andere URL oder schließen Sie den Browser.

- Über die DSMC-Befehlszeile:
  - Im Stapelmodus stellt jeder Befehl dsmc, den Sie eingeben, eine vollständige Sitzung dar. Der Client beendet die Sitzung, wenn die Verarbeitung des Befehls beendet ist.
  - Um eine interaktive Sitzung zu beenden, geben Sie quit bei der Eingabeaufforderung `Protect>` ein.
  - Soll ein Befehl dsmc abgebrochen werden, bevor der Client die Verarbeitung beendet hat, geben Sie `QQ` an der IBM Spectrum Protect-Konsole ein. In vielen, aber nicht in allen Fällen wird der Befehl dadurch abgebrochen. Kann der Befehl nicht abgebrochen werden, geben Sie den UNIX-Befehl kill -9 über eine verfügbare Eingabeaufforderung ein. Sie dürfen nicht Strg-C drücken oder den UNIX-Befehl kill -15 verwenden, da dies zu unerwarteten Ergebnissen führen kann.

 Windows-Betriebssysteme

- Über das Hauptfenster der GUI des Clients für Sichern/Archivieren:
  - Klicken Sie auf Datei > Ende.
  - Drücken Sie die Tasten `Alt-X`.
  - Für den Web-Client: Öffnen Sie eine andere URL oder schließen Sie den Browser.
- Über die DSMC-Befehlszeile:
  - Im Stapelmodus stellt jeder Befehl dsmc, den Sie eingeben, eine vollständige Sitzung dar. Der Client beendet die Sitzung, wenn die Verarbeitung des Befehls beendet ist.
  - Um eine interaktive Sitzung zu beenden, geben Sie `quit` bei der Eingabeaufforderung `protect>` ein.
  - Soll ein Befehl dsmc abgebrochen werden, bevor der Client die Verarbeitung beendet hat, geben Sie `QQ` an der IBM Spectrum Protect-Konsole ein. In vielen, aber nicht in allen Fällen wird der Befehl dadurch abgebrochen. Kann der Befehl nicht abgebrochen werden, verwenden Sie den Windows-Task-Manager, um den Prozess dsmc zu beenden. Verwenden Sie nicht Strg-C, da diese Tastenkombination zwar die Sitzung beendet, jedoch auch zu unerwarteten Ergebnissen führen kann.

Zugehörige Verweise:
Loop

Onlineforen

Um an Benutzerdiskussionen zu IBM Spectrum Protect-Produkten teilnehmen zu können, können Sie eine Subskription für den Listenserver ADSM-L beantragen.

Informationen zu diesem Vorgang

Dieses Benutzerforum wird vom Marist College gepflegt. Obwohl es nicht offiziell von IBM® unterstützt wird, nehmen Produktentwickler und andere Mitarbeiter des IBM Support auf informeller Basis ebenfalls an diesem Forum teil und bemühen sich, Ihre Fragen bestmöglich zu beantworten. Da dieses Forum kein offizieller IBM Unterstützungskanal ist, sollten Sie sich an die technische Unterstützung von IBM wenden, falls Sie eine Antwort direkt von IBM benötigen. Andernfalls gibt es keine Garantie dafür, dass sich IBM um Ihr Anliegen kümmert, wenn Sie eine Frage auf den Listenserver gestellt haben.

Sie können sich beim Listenserver registrieren lassen, indem Sie eine E-Mail an folgende Adresse senden:

```
listserv@vm.marist.edu
```

Der Hauptteil der Nachricht muss Folgendes enthalten:

```
SUBSCRIBE ADSM-L vorname nachname
```

Der Listenserver sendet Ihnen eine Antwort, in der Sie aufgefordert werden, die Subskriptionsanforderung zu bestätigen. Sobald Sie die Subskriptionsanforderung bestätigt haben, sendet Ihnen der Listenserver weitere Anweisungen. Danach können Sie Nachrichten auf den Listenserver stellen, indem Sie eine E-Mail an folgende Adresse senden:

```
ADSM-L@vm.marist.edu
```

Wenn Sie zu einem späteren Zeitpunkt die Subskription für ADSM-L aufheben möchten, können Sie eine Nachricht an folgende E-Mail-Adresse senden:

```
listserv@vm.marist.edu
```

Der Hauptteil der Nachricht muss Folgendes enthalten:

```
SIGNOFF ADSM-L
```

Sie können außerdem die ADSM-L-Archive lesen und durchsuchen, sich Diskussionsforen anschließen und auf andere Ressourcen unter folgender URL zugreifen:

```
http://www.adsm.org
```

Daten mit Clients für Sichern/Archivieren sichern und zurückschreiben

Wenn Sie eine Kopie einer Datei von Ihrem Computer auf dem IBM Spectrum Protect-Server sichern wollen, verwenden Sie die Funktion *Sichern*. Falls die Originaldatei beschädigt wird oder verloren geht, können Sie die Sicherungsversion vom Server *zurückschreiben*.

- Daten sichern
  Verwenden Sie den Client für Sichern/Archivieren, um Sicherungsversionen Ihrer Dateien auf dem IBM Spectrum Protect-Server zu speichern. Sie können diese Sicherungsversionen zurückschreiben, wenn die ursprünglichen Dateien verloren gegangen oder beschädigt sind.
- Daten zurückschreiben
  Mit IBM Spectrum Protect können Sicherungsversionen bestimmter Dateien, einer Gruppe von Dateien mit ähnlichen Namen oder vollständiger Verzeichnisse zurückgeschrieben werden.

Daten sichern

Verwenden Sie den Client für Sichern/Archivieren, um Sicherungsversionen Ihrer Dateien auf dem IBM Spectrum Protect-Server zu speichern. Sie können diese Sicherungsversionen zurückschreiben, wenn die ursprünglichen Dateien verloren gegangen oder beschädigt sind.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeAlle Sicherungs- und Zurückschreibungsprozeduren des Clients gelten auch für den Web-Client.
Einschränkung: Der Web-Client stellt keinen Profileditor zum Definieren von Clientoptionen bereit.
Windows-BetriebssystemeAlle Sicherungs- und Zurückschreibungsprozeduren des Clients gelten auch für den Web-Client.
Einschränkung: Der Web-Client stellt keinen Profileditor zum Definieren von Clientoptionen bereit. Auf Windows-Clients bietet der Web-Client keinen Setup-Assistenten an, der in der GUI des Clients für Sichern/Archivieren verfügbar ist. Der Web-Client kann keine Netzressourcen durchsuchen.

Windows-BetriebssystemeSofern nicht anders angegeben, beziehen sich Verweise auf Windows auf alle unterstützten Windows-Betriebssysteme.

Windows-BetriebssystemeDer Client stellt Sicherungs- und Archivierungsservices für alle Dateien in den folgenden Dateisystemen bereit: FAT (File Allocation Table), FAT 32, NTFS und ReFS.

Es folgt eine Liste der primären Sicherungstasks.

- Windows-BetriebssystemeSicherungen planen (Windows)
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSicherungen planen
- Windows-BetriebssystemeHinweise vor der Sicherung (Windows)
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeHinweise vor der Sicherung (UNIX und Linux)
- Windows-BetriebssystemeTeilsicherung, selektive Sicherung oder Teilsicherung nach Datum (Windows)
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTeilsicherung, selektive Sicherung oder Teilsicherung nach Datum ausführen (UNIX und Linux)
- Windows-BetriebssystemeSicherungsdaten löschen
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSicherungsdaten löschen
- Windows-BetriebssystemeDateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (Windows)
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (UNIX und Linux)
- Windows-BetriebssystemeWindows-Systemstatus sichern
- Windows-BetriebssystemeDateien für automatische Systemwiederherstellung sichern
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeImagesicherung
- NAS-Dateisysteme mit Network Data Management Protocol sichern
- Windows-BetriebssystemeUmgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten
- Windows-BetriebssystemeVirtuelle Maschinen auf einem Hyper-V-System sichern
- Windows-BetriebssystemeNet Appliance-CIFS-Freigabedefinition sichern

- Windows-BetriebssystemeSicherungen planen (Windows)
  Als Erstbenutzer bzw. als Benutzer, der nur gelegentlich Dateien sichert, können Sie die Tabelle in diesem Abschnitt als Prüfliste für die Schritte verwenden, die vor einer Sicherung auszuführen sind.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSicherungen planen
  Als Erstbenutzer bzw. als Benutzer, der nur gelegentlich Dateien sichert, können Sie die Tabelle in diesem Abschnitt als Prüfliste für die Schritte verwenden, die vor einer Sicherung auszuführen sind.
- Welche Dateien werden gesichert?
  Wenn Sie eine Sicherung anfordern, sichert der Client eine Datei, wenn bestimmte Voraussetzungen erfüllt sind.
- Windows-BetriebssystemeUnterstützung offener Dateien für Sicherungsoperationen
  Der VSS-Momentaufnahmeprovider wird für die Unterstützung offener Dateien verwendet.
- Windows-BetriebssystemeDaten über die GUI sichern
  Mithilfe der GUI des Clients für Sichern/Archivieren können Sie bestimmte Dateien, eine Gruppe von Dateien mit ähnlichen Namen oder vollständige Verzeichnisse sichern.
- Windows-BetriebssystemeDaten über die Befehlszeile sichern
  Sie können Sicherungen mit dem Befehl incremental oder selective ausführen. Die folgende Tabelle enthält Beispiele zur Verwendung von Befehlen zum Ausführen verschiedener Tasks.
- Windows-BetriebssystemeSicherungsdaten löschen
  Wenn Sie vom Administrator entsprechend berechtigt wurden, können Sie einzelne Sicherungskopien aus dem IBM Spectrum Protect-

Server löschen, ohne den gesamten Dateibereich zu löschen.

- Wann werden Dateien gesichert und wann archiviert?
  Wenn der Client für Sichern/Archivieren eine Datei sichert oder archiviert, werden eine Kopie der Datei und die zugehörigen Attribute an den Server gesendet. Sicherungs- und Archivierungsoperationen dienen jedoch unterschiedlichen Zwecken.
-  Hinweise vor der Sicherung (Windows)
  Verschiedene Faktoren in Ihrem System oder Ihrer Umgebung können sich auf die Art und Weise auswirken, wie der Client für Sichern/Archivieren Daten verarbeitet. Lesen Sie diese Hinweise, bevor Sie Ihre Daten sichern.
-    Hinweise vor der Sicherung (UNIX und Linux)
  Verschiedene Faktoren in Ihrem System oder Ihrer Umgebung können sich auf die Art und Weise auswirken, wie der Client für Sichern/Archivieren Daten verarbeitet. Lesen Sie diese Hinweise, bevor Sie Ihre Daten sichern.
-  Teilsicherung, selektive Sicherung oder Teilsicherung nach Datum (Windows)
  Der Administrator kann Zeitpläne definieren, durch die Dateien automatisch gesichert werden. In diesem Abschnitt wird die Sicherung von Dateien ohne Zeitpläne beschrieben.
-    Teilsicherung, selektive Sicherung oder Teilsicherung nach Datum ausführen (UNIX und Linux)
  Der Administrator kann Zeitpläne definieren, durch die Dateien auf Ihrer Workstation automatisch gesichert werden. In den folgenden Abschnitten wird die Sicherung von Dateien ohne Zeitpläne beschrieben.
-  Dateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (Windows)
  Verwenden Sie den Befehl backup group, um eine Gruppe, aus einer Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen zu erstellen und in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server zu sichern.
-    Dateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (UNIX und Linux)
  Mit dem Befehl backup group können Sie eine Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen enthält, erstellen und in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server sichern.
-  Daten mit der Unterstützung für den Clientknoten-Proxy sichern (Windows)
  Sicherungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.
-    Daten mit der Unterstützung für den Clientknoten-Proxy sichern (UNIX und Linux)
  Sicherungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.
-  Lokale Momentaufnahme einem Serverdateibereich zuordnen (Windows)
  Verwenden Sie die Option snapshotroot in den Befehlen incremental und selective in Verbindung mit einer Anwendung eines anderen Herstellers zur Erstellung einer Momentaufnahme eines logischen Datenträgers, um die Daten in der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.
-    Lokale Momentaufnahme einem Serverdateibereich zuordnen (UNIX und Linux)
  Verwenden Sie die Option snapshotroot in den Befehlen incremental und selective in Verbindung mit einer Anwendung eines anderen Herstellers zur Erstellung einer Momentaufnahme eines logischen Datenträgers, um die Daten in der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.
-  Windows-Systemstatus sichern
  Der Client für Sichern/Archivieren verwendet VSS, um alle Systemstatuskomponenten als ein einziges Objekt zu sichern, um eine konsistente zeitpunktgesteuerte Momentaufnahme des Systemstatus bereitzustellen. Der Systemstatus besteht aus allen bootfähigen Systemstatus- und Systemservicekomponenten.
-  Dateien für automatische Systemwiederherstellung sichern
  Sie können Dateien für die automatische Systemwiederherstellung (Automated System Recovery - ASR) als Vorbereitung für die Wiederherstellung der Windows-Plattenkonfigurationsdaten und des Systemstatus im Falle eines schwerwiegenden System- oder Hardwarefehlers sichern.
-  Vorbereitung für automatische Systemwiederherstellung
  Für die automatische Systemwiederherstellung (ASR) unter Windows sind bestimmte Sicherungen und Datenträger erforderlich.
-     Imagesicherung
  Von Ihrer lokalen Workstation aus können Sie einen logischen Datenträger als einzelnes Objekt auf Ihrem System sichern (Imagesicherung).
-  Momentaufnahmebasierte Dateisicherung und -archivierung und momentaufnahmebasierte Imagesicherung
  Für Clients für Sichern/Archivieren, die als Rootbenutzer auf JFS2-Dateisystemen unter AIX 5.3 oder höher ausgeführt werden, werden standardmäßig momentaufnahmebasierte Imagesicherungen mithilfe von Momentaufnahmen erstellt.
-  Btrfs-Dateisysteme schützen
  Btrfs-Dateisysteme können als Dateispezifikationen für Sicherungs- und Zurückschreibungsbefehle, Archivierungs- und Abrufbefehle und in den Befehlen backup image und restore image angegeben werden. Außerdem können Sie Btrfs-Unterdatenträger als Dateispezifikation in den Sicherungs- und Zurückschreibungsfunktionen und in den Archivierungs- und Abruffunktionen angeben. Die Imagesicherungs- oder Imagezurückschreibungsbefehle des Clients für Sichern/Archivieren können Sie für einen Btrfs-Unterdatenträger nicht verwenden.
-    NAS-Dateisysteme mit Network Data Management Protocol sichern
  Windows-, AIX- und Solaris-Clients für Sichern/Archivieren können Network Data Management Protocol (NDMP) verwenden, um NAS-Dateisystemimages (NAS = Network Attached Storage) effizient zu sichern und zurückzuschreiben. Die Dateisystemimages können auf automatisierten Bandlaufwerken oder Speicherarchiven, die lokal an Network Appliance- oder EMC Celerra-NAS-Dateiserver

angeschlossen sind, oder auf Bandlaufwerken oder Speicherarchiven, die lokal an einen IBM Spectrum Protect-Server angeschlossen sind, gesichert und von diesen zurückgeschrieben werden.

- Windows-BetriebssystemeUnterstützung für CDP Persistent Storage Manager
  Persistent Storage Manager (PSM) ist die Momentaufnahmetechnologie, die in einer Reihe von NAS-Boxes, die auf Microsoft Server Appliance Kit basieren, enthalten ist, einschließlich IBM® TotalStorage NAS 200, 300 und 300G.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeNFS-Dateien sichern
  Sie können den Client für Sichern/Archivieren zum Schützen von Dateien konfigurieren, auf die mit dem NFS-Protokoll (NFS = Network File System) oder dem CIFS-Protokoll (CIFS = Common Internet File System) zugegriffen wird.
- AIX-BetriebssystemeAIX-Workloadpartitionsdateisysteme sichern
  Mit dem Client für Sichern/Archivieren unter AIX können Sie Dateidaten lokaler Partitionen innerhalb der globalen Partition mithilfe des Namensbereichs der lokalen Partition innerhalb der globalen Partition sichern und zurückschreiben.
- Oracle Solaris-BetriebssystemeSolaris Zettabyte-Dateisysteme (ZFS) sichern
  Auf Solaris SPARC- und Solaris x86-Systemen können Sie ZFS-Dateisysteme (Zettabyte File System) mithilfe von ZFS-Momentaufnahmen sichern. Der Vorteil dieser Methode im Vergleich zu einer normalen Teilsicherung oder selektiven Sicherung besteht darin, dass sich die Dateien und Ordner in einer Momentaufnahme immer im Lesezugriffsmodus befinden und daher während einer Sicherung nicht geändert werden können.
- AIX-BetriebssystemeVerschlüsseltes AIX JFS2-Dateisystem sichern
  Verwenden Sie das AIX JFS2-EFS-System (EFS = Encrypted File System - Verschlüsseltes Dateisystem), um Dateien entweder im Klartext oder im unformatierten Format zu sichern. Beim Format Klartext wird die Datei von EFS beim Lesen entschlüsselt. Beim unformatierten Format werden die Daten nicht entschlüsselt. Standardwert ist das unformatierte Format, aber wenn Sie die Option efsdecrypt auf yes setzen, erhalten Sie Sicherungen im Klartext.
- AIX-BetriebssystemeErweiterte AIX JFS2-Attribute sichern
  AIX Enhanced Journal File System (JFS2) bietet Sicherungsverarbeitung für benannte erweiterte Attribute für alle Dateisysteme, die benannte erweiterte Attribute unterstützen.
- Linux-BetriebssystemeWindows-BetriebssystemeVirtuelle VMware-Maschinen sichern
  Sie können mithilfe des Clients für Sichern/Archivieren eine virtuelle VMware-Maschine sichern und zurückschreiben. Gesamtsicherungen der virtuellen Maschine werden auf Plattenimageebene ausgeführt. Bei Teilsicherungen werden nur die Daten gesichert, die sich seit der vorherigen Gesamtsicherung geändert haben.
- Windows-BetriebssystemeVirtuelle Maschinen auf einem Hyper-V-System sichern
  Sie können mithilfe des Clients für Sichern/Archivieren virtuelle Maschinen sichern, die von einem Microsoft Hyper-V-Server verwaltet werden.
- Linux-BetriebssystemeWindows-BetriebssystemeTivoli Storage Manager FastBack-Daten sichern und archivieren
  Verwenden Sie Tivoli Storage Manager FastBack, um die neuesten Momentaufnahmen für die kurzfristige Aufbewahrung zu sichern und zu archivieren.
- Windows-BetriebssystemeNet Appliance-CIFS-Freigabedefinition sichern
  Network Appliance-CIFS-Freigabedefinitionen (NetApp-CIFS-Freigabedefinitionen) umfassen Freigabeberechtigungen, die auf dem Dateiserver definiert sind.
- Status der Sicherungsverarbeitung anzeigen
  Während einer Sicherung zeigt der Client für Sichern/Archivieren standardmäßig den Status jeder Datei an, die er zu sichern versucht.
- Windows-BetriebssystemeSicherung (Windows): Weitere Hinweise
  Dieser Abschnitt enthält zusätzliche Informationen, die beim Sichern von Daten berücksichtigt werden müssen.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSicherung (UNIX und Linux): Weitere Hinweise
  Sie sollten einige besondere Situationen bedenken, bevor Sie Ihre Daten sichern.

Windows-Betriebssysteme

Sicherungen planen (Windows)

Als Erstbenutzer bzw. als Benutzer, der nur gelegentlich Dateien sichert, können Sie die Tabelle in diesem Abschnitt als Prüfliste für die Schritte verwenden, die vor einer Sicherung auszuführen sind.

Lesen Sie die in dieser Tabelle aufgelisteten Tasks, um festzustellen, ob Sie für die Sicherung Ihrer Daten bereit sind.

Tabelle 1. Sicherungen planen

☐	Entscheiden Sie, ob Dateien gesichert oder archiviert werden sollen. Weitere Informationen siehe Wann werden Dateien gesichert und wann archiviert?.
☐	Der Abschnitt Hinweise vor der Sicherung (Windows) enthält wichtige Migrationsinformationen sowie Informationen zur Verbesserung der Leistung, bevor Dateien und Verzeichnisse gesichert werden.
☐	Erstellen Sie eine Einschluss-/Ausschlussliste, die Dateien und Verzeichnisse enthält, die von den Sicherungsservices ausgeschlossen werden sollen. Weitere Informationen siehe Verarbeitung mit einer Einschluss-/Ausschlussliste steuern.

☐	Entscheiden Sie, welche Sicherungsart sich für Ihre Anforderungen am besten eignet. Die folgenden Abschnitte enthalten weitere Informationen: • Teilsicherung, selektive Sicherung oder Teilsicherung nach Datum (Windows) • Dateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (Windows) • Windows-Systemstatus sichern • Dateien für automatische Systemwiederherstellung sichern • Imagesicherung • NAS-Dateisysteme mit Network Data Management Protocol sichern • Parallele Sicherungen virtueller Maschinen
☐	Weitere Hinweise zur Sicherung befinden sich im Abschnitt Sicherung (Windows): Weitere Hinweise.

Zugehörige Konzepte:
IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Zugehörige Tasks:
Clients für Sichern/Archivieren konfigurieren
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Sicherungen planen

Als Erstbenutzer bzw. als Benutzer, der nur gelegentlich Dateien sichert, können Sie die Tabelle in diesem Abschnitt als Prüfliste für die Schritte verwenden, die vor einer Sicherung auszuführen sind.

Lesen Sie die Liste der Tasks, um festzustellen, ob Sie für die Sicherung Ihrer Daten bereit sind.

- Entscheiden Sie, ob Dateien gesichert oder archiviert werden sollen. Weitere Informationen siehe Wann werden Dateien gesichert und wann archiviert?.
- Hinweise vor der Sicherung (UNIX und Linux) enthält wichtige Hinweise vor dem Sichern Ihrer Dateien und Verzeichnisse.
- Sollen Dateien von den Sicherungsservices ausgeschlossen werden? Weitere Informationen siehe Einschluss-/Ausschlussoptionen für die Verarbeitungssteuerung.

Zugehörige Konzepte:
IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Zugehörige Tasks:
Clients für Sichern/Archivieren konfigurieren

Welche Dateien werden gesichert?

Wenn Sie eine Sicherung anfordern, sichert der Client eine Datei, wenn bestimmte Voraussetzungen erfüllt sind.

Damit der Client eine Datei sichert, müssen die folgenden Voraussetzungen erfüllt sein:

- Die ausgewählte Verwaltungsklasse enthält eine Sicherungskopiengruppe.
- Die Datei erfüllt die in der Sicherungskopiengruppe definierten Anforderungen bezüglich der Durchnummerierung. Lautet der Wert des Durchnummerierungsparameters der Kopiengruppe static oder shrstatic und ändert sich die Datei während der Sicherung, wird die Datei nicht gesichert.
- Die Datei erfüllt die in der Sicherungskopiengruppe definierten Anforderungen bezüglich des Modus (mode). Lautet der Parameter mode der Kopiengruppe modified (Geändert), muss sich die Datei seit der letzten Sicherung geändert haben. Lautet der Modus (mode) absolute (Absolut), kann die Datei gesichert werden, auch wenn sie sich nicht ändert.
- Die Datei erfüllt die in der Sicherungskopiengruppe definierten Anforderungen bezüglich der Häufigkeit. Seit der letzten Sicherung muss die angegebene Mindestanzahl Tage vergehen, damit eine Datei gesichert wird.
- Die Datei ist nicht durch eine Exclude-Anweisung von der Sicherung ausgeschlossen.
- Die Datei ist nicht durch das Betriebssystem von der Sicherung ausgeschlossen. Diese ausgeschlossenen Dateien befinden sich im Registry-Unterschlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup.

Dateien, die zum Windows-Systemstatus gehören, können nur für die Sicherung ausgewählt werden, wenn der Systemstatus gesichert wird. Sie können den Systemstatus nur als Ganzes sichern, da Abhängigkeiten zwischen den Systemstatuskomponenten bestehen. Sie können die Dateien nicht einzeln sichern oder zurückschreiben. Da z. B. C:\windows\system32\ntoskrnl.exe zum Windows-Systemstatus gehört, wird diese Datei während einer Teilsicherung oder selektiven Sicherung des Laufwerks C:\ nicht gesichert.

Windows-Betriebssysteme

Unterstützung offener Dateien für Sicherungsoperationen

Der VSS-Momentaufnahmeprovider wird für die Unterstützung offener Dateien verwendet.

VSS ist der Momentaufnahmeprovider für Windows.

Einige Anwendungen können Dateien erstellen und diese Dateien so öffnen, dass allen anderen Prozessen auf einem Microsoft Windows-Betriebssystem der Zugriff verweigert wird. Obwohl dies kein allgemein übliches Verfahren ist, wird es manchmal von Datenbankanbietern oder anderen Anwendungen verwendet, die möglicherweise den Zugriff auf bestimmte Dateien beschränken wollen. Durch die Zugriffsbeschränkung auf diese Dateien werden Sicherungsprodukte daran gehindert, die Daten zu sichern. Diese gesperrten Dateien sind nicht gleichzusetzen mit Dateien, die offen oder im Gebrauch sind. Wird der Client für Sichern/Archivieren ohne die Funktion zur Unterstützung offener Dateien (OFS = Open File Support) ausgeführt, kann er offene oder im Gebrauch befindliche Dateien sichern; dies umfasst unter anderem Dateien, die zum Lesen oder Schreiben geöffnet sind, Dateien, die sich während der Sicherung ändern, ausführbare Dateien und dll-Dateien, die ausgeführt werden sowie Protokolldateien, denen Daten hinzugefügt werden.

Sie können OFS- oder Online-Imagesicherungen auf Workstations mit einem einzigen NTFS- oder ReFS-basierten Laufwerk `C:\` erstellen.

Die folgende Fehlernachricht wird im Fehlerprotokoll `dsmerror.log` angezeigt, wenn der Client eine dieser gesperrten Dateien findet, ohne dass die OFS-Unterstützung aktiviert ist:

```
ANS4987E Fehler bei der Verarbeitung von '\\machine1\d$\dir1\lockedfile.xyz':
Das Objekt wird von einem anderen Prozess verwendet

ANS1228E Senden von Objekt '\\machine1\d$\dir1\lockedfile.xyz' fehlgeschlagen
```

Verwenden Sie OFS nicht zum Sichern gesperrter Windows-Systemdateien wie dem Windows-Systemstatus. Der Client verfügt über erweiterte Funktionen zum Sichern von Daten, die in diesen Dateien enthalten sind. Das Sichern der in diesen Dateien enthaltenen Systemdaten erfordert zusätzliche Verarbeitung und muss in einer Gruppensicherung erfolgen, damit eine Zurückschreibung erfolgreich ist. Diese Dateien sind von der IBM Spectrum Protect-Sicherung auf Dateiebene ausgeschlossen.

Bei Datenbankanwendungen, die bestimmte Dateien für eine transaktionsorientierte Konsistenz verwenden (z. B. eine Wiederherstellungsprotokolldatei) ist es unter Umständen nicht möglich, diese Dateien ohne Datenbankkoordination zu sichern und zurückzuschreiben. Sichern Sie diese Datenbankdateien in diesen Situationen nicht mit der normalen Sicherung auf Dateiebene. Sie können diese Dateien mithilfe der Anweisung exclude oder exclude.dir von der Sicherungsverarbeitung ausschließen. Es sind verschiedene Datenschutzclients (IBM Spectrum Protect for Databases, IBM Spectrum Protect for Mail usw.) verfügbar, die diese Funktionen für die Datenbankkoordination und -sicherung sowie zusätzliche erweiterte Datenbanksicherungsfunktionen bereitstellen. Eine aktuelle Liste der Datenschutzclients finden Sie auf der folgenden Website: http://www.ibm.com/systems/storage/spectrum/protect/.

Für private Anwendungen oder andere Datenbankprodukte, für die kein Data Protection-Client verfügbar ist, können Sie die Option preschedulecmd verwenden, um der Datenbank oder der Anwendung zu signalisieren, einen der folgenden Schritte auszuführen:

- Die erforderlichen Schritte unternehmen, um diese Dateien in einen konsistenten und nicht offenen Status zu versetzen.
- Die Datenbank herunterfahren, bevor die Sicherung auf Dateiebene gestartet wird.
- Eine andere Methode programmieren oder durch ein Script festschreiben, um diese Daten zu sichern und diese Dateien von der Sicherung auf Dateiebene auszuschließen. In diesen Fällen ist die OFS-Funktion nicht notwendig, da diese Dateien nicht länger nicht verfügbar oder von der Anwendung gesperrt sind. Verwenden Sie nach Beendigung der Sicherung auf Dateiebene die Option postschedulecmd, um die Datenbank wieder online zu bringen, oder starten Sie die Anwendung neu.

Dauert die Ausführung der Sicherung auf Dateiebene zu lang, um die offenen Dateien offline zu halten (z. B. die Datenbank offline zu halten oder Transaktionen aufzuhalten), sollten Sie mit der OFS-Funktion eine Momentaufnahme nach Zeitpunkt des Datenträgers erstellen. Verwenden Sie in diesem Fall die Optionen presnapshotcmd und postsnapshotcmd, um der Datenbank oder der Anwendung zu signalisieren, sich mit der Sicherung dieser offenen Dateien zu koordinieren. Die Erstellung der Momentaufnahme, die zwischen dem Befehl vor der Momentaufnahme und dem Befehl nach der Momentaufnahme stattfindet, dauert in der Regel nur ein paar Sekunden. Dies ermöglicht es der Datenbank oder Anwendung, die Operationen schnell wieder aufzunehmen, während der Client weiterhin eine vollständige Teilsicherung des Datenträgers einschließlich der gesperrten Dateien ausführen kann. Es gibt andere Situationen, in denen diese von einer Anwendung gesperrten Dateien auf sichere Art und Weise und auf Basis einzelner Dateien gesichert und zurückgeschrieben werden können. In diesen Situationen können Sie die OFS-Funktion für denjenigen Datenträger aktivieren, auf dem die offenen Dateien vorhanden sind. Der Client hat dann Zugriff auf diese Dateien und sichert sie mithilfe von Sicherungs- und Archivierungsoperationen auf Dateiebene.

Informationen zu Einschränkungen und Problemen bei der Unterstützung offener Dateien (OFS) finden Sie in Technote 1248971.

Wenn die Unterstützung offener Dateien konfiguriert wurde, führt der Client eine Momentaufnahmesicherung oder -archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder "im Gebrauch") sind. Über die Momentaufnahme wird die Sicherung von einer Kopie des Dateisystems erstellt, die dem Dateisystemstatus zum Zeitpunkt der Erstellung der Momentaufnahme entspricht. Nachfolgende Änderungen am Dateisystem werden bei der Sicherung nicht berücksichtigt. Sie können den Parameter snapshotproviderfs der Option include.fs auf none setzen, um anzugeben, welche Laufwerke keine Unterstützung für offene Dateien verwenden.

Sie können die folgenden zusätzlichen Optionen in Ihrer Datei dsm.opt oder als Werte der Option include.fs angeben, um eine OFS-Operation (OFS = Open File Support = Unterstützung offener Dateien) zu steuern: snapshotproviderfs sowie presnapshotcmd und postsnapshotcmd.

Anmerkung:

1. Sie können die Option include.fs verwenden, um Momentaufnahmeoptionen pro Dateisystem festzulegen.
2. Die Unterstützung offener Dateien wird sowohl für die Sicherung als auch für die Archivierung zur Verfügung gestellt. Bei der Sicherung schließt dies Teilsicherung, Teilsicherung nach Datum, selektive Sicherung, Imageteilsicherung und journalbasierte Sicherung ein.
3. Die Unterstützung offener Dateien ist nur für lokale fixierte Datenträger (entweder an Laufwerkbuchstaben oder Datenträgermountpunkte angehängt) verfügbar, die mit FAT-, FAT32-, NTFS- oder ReFS-Dateisystemen formatiert sind. Diese Unterstützung schließt an ein SAN

angeschlossene Datenträger ein, die diese Anforderungen erfüllen.
4. Damit die OFS-Unterstützung in einer Clusterumgebung aktiviert werden kann, muss für alle Workstations im Cluster OFS konfiguriert sein. Geben Sie VSS als Momentaufnahmeprovider in der Option snapshotproviderfs an.

Zugehörige Konzepte:
Verarbeitungsoptionen
Zugehörige Tasks:
Windows-Systemstatus sichern
Unterstützung offener Dateien konfigurieren
 Windows-Betriebssysteme

Daten über die GUI sichern

Mithilfe der GUI des Clients für Sichern/Archivieren können Sie bestimmte Dateien, eine Gruppe von Dateien mit ähnlichen Namen oder vollständige Verzeichnisse sichern.

Informationen zu diesem Vorgang

Die zu sichernden Dateien können mithilfe einer Such- bzw. Filterfunktion gesucht werden. Beim Filtern werden nur die Dateien angezeigt, die mit den Filterkriterien für die Sicherung übereinstimmen. Dateien, die den Filterkriterien nicht entsprechen, werden nicht angezeigt.

Verwenden Sie die folgenden Schritte, um eine Sicherung mit der grafischen Benutzerschnittstelle auszuführen:

Vorgehensweise

1. Klicken Sie auf Sichern im Hauptfenster der grafischen Benutzerschnittstelle. Das Fenster Sichern wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen + klicken. Zum Anzeigen von Dateien in einem Ordner klicken Sie auf das Ordnersymbol. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol Suchen in der Funktionsleiste.
3. Klicken Sie auf das Auswahlfeld für die Objekte, die gesichert werden sollen.
4. Wählen Sie den Sicherungstyp aus dem Pulldown-Menü aus:
    a. Für eine Teilsicherung Teilsicherung (vollständig) auswählen.
    b. Für eine Teilsicherung nach Datum Teilsicherung (nur Datum) auswählen.
    c. Für eine selektive Sicherung Immer sichern auswählen.
    d. Für eine Teilsicherung ohne Verwendung der Journaldatenbank Teilsicherung (ohne Journal) auswählen. Wenn der Journalsteuerkomponentenservice installiert und aktiv ist, führt der Befehl Incremental automatisch eine journalbasierte Sicherung der ausgewählten Dateisysteme aus, die vom Journalsteuerkomponentenservice überwacht werden. Mit dieser Option wird eine traditionelle vollständige Teilsicherung anstelle der standardmäßigen journalbasierten Sicherung ausgeführt.
5. Klicken Sie auf Sichern. Im Fenster Taskliste für die Sicherung wird der Verarbeitungsstatus der Sicherung angezeigt. Nach Beendigung der Verarbeitung werden im Fenster Sicherungsbericht die Verarbeitungsdetails angezeigt.

Ergebnisse

Die folgenden Hinweise sind zu beachten, wenn Sie die GUI zum Sichern Ihrer Daten verwenden.

- IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden. Bei jeder Sicherung einer Datei wird ihr eine Verwaltungsklasse zugeordnet. Bei der verwendeten Verwaltungsklasse kann es sich um die Standardverwaltungsklasse handeln, die Ihnen zugeordnet wird, oder um eine Verwaltungsklasse, die Sie der Datei mit der Option include in der Einschluss-/Ausschlussoptionsliste zuordnen. Wählen Sie Dienstprogramme → Maßnahmeninformationen anzeigen in der GUI des Clients für Sichern/Archivieren oder des Web-Clients aus, um die Sicherungsstrategien anzuzeigen, die vom IBM Spectrum Protect-Server für Ihren Clientknoten definiert wurden. Wählen Sie Editieren → Clientvorgaben in der GUI des Clients für Sichern/Archivieren oder des Web-Clients aus und wählen Sie im Profileditor die Registerkarte Einschluss/Ausschluss aus, um Ihre Einschluss-/Ausschlussliste anzuzeigen.
- Um bestimmte Sicherungsoptionen zu ändern, klicken Sie auf die Schaltfläche Optionen. Die geänderten Optionen sind nur während der aktuellen Sitzung wirksam.
- Für nachfolgende Teilsicherungen können Sie im IBM Spectrum Protect-Hauptfenster das Menü Aktionen öffnen und Domäne sichern auswählen.
- In der GUI des Web-Clients können Netzressourcen nicht durchsucht werden, um eine Sicherung auszuführen. Es werden keine Freigaben aufgelistet, wenn Sie die Verzweigung Netz einblenden. Es ist möglich, eine Netzressource mithilfe des Web-Clients zu sichern, sofern die gesamte Datei verarbeitet wird. Zu diesem Zweck wird das Dateisystem mit der Option domain in `dsm.opt` angegeben (z. B. `domain all-local \\server\share`). Um die Sicherung auszuführen, wählen Sie Domäne sichern im Menü Aktionen aus. Dadurch werden alle Dateisysteme verarbeitet, die mit der Option domain angegeben werden. Sie können die Sicherung auch mit dem GUI-Client ausführen.
-  Windows-BetriebssystemeLaufwerke in Ihrer Domäne angeben
  Wenn Sie den Client starten, wird Ihre Standarddomäne auf die Laufwerke gesetzt, die mit der Option domain in der Datei dsm.opt angegeben sind.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
Zugehörige Tasks:

Daten über die GUI zurückschreiben
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren
Windows-Betriebssysteme

Daten über die Befehlszeile sichern

Sie können Sicherungen mit dem Befehl incremental oder selective ausführen. Die folgende Tabelle enthält Beispiele zur Verwendung von Befehlen zum Ausführen verschiedener Tasks.

Informationen zu diesem Vorgang

Tabelle 1. Beispiele für Sicherungsbefehle

Task	Befehl	Hinweise
Teilsicherungen		
Eine Teilsicherung Ihrer Clientdomäne ausführen.	dsmc incremental	Der Abschnitt Incremental enthält weitere Informationen zum Befehl incremental. Der Abschnitt Vollständige und partielle Teilsicherung enthält ausführliche Informationen zu Teilsicherungen.
Neben den Laufwerken `c:`, `d:` und `e:`, die in Ihrer Clientdomäne definiert sind, die Laufwerke `g:` und `h:` sichern.	`dsmc incremental -domain="g: h:"`	Weitere Informationen zur Option domain befinden sich im Abschnitt Domain.
Alle lokalen Datenträger in Ihrer Clientdomäne *außer* dem Laufwerk `c:` und der Domäne systemobject sichern.	`dsmc incremental -domain="all-local -c: -systemobject"`	Sie können den Operator Bindestrich (-) nicht vor dem Domänenschlüsselwort all-local verwenden. Weitere Informationen siehe Domain. Bei Windows-Clients können Sie auf diese Weise auch die Domäne systemstate von der Sicherungsverarbeitung ausschließen.
Alle lokalen Datenträger in Ihrer Clientdomäne *außer* dem Laufwerk `c:` und der Domäne systemstate sichern.	`dsmc incremental -domain="all-local -c: -systemstate"`	Sie können den Operator Bindestrich (-) nicht vor dem Domänenschlüsselwort all-local verwenden. Weitere Informationen siehe Domain.
Nur die Laufwerke `g:` und `h:` sichern.	`dsmc incremental g: h:`	Keine
Alle Dateien im Verzeichnis `c:\Accounting` und in allen seinen Unterverzeichnissen sichern.	`dsmc incremental c:\Accounting\* -sub=yes`	Weitere Informationen zur Option subdir befinden sich im Abschnitt Subdir.
Unter der Annahme, dass eine Momentaufnahme des Laufwerks `C:` initiiert und die Momentaufnahme als logischer Datenträger `\\florence\c$\snapshots\snapshot.0` angehängt wurde, eine Teilsicherung aller Dateien und Verzeichnisse unter der lokalen Momentaufnahme ausführen und auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen `C:` verwalten.	`dsmc incremental c: -snapshot= \\florence\c$\snapshots\ snapshot.0`	Weitere Informationen siehe Snapshotroot.
Teilsicherung nach Datum		
Eine Teilsicherung Ihrer Standardclientdomäne nach Datum ausführen.	`dsmc incremental -incrbydate`	Verwenden Sie die Option incrbydate im Befehl incremental, um neue und geänderte Dateien zu sichern, deren Änderungsdatum nach dem Datum der letzten auf dem Server gespeicherten Teilsicherung liegt. Incrbydate enthält weitere Informationen zur Option incrbydate.
Selektive Sicherungen		

Task	Befehl	Hinweise
Alle Dateien im Verzeichnis `d:\proj` sichern.	`dsmc selective d:\proj\`	Verwenden Sie den Befehl selective, um bestimmte Dateien, eine Gruppe von Dateien mit ähnlichen Namen oder leere Verzeichnisse und ihre Attribute zu sichern, unabhängig davon, ob diese Dateien oder Verzeichnisse während der letzten Teilsicherung gesichert wurden, und ohne Auswirkungen auf den Zähler für die letzte Teilsicherung des Sicherungsservers. Mithilfe von Platzhalterzeichen können mehrere Dateien gleichzeitig gesichert werden. Der Abschnitt Selective enthält weitere Informationen zum Befehl selective.
Das Verzeichnis `d:\proj` und alle seine Unterverzeichnisse sichern.	`dsmc selective d:\proj\ -subdir=yes`	Weitere Informationen zur Option subdir befinden sich im Abschnitt Subdir.
Die Dateien `d:\h1.doc` und `d:\test.doc` sichern.	`dsmc selective d:\h1.doc d:\test.doc`	Sie können so viele Dateispezifikationen angeben, wie die verfügbaren Ressourcen oder andere Betriebssystembeschränkungen erlauben. Trennen Sie die Dateispezifikationen durch ein Leerzeichen. Sie können auch die Option filelist verwenden, um eine Liste von Dateien zu verarbeiten. Der Client für Sichern/Archivieren öffnet die Datei, die Sie mit dieser Option angeben, und verarbeitet die darin enthaltene Liste der Dateien dem jeweiligen Befehl entsprechend. Weitere Informationen siehe Filelist.
Eine Liste von Dateien auf Laufwerk `c:` sichern.	`dsmc selective -filelist=c:\filelist.txt`	Verwenden Sie die Option filelist, um eine Liste von Dateien zu verarbeiten. Weitere Informationen siehe Filelist.
Unter der Annahme, dass eine Momentaufnahme des Laufwerks `C:` initiiert und die Momentaufnahme als logischer Datenträger `\\florence\c$\snapshots\snapshot.0` angehängt wurde, eine selektive Sicherung der Verzeichnisbaumstruktur `c:\dir1\sub1` von der lokalen Momentaufnahme ausführen und auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen `C:` verwalten.	`dsmc selective c:\dir1\sub1\* -subdir=yes snapshot=\\florence\c$\snapshots\ snapshot.0`	Weitere Informationen siehe Snapshotroot.

Zugehörige Konzepte:
Sicherung (Windows): Weitere Hinweise
Befehle verwenden
Windows-Betriebssysteme

Sicherungsdaten löschen

Wenn Sie vom Administrator entsprechend berechtigt wurden, können Sie einzelne Sicherungskopien aus dem IBM Spectrum Protect-Server löschen, ohne den gesamten Dateibereich zu löschen.

Informationen zu diesem Vorgang

Beispiel: Sie müssen unter Umständen sensible Daten löschen, die (absichtlich oder unabsichtlich) gesichert wurden und jetzt vom Server entfernt werden müssen. Oder Sie müssen möglicherweise Dateien löschen, die gesichert wurden, von denen später jedoch festgestellt wurde, dass sie Viren enthalten. Um festzustellen, ob Sie über die Berechtigung verfügen, einzelne Sicherungskopien vom IBM Spectrum Protect-Server zu löschen, ohne den gesamten Dateibereich löschen zu müssen, wählen Sie **Datei** → **Verbindungsinformationen** in der GUI des Clients für Sichern/Archivieren oder im Hauptmenü des Web-Clients aus. Ihr Berechtigungsstatus wird im Feld Sicherungsdateien löschen zur Verfügung gestellt.

Wichtig: Nach dem Löschen von Sicherungsdateien können diese ***nicht mehr zurückgeschrieben werden.*** Stellen Sie vor dem Löschen sicher, dass die gesicherten Dateien nicht mehr benötigt werden. IBM Spectrum Protect fordert eine Bestätigung für den Löschvorgang an. Geben Sie daraufhin *ja* an, werden die angegebenen Dateien sofort gelöscht und aus dem IBM Spectrum Protect-Serverspeicher entfernt.

Sicherungskopien werden über die IBM Spectrum Protect-GUI oder den Web-Client wie folgt gelöscht:

Vorgehensweise

1. Wählen Sie **Sicherungsdaten löschen** im Menü **Dienstprogramme** aus. Das Fenster 'Sicherung löschen' wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen **(+)** oder auf das Ordnersymbol neben dem Objekt, das eingeblendet werden soll, klicken.
3. Wählen Sie einen Eintrag aus der Dropdown-Liste im oberen Bereich des Fensters **Sicherung löschen** aus, um anzugeben, welche Art von 'Sicherung löschen' ausgeführt werden soll. Sie können aktive Sicherungsversionen, inaktive Sicherungsversionen oder alle in der Baumstruktur ausgewählten Objekte löschen. Ein Verzeichnis wird nur gelöscht, wenn Sie **Alle Objekte löschen** auswählen.

Ergebnisse

Zum Löschen von Sicherungskopien mithilfe des IBM Spectrum Protect-Befehlszeilenclients verwenden Sie den Befehl delete backup.

Zugehörige Verweise:
Delete Backup

Wann werden Dateien gesichert und wann archiviert?

Wenn der Client für Sichern/Archivieren eine Datei sichert oder archiviert, werden eine Kopie der Datei und die zugehörigen Attribute an den Server gesendet. Sicherungs- und Archivierungsoperationen dienen jedoch unterschiedlichen Zwecken.

Verwenden Sie Sicherungen, um die eigenen Dateien gegen unvorhergesehene Beschädigung zu schützen, und Archivierungen, um Versionen Ihrer Dateien längerfristig aufzubewahren.

Sicherungsdaten werden nach Version verwaltet, wobei vordefinierte, auf Maßnahmen basierende Regeln verwendet werden. Mithilfe dieser Regeln kann der IBM Spectrum Protect-Administrator die folgenden Prozesse steuern:

- Die Anzahl der auf dem IBM Spectrum Protect-Server aufbewahrten Versionen
- Die Anzahl der Tage, die jede zusätzliche Sicherungskopie aufbewahrt wird
- Was mit den Sicherungsversionen geschieht, wenn die Datei auf dem Clientsystem gelöscht wird

Jede auf dem Server gespeicherte Kopie der Datei wird als separate und eindeutige Version der Datei betrachtet.

Das Archivieren ist ein leistungsfähiger und flexibler Mechanismus zum Speichern von Langzeitdaten. Archivierungsdaten (Archivierungskopien) werden eine angegebene Anzahl Tage lang aufbewahrt. In der Archivierungsfunktion gibt es kein Konzept und keine Unterstützung für Versionen. Der Benutzer oder Administrator ist für die Festlegung der Dateien verantwortlich, die einer Archivierung hinzugefügt werden.

Tipp: Wird eine Datei mehrmals mit derselben Archivierungsbeschreibung archiviert, wird bei jeder Ausführung der Archivierungsoperation eine neue Kopie der Datei zum Archiv hinzugefügt. Sie sollten in jedem Archiv nur eine Kopie einer Datei speichern, um die Abrufoperation zu vereinfachen.

Sicherungen schützen vor Beschädigung oder Verlust von Dateien, die bei einem versehentlichen Löschen, bei einer Beschädigung oder bei Plattenfehlern auftreten können. Der Server verwaltet mindestens eine Sicherungsversion für jede Datei, die gesichert wird. Ältere Versionen werden gelöscht, wenn neue Versionen erstellt werden. Die Anzahl der vom Server verwalteten Sicherungsversionen wird von Ihrem Administrator festgelegt.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme
Archivierungskopien werden für die langfristige Speicherung gesichert. Ihr Administrator kann angeben, wie lange Archivierungskopien aufbewahrt werden sollen. Der Server kann eine unbegrenzte Anzahl Archivierungsversionen einer Datei speichern. Archivierungen sind nützlich, wenn eine bestimmte Version Ihrer Dateien wiederhergestellt werden muss oder wenn eine Datei auf Ihrer Workstation gelöscht und bei Bedarf später wieder abgerufen werden soll. Beispielsweise sollen Tabellenkalkulationen möglicherweise für Steuerzwecke gespeichert werden, aber nicht auf Ihrer Workstation bleiben, da sie nicht verwendet werden.

Zugehörige Konzepte:
 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDaten archivieren und abrufen (UNIX und Linux)
Daten aus einem Sicherungssatz zurückschreiben
 Windows-Betriebssysteme

Hinweise vor der Sicherung (Windows)

Verschiedene Faktoren in Ihrem System oder Ihrer Umgebung können sich auf die Art und Weise auswirken, wie der Client für Sichern/Archivieren Daten verarbeitet. Lesen Sie diese Hinweise, bevor Sie Ihre Daten sichern.

- Windows-BetriebssystemeLAN-unabhängige Datenversetzung
  Mit der LAN-unabhängigen Datenversetzung wird das Versetzen von Clientdaten vom DFV-Netz auf das Speicherbereichsnetz (SAN) verlagert. Dadurch wird die Belastung auf dem IBM Spectrum Protect-Server verringert.
- Windows-BetriebssystemeUnicode-Dateibereiche (Windows)
  Der Windows-Client ist Unicode-aktiviert. Clientversionen vor Version 4.2 waren jedoch nicht für Unicode aktiviert.
- Windows-BetriebssystemeTeilsicherungen auf Systemen mit Speicherengpässen
  Die Leistung einer Teilsicherung nimmt ab, wenn auf dem System vor dem Start der Sicherung nur wenig Speicher verfügbar ist.
- Windows-BetriebssystemeTeilsicherungen auf Systemen mit einer großen Anzahl an Dateien
  Der Client kann große Speicherkapazitätsanteile verwenden, um Teilsicherungsoperationen auszuführen, insbesondere auf Dateisystemen, die eine große Anzahl an Dateien enthalten.
- Windows-BetriebssystemeVerarbeitung mit einer Einschluss-/Ausschlussliste steuern
  Möglicherweise gibt es Dateien in Ihrem System, die Sie nicht sichern wollen. Hierbei kann es sich um Betriebssystem- oder Anwendungsdateien handeln, die durch eine erneute Installation des Programms wiederhergestellt werden können, oder andere Dateien, die ohne Schwierigkeiten wiederhergestellt werden können.
- Windows-BetriebssystemeDatenverschlüsselung während Sicherungs- oder Archivierungsoperationen
  Für eine stärkere Verschlüsselung verwenden Sie die 256-Bit-AES-Datenverschlüsselung (Advanced Encryption Standard) mit der Option encryptiontype. Die 128-Bit-AES-Verschlüsselung ist momentan der Standardwert.
- Windows-BetriebssystemeMaximale Dateigröße für Operationen
  Die maximale Dateigröße für Sicherung- und Zurückschreibungsoperationen sowie Archivierungs- und Abrufoperationen ist vom verwendeten Windows-Dateisystem abhängig.
- Windows-BetriebssystemeWie der Client lange Benutzer- und Gruppennamen handhabt
  Der Client für Sichern/Archivieren kann problemlos Benutzer- und Gruppennamen mit einer Länge von bis zu 64 Zeichen handhaben. Namen, deren Länge 64 Zeichen überschreitet, erfordern jedoch eine besondere Handhabung.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

LAN-unabhängige Datenversetzung

Mit der LAN-unabhängigen Datenversetzung wird das Versetzen von Clientdaten vom DFV-Netz auf das Speicherbereichsnetz (SAN) verlagert. Dadurch wird die Belastung auf dem IBM Spectrum Protect-Server verringert.

Das SAN stellt einen Pfad zur Verfügung, mit dem Sie Daten auf bzw. von einer an das SAN angeschlossenen Speichereinheit sichern, zurückschreiben, archivieren und abrufen können. Die Clientdaten werden mithilfe des IBM Spectrum Protect-Speicheragenten über das SAN auf die Speichereinheit versetzt. Der Speicheragent muss auf demselben System wie der Client installiert werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAIX-, Linux- und Solaris-Clients unterstützen die LAN-unabhängige Datenversetzung.

Windows-BetriebssystemeAlle Windows-Clients unterstützen die LAN-unabhängige Datenversetzung.

- Windows-BetriebssystemeVoraussetzungen für die LAN-unabhängige Datenversetzung
  Um die LAN-unabhängige Unterstützung zu aktivieren, müssen Sie den IBM Spectrum Protect for SAN-Speicheragenten auf der Client-Workstation installieren und konfigurieren.
- Windows-BetriebssystemeOptionen für die LAN-unabhängige Datenversetzung
  Um die LAN-unabhängige Datenversetzung zu aktivieren, können Sie verschiedene Clientoptionen verwenden. Sie müssen zunächst den Speicheragenten von IBM Spectrum Protect for SAN auf der Client-Workstation installieren und konfigurieren.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Voraussetzungen für die LAN-unabhängige Datenversetzung

Um die LAN-unabhängige Unterstützung zu aktivieren, müssen Sie den IBM Spectrum Protect for SAN-Speicheragenten auf der Client-Workstation installieren und konfigurieren.

IBM Spectrum Protect for SAN ist ein separates Produkt.

Weitere Informationen zum Installieren und Konfigurieren des Speicheragenten finden Sie in der Dokumentation zu IBM Spectrum Protect for SAN.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Optionen für die LAN-unabhängige Datenversetzung

Um die LAN-unabhängige Datenversetzung zu aktivieren, können Sie verschiedene Clientoptionen verwenden. Sie müssen zunächst den Speicheragenten von IBM Spectrum Protect for SAN auf der Client-Workstation installieren und konfigurieren.

Verwenden Sie die folgenden Optionen, um die LAN-unabhängige Datenversetzung zu aktivieren:

enablelanfree

Gibt an, ob ein verfügbarer LAN-unabhängiger Pfad zu einer an ein SAN angeschlossenen Speichereinheit aktiviert werden soll.

lanfreecommmethod
Gibt ein Übertragungsprotokoll zwischen dem Client und dem Speicheragenten an.

lanfreeshmport
Gibt die eindeutige Zahl an, die vom Client und vom Speicheragenten verwendet wird, um den für die Datenübertragung verwendeten gemeinsam benutzten Speicherbereich (Shared Memory) zu identifizieren.

lanfreetcpport
Gibt die Nummer des TCP/IP-Anschlusses an, an dem der Speicheragent empfangsbereit ist.

lanfreetcpserveraddress
Gibt die TCP/IP-Adresse für den Speicheragenten an.

Zugehörige Verweise:
Enablelanfree
Lanfreecommmethod
Lanfreeshmport
Lanfreessl
Lanfreetcpport
Lanfreetcpserveraddress
 Windows-Betriebssysteme

Unicode-Dateibereiche (Windows)

Der Windows-Client ist Unicode-aktiviert. Clientversionen vor Version 4.2 waren jedoch nicht für Unicode aktiviert.

Wenn Sie ein System sichern, das zu einer bestimmten Zeit einmal eine Clientversion verwendet hat, die älter als Version 4.2 war, und die Dateibereiche noch nicht nach Unicode migriert wurden, müssen Sie die Migration von Dateibereichen nach Unicode planen. Dies beinhaltet das Umbenennen Ihrer Dateibereiche auf dem Server und das Erstellen neuer Unicode-aktivierter Dateibereiche auf dem Server mithilfe der Option autofsrename.

Zugehörige Konzepte:
Hinweise für Clients, die für Unicode aktiviert wurden
Zugehörige Verweise:
Autofsrename
Detail
Query Filespace
Restore
Retrieve
 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeWindows-Betriebssysteme

Teilsicherungen auf Systemen mit Speicherengpässen

Die Leistung einer Teilsicherung nimmt ab, wenn auf dem System vor dem Start der Sicherung nur wenig Speicher verfügbar ist.

Ist der Speicher auf Ihrem System begrenzt, geben Sie die Option memoryefficientbackup *yes* in Ihrer Clientoptionsdatei an. Diese Option hat zur Folge, dass der Client für Sichern/Archivieren jeweils nur ein einzelnes Verzeichnis verarbeitet, wodurch der Speicherbedarf reduziert, die Sicherungszeit jedoch verlängert wird. Wenn Sie *yes* angeben, analysiert der Client jeweils nur ein einzelnes Verzeichnis für die Sicherung. Bleibt die Leistung schlecht, müssen Sie die Einstellungen des DFV-Puffers und die DFV-Verbindung zwischen Ihrem System und dem IBM Spectrum Protect-Server überprüfen. Steht auf Ihrem System genügend Speicher zur Verfügung, führt das Setzen der Option memoryefficientbackup auf *yes* zu einer Verschlechterung der Sicherungsleistung.

Zugehörige Verweise:
Memoryefficientbackup

Teilsicherungen auf Systemen mit einer großen Anzahl an Dateien

Der Client kann große Speicherkapazitätsanteile verwenden, um Teilsicherungsoperationen auszuführen, insbesondere auf Dateisystemen, die eine große Anzahl an Dateien enthalten.

Der Begriff *Speicher*, wie er hier verwendet wird, bezeichnet den adressierbaren Hauptspeicher, der für den Clientprozess verfügbar ist. Der adressierbare Hauptspeicher ist eine Kombination aus physischem Arbeitsspeicher (RAM) und virtuellem Speicher.

Der Client verwendet durchschnittlich ca. 300 Byte an Speicher pro Objekt (Datei oder Verzeichnis). Somit erfordert der Client für ein Dateisystem mit einer Million Dateien und Verzeichnisse im Durchschnitt ca. 300 MB Speicher. Die genaue Speicherkapazität, die pro Objekt verwendet wird, variiert abhängig von der Länge des Objektpfads und der Länge des Namens oder von der Verschachtelungstiefe der Verzeichnisse. Die Anzahl Datenbyte ist kein wichtiger Faktor bei der Ermittlung des Speicherbedarfs für den Client für Sichern/Archivieren.

Die maximale Anzahl Dateien kann ermittelt werden, indem die für einen Prozess verfügbare maximale Speicherkapazität durch die pro Objekt benötigte durchschnittliche Speicherkapazität dividiert wird.

Der Gesamtspeicherbedarf kann durch eine der folgenden Methoden reduziert werden:

- Verwenden Sie die Clientoption memoryefficientbackup diskcachemethod. Mit dieser Auswahl wird die Speicherbelegung auf Kosten der Leistung und einer signifikanten Zunahme des für die Sicherung erforderlichen Plattenspeicherplatzes auf ein Minimum reduziert. Die Dateibeschreibungsdaten vom Server sind in einer plattenresidenten temporären Datenbank gespeichert, nicht im Hauptspeicher. Sobald die Verzeichnisse auf der Workstation durchsucht werden, wird die Datenbank befragt, um festzustellen, ob die einzelnen Objekte gesichert, aktualisiert oder als verfallen markiert werden sollen. Bei Beendigung der Sicherung wird die Datenbankdatei gelöscht.
- Verwenden Sie die Clientoption memoryefficientbackup yes. Der durchschnittlich vom Client verwendete Speicher ergibt sich dann aus 300 Byte mal der Anzahl an Verzeichnissen plus 300 Byte pro Datei in dem Verzeichnis, das verarbeitet wird. Bei Dateisystemen mit einer großen Anzahl (Millionen) an Verzeichnissen ist der Client unter Umständen trotzdem nicht in der Lage, ausreichend Speicher zuzuordnen, um Teilsicherungen mit memoryefficientbackup yes auszuführen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeUNIX- und Linux-Clients können möglicherweise die Clientoption virtualmountpoint verwenden, um mehrere virtuelle Mountpunkte innerhalb eines einzelnen Dateisystems zu definieren, wobei jeder separat vom Client gesichert werden kann.
- Ist die Clientoption resourceutilization auf einen Wert größer als 4 gesetzt und werden mehrere Dateisysteme gesichert, wird durch Reduzieren von resourceutilization auf maximal 4 der Prozess auf die Teilsicherung jeweils eines einzelnen Dateisystems begrenzt. Diese Einstellung verringert den Speicherbedarf. Ist aus Leistungsaspekten eine parallele Sicherung mehrerer Dateisysteme erforderlich und überschreitet der kombinierte Speicherbedarf die Verarbeitungslimits, können mehrere Instanzen des Sicherungsclients verwendet werden, um mehrere Dateisysteme parallel zu sichern. Wenn Sie z. B. zwei Dateisysteme gleichzeitig sichern wollen, aber deren Speicherbedarf die Grenzwerte eines einzelnen Prozesses überschreitet, dann starten Sie eine Instanz des Clients, um das eine Dateisystem zu sichern, und starten eine zweite Instanz des Clients, um das andere Dateisystem zu sichern.
- Verwenden Sie die Clientoption -incrbydate, um eine "Teilsicherung nach Datum" auszuführen.
- Verwenden Sie die Clientoption exclude.dir, um zu verhindern, dass der Client Verzeichnisse traversiert und sichert, die nicht gesichert werden müssen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeVerwenden Sie mit Ausnahme von Mac OS X die Clientfunktion für Imagesicherung, um den gesamten Datenträger zu sichern. Eine Imagesicherung könnte in Wirklichkeit weniger Systemressourcen verwenden und schneller ausgeführt werden als eine Teilsicherung einiger Dateisysteme mit einer großen Anzahl kleiner Dateien.
- Reduzieren Sie die Anzahl Dateien pro Dateisystem, indem Sie die Daten auf mehrere Dateisysteme verteilen.

Zugehörige Verweise:
Snapdiff
Ausschlussoptionen
Incrbydate
Memoryefficientbackup
Resourceutilization
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeVirtualmountpoint
Windows-Betriebssysteme

Verarbeitung mit einer Einschluss-/Ausschlussliste steuern

Möglicherweise gibt es Dateien in Ihrem System, die Sie nicht sichern wollen. Hierbei kann es sich um Betriebssystem- oder Anwendungsdateien handeln, die durch eine erneute Installation des Programms wiederhergestellt werden können, oder andere Dateien, die ohne Schwierigkeiten wiederhergestellt werden können.

Verwenden Sie die Optionen include und exclude in der Clientoptionsdatei (dsm.opt), um die Dateien zu definieren, die in die Teilsicherungsverarbeitung oder die selektive Sicherungsverarbeitung eingeschlossen oder davon ausgeschlossen werden sollen. Eine Datei ist für die Sicherung auswählbar, wenn sie nicht durch die Option exclude ausgeschlossen ist. Zum Einschließen bestimmter Dateien in die Sicherung muss die Option include nur verwendet werden, wenn sich diese Dateien in einem Verzeichnis befinden, das andere Dateien enthält, die ausgeschlossen werden sollen.

Die Einschluss-/Ausschlussliste kann vom Server angegebene Elemente enthalten. Der Inhalt der Einschluss-/Ausschlussliste kann mit dem Befehl query inclexcl angezeigt werden.

IBM Spectrum Protect bestimmt mithilfe von *Verwaltungsklassen*, wie die Sicherungen auf dem Server verwaltet werden. Bei jeder Sicherung einer Datei wird ihr eine Verwaltungsklasse zugeordnet. Bei der Verwaltungsklasse kann es sich um die Standardverwaltungsklasse handeln, die für Sie ausgewählt wurde, oder um eine Verwaltungsklasse, die Sie der Datei mit der Option include in der Einschluss-/Ausschlussliste zuordnen. Wenn Sie eine Verwaltungsklasse zuordnen, muss sie eine Sicherungskopiengruppe enthalten, damit die Datei gesichert wird.

Sie können Einschluss-/Ausschlussanweisungen auch in der Verzeichnisstruktur der GUI des Clients für Sichern/Archivieren hinzufügen. Mit dem Befehl preview können Sie die Auswirkungen der gegenwärtig definierten Einschluss-/Ausschlussliste ansehen, ohne dass Sie eine tatsächliche Sicherungsoperation ausführen müssen.

Zugehörige Tasks:
Einschluss-/Ausschlussliste erstellen
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren
Zugehörige Verweise:
Preview Backup
Windows-Betriebssysteme

Datenverschlüsselung während Sicherungs- oder Archivierungsoperationen

Für eine stärkere Verschlüsselung verwenden Sie die 256-Bit-AES-Datenverschlüsselung (Advanced Encryption Standard) mit der Option encryptiontype. Die 128-Bit-AES-Verschlüsselung ist momentan der Standardwert.

Die Daten, die Sie einschließen, werden in verschlüsselter Form gespeichert; die Verschlüsselung hat keine Auswirkungen auf das gesendete oder empfangene Datenvolumen.

Achtung: Wenn das Kennwort für den Verschlüsselungsschlüssel nicht in der Windows-Registrierungsdatenbank gespeichert ist und Sie das Kennwort vergessen haben, können Ihre Daten nicht wiederhergestellt werden.

Die Option include.encrypt ist die einzige Möglichkeit, die Verschlüsselung auf dem Client für Sichern/Archivieren zu aktivieren. Werden keine Anweisungen include.encrypt verwendet, findet keine Verschlüsselung statt.

Die Verschlüsselung ist nicht kompatibel mit Sicherungen virtueller VMware-Maschinen im Modus der immer inkrementellen Sicherung (MODE=IFIncremental und MODE=IFFull). Ist der Client für die Verschlüsselung konfiguriert, können Sie nicht die immer inkrementelle Sicherung verwenden.

Um Dateidaten zu verschlüsseln, müssen Sie einen Kennwort für den Verschlüsselungsschlüssel auswählen, das der Client zum Generieren des Verschlüsselungsschlüssels zum Verschlüsseln und Entschlüsseln der Dateidaten generiert. Sie können angeben, ob das Kennwort für den Verschlüsselungsschlüssel in der Windows-Registrierungsdatenbank gesichert werden soll, indem Sie die Option encryptkey verwenden.

Die Verschlüsselung des IBM Spectrum Protect-Clients ermöglicht Ihnen, einen Wert mit einer Länge von bis zu 63 Zeichen einzugeben. Dieses Verschlüsselungskennwort muss bestätigt werden, wenn die Datei für die Sicherung verschlüsselt wird, und es muss außerdem eingegeben werden, wenn Zurückschreibungen verschlüsselter Dateien ausgeführt werden.

Beim Zurückschreiben einer verschlüsselten Datei werden Sie in folgenden Fällen zur Eingabe des Schlüsselkennworts für die Entschlüsselung der Datei aufgefordert:

- Wenn die Option encryptkey auf `Prompt` gesetzt ist.
- Wenn der vom Benutzer angegebene Schlüssel nicht übereinstimmt.
- Wenn die Option encryptkey auf `Save` gesetzt ist und das lokal gesicherte Schlüsselkennwort nicht mit der verschlüsselten Datei übereinstimmt.

Zugehörige Konzepte:
Sicherung (Windows): Weitere Hinweise
Zugehörige Verweise:
Encryptiontype
Encryptkey
Ausschlussoptionen
Einschlussoptionen
Windows-Betriebssysteme

Maximale Dateigröße für Operationen

Die maximale Dateigröße für Sicherung- und Zurückschreibungsoperationen sowie Archivierungs- und Abrufoperationen ist vom verwendeten Windows-Dateisystem abhängig.

Der folgenden Tabelle können Sie die maximale Dateigröße in Byte für das Sichern, Zurückschreiben und Abrufen von Daten entnehmen.

Tabelle 1. Maximale Dateigröße

Dateisystem	Maximale Dateigröße (in Byte)
Windows-BetriebssystemeFAT16	Windows-Betriebssysteme2 147 483 647 (2 GB)
Windows-BetriebssystemeFAT32	Windows-Betriebssysteme4 294 967 295 (4 GB)
Windows-BetriebssystemeNTFS und ReFS	Windows-Betriebssysteme17 592 185 978 880 (16 TB - 64 K)

Windows-Betriebssysteme

Wie der Client lange Benutzer- und Gruppennamen handhabt

Der Client für Sichern/Archivieren kann problemlos Benutzer- und Gruppennamen mit einer Länge von bis zu 64 Zeichen handhaben. Namen, deren Länge 64 Zeichen überschreitet, erfordern jedoch eine besondere Handhabung.

Einschränkung: Überschreiten Sie nicht den Grenzwert von 64 Zeichen für Benutzer- und Gruppennamen. Der Client kürzt den Namen unter Verwendung des folgenden Algorithmus so, dass dieser Grenzwert eingehalten wird: An die ersten 53 Zeichen wird ein Schrägstrich (/) und anschließend die numerische ID als Zeichenfolge angehängt.

Eine Fehlernachricht wird protokolliert, die sowohl den langen Namen als auch die daraus resultierende gekürzte Zeichenfolge enthält. Bei den meisten Funktionen müssen Sie sich über den gekürzten Namen nicht bewusst sein. Es gibt folgende Ausnahmen:

- Befehl set access
- Option fromowner
- (Berechtigungs-)Optionen users und groups

Wenn Sie einen Namen eingeben müssen, müssen Sie in jedem dieser Fälle entweder die Fehlernachricht mit der Konvertierung finden oder den Namen mithilfe der hier dargelegten Regel konstruieren.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-Betriebssysteme

Hinweise vor der Sicherung (UNIX und Linux)

Verschiedene Faktoren in Ihrem System oder Ihrer Umgebung können sich auf die Art und Weise auswirken, wie der Client für Sichern/Archivieren Daten verarbeitet. Lesen Sie diese Hinweise, bevor Sie Ihre Daten sichern.

-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeLAN-unabhängige Datenversetzung
  Mit der LAN-unabhängigen Datenversetzung wird das Versetzen von Clientdaten vom DFV-Netz auf das Speicherbereichsnetz (SAN) verlagert. Dadurch wird die Belastung auf dem IBM Spectrum Protect-Server verringert.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeTeilsicherungen auf Systemen mit Speicherengpässen
  Die Leistung einer Teilsicherung nimmt ab, wenn auf dem System vor dem Start der Sicherung nur wenig Speicher verfügbar ist.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeTeilsicherungen auf Systemen mit einer großen Anzahl an Dateien
  Der Client kann große Speicherkapazitätsanteile verwenden, um Teilsicherungsoperationen auszuführen, insbesondere auf Dateisystemen, die eine große Anzahl an Dateien enthalten.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme
  Einschluss-/Ausschlussoptionen für die Verarbeitungssteuerung
  Möglicherweise gibt es Dateien in Ihren Dateisystemen, die Sie nicht sichern wollen. Bei diesen Dateien kann es sich um Kerndateien, lokale Caches von Netzdateisystemen, Betriebssystem- oder Anwendungsdateien handeln, die durch Neuinstallation des Programms schnell wiederhergestellt werden könnten, oder um beliebige andere Dateien, die leicht wiederhergestellt werden könnten.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDatenverschlüsselung während Sicherungs- oder Archivierungsoperationen
  Die Datensicherheit wird durch die Verschlüsselung von Daten sichergestellt. Verwenden Sie die Datenverschlüsselung für den Schutz von Daten während einer Sicherungs- oder Archivierungsoperation. Die Standardverschlüsselungsoption ist 128-Bit-AES-Verschlüsselung (AES = Advanced Encryption Standard). Für die höchste Stufe der Datenverschlüsselung verwenden Sie die 256-Bit-AES-Datenverschlüsselung durch Angabe der Option encryptiontype.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDateisystem- und ACL-Unterstützung
  Spezielle Dateisysteme enthalten dynamische Informationen, die vom Betriebssystem generiert werden; sie enthalten jedoch keine Daten oder Dateien. Die UNIX- und Linux-Clients ignorieren spezielle Dateisysteme und ihren Inhalt.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeMaximale Dateigröße für Operationen
  Die maximale Dateigröße ist vom Typ eines Dateisystems abhängig. Der Client für Sichern/Archivieren überprüft während Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufoperationen keine Dateigrößenbegrenzung.
-  Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-Betriebssysteme  Oracle Solaris-Betriebssysteme
   Windows-BetriebssystemeLange Benutzer- und Gruppennamen
  Der Client für Sichern/Archivieren kann problemlos Benutzer- und Gruppennamen mit einer Länge von bis zu 64 Zeichen handhaben. Namen, deren Länge 64 Zeichen überschreitet, erfordern jedoch eine besondere Handhabung durch IBM Spectrum Protect.
-  Mac OS X-BetriebssystemeMac OS X-Datenträgernamen
  Der Client für Sichern/Archivieren sichert Datenträger auf der Basis der Namen ihrer UNIX-Mountpunkte.
-  Mac OS X-BetriebssystemeUnicode-Aktivierung für Mac OS X
  Der Mac OS X-Client ist Unicode-aktiviert. Für neue Clients, die zum ersten Mal Daten auf dem Server speichern, ist keine spezielle Konfiguration erforderlich.
-  Mac OS X-BetriebssystemeMac OS X Time Machine-Sicherungsplatte
  Time Machine ist die Sicherungsanwendung, die mit Mac OS X zur Verfügung gestellt wird.

 AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

LAN-unabhängige Datenversetzung

Mit der LAN-unabhängigen Datenversetzung wird das Versetzen von Clientdaten vom DFV-Netz auf das Speicherbereichsnetz (SAN) verlagert. Dadurch wird die Belastung auf dem IBM Spectrum Protect-Server verringert.

Das SAN stellt einen Pfad zur Verfügung, mit dem Sie Daten auf bzw. von einer an das SAN angeschlossenen Speichereinheit sichern, zurückschreiben, archivieren und abrufen können. Die Clientdaten werden mithilfe des IBM Spectrum Protect-Speicheragenten über das SAN auf die Speichereinheit versetzt. Der Speicheragent muss auf demselben System wie der Client installiert werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAIX-, Linux- und Solaris-Clients unterstützen die LAN-unabhängige Datenversetzung.

Windows-BetriebssystemeAlle Windows-Clients unterstützen die LAN-unabhängige Datenversetzung.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeVoraussetzungen für die LAN-unabhängige Datenversetzung
  Um die LAN-unabhängige Unterstützung zu aktivieren, müssen Sie den IBM Spectrum Protect for SAN-Speicheragenten auf der Client-Workstation installieren und konfigurieren.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeOptionen für die LAN-unabhängige Datenversetzung
  Um die LAN-unabhängige Datenversetzung zu aktivieren, können Sie verschiedene Clientoptionen verwenden. Sie müssen zunächst den Speicheragenten von IBM Spectrum Protect for SAN auf der Client-Workstation installieren und konfigurieren.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Voraussetzungen für die LAN-unabhängige Datenversetzung

Um die LAN-unabhängige Unterstützung zu aktivieren, müssen Sie den IBM Spectrum Protect for SAN-Speicheragenten auf der Client-Workstation installieren und konfigurieren.

IBM Spectrum Protect for SAN ist ein separates Produkt.

Weitere Informationen zum Installieren und Konfigurieren des Speicheragenten finden Sie in der Dokumentation zu IBM Spectrum Protect for SAN.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Optionen für die LAN-unabhängige Datenversetzung

Um die LAN-unabhängige Datenversetzung zu aktivieren, können Sie verschiedene Clientoptionen verwenden. Sie müssen zunächst den Speicheragenten von IBM Spectrum Protect for SAN auf der Client-Workstation installieren und konfigurieren.

Verwenden Sie die folgenden Optionen, um die LAN-unabhängige Datenversetzung zu aktivieren:

enablelanfree
: Gibt an, ob ein verfügbarer LAN-unabhängiger Pfad zu einer an ein SAN angeschlossenen Speichereinheit aktiviert werden soll.

lanfreecommmethod
: Gibt ein Übertragungsprotokoll zwischen dem Client und dem Speicheragenten an.

lanfreeshmport
: Gibt die eindeutige Zahl an, die vom Client und vom Speicheragenten verwendet wird, um den für die Datenübertragung verwendeten gemeinsam benutzten Speicherbereich (Shared Memory) zu identifizieren.

lanfreetcpport
: Gibt die Nummer des TCP/IP-Anschlusses an, an dem der Speicheragent empfangsbereit ist.

lanfreetcpserveraddress
: Gibt die TCP/IP-Adresse für den Speicheragenten an.

Zugehörige Verweise:
Enablelanfree
Lanfreecommmethod
Lanfreeshmport
Lanfreessl
Lanfreetcpport
Lanfreetcpserveraddress
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Teilsicherungen auf Systemen mit Speicherengpässen

Die Leistung einer Teilsicherung nimmt ab, wenn auf dem System vor dem Start der Sicherung nur wenig Speicher verfügbar ist.

Ist der Speicher auf Ihrem System begrenzt, geben Sie die Option memoryefficientbackup *yes* in Ihrer Clientoptionsdatei an. Diese Option hat zur Folge, dass der Client für Sichern/Archivieren jeweils nur ein einzelnes Verzeichnis verarbeitet, wodurch der Speicherbedarf reduziert, die Sicherungszeit jedoch verlängert wird. Wenn Sie *yes* angeben, analysiert der Client jeweils nur ein einzelnes Verzeichnis für die Sicherung. Bleibt die Leistung schlecht, müssen Sie die Einstellungen des DFV-Puffers und die DFV-Verbindung zwischen Ihrem System und dem IBM Spectrum Protect-Server überprüfen. Steht auf Ihrem System genügend Speicher zur Verfügung, führt das Setzen der Option memoryefficientbackup auf *yes* zu einer Verschlechterung der Sicherungsleistung.

Zugehörige Verweise:
Memoryefficientbackup

Teilsicherungen auf Systemen mit einer großen Anzahl an Dateien

Der Client kann große Speicherkapazitätsanteile verwenden, um Teilsicherungsoperationen auszuführen, insbesondere auf Dateisystemen, die eine große Anzahl an Dateien enthalten.

Der Begriff *Speicher*, wie er hier verwendet wird, bezeichnet den adressierbaren Hauptspeicher, der für den Clientprozess verfügbar ist. Der adressierbare Hauptspeicher ist eine Kombination aus physischem Arbeitsspeicher (RAM) und virtuellem Speicher.

Der Client verwendet durchschnittlich ca. 300 Byte an Speicher pro Objekt (Datei oder Verzeichnis). Somit erfordert der Client für ein Dateisystem mit einer Million Dateien und Verzeichnisse im Durchschnitt ca. 300 MB Speicher. Die genaue Speicherkapazität, die pro Objekt verwendet wird, variiert abhängig von der Länge des Objektpfads und der Länge des Namens oder von der Verschachtelungstiefe der Verzeichnisse. Die Anzahl Datenbyte ist kein wichtiger Faktor bei der Ermittlung des Speicherbedarfs für den Client für Sichern/Archivieren.

Die maximale Anzahl Dateien kann ermittelt werden, indem die für einen Prozess verfügbare maximale Speicherkapazität durch die pro Objekt benötigte durchschnittliche Speicherkapazität dividiert wird.

Der Gesamtspeicherbedarf kann durch eine der folgenden Methoden reduziert werden:

- Verwenden Sie die Clientoption memoryefficientbackup diskcachemethod. Mit dieser Auswahl wird die Speicherbelegung auf Kosten der Leistung und einer signifikanten Zunahme des für die Sicherung erforderlichen Plattenspeicherplatzes auf ein Minimum reduziert. Die Dateibeschreibungsdaten vom Server sind in einer plattenresidenten temporären Datenbank gespeichert, nicht im Hauptspeicher. Sobald die Verzeichnisse auf der Workstation durchsucht werden, wird die Datenbank befragt, um festzustellen, ob die einzelnen Objekte gesichert, aktualisiert oder als verfallen markiert werden sollen. Bei Beendigung der Sicherung wird die Datenbankdatei gelöscht.
- Verwenden Sie die Clientoption memoryefficientbackup yes. Der durchschnittlich vom Client verwendete Speicher ergibt sich dann aus 300 Byte mal der Anzahl an Verzeichnissen plus 300 Byte pro Datei in dem Verzeichnis, das verarbeitet wird. Bei Dateisystemen mit einer großen Anzahl (Millionen) an Verzeichnissen ist der Client unter Umständen trotzdem nicht in der Lage, ausreichend Speicher zuzuordnen, um Teilsicherungen mit memoryefficientbackup yes auszuführen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeUNIX- und Linux-Clients können möglicherweise die Clientoption virtualmountpoint verwenden, um mehrere virtuelle Mountpunkte innerhalb eines einzelnen Dateisystems zu definieren, wobei jeder separat vom Client gesichert werden kann.
- Ist die Clientoption resourceutilization auf einen Wert größer als 4 gesetzt und werden mehrere Dateisysteme gesichert, wird durch Reduzieren von resourceutilization auf maximal 4 der Prozess auf die Teilsicherung jeweils eines einzelnen Dateisystems begrenzt. Diese Einstellung verringert den Speicherbedarf. Ist aus Leistungsaspekten eine parallele Sicherung mehrerer Dateisysteme erforderlich und überschreitet der kombinierte Speicherbedarf die Verarbeitungslimits, können mehrere Instanzen des Sicherungsclients verwendet werden, um mehrere Dateisysteme parallel zu sichern. Wenn Sie z. B. zwei Dateisysteme gleichzeitig sichern wollen, aber deren Speicherbedarf die Grenzwerte eines einzelnen Prozesses überschreitet, dann starten Sie eine Instanz des Clients, um das eine Dateisystem zu sichern, und starten eine zweite Instanz des Clients, um das andere Dateisystem zu sichern.
- Verwenden Sie die Clientoption -incrbydate, um eine "Teilsicherung nach Datum" auszuführen.
- Verwenden Sie die Clientoption exclude.dir, um zu verhindern, dass der Client Verzeichnisse traversiert und sichert, die nicht gesichert werden müssen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeVerwenden Sie mit Ausnahme von Mac OS X die Clientfunktion für Imagesicherung, um den gesamten Datenträger zu sichern. Eine Imagesicherung könnte in Wirklichkeit weniger Systemressourcen verwenden und schneller ausgeführt werden als eine Teilsicherung einiger Dateisysteme mit einer großen Anzahl kleiner Dateien.
- Reduzieren Sie die Anzahl Dateien pro Dateisystem, indem Sie die Daten auf mehrere Dateisysteme verteilen.

Zugehörige Verweise:
Snapdiff
Ausschlussoptionen
Incrbydate
Memoryefficientbackup
Resourceutilization
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeVirtualmountpoint
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Einschluss-/Ausschlussoptionen für die Verarbeitungssteuerung

Möglicherweise gibt es Dateien in Ihren Dateisystemen, die Sie nicht sichern wollen. Bei diesen Dateien kann es sich um Kerndateien, lokale Caches von Netzdateisystemen, Betriebssystem- oder Anwendungsdateien handeln, die durch Neuinstallation des Programms schnell wiederhergestellt werden könnten, oder um beliebige andere Dateien, die leicht wiederhergestellt werden könnten.

Sie können mithilfe der Optionen exclude und include in der Einschluss-/Ausschlussoptionsliste angeben, welche Dateien von der Sicherungsverarbeitung ausgeschlossen werden sollen.

Verwenden Sie die Optionen include und exclude in dsm.sys, um die Dateien zu definieren, die in die Teilsicherungsverarbeitung oder die selektive Sicherungsverarbeitung eingeschlossen oder davon ausgeschlossen werden sollen. Eine Datei ist für die Sicherung auswählbar, wenn sie nicht durch die Option exclude ausgeschlossen ist. Zum Einschließen bestimmter Dateien in die Sicherung muss die Option include nur verwendet werden, wenn sich diese Dateien in einem Verzeichnis befinden, das andere Dateien enthält, die ausgeschlossen werden sollen.

IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden. Bei jeder Sicherung einer Datei wird ihr eine Verwaltungsklasse zugeordnet. Bei der Verwaltungsklasse kann es sich um die Standardverwaltungsklasse handeln, die für Sie ausgewählt wurde, oder um eine Verwaltungsklasse, die Sie der Datei mit der Option include in der Einschluss-/Ausschlussoptionsliste zuordnen. Wenn Sie eine Verwaltungsklasse zuordnen, muss sie eine Sicherungskopiengruppe enthalten, damit die Datei gesichert wird.

Zugehörige Tasks:
Einschluss-/Ausschlussliste erstellen
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

Datenverschlüsselung während Sicherungs- oder Archivierungsoperationen

Die Datensicherheit wird durch die Verschlüsselung von Daten sichergestellt. Verwenden Sie die Datenverschlüsselung für den Schutz von Daten während einer Sicherungs- oder Archivierungsoperation. Die Standardverschlüsselungsoption ist 128-Bit-AES-Verschlüsselung (AES = Advanced Encryption Standard). Für die höchste Stufe der Datenverschlüsselung verwenden Sie die 256-Bit-AES-Datenverschlüsselung durch Angabe der Option encryptiontype.

Die Daten, die Sie einschließen, werden in verschlüsselter Form gespeichert; die Verschlüsselung hat keine Auswirkungen auf das gesendete oder empfangene Datenvolumen.

Die Option include.encrypt ist die einzige Möglichkeit, die Verschlüsselung auf dem Client für Sichern/Archivieren zu aktivieren. Werden keine Anweisungen 'include.encrypt' verwendet, kann keine Verschlüsselung stattfinden.

 Linux-BetriebssystemeDie Verschlüsselung ist nicht kompatibel mit Sicherungen virtueller VMware-Maschinen im Modus der immer inkrementellen Sicherung (MODE=IFIncremental und MODE=IFFull). Ist der Client für die Verschlüsselung konfiguriert, können Sie nicht die immer inkrementelle Sicherung verwenden.

Verwenden Sie die Optionen include und exclude in dsm.sys, um die Dateien zu definieren, die in die Teilsicherungsverarbeitung oder die selektive Sicherungsverarbeitung eingeschlossen oder davon ausgeschlossen werden sollen. Eine Datei ist für die Sicherung auswählbar, wenn sie nicht durch die Option exclude ausgeschlossen ist. Zum Einschließen bestimmter Dateien in die Sicherung muss die Option include nur verwendet werden, wenn sich diese Dateien in einem Verzeichnis befinden, das andere Dateien enthält, die ausgeschlossen werden sollen.

Um Dateidaten zu verschlüsseln, müssen Sie einen Kennwort für den Verschlüsselungsschlüssel auswählen, das der Client zum Generieren des Verschlüsselungsschlüssels zum Verschlüsseln und Entschlüsseln der Dateidaten generiert. Bewahren Sie das Kennwort für den Verschlüsselungsschlüssel für die spätere Verwendung auf. Sie können angeben, ob das Kennwort für den Verschlüsselungsschlüssel in einer Datei mit dem Namen TSM.sth gespeichert werden soll, indem Sie die Option encryptkey verwenden.

Die Verschlüsselung des IBM Spectrum Protect-Clients ermöglicht Ihnen, einen Wert mit einer Länge von bis zu 63 Zeichen einzugeben. Dieses Verschlüsselungskennwort muss bestätigt werden, wenn die Datei für die Sicherung verschlüsselt wird, und es muss außerdem eingegeben werden, wenn Zurückschreibungen verschlüsselter Dateien ausgeführt werden.

Beim Zurückschreiben der verschlüsselten Datei werden Sie in folgenden Fällen vom Client zur Eingabe des Schlüsselkennworts für die Entschlüsselung der Datei aufgefordert:

- Die Option encryptkey ist auf `Prompt` gesetzt.
- Der vom Benutzer angegebene Schlüssel im vorherigen Fall stimmt nicht überein.
- Die Option encryptkey ist auf `Save` gesetzt und das lokal gespeicherte Schlüsselkennwort stimmt nicht mit der verschlüsselten Datei überein.

Zugehörige Verweise:
Encryptiontype
Encryptkey
Ausschlussoptionen
Einschlussoptionen
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Dateisystem- und ACL-Unterstützung

Spezielle Dateisysteme enthalten dynamische Informationen, die vom Betriebssystem generiert werden; sie enthalten jedoch keine Daten oder Dateien. Die UNIX- und Linux-Clients ignorieren spezielle Dateisysteme und ihren Inhalt.

Zu den speziellen Dateisystemen gehören die folgenden Typen:

- Dateisystem `/proc` auf den meisten UNIX-Plattformen
- Dateisystem `/dev/fd` unter Solaris
- `/dev/pts` unter Linux

Der Client für Sichern/Archivieren kann gängige spezifische Dateisystemtypen verarbeiten. Eine Liste der unterstützten Dateisystemtypen finden Sie in Tabelle 1.

Einschränkung: Die Tabelle zeigt vollständige Unterstützung für NFS unter AIX, einschließlich der Erhaltung von ACLs und erweiterten Attributen. Bei anderen Betriebssystemen werden NFS-Sicherungen unterstützt, aber die Sicherungen enthalten nur POSIX-Standardmetadaten (Zugriffsberechtigungen, Erstellungsdatum etc.). Weitere Informationen zur Sicherung von NFS-Dateisystemen finden Sie in NFS-Dateien sichern.

Tabelle 1. Unterstützte Dateisysteme und ACL-Unterstützung

Plattform	Dateisystem	ACL-Unterstützung
AIX-BetriebssystemeAIX	AIX-Betriebssysteme GPFS JFS JFS2 JFS2 NFSV4 VxFS	AIX-Betriebssysteme Ja Ja Ja Ja Ja
Linux-BetriebssystemeLinux x86_64	Linux-Betriebssysteme BtrfsXFS EXT2 EXT3 EXT4 ReiserFS GPFS JFS VxFS NSS	Linux-Betriebssysteme Ja Ja Ja Ja Ja Ja Ja Nein Nein Ja
Linux-BetriebssystemeLinux on Power Systems Servers	Linux-Betriebssysteme BtrfsXFS EXT2 EXT3 EXT4 ReiserFS JFS GPFS	Linux-Betriebssysteme Ja Ja Ja Ja Ja Ja Nein Ja
Linux-BetriebssystemeLinux on z Systems	Linux-Betriebssysteme BtrfsEXT2 EXT3 EXT4 ReiserFS JFS GPFS	Linux-Betriebssysteme Ja Ja Ja Ja Ja Nein Ja
Mac OS X-BetriebssystemeMac OS	Mac OS X-Betriebssysteme HFS Standard (HFS) HFS Extended (HFS+) HFS Extended mit Unterscheidung der Groß-/Kleinschreibung (HFSX) Xsan (XSAN) Universal Disk Format (UDF) ISO9660	Mac OS X-Betriebssysteme Ja Ja Ja Ja Ja Ja Ja
Oracle Solaris-Betriebssysteme Solaris	Oracle Solaris-Betriebssysteme UFS VxFS QFS ZFS	Oracle Solaris-Betriebssysteme Ja Ja Nein Ja

AIX-BetriebssystemeOracle Solaris-BetriebssystemeBei Dateisystemen, bei denen NFS V4-ACLs definiert sind und verwendet werden (Solaris ZFS und AIX JFS2 V2), wird die Datei oder das Verzeichnis erneut vollständig gesichert, selbst wenn sich nur die UNIX-Standardberechtigungen oder ACLs geändert haben (wie z. B. mit dem Befehl CHMOD). Bei anderen Dateisystemen verursacht diese Art der Änderung nur eine Attributaktualisierung auf dem IBM Spectrum Protect-Server.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeZur Verarbeitung aller anderen Dateisysteme verwenden Sie die Option virtualmountpoint, um Unterstützung für die folgenden Elemente zu aktivieren:

- Für Sicherung, Zurückschreibung, Archivierung und Abruf von Dateidaten
- Für grundlegende UNIX- und Linux-Berechtigungen
- Für Zeitmarken für Änderung, Zugriff und Modifikation und die Verzeichnisbaumstruktur

Keine anderen dateisystemspezifischen Attribute, z. B. die ACL, sind gültig. Der Dateisystemtyp für solche Dateisysteme wird auf "UNKNOWN" (UNBEKANNT) gesetzt.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeWird beispielsweise das Dateisystem `/media/abc/DATA1` vom Client nicht unterstützt, fügen Sie dsm.sys die folgende Anweisung hinzu, um die Daten in diesem Dateisystem zu sichern oder zu archivieren:

```
VIRTUALMOUNTPOINT /media/abc/DATA1
```

Diese Unterstützung steht nur zur Verfügung, wenn das Dateisystem selbst grundlegende POSIX-Systemaufrufe wie die Lese- und Schreibverarbeitung auf Ihrem System verwenden kann.
Die plattformübergreifende Sicherung und Zurückschreibung wird nicht unterstützt. Beispielsweise stehen Daten, die von einem AIX-Client gesichert wurden, nicht für die Zurückschreibung durch einen Windows-Client zur Verfügung und umgekehrt.
 Mac OS X-BetriebssystemeAnmerkung: Vom Mac OS X-Client gesicherte oder archivierte Daten können von keinem anderen Client zurückgeschrieben werden. Außerdem kann der Mac OS X-Client keine Daten von einem anderen Client zurückschreiben oder abrufen.

Die Methode zum Zurückschreiben oder Abrufen von ACL-Informationen in einen anderen Dateisystemtyp kann verwendet werden, wenn das ursprüngliche Dateisystem und das Zieldateisystem kompatible ACLs unterstützen. So können z. B. unter Solaris die ACL-Informationen, die von einem VxFS-Dateisystem gesichert wurden, auf ein UFS-Dateisystem zurückgeschrieben werden, da diese Dateisysteme kompatible ACLs unterstützen. Bei Operationen zum Zurückschreiben oder Abrufen in andere Dateisystemtypen werden die ACL-Informationen nicht zurückgeschrieben, wenn das ursprüngliche Dateisystem und das Zieldateisystem keine ACLs unterstützen.

Das Standalone-Paket LSCqfs 3.5.0 ist die einzig unterstützte Version von QFS. Zusätzlich gelten auch die folgenden Einschränkungen für das QFS-Dateisystem:

-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDie Imagesicherung wird auf QFS-Dateisystemen nicht unterstützt.
- Der Solaris-Client für Sichern/Archivieren unterstützt nicht die Kombination von QFS und SAM, die benötigt wird, um Dateien auf tertiärem Hintergrundspeicher wie z. B. Bändern zu archivieren. Stattdessen ruft er Dateien automatisch vom Band auf Platte zurück, wenn er während einer Sicherung umgelagerte Dateien findet.
- Ein QFS-Dateisystem enthält zwei verdeckte Systemdateien und ein Systemverzeichnis, die nicht gesichert werden können. Dies kann akzeptiert werden, da eine Sicherung dieser Dateien nicht notwendig ist. Sie enthalten interne Daten zum Verwalten des Dateisystems. Die internen Daten werden automatisch von einer Sicherung ausgeschlossen und vom Dateisystem selbst automatisch erneut erstellt, wenn eine Zurückschreibung von Dateien in diesem Dateisystem ausgeführt wird.

Unter AIX werden Sicherungs-, Archivierungs-, Zurückschreibungs- und Abrufoperationen mit den Verarbeitungsmodi Teil, selektiv und Dateiliste bei Veritas-Dateisystemen und den zugehörigen ACLs unterstützt. Die Zurückschreibung eines Veritas-Datenträgers auf einen Logical Volume Manager-Datenträger und umgekehrt ist möglich, wenn beide Datenträger denselben Dateisystemtyp verwenden.

 Mac OS X-BetriebssystemeDie folgenden Informationen gelten nur für Mac OS X-Systeme:

- Auf Mac OS X-Systemen unterscheiden die Dateisysteme UFS und HFSX die Groß-/Kleinschreibung, während das Dateisystem HFS+ die Groß-/Kleinschreibung nicht unterscheidet, jedoch vorhandene Groß-/Kleinschreibung beibehält. Dateien, die Sie auf einem UFS- oder HFSX-Dateisystem sichern (diese unterscheiden die Groß-/Kleinschreibung), werden auf einem HFS+-Dateisystem möglicherweise nicht korrekt zurückgeschrieben (dieses unterscheidet die Groß-/Kleinschreibung nicht). Beispiel: Auf einem UFS-Dateisystem werden die Dateien `Afile` und `afile` als verschiedene Dateien angesehen. Auf einem HFS+-Dateisystem werden diese beiden Dateien jedoch als identisch angesehen.
- Wenn unter Mac OS X HFS+- oder UFS-Dateisysteme verwendet werden, bei denen die Groß-/Kleinschreibung beachtet werden muss, ist es wichtig, dass die Daten des HFSX- oder UFS-Dateisystems nicht in einem HFS+-Dateisystem auf dem IBM Spectrum Protect-Server gesichert werden. Entweder muss ein neuer Name auf dem System verwendet werden oder der vorhandene Dateibereich auf dem IBM Spectrum Protect-Server muss umbenannt werden. Beispiel: Angenommen, ein System verfügt über ein Dateisystem mit dem Namen `/Volumes/fs2` und dieses System wird mit einem HFS+-Dateisystem mit Unterscheidung der Groß-/Kleinschreibung erneut partitioniert. Entweder muss das Dateisystem `/Volumes/fs2` auf dem IBM Spectrum Protect-Server umbenannt werden oder auf dem lokalen System muss ein neuer Name verwendet werden. Wenn diese Umbenennung nicht erfolgt, werden HFSX-Daten, bei denen die Groß-/Kleinschreibung beachtet werden muss, mit HFS+-Daten gemischt, bei denen die Groß-/Kleinschreibung nicht beachtet werden muss und die bereits auf dem IBM Spectrum Protect-Server gespeichert sind.
- Unter Mac OS X werden Aliasnamen und symbolische Verbindungen gesichert. Der Client sichert jedoch nicht die Daten, auf die die symbolischen Verbindungen verweisen.
- Wenn unter Mac OS X auf einem HFS-Datenträger gesicherte Daten auf einen UFS-Datenträger zurückgeschrieben werden, werden die Ressourcenzweige nicht den richtigen Eignern zugeordnet. Beheben Sie diesen Fehler durch Verwenden des Befehls chown für die Ressourcenzweigdatei, um den Eigner zu ändern. In der Ressourcenzweigdatei sind strukturierte Daten in einer Datei gespeichert.

 Linux-BetriebssystemeUnter Linux on POWER und Linux on System z müssen Sie libacl.so installieren, damit der Client ACLs sichert.

 AIX-Betriebssysteme  Linux-BetriebssystemeWichtig: Wenn Sie GPFS für AIX, GPFS für Linux x86_64 oder GPFS für Linux on z Systems in einem Cluster mit mehreren Knoten ausführen und alle Knoten ein angehängtes GPFS-Dateisystem gemeinsam nutzen, verarbeitet der Client dieses Dateisystem als lokales Dateisystem. Der Client sichert während einer Teilsicherung das Dateisystem auf jedem Knoten. Um dies zu vermeiden, können Sie einen der folgenden Schritte ausführen:

- Konfigurieren Sie explizit die Anweisung domain in der Clientbenutzeroptionsdatei (dsm.opt), sodass die Dateisysteme, die auf diesem Knoten gesichert werden sollen, aufgelistet werden.
- Definieren Sie die Option exclude.fs in der Datei dsm.sys, damit das GPFS-Dateisystem von den Sicherungsservices ausgeschlossen wird.

Wenn der GPFS-Cluster unterschiedliche Plattformen enthält, dürfen Sie Clients für Sichern/Archivieren nur auf einer einzigen Plattform verwenden, um ein einzelnes Dateisystem zu schützen. Sie dürfen Clients für Sichern/Archivieren nicht auf mehreren Plattformen verwenden, um ein GPFS-Dateisystem zu schützen, das von mehreren Plattformen gemeinsam genutzt wird.

Angenommen, ein Cluster enthält Knoten auf AIX-, Linux x86- und Linux zSeries-Systemen. Sie können Dateisystem A mit AIX-Clients für Sichern/Archivieren und Dateisystem B mit Linux zSeries-Clients für Sichern/Archivieren schützen. Es ist auch möglich, Dateisystem A und Dateisystem B mit AIX-Clients für Sichern/Archivieren zu schützen. Wenn Sie Dateisystem A mit einem AIX-Client für Sichern/Archivieren schützen, dürfen Sie Dateisystem A nicht mit einem Client für Sichern/Archivieren auf einer anderen Plattform als AIX schützen.

Unterstützung der betriebssystemübergreifenden Wiederherstellung für in IBM Spectrum Scale-Dateisystemen gespeicherte Dateien

In einem IBM Spectrum Scale-Cluster mit mehreren Betriebssystemtypen kann eine Datei, die ACL-Metadaten oder Metadaten für erweiterte Attribute enthält und auf einem Quellenbetriebssystem gesichert wurde, auf einem Zielbetriebssystem zurückgeschrieben werden. Die ACL-Metadaten oder Metadaten für erweiterte Attribute werden korrekt zurückgeschrieben, falls beide Betriebssystemtypen auf der Quelle und auf dem Ziel dieselbe Version von IBM Spectrum Scale verwenden.

Die folgenden Quellenbetriebssystemtypen werden unterstützt:

- AIX
- Linux for IBM System Power Big Endian (pBE)
- Linux x86
- Linux for IBM System z

Die folgenden Zielbetriebssystemtypen werden unterstützt:

- Linux for IBM System Power Little Endian (pLE)
- Linux x86
- Linux for IBM System z

Die Sicherheitseinstellungen für betroffene Benutzer und Gruppen müssen auf den Quellen- und Zielsystemen übereinstimmen.

Mischen Sie keine Betriebssystemtypen bei Sicherungsaktivitäten. Wählen Sie nur einen einzigen Betriebssystemtyp aus, der in Ihrem IBM Spectrum Scale-Cluster verfügbar ist, und verwenden Sie ihn für alle Sicherungsoperationen.

Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Maximale Dateigröße für Operationen

Die maximale Dateigröße ist vom Typ eines Dateisystems abhängig. Der Client für Sichern/Archivieren überprüft während Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufoperationen keine Dateigrößenbegrenzung.

Wenn das Dateisystem die Erstellung der Datei ermöglicht, sichert oder archiviert der Client die Datei.

In der folgenden Tabelle sind die maximalen Dateigrößen für die nativen Dateisysteme auf UNIX- und Linux-Clientplattformen angegeben.

Tabelle 1. Maximale Dateigröße

Plattform	Max. Dateigröße (in Byte)
AIX-BetriebssystemeAIX 6.1 (JFS2) - maximale Größe	AIX-Betriebssysteme Maximale JFS2-Dateisystemgröße: 32 TB Maximale JFS2-Dateigröße: 16 TB Minimale JFS2-Dateisystemgröße: 16 MB
Linux-BetriebssystemeAlle Linux-Clients	Linux-Betriebssysteme9 223 372 036 854 775 807 (8 EB - 1)
Mac OS X-BetriebssystemeMac OS X	Mac OS X-Betriebssysteme HFS - 2 147 485 648 (2 GB) HFS+, HFSX, XSAN und UFS - 9 223 372 036 854 775 808 (8 EB)
Oracle Solaris-BetriebssystemeSolaris	Oracle Solaris-Betriebssysteme1 099 511 627 775 (1 TB - 1)
Oracle Solaris-BetriebssystemeSolaris (ZFS)	Oracle Solaris-Betriebssysteme18 446 744 073 709 551 616 (16 EB)

Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme

Lange Benutzer- und Gruppennamen

Der Client für Sichern/Archivieren kann problemlos Benutzer- und Gruppennamen mit einer Länge von bis zu 64 Zeichen handhaben. Namen, deren Länge 64 Zeichen überschreitet, erfordern jedoch eine besondere Handhabung durch IBM Spectrum Protect.

Wichtig: Überschreiten Sie nicht den Grenzwert von 64 Zeichen für Benutzer- und Gruppennamen. Andernfalls kürzt der Client den Namen unter Verwendung der folgenden Umsetzung so, dass dieser Grenzwert eingehalten wird: An die ersten 53 Zeichen wird ein Schrägstrich (/) und anschließend die numerische ID als Zeichenfolge angehängt.

Eine Fehlernachricht wird protokolliert, die sowohl den langen Namen als auch die daraus resultierende gekürzte Zeichenfolge enthält. Bei den meisten Funktionen müssen Sie sich über den gekürzten Namen nicht bewusst sein. Es gibt folgende Ausnahmen:

- Befehl set access
- Option fromowner
- (Berechtigungs-)Optionen users und groups

Wenn Sie einen Namen eingeben müssen, müssen Sie in jedem dieser Fälle entweder die Fehlernachricht mit der Konvertierung finden oder den Namen mithilfe der hier dargelegten Regel konstruieren.

Mac OS X-Betriebssysteme

Mac OS X-Datenträgernamen

Der Client für Sichern/Archivieren sichert Datenträger auf der Basis der Namen ihrer UNIX-Mountpunkte.

IBM Spectrum Protect verwaltet jeden Datenträgernamen als separaten Zurückschreibungs- oder Abrufdatenträger. Diese Datenträgernamen werden als Namen der Dateibereiche auf dem Server verwendet.

Wenn Sie den Namen eines Datenträgers ändern, der bereits gesichert wurde, betrachtet der Client den Datenträger als neuen Datenträger, ohne ihn mit dem bereits vorhandenen Datenträger in Zusammenhang zu bringen. Bei Sicherungen werden die Dateien unter dem neuen Namen gesichert. Eine Abweichung kann auftreten, wenn Sie Ihre Datenträger umbenennen oder wenn Sie auf IBM Spectrum Protect von einer anderen Workstation aus zugreifen als derjenigen, von der die Daten gesichert wurden.

- Mac OS X-BetriebssystemeHinweise in Bezug auf Mac OS X-Datenträgernamen
  IBM Spectrum Protect erstellt alle neuen Dateibereiche auf dem Server mit dem UNIX-Mountpunkt des Datenträgers.
- Mac OS X-BetriebssystemeHinweise in Bezug auf Datenträgernamen für Mac OS X-Dual-Boot-Systeme
  Wenn Sie über mehrere Mac OS X-Versionen verfügen, zwischen denen Sie wechseln, müssen Sie verstehen, wie der Client die UNIX-Mountpfade für Dateibereichsnamen auf dem IBM Spectrum Protect-Server verwendet.

Mac OS X-Betriebssysteme

Hinweise in Bezug auf Mac OS X-Datenträgernamen

IBM Spectrum Protect erstellt alle neuen Dateibereiche auf dem Server mit dem UNIX-Mountpunkt des Datenträgers.

Sind zwei Datenträger mit Namen wie "`La Pomme`" und "`la pomme`" vorhanden, werden zwei eindeutige UNIX-Mountpunkte erstellt.

Die folgenden Beispiele zeigen die beiden Mountpunkte, die erstellt werden:

```
/Volumes/La Pomme
/Volumes/la pomme
```

Wenn doppelte Datenträger auf Ihrem Desktop doppelt vorhanden sind, können sich die UNIX-Mountpunkte von den Mountpunkten bei der letzten Sicherung unterscheiden, die vom Client ausgeführt wurde. Der Client sichert die Daten möglicherweise nicht im korrekten Dateisystem auf dem IBM Spectrum Protect-Server.

Sie können das Dateisystem überprüfen, in dem der Client die Daten sichert:

1. Wählen Sie im Fenster zum Durchführen von Sicherungen ein Dateisystem aus.
2. Klicken Sie auf **Datei** → **Info anzeigen**.

Der UNIX-Mountpunkt befindet sich im Informationsdialog.

Potenzielle Probleme mit Namen lassen sich am besten vermeiden, wenn Sie sicherstellen, dass die Datenträgernamen eindeutig sind.

Wichtig:

- Der Client verwendet weiterhin die vorhandenen Dateibereichsnamen auf dem IBM Spectrum Protect-Server. Nur bei neuen Dateibereichen wird der UNIX-Mountpunkt als Name verwendet.
- Geben Sie keine Datenträger an, deren Name Punkte enthält (...). Der Client verwendet die Punktesequenz als Teil der Einschluss-/Ausschlussverarbeitung. Der Client meldet eine ungültige Einschluss-/Ausschlussanweisung zurück, wenn ein

Datenträgername eine Punktesequenz enthält. Der Datenträger *muss* umbenannt werden.


Mac OS X-Betriebssysteme

Hinweise in Bezug auf Datenträgernamen für Mac OS X-Dual-Boot-Systeme

Wenn Sie über mehrere Mac OS X-Versionen verfügen, zwischen denen Sie wechseln, müssen Sie verstehen, wie der Client die UNIX-Mountpfade für Dateibereichsnamen auf dem IBM Spectrum Protect-Server verwendet.

Angenommen, ein Dual-Boot-System verfügt über zwei Datenträger, `El Capitan` und `Sierra`. Im Finder und in der GUI des Clients für Sichern/Archivieren werden diese als `El Capitan` und `Sierra` angezeigt. Die UNIX-Mountpunkte sind jedoch davon abhängig, welche Version von Mac OS aktiv ist. Wenn 'El Capitan' die Startdiskette ist, lauten die UNIX-Pfade wie folgt:

```
/
/Volumes/Sierra
```

Wenn 'Sierra' die Startdiskette ist, lauten die UNIX-Pfade wie folgt:

```
/
/Volumes/El Capitan
```

Wenn eine Sicherungs- oder Archivierungsoperation ausgeführt wird, sind die Dateibereichsnamen auch davon abhängig, welche Version von Mac OS X aktiv ist.

Unter beiden Mac OS X-Versionen werden Sicherungen in das Dateisystem `/` auf dem IBM Spectrum Protect-Server gestellt. Die Folge ist, dass die Dateisysteme vermischt werden.

Führen Sie eine der folgenden Tasks aus, um potenzielle Probleme mit Dual-Boot-Systemen zu vermeiden:

1. Wählen Sie eine Version von Mac OS X aus, unter der Sie IBM Spectrum Protect installieren und ausführen. Damit wird sichergestellt, dass UNIX-Mountpunkte jedes Mal, wenn der Client eine Sicherung ausführt, identisch sind.
2. Konfigurieren Sie jede Mac OS X-Version mit einem eindeutigen IBM Spectrum Protect-Knotennamen. Schließen Sie dann die andere Mac OS X-Version mit einer Anweisung 'domain' in der Systemoptionsdatei von der Sicherungsverarbeitung aus. Wenn beispielsweise der Datenträger 'Sierra' die Startdiskette ist, fügen Sie der Systemoptionsdatei die folgende Option hinzu:

   ```
   DOMAIN -/Volumes/El Capitan
   ```

   Wenn der Datenträger 'El Capitan' die Startdiskette ist, fügen Sie der Systemoptionsdatei Folgendes hinzu:

   ```
   DOMAIN -/Volumes/Sierra
   ```


Mac OS X-Betriebssysteme

Unicode-Aktivierung für Mac OS X

Der Mac OS X-Client ist Unicode-aktiviert. Für neue Clients, die zum ersten Mal Daten auf dem Server speichern, ist keine spezielle Konfiguration erforderlich.

Der Server speichert Dateien und Verzeichnisse automatisch als Unicode-aktiviert. Wenn Sie jedoch ein Upgrade auf den Unicode-aktivierten Client durchführen, müssen Sie die Migration der vorhandenen Dateibereiche planen, sodass diese Unicode unterstützen können.

Alle Dateibereiche, die sich bereits auf dem Server befinden, müssen umbenannt werden, damit Unicode-aktivierte Dateibereiche erstellt werden können. Verwenden Sie die Option autofsrename, um vorhandene Dateibereiche umzubenennen.

Zugehörige Verweise:
Autofsrename

Mac OS X-Betriebssysteme

Mac OS X Time Machine-Sicherungsplatte

Time Machine ist die Sicherungsanwendung, die mit Mac OS X zur Verfügung gestellt wird.

IBM Spectrum Protect kann zusammen mit der Anwendung Mac OS X Time Machine verwendet werden. Aufgrund des besonderen Sicherungsverfahrens der Anwendung Mac OS X Time Machine sind jedoch die folgenden Hinweise zu beachten, bevor Sie den Client für Sichern/Archivieren zum Sichern von Mac OS X Time Machine-Daten verwenden.

- Die Mac OS X Time Machine-Sicherungsplatte verwendet sehr viele feste Verbindungen für sowohl Dateien als auch Verzeichnisse, um die Plattenbelegung zu minimieren. Beträgt die Kapazität der mit der Anwendung Mac OS X Time Machine gesicherten Platte beispielsweise 5 GB, werden bei der ersten Sicherung 5 GB Daten auf die Mac OS X Time Machine-Sicherungsplatte kopiert.

  Bei nachfolgenden Sicherungen werden nur die Dateien kopiert, die sich seit der letzten Sicherung geändert haben. Für alle nicht geänderten Dateien und Verzeichnisse werden feste Verbindungen zu der Version erstellt, die bei der vorherigen Sicherung kopiert wurde.

Der Finder zeigt eine Größe von 5 GB für jede Sicherung an, sodass die Gesamtgröße 10 GB beträgt. Durch die Verwendung von festen Verbindungen liegt die gesamte Plattenbelegung jedoch nur knapp über 5 GB.

Alle fest verbundenen Objekte, die sich noch nicht auf dem IBM Spectrum Protect-Server befinden, werden gesichert.

So werden in dem Beispiel 10 GB Daten an den IBM Spectrum Protect-Server gesendet.

- Wenn fest verbundene Dateien zurückgeschrieben werden, erstellt der Client die ursprüngliche feste Verbindung erneut. Die erneute Erstellung der ursprünglichen festen Verbindung ist jedoch nur möglich, wenn *alle* fest verbundenen Dateien gleichzeitig zurückgeschrieben werden. Die gleichzeitige Zurückschreibung aller fest verbundenen Dateien ist keine praktische Methode für eine große Sicherungsplatte, die die Anwendung Mac OS X Time Machine verwendet.
- Wenn die Anwendung Mac OS X Time Machine Dateien auf die Sicherungsplatte kopiert, werden den Dateien Zugriffssteuerungslisten (ACLs) hinzugefügt, um ihre Löschung zu verhindern. Der Client für Sichern/Archivieren kann Dateien mit ACLs sichern und zurückschreiben. Bei allen zurückgeschriebenen Dateien müssen jedoch diese restriktiven ACLs in Kraft sein.

Tipp: Um die besten Ergebnisse zu erzielen, schließen Sie die Sicherungsdaten der Anwendung Time Machine aus. Alle Time Machine-Anwendungsdaten befinden sich in einem Verzeichnis mit dem Namen `Backups.backupdb`.

Zugehörige Konzepte:
Auszuschließende Systemdateien
Windows-Betriebssysteme

Teilsicherung, selektive Sicherung oder Teilsicherung nach Datum (Windows)

Der Administrator kann Zeitpläne definieren, durch die Dateien automatisch gesichert werden. In diesem Abschnitt wird die Sicherung von Dateien ohne Zeitpläne beschrieben.

Es gibt drei Arten der Teilsicherung: *vollständige Teilsicherung*, *partielle Teilsicherung* und *Teilsicherung nach Datum*.

Wenn Sie Dateien mit IBM Spectrum Protect HSM for Windows umlagern, kann dies Auswirkungen auf Sicherungsoperationen haben.

- Windows-BetriebssystemeVollständige und partielle Teilsicherung
  Bei einer Teilsicherung werden nur neue und geänderte Dateien gesichert. Der Typ der Teilsicherung ist von den Objekten abhängig, die Sie für die Sicherung auswählen.
- Windows-BetriebssystemeTeilsicherung nach Datum
  Um ein Dateisystem für Teilsicherungen nach Datum auswählen zu können, müssen Sie mindestens eine vollständige Teilsicherung dieses Dateisystems ausgeführt haben. Wird nur eine Teilsicherung für eine Verzeichnisverzweigung oder für eine einzelne Datei ausgeführt, kann das Dateisystem nicht für Teilsicherungen nach Datum ausgewählt werden.
- Windows-BetriebssystemeVergleich zwischen Teilsicherung nach Datum, journalbasierter Sicherung sowie NetApp-Momentaufnahmedifferenzsicherung und vollständiger Teilsicherung und partieller Teilsicherung
  Teilsicherung nach Datum, journalbasierte Sicherung und NetApp-Momentaufnahmedifferenzsicherung sind Alternativen zur vollständigen und partiellen Teilsicherung.
- Windows-BetriebssystemeMomentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung
  Sie können eine sichere HTTPS-Verbindung für die Kommunikation des Clients für Sichern/Archivieren mit einem NetApp-Dateiserver während einer Momentaufnahmedifferenzsicherung verwenden.
- Windows-BetriebssystemeSelektive Sicherung
  Verwenden Sie eine selektive Sicherung, wenn Sie bestimmte Dateien oder Verzeichnisse sichern möchten, unabhängig davon, ob eine aktuelle Kopie dieser Dateien auf dem Server vorhanden ist.

Zugehörige Konzepte:
Windows-Betriebssysteme Umgelagerte Dateien sichern und zurückschreiben
Zugehörige Tasks:
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren

Vollständige und partielle Teilsicherung

Bei einer Teilsicherung werden nur neue und geänderte Dateien gesichert. Der Typ der Teilsicherung ist von den Objekten abhängig, die Sie für die Sicherung auswählen.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWählen Sie vollständige Dateisysteme aus, führen Sie eine vollständige Teilsicherung aus. Wählen Sie eine Verzeichnisbaumstruktur oder einzelne Dateien aus, führen Sie eine partielle Teilsicherung durch.

Windows-BetriebssystemeWählen Sie vollständige Laufwerke aus, führen Sie eine vollständige Teilsicherung aus. Wählen Sie eine Verzeichnisbaumstruktur oder einzelne Dateien aus, führen Sie eine partielle Teilsicherung durch.

Bei der ersten Ausführung einer vollständigen Teilsicherung sichert der Client für Sichern/Archivieren alle angegebenen Dateien und Verzeichnisse. Die Sicherungsoperation kann sehr lange dauern, wenn die Anzahl der Dateien groß ist oder wenn eine oder mehrere große Dateien gesichert werden müssen. Bei nachfolgenden vollständigen Teilsicherungen werden nur neue und geänderte Dateien gesichert. Der

Sicherungsserver bewahrt aktuelle Versionen Ihrer Dateien auf, ohne Zeit oder Speicherplatz durch das Sichern von Dateien zu vergeuden, die im IBM Spectrum Protect-Serverspeicher vorhanden sind.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme Abhängig von Ihren Speicherverwaltungsmaßnahmen kann der IBM Spectrum Protect-Server mehrere Versionen Ihrer Dateien im Speicher aufbewahren. Die zuletzt gesicherten Dateien sind aktive Sicherungsversionen. Ältere Kopien Ihrer gesicherten Dateien sind inaktive Versionen. Löschen Sie jedoch eine Datei von Ihrer Workstation, wird die aktive Sicherungsversion der Datei bei der nächsten vollständigen Teilsicherung zu einer inaktiven Version. Sie können eine inaktive Version einer Datei zurückschreiben. Die Anzahl der inaktiven Versionen, die vom Server verwaltet werden, und die Dauer ihrer Aufbewahrung werden durch Verwaltungsmaßnahmen gesteuert, die Ihr IBM Spectrum Protect-Serveradministrator definiert. Die aktiven Versionen stellen die Dateien dar, die in Ihrem Dateisystem zum Zeitpunkt der letzten Sicherung vorhanden waren.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme Soll eine vollständige oder partielle Teilsicherung über die Client-GUI gestartet werden, wählen Sie Sichern und dann die Option Teilsicherung (vollständig) aus. In der Befehlszeile verwenden Sie den Befehl incremental und geben Sie Dateisysteme, Verzeichnisbaumstrukturen oder einzelne Dateien an, die bei der Sicherung berücksichtigt werden sollen.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme Während einer Teilsicherung fragt der Client den Server oder die Journaldatenbank ab, um den genauen Status Ihrer Dateien seit der letzten Teilsicherung zu bestimmen. Der Client verwendet diese Informationen für die folgenden Tasks:

- Neue Dateien sichern.
- Dateien sichern, deren Inhalt sich seit der letzten Sicherung geändert hat.
  Windows-BetriebssystemeDateien werden gesichert, wenn sich eins der folgenden Attribute ändert:
  - Dateigröße
  - Datum oder Uhrzeit der letzten Änderung
  - Erweiterte Attribute
  - Zugriffssteuerungsliste
  - Dateiattribute freie Bereiche, Analysepunkt oder Verschlüsselung
  - NTFS- oder ReFS-Dateisicherheitsdeskriptoren: Eignersicherheitskennung (SID), Gruppen-SID, eignerdefinierte Zugriffssteuerungsliste (Access Control List, ACL) und Systemzugriffssteuerungsliste.
  - Verzeichnisattribute

  Wenn sich nur die folgenden Attribute ändern, werden die Attribute auf dem IBM Spectrum Protect-Server aktualisiert, die Datei aber nicht gesichert:
  - Lesezugriff oder Schreib-/Lesezugriff
  - Verdeckt oder nicht verdeckt
  - Komprimiert oder nicht komprimiert

  Das Archivierungsattribut wird von IBM Spectrum Protect bei der Bestimmung der geänderten Dateien nicht berücksichtigt.
  Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDateien werden gesichert, wenn sich eins der folgenden Attribute ändert:
  - Dateigröße
  - Datum oder Uhrzeit der letzten Änderung
  - Erweiterte Attribute
  - Zugriffssteuerungsliste

  Wenn sich nur die folgenden Attribute ändern, werden die Attribute auf dem IBM Spectrum Protect-Server aktualisiert, die Datei aber nicht gesichert:
  - Dateieigner
  - Dateiberechtigungen
  - Dateiindex
  - Gruppen-ID
  - AIX-BetriebssystemeLinux-BetriebssystemeAttribut für die Änderungszeit (`ctime`) (nur für Objekte in GPFS-Dateisystemen und wenn die Option updatectime auf yes gesetzt ist). Weitere ausführliche Informationen finden Sie bei der Option updatectime.
  - Symbolposition (nur Mac OS X)
  - Typ oder Ersteller (nur Mac OS X)
- Verzeichnissicherung.
  Ein Verzeichnis wird in einer der folgenden Situationen gesichert:
  - Das Verzeichnis wurde noch nicht gesichert.
  - Die Verzeichnisberechtigungen haben sich seit der letzten Sicherung geändert.
  - Die Verzeichniszugriffssteuerungsliste hat sich seit der letzten Sicherung geändert.
  - Die erweiterten Attribute des Verzeichnisses haben sich seit der letzten Sicherung geändert.
  - AIX-BetriebssystemeLinux-BetriebssystemeDas Attribut für die Änderungszeit (`ctime`) wurde seit der letzten Sicherung aktualisiert (nur für GPFS-Dateisysteme). Weitere ausführliche Informationen finden Sie bei der Option updatectime.

  Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeVerzeichnisse werden bei der Anzahl der gesicherten Objekte mitgezählt. Sollen Verzeichnisse und ihr Inhalt von der Sicherung ausgeschlossen werden, verwenden Sie die Option exclude.dir.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeVerfallsverarbeitung für Sicherungsversionen von Dateien auf dem Server durchführen, für die keine entsprechenden Dateien auf der Workstation vorhanden sind. Das Ergebnis ist, dass für Dateien, die auf Ihrer Workstation nicht mehr

vorhanden sind, keine aktiven Sicherungsversionen mehr auf dem Server existieren. Inaktive Versionen werden jedoch gemäß den vom IBM Spectrum Protect-Administrator definierten Regeln aufbewahrt.

- Sicherungsversionen erneut binden, wenn sich die Zuordnung der Verwaltungsklassen ändert. Nur Objekte, die über aktive Sicherungsversionen verfügen, werden erneut gebunden. Objekte, für die nur inaktive Sicherungsversionen vorhanden sind, werden nicht erneut gebunden.
  Während einer partiellen Teilsicherung werden Objekte wie folgt erneut gebunden oder sie verfallen wie folgt:

  Wenn die Dateispezifikation allen Dateien in einem Pfad entspricht:
  Erneutes Binden und Verfallsverarbeitung finden für alle auswählbaren Sicherungsversionen statt, die der Dateispezifikation entsprechen. Dies ist der Fall für einen Teilsicherungsbefehl wie `dsmc incr c:\mydir\* -subdir=yes`.
  Wenn die Dateispezifikation nicht allen Dateien in einem Pfad entspricht:
  Erneutes Binden und Verfallsverarbeitung finden für alle auswählbaren Sicherungsversionen statt, die der Dateispezifikation entsprechen. Auswählbare Sicherungsversionen verfallen jedoch nicht bzw. werden nicht erneut gebunden, wenn sie sich in einem Verzeichnis befanden, das im Clientdateisystem nicht mehr vorhanden ist.

  Ziehen Sie einen Teilsicherungsbefehl wie `dsmc incr c:\mydir\*.txt -subdir=yes` in Betracht. Angenommen, einige Dateien in c:\mydir\ haben nicht den Dateityp txt. Erneutes Binden und Verfallsverarbeitung finden nur für Dateien statt, die der Spezifikation *.txt entsprechen und deren Verzeichnisse im Clientdateisystem noch vorhanden sind.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Sie können mit der Option preservelastaccessdate angeben, ob das Datum des letzten Zugriffs nach einer Sicherungs- oder Archivierungsoperation geändert werden soll. Standardmäßig ändert sich das Zugriffsdatum nach einer Sicherungs- oder Archivierungsoperation.

- Windows-BetriebssystemeJournalbasierte Sicherung
  Die journalbasierte Sicherung ist eine alternative Sicherungsmethode, die ein vom IBM Spectrum Protect-Journalserviceprozess verwaltetes Änderungsjournal verwendet.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
Zugehörige Verweise:
Ausschlussoptionen
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Preservelastaccessdate
AIX-BetriebssystemeLinux-BetriebssystemeUpdatectime

Teilsicherung nach Datum

Um ein Dateisystem für Teilsicherungen nach Datum auswählen zu können, müssen Sie mindestens eine vollständige Teilsicherung dieses Dateisystems ausgeführt haben. Wird nur eine Teilsicherung für eine Verzeichnisverzweigung oder für eine einzelne Datei ausgeführt, kann das Dateisystem nicht für Teilsicherungen nach Datum ausgewählt werden.

Windows-BetriebssystemeSoll eine Teilsicherung nach Datum über die grafische Benutzerschnittstelle ausgeführt werden, wählen Sie die Option Teilsicherung (nur Datum) im Pulldown-Menü *Sicherungsart* aus oder verwenden Sie die Option incrbydate im Befehl incremental.

Der Client sichert nur die Dateien, deren Änderungsdatum und -zeit nach dem Datum und der Zeit der letzten Teilsicherung des Dateisystems liegen, in dem sich die Dateien befinden. Dateien, die von dem Client nach der letzten Teilsicherung hinzugefügt wurden, aber deren Änderungsdatum vor der letzten Teilsicherung liegt, werden nicht gesichert.

Dateien, die nach der letzten Teilsicherung umbenannt wurden, aber ansonsten nicht geändert wurden, werden nicht gesichert. Durch das Umbenennen einer Datei werden das Änderungsdatum und die Änderungszeit der Datei nicht geändert. Durch das Umbenennen einer Datei wird jedoch das Änderungsdatum des Verzeichnisses, in dem sich die Datei befindet, geändert. In diesem Fall wird das Verzeichnis gesichert, nicht aber die Dateien, die es enthält.

Wird eine Teilsicherung nach Datum für das gesamte Dateisystem ausgeführt, aktualisiert der Server das Datum und die Uhrzeit der letzten Teilsicherung. Wird eine Teilsicherung nach Datum nur für einen Teil eines Dateisystems ausgeführt, aktualisiert der Server nicht das Datum der letzten vollständigen Teilsicherung. In diesem Fall werden diese Dateien bei der nächsten Teilsicherung nach Datum erneut gesichert.

Anmerkung: Anders als bei Teilsicherungen werden bei Teilsicherungen nach Datum gelöschte Dateien nicht als verfallen gekennzeichnet und Sicherungsversionen nicht an eine neue Verwaltungsklasse gebunden, wenn Sie die Verwaltungsklasse ändern.
Zugehörige Tasks:
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDaten über die Java-GUI sichern
Windows-BetriebssystemeAIX-BetriebssystemeLinux-Betriebssysteme

Vergleich zwischen Teilsicherung nach Datum, journalbasierter Sicherung sowie NetApp-Momentaufnahmedifferenzsicherung und vollständiger Teilsicherung und partieller Teilsicherung

Teilsicherung nach Datum, journalbasierte Sicherung und NetApp-Momentaufnahmedifferenzsicherung sind Alternativen zur vollständigen und partiellen Teilsicherung.

Teilsicherung nach Datum

Für eine Teilsicherung nach Datum wird weniger Verarbeitungszeit als für eine vollständige Teilsicherung und weniger Speicher benötigt.

Bei einer Teilsicherung nach Datum werden möglicherweise nicht dieselben Sicherungsdateien in den Serverspeicher gestellt, da bei der Teilsicherung nach Datum:

-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-BetriebssystemeKeine Sicherungsversionen von Dateien als verfallen gekennzeichnet werden, die Sie von der Workstation löschen.
- Keine Sicherungsversionen an eine neue Verwaltungsklasse gebunden werden, wenn Sie die Verwaltungsklasse ändern.
- Keine Dateien mit Attributen gesichert werden, die sich ändern, es sei denn, das Änderungsdatum und die Änderungszeit ändern sich ebenfalls.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-BetriebssystemeDas Kopiengruppenattribut für die Häufigkeit in Verwaltungsklassen ignoriert wird (bei journalbasierten Sicherungen wird dieses Attribut ebenfalls ignoriert).

Journalbasierte Sicherung

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeDer Speicherbedarf für eine anfängliche Journalfunktionsumgebung ist derselbe wie der für eine vollständige Dateibereichsteilsicherung, da journalbasierte Sicherungen eine vollständige Dateibereichsteilsicherung ausführen müssen, damit die Journaldatenbank als gültig definiert und die Basis für die Journalführung erstellt wird.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-BetriebssystemeDer Speicherbedarf für nachfolgende journalbasierte Sicherungen ist weitaus geringer. Journalsicherungssitzungen verlaufen parallel und werden durch die Clientoption resourceutilization auf dieselbe Weise geregelt wie normale Sicherungssitzungen. Die Größe der Journaldatenbankdatei wird auf eine minimale Größe (kleiner als 1 KB) zurückgesetzt, wenn der letzte Eintrag aus dem Journal gelöscht worden ist. Da Einträge aus dem Journal gelöscht werden, sobald sie vom Client verarbeitet wurden, sollte die vom Journal belegte Plattengröße nach einer vollständigen Journalsicherung minimal sein. Eine vollständige Teilsicherung mit aktiver Journalfunktion beansprucht weniger Verarbeitungszeit als eine Teilsicherung nach Datum.

 AIX-Betriebssysteme  Linux-BetriebssystemeBei der journalbasierten Sicherung gelten unter AIX und Linux einige Einschränkungen. Weitere Informationen finden Sie in Journalbasierte Sicherung unter AIX und Linux.

NetApp-Momentaufnahmedifferenz

 Linux-Betriebssysteme  Windows-BetriebssystemeBei NAS- und N-Series-Dateiservern, auf denen ONTAP 7.3.0 oder höher aktiv ist, können Sie die Option snapdiff zum Aufrufen der NetApp-Momentaufnahmedifferenzsicherung verwenden, wenn eine Teilsicherung des gesamten Datenträgers ausgeführt wird. Durch Verwendung dieser Option wird die Speicherbelegung reduziert und die Verarbeitung beschleunigt.

 Linux-Betriebssysteme  Windows-BetriebssystemeBeachten Sie die folgenden Einschränkungen bei der Ausführung einer Teilsicherung des gesamten Datenträgers über die Option snapdiff, um sicherzustellen, dass die Daten gesichert werden, wenn es erforderlich ist.

- Eine Datei ist aufgrund einer Ausschlussregel in der Einschluss-/Ausschlussdatei ausgeschlossen. Der Client führt eine Sicherung der aktuellen Momentaufnahme aus, während diese Ausschlussregel aktiv ist. Folgendes geschieht, wenn Sie keine Änderungen an der Datei vorgenommen, jedoch die Regel für den Ausschluss dieser Datei entfernt haben. NetApp erkennt diese Änderung an den Einschluss/Ausschlussregeln nicht, da nur Änderungen an Dateien durch den Vergleich von zwei Momentaufnahmen festgestellt werden.
- Wenn Sie der Optionsdatei eine Include-Anweisung hinzugefügt haben, tritt diese Einschlussoption erst in Kraft, wenn NetApp feststellt, dass die Datei sich geändert hat. Der Client überprüft während einer Sicherung nicht jede Datei auf dem Datenträger.
- Wenn Sie mit dem Befehl dsmc delete backup explizit eine Datei aus dem IBM Spectrum Protect-Bestand gelöscht haben, erkennt NetApp nicht, dass eine Datei manuell aus dem IBM Spectrum Protect-Speicher gelöscht wurde. Daher verbleibt die Datei ungeschützt im IBM Spectrum Protect-Speicher, bis sie auf dem Datenträger geändert wird und die Änderung von NetApp erkannt wird, wodurch der Client angewiesen wird, die Datei erneut zu sichern.
- Maßnahmenänderungen wie die Änderung der Maßnahme von mode=modified in mode=absolute werden nicht festgestellt.
- Der gesamte Dateibereich wird aus dem IBM Spectrum Protect-Datenbestand gelöscht. Diese Aktion bewirkt, dass die Option snapdiff eine neue Momentaufnahme erstellt, die als Quelle verwendet wird, und eine vollständige Teilsicherung ausgeführt wird.

Die NetApp-Software bestimmt, was ein geändertes Objekt ist, nicht IBM Spectrum Protect.

 Linux-BetriebssystemeWenn Sie eine Datenträgergesamtsicherung eines über NFS-Mount angehängten NetApp- oder N-Series-Datenträgers ausführen, werden möglicherweise auch alle Momentaufnahmen im Momentaufnahmeverzeichnis gesichert.

Führen Sie einen der folgenden Schritte aus, um zu vermeiden, dass alle Momentaufnahmen im Momentaufnahmeverzeichnis gesichert werden:

- NDMP-Sicherungen ausführen
- Sicherungen mithilfe der Option snapshotroot ausführen

- Teilsicherungen mithilfe der Option snapdiff ausführen
  Tipp: Wenn Sie eine Teilsicherung mit der Option snapdiff ausführen und regelmäßige Teilsicherungen planen, verwenden Sie die Option createnewbase=yes mit der Option snapdiff, um eine Basismomentaufnahme zu erstellen und als Quelle für eine Teilsicherung zu verwenden.
- Das Momentaufnahmeverzeichnis bei Sicherungen ausschließen
   Linux-BetriebssystemeAuf Linux-Systemen befindet sich das Momentaufnahmeverzeichnis in .snapshot.
  Anmerkung: Das Verzeichnis .snapshot wird bei einigen Versionen von Red Hat Linux nicht gesichert. Sie müssen es daher nicht ausschließen.

   Windows-BetriebssystemeAuf Windows-Systemen befindet sich das Momentaufnahmeverzeichnis in ~snapshot.

Windows-Betriebssysteme

Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung

Sie können eine sichere HTTPS-Verbindung für die Kommunikation des Clients für Sichern/Archivieren mit einem NetApp-Dateiserver während einer Momentaufnahmedifferenzsicherung verwenden.

Das HTTPS-Protokoll ist auf NetApp-Dateiservern standardmäßig aktiviert und kann nicht inaktiviert werden.

Wenn Sie eine Momentaufnahmedifferenzsicherung ausführen, baut der Client für Sichern/Archivieren eine Verwaltungssitzung mit einem NetApp-Dateiserver auf. Die Berechtigungsnachweise des Dateiservers (z. B. der Hostname oder die IP-Adresse des Dateiservers, der Benutzername, mit dem eine Verbindung zum Dateiserver hergestellt wird, und das Kennwort des Dateiservers) werden lokal auf dem Client für Sichern/Archivieren gespeichert. Diese Informationen müssen an den Dateiserver übertragen werden, um die authentifizierte Verwaltungssitzung aufbauen zu können. Es ist wichtig, eine sichere Verbindung zu verwenden, weil der Client für die Authentifizierung der Verwaltungssitzung des Dateiservers das Kennwort des Dateiservers in Klartext übertragen muss.

Sie müssen die Option snapdiffhttps bei jeder Ausführung einer Momentaufnahmedifferenzsicherung angeben, um eine sichere Verbindung mithilfe des HTTPS-Übertragungsprotokolls herzustellen. Ohne die Option snapdiffhttps kann der Client für Sichern/Archivieren Dateiserversitzungen nur mit dem HTTP-Protokoll aufbauen, was eine Aktivierung des HTTP-Verwaltungszugriffs auf dem Dateiserver erforderlich machen würde. Mit der Option snapdiffhttps können Sie eine sichere Verwaltungssitzung mit dem NetApp-Dateiserver aufbauen, ohne dass hierfür der HTTP-Verwaltungszugriff auf dem NetApp-Dateiserver aktiviert sein muss.

Einschränkungen:

Für Momentaufnahmedifferenzsicherungen mit HTTPS gelten die folgenden Einschränkungen:

- Die HTTPS-Verbindung wird nur für die sichere Übertragung von Daten über die Verwaltungssitzung zwischen dem Client für Sichern/Archivieren und dem NetApp-Dateiserver verwendet. Zu den Daten der Verwaltungssitzung gehören z. B. Berechtigungsnachweise des Dateiservers, Momentaufnahmeinformationen sowie Dateinamen und Attribute, die durch den Momentaufnahmedifferenzierungsprozess generiert werden. Über die HTTPS-Verbindung werden keine normalen Dateidaten übertragen, auf die der Client über die Dateifreigabe auf dem Dateiserver zugreift. Die HTTPS-Verbindung ist auch nicht für normale Dateidaten gültig, die der Client über das normale IBM Spectrum Protect-Client/Server-Protokoll an den IBM Spectrum Protect-Server überträgt.
- Die Option snapdiffhttps gilt nicht für vFilers, da das HTTPS-Protokoll auf dem NetApp vFiler nicht unterstützt wird.
- Die Option snapdiffhttps ist nur bei Verwendung der Befehlszeilenschnittstelle verfügbar. In der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren kann sie nicht verwendet werden.

-  Windows-BetriebssystemeMomentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung ausführen
  Wenn Sie eine Momentaufnahmedifferenzsicherung ausführen, können Sie mit der Option snapdiffhttps eine sichere HTTPS-Verbindung zwischen dem Client für Sichern/Archivieren und dem NetApp-Dateiserver erstellen.

Zugehörige Konzepte:
 Windows-BetriebssystemeVergleich zwischen Teilsicherung nach Datum, journalbasierter Sicherung sowie NetApp-Momentaufnahmedifferenzsicherung und vollständiger Teilsicherung und partieller Teilsicherung
Zugehörige Tasks:
NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren
 Windows-BetriebssystemeMomentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung ausführen
Linux-BetriebssystemeMomentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung ausführen
Zugehörige Verweise:
Snapdiffhttps
Snapdiff

Selektive Sicherung

Verwenden Sie eine selektive Sicherung, wenn Sie bestimmte Dateien oder Verzeichnisse sichern möchten, unabhängig davon, ob eine aktuelle Kopie dieser Dateien auf dem Server vorhanden ist.

Teilsicherungen sind im Allgemeinen Teil eines automatisierten Systems zum Sichern vollständiger Dateisysteme. Dagegen können Sie mit selektiven Sicherungen eine Gruppe zu sichernder Dateien manuell auswählen, unabhängig davon, ob sich die Dateien seit der letzten Teilsicherung geändert haben.

Im Gegensatz zu Teilsicherungen bietet eine selektive Sicherung folgende Merkmale:

- Sie bewirkt keine Aktualisierung des Datums und der Uhrzeit der letzten Teilsicherung durch den Server.
- Verzeichnis- und Dateieinträge werden auch dann gesichert, wenn sich ihre Größe, ihre Änderungszeitmarken oder ihre Berechtigungen nicht geändert haben.
- Gelöschte Dateien verfallen nicht.
- Keine Sicherungsversionen an eine neue Verwaltungsklasse gebunden werden, wenn Sie die Verwaltungsklasse ändern.

Zugehörige Tasks:
Windows-BetriebssystemeDaten über die GUI sichern
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDaten über die Java-GUI sichern
Zugehörige Verweise:
Selective
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Teilsicherung, selektive Sicherung oder Teilsicherung nach Datum ausführen (UNIX und Linux)

Der Administrator kann Zeitpläne definieren, durch die Dateien auf Ihrer Workstation automatisch gesichert werden. In den folgenden Abschnitten wird die Sicherung von Dateien ohne Zeitpläne beschrieben.

Es gibt zwei Arten der Teilsicherung: *vollständige Teilsicherung* und *partielle Teilsicherung*.

- AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeVollständige und partielle Teilsicherung
  Bei einer Teilsicherung werden nur neue und geänderte Dateien gesichert. Der Typ der Teilsicherung ist von den Objekten abhängig, die Sie für die Sicherung auswählen.
- AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeTeilsicherung nach Datum
  Um ein Dateisystem für Teilsicherungen nach Datum auswählen zu können, müssen Sie mindestens eine vollständige Teilsicherung dieses Dateisystems ausgeführt haben. Wird nur eine Teilsicherung für eine Verzeichnisverzweigung oder für eine einzelne Datei ausgeführt, kann das Dateisystem nicht für Teilsicherungen nach Datum ausgewählt werden.
- AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeVergleich zwischen Teilsicherung nach Datum, journalbasierter Sicherung sowie NetApp-Momentaufnahmedifferenzsicherung und vollständiger Teilsicherung und partieller Teilsicherung
  Teilsicherung nach Datum, journalbasierte Sicherung und NetApp-Momentaufnahmedifferenzsicherung sind Alternativen zur vollständigen und partiellen Teilsicherung.
- AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung
  Sie können eine sichere HTTPS-Verbindung für die Kommunikation des Clients für Sichern/Archivieren mit einem NetApp-Dateiserver während einer Momentaufnahmedifferenzsicherung verwenden.
- AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeSelektive Sicherung
  Verwenden Sie eine selektive Sicherung, wenn Sie bestimmte Dateien oder Verzeichnisse sichern möchten, unabhängig davon, ob eine aktuelle Kopie dieser Dateien auf dem Server vorhanden ist.
- Oracle Solaris-BetriebssystemeSicherungen der globalen Zone und der nicht globalen Zonen in Solaris
  Bei Solaris Zones führen Sie Teilsicherungen und selektive Sicherungen von Dateisystemen innerhalb der Zone aus, in der diese Dateisysteme erstellt wurden.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeZugriffsberechtigungen sichern
  Während Sie Ihre Dateien sichern, sichert der Client für Sichern/Archivieren auch UNIX-Standardzugriffsberechtigungen, die den Dateien zugeordnet sind.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeVirtuellen Mountpunkt definieren
  Wenn Sie ein berechtigter Benutzer sind und Dateien ab einem bestimmten Verzeichnis innerhalb eines Dateisystems sichern wollen, können Sie dieses Verzeichnis als virtuellen Mountpunkt definieren.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDaten über die Java-GUI sichern
  Aus der Verzeichnisbaumstruktur können bestimmte Dateien, vollständige Verzeichnisse oder vollständige Dateisysteme gesichert werden.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDaten über die Befehlszeile sichern
  Sie können den Befehl incremental oder selective verwenden, um Sicherungen auszuführen.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeSicherungsdaten löschen
  Wenn Sie vom Administrator entsprechend berechtigt wurden, können Sie einzelne Sicherungskopien aus dem IBM Spectrum Protect-Server löschen, ohne den gesamten Dateibereich zu löschen. Um festzustellen, ob Sie über diese Berechtigung verfügen, wählen Sie Datei

> Verbindungsinformationen in der GUI des Clients für Sichern/Archivieren oder im Hauptmenü des Web-Clients aus. Ihr Berechtigungsstatus wird im Feld Sicherungsdateien löschen zur Verfügung gestellt.

-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDateibereiche löschen
  Erteilt der IBM Spectrum Protect-Administrator einem Benutzer die Berechtigung, kann der Benutzer vollständige Dateibereiche aus dem Server löschen. Beim Löschen eines Dateibereichs werden alle Dateien und Images, sowohl Sicherungsversionen als auch Archivierungskopien, innerhalb dieses Dateibereichs gelöscht. Wird beispielsweise der Dateibereich `/tmp` gelöscht, werden alle Sicherungsversionen für alle Dateien in diesem Dateisystem und alle aus diesem Dateisystem archivierten Dateien gelöscht. Das Löschen eines Dateibereichs muss gründlich überlegt werden.

Zugehörige Tasks:
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren

Vollständige und partielle Teilsicherung

Bei einer Teilsicherung werden nur neue und geänderte Dateien gesichert. Der Typ der Teilsicherung ist von den Objekten abhängig, die Sie für die Sicherung auswählen.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeWählen Sie vollständige Dateisysteme aus, führen Sie eine vollständige Teilsicherung aus. Wählen Sie eine Verzeichnisbaumstruktur oder einzelne Dateien aus, führen Sie eine partielle Teilsicherung durch.

 Windows-BetriebssystemeWählen Sie vollständige Laufwerke aus, führen Sie eine vollständige Teilsicherung aus. Wählen Sie eine Verzeichnisbaumstruktur oder einzelne Dateien aus, führen Sie eine partielle Teilsicherung durch.

Bei der ersten Ausführung einer vollständigen Teilsicherung sichert der Client für Sichern/Archivieren alle angegebenen Dateien und Verzeichnisse. Die Sicherungsoperation kann sehr lange dauern, wenn die Anzahl der Dateien groß ist oder wenn eine oder mehrere große Dateien gesichert werden müssen. Bei nachfolgenden vollständigen Teilsicherungen werden nur neue und geänderte Dateien gesichert. Der Sicherungsserver bewahrt aktuelle Versionen Ihrer Dateien auf, ohne Zeit oder Speicherplatz durch das Sichern von Dateien zu vergeuden, die im IBM Spectrum Protect-Serverspeicher vorhanden sind.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme
Abhängig von Ihren Speicherverwaltungsmaßnahmen kann der IBM Spectrum Protect-Server mehrere Versionen Ihrer Dateien im Speicher aufbewahren. Die zuletzt gesicherten Dateien sind aktive Sicherungsversionen. Ältere Kopien Ihrer gesicherten Dateien sind inaktive Versionen. Löschen Sie jedoch eine Datei von Ihrer Workstation, wird die aktive Sicherungsversion der Datei bei der nächsten vollständigen Teilsicherung zu einer inaktiven Version. Sie können eine inaktive Version einer Datei zurückschreiben. Die Anzahl der inaktiven Versionen, die vom Server verwaltet werden, und die Dauer ihrer Aufbewahrung werden durch Verwaltungsmaßnahmen gesteuert, die Ihr IBM Spectrum Protect-Serveradministrator definiert. Die aktiven Versionen stellen die Dateien dar, die in Ihrem Dateisystem zum Zeitpunkt der letzten Sicherung vorhanden waren.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme
Soll eine vollständige oder partielle Teilsicherung über die Client-GUI gestartet werden, wählen Sie Sichern und dann die Option Teilsicherung (vollständig) aus. In der Befehlszeile verwenden Sie den Befehl incremental und geben Sie Dateisysteme, Verzeichnisbaumstrukturen oder einzelne Dateien an, die bei der Sicherung berücksichtigt werden sollen.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme
Während einer Teilsicherung fragt der Client den Server oder die Journaldatenbank ab, um den genauen Status Ihrer Dateien seit der letzten Teilsicherung zu bestimmen. Der Client verwendet diese Informationen für die folgenden Tasks:

- Neue Dateien sichern.
- Dateien sichern, deren Inhalt sich seit der letzten Sicherung geändert hat.
  Windows-BetriebssystemeDateien werden gesichert, wenn sich eins der folgenden Attribute ändert:
  - Dateigröße
  - Datum oder Uhrzeit der letzten Änderung
  - Erweiterte Attribute
  - Zugriffssteuerungsliste
  - Dateiattribute freie Bereiche, Analysepunkt oder Verschlüsselung
  - NTFS- oder ReFS-Dateisicherheitsdeskriptoren: Eignersicherheitskennung (SID), Gruppen-SID, eignerdefinierte Zugriffssteuerungsliste (Access Control List, ACL) und Systemzugriffssteuerungsliste.
  - Verzeichnisattribute

  Wenn sich nur die folgenden Attribute ändern, werden die Attribute auf dem IBM Spectrum Protect-Server aktualisiert, die Datei aber nicht gesichert:
  - Lesezugriff oder Schreib-/Lesezugriff
  - Verdeckt oder nicht verdeckt
  - Komprimiert oder nicht komprimiert

  Das Archivierungsattribut wird von IBM Spectrum Protect bei der Bestimmung der geänderten Dateien nicht berücksichtigt.
   Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDateien werden gesichert, wenn sich eins der folgenden Attribute ändert:
  - Dateigröße
  - Datum oder Uhrzeit der letzten Änderung
  - Erweiterte Attribute

- Zugriffssteuerungsliste

Wenn sich nur die folgenden Attribute ändern, werden die Attribute auf dem IBM Spectrum Protect-Server aktualisiert, die Datei aber nicht gesichert:

- Dateieigner
- Dateiberechtigungen
- Dateiindex
- Gruppen-ID
- AIX-BetriebssystemeLinux-BetriebssystemeAttribut für die Änderungszeit (`ctime`) (nur für Objekte in GPFS-Dateisystemen und wenn die Option updatectime auf yes gesetzt ist). Weitere ausführliche Informationen finden Sie bei der Option updatectime.
- Symbolposition (nur Mac OS X)
- Typ oder Ersteller (nur Mac OS X)

- Verzeichnissicherung.
  Ein Verzeichnis wird in einer der folgenden Situationen gesichert:
  - Das Verzeichnis wurde noch nicht gesichert.
  - Die Verzeichnisberechtigungen haben sich seit der letzten Sicherung geändert.
  - Die Verzeichniszugriffssteuerungsliste hat sich seit der letzten Sicherung geändert.
  - Die erweiterten Attribute des Verzeichnisses haben sich seit der letzten Sicherung geändert.
  - AIX-BetriebssystemeLinux-BetriebssystemeDas Attribut für die Änderungszeit (`ctime`) wurde seit der letzten Sicherung aktualisiert (nur für GPFS-Dateisysteme). Weitere ausführliche Informationen finden Sie bei der Option updatectime.

  Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme
  Windows-BetriebssystemeVerzeichnisse werden bei der Anzahl der gesicherten Objekte mitgezählt. Sollen Verzeichnisse und ihr Inhalt von der Sicherung ausgeschlossen werden, verwenden Sie die Option exclude.dir.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme
  Windows-BetriebssystemeVerfallsverarbeitung für Sicherungsversionen von Dateien auf dem Server durchführen, für die keine entsprechenden Dateien auf der Workstation vorhanden sind. Das Ergebnis ist, dass für Dateien, die auf Ihrer Workstation nicht mehr vorhanden sind, keine aktiven Sicherungsversionen mehr auf dem Server existieren. Inaktive Versionen werden jedoch gemäß den vom IBM Spectrum Protect-Administrator definierten Regeln aufbewahrt.
- Sicherungsversionen erneut binden, wenn sich die Zuordnung der Verwaltungsklassen ändert. Nur Objekte, die über aktive Sicherungsversionen verfügen, werden erneut gebunden. Objekte, für die nur inaktive Sicherungsversionen vorhanden sind, werden nicht erneut gebunden.
  Während einer partiellen Teilsicherung werden Objekte wie folgt erneut gebunden oder sie verfallen wie folgt:

  Wenn die Dateispezifikation allen Dateien in einem Pfad entspricht:
  Erneutes Binden und Verfallsverarbeitung finden für alle auswählbaren Sicherungsversionen statt, die der Dateispezifikation entsprechen. Dies ist der Fall für einen Teilsicherungsbefehl wie `dsmc incr c:\mydir\* -subdir=yes`.
  Wenn die Dateispezifikation nicht allen Dateien in einem Pfad entspricht:
  Erneutes Binden und Verfallsverarbeitung finden für alle auswählbaren Sicherungsversionen statt, die der Dateispezifikation entsprechen. Auswählbare Sicherungsversionen verfallen jedoch nicht bzw. werden nicht erneut gebunden, wenn sie sich in einem Verzeichnis befanden, das im Clientdateisystem nicht mehr vorhanden ist.

  Ziehen Sie einen Teilsicherungsbefehl wie `dsmc incr c:\mydir\*.txt -subdir=yes` in Betracht. Angenommen, einige Dateien in c:\mydir\ haben nicht den Dateityp txt. Erneutes Binden und Verfallsverarbeitung finden nur für Dateien statt, die der Spezifikation *.txt entsprechen und deren Verzeichnisse im Clientdateisystem noch vorhanden sind.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Sie können mit der Option preservelastaccessdate angeben, ob das Datum des letzten Zugriffs nach einer Sicherungs- oder Archivierungsoperation geändert werden soll. Standardmäßig ändert sich das Zugriffsdatum nach einer Sicherungs- oder Archivierungsoperation.

- AIX-BetriebssystemeJournalbasierte Sicherung unter AIX und Linux
  Die journalbasierte Sicherung ist eine alternative Sicherungsmethode, die ein vom IBM Spectrum Protect-Journaldämonprozess verwaltetes Änderungsjournal verwendet.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
Zugehörige Verweise:
Ausschlussoptionen
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Preservelastaccessdate
AIX-BetriebssystemeLinux-BetriebssystemeUpdatectime

Teilsicherung nach Datum

Um ein Dateisystem für Teilsicherungen nach Datum auswählen zu können, müssen Sie mindestens eine vollständige Teilsicherung dieses Dateisystems ausgeführt haben. Wird nur eine Teilsicherung für eine Verzeichnisverzweigung oder für eine einzelne Datei ausgeführt, kann das Dateisystem nicht für Teilsicherungen nach Datum ausgewählt werden.

Windows-BetriebssystemeSoll eine Teilsicherung nach Datum über die grafische Benutzerschnittstelle ausgeführt werden, wählen Sie die Option Teilsicherung (nur Datum) im Pulldown-Menü *Sicherungsart* aus oder verwenden Sie die Option incrbydate im Befehl incremental.

Der Client sichert nur die Dateien, deren Änderungsdatum und -zeit nach dem Datum und der Zeit der letzten Teilsicherung des Dateisystems liegen, in dem sich die Dateien befinden. Dateien, die von dem Client nach der letzten Teilsicherung hinzugefügt wurden, aber deren Änderungsdatum vor der letzten Teilsicherung liegt, werden nicht gesichert.

Dateien, die nach der letzten Teilsicherung umbenannt wurden, aber ansonsten nicht geändert wurden, werden nicht gesichert. Durch das Umbenennen einer Datei werden das Änderungsdatum und die Änderungszeit der Datei nicht geändert. Durch das Umbenennen einer Datei wird jedoch das Änderungsdatum des Verzeichnisses, in dem sich die Datei befindet, geändert. In diesem Fall wird das Verzeichnis gesichert, nicht aber die Dateien, die es enthält.

Wird eine Teilsicherung nach Datum für das gesamte Dateisystem ausgeführt, aktualisiert der Server das Datum und die Uhrzeit der letzten Teilsicherung. Wird eine Teilsicherung nach Datum nur für einen Teil eines Dateisystems ausgeführt, aktualisiert der Server nicht das Datum der letzten vollständigen Teilsicherung. In diesem Fall werden diese Dateien bei der nächsten Teilsicherung nach Datum erneut gesichert.

Anmerkung: Anders als bei Teilsicherungen werden bei Teilsicherungen nach Datum gelöschte Dateien nicht als verfallen gekennzeichnet und Sicherungsversionen nicht an eine neue Verwaltungsklasse gebunden, wenn Sie die Verwaltungsklasse ändern.
Zugehörige Tasks:
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDaten über die Java-GUI sichern
Windows-BetriebssystemeAIX-BetriebssystemeLinux-Betriebssysteme

Vergleich zwischen Teilsicherung nach Datum, journalbasierter Sicherung sowie NetApp-Momentaufnahmedifferenzsicherung und vollständiger Teilsicherung und partieller Teilsicherung

Teilsicherung nach Datum, journalbasierte Sicherung und NetApp-Momentaufnahmedifferenzsicherung sind Alternativen zur vollständigen und partiellen Teilsicherung.

Teilsicherung nach Datum
Für eine Teilsicherung nach Datum wird weniger Verarbeitungszeit als für eine vollständige Teilsicherung und weniger Speicher benötigt.

Bei einer Teilsicherung nach Datum werden möglicherweise nicht dieselben Sicherungsdateien in den Serverspeicher gestellt, da bei der Teilsicherung nach Datum:

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeKeine Sicherungsversionen von Dateien als verfallen gekennzeichnet werden, die Sie von der Workstation löschen.
- Keine Sicherungsversionen an eine neue Verwaltungsklasse gebunden werden, wenn Sie die Verwaltungsklasse ändern.
- Keine Dateien mit Attributen gesichert werden, die sich ändern, es sei denn, das Änderungsdatum und die Änderungszeit ändern sich ebenfalls.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeDas Kopiengruppenattribut für die Häufigkeit in Verwaltungsklassen ignoriert wird (bei journalbasierten Sicherungen wird dieses Attribut ebenfalls ignoriert).

Journalbasierte Sicherung

AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeDer Speicherbedarf für eine anfängliche Journalfunktionsumgebung ist derselbe wie der für eine vollständige Dateibereichsteilsicherung, da journalbasierte Sicherungen eine vollständige Dateibereichsteilsicherung ausführen müssen, damit die Journaldatenbank als gültig definiert und die Basis für die Journalführung erstellt wird.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeDer Speicherbedarf für nachfolgende journalbasierte Sicherungen ist weitaus geringer. Journalsicherungssitzungen verlaufen parallel und werden durch die Clientoption resourceutilization auf dieselbe Weise geregelt wie normale Sicherungssitzungen. Die Größe der Journaldatenbankdatei wird auf eine minimale Größe (kleiner als 1 KB) zurückgesetzt, wenn der letzte Eintrag aus dem Journal gelöscht worden ist. Da Einträge aus dem Journal gelöscht werden, sobald sie vom Client verarbeitet wurden, sollte die vom Journal belegte Plattengröße nach einer vollständigen Journalsicherung minimal sein. Eine vollständige Teilsicherung mit aktiver Journalfunktion beansprucht weniger Verarbeitungszeit als eine Teilsicherung nach Datum.

AIX-BetriebssystemeLinux-BetriebssystemeBei der journalbasierten Sicherung gelten unter AIX und Linux einige Einschränkungen. Weitere Informationen finden Sie in Journalbasierte Sicherung unter AIX und Linux.

NetApp-Momentaufnahmedifferenz

Linux-BetriebssystemeWindows-BetriebssystemeBei NAS- und N-Series-Dateiservern, auf denen ONTAP 7.3.0 oder höher aktiv ist, können Sie die Option snapdiff zum Aufrufen der NetApp-Momentaufnahmedifferenzsicherung verwenden, wenn eine Teilsicherung des gesamten Datenträgers ausgeführt wird. Durch Verwendung dieser Option wird die Speicherbelegung reduziert und die Verarbeitung beschleunigt.

Linux-BetriebssystemeWindows-BetriebssystemeBeachten Sie die folgenden Einschränkungen bei der Ausführung einer Teilsicherung des gesamten Datenträgers über die Option snapdiff, um sicherzustellen, dass die Daten gesichert werden, wenn es erforderlich ist.

- Eine Datei ist aufgrund einer Ausschlussregel in der Einschluss-/Ausschlussdatei ausgeschlossen. Der Client führt eine Sicherung der aktuellen Momentaufnahme aus, während diese Ausschlussregel aktiv ist. Folgendes geschieht, wenn Sie keine Änderungen an der Datei vorgenommen, jedoch die Regel für den Ausschluss dieser Datei entfernt haben. NetApp erkennt diese Änderung an den Einschluss/Ausschlussregeln nicht, da nur Änderungen an Dateien durch den Vergleich von zwei Momentaufnahmen festgestellt werden.
- Wenn Sie der Optionsdatei eine Include-Anweisung hinzugefügt haben, tritt diese Einschlussoption erst in Kraft, wenn NetApp feststellt, dass die Datei sich geändert hat. Der Client überprüft während einer Sicherung nicht jede Datei auf dem Datenträger.
- Wenn Sie mit dem Befehl dsmc delete backup explizit eine Datei aus dem IBM Spectrum Protect-Bestand gelöscht haben, erkennt NetApp nicht, dass eine Datei manuell aus dem IBM Spectrum Protect-Speicher gelöscht wurde. Daher verbleibt die Datei ungeschützt im IBM Spectrum Protect-Speicher, bis sie auf dem Datenträger geändert wird und die Änderung von NetApp erkannt wird, wodurch der Client angewiesen wird, die Datei erneut zu sichern.
- Maßnahmenänderungen wie die Änderung der Maßnahme von mode=modified in mode=absolute werden nicht festgestellt.
- Der gesamte Dateibereich wird aus dem IBM Spectrum Protect-Datenbestand gelöscht. Diese Aktion bewirkt, dass die Option snapdiff eine neue Momentaufnahme erstellt, die als Quelle verwendet wird, und eine vollständige Teilsicherung ausgeführt wird.

Die NetApp-Software bestimmt, was ein geändertes Objekt ist, nicht IBM Spectrum Protect.

Linux-BetriebssystemeWenn Sie eine Datenträgergesamtsicherung eines über NFS-Mount angehängten NetApp- oder N-Series-Datenträgers ausführen, werden möglicherweise auch alle Momentaufnahmen im Momentaufnahmeverzeichnis gesichert.

Führen Sie einen der folgenden Schritte aus, um zu vermeiden, dass alle Momentaufnahmen im Momentaufnahmeverzeichnis gesichert werden:

- NDMP-Sicherungen ausführen
- Sicherungen mithilfe der Option snapshotroot ausführen
- Teilsicherungen mithilfe der Option snapdiff ausführen
  Tipp: Wenn Sie eine Teilsicherung mit der Option snapdiff ausführen und regelmäßige Teilsicherungen planen, verwenden Sie die Option createnewbase=yes mit der Option snapdiff, um eine Basismomentaufnahme zu erstellen und als Quelle für eine Teilsicherung zu verwenden.
- Das Momentaufnahmeverzeichnis bei Sicherungen ausschließen
  Linux-BetriebssystemeAuf Linux-Systemen befindet sich das Momentaufnahmeverzeichnis in .snapshot.
  Anmerkung: Das Verzeichnis .snapshot wird bei einigen Versionen von Red Hat Linux nicht gesichert. Sie müssen es daher nicht ausschließen.

  Windows-BetriebssystemeAuf Windows-Systemen befindet sich das Momentaufnahmeverzeichnis in ~snapshot.

Linux-Betriebssysteme

Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung

Sie können eine sichere HTTPS-Verbindung für die Kommunikation des Clients für Sichern/Archivieren mit einem NetApp-Dateiserver während einer Momentaufnahmedifferenzsicherung verwenden.

Das HTTPS-Protokoll ist auf NetApp-Dateiservern standardmäßig aktiviert und kann nicht inaktiviert werden.

Wenn Sie eine Momentaufnahmedifferenzsicherung ausführen, baut der Client für Sichern/Archivieren eine Verwaltungssitzung mit einem NetApp-Dateiserver auf. Die Berechtigungsnachweise des Dateiservers (z. B. der Hostname oder die IP-Adresse des Dateiservers, der Benutzername, mit dem eine Verbindung zum Dateiserver hergestellt wird, und das Kennwort des Dateiservers) werden lokal auf dem Client für Sichern/Archivieren gespeichert. Diese Informationen müssen an den Dateiserver übertragen werden, um die authentifizierte Verwaltungssitzung aufbauen zu können. Es ist wichtig, eine sichere Verbindung zu verwenden, weil der Client für die Authentifizierung der Verwaltungssitzung des Dateiservers das Kennwort des Dateiservers in Klartext übertragen muss.

Sie müssen die Option snapdiffhttps bei jeder Ausführung einer Momentaufnahmedifferenzsicherung angeben, um eine sichere Verbindung mithilfe des HTTPS-Übertragungsprotokolls herzustellen. Ohne die Option snapdiffhttps kann der Client für Sichern/Archivieren Dateiserversitzungen nur mit dem HTTP-Protokoll aufbauen, was eine Aktivierung des HTTP-Verwaltungszugriffs auf dem Dateiserver erforderlich machen würde. Mit der Option snapdiffhttps können Sie eine sichere Verwaltungssitzung mit dem NetApp-Dateiserver aufbauen, ohne dass hierfür der HTTP-Verwaltungszugriff auf dem NetApp-Dateiserver aktiviert sein muss.

Einschränkungen:

Für Momentaufnahmedifferenzsicherungen mit HTTPS gelten die folgenden Einschränkungen:

- Die HTTPS-Verbindung wird nur für die sichere Übertragung von Daten über die Verwaltungssitzung zwischen dem Client für Sichern/Archivieren und dem NetApp-Dateiserver verwendet. Zu den Daten der Verwaltungssitzung gehören z. B. Berechtigungsnachweise des Dateiservers, Momentaufnahmeinformationen sowie Dateinamen und Attribute, die durch den Momentaufnahmedifferenzierungsprozess generiert werden. Über die HTTPS-Verbindung werden keine normalen Dateidaten übertragen, auf die der Client über die Dateifreigabe auf dem Dateiserver zugreift. Die HTTPS-Verbindung ist auch nicht für normale Dateidaten gültig, die der Client über das normale IBM Spectrum Protect-Client/Server-Protokoll an den IBM Spectrum Protect-Server überträgt.
- Die Option snapdiffhttps gilt nicht für vFilers, da das HTTPS-Protokoll auf dem NetApp vFiler nicht unterstützt wird.
- Die Option snapdiffhttps ist nur bei Verwendung der Befehlszeilenschnittstelle verfügbar. In der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren kann sie nicht verwendet werden.

- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme Momentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung ausführen
  Wenn Sie eine Momentaufnahmedifferenzsicherung ausführen, können Sie mit der Option snapdiffhttps eine sichere HTTPS-Verbindung zwischen dem Client für Sichern/Archivieren und dem NetApp-Dateiserver erstellen.

Zugehörige Konzepte:
Windows-BetriebssystemeVergleich zwischen Teilsicherung nach Datum, journalbasierter Sicherung sowie NetApp-Momentaufnahmedifferenzsicherung und vollständiger Teilsicherung und partieller Teilsicherung
Zugehörige Tasks:
NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren
Windows-BetriebssystemeMomentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung ausführen
Linux-BetriebssystemeMomentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung ausführen
Zugehörige Verweise:
Snapdiffhttps
Snapdiff

Selektive Sicherung

Verwenden Sie eine selektive Sicherung, wenn Sie bestimmte Dateien oder Verzeichnisse sichern möchten, unabhängig davon, ob eine aktuelle Kopie dieser Dateien auf dem Server vorhanden ist.

Teilsicherungen sind im Allgemeinen Teil eines automatisierten Systems zum Sichern vollständiger Dateisysteme. Dagegen können Sie mit selektiven Sicherungen eine Gruppe zu sichernder Dateien manuell auswählen, unabhängig davon, ob sich die Dateien seit der letzten Teilsicherung geändert haben.

Im Gegensatz zu Teilsicherungen bietet eine selektive Sicherung folgende Merkmale:

- Sie bewirkt keine Aktualisierung des Datums und der Uhrzeit der letzten Teilsicherung durch den Server.
- Verzeichnis- und Dateieinträge werden auch dann gesichert, wenn sich ihre Größe, ihre Änderungszeitmarken oder ihre Berechtigungen nicht geändert haben.
- Gelöschte Dateien verfallen nicht.
- Keine Sicherungsversionen an eine neue Verwaltungsklasse gebunden werden, wenn Sie die Verwaltungsklasse ändern.

Zugehörige Tasks:
Windows-BetriebssystemeDaten über die GUI sichern
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDaten über die Java-GUI sichern
Zugehörige Verweise:
Selective
Oracle Solaris-Betriebssysteme

Sicherungen der globalen Zone und der nicht globalen Zonen in Solaris

Bei Solaris Zones führen Sie Teilsicherungen und selektive Sicherungen von Dateisystemen innerhalb der Zone aus, in der diese Dateisysteme erstellt wurden.

Behandeln Sie jede nicht globale Zone als separates System mit einem eigenen IBM Spectrum Protect-Knotennamen und führen Sie Sicherungen aus jeder der Zonen heraus aus.

Wenn Sie Teilsicherungen oder selektive Sicherungen nicht globaler Zonen aus der globalen Zone heraus ausführen, muss der Administrator der globalen Zone entscheiden, welche Dateien in der nicht globalen Zone bei Sicherungen berücksichtigt oder ausgeschlossen werden. Beispielsweise werden Einheiten-, System- und Kerneldateien der nicht globalen Zonen nicht automatisch von Sicherungen ausgeschlossen, sie dürfen jedoch nicht gesichert werden. Das Zurückschreiben solcher Dateien kann eine nicht globale Zone unbrauchbar machen.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Zugriffsberechtigungen sichern

Während Sie Ihre Dateien sichern, sichert der Client für Sichern/Archivieren auch UNIX-Standardzugriffsberechtigungen, die den Dateien zugeordnet sind.

Abhängig vom Betriebssystem werden auch erweiterte Berechtigungen gesichert. Beispielsweise sichert der Client Zugriffssteuerungslisten für Dateien auf einer AIX-Workstation.

Ein berechtigter Benutzer kann Dateien für einen anderen Benutzer sichern, dies darf jedoch nicht zu Konflikten bei den Eigentumsrechten führen. Der Sicherungsserver zeichnet ordnungsgemäß auf, dass die Datei dem ursprünglichen Eigner gehört. Der berechtigte Benutzer muss dem ursprünglichen Eigner nicht den Zugriff auf die Sicherungsversionen erteilen.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Virtuellen Mountpunkt definieren

Wenn Sie ein berechtigter Benutzer sind und Dateien ab einem bestimmten Verzeichnis innerhalb eines Dateisystems sichern wollen, können Sie dieses Verzeichnis als virtuellen Mountpunkt definieren.

Das Definieren eines virtuellen Mountpunkts innerhalb eines Dateisystems stellt einen direkten Pfad auf die zu sichernden Dateien zur Verfügung, wodurch Verarbeitungszeit eingespart wird. Dies ist effizienter als zunächst das Dateisystem mit der Option domain zu definieren und anschließend mit der Option exclude die Dateien auszuschließen, die nicht gesichert werden sollen. Außerdem können hiermit Sicherungen und Archivierungen für bestimmte Verzeichnisse in separaten Dateibereichen im Speicher gespeichert werden.

Zugehörige Verweise:
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeVirtualmountpoint
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Daten über die Java-GUI sichern

Aus der Verzeichnisbaumstruktur können bestimmte Dateien, vollständige Verzeichnisse oder vollständige Dateisysteme gesichert werden.

Informationen zu diesem Vorgang

Die zu sichernden Dateien können mithilfe einer Such- bzw. Filterfunktion gesucht werden. Beim Filtern werden nur die Dateien angezeigt, die mit den Filterkriterien für die Sicherung übereinstimmen.

Verwenden Sie die Java™-GUI des Clients für Sichern/Archivieren, um Ihre Daten wie folgt zu sichern:

Vorgehensweise

1. Klicken Sie auf **Sichern** im Fenster IBM Spectrum Protect. Das Fenster 'Sichern' wird angezeigt.
2. Falls erforderlich, erweitern Sie die Verzeichnisbaumstruktur. Klicken Sie auf die Auswahlfelder neben den zu sichernden Objekten. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol **Suchen** in der Funktionsleiste.
3. Geben Sie die Suchkriterien in das Fenster 'Dateien suchen (Sichern)' ein.
4. Klicken Sie auf die Schaltfläche **Suchen**. Das Fenster 'Übereinstimmende Dateien (Sichern)' wird angezeigt.
5. Klicken Sie auf die Auswahlfelder neben den Dateien, die gesichert werden sollen, und schließen Sie das Fenster 'Übereinstimmende Dateien (Sichern)'.
6. Geben Sie die Filterkriterien in das Fenster 'Dateien suchen (Sichern)' ein.
7. Klicken Sie auf die Schaltfläche **Filter**. Das Fenster 'Sichern' zeigt die gefilterten Dateien an.
8. Klicken Sie auf die Auswahlfelder neben den gefilterten Dateien oder Verzeichnissen, die gesichert werden sollen.
9. Wählen Sie eine der folgenden Sicherungsarten im Pulldown-Menü aus: (1) Zum Ausführen einer Teilsicherung klicken Sie auf **Teilsicherung (vollständig)**. (2) Zum Ausführen einer Teilsicherung nach Datum klicken Sie auf **Teilsicherung (nur Datum)**. (3) Zum Ausführen einer selektiven Sicherung klicken Sie auf **Immer sichern**.
10. Klicken Sie auf **Sichern**. Im Fenster **Task-Liste** für die Sicherung wird der Verarbeitungsstatus der Sicherung angezeigt.

Ergebnisse

Beachten Sie die folgenden Hinweise, wenn Sie Ihre Daten über die Java-GUI sichern.

- Um bestimmte Sicherungsoptionen zu ändern, klicken Sie auf die Schaltfläche **Optionen**. Die ausgewählten Optionen sind *nur* während der aktuellen Sitzung wirksam.
- IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden. Bei jeder Sicherung einer Datei wird ihr eine Verwaltungsklasse zugeordnet. Bei der verwendeten Verwaltungsklasse kann es sich um die Standardverwaltungsklasse handeln, die Ihnen zugeordnet wird, oder um eine Verwaltungsklasse, die Sie der Datei mit der Option ***include*** in der Einschluss-/Ausschlussoptionsliste zuordnen. Wählen Sie **Dienstprogramme** > **Maßnahmeninformationen anzeigen** in der Java-GUI des Clients für Sichern/Archivieren oder in der Web-Client-GUI aus, um die Sicherungsmaßnahmen anzuzeigen, die vom IBM Spectrum Protect-Server für Ihren Clientknoten definiert wurden.
- Um eine automatische Teilsicherung Ihrer Standarddomäne auszuführen, wählen Sie **Aktionen →Domäne sichern** aus. Ihre Standarddomäne wird über die Option ***domain*** in Ihrer Clientbenutzeroptionsdatei (dsm.opt) definiert. Wenn Sie die Option ***domain*** nicht definiert haben, umfasst die Standarddomäne *alle lokalen Dateisysteme*.
- Sie können den Profileditor verwenden, um Dateisysteme in Ihrer Standarddomäne von der Sicherung auszuschließen.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
Zugehörige Verweise:
Domain
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Daten über die Befehlszeile sichern

Sie können den Befehl incremental oder selective verwenden, um Sicherungen auszuführen.

Die folgende Tabelle enthält Beispiele zur Verwendung dieser Befehle, um verschiedene Tasks auszuführen.

Tabelle 1. Beispiele für die Sicherung über die Befehlszeile

Task	**Befehl**	**Hinweise**
Teilsicherungen		
Eine Teilsicherung Ihrer Clientdomäne ausführen.	`dsmc incremental`	Der Abschnitt Incremental enthält weitere Informationen zum Befehl incremental.
Zusätzlich zu den Dateisystemen /home, /usr und /datasave in Ihrer Clientdomäne die Dateisysteme /fs1 und /fs2 sichern.	`dsmc incremental -domain="/fs1 /fs2"`	Weitere Informationen zur Option domain befinden sich im Abschnitt Domain.
Die Dateisysteme /Volumes/fs1 und /Volumes/fs2 neben den Datenträgern sichern, die in Ihrer Clientdomäne definiert sind.	`dsmc incremental -domain="/Volumes/fs1 /Volumes/fs2"`	Weitere Informationen zur Option domain befinden sich im Abschnitt Domain.
Alle lokalen Dateisysteme in Ihrer Clientdomäne außer dem Dateisystem `/home` sichern.	`dsmc incremental -domain="all-local -/home"`	Sie können den Operator Bindestrich (–) nicht vor dem Domänenschlüsselwort all-local verwenden. Weitere Informationen siehe Domain. Bei Windows-Clients können Sie auf diese Weise auch die Domäne systemstate von der Sicherungsverarbeitung ausschließen.
Nur die Dateisysteme /fs1 und /fs2 sichern.	`dsmc incremental /fs1 /fs2`	Keine
Alle Dateien im Verzeichnis /home und in allen seinen Unterverzeichnissen sichern.	`dsmc incremental /home/ -subdir=yes`	Weitere Informationen zur Option subdir befinden sich im Abschnitt Subdir.
Alle Dateien im Verzeichnis /Users und in allen seinen Unterverzeichnissen sichern.	`dsmc incremental /Users/ -subdir=yes`	Weitere Informationen zur Option subdir befinden sich im Abschnitt Subdir.
Angenommen, Sie haben eine Momentaufnahme des Dateisystems /usr gestartet und die Momentaufnahme als /snapshot/day1 angehängt. Führen Sie eine Teilsicherung aller Dateien und Verzeichnisse unter der lokalen Momentaufnahme aus und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen /usr.	`dsmc incremental /usr -snapshotroot=/snapshot/day1`	Der Client für Sichern/Archivieren betrachtet den Wert für snapshotroot als Dateibereichsnamen. Weitere Informationen finden Sie in Snapshotroot.
Teilsicherung nach Datum		
Eine Teilsicherung Ihrer Standardclientdomäne nach Datum ausführen.	`dsmc incremental -incrbydate`	Verwenden Sie die Option incrbydate im Befehl incremental, um neue und geänderte Dateien zu sichern, deren Änderungsdatum nach dem Datum der letzten auf dem Server gespeicherten Teilsicherung liegt. Incrbydate enthält weitere Informationen zur Option incrbydate.
Selektive Sicherungen		
Alle Dateien im Verzeichnis /home/proj oder /Users/van/Documents sichern.	`dsmc selective /home/proj/` oder `dsmc selective /Users/van/Documents/`	Verwenden Sie den Befehl selective, um bestimmte Dateien oder Verzeichnisse unabhängig davon zu sichern, ob sich die Dateien seit der letzten Teilsicherung geändert haben. Mithilfe von Platzhalterzeichen können mehrere Dateien gleichzeitig gesichert werden. Der Abschnitt Selective enthält weitere Informationen zum Befehl selective.

Task	Befehl	Hinweise
Alle Dateien im Verzeichnis /home/proj und in allen seinen Unterverzeichnissen sichern.	`dsmc selective /home/proj/ -subdir=yes`	Wenn Sie beim Sichern eines bestimmten Pfads und einer bestimmten Datei -subdir=*yes* angeben, sichert der Client rekursiv alle Unterverzeichnisse unter diesem Pfad und alle Instanzen der angegebenen Datei, die sich unter einem dieser Unterverzeichnisse befinden. Wenn es sich bei einem Unterverzeichnis um ein angehängtes Dateisystem handelt, sichert der Client die Dateien in diesem Unterverzeichnis nicht, wenn Sie die Option subdir=*yes* verwenden. Weitere Informationen zur Option subdir finden Sie in Subdir.
Alle Dateien im Verzeichnis /Users/van/Documents und in allen seinen Unterverzeichnissen sichern.	`dsmc selective /Users/van/Documents/ -subdir=yes`	Wenn Sie beim Sichern eines bestimmten Pfads und einer bestimmten Datei die Option -subdir=*yes* angeben, sichert der Client rekursiv alle Unterverzeichnisse unter diesem Pfad und alle Instanzen der angegebenen Datei, die sich unter einem dieser Unterverzeichnisse befinden. Wenn es sich bei einem Unterverzeichnis um ein angehängtes Dateisystem handelt, sichert der Client die Dateien in diesem Unterverzeichnis nicht, wenn Sie die Option subdir=*yes* verwenden. Weitere Informationen zur Option subdir finden Sie in Subdir.
Die Dateien /home/dir1/h1.doc und /home/dir1/test.doc sichern.	`dsmc selective /home/dir1/h1.doc /home/dir1/test.doc`	Geben Sie die Option removeoperandlimit mit dem Befehl incremental oder selective an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Dies ermöglicht Ihnen, mehr als 20 Dateien in einem einzelnen Befehl anzugeben. Weitere Informationen zu dieser Option siehe Removeoperandlimit.
Die Dateien /Users/ann/Documents/ h1.doc und /Users/ann/Documents/ test.doc sichern.	`dsmc selective /Users/ann/Documents/h1.doc /Users/ann/Documents/test.doc`	Geben Sie die Option removeoperandlimit mit dem Befehl incremental oder selective an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Dies ermöglicht Ihnen, mehr als 20 Dateien in einem einzelnen Befehl anzugeben. Weitere Informationen zu dieser Option finden Sie in Removeoperandlimit.
Eine Liste von Dateien in der Datei /home/filelist.txt sichern.	`selective -filelist=/home/filelist.txt`	Verwenden Sie die Option filelist, um eine Liste von Dateien zu verarbeiten. Weitere Informationen siehe Filelist.
Alle Dateien sichern, die in der Datei /Users/filelist.txt aufgeführt sind.	`dsmc selective -filelist=/Users/filelist.txt`	Verwenden Sie die Option filelist, um eine Liste von Dateien zu verarbeiten. Weitere Informationen siehe Filelist.
Angenommen, Sie haben eine Momentaufnahme des Dateisystems /usr gestartet und die Momentaufnahme als /snapshot/day1 angehängt. Führen Sie eine selektive Sicherung der Verzeichnisbaumstruktur /usr/dir1/sub1 aus der lokalen Momentaufnahme durch und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen /usr.	`dsmc selective /usr/dir1/sub1/ -subdir=yes -snapshotroot=/snapshot/day1`	Der Client betrachtet den Wert für snapshotroot als Dateibereichsnamen. Weitere Informationen finden Sie in Snapshotroot.

Zugehörige Verweise:
Incremental
Selective

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Sicherungsdaten löschen

Wenn Sie vom Administrator entsprechend berechtigt wurden, können Sie einzelne Sicherungskopien aus dem IBM Spectrum Protect-Server löschen, ohne den gesamten Dateibereich zu löschen. Um festzustellen, ob Sie über diese Berechtigung verfügen, wählen Sie Datei > Verbindungsinformationen in der GUI des Clients für Sichern/Archivieren oder im Hauptmenü des Web-Clients aus. Ihr Berechtigungsstatus wird im Feld Sicherungsdateien löschen zur Verfügung gestellt.

Informationen zu diesem Vorgang

Wichtig: Nach dem Löschen von Sicherungsdateien können diese ***nicht mehr zurückgeschrieben werden.*** Stellen Sie vor dem Löschen sicher, dass die gesicherten Dateien nicht mehr benötigt werden. Der Client fordert eine Bestätigung für den Löschvorgang an. Geben Sie daraufhin *ja* an, werden die angegebenen Dateien sofort gelöscht und aus dem IBM Spectrum Protect-Serverspeicher entfernt.

Um Sicherungskopien mithilfe der GUI des Clients für Sichern/Archivieren oder des Web-Clients zu löschen, gehen Sie wie folgt vor:

Vorgehensweise

1. Wählen Sie **Sicherungsdaten löschen** im Menü **Dienstprogramme** aus. Das Fenster 'Sicherung löschen' wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen **(+)** oder auf das Ordnersymbol neben dem Objekt, das eingeblendet werden soll, klicken.
3. Klicken Sie auf die Auswahlfelder neben den Objekten, die gelöscht werden sollen.
4. Wählen Sie einen Eintrag aus der Dropdown-Liste im oberen Bereich des Fensters **Sicherung löschen** aus, um anzugeben, welche Art von 'Sicherung löschen' ausgeführt werden soll. Sie können aktive Sicherungsversionen, inaktive Sicherungsversionen oder alle in der Baumstruktur ausgewählten Objekte löschen.

Ergebnisse

Anmerkung:

1. Ein Verzeichnis wird nur gelöscht, wenn Sie **Alle Objekte löschen** auswählen.
2. Um Sicherungskopien mithilfe des Befehlszeilenclients zu löschen, verwenden Sie den Befehl delete backup.

Zugehörige Verweise:
Delete Backup
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Dateibereiche löschen

Erteilt der IBM Spectrum Protect-Administrator einem Benutzer die Berechtigung, kann der Benutzer vollständige Dateibereiche aus dem Server löschen. Beim Löschen eines Dateibereichs werden alle Dateien und Images, sowohl Sicherungsversionen als auch Archivierungskopien, innerhalb dieses Dateibereichs gelöscht. Wird beispielsweise der Dateibereich `/tmp` gelöscht, werden alle Sicherungsversionen für alle Dateien in diesem Dateisystem und alle aus diesem Dateisystem archivierten Dateien gelöscht. Das Löschen eines Dateibereichs muss gründlich überlegt werden.

Informationen zu diesem Vorgang

Sie können einen Dateibereich auch mit dem Befehl delete filespace löschen. Verwenden Sie die Option class im Befehl delete filespace, um NAS-Dateibereiche zu löschen.

Sie können einzelne Sicherungsversionen löschen, indem Sie den Befehl delete backup verwenden.

Sie können Dateibereiche mithilfe der GUI des Clients für Sichern/Archivieren oder mithilfe von Befehlszeilenclients löschen. Um NAS-Dateibereiche zu löschen, verwenden Sie den Web-Client oder den Befehlszeilenclient.

Soll ein Dateibereich mit der grafischen Benutzerschnittstelle gelöscht werden, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Wählen Sie im Hauptfenster die Optionen Dienstprogramme > Dateibereiche löschen aus.
2. Klicken Sie auf die Auswahlfelder neben den Dateibereichen, die gelöscht werden sollen.
3. Klicken Sie auf die Schaltfläche Löschen. Der Client fordert Sie zur Bestätigung auf, bevor der Dateibereich gelöscht wird.

Zugehörige Verweise:
Class
Delete Backup
Delete Filespace

Windows-Betriebssysteme

Dateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (Windows)

Verwenden Sie den Befehl backup group, um eine Gruppe, aus einer Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen zu erstellen und in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server zu sichern.

Informationen zu diesem Vorgang

Über eine *Gruppensicherung* wird eine konsistente zeitpunktgesteuerte Sicherung für eine Gruppe von Dateien erstellt, die gemeinsam als logische Einheit verwaltet werden:

- Allen Objekten in der Gruppe wird dieselbe Verwaltungsklasse zugeordnet. Verwenden Sie die Option include, um eine Gruppe an eine Verwaltungsklasse zu binden.
- Vorhandene Anweisungen exclude für Dateien in der Gruppe werden ignoriert.
- Alle Objekte in der Gruppe werden gemeinsam exportiert.
- Alle Objekte in der Gruppe verfallen gemeinsam wie in der Verwaltungsklasse angegeben. Keine Objekte in der Gruppe verfallen, bevor nicht alle anderen Objekte in der Gruppe verfallen, selbst wenn eine andere Gruppe, zu denen diese Objekte gehören, verfällt.

Eine Gruppensicherung kann zu einem Sicherungssatz hinzugefügt werden.

Mithilfe der Option mode können Sie eine Gesamtsicherung oder eine Differenzsicherung ausführen.

Vorgehensweise

Geben Sie den Befehl backup group ein, um eine Gruppensicherung zu starten.
Beispiel: Geben Sie folgenden Befehl ein, um eine Gesamtsicherung aller Dateien in der Datei `c:\dir1\filelist1` auf den virtuellen Dateibereich `\virtfs` auszuführen, der das Hauptmember `c:\group1` enthält:

```
dsmc backup group -filelist=c:\dir1\filelist1 -groupname=group1 -virtualfsname=
\virtfs -mode=full
```

Zugehörige Konzepte:
Daten aus einem Sicherungssatz zurückschreiben
Zugehörige Verweise:
Backup Group
Einschlussoptionen
Mode
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Dateien aus einem oder mehreren Dateibereichen für eine Gruppensicherung sichern (UNIX und Linux)

Mit dem Befehl backup group können Sie eine Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen enthält, erstellen und in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server sichern.

Einschränkung: Der Befehl backup group gilt nicht für Mac OS X.

Über eine *Gruppensicherung* können Sie eine konsistente zeitpunktgesteuerte Sicherung für eine Gruppe von Dateien erstellen, die gemeinsam als logische Einheit verwaltet werden:

- Allen Objekten in der Gruppe wird dieselbe Verwaltungsklasse zugeordnet.
- Vorhandene Anweisungen *exclude* für Dateien in der Gruppe werden ignoriert.
- Alle Objekte in der Gruppe werden gemeinsam exportiert.
- Alle Objekte in der Gruppe verfallen gemeinsam wie in der Verwaltungsklasse angegeben. Keine Objekte in der Gruppe verfallen, bevor nicht alle anderen Objekte in der Gruppe verfallen, selbst wenn eine andere Gruppe, zu denen diese Objekte gehören, verfällt.

Eine Gruppensicherung kann zu einem Sicherungssatz hinzugefügt werden.

Mithilfe der Option mode können Sie eine Gesamtsicherung oder eine Differenzsicherung ausführen.

Beispiel: Geben Sie Folgendes ein, um eine Gesamtsicherung aller in der Datei `/home/dir1/filelist1` aufgeführten Dateien auf den virtuellen Dateibereich `/virtfs` auszuführen, der das Hauptmember `/home/group1` enthält:

```
dsmc backup group -filelist=/home/dir1/filelist1 -groupname=group1 -virtualfsname=
/virtfs -mode=full
```

Zugehörige Konzepte:

Daten aus einem Sicherungssatz zurückschreiben
Zugehörige Verweise:
Backup Group
Einschlussoptionen
Mode
 Windows-Betriebssysteme

Daten mit der Unterstützung für den Clientknoten-Proxy sichern (Windows)

Sicherungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.

Vorbereitende Schritte

Die folgenden Hinweise gelten, wenn Sie einen Proxy-Knoten verwenden, um Daten auf anderen Knoten zu sichern oder zurückzuschreiben:

- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise maxnummp und deduplication) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.
- Sie können asnodename nicht mit dem Befehl backup nas verwenden.
- Sie können asnodename nicht mit der Option fromnode verwenden.
- Wenn Sie asnodename zum Sichern und Zurückschreiben von Datenträgern in Clusterkonfigurationen verwenden, darf clusternode yes nicht verwendet werden.
- Sie können asnodename nicht zum Sichern oder Zurückschreiben des Systemstatus verwenden.
- Wenn ein Agentenknoten Daten aus einem Sicherungssatz zurückschreibt, wird das Systemstatusobjekt in dem Sicherungssatz nicht zurückgeschrieben.
- Sie können asnodename mit dem Befehl backup image verwenden; Sie müssen den Datenträger jedoch mit dem UNC-Namen angeben. Sie können nicht den Laufwerkbuchstaben verwenden.
- Wenn Sie denselben asnodename-Wert verwenden, um Dateien von verschiedenen Maschinen zu sichern, müssen Sie den Überblick darüber behalten, welche Dateien oder Datenträger von jedem System gesichert werden, damit Sie sie an die korrekte Position zurückschreiben können.
- In einer Umgebung mit mehreren Knoten sollten alle Agentenknoten denselben Plattformtyp aufweisen.
- Verwenden Sie Zielknoten nicht als traditionelle Knoten, insbesondere wenn Sie die Dateien verschlüsseln, bevor Sie sie auf dem Server sichern.

Informationen zu diesem Vorgang

Ein *Agentenknoten* ist ein Clientknoten, dem die Berechtigung erteilt wurde, Clientoperationen im Namen eines Zielknotens auszuführen.

Ein *Zielknoten* ist ein Clientknoten, der einem (oder mehreren) Agentenknoten die Berechtigung erteilt, in seinem Namen Clientoperationen auszuführen.

Die Verwendung eines Agentenknotens für die Sicherung von Zielknoten ist nützlich, wenn die für die Durchführung der Sicherung verantwortliche Workstation sich mit der Zeit ändern kann, wie es z. B. bei einer Clusterkonfiguration der Fall ist.

Mit der Option asnodename können Daten von einem anderen System zurückgeschrieben werden als dem, auf dem die Sicherung ausgeführt wurde.

Verwenden Sie die Option asnodename mit dem entsprechenden Befehl, um unter dem Zielknotennamen Daten auf dem IBM Spectrum Protect-Server zu sichern, zu archivieren, zurückzuschreiben oder abzurufen. Diese Unterstützung ist nur mit dem IBM Spectrum Protect-Server und -Client der Version 5.3 und höher verfügbar.

Vorgehensweise

Um diese Option zu aktivieren, führen Sie folgende Schritte aus:

1. Installieren Sie den Client für Sichern/Archivieren auf allen Knoten in einer gemeinsamen Datenumgebung.
2. Registrieren Sie jeden Knoten beim IBM Spectrum Protect-Server, falls er nicht existiert. Registrieren Sie den einheitlichen Zielknotennamen, damit er von allen Agentenknoten in Ihrer gemeinsamen Datenumgebung gemeinsam genutzt werden kann.
3. Registrieren Sie jeden Knoten in der gemeinsamen Datenumgebung beim IBM Spectrum Protect-Server. Dies ist der Agentenknotenname, der für Authentifizierungszwecke verwendet wird. Es werden keine Daten unter Verwendung des Knotennamens gespeichert, wenn die Option asnodename verwendet wird.
4. Erteilen Sie mithilfe des Befehls GRANT PROXYNODE allen Knoten in der gemeinsam genutzten Umgebung Proxy-Berechtigung, damit sie auf den Zielknotennamen auf dem IBM Spectrum Protect-Server zugreifen können (IBM Spectrum Protect-Administrator).
5. Verwenden Sie den Verwaltungsclientbefehl QUERY PROXYNODE, um die Clientknoten des berechtigten Benutzers anzuzeigen, denen mit dem Befehl GRANT PROXYNODE die Berechtigung erteilt wurde.

-  Windows-BetriebssystemeOperationen mit mehreren Knoten von der GUI aktivieren
  In der GUI können Sie Operationen mit mehreren Knoten aktivieren. Hierzu geben Sie im Profileditor den Namen des Zielknotens an, für

den Ihnen Proxy-Berechtigung erteilt wurde.

- Windows-BetriebssystemeVerschlüsselung definieren
  In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um die Verschlüsselung mit der Option encryptkey einzurichten.
- Windows-BetriebssystemeSicherungen mit der Unterstützung für den Clientknoten-Proxy planen
  Es können mehrere Knoten verwendet werden, um Sicherungsoperationen mithilfe des Schedulers auszuführen.

Zugehörige Verweise:
Asnodename
Windows-BetriebssystemeMac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Operationen mit mehreren Knoten von der GUI aktivieren

In der GUI können Sie Operationen mit mehreren Knoten aktivieren. Hierzu geben Sie im Profileditor den Namen des Zielknotens an, für den Ihnen Proxy-Berechtigung erteilt wurde.

Vorgehensweise

1. Prüfen Sie, ob der Clientknoten Proxy-Berechtigung für einen Zielknoten hat (oder berechtigt ist, als Zielknoten zu handeln). Verwenden Sie dazu den Verwaltungsclientbefehl QUERY PROXYNODE.
2. Wählen Sie Editieren > Clientvorgaben aus, um das Fenster 'Vorgaben' zu öffnen.
3. Wählen Sie die Registerkarte Allgemein aus und füllen Sie das Feld Wie Knotenname mit dem Namen des Zielknotens aus.
4. Klicken Sie auf Anwenden und anschließend auf OK, um das Fenster 'Vorgaben' zu schließen.

Nächste Schritte

Führen Sie einen der folgenden Schritte aus, um zu bestätigen, dass Ihr Clientknoten jetzt als Zielknoten auf den Server zugreift:

- Öffnen Sie das Baumstrukturfenster und überprüfen Sie, ob der Zielknotenname, der im Feld Wie Knotenname angegeben ist, angezeigt wird.
- Bestätigen Sie den Zielknotennamen im Feld Zugriff als Knoten im Fenster Verbindungsinformationen.

Um zur Operation mit Einzelknoten zurückzukehren, löschen Sie Wie Knotenname im Feld Zugriff als Knoten auf der Registerkarte Allgemein > Vorgaben.

Windows-Betriebssysteme

Verschlüsselung definieren

In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um die Verschlüsselung mit der Option encryptkey einzurichten.

Vorgehensweise

1. Geben Sie `encryptkey=save` in der Optionsdatei an.
2. Sichern Sie mindestens eine Datei mit `asnode=ProxyNodeName`, um auf jedem Agentenknoten in der Mehrfachknotenumgebung einen lokalen Verschlüsselungsschlüssel zu erstellen.

Ergebnisse

Führen Sie die folgenden Schritte aus, um mit der Option `encryptkey=prompt` die Verschlüsselung zu definieren:

1. Geben Sie `encryptkey=prompt` in der Optionsdatei an.
2. Stellen Sie sicher, dass die Benutzer der Agentenknoten in der Mehrfachknotenumgebung denselben Verschlüsselungsschlüssel verwenden.

Wichtig:

- Wenn Sie den Verschlüsselungsschlüssel ändern, müssen Sie die vorherigen Schritte wiederholen.
- Verwenden Sie denselben Verschlüsselungsschlüssel für alle Dateien, die in der gemeinsam genutzten Knotenumgebung gesichert wurden.

Windows-Betriebssysteme

Sicherungen mit der Unterstützung für den Clientknoten-Proxy planen

Es können mehrere Knoten verwendet werden, um Sicherungsoperationen mithilfe des Schedulers auszuführen.

Informationen zu diesem Vorgang

Wenn Sie den Agentenknoten Proxy-Berechtigung erteilen, führen diese geplante Sicherungsoperationen für den Zielknoten aus. Jeder Agentenknoten muss die Option asnodename innerhalb seines Zeitplans verwenden, um eine Mehrfachknotensicherung für den Agentenknoten auszuführen.

Führen Sie die folgenden Schritte aus, um die Zeitplanung mehrerer Knoten zu aktivieren:

1. Stellen Sie sicher, dass alle Agentenknoten Proxy-Berechtigung über einen gemeinsamen Zielknoten haben
2. Stellen Sie sicher, dass alle Agentenknoten einen Zeitplan auf dem Server definiert haben:

   ```
   def sched domain_name sched_name options='-asnode=target'
   ```

3. Stellen Sie sicher, dass jeder Agentenknoten seinen Zeitplan einem Knoten zugeordnet hat:

   ```
   def association domain_name schedule_name <Name des Agentenknotens>
   ```

Die folgenden Beispiele zeigen die Client/Server-Verwaltungsbefehle unter Verwendung des Schedulers auf mehreren Knoten.

- Der Administrator registriert alle zu verwendenden Knoten, indem er die folgenden Befehle ausgibt:
  - `register node NODE-A`
  - `register node NODE-B`
  - `register node NODE-C`
- Der Administrator erteilt jedem Agentenknoten Proxy-Berechtigung, indem er die folgenden Befehle ausgibt:
  - `grant proxynode target=NODE-Z agent=NODE-A`
  - `grant proxynode target=NODE-Z agent=NODE-B`
  - `grant proxynode target=NODE-Z agent=NODE-C`
- Der Administrator definiert die Zeitpläne, indem er die folgenden Befehle ausgibt:
  - `define schedule standard proxy1 description="NODE-A proxy schedule" action=incremental options="-asnode=NODE-Z" objects=C: startdate=05/21/2005 starttime=01:00`
  - `define schedule standard proxy2 description="NODE-B proxy schedule" action=incremental options="-asnode=NODE-Z" objects=D: startdate=05/21/2005 starttime=01:00`
  - `define schedule standard proxy3 description="NODE-C proxy schedule" action=incremental options="-asnode=NODE-Z" objects=E: startdate=05/21/2005 starttime=01:00`

Anmerkung: Fügen Sie die Option asnodename nur in die Zeitplandefinition ein. Fügen Sie sie nicht in die Clientoptionsdatei, in die Befehlszeile oder an einer anderen Position ein.

Starten Sie die Zeitpläne, indem Sie entweder einen Scheduler-Service konfigurieren oder den folgenden Clientbefehl verwenden: `dsmc sched`

Sie können auch den Clientakzeptor verwenden, wenn die Option managedservices in der Systemoptionsdatei auf 'schedule' gesetzt ist.
Wichtig:

- Jeder Zeitplan kann von einer anderen Workstation oder logischen Partition gestartet werden.
- Nachdem die Zeitpläne ausgeführt worden sind, kann jeder Proxy-Client alle gesicherten Daten abfragen und zurückschreiben.
- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise maxnummp und deduplication) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.

Zugehörige Verweise:
Asnodename
Sitzungseinstellungen und Zeitpläne für eine Proxy-Operation
Befehl DEFINE SCHEDULE
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Daten mit der Unterstützung für den Clientknoten-Proxy sichern (UNIX und Linux)

Sicherungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.

Informationen zu diesem Vorgang

Die Konsolidierung von Sicherungen zu einem einheitlichen Zielknotennamen auf dem Server ist bei Konfigurationen hilfreich, bei denen sich die für die Durchführung der Sicherung zuständige Workstation mit der Zeit ändern kann, wie es beispielsweise bei einem Cluster der Fall ist.

Ein Agentenknoten ist ein Clientknoten, dem die Berechtigung erteilt wird, Clientoperationen im Namen eines Zielknotens auszuführen.

Ein Zielknoten ist ein Clientknoten, der einem oder mehreren Agentenknoten die Berechtigung erteilt, in seinem Namen Clientoperationen auszuführen.

Verwenden Sie die Option asnodename mit dem entsprechenden Befehl, um Daten unter dem Zielknotennamen auf dem Server zu sichern, zu archivieren, zurückzuschreiben und abzurufen.

Mit der Option asnodename können Daten außerdem von einem anderen System zurückgeschrieben werden als dem, auf dem die Sicherung ausgeführt wurde.

Beachten Sie Folgendes, wenn Sie einen Proxy-Knoten verwenden, um Daten auf anderen Knoten zu sichern oder zurückzuschreiben:

- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise maxnummp und deduplication) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.
- Auf allen Agentenknoten in der Mehrfachknotenumgebung muss derselben Betriebssystemtyp ausgeführt werden.
- Verwenden Sie keine Zielknoten als herkömmliche Knoten, insbesondere, wenn Sie Ihre Dateien vor der Sicherung auf dem Server verschlüsseln.
- Sie können nicht auf einen anderen Knoten zugreifen (weder über die GUI-Dropdown-Liste noch mithilfe der Option fromnode).
- Sie können keine NAS-Sicherung oder -Zurückschreibung durchführen.

Vorgehensweise

1. Installieren Sie den Client für Sichern/Archivieren auf allen Knoten in einer gemeinsamen Datenumgebung.
2. Registrieren Sie jeden Knoten beim IBM Spectrum Protect-Server. Registrieren Sie den einheitlichen Zielknotennamen, damit er von allen Agentenknoten in Ihrer gemeinsamen Datenumgebung gemeinsam genutzt werden kann.
3. Registrieren Sie jeden Knoten in der gemeinsamen Datenumgebung beim IBM Spectrum Protect-Server. Registrieren Sie den Agentenknotennamen, der für Authentifizierungzwecke verwendet wird. Daten werden nicht unter diesem Knotennamen auf dem Server gespeichert, wenn die Option asnodename verwendet wird.
4. Der IBM Spectrum Protect-Serveradministrator muss mithilfe des Befehls GRANT PROXYNODE allen Knoten in der gemeinsam genutzten Umgebung Proxy-Berechtigung erteilen, damit sie auf den Zielknotennamen zugreifen können.
5. Verwenden Sie den Verwaltungsclientbefehl QUERY PROXYNODE, um die Clientknoten des berechtigten Benutzers anzuzeigen, dem mit dem Befehl GRANT PROXYNODE die Berechtigung erteilt wurde.

- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeOperationen mit mehreren Knoten von der GUI aktivieren
  In der GUI können Sie Operationen mit mehreren Knoten aktivieren. Hierzu geben Sie im Profileditor den Namen des Zielknotens an, für den Ihnen Proxy-Berechtigung erteilt wurde.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeVerschlüsselung definieren
  In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um die Verschlüsselung mit der Option encryptkey einzurichten.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeSicherungen mit der Unterstützung für den Clientknoten-Proxy planen
  Es können mehrere Knoten verwendet werden, um Sicherungsoperationen mithilfe des Schedulers auszuführen.

Zugehörige Verweise:
Asnodename
Windows-Betriebssysteme Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Operationen mit mehreren Knoten von der GUI aktivieren

In der GUI können Sie Operationen mit mehreren Knoten aktivieren. Hierzu geben Sie im Profileditor den Namen des Zielknotens an, für den Ihnen Proxy-Berechtigung erteilt wurde.

Vorgehensweise

1. Prüfen Sie, ob der Clientknoten Proxy-Berechtigung für einen Zielknoten hat (oder berechtigt ist, als Zielknoten zu handeln). Verwenden Sie dazu den Verwaltungsclientbefehl QUERY PROXYNODE.
2. Wählen Sie Editieren > Clientvorgaben aus, um das Fenster 'Vorgaben' zu öffnen.
3. Wählen Sie die Registerkarte Allgemein aus und füllen Sie das Feld Wie Knotenname mit dem Namen des Zielknotens aus.
4. Klicken Sie auf Anwenden und anschließend auf OK, um das Fenster 'Vorgaben' zu schließen.

Nächste Schritte

Führen Sie einen der folgenden Schritte aus, um zu bestätigen, dass Ihr Clientknoten jetzt als Zielknoten auf den Server zugreift:

- Öffnen Sie das Baumstrukturfenster und überprüfen Sie, ob der Zielknotenname, der im Feld Wie Knotenname angegeben ist, angezeigt wird.
- Bestätigen Sie den Zielknotennamen im Feld Zugriff als Knoten im Fenster Verbindungsinformationen.

Um zur Operation mit Einzelknoten zurückzukehren, löschen Sie Wie Knotenname im Feld Zugriff als Knoten auf der Registerkarte Allgemein > Vorgaben.

Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Verschlüsselung definieren

In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um die Verschlüsselung mit der Option encryptkey einzurichten.

Vorgehensweise

1. Geben Sie encryptkey=save in der Optionsdatei an.
2. Sichern Sie mindestens eine Datei mit asnode=ProxyNodeName, um auf jedem Agentenknoten in der Mehrfachknotenumgebung einen lokalen Verschlüsselungsschlüssel zu erstellen.

Ergebnisse

Führen Sie die folgenden Schritte aus, um mit der Option encryptkey=prompt die Verschlüsselung zu definieren:

1. Geben Sie encryptkey=prompt in der Optionsdatei an.
2. Stellen Sie sicher, dass die Benutzer der Agentenknoten in der Mehrfachknotenumgebung denselben Verschlüsselungsschlüssel verwenden.

Wichtig:

- Wenn Sie den Verschlüsselungsschlüssel ändern, müssen Sie die vorherigen Schritte wiederholen.
- Verwenden Sie denselben Verschlüsselungsschlüssel für alle Dateien, die in der gemeinsam genutzten Knotenumgebung gesichert wurden.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Sicherungen mit der Unterstützung für den Clientknoten-Proxy planen

Es können mehrere Knoten verwendet werden, um Sicherungsoperationen mithilfe des Schedulers auszuführen.

Informationen zu diesem Vorgang

Wenn Sie den Agentenknoten Proxy-Berechtigung erteilen, führen diese geplante Sicherungsoperationen für den Zielknoten aus. Jeder Agentenknoten muss die Option asnodename innerhalb seines Zeitplans verwenden, um eine Mehrfachknotensicherung für den Agentenknoten auszuführen.

Starten Sie die Zeitpläne mit dem Clientbefehl `dsmc sched`:

Die folgenden Beispiele zeigen die Client/Server-Verwaltungsbefehle unter Verwendung des Schedulers auf mehreren Knoten.

- Der Administrator registriert alle zu verwendenden Knoten, indem er die folgenden Befehle ausgibt:
  - `register node NODE-A`
  - `register node NODE-B`
  - `register node NODE-C`
- Der Administrator erteilt mithilfe der folgenden Befehle jedem Agentenknoten Proxy-Berechtigung:
  - `grant proxynode target=NODE-Z agent=NODE-A`
  - `grant proxynode target=NODE-Z agent=NODE-B`
  - `grant proxynode target=NODE-Z agent=NODE-C`
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme
  Mac OS X-BetriebssystemeDer Administrator definiert die Zeitpläne mithilfe der folgenden Befehle:
  - `define schedule standard proxy1 description="NODE-A proxy schedule" action=incremental options="-asnode=NODE-Z" objects=/Volumes/Xsan1 startdate=05/21/2005 starttime=01:00`
  - `define schedule standard proxy2 description="NODE-B proxy schedule" action=incremental options="-asnode=NODE-Z" objects=/Volumes/Xsan2 startdate=05/21/2005 starttime=01:00`
  - `define schedule standard proxy3 description="NODE-C proxy schedule" action=incremental options="-asnode=NODE-Z" objects=/Volumes/Xsan3 startdate=05/21/2005 starttime=01:00`

Anmerkung: Fügen Sie die Option asnodename nur in die Zeitplandefinition ein. Fügen Sie sie nicht in die Clientoptionsdatei, in die Befehlszeile oder an einer anderen Position ein.
Sie können auch den Clientakzeptordämon (dsmcad) verwenden, wenn managedservices in der Systemoptionsdatei auf schedule gesetzt ist.
Anmerkung:

- Jeder Zeitplan kann von einer anderen Workstation oder logischen Partition gestartet werden.
- Nachdem die Zeitpläne ausgeführt worden sind, kann jeder Proxy-Client alle gesicherten Daten abfragen und zurückschreiben.
- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise maxnummp und deduplication) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.

- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeBeispiele für die Planung einer Sicherung eines IBM PowerHA SystemMirror-Clusters
  Dieser Abschnitt enthält einige Beispiele für das Sichern eines IBM® PowerHA SystemMirror-Clusters.
- AIX-Betriebssysteme Linux-BetriebssystemeSicherung eines GPFS-Dateisystems planen
  Sie sichern ein GPFS-Dateisystem mithilfe des Schedulers und der Proxy-Beziehungen.

Zugehörige Verweise:
Asnodename
Sitzungseinstellungen und Zeitpläne für eine Proxy-Operation
Befehl DEFINE SCHEDULE
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Beispiele für die Planung einer Sicherung eines IBM PowerHA SystemMirror-Clusters

Dieser Abschnitt enthält einige Beispiele für das Sichern eines IBM® PowerHA SystemMirror-Clusters.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Zeitplanung mehrerer Knoten zu aktivieren:

1. Stellen Sie sicher, dass alle Agentenknoten Proxy-Berechtigung über einen gemeinsamen Zielknoten haben
2. Stellen Sie sicher, dass alle Agentenknoten einen Zeitplan auf dem Server definiert haben:

   ```
   def sched domain_name sched_name options='-asnode=target'
   ```

3. Stellen Sie sicher, dass jeder Agentenknoten seinen Zeitplan einem Knoten zugeordnet hat:

   ```
   def association domain_name schedule_name <Name des Agentenknotens>
   ```

In den folgenden Beispielen ist IBM PowerHA SystemMirror für zwei AIX-Hosts konfiguriert, `host_a` und `host_b`. Neben ihren eigenen lokalen Daten nutzen die Hosts Plattenspeicher gemeinsam, der über zwei Dateibereiche verfügt: `/disk1` und `/disk2`.

Das Beispiel mit CLUSTERNODE zeigt, wie die Option clusternode in einer aktuellen IBM PowerHA SystemMirror-Umgebung verwendet wird.

- Der Administrator definiert 3 Knoten auf dem IBM Spectrum Protect-Server: `host_a`, `host_b`, `cluster_group`. Hierzu werden die folgenden Befehle verwendet: (1) `REGISTER NODE host_a mysecretpa5s`, (2) `REGISTER NODE host_b mysecretpa5s`, (3) `REGISTER NODE cluster_group mysecretpa5s`.
- Der Administrator definiert eine Datei dsm.opt auf `host_a` und `host_b` (beachten Sie, dass sich die opt-Dateien auf den Hosts unterscheiden). Dazu verwendet er die folgenden Befehle: (1) `NODENAME host_a (Standardwert der Option kann verwendet werden)`, (2) `DOMAIN /home /usr ... etc.`.
- Der Administrator definiert die Datei dsm.opt, die sich auf einer der Clusterplattengruppen befindet, beispielsweise `/disk1/tsm/dsm.opt`. Dazu verwendet er die folgenden Befehle: (1) `NODENAME cluster_group`, (2) `DOMAIN /disk1 /disk2`, (3) `CLUSTERNODE YES`.
- Der Administrator definiert mit dem folgenden Befehl einen Zeitplan auf dem IBM Spectrum Protect-Server: `DEFINE SCHEDULE STANDARD CLUSTER_BACKUP`.
- Der Administrator definiert mit dem folgenden Befehl Zuordnungen für jeden der 3 Knoten: `DEFINE ASSOC STANDARD CLUSTER_BACKUP host_a,host_b,cluster_group`. Es werden jeweils drei Instanzen des Schedulers des Clients für Sichern/Archivieren ausgeführt. (Dabei ist der Scheduler für `cluster_group` Teil der Clusterressourcen, für die eine Übernahme erfolgt, wenn für die Plattenressourcen der Clustergruppe eine Übernahme erfolgt. Somit würde er entweder auf `host_a` oder auf `host_b`, aber nicht auf beiden gleichzeitig ausgeführt werden.)
- Alle drei Knotennamen enthalten Daten auf dem IBM Spectrum Protect-Server.

Das Beispiel mit ASNODE zeigt eine generische Lösung, die für nicht unterstützte UNIX-Clusterlösungen angewendet werden könnte, z. B. Veritas Cluster Server für Solaris.

- Der Administrator definiert 3 Knoten auf dem IBM Spectrum Protect-Server, `host_a`, `host_b`, `cluster_group`:

  ```
  REGISTER NODE host_a mysecretpa5s
  REGISTER NODE host_b mysecretpa5s
  REGISTER NODE cluster_group mysecretpa5s
  ```

- Der Administrator definiert eine Proxy-Knotenbeziehung von `host_a` und `host_b` zu `hacmp_cluster`:

  ```
  GRANT PROXYNODE TARGET=cluster_group AGENT=host_a,host_b
  ```

- Der Administrator definiert eine Datei dsm.opt auf `host_a` und `host_b`, um die lokalen Dateisysteme zu verarbeiten:

  ```
  NODENAME        host_a (Standardwert der Option kann verwendet werden)
  DOMAIN                 /home /usr ... etc.
  NODENAME         host_b (Standardwert der Option kann verwendet werden)
  DOMAIN                 /home /usr ... etc.
  ```

- Der Administrator definiert eine Datei dsm.opt auf der Clusterressource, um die Sicherung der Clusterressourcen zu verarbeiten, z. B. `/disk1/tsm/dsmcluster.opt` (der Knotenname ist der Standardknotenname, der entweder `host_a` oder `host_b` lautet, abhängig davon, welche Workstation zu dem jeweiligen Zeitpunkt die Clustergruppe enthält):

  ```
  DOMAIN          /disk1 /disk2
  ASNODE    cluster_group
  ```

- Der Administrator definiert einen Zeitplan auf dem IBM Spectrum Protect-Server:

  ```
  DEFINE SCHEDULE STANDARD CLUSTER_BACKUP
  ```

- Der Administrator definiert Zuordnungen für alle 3 Knoten:

  ```
  DEFINE ASSOC STANDARD CLUSTER_BACKUP host_a,host_b,cluster_group
  ```

- Es werden jeweils drei Instanzen des Schedulers des Clients für Sichern/Archivieren ausgeführt. Dabei wird der Scheduler für den Knoten `hacmp_cluster` entweder auf `host_a` oder auf `host_b`, aber nicht auf beiden ausgeführt (er ist in den Clusterressourcen enthalten, für die eine Übernahme erfolgen würde). Dieser Scheduler würde auf die Datei `dsmcluster.opt` zeigen, die auf jedem Host definiert ist. Die drei Instanzen würden folgendermaßen gestartet werden:

  ```
  [host_a]                   dsmc sched
  [host_b]                      dsmc sched
  [cluster_group] dsmc sched -optfile=/disk/tsm/dsmcluster.opt
  ```

- Alle drei Knotennamen enthalten Daten auf dem IBM Spectrum Protect-Server.

Weitere Informationen zu den Server-Schedulerbefehlen enthält die Dokumentation zum Server.

AIX-BetriebssystemeLinux-Betriebssysteme

Sicherung eines GPFS-Dateisystems planen

Sie sichern ein GPFS-Dateisystem mithilfe des Schedulers und der Proxy-Beziehungen.

Informationen zu diesem Vorgang

Es wird vorausgesetzt, dass drei Knoten in einem GPFS-Cluster an der Sicherungsoperation beteiligt sind. Die Knoten node_1, node_2 und node_3 werden nur für die Authentifizierung verwendet. Die Objekte werden in Dateibereichen gesichert, die zum Knoten node_gpfs gehören.

Vorgehensweise

1. Definieren Sie vier Knoten auf dem IBM Spectrum Protect-Server.

   ```
   REGISTER NODE node_1 mysecretpa5s

   REGISTER NODE node_2 mysecretpa5s

   REGISTER NODE node_3 mysecretpa5s

   REGISTER NODE node_gpfs mysecretpa5s
   ```

2. Definieren Sie eine Proxy-Beziehung zwischen den Knoten.

   ```
   GRANT PROXYNODE TARGET=node_gpfs AGENT=node_1, node_2, node_3
   ```

3. Definieren Sie einen Zeitplan.

   ```
   DEFINE SCHEDULE STANDARD GPFS_SCHEDULE ACTION=incremental
   OBJECTS="/gpfs"

   DEFINE ASSOCIATION STANDARD GPFS_SCHEDULE node_gpfs
   ```

4. Wählen Sie eines der GPFS-Systeme für die Ausführung des Zeitplans aus. Geben Sie die Optionen nodename und asnodename in der Optionsdatei dsm.sys auf allen Systemen in dem GPFS-Cluster an. Der Wert für die Option asnodename muss auf allen Systemen identisch sein.

   Definitionen in der Optionsdatei dsm.sys auf node 1:

   ```
   nodename node_1
   asnodename node_gpfs
   ```

   Definitionen in der Optionsdatei dsm.sys auf node 2:

   ```
   nodename node_2
   asnodename node_gpfs
   ```

   Definitionen in der Optionsdatei dsm.sys auf node 3:

```
nodename node_3
asnodename node_gpfs
```

5. Starten Sie den Scheduler auf dem System, das für die Ausführung des Zeitplans ausgewählt wurde.

```
DSMC SCHED
```

Zugehörige Informationen:
AIX-Betriebssysteme Linux-Betriebssysteme Befehl 'mmbackup': IBM Spectrum Protect-Voraussetzungen
AIX-Betriebssysteme Linux-Betriebssysteme Anleitung für die Integration von IBM Spectrum Scale AFM mit IBM Spectrum Protect
AIX-Betriebssysteme Linux-Betriebssysteme Verwendung der Einschluss- und Ausschlussoptionen von IBM Spectrum Protect in Verbindung mit dem IBM Spectrum Scale-Befehl 'mmbackup'
Windows-Betriebssysteme

Lokale Momentaufnahme einem Serverdateibereich zuordnen (Windows)

Verwenden Sie die Option snapshotroot in den Befehlen incremental und selective in Verbindung mit einer Anwendung eines anderen Herstellers zur Erstellung einer Momentaufnahme eines logischen Datenträgers, um die Daten in der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

Die Option snapshotroot bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

Zugehörige Verweise:
Snapshotroot
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Lokale Momentaufnahme einem Serverdateibereich zuordnen (UNIX und Linux)

Verwenden Sie die Option snapshotroot in den Befehlen incremental und selective in Verbindung mit einer Anwendung eines anderen Herstellers zur Erstellung einer Momentaufnahme eines logischen Datenträgers, um die Daten in der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

Die Option snapshotroot bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

Zugehörige Verweise:
Snapshotroot
Windows-Betriebssysteme

Windows-Systemstatus sichern

Der Client für Sichern/Archivieren verwendet VSS, um alle Systemstatuskomponenten als ein einziges Objekt zu sichern, um eine konsistente zeitpunktgesteuerte Momentaufnahme des Systemstatus bereitzustellen. Der Systemstatus besteht aus allen bootfähigen Systemstatus- und Systemservicekomponenten.

Informationen zu diesem Vorgang

Der Client unterstützt den Microsoft Volumeschattenkopie-Dienst (VSS = Volume Shadowcopy Service) auf den unterstützten Windows-Clients.

Der Systemstatus wird von verschiedenen VSS-Ausgabeprogrammen durch den Typ "bootfähiger Systemstatus" und "Systemservice" dargestellt. Im Hinblick auf die Anzahl Dateien und den Umfang der Daten ist System Writer der größte Bestandteil des Systemstatus. Für System Writer wird standardmäßig eine Teilsicherung ausgeführt. Sie können die Option systemstatebackupmethod verwenden, um Gesamtsicherungen von System Writer auszuführen. Weitere Informationen zu dieser Option finden Sie in Systemstatebackupmethod. Der Client sichert alle anderen Ausgabeprogramme immer vollständig.

Die Liste der bootfähigen Systemstatus- und Systemservicekomponenten ist dynamisch und kann sich abhängig von installierten Service-Packs und Betriebssystemfeatures ändern. Der Client ermöglicht die dynamische Erkennung und Sicherung dieser Komponenten.

Sie müssen ein Mitglied der Gruppe 'Administratoren' oder der Gruppe 'Sicherungsoperatoren' sein, um Systemstatusinformationen sichern zu können.

Führen Sie folgende Schritte aus, um ein Systemstatusobjekt über die Befehlszeile zu sichern:

1. Verwenden Sie in der Befehlszeile den Befehl **backup systemstate**, um alle Systemstatus- oder Systemservicekomponenten als Einzelobjekt zu sichern.
2. Verwenden Sie den Befehl **query systemstate**, um Informationen zu einer Sicherung des Systemstatus auf dem IBM Spectrum Protect-Server anzuzeigen.

Führen Sie folgende Schritte aus, um ein Systemstatusobjekt über die GUI zu sichern:

1. Klicken Sie auf **Sichern** im Hauptfenster der grafischen Benutzerschnittstelle. Das Fenster 'Sichern' wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) klicken. Zum Anzeigen von Dateien in einem Ordner klicken Sie auf das Ordnersymbol.
3. Suchen Sie den Knoten Systemstatus in der Verzeichnisbaumstruktur. Sie können den Knoten Systemstatus erweitern, um die Komponenten anzuzeigen.
4. Klicken Sie auf das Auswahlfeld neben dem Knoten Systemstatus, um das gesamte Systemstatusobjekt zu sichern. Sie können den Knoten Systemstatus nur als Ganzes sichern, da Abhängigkeiten zwischen den Systemstatuskomponenten bestehen. Standardmäßig sind alle Komponenten ausgewählt; Sie können keine einzelnen Systemstatuskomponenten sichern.
5. Klicken Sie auf **Sichern**. Im Fenster Taskliste für die Sicherung wird der Verarbeitungsstatus der Sicherung angezeigt. Nach Beendigung der Verarbeitung werden im Fenster "Sicherungsbericht" die Verarbeitungsdetails angezeigt.

System- und Bootdateien werden nur als Gruppe gesichert, wenn ein Member der Gruppe (eine der Dateien) geändert wird. Haben sich die Dateien seit der letzten Sicherung nicht geändert, werden die System- und Bootdateien nicht redundant gesichert.

Systemstatussicherungen werden standardmäßig an die Standardverwaltungsklasse gebunden. Sollen sie an eine andere Verwaltungsklasse gebunden werden, müssen Sie die Option include.systemstate verwenden; geben Sie all als Muster an und geben Sie den Namen der neuen Verwaltungsklasse an.

Mithilfe der Option domain können Sie den gesamten Systemstatus von der Domänenteilsicherungsverarbeitung ausschließen.

Das Systemverzeichnis `dllcache` ist jetzt bei der Sicherung der Bootpartition auf Windows-Systemen eingeschlossen. Sind die `dllcache`-Dateien bei der Zurückschreibung eines Windows-Computers nicht verfügbar, werden möglicherweise die Installationsmedien des Betriebssystems für die Systemwiederherstellung benötigt. Durch das Sichern des Verzeichnisses `dllcache` können Sie vermeiden, dass während der Systemzurückschreibungen die Installationsmedien benötigt werden.

Wenn Sie nicht wollen, dass das Verzeichnis `dllcache` in die Sicherung Ihrer Bootpartition einbezogen wird und Sie die Einschränkungen einer Nichtsicherung des Verzeichnisses `dllcache` verstehen, können Sie eine Anweisung exclude.dir verwenden, um das Sichern dieser Dateien zu unterdrücken. Zum Beispiel:

```
exclude.dir c:\windows\system32\dllcache
```

Auf Windows-Clients werden mit dem Befehl backup systemstate auch ASR-Daten gesichert.

Zugehörige Tasks:
Windows-Systemstatus zurückschreiben
Zugehörige Verweise:
Backup Systemstate
Domain
Ausschlussoptionen
Einschlussoptionen
Query Systemstate
Restore Systemstate
 Windows-Betriebssysteme

Dateien für automatische Systemwiederherstellung sichern

Sie können Dateien für die automatische Systemwiederherstellung (Automated System Recovery - ASR) als Vorbereitung für die Wiederherstellung der Windows-Plattenkonfigurationsdaten und des Systemstatus im Falle eines schwerwiegenden System- oder Hardwarefehlers sichern.

Informationen zu diesem Vorgang

Der Client für Sichern/Archivieren sichert ASR-Daten, wenn der Client für Sichern/Archivieren den Windows-Systemstatus sichert.

Vorgehensweise

Für die Sicherung von ASR-Dateien auf Windows-Betriebssystemen verwenden Sie den Befehl backup systemstate.

Ergebnisse

Der Client generiert die ASR-Dateien im Verzeichnis zur Zwischenspeicherung, \adsm.sys\ASR, auf dem Systemlaufwerk Ihrer lokalen Workstation und speichert diese Dateien im Dateibereich ASR auf dem IBM Spectrum Protect-Server.

Zugehörige Konzepte:
Vorbereitung für automatische Systemwiederherstellung
Zugehörige Tasks:
Dateien für die automatische Systemwiederherstellung zurückschreiben
Zugehörige Verweise:
Backup Systemstate
 Windows-Betriebssysteme

Vorbereitung für automatische Systemwiederherstellung

Für die automatische Systemwiederherstellung (ASR) unter Windows sind bestimmte Sicherungen und Datenträger erforderlich.

- Windows-BetriebssystemeClientoptionsdatei für die automatische Systemwiederherstellung erstellen
  Bevor Sie einen Windows-Computer unter Verwendung der automatischen Systemwiederherstellung (Automated System Recovery, ASR) wiederherstellen können, müssen Sie eine Optionsdatei erstellen. Die Optionsdatei ist für jeden Computer eindeutig.
- Windows-BetriebssystemeBootlaufwerk und Systemlaufwerk für die automatische Systemwiederherstellung sichern
  Bevor Sie Ihren Windows-Computer mithilfe der automatischen Systemwiederherstellung (Automated System Recovery, ASR) wiederherstellen können, benötigen Sie eine vollständige Sicherung des Bootlaufwerks und des Systemlaufwerks.

Windows-Betriebssysteme

Clientoptionsdatei für die automatische Systemwiederherstellung erstellen

Bevor Sie einen Windows-Computer unter Verwendung der automatischen Systemwiederherstellung (Automated System Recovery, ASR) wiederherstellen können, müssen Sie eine Optionsdatei erstellen. Die Optionsdatei ist für jeden Computer eindeutig.

Informationen zu diesem Vorgang

Bei dieser Task wird vorausgesetzt, dass Sie eine generische bootfähige WinPE-CD oder -DVD erstellt haben. Eine generische bootfähige WinPE-CD enthält nicht die Clientoptionsdatei (dsm.opt), da die Optionsdatei für jeden Computer eindeutig ist. Diese Task hilft Ihnen bei der Erstellung einer computerspezifischen Optionsdatei.

Die Windows-Vorinstallationsumgebung (WinPE) erfordert bestimmte Optionswerte.

Vorgehensweise

1. Suchen Sie nach einer Kopie der Clientoptionsdatei. Sie können die Datei an verschiedenen Positionen finden:
   - Im Installationsverzeichnis eines installierten IBM Spectrum Protect-Clients befindet sich eine Optionsdatei. Die Standardinstallationsposition ist C:\Programme\Tivoli\TSM\baclient\dsm.opt. Wenn Sie die Optionsdatei für den Computer haben, der zurückgeschrieben werden soll, erfordert diese Optionsdatei die wenigsten Änderungen.
   - Im Clientinstallationspaket ist eine Beispieloptionsdatei enthalten. Der Pfad in dem Paket lautet TSM_BA_Client\Programme\Tivoli\TSM\config\dsm.smp. Benennen Sie die Datei in dsm.opt um.
2. Editieren Sie die Datei dsm.opt.
   a. Geben Sie eine beschreibbare Position für das Fehlerprotokoll ein. Der Client für Sichern/Archivieren erstellt mehrere Protokolldateien. Verwenden Sie die Option errorlogname, um die Position der Protokolldatei anzugeben. Geben Sie beispielsweise in dsm.opt `errorlogname x:\dsmerror.log` an.
   Anmerkung: In diesem Beispiel wird x: verwendet, da im WinPE-Modus das Standardsystemlaufwerk x: ist.
   b. Geben Sie den Clientknotennamen über die Option nodename ein.
   c. Optional: Wenn Sie planen, den Systemstatus von Dateien zurückzuschreiben, die auf dem IBM Spectrum Protect-Server gespeichert sind, geben Sie die Serververbindungsinformationen ein. Geben Sie die entsprechenden Werte für die Optionen commmethod und tcpserveraddress ein.
   d. Optional: Wenn Ihnen das Kennwort für den Knoten bekannt ist, geben Sie das Kennwort mit der Option password ein.
3. Kopieren Sie die Datei dsm.opt auf Datenträger, die der Zielcomputer während der automatischen Systemwiederherstellung lesen kann.
4. Optional: Kopieren Sie Registrierungsinformationen des IBM Spectrum Protect-Clients auf Datenträger, die der Zielcomputer während der automatischen Systemwiederherstellung lesen kann. Verwenden Sie das Dienstprogramm regedit.exe, um Registrierungseinträge des IBM Spectrum Protect-Clients aus dem Schlüssel HKLM\SOFTWARE\IBM zu exportieren. Führen Sie beispielsweise in einem Fenster mit Eingabeaufforderung den folgenden Befehl aus:

   ```
   regedit /e tsmregistry.out "HKEY_LOCAL_MACHINE\SOFTWARE\IBM"
   ```

   Kopieren Sie die Datei tsmregistry.out auf Datenträger, die der Zielcomputer während der automatischen Systemwiederherstellung lesen kann.
   Während der automatischen Systemwiederherstellung können Sie die Registrierungseinträge aus der Datei tsmregistry.out importieren. Der Client für Sichern/Archivieren kann die Registrierungseinträge in der WinPE-Umgebung verwenden, um auf Sicherungskopien auf dem IBM Spectrum Protect-Server zuzugreifen.
   Anmerkung: Das Sichern der Registrierungseinträge ist optional, da andere Möglichkeiten bestehen, um auf den kennwortgeschützten IBM Spectrum Protect-Server zuzugreifen. Für den Zugriff auf den Server haben Sie folgende Möglichkeiten:
   - Wenn Ihnen das Kennwort für den Knoten bekannt ist, können Sie das Kennwort eingeben, wenn Sie während der Wiederherstellung dazu aufgefordert werden.
   - Bitten Sie den IBM Spectrum Protect-Administrator, das Kennwort für den Knoten zu ändern und Ihnen das neue Kennwort zum Zeitpunkt der Wiederherstellung mitzuteilen.
   - Stellen Sie die Kennwortinformationen in der Datei dsm.opt bereit.

   Sind die Dateien, die zurückgeschrieben werden sollen, in einem Sicherungssatz auf Band oder auf einer CD oder DVD enthalten, müssen Sie nicht auf den IBM Spectrum Protect-Server zugreifen.

Ergebnisse

Sie haben eine Optionsdatei erstellt, die Clientkonfigurationsinformationen enthält, die für jeden Computer eindeutig sind. Diese Informationen ergänzen die generische bootfähige WinPE-CD.

Zugehörige Tasks:
Bootfähige WinPE-CD erstellen
 Windows-Betriebssysteme

Bootlaufwerk und Systemlaufwerk für die automatische Systemwiederherstellung sichern

Bevor Sie Ihren Windows-Computer mithilfe der automatischen Systemwiederherstellung (Automated System Recovery, ASR) wiederherstellen können, benötigen Sie eine vollständige Sicherung des Bootlaufwerks und des Systemlaufwerks.

Vorgehensweise

1. Führen Sie eine vollständige Teilsicherung Ihrer System- und Bootlaufwerke durch. Unter der Annahme, dass sich Ihre System- und Bootdateien auf Laufwerk c: befinden, geben Sie den folgenden Befehl ein:

   ```
   dsmc incremental c:
   ```

2. Den Systemstatus sichern. Geben Sie den folgenden Befehl ein, um den Systemstatus zu sichern:

   ```
   dsmc backup systemstate
   ```

   Geben Sie den folgenden Befehl ein, um zu prüfen, ob der Systemstatus gesichert wurde:

   ```
   dsmc query systemstate
   ```

   Sie können `-showmembers=yes` angeben, um Details auf Dateiebene anzuzeigen.

Zugehörige Konzepte:
Vollständige und partielle Teilsicherung
Zugehörige Tasks:
Windows-Systemstatus sichern
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Imagesicherung

Von Ihrer lokalen Workstation aus können Sie einen logischen Datenträger als einzelnes Objekt auf Ihrem System sichern (Imagesicherung).

Die traditionelle statische Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeSie müssen Root sein, um diese Task auszuführen, und die Imagesicherung gilt nicht für Mac OS X.

 Windows-BetriebssystemeBei diesen Datenträgern kann es sich um formatierte NTFS- oder ReFS-Datenträger oder um unformatierte (RAW) Datenträger handeln. Ist ein Datenträger mit NTFS formatiert, werden nur diejenigen Blöcke gesichert, die vom Dateisystem verwendet werden oder kleiner als der Parameter imagegapsize sind.

 Windows-BetriebssystemeNormalerweise können Sie eine Imagesicherung des Systemlaufwerks nicht an dieselbe Position zurückschreiben, da eine exklusive Sperre des Systemlaufwerks nicht möglich ist. In einer Windows-Vorinstallationsumgebung (WinPE) ist jedoch eine Imagezurückschreibung des Systemlaufwerks möglich. Informationen zum Zurückschreiben von Daten in einer WinPE-Umgebung finden Sie in Technote 7005028.

 Windows-BetriebssystemeSie können eine Imagesicherung nicht auf den Datenträger zurückschreiben, auf dem der Client gerade ausgeführt wird. Ziehen Sie eine Installation des Clients für Sichern/Archivieren auf dem Systemlaufwerk in Betracht.

 Windows-BetriebssystemeBei der Imagesicherung ist die Konsistenz von Systemobjekten, wie beispielsweise Active Directory, nicht gesichert. Systemobjekte können über mehrere Datenträger verteilt sein, und es empfiehlt sich, sie mit dem Befehl backup systemstate zu sichern.

Eine Imagesicherung bietet die folgenden Vorteile:

- Schnellere Sicherung von Dateisystemen, die eine große Anzahl Dateien enthalten, im Vergleich zu einer Teilsicherung des gesamten Dateisystems.
- Verbesserung der Geschwindigkeit, mit der der Client Dateisysteme zurückschreibt, die viele kleine Dateien enthalten.
- Ressourceneinsparung auf dem Server während der Sicherung, da für ein Image nur ein Eintrag erforderlich ist.
- Bereitstellung eines Bildes Ihres logischen Datenträgers zu einem bestimmten Zeitpunkt, das im Bedarfsfall abgerufen werden kann.
- Zurückschreibung eines beschädigten Dateisystems oder unformatierten logischen Datenträgers. Nach dem Zurückschreiben haben die Daten denselben Status wie bei der letzten Sicherung des logischen Datenträgers.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDie traditionelle statische Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen. Verwenden Sie die Option dynamicimage, um den Datenträger im aktuellen Status ohne erneutes Anhängen mit Lesezugriff zu sichern. Die Sicherung kann beschädigt werden, wenn Anwendungen auch während der Ausführung der Sicherung weiter auf den Datenträger schreiben. Wird während der Ausführung einer Imagesicherung auf einen Datenträger geschrieben, kann es nach einer Zurückschreibungsoperation zu Dateninkonsistenzen und Datenverlust kommen. Die Option dynamicimage überschreibt den Kopiennummerierungswert in der Verwaltungsklasse bei der Durchführung von Imagesicherungen. Führen Sie nach dem Zurückschreiben einer Imagesicherung, die mit der Option dynamicimage erfolgt ist, immer das Dienstprogramm `chkdsk` aus.

Windows-BetriebssystemeDie traditionelle offline ausgeführte Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen. Wenn Sie ein Image mit der Angabe `snapshotproviderimage=none` sichern, führen Sie nach dem Zurückschreiben der Daten immer das Dienstprogramm fsck aus.

Um eine Imagesicherung eines Datenträgers zurückschreiben zu können, muss der Client für Sichern/Archivieren eine exklusive Sperre des Datenträgers erlangen können, der gerade zurückgeschrieben wird.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeEinschränkung: Verwenden Sie dynamische Imagesicherungen nicht für Dateisysteme, da das Dateisystem möglicherweise selbst dann inkonsistente Daten bereitstellt, wenn keine Schreibaktivität stattfindet. Die dynamische Imagesicherung kann außerdem zu einem nicht exakten Image führen, das bei der Zurückschreibung möglicherweise ungültig oder unvollständig ist.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWenn der Client für Sichern/Archivieren das Dateisystem nach dem Zurückschreiben eines Image nicht anhängen kann, führen Sie fsck aus. Das Ausführen von fsck kann sich jedoch auf die Integrität großer Datenvolumen auswirken. Verwenden Sie die dynamische Imagesicherung nicht für JFS2-Dateisysteme unter AIX. Der Client lässt dynamische Imagesicherungen für JFS2-Dateisysteme unter AIX nicht zu. Wenn Sie `dynamicimage=yes` für ein JFS2-Dateisystem angeben, führt der Client eine momentaufnahmebasierte Imagesicherung aus. Wenn die Momentaufnahme aus irgendeinem Grund nicht erstellt werden kann, führt der Client stattdessen eine statische Imagesicherung aus.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAchtung: Um Datenverluste zu verhindern, sollten Sie die Verwendung der Option dynamicimage vermeiden und sicherstellen, dass keine Schreibaktivität auf dem Datenträger stattfindet, während die Sicherung ausgeführt wird.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeFür AIX JFS2-Dateisysteme wird das Datenvolumen reduziert, das bei einer statischen Imagesicherung oder einer Momentaufnahmeimagesicherung auf dem IBM Spectrum Protect-Server gesichert wird, indem nur diejenigen Blöcke gesichert werden, die vom Dateisystem verwendet werden oder kleiner als der Wert der Option imagegapsize sind. Diese Methode der Datensicherung verbessert die Leistung der Imagesicherung. Weitere Informationen siehe Imagegapsize.

AIX-BetriebssystemeNur für AIX-Clients: Standardmäßig führt der Client eine Onlinemomentaufnahmeimagesicherung der JFS2-Dateisysteme aus, während der der Datenträger für andere Systemanwendungen verfügbar ist.

Linux-BetriebssystemeNur für Linux-Clients: Standardmäßig führt der Client eine Momentaufnahmeimagesicherung der Dateisysteme auf einem logischen Datenträger aus, der von Linux Logical Volume Manager erstellt wurde. Der Datenträger steht anderen Systemanwendungen zur Verfügung, während die Momentaufnahmeimagesicherung ausgeführt wird.

Linux-BetriebssystemeFür Linux-Clients: Die Imagesicherung von DASD-Einheiten mit dem Modus 'raw_track_access' unter Linux on z Systems wird nicht unterstützt.

Windows-BetriebssystemeWenn die Online-Imageunterstützung konfiguriert ist, führt der Client eine Online-Imagesicherung aus, während der der Datenträger für andere Systemanwendungen verfügbar ist. Der durch die Option snapshotproviderimage angegebene Momentaufnahmeprovider erhält während der Online-Imagesicherung ein konsistentes Image eines Datenträgers aufrecht.

Windows-BetriebssystemeSie können mit der Option snapshotproviderimage im Befehl backup image oder mit der Option include.image angeben, ob eine Offline- oder Online-Imagesicherung ausgeführt werden soll.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAchtung: Von IBM Spectrum Protect for Space Management verwaltete Dateisysteme sind nicht für die Imagesicherung aktiviert.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeVorausgesetzte Tasks vor der Erstellung einer Imagesicherung ausführen
  In diesem Abschnitt sind einige Punkte aufgelistet, die zu berücksichtigen sind, bevor Sie eine Imagesicherung ausführen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeVerwendung von Imagesicherungen für die Ausführung von Dateisystemteilsicherungen
  In diesem Abschnitt sind die Methoden und Schritte zum Ausführen effizienter Teilsicherungen Ihres Dateisystems mithilfe von Imagesicherungen aufgelistet.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeImagesicherung über die GUI ausführen
  Wenn die Imagesicherungsfunktion konfiguriert ist, können Sie eine Imagesicherung erstellen, während der der reale Datenträger für andere Systemanwendungen verfügbar ist.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeImagesicherung über die Befehlszeile ausführen
  Imagesicherungs- und -zurückschreibungsoperationen für einen einzelnen Datenträger werden mit dem Befehl backup image bzw. restore image ausgeführt.

Zugehörige Tasks:
Windows-BetriebssystemeUnterstützung für Online-Imagesicherung konfigurieren
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeMomentaufnahmebasierte Dateisicherung und -archivierung und momentaufnahmebasierte Imagesicherung
Zugehörige Verweise:
Windows-BetriebssystemeSnapshotproviderimage
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme

Vorausgesetzte Tasks vor der Erstellung einer Imagesicherung ausführen

In diesem Abschnitt sind einige Punkte aufgelistet, die zu berücksichtigen sind, bevor Sie eine Imagesicherung ausführen.

Informationen zu diesem Vorgang

Die folgenden Hinweise sind für Imagesicherungen zu beachten.

- Windows-Betriebssysteme*Sie müssen über Administratorberechtigung für das System verfügen, um Offline- oder Online-Imagesicherungen durchführen zu können.*
- Windows-BetriebssystemeSie benötigen nicht mehr als ein Laufwerk, um eine Imagesicherung auszuführen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeStellen Sie sicher, dass keine andere Anwendung den Datenträger verwendet, wenn Sie eine statische Imagesicherung ausführen. Um während der Sicherungsverarbeitung ein konsistentes Image sicherzustellen, hängt der Client den Datenträger ab und schreibgeschützt wieder an, sodass keine andere Anwendung auf den Datenträger schreiben kann, wenn ein Dateibereich auf dem Datenträger festgestellt wird. Ist der Datenträger im Gebrauch, wenn der Client versucht, ihn abzuhängen, schlägt die Sicherung fehl. Wenn der Client den Datenträger nicht abhängen und schreibgeschützt wieder anhängen kann, da dieser in Gebrauch ist, und keine Momentaufnahmeimagesicherung verfügbar ist, können Sie die Option dynamicimage verwenden. Damit können Sie den Client zwingen, eine Imagesicherung auszuführen, ohne den Datenträger abzuhängen und im schreibgeschützten Modus wieder anzuhängen. Setzen Sie in einer Anweisung include.image oder in der Befehlszeile die Option dynamicimage. Die Sicherung kann beschädigt werden, wenn Anwendungen auf den Datenträger schreiben, während die Sicherung gerade ausgeführt wird. Dieses Problem kann durch Ausführen von `fsck` nach dem Zurückschreiben behoben werden, um eventuell beschädigte Blöcke zu reparieren.

  Wenn auf dem zu sichernden Datenträger kein Dateisystem erkannt wird, stellen Sie sicher, dass alle Anwendungen, die auf die Datenträger schreiben, stillgelegt werden. Der Client für Sichern/Archivieren verwendet die Dateisystemtabelle und die Ladetabelle, um die unterstützten Dateisysteme zu ermitteln.

  Schließen Sie *keine* Systemdateien in eine Imagesicherung ein, da aktiv verwendete Dateisysteme nicht abgehängt werden können.

  Nur für AIX und Linux: Wenn Sie eine Imagesicherung eines angehängten Dateisystems ausführen, das an einen anderen Mountpunkt angehängt und in der Dateisystemtabelle angegeben ist, gehen nach Durchführung der Imagesicherung alle Mountoptionen für dieses Dateisystem außer dem Lese- oder Schreibstatus verloren.

  Wichtig: Verfügt ein angehängtes Dateisystem über verschachtelte Mountpunkte, müssen diese vor dem Versuch einer Sicherung abgehängt werden. Andernfalls kann der Client die Bereitstellung des Datenträgers nicht aufheben. Das Dateisystem wird als *aktiv* angesehen, wenn es angehängt ist.

- Windows-BetriebssystemeStellen Sie sicher, dass keine andere Anwendung den Datenträger verwendet, wenn Sie eine Offline-Imagesicherung ausführen. Um während der Sicherungsverarbeitung ein konsistentes Image sicherzustellen, sperrt der Client den Datenträger, sodass keine andere Anwendung auf den Datenträger schreiben kann. Ist der Datenträger im Gebrauch, wenn der Client versucht, ihn zu sperren, schlägt die Sicherung fehl. Kann der Client einen Datenträger nicht sperren, da dieser in Gebrauch ist, können Sie eine Online-Imagesicherung ausführen.
- Verwenden Sie die Option include.image, um dem Datenträgerimage eine Verwaltungsklasse zuzuordnen. Wenn Sie keine Verwaltungsklasse zuordnen, wird die Standardverwaltungsklasse für das Image verwendet.
  Windows-BetriebssystemeAnmerkung: Ist die Option snapshotproviderimage auf *none* gesetzt, werden die durch die Verwaltungsklasse definierten Kopiennummerierungsparameter verwendet.
- Über die Option exclude.image können Sie einen Datenträger von der Imagesicherung ausschließen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeSie müssen den Mountpunkt für den Dateisystemdatenträger verwenden, für den eine Imagesicherung ausgeführt werden soll. Der Client sichert keinen Dateisystemdatenträger ohne die Verwendung eines Mountpunkts. Sichern Sie Dateisysteme mithilfe des Mountnamens. Beispiel: Ist `/dev/lv01` als Dateisystem formatiert, das an `/home` angehängt ist, geben Sie den folgenden Befehl ein, um eine Imagesicherung dieses Datenträgers auszuführen:

  ```
  dsmc backup image /home
  ```

  Sichern Sie unformatierte Datenträger mithilfe des Einheitennamens. Beispiel: Wenn `/dev/lv02` ein unformatierter Datenträger ist, geben Sie den folgenden Befehl ein, um eine Imagesicherung dieses Datenträgers durchzuführen:

  ```
  dsmc backup image /dev/lv02
  ```

  Wenn Sie einen unformatierten Datenträger sichern, der als Dateisystem formatiert ist, stellen Sie sicher, dass das Dateisystem nicht angehängt ist und keinen Eintrag in `/etc/filesystems` hat.

- Windows-BetriebssystemeSie müssen den Mountpunkt oder Laufwerkbuchstaben für den Datenträger verwenden, für den eine Imagesicherung ausgeführt werden soll. Der Client sichert keinen Datenträger ohne die Verwendung eines Laufwerkbuchstabens oder Mountpunkts.
- Windows-BetriebssystemeSchließen Sie das Systemlaufwerk nicht in eine Imagesicherung ein, da der Client das Systemlaufwerk beim Zurückschreiben nicht exklusiv sperren kann. Das Systemlaufwerkimage kann dann nicht an dieselbe Position zurückgeschrieben werden. Bei der Imagesicherung ist die Konsistenz von Systemobjekten, wie beispielsweise Active Directory, nicht gesichert. Systemobjekte können über mehrere Datenträger verteilt sein, und es empfiehlt sich, sie über die jeweiligen Sicherungsbefehle zu sichern. Da eine Imagesicherung nicht auf einen Datenträger zurückgeschrieben werden kann, von dem der Client gerade ausgeführt wird (oder auf einen Datenträger, den der Client nicht exklusiv sperren kann), sollten Sie das Clientprogramm auf dem Systemlaufwerk installieren.
  Anmerkung: Wenn Sie jedoch WinPE verwenden, ist eine Imagezurückschreibung des Systemlaufwerks möglich. Weitere Informationen enthält die Veröffentlichung IBM Spectrum Protect Recovery Techniques Using Windows Preinstallation Environment (Windows PE).
- Windows-BetriebssystemeWerden bei einer LAN-unabhängigen oder LAN-gestützten Imagesicherung defekte Plattensektoren auf dem Quellenlaufwerk festgestellt, kann es unter Umständen zu einem Datenverlust kommen. In diesem Fall werden defekte Sektoren übersprungen, wenn die Imagedaten auf den IBM Spectrum Protect-Server gesendet werden. Werden fehlerhafte Sektoren während der Imagesicherung festgestellt, wird nach Abschluss der Imagesicherung eine Warnung ausgegeben.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeUnterstützung für eine Imagesicherung nach Einheitentyp des Datenträgers
  In diesem Abschnitt sind einige Einheiten aufgelistet, die vom Befehl backup image unterstützt werden.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
Zugehörige Verweise:
Ausschlussoptionen
Einschlussoptionen
Windows-BetriebssystemeSnapshotproviderimage
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Verwendung von Imagesicherungen für die Ausführung von Dateisystemteilsicherungen

In diesem Abschnitt sind die Methoden und Schritte zum Ausführen effizienter Teilsicherungen Ihres Dateisystems mithilfe von Imagesicherungen aufgelistet.

Mithilfe dieser Sicherungsmethoden können Sie eine zeitpunktgesteuerte Zurückschreibung für Ihre Dateisysteme ausführen und den Durchsatz beim Sichern und Zurückschreiben verbessern. Sie können die Sicherung nur auf formatierten Datenträgern und nicht auf unformatierten logischen Datenträgern ausführen.

Verwenden Sie eine der folgenden Methoden, um Imagesicherungen für Datenträger mit angehängten Dateisystemen auszuführen.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeMethode 1: Imagesicherungen mit Teilsicherungen des Dateisystems verwenden
  In diesem Abschnitt sind die Schritte aufgelistet, die Sie durchführen müssen, um Imagesicherungen mit Teilsicherungen des Dateisystems auszuführen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeMethode 2: Imagesicherungen mit Imageteilsicherungen nach Datum verwenden
  In diesem Abschnitt sind die Schritte aufgelistet, die Sie durchführen müssen, um Imagesicherungen mit Imageteilsicherungen nach Datum auszuführen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeVergleich der Methoden 1 und 2
  Dieser Abschnitt enthält einen Vergleich der Methoden 1 und 2: (1) Imagesicherung mit Teilsicherungen des Dateisystems verwenden oder (2) Imagesicherung mit Imageteilsicherung nach Datum verwenden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Methode 1: Imagesicherungen mit Teilsicherungen des Dateisystems verwenden

In diesem Abschnitt sind die Schritte aufgelistet, die Sie durchführen müssen, um Imagesicherungen mit Teilsicherungen des Dateisystems auszuführen.

Informationen zu diesem Vorgang

Vorgehensweise

1. Führen Sie eine vollständige Teilsicherung des Dateisystems aus. Dies ist die Basis für die späteren Teilsicherungen.
2. Führen Sie eine Imagesicherung desselben Dateisystems aus, damit Imagezurückschreibungen möglich sind.

3. Führen Sie in regelmäßigen Abständen Teilsicherungen des Dateisystems aus, damit alle hinzugefügten und gelöschten Dateien auf dem Server aufgezeichnet werden.
4. Führen Sie in regelmäßigen Abständen eine Imagesicherung aus, um die Zurückschreibungszeit zu verkürzen.
5. Schreiben Sie Ihre Daten über eine Teilzurückschreibung zurück. Stellen Sie sicher, dass Sie **Image plus Teilsicherung von Verzeichnissen und Dateien** und **Inaktive Dateien von Lokal löschen** im Fenster für Zurückschreibungsoptionen ausgewählt haben, bevor Sie die Zurückschreibung starten. Während der Zurückschreibung führt der Client Folgendes durch:

Ergebnisse

- Er schreibt das neueste Image auf dem Server zurück.
- Er löscht alle im vorherigen Schritt zurückgeschriebenen Dateien, die auf dem Server inaktiv sind. Dies sind Dateien, die zum Zeitpunkt der Imagesicherung vorhanden waren, aber danach gelöscht und durch eine spätere Teilsicherung aufgezeichnet wurden.
- Er schreibt neue und geänderte Dateien aus den Teilsicherungen zurück.

Anmerkung: Wenn eine Teilsicherung nach der Sicherung eines Image mehrmals ausgeführt wird, müssen Sie sicherstellen, dass die Sicherungskopiengruppe des IBM Spectrum Protect-Servers über genügend Versionen für vorhandene und gelöschte Dateien auf dem Server verfügt, damit das nachfolgende Zurückschreibungsimage mit den Optionen incremental und deletefiles die Dateien ordnungsgemäß löschen kann.

Zugehörige Tasks:
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDaten über die Java-GUI sichern
Windows-BetriebssystemeDaten über die GUI sichern
Imagesicherung über die GUI ausführen
Image über die GUI zurückschreiben
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme

Methode 2: Imagesicherungen mit Imageteilsicherungen nach Datum verwenden

In diesem Abschnitt sind die Schritte aufgelistet, die Sie durchführen müssen, um Imagesicherungen mit Imageteilsicherungen nach Datum auszuführen.

Vorgehensweise

1. Führen Sie eine Imagesicherung des Dateisystems aus.
2. Führen Sie eine Imageteilsicherung nach Datum für das Dateisystem aus. Hierdurch werden nur die Dateien an den Server gesendet, die seit der letzten Imagesicherung hinzugefügt oder geändert wurden.
3. Führen Sie in regelmäßigen Abständen vollständige Imagesicherungen aus.
4. Schreiben Sie Ihren Datenträger über eine Teilzurückschreibung zurück. Stellen Sie sicher, dass Sie die Option **Image plus Teilsicherung von Verzeichnissen und Dateien** im Fenster für Zurückschreibungsoptionen ausgewählt haben, bevor Sie die Zurückschreibung starten. Damit werden zunächst das neueste Image und anschließend alle Teilsicherungen seit diesem Datum zurückgeschrieben.

Ergebnisse

Anmerkung: In den folgenden Fällen sollten Sie regelmäßige vollständige Imagesicherungen ausführen:

- Wenn der Änderungsumfang des Dateisystems hoch ist (mehr als 40 %), wie in Schritt 4 bei Methode 1 und Schritt 3 bei Methode 2 angegeben. Beim Zurückschreiben erhalten Sie auf diese Weise ein Dateisystemimage, das dem Image bei der letzten Teilsicherung nach Datum ähnlich ist; außerdem wird die Zurückschreibungsdauer verkürzt.
- Entsprechend den Anforderungen in Ihrer Umgebung.

Dadurch wird die Zurückschreibungszeit verbessert, da weniger Änderungen von Teilsicherungen angewendet werden.

Bei Verwendung von Methode 2 gelten folgende Einschränkungen:

- Das Dateisystem darf keine früheren vollständigen Teilsicherungen aufweisen.
- Durch eine Imageteilsicherung nach Datum werden Dateien auf dem Server nicht inaktiviert; demzufolge sind, wenn Sie ein Image mit der Option incremental zurückschreiben, Dateien vorhanden, die nach der ursprünglichen Imagesicherung gelöscht wurden.
- Bei der ersten Imagesicherung des Dateisystems wird eine vollständige Imagesicherung ausgeführt.
- Wenn die maximale Kapazität der Dateisysteme bereits oder fast erreicht ist, kann hierdurch eine Bedingung 'Zu wenig Speicherbereich' während der Zurückschreibung auftreten.

Zugehörige Tasks:
Imagesicherung über die GUI ausführen
Image über die GUI zurückschreiben
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme

Vergleich der Methoden 1 und 2

Dieser Abschnitt enthält einen Vergleich der Methoden 1 und 2: (1) Imagesicherung mit Teilsicherungen des Dateisystems verwenden oder (2) Imagesicherung mit Imageteilsicherung nach Datum verwenden.

Als Hilfe bei der Entscheidung, welche Methode für Ihre Umgebung geeignet ist, enthält die folgende Tabelle einen Vergleich der Methoden 1 und 2.

Tabelle 1. Vergleich der Methoden zur Imageteilsicherung

Methode 1: Imagesicherung mit Teilsicherungen des Dateisystems verwenden	**Methode 2: Imagesicherung mit Imageteilsicherung nach Datum verwenden**
Dateien werden auf dem Server als verfallen gekennzeichnet, wenn sie aus dem Dateisystem gelöscht werden. Beim Zurückschreiben haben Sie die Möglichkeit, die auf dem Server verfallenen Dateien aus dem Image zu löschen.	Dateien werden auf dem Server nicht als verfallen gekennzeichnet. Nach der Imageteilzurückschreibung sind alle Dateien, die nach der Imagesicherung aus dem Dateisystem gelöscht wurden, wieder vorhanden. Wenn die maximale Kapazität der Dateisysteme bereits oder fast erreicht ist, kann hierdurch eine Bedingung 'Zu wenig Speicherbereich' auftreten.
Die für Teilsicherungen erforderliche Zeit entspricht der Zeit, die für normale Teilsicherungen erforderlich ist.	Die für Imageteilsicherungen erforderliche Zeit ist kürzer, da der Client nicht jede zu kopierende Datei beim Server abfragen muss.
Die Zurückschreibung erfolgt wesentlich schneller im Vergleich zu einer vollständigen Teilzurückschreibung des Dateisystems.	Die Zurückschreibung erfolgt wesentlich schneller im Vergleich zu einer vollständigen Teilzurückschreibung des Dateisystems.
Verzeichnisse, die nach der letzten Imagesicherung aus dem Dateisystem gelöscht wurden, sind nicht als verfallen gekennzeichnet.	Verzeichnisse und Dateien, die nach der letzten Imagegesamtsicherung aus dem Dateisystem gelöscht wurden, sind nicht als verfallen gekennzeichnet.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Imagesicherung über die GUI ausführen

Wenn die Imagesicherungsfunktion konfiguriert ist, können Sie eine Imagesicherung erstellen, während der der reale Datenträger für andere Systemanwendungen verfügbar ist.

Informationen zu diesem Vorgang

Während der Imagesicherung wird ein konsistentes Image des Datenträgers aufrechterhalten.

Windows-BetriebssystemeWenn Sie eine Imagesicherung mit der Option image backup der Client-GUI ausführen, wird die Sicherungsoperation gemäß der Einstellung für snapshotproviderimage in Ihrer Clientoptionsdatei (dsm.opt) ausgeführt. Wenn die Online-Imageunterstützung konfiguriert ist, führt der Client eine Online-Imagesicherung aus, während der der Datenträger für andere Systemanwendungen verfügbar ist.

AIX-BetriebssystemeLinux-BetriebssystemeWenn Sie eine Imagesicherung mit der Option image backup der GUI des Clients für Sichern/Archivieren ausführen, wird die Sicherungsoperation gemäß der Einstellung für die Option snapshotproviderimage ausgeführt. Der Standardwert für die Option snapshotproviderimage ist eine AIX JFS2-Momentaufnahme für AIX und eine Linux LVM-Momentaufnahme für Linux. Sie können den Standardwert auf der Registerkarte 'Momentaufnahme' unter den Vorgaben für Momentaufnahmeimage im Profileditor überschreiben.

Oracle Solaris-BetriebssystemeFür Solaris-Clients: Bei Auswahl der Option image backup wird standardmäßig eine statische Imagesicherung ausgeführt. Bei der statischen Imagesicherung hängt der Client den Datenträger ab und schreibgeschützt wieder an, damit keine anderen Anwendungen auf ihn zugreifen können. Sie können den Standardwert überschreiben, indem Sie die Option include.image verwenden und dynamicimage *yes* auswählen. Bei der dynamischen Imagesicherung führt der Client die Imagesicherung aus, ohne das Dateisystem während der Sicherung schreibgeschützt zu machen.

Zur Erstellung einer Imagesicherung des Dateisystems oder des unformatierten logischen Datenträgers sind folgende Schritte auszuführen:

Vorgehensweise

1. Klicken Sie auf die Schaltfläche **Sichern** im IBM Spectrum Protect-Hauptfenster. Das Fenster 'Sichern' wird angezeigt.
2. Erweitern Sie die Verzeichnisstruktur und wählen Sie die zu sichernden Objekte aus. Zum Sichern eines unformatierten logischen Datenträgers das Objekt RAW in der Verzeichnisstruktur suchen und erweitern.
3. Klicken Sie auf Sichern. Im Fenster Task-Liste für die Sicherung wird der Verarbeitungsstatus der Sicherung angezeigt. Das Fenster 'Sicherungsbericht' zeigt einen ausführlichen Statusbericht an.

Ergebnisse

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeZum Ausführen einer statischen Imagesicherung wählen Sie **Imagesicherung** in der Dropdown-Liste aus.
- Windows-BetriebssystemeZum Ausführen einer Offline-Imagesicherung wählen Sie **Imagesicherung** in der Dropdown-Liste aus.

- Windows-BetriebssystemeZum Ausführen einer Online-Imagesicherung wählen Sie **Momentaufnahmeimagesicherung** in der Dropdown-Liste aus.
- AIX-BetriebssystemeLinux-Betriebssysteme*Nur* für AIX- und Linux-Clients: Zum Ausführen einer Momentaufnahmeimagesicherung verwenden Sie die Option snapshotproviderimage.
- Zum Ausführen einer Imageteilsicherung nach Datum wählen Sie **Imageteilsicherung (nur Datum)** in der Dropdown-Liste aus.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDie folgenden Hinweise sind zu beachten, wenn Sie eine momentaufnahmebasierte Imagesicherung ausführen:

Windows-BetriebssystemeDie folgenden Hinweise sind zu beachten, wenn Sie eine Online-Imagesicherung ausführen:

- Um bestimmte Sicherungsoptionen zu ändern, klicken Sie auf die Schaltfläche Optionen. Die ausgewählten Optionen sind nur während der aktuellen Sitzung wirksam.
- Windows-BetriebssystemeDa bei Imagesicherungen nur die belegten Blöcke in einem Dateisystem gesichert werden können, kann die Größe des auf dem IBM Spectrum Protect-Server gespeicherten Image kleiner sein als die Datenträgergröße. Bei Online-Imagesicherungen kann das gespeicherte Image größer als das Dateisystem sein. Ursache dafür ist die Größe der Cachedateien. Um die tatsächliche Größe des gespeicherten Image zu bestimmen, wählen Sie Anzeigen > Dateiinformationen aus. Die tatsächliche Größe des gespeicherten Image wird im Feld 'Gespeicherte Größe' angegeben.

- Um bestimmte Sicherungsoptionen zu ändern, klicken Sie auf die Schaltfläche Optionen. Die ausgewählten Optionen sind nur während der aktuellen Sitzung wirksam.
- Windows-BetriebssystemeDa bei Imagesicherungen nur die belegten Blöcke in einem Dateisystem gesichert werden können, kann die Größe des auf dem IBM Spectrum Protect-Server gespeicherten Image kleiner sein als die Datenträgergröße. Bei Online-Imagesicherungen kann das gespeicherte Image größer als das Dateisystem sein. Ursache dafür ist die Größe der Cachedateien. Um die tatsächliche Größe des gespeicherten Image zu bestimmen, wählen Sie Anzeigen > Dateiinformationen aus. Die tatsächliche Größe des gespeicherten Image wird im Feld 'Gespeicherte Größe' angegeben.

Linux-BetriebssystemeNur für Linux: Der IBM Spectrum Protect-Client der Version 5.4 (und höher) erkennt keine LVM1-Datenträger für Imageoperationen. Er lässt jedoch zu, dass vorherige Imagesicherungen von LVM1-Datenträgern auf LVM2-Datenträger zurückgeschrieben werden. Tabelle 1 zeigt die Kombinationen, die die alten und neuen Versionen des Clients einbeziehen, die die LVM1- und LVM2-Datenträger für verschiedene Imageoperationen handhaben.

Linux-Betriebssysteme

Tabelle 1. Vergleiche der LVM1- und LVM2-Imageoperationen

			Gemischte Datenträger	
IBM Spectrum Protect-Clientversion	**LVM1-Sicherung und -Zurückschreibung**	**LVM2-Sicherung und -Zurückschreibung**	**Sicherung: LVM1, Zurückschreibung: LVM2**	**Sicherung: LVM2, Zurückschreibung: LVM1**
V5.3 und früher	YES	Nur statisches Image für Dateisystem	NO	NEIN - unformatierte Datenträger werden nicht unterstützt
V5.4 und später	NEIN Fehlernachricht ANS1090E wird angezeigt	YES	JA Datenträger LVM1 muss mit einem früheren Clientgesichert worden sein	NEIN Zurückschreibung auf Datenträger LVM1 schlägt fehl

Zugehörige Verweise:
Snapshotproviderimage
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Imagesicherung über die Befehlszeile ausführen

Imagesicherungs- und -zurückschreibungsoperationen für einen einzelnen Datenträger werden mit dem Befehl backup image bzw. restore image ausgeführt.

Windows-BetriebssystemeSie können die Option snapshotproviderimage im Befehl backup image oder die Option include.image in Ihrer Datei dsm.opt oder in der Befehlszeile verwenden, um anzugeben, ob eine Offline- oder Online-Imagesicherung ausgeführt werden soll.

Verwenden Sie die Option mode im Befehl backup image, um eine Imageteilsicherung nach Datum auszuführen, bei der nur die seit der letzten vollständigen Imagesicherung neu erstellten oder geänderten Dateien gesichert werden. Bei dieser Prozedur werden jedoch nur Dateien mit einem geändertem Datum gesichert, aber keine Dateien mit geänderten Berechtigungen.

Zugehörige Verweise:
Backup Image
Mode
Restore Image
Windows-BetriebssystemeSnapshotproviderimage
AIX-Betriebssysteme

Momentaufnahmebasierte Dateisicherung und -archivierung und momentaufnahmebasierte Imagesicherung

Für Clients für Sichern/Archivieren, die als Rootbenutzer auf JFS2-Dateisystemen unter AIX 5.3 oder höher ausgeführt werden, werden standardmäßig momentaufnahmebasierte Imagesicherungen mithilfe von Momentaufnahmen erstellt.

Informationen zu diesem Vorgang

Wahlweise können Sie momentaufnahmebasierte Sicherungs- und Archivierungsoperationen auf Dateiebene aktivieren, indem Sie die Option snapshotproviderfs angeben. Falls aus irgendeinem Grund keine Momentaufnahme erstellt werden kann, versucht der Client, eine statische Imagesicherung oder eine normale Dateisicherung auszuführen.

Um eine momentaufnahmebasierte Dateisicherung und -archivierung anzugeben, setzen Sie die Option snapshotproviderfs auf JFS2. Dies ist auf alle JFS2-Dateisysteme für diesen Client anwendbar.

Wichtig: Verwenden Sie die momentaufnahmebasierte Dateisicherung und -archivierung und die momentaufnahmebasierte Imagesicherung für alle Ihre JFS2-Dateisysteme unter AIX.

Beispiel: Geben Sie Folgendes in die Serverzeilengruppe in der Datei dsm.sys ein, um die momentaufnahmebasierte Dateisicherung und -archivierung für alle JFS2-Dateisysteme auf dem Client *einzuschalten*:

```
snapshotproviderfs JFS2
```

Geben Sie Folgendes in die Serverzeilengruppe in der Datei dsm.sys ein, um die momentaufnahmebasierte Dateisicherung und -archivierung für alle JFS2-Dateisysteme auf dem Client explizit *auszuschalten*:

```
snapshotproviderfs   NONE
```

Geben Sie Folgendes in die Serverzeilengruppe in der Datei dsm.sys ein, um die momentaufnahmebasierte Dateisicherung und -archivierung für ein bestimmtes JFS2-Dateisystem auf dem Client *einzuschalten*:

```
snapshotproviderfs   NONE

     include.fs   /kalafs1   snapshotproviderfs=JFS2
```

Geben Sie Folgendes in die Serverzeilengruppe in der Datei dsm.sys ein, um die momentaufnahmebasierte Dateisicherung und -archivierung für ein bestimmtes JFS2-Dateisystem auf dem Client *auszuschalten*:

```
snapshotproviderfs   JFS2

     include.fs    /kalafs2    snapshotproviderfs=NONE
```

Geben Sie Folgendes in der Befehlszeile ein, um die momentaufnahmebasierte Dateisicherung und -archivierung nur für eine bestimmte Operation auf dem Client *einzuschalten*:

```
dsmc incr   -snapshotproviderfs=JFS2  /kalafs1
```

Geben Sie Folgendes in der Befehlszeile ein, um die momentaufnahmebasierte Dateisicherung und -archivierung nur für eine bestimmte Operation auf dem Client *auszuschalten*:

```
 snapshotproviderfs   JFS2
```

Führen Sie dann den Sicherungsbefehl aus. Zum Beispiel:

```
 dsmc incr -snapshotproviderfs=NONE /kalafs2
```

Zugehörige Verweise:
Snapshotproviderfs
Linux-Betriebssysteme

Btrfs-Dateisysteme schützen

Btrfs-Dateisysteme können als Dateispezifikationen für Sicherungs- und Zurückschreibungsbefehle, Archivierungs- und Abrufbefehle und in den Befehlen backup image und restore image angegeben werden. Außerdem können Sie Btrfs-Unterdatenträger als Dateispezifikation in den Sicherungs- und Zurückschreibungsfunktionen und in den Archivierungs- und Abruffunktionen angeben. Die Imagesicherungs- oder Imagezurückschreibungsbefehle des Clients für Sichern/Archivieren können Sie für einen Btrfs-Unterdatenträger nicht verwenden.

Btrfs-Dateisysteme werden unter SLES 11 SP2 oder höher, unter IBM®System x, System p und System z unterstützt.

Wenn Sie eine statische Imagesicherung des gesamten Btrfs-Dateisystems erstellen wollen, müssen Sie alle Unterdatenträger abhängen, damit der Client für Sichern/Archivieren das Btrfs-Dateisystem während des Sicherungsprozesses ab- oder anhängen kann. Sie können die

Anforderungen für das An- und Abhängen vermeiden, wenn Sie anstelle einer statischen Imagesicherung eine momentaufnahmebasierte Imagesicherung des Btrfs-Dateisystems ausführen.

Die Imagesicherungs- und Imagezurückschreibungsfunktionalität steht für Btrfs-Unterdatenträger nicht zur Verfügung. Wenn Sie versuchen, einen Unterdatenträger mit dem Befehl image backup zu sichern, wird die folgende Nachricht angezeigt:

```
ANS1162E Dateisystem konnte nicht angehängt werden
```

Sie können einen Btrfs-Unterdatenträger entweder mithilfe des Unterdatenträgernamens oder der Unterdatenträger-ID anhängen.

Auf Btrfs-Dateisystemen kann die Journalsicherung sowohl auf Dateisystemebene als auch auf Unterdatenträgerebene ausgeführt werden. Wenn Sie die journalbasierte Sicherung für ein Btrfs-Dateisystem ausführen, gilt das erstellte Journal für das gesamte Dateisystem; es gibt kein separates Journal für jeden Unterdatenträger.

Einschränkung: Auf Linux-Systemen verwenden einige Dateisysteme (z. B. ext2, ext3, ext4, btrfs und xfs) eine UUID (Universally Unique Identifier), um sich selbst im Betriebssystem zu identifizieren. Wenn Sie eine Imagesicherung eines solchen Datenträgers erstellen und an eine andere Position zurückschreiben, kann es sein, dass es zwei Datenträger mit derselben UUID gibt. Wenn Sie Ihre Dateisysteme mit einer UUID in /etc/fstab definieren, denken Sie daran, dass der Client für Sichern/Archivieren das zurückgeschriebene Dateisystem unter Umständen wegen eines UUID-Konflikts nicht korrekt anhängen kann. Um diese Situation zu vermeiden, sollten Sie das Image an seine ursprüngliche Position zurückschreiben. Wenn Sie es an eine andere Position zurückschreiben müssen, ändern Sie die UUID des ursprünglichen oder des zurückgeschriebenen Datenträgers, bevor Sie das zurückgeschriebene Dateisystem anhängen. Informationen zur Änderung einer UUID finden Sie in der Linux-Dokumentation. Möglicherweise müssen Sie auch die Datei /etc/fstab manuell bearbeiten, damit der ursprüngliche Datenträger und/oder der zurückgeschriebene Datenträger angehängt werden können.

- Linux-BetriebssystemeBtrfs-Dateisysteme sichern und zurückschreiben
  Sie können Btrfs-Dateisysteme mit den Befehlen incremental, selective, restore, archive und retrieve des Clients für Sichern/Archivieren sichern, zurückschreiben, archivieren und abrufen.
- Linux-BetriebssystemeBtrfs-Unterdatenträger sichern und zurückschreiben
  Sie können Btrfs-Unterdatenträger mit den Befehlen incremental, selective, restore, archive und retrieve des Clients für Sichern/Archivieren sichern, zurückschreiben, archivieren und abrufen.

Linux-Betriebssysteme

Btrfs-Dateisysteme sichern und zurückschreiben

Sie können Btrfs-Dateisysteme mit den Befehlen incremental, selective, restore, archive und retrieve des Clients für Sichern/Archivieren sichern, zurückschreiben, archivieren und abrufen.

Informationen zu diesem Vorgang

Beim Sichern eines Btrfs-Dateisystems mit einer Version des Clients für Sichern/Archivieren vor Version 7.1 wurde der Dateisystemtyp in der GUI und Befehlsausgabe des IBM Spectrum Protect-Servers als `Unbekannt` aufgelistet. Der Dateisystemtyp `Unbekannt` wird angezeigt, weil Btrfs-Dateisysteme vor IBM Spectrum Protect Version 7.1 offiziell nicht unterstützt wurden. Wenn Sie dasselbe Btrfs-Dateisystem mit einem Client für Sichern/Archivieren der Version 7.1 (oder höher) sichern, werden alle Dateien, die über Zugriffssteuerungslisten (ACLs) und erweiterte Attribute (XATTRs) verfügen, selbst dann erneut gesichert, wenn sich ihr Inhalt seit der letzten Sicherung, die mit der früheren Clientversion erstellt wurde, nicht geändert hat. Außerdem wird nach der Sicherung eines Btrfs-Dateisystems mit dem Client der Version 7.1 (oder höher) der Dateisystemtyp in der GUI und Befehlsausgabe des IBM Spectrum Protect-Servers korrekt als `Btrfs` angezeigt.

Auch bei einem Client der Version 7.1 oder höher kann es dazu kommen, dass eine Datei in der nächsten Sicherungsoperation enthalten ist, wenn die Datei in einem Btrfs-Dateisystem kopiert wird. Wenn Sie eine Datei beispielsweise mit dem Befehl cp und der Option -p oder -preserve (Modus, Eigentumsrecht und Zeitmarken beibehalten) kopieren und wenn sich die Attribute der Datei ändern, wird das erweiterte Attribut für die Zugriffs-ACL (system.posix_acl_access) geändert. Da sich ein erweitertes Attribut ändert, sichert der Client die gesamte Datei und aktualisiert nicht nur die Attribute für die Datei.

Vorgehensweise

1. Hängen Sie das Dateisystem an, das Sie schützen oder wiederherstellen wollen. Das folgende Beispiel zeigt die Syntax zum Anhängen eines Dateisystems: `mount /dev/sdb1 on /btreefs1 type btrfs (rw)`
2. Führen Sie eine der folgenden Operationen aus, um das Dateisystem zu schützen oder wiederherzustellen:

Operation	Befehl
Dateisystem sichern	`dsmc incr /btreefs1`
Dateisystem zurückschreiben	`dsmc restore /btreefs1/ -subdir=yes -replace=yes`
Dateisystem archivieren	`dsmc archive /btreefs1/ -subdir=yes`

Operation	Befehl
Dateisystem abrufen	`dsmc retrieve /btreefs1/ -subdir=yes -replace=yes`

Dateisystemmomentaufnahme sichern	Erstellen Sie die Dateisystemmomentaufnahme. Verwenden Sie den Befehl btrfs subvolume snapshot. In diesem Beispiel wird das Verzeichnis btreefs1_snap in dem Dateisystem /btreefs1 als Momentaufnahmeverzeichnis angegeben.
	`btrfs subvolume snapshot /btreefs1/ /btreefs1/btreefs1_snap`
	Geben Sie den Befehl incremental des Clients für Sichern/Archivieren aus. Geben Sie die Option snapshotroot und die Position der Btrfs-Momentaufnahme an.
	`$DSM_DIR/dsmc incr /btreefs1 -snapshotroot=/btreefs1/btreefs1_snap`

Imagesicherung ausführen	Bevor Sie eine Imagesicherung erstellen, müssen alle Unterdatenträger abgehängt werden.
	`dsmc backup image /btreefs1 -snapshotproviderimage=none`
	Um zu vermeiden, dass die Unterdatenträger abgehängt werden müssen, erstellen Sie eine momentaufnahmebasierte Imagesicherung.
	`dsmc backup image /btreefs1`

Imagesicherung zurückschreiben	Bevor Sie eine Imagesicherung zurückschreiben, müssen alle Unterdatenträger abgehängt werden. `dsmc restore image /btreefs1`

Linux-Betriebssysteme

Btrfs-Unterdatenträger sichern und zurückschreiben

Sie können Btrfs-Unterdatenträger mit den Befehlen incremental, selective, restore, archive und retrieve des Clients für Sichern/Archivieren sichern, zurückschreiben, archivieren und abrufen.

Vorgehensweise

1. Listen Sie die Unterdatenträger auf und ermitteln Sie ihre IDs.

```
btrfs subvolume list /btreefs1
 ID 256 top level 5 path @
 ID 262 top level 5 path @/btreefs1_sub1
```

2. Erstellen Sie das Verzeichnis, das als Mountpunkt für den Unterdatenträger verwendet werden soll.

```
mkdir /btreefs1_sub1
```

3. Hängen Sie den Unterdatenträger an. Verwenden Sie beispielsweise die folgende Syntax, um den Unterdatenträger auf der Einheit sdb1 bei /btreefs1_sub1 anzuhängen: `mount -t btrfs -o subvolid=262 /dev/sdb1 /btreefs1_sub1`

   Führen Sie eine oder mehrere der folgenden Operationen aus, um den Unterdatenträger zu schützen bzw. wiederherzustellen:

Operation	Befehl

Unterdatenträger sichern	Sowohl Teilsicherungen als auch selektive Sicherungen werden unterstützt.
	`dsmc incr /btreefs1_sub1`
	`dsmc sel /btreefs1_sub1/ -subdir=yes`

Unterdatenträger zurückschreiben	`dsmc restore /btreefs1_sub1/ -subdir=yes -replace=yes`
Unterdatenträger archivieren	`dsmc archive /btreefs1_sub1/ -subdir=yes`
Unterdatenträger abrufen	`dsmc retrieve /btreefs1_sub1/ -subdir=yes -replace=yes`

Operation	Befehl

Momentaufnahme eines Btrfs-Unterdatenträgers sichern	Erstellen Sie die Unterdatenträgermomentaufnahme. Verwenden Sie den Befehl btrfs subvolume snapshot. In diesem Beispiel wird das Verzeichnis /btreefs1/btreefs1_sub1_snap für den Unterdatenträger mit dem Namen btreefs1_sub1 als Momentaufnahmeverzeichnis angegeben.
	`btrfs subvolume snapshot`
	`/btreefs1/btreefs1_sub1`
	`/btreefs1/btreefs1_sub1_snap`
	
	Geben Sie den Befehl incremental des Clients für Sichern/Archivieren aus. Geben Sie die Option snapshotroot und die Position der Btrfs-Momentaufnahme an.
	`dsmc incr /btreefs1_sub1`
	`-snapshotroot=/btreefs1`
	`/btreefs1_sub1_snap`

 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

NAS-Dateisysteme mit Network Data Management Protocol sichern

Windows-, AIX- und Solaris-Clients für Sichern/Archivieren können Network Data Management Protocol (NDMP) verwenden, um NAS-Dateisystemimages (NAS = Network Attached Storage) effizient zu sichern und zurückzuschreiben. Die Dateisystemimages können auf automatisierten Bandlaufwerken oder Speicherarchiven, die lokal an Network Appliance- oder EMC Celerra-NAS-Dateiserver angeschlossen sind, oder auf Bandlaufwerken oder Speicherarchiven, die lokal an einen IBM Spectrum Protect-Server angeschlossen sind, gesichert und von diesen zurückgeschrieben werden.

NDMP-Unterstützung ist nur für IBM Spectrum Protect Extended Edition verfügbar.

Für Linux x86_64-Clients können auch Teilsicherungen verwendet werden, um NAS-Dateisysteme zu sichern. Weitere Informationen finden Sie in der Beschreibung des Befehls incremental und der Optionen snapshotroot, snapdiff, createnewbase und diffsnapshot.

Nach der Konfiguration der NDMP-Unterstützung stellt der Server eine Verbindung zu der NAS-Einheit her und verwendet NDMP, um jede Sicherungs- und Zurückschreibungsoperation einzuleiten, zu steuern und zu überwachen. Die NAS-Einheit führt die externe Datenübertragung zu und von dem NAS-Dateisystem zu einem lokal angeschlossenen Speicherarchiv durch.

Für NAS-Einheiten, die NDMP Version 4 unterstützen, ist die Datenübertragung vom Dateiserver zum Server verfügbar.

Zu den Vorteilen von Sicherungen mit NDMP gehören:

- LAN-unabhängige Datenübertragung.
- Hochleistungsfähige und skalierbare Sicherungen und Zurückschreibungen.
- Sicherung auf lokale Bandeinheiten ohne Datenaustausch auf dem Netz.

Die folgende Unterstützung wird zur Verfügung gestellt:

- Vollständige Dateisystemimagesicherung aller Dateien innerhalb eines NAS-Dateisystems.
- Differenzdateisystemimagesicherung aller Dateien, die sich seit der letzten vollständigen Imagesicherung geändert haben.
- Parallele Sicherungs- und Zurückschreibungsoperationen bei der Verarbeitung mehrerer NAS-Dateisysteme.
- Auswahl von Schnittstellen zum Einleiten, Überwachen oder Abbrechen von Sicherungs- und Zurückschreibungsoperationen:
  - Web-Client (nur für Verbindungen zu Servern mit IBM Spectrum Protect Version 8.1.1, 8.1.0, 7.1.7 oder einer früheren Version)
  - Befehlsschnittstelle des Clients für Sichern/Archivieren (nur für Verbindungen zu Servern mit IBM Spectrum Protect Version 8.1.1, 8.1.0, 7.1.7 oder einer früheren Version)
  - Befehlszeilenschnittstelle des Verwaltungsclients (Sicherungs- und Zurückschreibungsoperationen können mit dem Verwaltungsbefehlsscheduler geplant werden)
  - Web-Client für Verwaltung

Die folgenden Funktionen werden *nicht* unterstützt:

- Archivieren und Abrufen
- Clientzeitplanung. Verwenden Sie Serverbefehle zum Planen einer NAS-Sicherung.
- Erkennung von beschädigten Dateien.
- Datenübertragungsoperationen für NAS-Daten, die von IBM Spectrum Protect gespeichert werden:
  - Umlagerung
  - Wiederherstellung
  - Export
  - Generierung von Sicherungssätzen

-  AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-BetriebssystemeNAS-Dateisysteme mit der Web-Client-GUI unter Verwendung des NDMP-Protokolls sichern
  Sowohl für die Web-Client-GUI als auch für die Clientbefehlszeilenschnittstelle müssen Sie passwordaccess=generate angeben (dies ist eine aktuelle Web-Client-Einschränkung für den Clientknoten) und set authentication=on muss auf dem Server angegeben werden.

- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeNAS-Dateisysteme über die Befehlszeile sichern
  Sie können die Befehlszeile verwenden, um NAS-Dateisystemimages zu sichern.
- Windows-BetriebssystemeMethoden zum Sichern und Wiederherstellen von Daten auf NAS-Dateiservern bei Zugriff mit dem CIFS-Protokoll
  Der Client für Sichern/Archivieren kann NAS-Dateiserverdaten (NAS = Network-attached Storage) verarbeiten, auf die mithilfe des CIFS-Protokolls (CIFS = Common Internet File System) zugegriffen wird.

Zugehörige Konzepte:
Voraussetzungen für NDMP-Unterstützung (nur Extended Edition)
Zugehörige Verweise:
Diffsnapshot
Incremental
Snapdiff
Snapshotroot
AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

NAS-Dateisysteme mit der Web-Client-GUI unter Verwendung des NDMP-Protokolls sichern

Sowohl für die Web-Client-GUI als auch für die Clientbefehlszeilenschnittstelle müssen Sie passwordaccess=generate angeben (dies ist eine aktuelle Web-Client-Einschränkung für den Clientknoten) und set authentication=on muss auf dem Server angegeben werden.

Sie werden immer zur Eingabe einer Benutzer-ID und eines Kennworts aufgefordert. Um NAS-Knoten anzuzeigen und NAS-Funktionen auszuführen, müssen Sie eine berechtigte Verwaltungsbenutzer-ID und das Kennwort eingeben. Die berechtigte Verwaltungsbenutzer-ID sollte mindestens die Clienteignerberechtigung sowohl über den NAS-Knoten als auch den Client-Workstationknoten besitzen, der entweder von der Befehlszeile oder vom Web aus verwendet wird.

Sie können die Option toc zusammen mit der Option include.fs.nas in der Clientoptionsdatei verwenden, um anzugeben, ob der Client für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Wenn Sie TOC-Informationen speichern, können Sie den Windows-Web-Client verwenden, um die gesamte Baumstruktur des Dateisystems zu überprüfen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen. Die Erstellung eines Inhaltsverzeichnisses erfordert, dass Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsimage gebunden wird. Beachten Sie, dass die TOC-Erstellung während der Sicherungsoperation eine zusätzliche Verarbeitung, zusätzliche Netzressourcen, zusätzlichen Speicherpoolspeicher und möglicherweise einen zusätzlichen Mountpunkt erfordert.

Die Web-Client-Schnittstelle ist nur für Verbindungen zu einem Server mit IBM Spectrum Protect Version 8.1.1, 8.1.0, 7.1.7 oder einer früheren Version verfügbar.

Gehen Sie wie folgt vor, um NAS-Dateisysteme mit der grafischen Benutzerschnittstelle des Web-Clients zu sichern:

1. Klicken Sie auf Sichern im Hauptfenster. Das Fenster Sichern wird angezeigt.
2. Falls erforderlich, erweitern Sie die Verzeichnisbaumstruktur.
   Anmerkung:
   a. Der Anfangsknoten mit dem Namen Knoten ist nicht auswählbar. Dieser Knoten wird nur angezeigt, wenn ein NAS-Plug-in auf der Client-Workstation vorhanden ist.
   b. NAS-Knoten werden auf derselben Stufe wie der Knoten der Client-Workstation angezeigt. Es werden nur Knoten angezeigt, für die der Administrator berechtigt ist.
   c. Sie können NAS-Knoten erweitern, um Dateibereiche offen zu legen, aber eine darüber hinaus gehende Erweiterung ist nicht verfügbar (keine Dateinamen).
3. Klicken Sie auf die Auswahlfelder neben den Knoten oder den Dateisystemen, die Sie sichern wollen.
4. Klicken Sie im Pulldown-Menü für die Sicherungsart die Art der Sicherung an, die ausgeführt werden soll. Die Liste 'NAS-Sicherungsart' ist nur aktiv, wenn Sie zuerst NAS-Sicherungsobjekte auswählen. Bei einer Gesamtsicherung wird das gesamte Dateisystem gesichert. Bei einer Differenzsicherung werden die Änderungen seit der jüngsten Gesamtsicherung gesichert.
5. Klicken Sie auf Sichern. Im Fenster Task-Liste für die NAS-Sicherung werden der Verarbeitungsstatus der Sicherung und die Statusleiste angezeigt. Die Zahl neben der Statusleiste gibt die Anzahl Byte an, die bisher gesichert wurden. Nachdem die Sicherung beendet ist, zeigt das Fenster mit dem NAS-Sicherungsbericht Verarbeitungsdetails einschließlich der tatsächlichen Größe der Sicherung und der Summe der gesicherten Byte an.
   Anmerkung: Ist es erforderlich, die Web-Browser-Sitzung zu schließen, werden aktuelle NAS-Operationen nach der Trennung der Verbindung fortgesetzt. Sie können die Schaltfläche Verlassen im Fenster Task-Liste für die NAS-Sicherung verwenden, um die Verarbeitungsüberwachung zu verlassen, ohne die aktuelle Operation zu beenden.
6. (Optional) Um die Verarbeitung einer Operation vom Hauptfenster der grafischen Benutzerschnittstelle aus zu überwachen, öffnen Sie das Menü Aktionen und wählen Sie IBM Spectrum Protect-Aktivitäten aus. Während einer Sicherung zeigt die Statusleiste den Verarbeitungsstatus an. Eine prozentuale Schätzung wird für Differenzsicherungen nicht angezeigt.

Die folgenden Hinweise sind zu beachten, wenn Sie NAS-Dateisysteme mit der Web-Client-GUI sichern:

- Workstationsicherungen und ferne Sicherungen (NAS-Sicherungen) schließen sich in einem Sicherungsfenster gegenseitig aus. Wenn ein Element für die Sicherung ausgewählt wurde, muss das nächste Element, das Sie auswählen, denselben Typ aufweisen (entweder NAS oder Nicht-NAS).

- Für NAS-Knoten oder Dateisysteme werden keine Details auf der rechten Seite des Fensters Sichern angezeigt. Um Informationen zu Objekten in einem NAS-Knoten anzuzeigen, heben Sie das Objekt hervor und wählen Sie Anzeigen > Dateiinformationen im Menü aus.
- Um NAS-Dateibereiche zu löschen, wählen Sie Dienstprogramme > Dateibereiche löschen aus.
- Die Sicherungsoptionen gelten nicht für NAS-Dateibereiche und werden während einer NAS-Sicherungsoperation ignoriert.

Zugehörige Konzepte:
Übersicht über die Konfiguration des Web-Clients
NAS-Dateisysteme zurückschreiben
Zugehörige Verweise:
Toc
 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

NAS-Dateisysteme über die Befehlszeile sichern

Sie können die Befehlszeile verwenden, um NAS-Dateisystemimages zu sichern.

Sie können den Befehlszeilenclient nur verwenden, wenn Sie eine Verbindung zu einem Server mit IBM Spectrum Protect Version 8.1.1, 8.1.0, 7.1.7 oder einer früheren Version herstellen. Für Server mit IBM Spectrum Protect Version 8.1.2 oder höher verwenden Sie Serverbefehle im Verwaltungsbefehlszeilenclient (dsmadmc).

In Tabelle 1 sind die Befehle und Optionen aufgelistet, die Sie zum Sichern von NAS-Dateisystemimages über die Befehlszeile verwenden können.

Tabelle 1. NAS-Optionen und -Befehle

Option oder Befehl	Definition	Seite
domain.nas	Mit der Option domain.nas geben Sie die Datenträger an, die für NAS-Sicherungen in Ihre Standarddomäne einbezogen werden sollen.	Domain.nas
exclude.fs.nas	Mit der Option exclude.fs.nas schließen Sie Dateisysteme auf dem NAS-Dateiserver von einer Imagesicherung aus, wenn sie zusammen mit dem Befehl backup nas verwendet wird.  AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist *nur* für AIX- und Solaris-Clients gültig.  Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.	Ausschlussoptionen
include.fs.nas	Verwenden Sie die Option include.fs.nas, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Sie können auch angeben, ob während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) unter Verwendung der Option ***toc*** mit der Option include.fs.nas in Ihrer Clientoptionsdatei gespeichert werden.  AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist *nur* für AIX- und Solaris-Clients gültig.  Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.	Einschlussoptionen
query node	Mit dem Befehl query node können Sie alle Knoten anzeigen, für die eine bestimmte Verwaltungsbenutzer-ID die Berechtigung zum Ausführen von Operationen hat. Die Verwaltungsbenutzer-ID sollte mindestens die Clienteignerberechtigung sowohl über den NAS-Knoten als auch den Client-Workstationknoten, die verwendet werden, besitzen.	Query Node
backup nas	Mit dem Befehl backup nas können Sie eine Imagesicherung eines oder mehrerer Dateisysteme, die zu einem NAS-Dateiserver gehören, erstellen.	Backup NAS
toc	Verwenden Sie die Option toc im Befehl backup nas oder mit der Option include.fs.nas, um anzugeben, ob für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) gespeichert werden.	Toc

Option oder Befehl	Definition	Seite
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme monitor process	Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeMit dem Befehl monitor process können Sie aktuelle Sicherungs- und Zurückschreibungsprozesse für alle NAS-Knoten anzeigen, für die ein Benutzer mit Verwaltungsaufgaben berechtigt ist. Der Benutzer mit Verwaltungsaufgaben kann dann einen Prozess für die Überwachung auswählen.	Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme Monitor Process
cancel process	Mit dem Befehl cancel process können Sie aktuelle Sicherungs- und Zurückschreibungsprozesse für alle NAS-Knoten anzeigen, für die ein Benutzer mit Verwaltungsaufgaben berechtigt ist. In der Anzeige kann der Benutzer mit Verwaltungsaufgaben einen Prozess zum Abbrechen auswählen.	Cancel Process
query backup	Verwenden Sie den Befehl query backup mit der Option class, um Informationen zu den Dateisystemimages anzuzeigen, die für einen NAS-Dateiserver gesichert wurden.	Query Backup
query filespace	Verwenden Sie den Befehl query filespace mit der Option class, um eine Liste der Dateibereiche anzuzeigen, die zu einem NAS-Knoten gehören.	Query Filespace
delete filespace	Verwenden Sie den Befehl delete filespace mit der Option class, um eine Liste der Dateibereiche anzuzeigen, die zu einem NAS-Knoten gehören. In dieser Liste können Sie einen Dateibereich zum Löschen auswählen.	Delete Filespace

Windows-BetriebssystemeFür eine NAS-Dateisystemspezifikation werden folgende Konventionen verwendet:

- NAS-Knoten stellen eine neue Knotenart dar. Der Name des NAS-Knotens identifiziert einen NAS-Dateiserver und seine Daten eindeutig für IBM Spectrum Protect. Sie können den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Include-Anweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, gilt das angegebene Dateisystem für alle NAS-Dateiserver.
- Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: `/vol/vol0`.
- Windows-BetriebssystemeFür NAS-Dateisystembezeichnungen in der Befehlszeile müssen geschweifte Klammern `{}` als Begrenzer um Dateinamen verwendet werden, beispielsweise `{/vol/vol0}`. Verwenden Sie keine geschweiften Klammern als Begrenzer in der Optionsdatei.

Anmerkung: Wird eine NAS-Sicherungsoperation mithilfe der Befehlszeilenschnittstelle des Clients, der Client-GUI oder des Web-Clients eingeleitet, startet der Server einen Prozess, um die Operation einzuleiten, zu steuern und zu überwachen. Der Fortschritt in der Befehlszeilenschnittstelle des Clients lässt sich erst nach kurzer Zeit feststellen, da der Server eine Ladeoperation und andere erforderliche Tasks ausführen muss, bevor die Datenversetzung erfolgt.

Zugehörige Verweise:
Toc
Windows-Betriebssysteme

Methoden zum Sichern und Wiederherstellen von Daten auf NAS-Dateiservern bei Zugriff mit dem CIFS-Protokoll

Der Client für Sichern/Archivieren kann NAS-Dateiserverdaten (NAS = Network-attached Storage) verarbeiten, auf die mithilfe des CIFS-Protokolls (CIFS = Common Internet File System) zugegriffen wird.

Sie können folgende Methoden zum Sichern und Wiederherstellen von Daten auf NAS-Einheiten verwenden:

- Verwenden Sie den Client für Sichern/Archivieren zum Sichern und Zurückschreiben von Daten, indem mithilfe von CIFS vom Client für Sichern/Archivieren auf Dateien zugegriffen wird. Die Daten können auf dem IBM Spectrum Protect-Server unter Verwendung der fortlaufenden Teilsicherungsmethode mit Unterteilung nach Dateiebene gespeichert werden. Die Daten werden in der IBM Spectrum Protect-Speicherhierarchie gespeichert und können umgelagert, wiederhergestellt oder in einem Kopienspeicherpool gesichert werden.

  Diese Methode erhöht die Prozessorauslastung, wenn der Client auf einzelne Dateien zugreift. Die Methode erfordert den Fluss der Daten durch den Client. Außerdem erfordert diese Methode den Fluss der Daten durch den IBM Spectrum Protect-Server, wenn keine LAN-unabhängige Konfiguration verwendet wird.

- Verwenden Sie die Option snapdiff, um die Leistungsprobleme bei CIFS-Sicherungen abzuschwächen. Diese Option speichert Daten unter Verwendung fortlaufender Teilsicherung mit Unterteilung nach Dateiebene für CIFS.
- Verwenden Sie einen Client für Sichern/Archivieren, der auf der NAS-Einheit ausgeführt wird, wenn das NAS-Betriebssystem die Verwendung externer Programme zulässt.

Bei dieser Methode wird die Prozessorauslastung durch CIFS verringert. Daten können auf dem IBM Spectrum Protect-Server unter Verwendung fortlaufender Teilsicherung mit Unterteilung nach Dateiebene gespeichert werden. Die Daten werden in der IBM Spectrum Protect-Speicherhierarchie gespeichert und können umgelagert, wiederhergestellt oder in einem Kopienspeicherpool gesichert werden. Diese Methode erfordert den Fluss des Daten durch den Client für Sichern/Archivieren. Außerdem erfordert diese Methode den Fluss der Daten über ein Netz und durch den IBM Spectrum Protect-Server, wenn keine LAN-unabhängige Konfiguration verwendet wird.

- Verwenden Sie NDMP mit dem Client für Sichern/Archivieren. Dateisysteme werden als vollständige Images (alle Dateien) oder als Differenzimages (alle Dateien, die sich seit der letzten Gesamtsicherung geändert haben) gesichert. Gesicherte Images werden auf einer Bandeinheit gespeichert, auf die vom NAS-Dateiserver aus zugegriffen wird. Diese Methode bietet eine hohe Leistung, da es keinen Datenfluss durch einen Client für Sichern/Archivieren oder einen IBM Spectrum Protect-Server gibt. Daten, die mit NDMP auf dem Server gesichert werden, können nicht in einen Kopienspeicherpool umgelagert, konsolidiert oder gesichert werden.

Für NAS-Dateiserverdaten bestehen die folgenden Einschränkungen, wenn mit CIFS auf die Daten zugegriffen wird:

- Der Zugriff auf Sicherheitsinformationen für Dateien und Verzeichnisse ist unter Umständen nicht möglich, wenn das Windows-Konto, das die Sicherung ausführt, nicht zur Gruppe 'Domänen-Admins' der Domäne gehört, in der der NAS-Dateiserver ein anerkanntes Mitglied ist. Es ist auch möglich, dass diese Sicherheitszugriffsfehler verhindern könnten, dass die gesamte Datei bzw. das gesamte Verzeichnis gesichert wird.
- Es kommt zu Leistungseinbußen, da über Fernzugriff auf Daten zugegriffen wird.
- Die zugeordneten Laufwerke sehen für den Client wie NTFS-Dateisysteme aus; sie verfügen jedoch möglicherweise nicht über die vollständige NTFS-Funktionalität. Ein Beispiel: Das Verschlüsselungsattribut einer Datei ist gesetzt. Wenn der Client die Datei sichert, schlägt die Sicherung jedoch fehl, da die Verschlüsselungseinstellung auf Datenträgerebene angibt, dass keine Verschlüsselung für den Datenträger verwendet werden kann. ReFS-Dateisysteme sehen für den Client ebenfalls wie NTFS-Dateisysteme aus.
  Tipp: Verwenden Sie NDMP mit dem Client für Sichern/Archivieren auf einem NAS-Dateiserver, um die Datenträger zu sichern und zurückzuschreiben, anstatt die Datenträger über ferne zugeordnete Laufwerke zu sichern und zurückzuschreiben.

Zugehörige Verweise:
Snapdiff
Windows-Betriebssysteme

Unterstützung für CDP Persistent Storage Manager

Persistent Storage Manager (PSM) ist die Momentaufnahmetechnologie, die in einer Reihe von NAS-Boxes, die auf Microsoft Server Appliance Kit basieren, enthalten ist, einschließlich IBM® TotalStorage NAS 200, 300 und 300G.

Mithilfe des Clients für Sichern/Archivieren können Sie die von PSM generierten konstanten Image (PI = Persistent Image) eines Datenträgers sichern. Zuerst müssen Sie sicherstellen, dass der Datenträger einen Kennsatz hat. Dann können Sie mithilfe von PSM ein konstantes Image mit einem bestimmten Imagenamen (wie beispielsweise `snapshot.daily`) planen oder erstellen und die Anzahl der zu sichernden Images auf 1 setzen. PSM überschreibt das konstante Image wie erforderlich und Sie können das konstante Image mit dem Client in Teilsicherungen sichern. In diesem Fall sichert der Client nur die Dateien, die sich zwischen Momentaufnahmen geändert haben. Ein Vorteil des Sicherns eines konstanten PSM-Image anstelle des tatsächlichen Datenträgers besteht darin, dass in dem konstanten Image keine offenen Dateien vorhanden sind.

Beachten Sie die folgenden Hinweise, bevor Sie Persistent Storage Manager verwenden:

- Standardmäßig verwendet ein PSM-Zeitplan einen variablen Namen (*snapshot.%i*) und bewahrt eine Reihe von Images auf.
  Wichtig: Verwenden Sie den Client nicht auf diese Art und Weise mit PSM. Der Client betrachtet jedes Image als eindeutig und erstellt eine vollständige Kopie jedes Image.
- Der Client erfordert, dass der Datenträger, der zum Erstellen des konstanten Image verwendet wird, über einen Kennsatz verfügt. Wenn der Datenträger keinen Kennsatz hat, sichert der Client das konstante Image nicht.
- Sie verwenden die Imagesicherungsfunktion zum Sichern des ursprünglichen Datenträgers, der zum Erstellen des konstanten Image verwendet wird. Sie können die Imagesicherungsfunktion jedoch nicht zum Sichern des PI verwenden.
- Fügen Sie folgende Einträge in Ihrer Clientoptionsdatei (dsm.opt) hinzu, wenn Sie vermeiden wollen, dass beim Sichern von PSM nicht benötigte Dateien gesichert werden:

```
exclude.dir "Persistent Storage Manager State"
exclude.file "*.psm"
exclude.file "*.otm"
```

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme

NFS-Dateien sichern

Sie können den Client für Sichern/Archivieren zum Schützen von Dateien konfigurieren, auf die mit dem NFS-Protokoll (NFS = Network File System) oder dem CIFS-Protokoll (CIFS = Common Internet File System) zugegriffen wird.

Die Sicherungsleistung ist besser, wenn Sie den Client für Sichern/Archivieren an der Position installieren, an der das Dateisystem physisch vorhanden ist. Manchmal ist es jedoch notwendig, zum Sichern oder Wiederherstellen von Daten auf gemeinsam genutzten fernen Laufwerken mithilfe von NFS oder CIFS auf Dateisysteme zuzugreifen. Der Client für Sichern/Archivieren unter AIX-, Linux-, Mac OS X- und Solaris-Betriebssystemen kann Dateidaten auf einem über NFS oder CIFS angehängten gemeinsam genutzten Laufwerk sichern, archivieren,

zurückschreiben und abrufen. Die Operationen sind bei allen Versionen des NFS-Protokolls gültig, einschließlich NFS Version 2, NFS Version 3 und NFS Version 4.

Der Client für Sichern/Archivieren kann Zugriffssteuerungslisten sichern und zurückschreiben, wenn er für die Verwendung von NFS Version 4 konfiguriert ist.

Die folgenden Einschränkungen gelten, wenn der Client für Sichern/Archivieren Daten auf NFS-Datenträgern schützt:

- Clients für Sichern/Archivieren können keine Imagesicherungen von NFS-Datenträgern ausführen.
- Clients für Sichern/Archivieren unter AIX können auf NFS-Datenträgern keine momentaufnahmebasierten Dateisicherungen ausführen oder Dateien archivieren.
- Clients für Sichern/Archivieren können keine journalbasierten Sicherungen von NFS-Datenträgern ausführen.
- Clients für Sichern/Archivieren können möglicherweise keine NetApp-Datenträgermomentaufnahmen sichern, wenn über das NFS-Protokoll auf sie zugegriffen wird. Wenn der NetApp-Dateiserver für seine Datenträgermomentaufnahmen unterschiedliche Einheitenkennungen bereitstellt, werden diese Momentaufnahmen möglicherweise von Sicherungen ausgeschlossen. Das Verhalten ist von der Betriebssystemversion, von der Version des NetApp-Dateiservers und von den Einstellungen abhängig.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeNFS-Dateisysteme mit der globalen Namensbereichsfunktion sichern
  NFS-V4-Clients können NFS-Dateisysteme sichern, die mithilfe der globalen Namensbereichsfunktion (als *Linktechnik* bezeichnet) angehängt wurden. Alle Dateisysteme im globalen Namensbereich werden unter einem einzigen Dateibereich gesichert.

AIX-Betriebssysteme

AIX-Workloadpartitionsdateisysteme sichern

Mit dem Client für Sichern/Archivieren unter AIX können Sie Dateidaten lokaler Partitionen innerhalb der globalen Partition mithilfe des Namensbereichs der lokalen Partition innerhalb der globalen Partition sichern und zurückschreiben.

Jede Workloadpartition (WPAR) verfügt über ihre eigene Sicherheitsdomäne, sodass nur der globale Root einen garantierten Zugriff auf alle Daten hat.

Die Workloadpartitionen sind Partitionen, die innerhalb eines einzelnen AIX-Systemimages vollständig in Software erstellt werden und folgende Attribute aufweisen:

- Normalerweise erscheint die Workloadpartition als vollständiges und eigenständiges AIX-System.
- Es gibt keinen Hardwareassistenten und keine Konfiguration.

Workloadpartitionen stellen eine gesicherte und isolierte Umgebung für Unternehmensanwendungen in Bezug auf Verarbeitung, Signalgebung und Dateisystemspeicherbereich zur Verfügung. Software, die im Kontext einer Workloadpartition ausgeführt wird, erscheint, als ob sie ihre eigene separate Instanz von AIX hätte.

Das folgende Beispiel zeigt eine WPAR-Konfiguration innerhalb der globalen Workloadpartition:

Globale Partition:
    Systemname: `shimla`
    Dateisystem: `/home /opt`
WPAR #1-Konfiguration:
    Name: `wpar1`
    Dateisystem: `/home; Name in globaler WPAR: /wpars/wpar1/home`
WPAR #2-Konfiguration:
    Name: `wpar2`
    Dateisystem: `/data; Name in globaler WPAR: /wpars/wpar2/data`

Es gibt - wie folgt - zwei Arten, WPAR-Daten zu sichern:

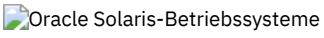
- Alle WPAR-Dateisysteme als Dateibereiche innerhalb der globalen Partition sichern. Mit dem Namen des Dateibereichs muss die Workloadpartition identifiziert werden, zu der der Dateibereich gehört. Alle Daten werden mithilfe eines einzigen Zeitplans auf einem einzigen Knoten verwaltet. Unter Verwendung der Beispielkonfiguration zeigt das folgende Beispiel eine Musterdatei dsm.sys mit einer Serverzeilengruppe für alle Systeme, sowohl global als auch lokal:

  ```
  SErvername  shimla
     TCPPort            1500
     TCPServeraddress   server.example.com
     nodename           shimla
     PasswordAccess     generate
     Domain             /wpars/wpar1/home /wpars/wpar2/data /home /opt
  ```

- Jedes einzelne WPAR-Dateisystem unter einem anderen Knotennamen sichern. Bei dieser Methode wird für jede Workloadpartition eine Dateibereichsnamenstrennung bereitgestellt. Jede Workloadpartition muss einen separaten Knotennamen und einen Scheduler haben, der innerhalb der globalen Partition ausgeführt wird. Außerdem müssen drei Scheduler-Services definiert werden, wobei jeder Service entsprechend dem Namen der Serverzeilengruppe eine andere Datei dsm.opt verwendet. Diese Methode ermöglicht, dass jede WPAR-

Sicherungsoperation unabhängig von den anderen verwaltet wird. Unter Verwendung der Beispielkonfiguration zeigt das folgende Beispiel eine Musterdatei dsm.sys mit drei Serverzeilengruppen: eine für `wpar1`, eine für `wpar2` und eine für die globale Partition `shimla`:

```
SErvername  shimla_wpar1
   TCPPort            1500
   TCPServeraddress   server.example.com
   nodename           wpar1
   PasswordAccess     generate
   Domain             /wpars/wpar1/home

SErvername  shimla_wpar2
   TCPPort            1500
   TCPServeraddress   server.example.com
   nodename           wpar2
   PasswordAccess     generate
   Domain             /wpars/wpar2/data

SErvername  shimla
   TCPPort            1500
   TCPServeraddress   server.example.com
   nodename           shimla
   PasswordAccess     generate
   Domain             /home /opt
```



Solaris Zettabyte-Dateisysteme (ZFS) sichern

Auf Solaris SPARC- und Solaris x86-Systemen können Sie ZFS-Dateisysteme (Zettabyte File System) mithilfe von ZFS-Momentaufnahmen sichern. Der Vorteil dieser Methode im Vergleich zu einer normalen Teilsicherung oder selektiven Sicherung besteht darin, dass sich die Dateien und Ordner in einer Momentaufnahme immer im Lesezugriffsmodus befinden und daher während einer Sicherung nicht geändert werden können.

Informationen zu diesem Vorgang

Eine ZFS-Momentaufnahme erstellen Sie mithilfe von Oracle Solaris-ZFS-Befehlen. Beispiel:

```
zfs snapshot tank/myZFS@mySnapshot
```

In diesem Beispiel lautet der ZFS-Poolname tank und der Name des ZFS-Dateisystems ist myZFS. Dateien, die zu dieser ZFS-Momentaufnahme gehören, befinden sich in dem Unterverzeichnis tank/myZFS/.zfs/snapshot/mySnapshot/.

Vorgehensweise

Verwenden Sie eine dieser beiden Methoden, um eine ZFS-Momentaufnahme zu sichern.

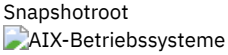
- Sichern Sie jede Datei der Momentaufnahme mithilfe der Option snapshotroot. Beispiel:

  ```
  dsmc inc -snapshotroot=/tank/myZFS/.zfs/snapshot/mySnapshot /tank/myZFS
  ```

  Mit dieser Option kann der Administrator den aktuellen Momentaufnahmepfad durch den ZFS-Dateisystempfad ersetzen, so dass die Dateien und Ordner mit dem ursprünglichen Dateisystem gesichert werden.
- Sichern Sie die vollständige Momentaufnahme mithilfe von Oracle Solaris-ZFS-Befehlen. Beispiel:

  ```
  zfs send tank/myZFS@mySnapshot > /tmpdir/mySnapshotFile
  ```

  Der Vorteil des Sicherns der vollständigen Momentaufnahme liegt darin, dass im Notfall das gesamte Dateisystem zurückgeschrieben werden kann.

Zugehörige Konzepte:
Solaris Zettabyte-Dateisysteme (ZFS) zurückschreiben
Zugehörige Verweise:
Snapshotroot


Verschlüsseltes AIX JFS2-Dateisystem sichern

Verwenden Sie das AIX JFS2-EFS-System (EFS = Encrypted File System - Verschlüsseltes Dateisystem), um Dateien entweder im Klartext oder im unformatierten Format zu sichern. Beim Format Klartext wird die Datei von EFS beim Lesen entschlüsselt. Beim unformatierten Format werden die Daten nicht entschlüsselt. Standardwert ist das unformatierte Format, aber wenn Sie die Option efsdecrypt auf yes setzen, erhalten Sie Sicherungen im Klartext.

Informationen zu diesem Vorgang

Wichtig: Immer, wenn Sie eine Sicherung ausführen, die auf einem EFS verschlüsselte Dateien einschließt, müssen Sie sicherstellen, dass Sie die korrekte Spezifikation der Option efsdecrypt verwenden. Falls sich der Optionswert efsdecrypt zwischen zwei Teilsicherungen ändert, werden alle verschlüsselten Dateien auf EFS-Dateisystemen erneut gesichert, selbst wenn sie sich seit der letzten Sicherung nicht geändert haben. Wenn Sie z. B. eine Teilsicherung verschlüsselter Dateien ausführen, die zuvor als unformatiert gesichert wurden, müssen Sie sicherstellen, dass efsdecrypt auf no gesetzt wird. Wenn Sie efsdecrypt in yes ändern, werden alle Dateien im Klartext erneut gesichert, selbst wenn sie unverändert sind. Stellen Sie deshalb sicher, dass Sie diese Option mit Vorsicht verwenden.

Wenn Sie versuchen, eine verschlüsselte Datei entweder auf eine Workstation, die EFS nicht unterstützt, oder in ein Dateisystem, in dem EFS nicht aktiv ist, zurückzuschreiben, wird eine Fehlernachricht geschrieben und die Datei wird übersprungen.

Einige Gründe für das Sichern von EFS mit der Verschlüsselung im Klartext:

- Diese Entschlüsselungsart ist nützlich, wenn Sie die Verschlüsselung des IBM Spectrum Protect-Clients für Sichern/Archivieren oder eine andere Art von Hardwareverschlüsselung (z. B. für Bandsysteme) verwenden wollen.
- Sie können Klartext für eine langfristige Archivierung von Daten verwenden, da die Daten unabhängig von der Plattform oder dem Verschlüsselungsschema gespeichert werden.

Nachfolgend einige Dinge, die zu beachten sind, wenn Sie eine Datei im Klartext sichern:

- Der Benutzer, von dem der Client für Sichern/Archivieren aufgerufen wurde, muss die Datei entschlüsseln können.
- Der Benutzer kann Lesezugriff auf eine Datei, aber keinen Zugriff auf den Schlüssel haben.

In den folgenden Szenarios wird eine Fehlernachricht ausgegeben:

Vorgehensweise

1. Der Benutzer wird im Modus Rootwächter ausgeführt, und EFS verfügt über das Konzept von zwei Roottypen. Rootadministrator ist der traditionelle Modus. Ein Root im Wächtermodus hat keinen Zugriff auf die unverschlüsselten Daten, es sei denn, der Benutzer ist der Eigner oder ein Mitglied der Dateigruppe.
2. Der Benutzer wird mit einer Nicht-Rootbenutzer-ID ausgeführt und versucht die Archivierung einer Datei, auf die er Lesezugriff hat, aber der Benutzer ist nicht der Eigner oder ein Mitglied der Dateigruppe. EFS wird es nicht zulassen, dass die Daten entschlüsselt werden.

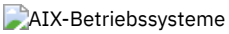
Ergebnisse

Nachfolgend einige Hinweise zum Sichern von unformatierten EFS-Daten:

- Die Clientverschlüsselungseinstellung, die eine doppelte Verschlüsselung verhindert (dies aber nur auf dem Client), wird vom Client für Sichern/Archivieren nicht berücksichtigt. Der Server weiß nicht, dass die Daten verschlüsselt sind; dies bedeutet, dass eine Verschlüsselung, die z. B. von einem Bandlaufwerk erfolgt, trotzdem vorkommen kann.
- Die Komprimierungseinstellung wird vom Client nicht berücksichtigt, sodass der Client gar nicht erst versuchen wird, die Daten zu komprimieren.
- Die Schlüsselspeicherdatei wird vom Client nicht automatisch gesichert oder zurückgeschrieben. Wenn Sie verschlüsselte Dateien zurückschreiben, müssen Sie unter Umständen auch die Schlüsselspeicherdateien zurückschreiben, damit die Daten entschlüsselt werden können.

  Tipps:

  1. Stellen Sie zum Schutz des Schlüsselspeichers sicher, dass der Inhalt von /var/efs in Ihre regelmäßigen Sicherungen eingeschlossen wird.
  2. Für die Schlüsselspeicherdaten verwenden Sie die IBM Spectrum Protect-Speichermaßnahme mit einer unbegrenzten Anzahl Versionen.
- EFS-Dateien, die im unformatierten Modus (Standardwert) gesichert wurden, können nicht von einem Client für Sichern/Archivieren vor Version 5.5 oder einem Client auf einer anderen UNIX-Plattform zurückgeschrieben werden.



Erweiterte AIX JFS2-Attribute sichern

AIX Enhanced Journal File System (JFS2) bietet Sicherungsverarbeitung für benannte erweiterte Attribute für alle Dateisysteme, die benannte erweiterte Attribute unterstützen.

Diese erweiterten Attribute werden automatisch mit jedem Objekt gesichert, das Daten mit erweiterten Attributen enthält, und es ist keine weitere Aktion erforderlich.

Ist das Dateisystem mit dem V2-Format definiert, ist JFS2 das einzige Dateisystem, das erweiterte Attribute unterstützt. Sie können JFS2 für erweiterte Attribute bei Dateien und Verzeichnissen verwenden; Sie können JFS2 jedoch nicht für erweiterte Attribute bei symbolischen Verbindungen verwenden.


Virtuelle VMware-Maschinen sichern

Sie können mithilfe des Clients für Sichern/Archivieren eine virtuelle VMware-Maschine sichern und zurückschreiben. Gesamtsicherungen der virtuellen Maschine werden auf Plattenimageebene ausgeführt. Bei Teilsicherungen werden nur die Daten gesichert, die sich seit der vorherigen Gesamtsicherung geändert haben.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Linux-BetriebssystemeTabelle 1 enthält die Sicherungs- und Zurückschreibungsfunktionalität für virtuelle VMware-Maschinen, die der Client für Sichern/Archivieren auf Linux-Plattformen implementieren kann.

Tabelle 1. Sicherungs- und Zurückschreibungsfunktionalität für virtuelle VMware-Maschinen auf Linux-Plattformen

Funktion	Kommentar
Immer inkrementelle VM-Gesamtsicherung:	Eine VM-Gesamtsicherung ist erforderlich, bevor Sie Teilsicherungen erstellen können. Wenn Sie immer inkrementelle Sicherungen planen, wird dieser Sicherungstyp automatisch für die erste Sicherung ausgewählt, wenn noch keine Gesamtsicherung erstellt wurde. Daten aus Teilsicherungen werden mit Daten aus der Gesamtsicherung kombiniert, um daraus ein synthetisches Gesamtsicherungsimage zu erstellen. Bei nachfolgenden immer inkrementellen VM-Gesamtsicherungen werden alle verwendeten Blöcke gelesen und auf den IBM Spectrum Protect-Server kopiert. Bei jeder immer inkrementellen VM-Gesamtsicherung werden alle verwendeten Blöcke, unabhängig davon, ob die Blöcke seit der letzten Sicherung geändert wurden oder nicht, gelesen und kopiert. Sie können weiterhin eine VM-Gesamtsicherung planen, obwohl eine Gesamtsicherung nicht mehr erforderlich ist. Sie können beispielsweise eine VM-Gesamtsicherung ausführen, um eine Sicherung für einen anderen Knotennamen mit anderen Aufbewahrungseinstellungen zu erstellen. Sie können diesen Sicherungsmodus nicht für die Sicherung einer virtuellen VMware-Maschine verwenden, wenn die Verschlüsselung der Sicherungsdaten auf dem Client konfiguriert ist.
Immer inkrementelle VM-Teilsicherung:	Sie müssen nur einmal eine VM-Gesamtsicherung erstellen. Bei der VM-Gesamtsicherung werden alle verwendeten Plattenblöcke, deren Eigner eine virtuelle Maschine ist, auf den IBM Spectrum Protect-Server kopiert. Nach dem Abschluss der ersten Gesamtsicherung sind alle nachfolgenden Sicherungen der virtuellen Maschine immer inkrementelle Teilsicherungen. Bei jeder immer inkrementellen Teilsicherung werden nur die Blöcke kopiert, die seit der letzten Sicherung geändert wurden, unabhängig vom Typ der letzten Sicherung. Der Server verwendet eine Gruppierungstechnologie, mit der die geänderten Blöcke aus der neuesten Sicherung den Daten zugeordnet werden, die bereits aus vorherigen Sicherungen auf dem Server gespeichert sind. Eine neue vollständige Sicherung wird dann jedes Mal effektiv erstellt, wenn bei einer immer inkrementellen Teilsicherung geänderte Blöcke auf den Server kopiert werden. Der Sicherungsmodus für immer inkrementelle Teilsicherungen bietet die folgenden Vorteile: • Verbessert die Effizienz beim Sichern virtueller Maschinen. • Vereinfacht Datenzurückschreibungsoperationen. • Optimiert Datenzurückschreibungsoperationen. Bei einer Zurückschreibungsoperation können Sie für die Wiederherstellung von Daten Optionen für den Zeitpunkt und das Datum angeben. Die Daten werden aus der ursprünglichen vollständigen Sicherung und allen geänderten Blöcken zurückgeschrieben, die den Daten zugeordnet sind. Sie können diesen Sicherungsmodus nicht für die Sicherung einer virtuellen VMware-Maschine verwenden, wenn die Verschlüsselung der Sicherungsdaten auf dem Client konfiguriert ist.
Wiederherstellung von Objekten für Dateien und Ordner aus einer vollständigen Sicherung der virtuellen Maschine:	Ermöglicht das Wiederherstellen von Dateien und Ordnern aus einer vollständigen Sicherung einer virtuellen Maschine. Die Wiederherstellung von Elementen ist nur mit IBM Spectrum Protect Recovery Agent verfügbar.
Vollständige Zurückschreibung der virtuellen Maschine:	Schreibt alle Dateisysteme, virtuellen Platten und die Konfiguration der virtuellen Maschine zurück.

Windows-BetriebssystemeTabelle 2 enthält die Sicherungs- und Zurückschreibungsfunktionalität für virtuelle VMware-Maschinen, die der Client für Sichern/Archivieren auf Windows-Plattformen implementieren kann.
Einschränkung: Sie können VMware-Sicherungs- und Zurückschreibungsoperationen mit dem Client für Sichern/Archivieren nur unter 64-Bit-Windows-Betriebssystemen ausführen.

Tabelle 2. Sicherungs- und Zurückschreibungsfunktionalität für virtuelle VMware-Maschinen auf Windows-Plattformen

Funktion	Kommentar

Funktion	Kommentar
Immer inkrementelle VM-Gesamtsicherung:	Das lizenzierte Produkt 'IBM Spectrum Protect for Virtual Environments' ist hierfür erforderlich. Eine VM-Gesamtsicherung ist erforderlich, bevor Sie Teilsicherungen erstellen können. Wenn Sie immer inkrementelle Sicherungen planen, wird dieser Sicherungstyp automatisch für die erste Sicherung ausgewählt, wenn noch keine Gesamtsicherung erstellt wurde. Daten aus Teilsicherungen werden mit Daten aus der Gesamtsicherung kombiniert, um daraus ein synthetisches Gesamtsicherungsimage zu erstellen. Bei nachfolgenden immer inkrementellen VM-Gesamtsicherungen werden alle verwendeten Blöcke gelesen und auf den IBM Spectrum Protect-Server kopiert. Bei jeder immer inkrementellen VM-Gesamtsicherung werden alle verwendeten Blöcke, unabhängig davon, ob die Blöcke seit der letzten Sicherung geändert wurden oder nicht, gelesen und kopiert. Sie können weiterhin eine VM-Gesamtsicherung planen, obwohl eine Gesamtsicherung nicht mehr erforderlich ist. Sie können beispielsweise eine VM-Gesamtsicherung ausführen, um eine Sicherung für einen anderen Knotennamen mit anderen Aufbewahrungseinstellungen zu erstellen. Sie können diesen Sicherungsmodus nicht für die Sicherung einer virtuellen VMware-Maschine verwenden, wenn die Verschlüsselung der Sicherungsdaten auf dem Client konfiguriert ist.
Immer inkrementelle VM-Teilsicherung:	Das lizenzierte Produkt 'IBM Spectrum Protect for Virtual Environments' ist hierfür erforderlich. Sie müssen nur einmal eine VM-Gesamtsicherung erstellen. Bei der VM-Gesamtsicherung werden alle verwendeten Plattenblöcke, deren Eigner eine virtuelle Maschine ist, auf den IBM Spectrum Protect-Server kopiert. Nach dem Abschluss der ersten Gesamtsicherung sind alle nachfolgenden Sicherungen der virtuellen Maschine immer inkrementelle Teilsicherungen. Bei jeder immer inkrementellen Teilsicherung werden nur die Blöcke kopiert, die seit der letzten Sicherung geändert wurden, unabhängig vom Typ der letzten Sicherung. Der Server verwendet eine Gruppierungstechnologie, mit der die geänderten Blöcke aus der neuesten Sicherung den Daten zugeordnet werden, die bereits aus vorherigen Sicherungen auf dem Server gespeichert sind. Eine neue vollständige Sicherung wird dann jedes Mal effektiv erstellt, wenn bei einer immer inkrementellen Teilsicherung geänderte Blöcke auf den Server kopiert werden. Der Sicherungsmodus für immer inkrementelle Teilsicherungen bietet die folgenden Vorteile: • Verbessert die Effizienz beim Sichern virtueller Maschinen. • Vereinfacht Datenzurückschreibungsoperationen. • Optimiert Datenzurückschreibungsoperationen. Bei einer Zurückschreibungsoperation können Sie für die Wiederherstellung von Daten Optionen für den Zeitpunkt und das Datum angeben. Die Daten werden aus der ursprünglichen vollständigen Sicherung und allen geänderten Blöcken zurückgeschrieben, die den Daten zugeordnet sind. Sie können diesen Sicherungsmodus nicht für die Sicherung einer virtuellen VMware-Maschine verwenden, wenn die Verschlüsselung der Sicherungsdaten auf dem Client konfiguriert ist.
Wiederherstellung von Objekten für Dateien und Ordner aus einer vollständigen Sicherung der virtuellen Maschine:	Das lizenzierte Produkt 'IBM Spectrum Protect for Virtual Environments' ist hierfür erforderlich. Ermöglicht das Wiederherstellen von Dateien und Ordnern aus einer vollständigen Sicherung einer virtuellen Maschine. Die Wiederherstellung von Elementen ist nur mit IBM Spectrum Protect Recovery Agent verfügbar.
Vollständige Zurückschreibung der virtuellen Maschine:	Schreibt alle Dateisysteme, virtuellen Platten und die Konfiguration der virtuellen Maschine zurück.
Zurückschreibung auf Dateiebene der virtuellen Maschine:	Die Zurückschreibungsmethode ist vom Sicherungstyp der virtuellen Maschine abhängig: • Wenn Sie über eine Lizenz für IBM Spectrum Protect for Virtual Environments verfügen, können Sie Dateien und Verzeichnisse aus einer vollständigen VM-Imagesicherung zurückschreiben. • Benutzer des Clients für Sichern/Archivieren können Dateien und Verzeichnisse zurückschreiben, die erstellte Sicherungen auf Dateiebene einer virtuellen Maschine sind. Zum Zurückschreiben einzelner Dateien aus einer Sicherung auf Dateiebene einer virtuellen Maschine verwenden Sie den Befehl restore, nicht den Befehl restore vm. Anmerkung: Sicherungen auf Dateiebene wurden mit Clients für Sichern/Archivieren der Version 7.1 oder früher erstellt.

- Linux-BetriebssysteWindows-BetriebssystemeUmgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten
  Zur Vorbereitung der VMware-Umgebung auf die Sicherung vollständiger virtueller VMware-Maschinen führen Sie die folgenden Schritte aus. Auf dem vStorage-Sicherungsserver kann entweder ein Windows- oder ein Linux-Client ausgeführt werden.
- Linux-BetriebssysteWindows-BetriebssystemeGesamtsicherungen für virtuelle VMware-Maschinen erstellen
  Bei einer Gesamtsicherung einer virtuellen VMware-Maschine wird die gesamte virtuelle Maschine, einschließlich der virtuellen Platten und der Konfigurationsdatei der virtuellen Maschine, gesichert. Dieser Sicherungstyp ähnelt einer Imagesicherung. Für die Erstellung der Gesamtsicherung konfigurieren Sie den Client für Sichern/Archivieren auf dem vStorage-Sicherungsserver. Auf dem vStorage-Sicherungsserver muss ein Windows- oder Linux-Client ausgeführt werden.

- Linux-BetriebssystemeWindows-BetriebssystemeParallele Sicherungen virtueller Maschinen
  Bei der parallelen Sicherungsverarbeitung können Sie einen einzigen Knoten einer Einheit zum Versetzen von Daten verwenden, um mehrere virtuelle Maschinen (VMs) gleichzeitig zu sichern, um Ihre Sicherungsleistung zu optimieren.

Linux-BetriebssystemeWindows-Betriebssysteme

Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten

Zur Vorbereitung der VMware-Umgebung auf die Sicherung vollständiger virtueller VMware-Maschinen führen Sie die folgenden Schritte aus. Auf dem vStorage-Sicherungsserver kann entweder ein Windows- oder ein Linux-Client ausgeführt werden.

Vorbereitende Schritte

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Vorgehensweise

1. Gehen Sie wie folgt vor, um die Speicherumgebung für die Sicherung zu konfigurieren:
   a. Konfigurieren Sie Ihre Speicherumgebung so, dass der vStorage-Sicherungsserver auf die Speicherdatenträger zugreifen kann, die sich in Ihrer ESX-Server-Farm befinden.
   b. Wenn Sie NAS (Network-Attached Storage) oder DAS (Direct-Attached Storage) verwenden, stellen Sie sicher, dass der vStorage-Sicherungsserver mit einer netzbasierten Transportmethode auf die Datenträger zugreift.
   c. Optional: Nehmen Sie für den Datenzugriff die folgenden Einstellungen vor:
      - Erstellen Sie SAN-Zonen, mit denen Ihr vStorage-Sicherungsserver auf die logischen Speichereinheiten zugreifen kann, in denen sich Ihre VMware-Datenspeicher befinden (SAN - storage area network, Speicherbereichsnetz).
      - Konfigurieren Sie die Hostzuordnungen des Plattensubsystems, so dass alle ESX-Server und der Sicherungs-Proxy auf dieselben Plattendatenträger zugreifen können.
2. Gehen Sie wie folgt vor, um den vStorage-Sicherungsserver zu konfigurieren:
   a. Linux-BetriebssystemeLegen Sie die Umgebungsvariable LD_LIBRARY_PATH so fest, dass sie auf das Clientinstallationsverzeichnis verweist, und exportieren Sie die Umgebungsvariable. Beispiel:

      ```
      export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
      ```

   b. Linux-BetriebssystemeFügen Sie das Clientinstallationsverzeichnis zum Pfad jedes Konto hinzu, das Befehle des Clients für Sichern/Archivieren verwendet, z. B. dsmc, dsmcad oder dsmj.
   c. Windows-BetriebssystemeWenn der Client für Sichern/Archivieren auf einem vStorage-Sicherungsserver ausgeführt wird, wird diese Clientkonfiguration als IBM Spectrum Protect-*Knoten der Einheit zum Versetzen von Daten* bezeichnet. Auf einem Windows-System, das eine Einheit zum Versetzen von Daten ist, muss der Windows-64-Bit-Client installiert sein. Ein Knoten der Einheit zum Versetzen von Daten verwendet zum Sichern und Zurückschreiben von Daten normalerweise das SAN (Speicherbereichsnetz). Falls Sie den Knoten der Einheit zum Versetzen von Daten für den direkten Zugriff auf die Speicherdatenträger konfigurieren, inaktivieren Sie die automatische Laufwerkzuordnung. Wird die automatische Laufwerkzuordnung nicht inaktiviert, kann der Client auf dem Knoten der Einheit zum Versetzen von Daten das Raw Device Mapping (RDM) der virtuellen Platten beschädigen. Wenn das RDM der virtuellen Platte beschädigt ist, schlägt die Sicherung fehl. Beachten Sie bei den Zurückschreibungskonfigurationen die folgenden Bedingungen:

      Der Knoten der Einheit zum Versetzen von Daten befindet sich auf einem Windows Server 2012- oder Windows Server 2012 R2-System:

      Wenn Sie planen, Daten mithilfe des SAN zurückzuschreiben, müssen Sie OnlineAll für die Windows-SAN-Maßnahme angeben. Führen Sie diskpart.exe aus und geben Sie die folgenden Befehle ein, um die automatische Laufwerkzuordnung zu inaktivieren und die SAN-Maßnahme auf OnlineAll zu setzen:

      ```
      diskpart
        automount disable
        automount scrub
        san policy OnlineAll
        exit
      ```

      Der Client für Sichern/Archivieren ist in einer virtuellen Maschine auf einem Windows Server 2012- oder Windows Server 2012 R2-System installiert:

      Wenn Sie planen, Daten mit der Transportmethode `hotadd` von dynamisch hinzugefügten Platten zurückzuschreiben, müssen Sie auch OnlineAll für die SAN-Maßnahme auf diesem System angeben.
      Unabhängig davon, ob der Client das SAN oder die Transportmethode `hotadd` verwendet, muss die Windows-SAN-Maßnahme auf OnlineAll gesetzt werden. Wenn die SAN-Maßnahme nicht auf OnlineAll gesetzt wird, schlagen Zurückschreibungsoperationen fehl und die folgende Nachricht wird ausgegeben:

      ```
      ANS9365E VMware vStorage API error.
      IBM Spectrum Protect function name: vddksdk Write
      IBM Spectrum Protect file : vmvddkdsk.cpp (2271)
      API return code : 1
      API error message : Unknown error
      ```

```
ANS0361I DIAG: ANS1111I VmRestoreExtent(): VixDiskLib_Write
FAILURE startSector=512 sectorSize=512 byteOffset=262144,
rc=-1
```

Eine Beschreibung der vStorage-Transporteinstellungen und wie Sie die Standardwerte überschreiben können, finden Sie in folgendem Abschnitt:

Linux-BetriebssystemeWindows-BetriebssystemeVmvstortransport

d. Windows-BetriebssystemeInstallieren Sie den Client für Sichern/Archivieren auf dem vStorage-Sicherungsserver. Wählen Sie auf der Seite für die angepasste Installation des Installationsassistenten VMware vStorage-API-Laufzeitdateien aus.
Wichtig: Wenn Sie die Sicherungsdaten mithilfe von Sicherungen versetzen, die sich nicht in einem LAN befinden, muss das SAN über separate Verbindungen für Band und Platte verfügen.

3. Gehen Sie wie folgt vor, um IBM Spectrum Protect zu ändern:
   a. Greifen Sie auf die Verwaltungsbefehlszeile des Clients für Sichern/Archivieren zu.
   b. Führen Sie im Client für Sichern/Archivieren auf dem vStorage-Sicherungsserver den folgenden Befehl aus, um den Knoten zu registrieren:

      ```
      register node Servername Kennwort
      ```

      Dabei gibt *Servername* den vollständigen Computernamen des vStorage-Sicherungsservers und *Kennwort* das Kennwort für den Zugriff auf den Server an.
      Windows-BetriebssystemeTipp: Auf Windows-Systemen können Sie den vollständigen Computernamen des Servers abrufen, indem Sie mit der rechten Maustaste auf Arbeitsplatz klicken. Klicken Sie auf die Registerkarte 'Computername' und suchen Sie nach dem Namen neben Computername.
   c. Windows-BetriebssystemeFühren Sie im Client für Sichern/Archivieren auf dem vStorage-Sicherungsserver den folgenden Befehl aus, um den Knoten zu registrieren:

      ```
      register node VM-Name Kennwort
      ```

      Dabei gibt *VM-Name* den vollständigen Namen der virtuellen Maschine an, die gesichert wird.
4. Windows-BetriebssystemeWenn Sie eine virtuelle Maschine sichern, in der Datenträger nicht Laufwerkbuchstaben, sondern Verzeichnissen zugeordnet sind, werden Dateien möglicherweise nicht an der richtigen Position gespeichert. Ein Fehler könnte verursacht werden, weil der Mountpunkt nicht den tatsächlichen Mountpunkten gesicherter Dateien entspricht. Ein Fehler wird verursacht, weil die Mountpunkte für eine virtuelle Maschine, in der Windows ausgeführt wird, keine Laufwerkzuordnung aufweisen. Wenn Sie die VMware-vStorage-APIs for Data Protection verwenden, wird ein `Dateibereichsname` erstellt, der eine Nummernzuordnung enthält. Die `Dateibereichsnamen`, die für den Mountpunkt erstellt werden, entsprechen nicht den tatsächlichen Mountpunkten der gesicherten Datei.

   Um Dateien an ihrer ursprünglichen Position zu sichern oder Dateien in ihre ursprüngliche Position zurückzuschreiben, führen Sie die folgenden Schritte aus:

   a. Um die Dateien an ihre ursprüngliche Position zurückzuschreiben, ordnen Sie das Laufwerk zu oder ordnen Sie dem Mountpunkt der virtuellen Maschine einen Laufwerkbuchstaben zu.
   b. Wenn Sie eine Datei zurückschreiben, die von der VMware-vStorage-API umbenannt wurde, wählen Sie eine andere Position für die Zurückschreibung aus.
   c. Werden Mountpunkte ohne Zuordnungen von Laufwerkbuchstaben verwendet, verwenden Sie eine Einschluss- oder Ausschlussanweisung für diesen Datenträger. Siehe das folgende Beispiel einer Ausschlussanweisung:

      ```
      exclude \\machine\3$\dir1\...\*.doc
      ```

Zugehörige Tasks:
Linux-BetriebssystemeWindows-BetriebssystemeGesamtsicherungen für virtuelle VMware-Maschinen erstellen
Zugehörige Verweise:
Linux-BetriebssystemeWindows-BetriebssystemeBackup VM
Linux-BetriebssystemeWindows-BetriebssystemeQuery VM
Linux-BetriebssystemeWindows-BetriebssystemeRestore VM
Linux-BetriebssystemeWindows-BetriebssystemeVmchost
Linux-BetriebssystemeWindows-BetriebssystemeVmcpw
Linux-BetriebssystemeWindows-BetriebssystemeVmcuser
Linux-BetriebssystemeWindows-BetriebssystemeVmvstortransport
Linux-BetriebssystemeWindows-Betriebssysteme

Gesamtsicherungen für virtuelle VMware-Maschinen erstellen

Bei einer Gesamtsicherung einer virtuellen VMware-Maschine wird die gesamte virtuelle Maschine, einschließlich der virtuellen Platten und der Konfigurationsdatei der virtuellen Maschine, gesichert. Dieser Sicherungstyp ähnelt einer Imagesicherung. Für die Erstellung der Gesamtsicherung konfigurieren Sie den Client für Sichern/Archivieren auf dem vStorage-Sicherungsserver. Auf dem vStorage-Sicherungsserver muss ein Windows- oder Linux-Client ausgeführt werden.

Vorbereitende Schritte

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Vorgehensweise

1. Führen Sie die Schritte im folgenden Abschnitt aus, um die Umgebung vorzubereiten:

   Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten

2. Gehen Sie wie folgt vor, um den Client für Sichern/Archivieren auf dem vStorage-Sicherungsserver zu konfigurieren:
   a. Klicken Sie auf der Begrüßungsseite der GUI des Clients für Sichern/Archivieren auf Editieren > Clientvorgaben.
   b. Wählen Sie die Registerkarte VM-Sicherung aus.
   c. Wählen Sie VMWare - Vollständige VM aus.
   d. Wählen Sie in der Liste Sicherungstypen für Domäne die Option Vollständige VM-Sicherung für Domäne aus.
   e. Geben Sie in das Feld Host entweder den Hostnamen jedes ESX-Servers oder den Hostnamen des Virtual Center ein. Wenn Sie das Virtual Center angeben, können Sie virtuelle Maschinen auf allen VMware-Servern sichern, die vom Virtual Center verwaltet werden.
   f. Geben Sie die Benutzer-ID und das Kennwort für den Host ein, den Sie im Feld Host angeben.
   g. Optional: Falls Sie die Standardverwaltungsklasse für Gesamtsicherungen von virtuellen Maschinen überschreiben wollen, geben Sie die Verwaltungsklasse an, die verwendet werden soll.
   h. Geben Sie in das Feld Datenspeicherposition den Pfad des Verzeichnisses ein, in dem die Dateien gespeichert werden.
   i. Klicken Sie auf OK, um Ihre Änderungen zu speichern.
3. Gehen Sie wie folgt vor, um eine Sicherung einer der virtuellen Maschinen zu erstellen:
   a. Führen Sie über die Befehlszeile des vStorage-Sicherungsservers den folgenden Befehl aus:

      ```
      dsmc backup vm Name_der_eigenen_VM -mode=iffull -vmbackuptype=fullvm
      ```

      Dabei gibt *Name_der_eigenen_VM* den Namen der virtuellen Maschine an.
   b. Überprüfen Sie, ob der Befehl fehlerfrei ausgeführt wurde. Die folgende Nachricht zeigt eine erfolgreiche Ausführung an:

      ```
      Befehl 'Backup VM' ausgeführt
      Gesamtzahl der erfolgreich gesicherten virtuellen Maschinen: 1
      Virtuelle Maschine 'VM-Name' auf Knotenname NODE gesichert
      Gesamtzahl der fehlgeschlagenen virtuellen Maschinen: 0
      Gesamtzahl der verarbeiteten virtuellen Maschinen: 1
      ```

4. Linux-BetriebssystemeGehen Sie wie folgt vor, um zu überprüfen, ob Sie die Dateien für die virtuelle Maschine zurückschreiben können:
   a. Führen Sie über die Befehlszeilenschnittstelle des vStorage-Sicherungsservers den folgenden Befehl aus:

      ```
      dsmc restore vm VM-Name
      ```

   b. Wenn während der Zurückschreibungsverarbeitung Fehler auftreten, suchen Sie im Clientfehlerprotokoll nach weiteren Informationen.
      Tipp: Die Protokolldatei wird unter `/opt/ibm/Tivoli/TSM/baclient/dsmerror.log` gespeichert.
5. Windows-BetriebssystemeGehen Sie wie folgt vor, um zu überprüfen, ob Sie die Dateien für die virtuelle Maschine zurückschreiben können:
   a. Führen Sie über die Befehlszeilenschnittstelle des vStorage-Sicherungsservers den folgenden Befehl aus:

      ```
      dsmc restore vm VM-Name
      ```

      Windows-BetriebssystemeDie Standardposition für die Zurückschreibung ist das folgende Verzeichnis: c:\mnt\tsmvmbackup*VM-Name*\fullvm\RESTORE_DATE_jjjj_mm_tt[hh_mm_ss].

   b. Wenn während der Zurückschreibungsverarbeitung Fehler auftreten, suchen Sie im Clientfehlerprotokoll nach weiteren Informationen.
      Tipp: Das Fehlerprotokoll wird in der folgenden Datei gespeichert:

      ```
      c:\Programme\Tivoli\TSM\baclient\dsmerror.log
      ```

Zugehörige Konzepte:
Linux-BetriebssystemeWindows-BetriebssystemeParallele Sicherungen virtueller Maschinen
Zugehörige Tasks:
Linux-BetriebssystemeWindows-BetriebssystemeUmgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten
Zugehörige Verweise:
Linux-BetriebssystemeWindows-BetriebssystemeBackup VM
Linux-BetriebssystemeWindows-BetriebssystemeDomain.vmfull
Linux-BetriebssystemeWindows-BetriebssystemeQuery VM
Linux-BetriebssystemeWindows-BetriebssystemeRestore VM
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeMode
Linux-BetriebssystemeWindows-BetriebssystemeVmchost
Linux-BetriebssystemeWindows-BetriebssystemeVmcpw
Linux-BetriebssystemeWindows-BetriebssystemeVmcuser
Linux-BetriebssystemeWindows-BetriebssystemeVmmc
Linux-BetriebssystemeWindows-BetriebssystemeVmvstortransport

Linux-BetriebssystemeWindows-Betriebssysteme

Parallele Sicherungen virtueller Maschinen

Bei der parallelen Sicherungsverarbeitung können Sie einen einzigen Knoten einer Einheit zum Versetzen von Daten verwenden, um mehrere virtuelle Maschinen (VMs) gleichzeitig zu sichern, um Ihre Sicherungsleistung zu optimieren.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Informationen zu parallelen Sicherungsoperationen finden Sie in Mehrere virtuelle Maschinen parallel sichern.

Windows-Betriebssysteme

Virtuelle Maschinen auf einem Hyper-V-System sichern

Sie können mithilfe des Clients für Sichern/Archivieren virtuelle Maschinen sichern, die von einem Microsoft Hyper-V-Server verwaltet werden.

Informationen zum Schützen von virtuellen Hyper-V-Maschinen finden Sie in IBM Spectrum Protect for Virtual Environments, Data Protection for Microsoft Hyper-V.

- Windows-BetriebssystemeEinschränkungen bei der Unterstützung für Hyper-V-Sicherungen
  Aufgrund der nahtlosen Integration der Microsoft Failover-Clusterunterstützung mit freigegebenen Clustervolumes und Hyper-V gelten bei Verwendung des Clients für Sichern/Archivieren die folgenden Einschränkungen.

Linux-BetriebssystemeWindows-Betriebssysteme

Tivoli Storage Manager FastBack-Daten sichern und archivieren

Verwenden Sie Tivoli Storage Manager FastBack, um die neuesten Momentaufnahmen für die kurzfristige Aufbewahrung zu sichern und zu archivieren.

Verwenden Sie die Befehle archive fastback und backup fastback, um Datenträger für die kurzfristige Aufbewahrung zu sichern und zu archivieren, die durch die Optionen fbpolicyname, fbclientname und fbvolumename angegeben sind.

Zugehörige Konzepte:
Installationsvoraussetzungen für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Clientdaten
Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren
Zugehörige Verweise:
Fbclientname
Fbpolicyname
Fbvolumename
Windows-Betriebssysteme

Net Appliance-CIFS-Freigabedefinition sichern

Network Appliance-CIFS-Freigabedefinitionen (NetApp-CIFS-Freigabedefinitionen) umfassen Freigabeberechtigungen, die auf dem Dateiserver definiert sind.

Informationen zu diesem Vorgang

Der Windows-Client sichert die CIFS-Freigabedefinition unter dem Stammverzeichnis, der zugeordneten CIFS-Freigabe oder dem UNC-Namen. Diese Unterstützung erfordert, dass der Net Appliance-Dateiserver DATA ONTAP-Software ausführt, die CIFS-Freigaben fernen Clients als normale ferne NTFS-Freigaben darstellt.

Das Stammverzeichnis einer CIFS-Freigabe wird mit einer vollständigen progressiven Teilsicherung des zugeordneten Laufwerks/UNC-Namens gesichert. Siehe hierzu die zwei folgenden Beispiele:

```
net use x: \\NetAppFiler\CifsShareName
dsmc incr x:

dsmc incr \\NetAppFiler\CifsShareName
```

Die folgende Ausgabe wird angezeigt, wenn das Stammverzeichnis (und die Freigabedefinition) gesichert wurde:

```
Verzeichnis-->                  0 \\NetAppFiler\CifsShare\ [Gesendet]
```

Zugehörige Konzepte:
Net Appliance-CIFS-Freigaben zurückschreiben
Zugehörige Verweise:

Status der Sicherungsverarbeitung anzeigen

Während einer Sicherung zeigt der Client für Sichern/Archivieren standardmäßig den Status jeder Datei an, die er zu sichern versucht.

Der Client meldet die Größe, den Pfad, den Dateinamen sowie die Gesamtzahl übertragener Byte zurück und gibt an, ob der Sicherungsversuch für die Datei erfolgreich war. Diese Angaben werden außerdem in der Datei `dsmsched.log` für geplante Befehle aufgezeichnet.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDie Java™-GUI des Web-Clients und des Clients für Sichern/Archivieren stellt das Fenster Task-Liste zur Verfügung, in dem Informationen zu gerade verarbeiteten Dateien angezeigt werden. Nach Beendigung einer Task werden im Fenster Sicherungsbericht die Verarbeitungsdetails angezeigt. Klicken Sie auf die Schaltfläche Hilfe im Fenster Sicherungsbericht, um hierzu den Hilfetext aufzurufen.

Windows-BetriebssystemeDie GUI des Web-Clients und des Clients für Sichern/Archivieren stellt das Fenster Task-Liste zur Verfügung, in dem Informationen zu gerade verarbeiteten Dateien angezeigt werden. Nach Beendigung einer Task werden im Fenster Sicherungsbericht die Verarbeitungsdetails angezeigt. Klicken Sie auf die Schaltfläche Hilfe im Fenster Sicherungsbericht, um hierzu den Hilfetext aufzurufen.

In der Befehlszeile des Clients für Sichern/Archivieren wird der Name jeder Datei angezeigt, nachdem sie zum Server gesendet wurde. Das Statusanzeigefeld zeigt den Gesamtfortschritt an.

In Tabelle 1 sind einige Informationsnachrichten mit ihrer Bedeutung aufgelistet.

Tabelle 1. Informationsnachrichten der Clientbefehlszeile

Informationsnachricht	**Bedeutung**
`Verzeichnis-->`	Gibt das Verzeichnis an, das gesichert wird.
Mac OS X-Betriebssysteme AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme`Normale Datei-->`.	Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeJede Datei, die weder ein Verzeichnis noch eine symbolische Verbindung noch eine Gerätedatei ist.
Mac OS X-Betriebssysteme AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme`Gerätedatei-->`	Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeGerätedateien definieren Einheiten für das System oder temporäre Dateien, die durch Prozesse erstellt werden. Es gibt drei Grundtypen der Gerätedateien: FIFO (First-In, First-Out), Block und Zeichen. FIFO-Dateien werden auch als Pipe bezeichnet. Pipes werden durch einen Prozess erstellt, um eine vorübergehende Kommunikation mit einem anderen Prozess zu ermöglichen. Diese Dateien sind nicht mehr vorhanden, wenn der erste Prozess beendet ist. Blockbelegungs- und Zeichendateien definieren Einheiten. Der Client verarbeitet nur einheiten- und benannte-Pipe-orientierte Gerätedateien. Socket-Gerätedateien werden nicht verarbeitet.
Mac OS X-Betriebssysteme AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme`Symbolische Verbindung-->`	Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeGibt an, dass der Client eine symbolische Verbindung sichert.
`Aktualisieren-->`	Gibt an, dass nur die Dateimetadaten gesendet werden und nicht die Daten selbst.
`Verfall-->`	Gibt ein Objekt (Datei oder Verzeichnis) auf dem Server an, das auf dem Client nicht mehr vorhanden ist. Das Objekt ist verfallen und wird auf dem Server inaktiviert.
`Gesamtanzahl geprüfter Objekte:`	Wie angezeigt. Bei der journalbasierten Sicherung ist die Anzahl der geprüften Objekte möglicherweise kleiner als die der gesicherten Objekte. Bei Verwendung der Teilsicherung unter Verwendung der Momentaufnahmedifferenz beträgt die Anzahl der geprüften Objekte null. Die Anzahl beträgt null, weil der Client eine Teilsicherung der Dateien durchführt, die NetApp als geändert gemeldet hat. Der Client überprüft den Datenträger nicht auf Dateien, die sich geändert haben.
`Gesamtanzahl gesicherter Objekte:`	Wie angezeigt.
`Gesamtzahl verschlüsselter Objekte:`	Hierbei handelt es sich um die Anzahl der Objekte, die während der Sicherungs- oder Archivierungsverarbeitung verschlüsselt wurden.
`Datenverschlüsselungstyp:`	Gibt die Art des Verschlüsselungsalgorithmus (z. B. 256-Bit AES) an, wenn mindestens ein Objekt während der Sicherungs- oder Archivierungsverarbeitung verschlüsselt wird.
`Gesamtanzahl aktualisierter Objekte:`	Hierbei handelt es sich um Dateien, deren Attribute, wie z. B. Dateieigner oder Dateiberechtigungen, geändert wurden.
`Gesamtanzahl erneut gebundener Objekte:`	Weitere Informationen siehe Verwaltungsklassen an Dateien binden.

Informationsnachricht	Bedeutung
`Gesamtanzahl gelöschter Objekte:`	Hierbei handelt es sich um die Anzahl der Objekte, die von der Client-Workstation gelöscht wurden, nachdem sie erfolgreich auf dem Server archiviert wurden. Die Anzahl ist für alle Sicherungsbefehle null.
`Gesamtanzahl verfallener Objekte:`	Weitere Informationen enthält der Abschnitt über vollständige und partielle Teilsicherungen.
`Gesamtanzahl fehlgeschlagener Objekte:`	Objekte können aus verschiedenen Gründen fehlschlagen. Weitere Einzelheiten hierzu sind in der Datei `dsmerror.log` enthalten.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Windows-Betriebssysteme`Gesamtzahl Momentaufnahmedifferenzobjekte`	AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeBei Teilsicherungen unter Verwendung der Momentaufnahmedifferenz stellt dies die Gesamtzahl der gesicherten Objekte und die Gesamtzahl der verfallenen Objekte dar.
`Gesamtzahl deduplizierter Objekte`	Gibt die Anzahl der deduplizierten Dateien an.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-Betriebssysteme`Gesamtzahl der überprüften Byte:`	AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeGibt die Summe der Größe der Dateien an, die für die Operation ausgewählt sind. Beispiel: Die Gesamtzahl der überprüften Byte für den folgenden Befehl ist die Anzahl der Byte, die auf dem Datenträger `/Volumes/BUILD` belegt sind: `dsmc INCREMENTAL /Volumes/BUILD/* -SU=Yes`
`Gesamtzahl der Byte vor der Deduplizierung:`	Gibt die Anzahl der Byte an, die an den IBM Spectrum Protect-Server gesendet werden sollen, wenn der Client redundante Daten nicht entfernt. Vergleichen Sie diesen Betrag mit `Gesamtzahl der Byte nach der Deduplizierung`.Beinhaltet die Metadatengröße und könnte größer sein als die Anzahl der überprüften Byte.
`Gesamtzahl der Byte nach der Deduplizierung:`	Gibt die Anzahl der Byte an, die nach der Deduplizierung der Dateien auf dem Client-Computer an den IBM Spectrum Protect-Server gesendet werden. Beinhaltet die Metadatengröße und könnte größer sein als die Anzahl der verarbeiteten Byte.
 Windows-Betriebssysteme`Gesamtzahl der überprüften Byte:`	Windows-BetriebssystemeGibt die Summe der Größe der Dateien an, die für die Operation ausgewählt sind. Beispiel: Die Gesamtzahl der überprüften Byte für den folgenden Befehl ist die Anzahl der Byte, die im Verzeichnis `C:\Users` belegt sind: `dsmc.exe INCREMENTAL C:\Users\* -su=yes`
`Gesamtzahl der verarbeiteten Byte:`	Gibt die Summe der Größe der Dateien an, die für die Operation verarbeitet werden.
`Datenübertragungszeit:`	Die Gesamtzeit der Datenübertragung über das Netz. Wenn die Operation wegen eines Übertragungs- oder Sitzungsfehlers wiederholt wurde, entsprechen die Übertragungsstatistiken möglicherweise nicht den Dateistatistiken. Die Übertragungsstatistik zeigt die Anzahl Bytes an, die während aller Befehlsversuche übertragen werden sollte.
`Datenübertragungsgeschwindigkeit im Netz:`	Die Durchschnittsgeschwindigkeit, mit der im Netz Daten zwischen dem Client und dem Server übertragen werden. Die Übertragungsgeschwindigkeit wird berechnet, indem die Gesamtzahl übertragener Byte durch die Zeit für die Übertragung der Daten über das Netz dividiert wird. Die Zeit, die für die Verarbeitung von Objekten benötigt wird, wird bei der Datenübertragungsgeschwindigkeit im Netz nicht berücksichtigt. Daher ist die Datenübertragungsgeschwindigkeit im Netz größer als die Gesamtübertragungsgeschwindigkeit.

Informationsnachricht	Bedeutung
`Datenübertragungsgeschwindigkeit Gesamt:`	Die Durchschnittsgeschwindigkeit, mit der IBM Spectrum Protect und das Netz Daten zwischen dem Client und dem Server übertragen. Die Übertragungsgeschwindigkeit wird berechnet, indem die Gesamtzahl übertragener Byte durch die Zeit vom Anfang bis zum Ende des Prozesses dividiert wird. Sowohl die IBM Spectrum Protect-Verarbeitungszeit als auch die Netzübertragungszeit werden bei der Gesamtübertragungsgeschwindigkeit berücksichtigt. Daher ist die Gesamtübertragungsgeschwindigkeit kleiner als die Datenübertragungsgeschwindigkeit im Netz.  Windows-Betriebssysteme**Hinweis:** Unter Umständen kann die Gesamtdatenübertragungsgeschwindigkeit höher als die Datenübertragungsgeschwindigkeit im Netz sein. Der Grund hierfür ist, dass der Client für Sichern/Archivieren mehrere gleichzeitige Sitzungen mit dem Sicherungsserver haben kann. Wenn Sie die Option resourceutilization definieren, versucht der Client, die Leistung und den Lastausgleich zu verbessern, indem er bei der Sicherung eines Datenträgers oder einer anderen Dateigruppe mehrere Sitzungen verwendet. Sind mehrere Sitzungen bei der Sicherung geöffnet, gibt die Datenübertragungszeit die Summe der von allen Sitzungen berichteten Zeitangaben an. In diesem Fall wird für die Gesamtdatenübertragungszeit fälschlicherweise ein höherer Wert zurückgemeldet. Wird jedoch nur eine einzige Sitzung ausgeführt, sollte für die Gesamtdatenübertragungsgeschwindigkeit immer ein niedrigerer Wert als für die Datenübertragungsgeschwindigkeit im Netz zurückgemeldet werden.  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme Anmerkung: Unter Umständen kann die Gesamtdatenübertragungsgeschwindigkeit höher als die Datenübertragungsgeschwindigkeit im Netz sein. Der Grund hierfür ist, dass der Client für Sichern/Archivieren mehrere gleichzeitige Sitzungen mit dem Sicherungsserver haben kann. Wenn Sie die Option resourceutilization definieren, versucht der Client, die Leistung und den Lastausgleich zu verbessern, indem er bei der Sicherung eines Dateibereichs oder einer anderen Dateigruppe mehrere Sitzungen verwendet. Sind mehrere Sitzungen bei der Sicherung geöffnet, gibt die Datenübertragungszeit die Summe der von allen Sitzungen berichteten Zeitangaben an. In diesem Fall wird für die Gesamtdatenübertragungszeit fälschlicherweise ein höherer Wert zurückgemeldet. Wird jedoch nur eine einzige Sitzung ausgeführt, sollte für die Gesamtdatenübertragungsgeschwindigkeit immer ein niedrigerer Wert als für die Datenübertragungsgeschwindigkeit im Netz zurückgemeldet werden.
`Objekte komprimiert um:`	Gibt den Prozentsatz der über das Netz gesendeten Daten an, geteilt durch die Originalgröße der Datei auf der Platte. Beispiel: Wenn die Netzdatenbyte 10 K betragen und die Datei 100 K groß ist, ist das Ergebnis für "Objekte komprimiert um": == (1 - (10240/102400)) x 100 == 90%.
`Gesamtzahl größer gewordener Objekte:`	Die Gesamtzahl Dateien, die infolge der Komprimierung größer wurden.
`Reduzierung durch Deduplizierung:`	Gibt die Größe der gefundenen doppelten Bereiche an, dividiert durch die ursprüngliche Dateigröße oder Datenmenge. Beispiel: Die ursprüngliche Objektgröße ist 100 MB und die Größe nach der Deduplizierung ist 25 MB. Die Reduzierung beträgt (1 - 25/100) * 100 = 75 %.
`Gesamtverhältnis der Datenreduktion:`	Addiert die Auswirkungen der Teilsicherung und Komprimierung. Beispiel: Die Anzahl der überprüften Byte beträgt 100 MB und die Anzahl der gesendeten Byte beträgt 10 MB. Die Reduzierung beträgt (1 - 10/100) * 100 = 90 %.
`Verarbeitungszeit:`	Die aktive Verarbeitungszeit für die Ausführung eines Befehls. Die Verarbeitungszeit wird berechnet, indem die Startzeit der Befehlsverarbeitung von der Endzeit der beendeten Befehlsverarbeitung abgezogen wird.
`Gesamtanzahl übertragener Byte:`	Wie angezeigt.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme`Übertragene LAN-unabhängige Byte:`	 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-BetriebssystemeDie Anzahl der Datenbyte, die bei einer LAN-unabhängigen Operation übertragen wurden. Ist die Option enablelanfree auf *no* gesetzt, wird diese Zeile nicht ausgegeben.
`Gesamtzahl der überprüften Byte:`	Die Summe der Größe der Dateien, die für die Operation ausgewählt sind.

Informationsnachricht	Bedeutung
`Gesamtzahl Neuversuche:`	Die Gesamtzahl Neuversuche während einer Sicherungsoperation. Abhängig von den Einstellungen für das Nummerierungsattribut und der Option changingretries wird eine Datei, die von einem anderen Prozess geöffnet wird, möglicherweise beim ersten Sicherungsversuch nicht gesichert. Möglicherweise versucht der Client für Sichern/Archivieren während einer Sicherungsoperation mehrmals, eine Datei zu sichern. Diese Nachricht gibt die Gesamtzahl Neuversuche für alle Dateien an, die in die Sicherungsoperation eingeschlossen sind.

 Windows-Betriebssysteme

Sicherung (Windows): Weitere Hinweise

Dieser Abschnitt enthält zusätzliche Informationen, die beim Sichern von Daten berücksichtigt werden müssen.

-  Windows-BetriebssystemeOffene Dateien
  Einige Dateien auf dem System des Benutzers sind möglicherweise im Gebrauch, wenn sie gesichert werden sollen. Diese Dateien werden als *offene Dateien* bezeichnet, weil sie von einer Anwendung für deren exklusive Benutzung gesperrt wurden.
-  Windows-BetriebssystemeMehrdeutige Dateibereichsnamen in Dateispezifikationen
  Haben Sie zwei oder mehr Dateibereiche, bei denen ein Dateibereichsname mit dem Anfang eines anderen Dateibereichsnamens übereinstimmt, ist eine Mehrdeutigkeit vorhanden, wenn eine Zurückschreibung, ein Abruf, eine Abfrage oder eine andere Operation ausgeführt wird, die den Dateibereichsnamen als Teil der Dateispezifikation erfordert.
-  Windows-BetriebssystemeVerwaltungsklassen
  IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden.
-  Windows-BetriebssystemeGelöschte Dateisysteme
  Wenn ein Dateisystem oder Laufwerk gelöscht wurde oder nicht mehr vom Client gesichert wird, werden die vorhandenen Sicherungsversionen für jede Datei gemäß den folgenden Maßnahmenattributen verwaltet: Anzahl Tage für die Aufbewahrung inaktiver Sicherungsversionen und Anzahl Tage für die Aufbewahrung der letzten Sicherungsversion (falls keine aktive Version vorhanden ist).
-  Windows-BetriebssystemeSicherung austauschbarer Datenträger
  Der Client für Sichern/Archivieren sichert austauschbare Datenträger (wie beispielsweise Bänder, Kassetten oder Disketten) auf der Basis der Laufwerkbezeichnung und nicht auf der Basis ds Laufwerkbuchstabens.
-  Windows-BetriebssystemeFestplattenlaufwerke
  Der Client für Sichern/Archivieren kann Festplattenlaufwerke selbst dann sichern, wenn sie über keinen Kennsatz verfügen, einschließlich Laufwerkaliasnamen, die mit dem DOS-Befehl **subst** erstellt wurden. Dies gilt sowohl für den Laufwerkaliasnamen als auch für das zugrunde liegende physische Laufwerk, da der Aliasname und der Kennsatz für das physische Laufwerk identisch sind.
-  Windows-BetriebssystemeNTFS- und ReFS-Dateibereiche
  Wenn Sie Dateien auf NTFS- oder ReFS-Partitionen sichern, sichert der Client auch Dateisicherheitsinformationen und Dateideskriptoren.
-  Windows-BetriebssystemeNamen der allgemeinen Namenskonvention
  Ein UNC-Name (Name, der der allgemeinen Namenskonvention entspricht) ist ein Netzressourcenname für einen Freigabepunkt auf einer Workstation.
-  Windows-BetriebssystemeMethoden für den Schutz von Microsoft DFS-Dateien
  Es stehen einige Methoden zur Verfügung, mit denen Sie die Daten in Ihrer Microsoft DFS-Umgebung schützen können.

 Windows-Betriebssysteme

Offene Dateien

Einige Dateien auf dem System des Benutzers sind möglicherweise im Gebrauch, wenn sie gesichert werden sollen. Diese Dateien werden als *offene Dateien* bezeichnet, weil sie von einer Anwendung für deren exklusive Benutzung gesperrt wurden.

Es ist im Allgemeinen nicht üblich, dass Dateien im gesperrten Modus geöffnet werden. Eine Anwendung kann auf diese Weise eine Datei öffnen, um zu verhindern, dass andere Anwendungen oder Benutzer die Datei lesen oder auf sie zugreifen. Dies kann jedoch bewirken, dass Sicherungsprodukte die Datei für eine Sicherung nicht lesen können.

Möglicherweise ist es nicht immer sinnvoll, die Funktion zur Unterstützung offener Dateien zum Sichern geöffneter oder gesperrter Dateien zu verwenden. Manchmal öffnet eine Anwendung eine Datei oder Dateigruppe in diesem gesperrten Modus, um den Zugriff auf diese Dateien in einem inkonsistenten Status zu verhindern.

Beachten Sie die folgenden Hinweise, um eine höhere Prozessorauslastung beim Erstellen einer Datenträgermomentaufnahme für jede Sicherung zu vermeiden, sowie auf Plattformen, auf denen die Funktion für offene Dateien nicht verfügbar ist oder nicht verwendet wird:

- Handelt es sich um eine Datei, die unwichtig oder leicht wiederherzustellen ist (z. B. eine temporäre Datei), ist eine Sicherung der Datei möglicherweise nicht unbedingt erforderlich. In diesem Fall kann die Datei von der Sicherung ausgeschlossen werden.
- Wenn es sich um eine wichtige Datei handelt:
  - Sicherstellen, dass die Datei geschlossen wird, bevor sie gesichert wird. Werden die Sicherungen nach einem Zeitplan ausgeführt, kann mit der Option preschedulecmd ein Befehl eingegeben werden, der die Datei schließt. Handelt es sich bei der offenen Datei beispielsweise um eine Datenbank, geben Sie einen Befehl zum Schließen der Datenbank ein. Nach Beendigung der Sicherung kann

die Anwendung, die die Datei verwendet, mit der Option postschedulecmd erneut gestartet werden. Wird kein Zeitplan für die Sicherung verwendet, muss die Anwendung, die die Datei verwendet, vor Beginn der Sicherung geschlossen werden.
- Der Client kann die Datei selbst dann sichern, wenn sie während der Sicherung offen ist und geändert wird. Dies ist nur sinnvoll, wenn die Datei noch verwendbar ist, auch wenn sie sich während der Sicherung ändert. Damit diese Dateien gesichert werden, muss ihnen eine Verwaltungsklasse mit der Durchnummerierung *Dynamisch* oder *Gemeinsam dynamisch* zugeordnet werden.

Anmerkung: Wenn die Unterstützung offener Dateien nicht konfiguriert ist: Der Client versucht zwar, offene Dateien zu sichern; dies ist jedoch nicht immer möglich. Einige Dateien sind ausschließlich für die Anwendung offen, von der sie geöffnet wurden. Wenn der Client eine derartige Datei findet, kann er die Datei zu Sicherungszwecken nicht lesen. Sind Ihnen solche Dateitypen in Ihrer Umgebung bekannt, sollten sie von der Sicherung ausgeschlossen werden, um die Anzeige von Fehlernachrichten in der Protokolldatei zu vermeiden.

Zugehörige Konzepte:
Informationen zu Verwaltungsklassen und Kopiengruppen anzeigen
Verwaltungsklasse für Dateien auswählen
Windows-Betriebssysteme

Mehrdeutige Dateibereichsnamen in Dateispezifikationen

Haben Sie zwei oder mehr Dateibereiche, bei denen ein Dateibereichsname mit dem Anfang eines anderen Dateibereichsnamens übereinstimmt, ist eine Mehrdeutigkeit vorhanden, wenn eine Zurückschreibung, ein Abruf, eine Abfrage oder eine andere Operation ausgeführt wird, die den Dateibereichsnamen als Teil der Dateispezifikation erfordert.

Betrachten Sie beispielsweise die folgenden Dateibereiche und die Sicherungskopien, die darin enthalten sind:

Dateibereichsname	Dateiname
\\storman\home	amr\project1.doc
\\storman\home\amr	project2.doc

Beachten Sie, dass der Name des ersten Dateibereichs, \\storman\home, mit dem Anfang des Namens des zweiten Dateibereichs, \\storman\home\amr, übereinstimmt. Wenn Sie die Befehlszeilenschnittstelle des Clients für Sichern/Archivieren verwenden, um eine Datei aus einem dieser Dateibereiche zurückzuschreiben oder abzufragen, gleicht der Client standardmäßig den längsten Dateibereichsnamen in der Dateispezifikation (in diesem Beispiel \\storman\home\amr) ab. Um mit Dateien in dem Dateibereich mit dem kürzeren Namen (\\storman\home) zu arbeiten, schließen Sie den Teil des Dateibereichsnamens der Dateispezifikation in geschweifte Klammern ein.

Dies bedeutet, dass der folgende Abfragebefehl project2.doc findet, aber project1.doc nicht findet:

```
dsmc query backup "\\storman\home\amr\*"
```

Dies liegt daran, dass der längere der beiden Dateibereichsnamen \\storman\home\amr ist und dieser Dateibereich die Sicherung für project2.doc enthält.

Um project1.doc zu finden, schließen Sie den Dateibereichsnamen in geschweifte Klammern ein. Der folgende Befehl findet project1.doc, aber nicht project2.doc:

```
dsmc query backup "{\\storman\home}\amr\*"
```

Genauso schreibt der folgende Befehl project1.doc, aber nicht project2.doc zurück:

```
dsmc restore {\\storman\home}\amr\project1.doc
```
 Windows-Betriebssysteme

Verwaltungsklassen

IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden.

Bei jeder Sicherung einer Datei wird ihr eine Verwaltungsklasse zugeordnet. Bei der verwendeten Verwaltungsklasse kann es sich um die Standardverwaltungsklasse handeln, die Ihnen zugeordnet wird, oder um eine Verwaltungsklasse, die Sie der Datei mit der Option include in der Einschluss-/Ausschlussoptionsliste zuordnen. Die ausgewählte Verwaltungsklasse muss eine Sicherungskopiengruppe enthalten, damit die Datei gesichert wird.

Wählen Sie **Dienstprogramme** → **Maßnahmeninformationen anzeigen** in der GUI des Clients für Sichern/Archivieren oder des Web-Clients aus, um die Sicherungsstrategien anzuzeigen, die vom IBM Spectrum Protect-Server für Ihren Clientknoten definiert wurden.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
Zugehörige Tasks:
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren
 Windows-Betriebssysteme

Gelöschte Dateisysteme

Wenn ein Dateisystem oder Laufwerk gelöscht wurde oder nicht mehr vom Client gesichert wird, werden die vorhandenen Sicherungsversionen für jede Datei gemäß den folgenden Maßnahmenattributen verwaltet: Anzahl Tage für die Aufbewahrung inaktiver Sicherungsversionen und Anzahl Tage für die Aufbewahrung der letzten Sicherungsversion (falls keine aktive Version vorhanden ist).

Wenn Sie nichts weiter unternehmen, verbleiben aktive Sicherungsversionen unbegrenzt. Falls Sie die aktiven Versionen nicht unbegrenzt aufbewahren müssen, können Sie mit dem Befehl expire die aktiven Versionen inaktivieren.

Sie können auch den Befehl delete backup verwenden, um einzelne Sicherungsversionen zu löschen, oder den Befehl delete filespace, um den gesamten Dateibereich zu löschen. Ihr IBM Spectrum Protect-Serveradministrator muss Ihnen die Berechtigung "delete backup" erteilen, damit Sie diese Befehle verwenden können. Enthält der Dateibereich auch Archivierungsversionen, müssen Sie außerdem die Berechtigung zum Löschen von Archivierungen haben, um delete filespace verwenden zu können.

Mithilfe des Befehls query session können Sie feststellen, ob Sie die Berechtigung "delete backup" und "delete archive" besitzen. Alternativ dazu können Sie Ihren IBM Spectrum Protect-Serveradministrator bitten, den Dateibereich für Sie zu löschen.

Das Löschen eines Dateisystems hat keine Auswirkungen auf vorhandene Archivierungsversionen. Wenn Sie jedoch die Archivierungsversionen nicht mehr benötigen, können Sie mit den Befehlen delete archive oder delete filespace Archivierungen löschen.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
Windows-Betriebssysteme

Sicherung austauschbarer Datenträger

Der Client für Sichern/Archivieren sichert austauschbare Datenträger (wie beispielsweise Bänder, Kassetten oder Disketten) auf der Basis der Laufwerkbezeichnung und nicht auf der Basis ds Laufwerkbuchstabens.

Verfügt ein Laufwerk über keine Bezeichnung, erfolgt keine Sicherung. Die Verwendung von Laufwerkbezeichnungen ermöglicht beispielsweise das Sichern verschiedener Disketten aus dem Laufwerk `a:`.

Für eine Zurückschreibung oder einen Abruf wird ein separater Dateibereich für jede Laufwerkbezeichnung verwaltet. Diese Bezeichnungen werden zu den Namen der Dateibereiche auf dem IBM Spectrum Protect-Server. Wenn Sie die Bezeichnung eines bereits gesicherten Laufwerks ändern, betrachtet der Client das Laufwerk als neues Laufwerk, ohne es mit dem bereits vorhandenen Laufwerk in Zusammenhang zu bringen.

Da der Client die Bezeichnungen für die Verwaltung der Sicherungen und Archivierungen Ihrer austauschbaren Datenträger verwendet, müssen Sie diese Bezeichnungen gelegentlich zur Suche nach Daten verwenden, wenn Befehle verwendet werden. Soll beispielsweise eine Datei auf Diskette oder DVD–ROM mit dem Dateinamen `d:\projx\file.exe` zurückgeschrieben werden, ersetzt IBM Spectrum Protect das `d:` durch die aktuelle Bezeichnung des Laufwerks `d:`. Lautet die Laufwerkbezeichnung `d:` wie folgt: `d-disk`, wird `d:\projx\file.exe` durch `{d-disk}\projx\file.exe` ersetzt und die Bezeichnung wird in geschweifte Klammern eingeschlossen.

Entspricht die Bezeichnung des Laufwerks `d:` keinem Dateibereichsnamen auf dem Server, kann IBM Spectrum Protect die Dateien mithilfe der aktuellen Bezeichnung des Laufwerks `d:` nicht finden. Der Client kann die Dateien jedoch finden, wenn Sie den Dateibereichsnamen auf der Basis der ursprünglichen Laufwerkbezeichnung verwenden. Eine fehlende Übereinstimmung zwischen einer Bezeichnung und einem Dateibereichsnamen ist möglich, wenn die Laufwerkbezeichnungen geändert werden oder wenn auf IBM Spectrum Protect von einer anderen Workstation zugegriffen wird, als die, von der die Dateien gesichert wurden. Wurde die Laufwerkbezeichnung nicht geändert und befindet sich der Benutzer an derselben Workstation, von der die Datei gesichert wurde, kann der Laufwerkbuchstabe als Abkürzung für den Dateibereichsnamen (Laufwerkbezeichnung) verwendet werden.

 Windows-Betriebssysteme

Festplattenlaufwerke

Der Client für Sichern/Archivieren kann Festplattenlaufwerke selbst dann sichern, wenn sie über keinen Kennsatz verfügen, einschließlich Laufwerkaliasnamen, die mit dem DOS-Befehl **subst** erstellt wurden. Dies gilt sowohl für den Laufwerkaliasnamen als auch für das zugrunde liegende physische Laufwerk, da der Aliasname und der Kennsatz für das physische Laufwerk identisch sind.

 Windows-Betriebssysteme

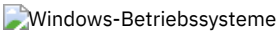
NTFS- und ReFS-Dateibereiche

Wenn Sie Dateien auf NTFS- oder ReFS-Partitionen sichern, sichert der Client auch Dateisicherheitsinformationen und Dateideskriptoren.

Die folgenden Dateideskriptoren werden gesichert:

- Eignersicherheitsinformationen (SID)
- Primärgruppen-SID
- Eignerdefinierte Zugriffssteuerungsliste
- Systemzugriffssteuerungsliste

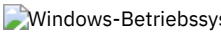
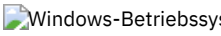
Sie müssen einen Dateibereichsnamen in Groß-/Kleinschreibung oder in Kleinschreibung angeben, der zwischen Anführungszeichen und geschweiften Klammern steht. Zum Beispiel `{"NTFSDrive"}`. Hochkommas oder Anführungszeichen sind im Schleifenmodus gültig. Beispielsweise ist sowohl `{"NTFSDrive"}` als auch `{'NTFSDrive'}` gültig. Im Stapelmodus sind nur Hochkommas gültig. Die Einschränkung auf Hochkommas ist im Betriebssystem begründet.

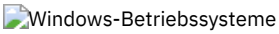

Windows-Betriebssysteme

Namen der allgemeinen Namenskonvention

Ein UNC-Name (Name, der der allgemeinen Namenskonvention entspricht) ist ein Netzressourcenname für einen Freigabepunkt auf einer Workstation.

Der Ressourcenname umfasst den der Workstation zugeordneten Einheitennamen und einen Namen, den der Benutzer einem Laufwerk oder Verzeichnis zuordnet, damit es gemeinsam benutzt werden kann. Der vom Benutzer zugeordnete Name wird auch als *Name des Freigabepunkts* bezeichnet.

- 
Windows-BetriebssystemeBeispiele: UNC-Namen in Domänenlisten
Dieser Abschnitt enthält einige Beispiele für die Verwendung von UNC-Namen zur Angabe einer Domänenliste.
- 
Windows-BetriebssystemeBeispiele: Sicherung unter Verwendung der allgemeinen Namenskonvention
Gemeinsam benutzte Dateien in einem Netz können unter Verwendung von Namen, die der allgemeinen Namenskonvention entsprechen, (UNC-Namen) gesichert werden. Dieser Abschnitt enthält einige Beispiele für das Sichern von Dateien mit UNC-Namen (UNC - Universal Naming Convention, allgemeine Namenskonvention).


Windows-Betriebssysteme

Beispiele: UNC-Namen in Domänenlisten

Dieser Abschnitt enthält einige Beispiele für die Verwendung von UNC-Namen zur Angabe einer Domänenliste.

Informationen zu diesem Vorgang

Sie müssen die folgenden Informationen angeben:

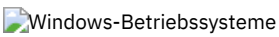
- Ein Laufwerkbuchstabe für austauschbare Datenträger
- Laufwerkbuchstaben oder der allgemeinen Namenskonvention entsprechender Name für lokale Festplattenlaufwerke
- Laufwerkbuchstaben oder der allgemeinen Namenskonvention entsprechender Name für ferne, zugeordnete Laufwerke
- Der allgemeinen Namenskonvention entsprechende Namen für ferne, nicht zugeordnete Laufwerke

Beispiel 1: Um Laufwerk a: mit einem austauschbaren Datenträger anzugeben, Folgendes eingeben:

```
domain a: \\local\c$
```

Beispiel 2: Um Festplattenlaufwerk c: anzugeben, Folgendes eingeben:

```
domain c: \\remote\share1 \\remote\c$
```


Windows-Betriebssysteme

Beispiele: Sicherung unter Verwendung der allgemeinen Namenskonvention

Gemeinsam benutzte Dateien in einem Netz können unter Verwendung von Namen, die der allgemeinen Namenskonvention entsprechen, (UNC-Namen) gesichert werden. Dieser Abschnitt enthält einige Beispiele für das Sichern von Dateien mit UNC-Namen (UNC - Universal Naming Convention, allgemeine Namenskonvention).

Ein Name, der der allgemeinen Namenskonvention entspricht, ist ein Netzressourcenname für einen Freigabepunkt auf einer Workstation. Der Ressourcenname umfasst den der Workstation zugeordneten Einheitennamen und einen Namen, den der Benutzer einem Laufwerk oder Verzeichnis zuordnet, damit es gemeinsam benutzt werden kann. Der vom Benutzer zugeordnete Name wird auch als Name des Freigabepunkts bezeichnet.

Unter Verwendung eines Namens, der der allgemeinen Namenskonvention entspricht, können bestimmte gemeinsam benutzte Verzeichnisse in einem separaten Dateibereich gesichert werden. Dies ist nützlich, wenn ein Benutzer oder Administrator einen kleinen Teil von Daten sichern will, auf den sonst nicht zugegriffen werden könnte. Laufwerke werden nicht in einem separaten Dateibereich gesichert.

Der Zugriff auf alle lokalen Laufwerke ist mithilfe einer allgemeinen Namenskonvention (UNC-Namen) möglich, mit Ausnahme von Laufwerken mit austauschbaren Datenträgern (z. B. Bänder, Bandkassetten oder Disketten). Der Zugriff auf diese Laufwerke ist mithilfe eines vordefinierten gemeinsamen Verwaltungsnamens möglich, der aus dem Workstationnamen, dem lokalen Laufwerkbuchstaben und dem Zeichen `$` besteht. Um beispielsweise auf Laufwerk `c:` für die Workstation `ocean` einen Namen anzugeben, der der allgemeinen Namenskonvention entspricht, Folgendes eingeben:

```
\\ocean\c$
```

Das Zeichen `$` *muss* dem Laufwerkbuchstaben hinzugefügt werden.

Um für die Workstation `ocean` und den Freigabepunkt `wave` einen UNC-Namen anzugeben, geben Sie Folgendes ein:

```
\\ocean\wave
```

Beim Zugriff auf Dateien muss der Laufwerkbuchstabe nur für Laufwerke mit austauschbaren Datenträgern eingegeben werden.

Die in der folgenden Tabelle enthaltenen Beispiele zeigen die selektive Sicherung von Dateien unter Verwendung von Namen, die der allgemeinen Namenskonvention entsprechen. Für diese Beispiele gelten folgende Voraussetzungen:

- Die Workstation, auf der **dsmc** ausgeführt wird, ist `major`.
- Die gemeinsamen Namen `betarc` und `testdir` von der Workstation `alpha1` werden dem Laufwerk r bzw. t zugeordnet.

Tabelle 1. Beispiele für die allgemeine Namenskonvention

Beispiel	Kommentar
`dsmc sel \\alpha1\c$\`	Name des fernen Dateibereichs ist `\\alpha1\c$`
`dsmc sel \\major\c$\`	Name des lokalen, festen Dateibereichs ist `\\major\c$`
`dsmc sel a:\`	Name des lokalen, austauschbaren Dateibereichs ist Datenträgerkennsatz von `a:`
`dsmc sel \\alpha1\betarc\`	Name des fernen Dateibereichs ist `\\alpha1\betarc`
`dsmc sel \\alpha1\testdir\`	Name des fernen Dateibereichs ist `\\alpha1\testdir`
`dsmc sel d:\`	Name des lokalen, festen Dateibereichs ist `\\major\d$`
`dsmc sel c:\`	Dateibereichsname ist `\\major\c$`
`dsmc sel r:\`	Dateibereichsname ist `\\alpha1\betarc`

Sie können der allgemeinen Namenskonvention entsprechende Namen auch für Dateien in Ihrer Einschluss-/Ausschluss- und Domänenliste angeben.

Zugehörige Tasks:
Einschluss-/Ausschlussliste erstellen
Zugehörige Verweise:
Domain
Windows-Betriebssysteme

Methoden für den Schutz von Microsoft DFS-Dateien

Es stehen einige Methoden zur Verfügung, mit denen Sie die Daten in Ihrer Microsoft DFS-Umgebung schützen können.

Informationen zu diesem Vorgang

Die folgenden Methoden sollten Sie verwenden, um Ihre Microsoft DFS-Daten zu schützen:

Vorgehensweise

1. Sichern Sie von der Workstation, auf der sich der DFS-Stamm befindet, die DFS-Verknüpfungsmetadaten und die eigentlichen Daten auf dem von jeder Verknüpfung gemeinsam genutzten Ziel. Durch diese Methode wird das Sichern und Zurückschreiben vereinfacht, da alle IBM Spectrum Protect-Aktivitäten auf einer einzelnen Workstation konsolidiert werden. Der Nachteil dieser Methode besteht darin, dass bei der Sicherung eine zusätzliche Netzübertragung erforderlich ist, um auf die Daten zugreifen zu können, die auf den Verknüpfungszielen gespeichert sind.
2. Sichern Sie nur die DFS-Verknüpfungsmetadaten, die für die Workstation, auf der sich der DFS-Stamm befindet, lokal sind. Sichern Sie von der Workstation aus, für die die Daten lokal sind, auch die Daten auf dem Ziel jeder Verknüpfung. Durch diese Methode wird die Sicherungs- und Zurückschreibungsleistung verbessert, da die zusätzliche Netzübertragung entfällt; sie erfordert jedoch die Koordination von Sicherungs- und Zurückschreibungsoperationen auf mehreren Workstations.

Ergebnisse

Anmerkung:

1. Die README-Datei des Produkts enthält die aktuellen Einschränkungen dieser Funktion.

Auf Dateien, die sich in einer DFS-Serverkomponente befinden, wird mithilfe von Standardnamen, die der allgemeinen Namenskonvention entsprechen, zugegriffen. Zum Beispiel:

```
\\servername\dfsroot\
```

Hierbei ist servername der Name des Hosts und dfsroot ist der Name des DFS-Stamms.

Wenn Sie die Option dfsbackupmntpnt auf *yes* (den Standardwert) setzen, traversiert eine Teilsicherung eines DFS-Stamms nicht die DFS-Zusammenführungen. Es werden nur die Metadaten der Zusammenführung gesichert. Dies ist die empfohlene Einstellung, damit der Client verwendet werden kann, um die DFS-Verknüpfungen zurückzuschreiben.

Mithilfe der Option dfsbackupmntpnt können Sie angeben, ob der Client einen DFS-Mountpunkt als Microsoft DFS-Zusammenführung oder als Verzeichnis ansieht.

Wichtig: Schreiben Sie die Metadaten der DFS-Zusammenführung zuerst zurück. Dadurch werden die Verknüpfungen erneut erstellt. Schreiben Sie danach die einzelnen Zusammenführungen und die Daten auf den einzelnen Zusammenführungen separat zurück. Wenn Sie die Metadaten der Zusammenführung nicht zuerst zurückschreiben, erstellt der Client ein Verzeichnis unter dem DFS-Stamm mit dem Namen des Zusammenführungspunkts und schreibt die Daten in dieses Verzeichnis zurück.
Das folgende Beispiel bezieht sich auf Methode 1 (siehe oben) und veranschaulicht, wie Sie mithilfe des Clients eine Microsoft-DFS-Umgebung sichern und zurückschreiben können. Es wird davon ausgegangen, dass eine DFS-Domänenumgebung vorhanden ist, die von der Workstation `wkst1` gehostet wird:

DFS-Stamm
    \\wkst1\abc64test
DFS-Verknüpfung1
    \\wkst1\abc64test\tools
DFS-Verknüpfung2
    \\wkst1\abc64test\trees

Sicherungsprozedur:

1. Setzen Sie die Option dfsbackupmntpnt in Ihrer Clientoptionsdatei (dsm.opt) auf *yes*.
2. Geben Sie den folgenden Befehl ein, um die Informationen der Verknüpfungszusammenführungen zu sichern:

   ```
   dsmc inc \\wkst1\abc64test
   ```

3. Geben Sie den folgenden Befehl ein, um die Daten der Verknüpfung tools zu sichern:

   ```
   dsmc inc \\wkst1\abc64test\tools
   ```

4. Geben Sie den folgenden Befehl ein, um die Daten der Verknüpfung trees zu sichern:

   ```
   dsmc inc \\wkst1\abc64test\trees
   ```

Anmerkung: Die DFS-Replizierung verwendet Ordner zum Zwischenspeichern, um als Cache für neue und geänderte Dateien zu agieren, die von sendenden Mitgliedern an empfangende Mitglieder repliziert werden. Wenn Sie diese Dateien nicht sichern wollen, können Sie sie mit der Option exclude.dir aus Ihrer Sicherung ausschließen.

```
exclude.dir x:\...\Dfsrprivate
```

Zurückschreibungsprozedur:

1. Erstellen Sie Freigaben nur dann erneut auf den Zielworkstations, wenn sie nicht mehr vorhanden sind.
2. Erstellen Sie den DFS-Stamm mit exakt demselben Namen erneut, der zum Zeitpunkt der Sicherung definiert war.
3. Geben Sie den folgenden Befehl ein, um Daten der Verknüpfung tools wiederherzustellen. Dieser Schritt ist nicht erforderlich, wenn die Daten noch am Verknüpfungsziel vorhanden sind:

   ```
   dsmc restore \\wkst1\abc64test\tools\* -sub=yes
   ```

4. Geben Sie den folgenden Befehl ein, um Daten der Verknüpfung trees wiederherzustellen. Dieser Schritt ist nicht erforderlich, wenn die Daten noch am Verknüpfungsziel vorhanden sind:

   ```
   dsmc restore \\wkst1\abc64test\trees\* -sub=yes
   ```

5. Verwenden Sie das Snap-in der Verwaltungskonsole des verteilten Dateisystems, um bei Bedarf die Replikation für jede einzelne Verknüpfung wiederherzustellen.

Für die Zurückschreibung von Microsoft DFS-Daten gelten die folgenden Einschränkungen:

- Der Client schreibt nicht den DFS-Stamm zurück. Um die DFS-Baumstruktur erneut zu erstellen, müssen Sie zuerst den DFS-Stamm manuell erstellen und anschließend die Zurückschreibung starten, um die Verknüpfungen wiederherzustellen.
- Der Client kann nur die DFS-Baumstruktur (sowohl von DFS auf Domänenbasis als auch von eigenständigem DFS) sichern, die sich auf der lokalen Workstation befindet. Sie können das DFS nicht sichern, wenn der DFS-Host-Server nicht Ihre lokale Workstation ist.
- Der Client kann beim Zurückschreiben keine gemeinsam genutzten Ordner erneut erstellen. Wenn Sie beispielsweise die Zusammenführung und den gemeinsam genutzten Ordner löschen, auf den die Zusammenführung verweist, wird beim Zurückschreiben des DFS-Stamms die DFS-Zusammenführung erneut erstellt; beim Zurückschreiben einer Zusammenführung wird jedoch anstelle des ursprünglich gesicherten gemeinsam genutzten Netzordners ein lokaler Ordner erstellt.

- Wenn eine DFS-Verknüpfung mit einem Replikat erstellt wird und sich das gemeinsam genutzte Replikat auf einem anderen Server befindet, zeigt der Client die Replikatdaten nicht an.
- Wird ein DFS-Stamm hinzugefügt oder geändert, wird er vom Client nicht gesichert. Sie müssen den DFS-Stamm in der Option domain in der Clientoptionsdatei (dsm.opt) angeben und zwar unabhängig davon, ob DOMAIN ALL-LOCAL angegeben ist.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Sicherung (UNIX und Linux): Weitere Hinweise

Sie sollten einige besondere Situationen bedenken, bevor Sie Ihre Daten sichern.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeGespeicherte Dateien
  Werden Dateien gesichert und archiviert, speichert IBM Spectrum Protect die Sicherungen und Archivierungen in einem Dateibereich im Speicher, der denselben Namen wie das Dateisystem oder der virtuelle Mountpunkt hat, aus dem die Dateien stammen.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSpezielle Dateisysteme
  Spezielle Dateisysteme enthalten dynamische Informationen, die vom Betriebssystem generiert werden; sie enthalten jedoch keine Daten oder Dateien. Der Client für Sichern/Archivieren ignoriert spezielle Dateisysteme und ihren Inhalt.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeNFS- oder virtuelle Mountpunkte
  Wenn Dateien von einem Dateisystem oder virtuellen Mountpunkt gesichert und archiviert werden, folgt der Client nicht den verschachtelten NFS- oder virtuellen Mountpunkten (sofern derartige Mountpunkte in einem Dateisystem definiert sind). Die verschachtelten NFS- oder virtuellen Mountpunkte werden nicht gesichert oder archiviert.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeVerwaltungsklassen
  IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSymbolische Verbindungen sichern
  Der Client für Sichern/Archivieren verfährt beim Sichern symbolischer Verbindungen anders als bei regulären Dateien und Verzeichnissen.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeFeste Verbindungen
  Wenn Sie Dateien sichern, die fest verbunden sind, sichert der Client für Sichern/Archivieren jede Instanz der fest verbundenen Datei.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDateien mit freien Bereichen
  Dateien mit freien Bereichen haben keinen Plattenspeicherplatz für jeden Block im gesamten Adressraum zugeordnet, was zu freien Datenbereichen innerhalb der Datei führt. Freie Datenbereiche werden durch ihren Inhalt erkannt, der immer Null ist, und diese Nullen nehmen Speicherplatz ein.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAbsolute und bedingte NFS-Mounts
  Wenn der Client für Sichern/Archivieren die Verbindung zu einem NFS-Dateisystem herstellt, kann entweder ein absoluter Mount oder ein bedingter Mount verwendet werden.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeGelöschte Dateisysteme
  Wenn ein Dateisystem oder Laufwerk gelöscht wurde oder nicht mehr vom Client für Sichern/Archivieren gesichert wird, werden die vorhandenen Sicherungsversionen für jede Datei gemäß den folgenden Maßnahmenattributen verwaltet: Anzahl Tage für die Aufbewahrung inaktiver Sicherungsversionen und Anzahl Tage für die Aufbewahrung der letzten Sicherungsversion (falls keine aktive Version vorhanden ist).
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeGeöffnete Dateien
  Der Client für Sichern/Archivieren sucht nach Dateien, die sich zwischen dem Start und dem Ende der Dateisicherung geändert haben.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemePlatzhalterzeichen
  Beim Client für Sichern/Archivieren können die Platzhalterzeichen des Betriebssystems in Dateispezifikationen verwendet werden. Mithilfe dieser Zeichen können Gruppen von Dateien mit ähnlichen Namen ausgewählt werden.

Mac OS X-BetriebssystemeMac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Gespeicherte Dateien

Werden Dateien gesichert und archiviert, speichert IBM Spectrum Protect die Sicherungen und Archivierungen in einem Dateibereich im Speicher, der denselben Namen wie das Dateisystem oder der virtuelle Mountpunkt hat, aus dem die Dateien stammen.

Ist beispielsweise ein Dateisystem mit dem Namen `/home` vorhanden und wird eine Datei mit dem Namen `doc1` im Verzeichnis `/home/monnett` gesichert, speichert IBM Spectrum Protect die Datei in einem Dateibereich mit dem Namen `/home`. Wenn Sie `/home/monnett` später als virtuellen Mountpunkt definieren, werden alle Dateien, die aus dem Verzeichnis `/home/monnett` gesichert werden (z. B. `doc2`), in einem Dateibereich mit dem Namen `/home/monnett` gespeichert. Bei Eingabe des Befehls

```
dsmc query backup "/home/monnett/*"
```

sucht IBM Spectrum Protect nach Dateien in dem Dateibereich `/home/monnett`. Es wird immer nach einer Datei in dem Dateibereich mit dem längsten Namen gesucht, der mit der Dateispezifikation übereinstimmt, die in einem Befehl angegeben wird. Das Programm findet die Datei mit dem Namen `doc2`, die gesichert wurde, nachdem der virtuelle Mountpunkt definiert wurde. Die Datei `doc1` wird jedoch nicht gefunden, da diese Datei gesichert wurde, bevor der virtuelle Mountpunkt definiert wurde und die Sicherung in dem Dateibereich `/home` gespeichert wurde.

Um die Datei `doc1` mithilfe eines Befehls aufzulisten oder zurückzuschreiben, muss der Name des Dateibereichs explizit angegeben werden, indem er in geschweifte Klammern eingeschlossen wird. Beispiel:

```
dsmc query backup "{/home}/monnett/*"
   dsmc restore {/home}/monnett/doc1
```

Wenn Sie anschließend den virtuellen Mountpunkt `/home/monnett` entfernen und dann weitere Dateien in dem Verzeichnis `/home/monnett` sichern, werden die Sicherungen erneut in dem Dateibereich `/home` gespeichert. Wird beispielsweise jetzt eine Datei mit dem Namen `doc3` im Verzeichnis `/home/monnett` gesichert, wird sie in dem Dateibereich `/home` gespeichert. Sie wird nicht in dem vorhandenen Dateibereich `/home/monnett` gespeichert.

Da jedoch der Dateibereich `/home/monnett` bei dem Versuch, die Datei `doc3` abzufragen oder zurückzuschreiben, bereits vorhanden ist, sucht IBM Spectrum Protect in dem Dateibereich `/home/monnett` nach der Datei, es sei denn, der korrekte Dateibereichsname wird angegeben. Zum Beispiel:

```
dsmc query backup "{/home}/monnett/*"
   dsmc restore {/home}/monnett/doc2
```

Anmerkung: Der Dateibereichsname muss nur dann explizit angegeben werden, wenn die eingegebene Dateispezifikation mehrere Auflösungen zulässt.

Sind z. B. die Dateibereiche

```
/home
   /home/monnett
   /home/monnett/project1
   /home/monnett/project1/planning
```

im Speicher vorhanden, Folgendes eingeben:

```
dsmc query backup "/home/monnett/project1/planning/*"
```

IBM Spectrum Protect sucht nur in dem Dateibereich `/home/monnett/project1/planning` nach Dateien, auch wenn einer oder mehrere der anderen Dateibereiche einen Pfad mit demselben Namen enthalten. Wird aber einer der folgenden Befehle eingegeben:

```
dsmc query backup "{/home}/monnett/project1/planning/*"
   dsmc query backup "{/home/monnett}/project1/planning/*"
   dsmc query backup "{/home/monnett/project1}/planning/*"
```

sucht IBM Spectrum Protect nur im Dateibereich `/home`, im Dateibereich `/home/monnett` oder im Dateibereich `/home/monnett/project1` nach Dateien, je nach verwendeter Form.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Spezielle Dateisysteme

Spezielle Dateisysteme enthalten dynamische Informationen, die vom Betriebssystem generiert werden; sie enthalten jedoch keine Daten oder Dateien. Der Client für Sichern/Archivieren ignoriert spezielle Dateisysteme und ihren Inhalt.

Spezielle Dateisysteme umfassen Folgendes:

- Das Dateisystem `/proc` auf den meisten UNIX-Plattformen
- Das Dateisystem `/dev/fd` unter Solaris
- `/dev/pts` unter Linux

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

NFS- oder virtuelle Mountpunkte

Wenn Dateien von einem Dateisystem oder virtuellen Mountpunkt gesichert und archiviert werden, folgt der Client nicht den verschachtelten NFS- oder virtuellen Mountpunkten (sofern derartige Mountpunkte in einem Dateisystem definiert sind). Die verschachtelten NFS- oder virtuellen Mountpunkte werden nicht gesichert oder archiviert.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Verwaltungsklassen

IBM Spectrum Protect bestimmt mithilfe von Verwaltungsklassen, wie die Sicherungen auf dem Server verwaltet werden.

Bei jeder Sicherung einer Datei wird ihr eine Verwaltungsklasse zugeordnet. Bei der verwendeten Verwaltungsklasse kann es sich um die Standardverwaltungsklasse handeln oder um eine Verwaltungsklasse, die der Datei mit der Option include in der Einschluss-/Ausschlussoptionsliste zugeordnet wird. Die ausgewählte Verwaltungsklasse muss eine Sicherungskopiengruppe enthalten, damit die Datei gesichert wird.

Wählen Sie **Dienstprogramme** → **Maßnahmeninformationen anzeigen** in der Java™-GUI oder der Web-Client-GUI aus, um die Sicherungsmaßnahmen anzuzeigen, die vom IBM Spectrum Protect-Server für Ihren Clientknoten definiert wurden.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Symbolische Verbindungen sichern

Der Client für Sichern/Archivieren verfährt beim Sichern symbolischer Verbindungen anders als bei regulären Dateien und Verzeichnissen.

Wie der Client symbolische Verbindungen sichert, ist von Optionseinstellungen, von der Verfügbarkeit des Zielverzeichnisses und von der Angabe der Objekte abhängig.

Eine *symbolische Verbindung ist unter UNIX* eine Datei, die einen Zeiger auf eine andere Datei oder ein anderes Verzeichnis enthält. Das Objekt, auf das die symbolische Verbindung zeigt, wird als Zielobjekt bezeichnet.

Eine symbolische Verbindung kann entweder als Pfadangabe für das Zielverzeichnis oder als Verzeichnis gesichert werden. Wird die symbolische Verbindung als Verzeichnis gesichert, können auch die Dateien und Ordner im Zielverzeichnis gesichert werden.

Anmerkung: Die hier beschriebene Verarbeitung symbolischer Verbindungen gilt nicht für Mac OS X. Symbolische Verbindungen werden immer als Dateien gesichert und den Zeigern wird nicht gefolgt.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeBeispiele: Teilsicherung oder selektive Sicherung von symbolischen Verbindungen
  Wie der Client eine symbolische Verbindung sichert, ist davon abhängig, ob das Ziel der symbolischen Verbindung eine Datei oder ein Verzeichnis ist und wie Sie die symbolische Verbindung in dem Befehl für die Teilsicherung oder selektive Sicherung angeben.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTeilsicherung nur für eine Domäne
  Der Client sichert eine symbolische Verbindung während einer Teilsicherung der Domäne, wenn die symbolische Verbindung als virtueller Mountpunkt definiert und die Option followsymbolic auf yes gesetzt ist.

Zugehörige Verweise:
Archsymlinkasfile
Followsymbolic
Virtualmountpoint
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Beispiele: Teilsicherung oder selektive Sicherung von symbolischen Verbindungen

Wie der Client eine symbolische Verbindung sichert, ist davon abhängig, ob das Ziel der symbolischen Verbindung eine Datei oder ein Verzeichnis ist und wie Sie die symbolische Verbindung in dem Befehl für die Teilsicherung oder selektive Sicherung angeben.

Wenn eine symbolische Verbindung auf eine Datei zeigt, sichert der Client nur die Pfadangabe. Der Client sichert keine Datei, die das Ziel einer symbolischen Verbindung ist.

Wenn eine symbolische Verbindung auf ein Verzeichnis zeigt, ist die Sicherung davon abhängig, wie das Verzeichnis im Befehl angegeben ist.

Wird ein Verzeichnis in einem Befehl für selektive Sicherung oder Teilsicherung mit einem abschließenden Schrägstrich angegeben, sichert der Client die symbolische Verbindung als Verzeichnis und sichert den Inhalt des Zielverzeichnisses.

Wird die symbolische Verbindung ohne abschließenden Schrägstrich eingegeben oder wird eine symbolische Verbindung nicht explizit in einer Dateispezifikation für die Sicherung angegeben, sichert der Client nur die Pfadangabe für das Zielverzeichnis. Der Inhalt des Zielverzeichnisses wird nicht gesichert.

Für die folgenden Beispiele wird angenommen, dass `symdir` eine symbolische Verbindung zu dem Zielverzeichnis `/fs1/guest/` ist. `/fs1/guest/` enthält die folgenden Objekte:

- `/fs1/guest/file` (eine Datei)
- `/fs1/guest/dir1` (ein Verzeichnis)
- `/fs1/guest/dir1/file1` (eine Datei)

Beispiel 1
```
dsmc incr /home/gillis/symdir/
```

In diesem Beispiel sichert der Client die symbolische Verbindung als Verzeichnis und sichert den Inhalt des Zielverzeichnisses `/fs1/guest/`. Wenn Sie die Option subdir=yes angeben, sichert der Client die Unterverzeichnisse von `/fs1/guest/`.

Beispiel 2
```
dsmc incr /home/gillis/symdir/dir1
```
Beispiel 3
```
dsmc incr /home/gillis/symdir/dir1/
```

In Beispiel 2 und Beispiel 3 sichert der Client die symbolische Verbindung als Verzeichnis und sichert das Unterverzeichnis `/dir1/` des Zielverzeichnisses. Der abschließende Schrägstrich ist nur für die symbolische Verbindung relevant; er ist bei den Unterverzeichnissen der symbolischen Verbindung unerheblich. Wenn Sie die Option subdir=yes angeben, sichert der Client Unterverzeichnisse des Verzeichnisses `/fs1/guest/dir1`. Auf dem IBM Spectrum Protect-Server gespeicherte Sicherungskopien haben den Pfad `/home/gillis/symdir/dir1/file1`.

Beispiel 4

```
dsmc incr /home/gillis/symdir
```

In Beispiel 4 sichert der Client nur den Pfad zu dem Zielverzeichnis, da die symbolische Verbindung keinen abschließenden Schrägstrich enthält. Der Client sichert die symbolische Verbindung nicht als Verzeichnis und sichert keine Dateien oder Ordner im Zielverzeichnis.

Beispiel 5

```
dsmc incr /home/gillis/
```

In Beispiel 5 sichert der Client nur den Pfad zu dem Zielverzeichnis, da die symbolische Verbindung nicht explizit in der Dateispezifikation für die Sicherung angegeben ist. Wie in Beispiel 3 sichert der Client die symbolische Verbindung nicht als Verzeichnis und sichert keine Dateien oder Ordner im Zielverzeichnis.

Einschränkung: Wenn Sie eine symbolische Verbindung als Verzeichnis sichern, in einer zukünftigen Teilsicherung diese symbolische Verbindung jedoch nicht als Verzeichnis sichern, verfallen diese als Verzeichnis gesicherte symbolische Verbindung sowie die Dateien und Verzeichnisse in diesem Verzeichnis.

Beispiel: Angenommen, Sie sichern die symbolische Verbindung `symdir` zunächst als Verzeichnis und sichern den Inhalt des Zielverzeichnisses. Der in Beispiel 1 angegebene Befehl führt diese Operation aus. Der Client erstellt Sicherungskopien mit dem übergeordneten Pfad `/home/gillis/symdir/`. In diesem Beispiel erstellt der Client Sicherungskopien mit den folgenden Pfaden:

- `/home/gillis/symdir/`
- `/home/gillis/symdir/file`
- `/home/gillis/symdir/dir1`
- `/home/gillis/symdir/dir1/file1`

Der Inhalt von `/home/gillis` wird mit dem folgenden Befehl gesichert:

```
dsmc inc /home/gillis/ -subdir=yes
```

Dieser Befehl verarbeitet den Wert `symdir` als symbolische Verbindung und verarbeitet nicht die Objekte, auf die die symbolische Verbindung zeigt. Daher kennzeichnet der Client Sicherungskopien im Verzeichnis `/home/gillis/symdir/`, die in Beispiel 1 erstellt wurden, als verfallen.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Teilsicherung nur für eine Domäne

Der Client sichert eine symbolische Verbindung während einer Teilsicherung der Domäne, wenn die symbolische Verbindung als virtueller Mountpunkt definiert und die Option followsymbolic auf yes gesetzt ist.

Der Client sichert eine symbolische Verbindung und das Zielverzeichnis, wenn alle folgenden Bedingungen erfüllt sind:

- Der Client führt eine Teilsicherung der Domäne aus.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDie symbolische Verbindung ist mit der Option virtualmountpoint als virtueller Mountpunkt definiert.
- `followsymbolic=yes`

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDie Optionen virtualmountpoint und followsymbolic fügen der Domäne die symbolische Verbindung hinzu. Der Befehl incremental sichert die Domäne, die das Ziel der symbolischen Verbindung umfasst.

Zugehörige Verweise:
Followsymbolic
Virtualmountpoint
 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Feste Verbindungen

Wenn Sie Dateien sichern, die fest verbunden sind, sichert der Client für Sichern/Archivieren jede Instanz der fest verbundenen Datei.

Wenn Sie beispielsweise zwei Dateien sichern, die fest verbunden sind, sichert der Client die Dateidaten zweimal.

Wenn Sie fest verbundene Dateien zurückschreiben, versucht der Client, die Verbindungen wiederherzustellen. Hatten Sie beispielsweise ein Dateipaar mit fester Verbindung und ist nur eine der fest verbundenen Dateien auf Ihrer Workstation, werden beide Dateien beim Zurückschreiben fest verbunden. Werden beide Dateien zusammen mit einem einzigen Befehl zurückgeschrieben, werden die Dateien auch dann fest verbunden, wenn keine der Dateien zum Zeitpunkt der Zurückschreibung vorhanden ist. Bei diesem Verfahren gibt es eine Ausnahme, und zwar, wenn Sie zwei fest verbundene Dateien sichern und dann die Verbindung zwischen diesen Dateien auf der Workstation unterbrechen. Wenn

Sie die beiden Dateien über den Standardzurückschreibungsprozess (oder klassischen Zurückschreibungsprozess) vom Server zurückschreiben, respektiert der Client das aktuelle Dateisystem und stellt die feste Verbindung nicht wieder her.

Wichtig: Wenn nicht alle fest verbundenen Dateien gleichzeitig gesichert oder zurückgeschrieben werden, können Probleme auftreten. Um sicherzustellen, dass fest verbundene Dateien synchronisiert bleiben, führen Sie die Sicherung und den Zurückschreibung fest verbundener Dateien immer gleichzeitig durch.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Dateien mit freien Bereichen

Dateien mit freien Bereichen haben keinen Plattenspeicherplatz für jeden Block im gesamten Adressraum zugeordnet, was zu freien Datenbereichen innerhalb der Datei führt. Freie Datenbereiche werden durch ihren Inhalt erkannt, der immer Null ist, und diese Nullen nehmen Speicherplatz ein.

Standardwert ist, die Datei mit freien Bereichen ohne die freien Datenbereiche zurückzuschreiben, was mehr freien Plattenspeicherplatz lassen würde. Der Client für Sichern/Archivieren erkennt Dateien mit freien Bereichen während einer Sicherungsoperation und markiert sie als solche auf dem IBM Spectrum Protect-Server.

Anmerkung: Dateien mit freien Bereichen gelten nicht für Mac OS X.

Der Client für Sichern/Archivieren sichert eine Datei mit freien Bereichen als reguläre Datei, wenn die Clientkomprimierung inaktiviert ist.

Zugehörige Verweise:
Compression
Makesparsefile
Mac OS X-BetriebssystemeMac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Absolute und bedingte NFS-Mounts

Wenn der Client für Sichern/Archivieren die Verbindung zu einem NFS-Dateisystem herstellt, kann entweder ein absoluter Mount oder ein bedingter Mount verwendet werden.

Der Client bestimmt mithilfe des Werts für die Option nfstimeout die Wartezeit für eine Antwort auf einen NFS-Systemaufruf, bevor eine Zeitlimitüberschreitung auftritt; diese Einstellung gilt für absolute und bedingte Mounts. Der Standardwert ist 0 Sekunden. Dies bedeutet, dass der Client das Standardverhalten von NFS-Systemaufrufen verwendet.

Sie sollten sich über die Auswirkungen absoluter und bedingter Mounts im Klaren sein, falls der Mount nicht mehr aktuell ist (wenn beispielsweise der Server für das Dateisystem nicht mehr verfügbar ist).

Absoluter Mount
: Bei einem NFS-Dateisystem mit absolutem Mount versuchen die NFS-Dämonen ständig, mit dem Server Verbindung aufzunehmen. Für die Neuversuche der NFS-Dämonen tritt keine Zeitlimitüberschreitung auf, sie beeinträchtigen die Systemleistung und der Benutzer kann sie nicht unterbrechen; die Steuerung wird jedoch an den Client zurückgegeben, wenn der Wert für nfstimeout erreicht ist.

Bedingter Mount
: Bei einem NFS-Dateisystem mit bedingtem Mount versucht NFS so lange mit dem Server Verbindung aufzunehmen, bis eine der folgenden Situationen eintritt:

  - Eine Verbindung wird aufgebaut
  - Die NFS-Wiederholungsschwelle wird erreicht
  - Der Wert für nfstimeout wird erreicht

  Tritt eines dieser Ereignisse ein, wird die Steuerung an das aufrufende Programm zurückgegeben.

  Anmerkung: Auf UNIX- und Linux-Systemen kann die Option nfstimeout fehlschlagen, wenn der NFS-Mount ein absoluter Mount ist. Tritt eine Blockierung auf, müssen Sie die Option nfstimeout inaktivieren und das NFS-Dateisystem wie folgt mit einem bedingten Mount anhängen:

  ```
  mount -o soft,timeo=5,retry=5 machine:/filesystem /mountpoint
  ```

  Die Parameter sind wie folgt definiert:

  soft
  : Generiert einen bedingten Mount des NFS-Dateisystems. Tritt ein Fehler auf, gibt die Funktion stat() einen Fehler zurück. Wird die Option hard verwendet, gibt stat() erst dann einen Rückkehrcode aus, wenn das Dateisystem verfügbar ist.

  timeo=n
  : Setzt das Zeitlimitintervall für den Fehler eines bedingten Mounts auf *n* Zehntel einer Sekunde.

  retry=n
  : Legt die Anzahl der Mountversuche fest (hierbei ist *n* eine ganze Zahl). Der Standardwert ist 10000.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Gelöschte Dateisysteme

Wenn ein Dateisystem oder Laufwerk gelöscht wurde oder nicht mehr vom Client für Sichern/Archivieren gesichert wird, werden die vorhandenen Sicherungsversionen für jede Datei gemäß den folgenden Maßnahmenattributen verwaltet: Anzahl Tage für die Aufbewahrung inaktiver Sicherungsversionen und Anzahl Tage für die Aufbewahrung der letzten Sicherungsversion (falls keine aktive Version vorhanden ist).

Wenn Sie nichts weiter unternehmen, verbleiben aktive Sicherungsversionen unbegrenzt. Falls Sie die aktiven Versionen nicht unbegrenzt aufbewahren müssen, können Sie mit dem Befehl expire die aktiven Versionen inaktivieren.

Wenn Sie keine der aktiven Versionen aufbewahren müssen, können Sie mit dem Befehl delete backup alle Sicherungsversionen im Dateibereich löschen. Ihr IBM Spectrum Protect-Serveradministrator muss Ihnen die Berechtigung zur Verwendung dieses Befehls geben. Mithilfe des Befehls query session können Sie feststellen, ob Sie die Berechtigung "delete backup" besitzen. Alternativ dazu können Sie Ihren IBM Spectrum Protect-Serveradministrator bitten, den Dateibereich für Sie zu löschen.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Geöffnete Dateien

Der Client für Sichern/Archivieren sucht nach Dateien, die sich zwischen dem Start und dem Ende der Dateisicherung geändert haben.

Einige Dateien auf Ihrem System sind möglicherweise im Gebrauch oder geöffnet, wenn Sie versuchen, sie zu sichern. Da sich eine offene Datei ändern kann, spiegelt eine Sicherungsaktion den Inhalt der Datei zu einem bestimmten Zeitpunkt nicht korrekt wider.

Überlegen Sie, ob die Datei wichtig ist und ob sie sie erneut erstellen können. Wenn die Datei nicht wichtig ist, ist eine Sicherung eventuell nicht erforderlich. Wenn die Datei wichtig ist, kann ein Root auf Ihrer Workstation sicherstellen, dass die Datei vor dem Sichern geschlossen wird.

Werden die Sicherungen nach einem Zeitplan ausgeführt, kann ein Root mit der Option preschedulecmd einen Befehl eingeben, der die Datei schließt. Handelt es sich bei der offenen Datei beispielsweise um eine Datenbank, verwenden Sie den Befehl quiesce der Datenbank, um sie zu beenden. Nach Beendigung der Sicherung kann ein Root die Anwendung, die die Datei verwendet, mit der Option postschedulecmd erneut starten. Wird kein Zeitplan für die Sicherung verwendet, muss die Anwendung, die die Datei verwendet, vor Beginn der Sicherung geschlossen werden.

Der Client kann die Datei selbst dann sichern, wenn sie während der Sicherung offen ist und geändert wird. Dies ist nur sinnvoll, wenn die Datei noch verwendbar ist, auch wenn sie sich während der Sicherung ändert. Damit diese Dateien gesichert werden, muss ihnen eine Verwaltungsklasse mit der Durchnummerierung *Dynamisch* oder *Gemeinsam dynamisch* zugeordnet werden.

Zugehörige Konzepte:
Informationen zu Verwaltungsklassen und Kopiengruppen anzeigen
Verwaltungsklasse für Dateien auswählen
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Platzhalterzeichen

Beim Client für Sichern/Archivieren können die Platzhalterzeichen des Betriebssystems in Dateispezifikationen verwendet werden. Mithilfe dieser Zeichen können Gruppen von Dateien mit ähnlichen Namen ausgewählt werden.

In einem Befehl können Platzhalterzeichen nur innerhalb des Dateinamens oder innerhalb der Erweiterung verwendet werden. Sie können nicht für Zieldateien, Dateisysteme oder Verzeichnisse angegeben werden. Werden Platzhalterzeichen in einem anderen Modus als dem Schleifenmodus verwendet, wie z. B. in `dsmc sel "/home/ledger.*"`, muss der Parameter, der den Stern enthält, in Anführungszeichen gesetzt werden, um sicherzustellen, dass das System das Platzhalterzeichen nicht interpretiert und unerwartete Ergebnisse liefert. Die folgende Tabelle enthält Informationen über Platzhalterzeichen.

Wichtig: Verwenden Sie einen Stern (*) statt eines Fragezeichens (?) als Platzhalterzeichen, wenn Sie nach einer Übereinstimmung mit einem Muster in einer Mehrfachbyte-Codepage suchen, um unerwartete Ergebnisse zu verhindern.

Die folgende Tabelle zeigt einige Platzhalterzeichenmuster und ihre Angabe.

*** *(Stern)***	**Null oder mehr Zeichen, die Dateien mit folgenden Merkmalen entsprechen:**
***.cpp**	Dateinamen mit der Erweiterung cpp
hm*.*	Dateinamen, die mit hm beginnen und eine beliebige Erweiterung haben, aber das Zeichen **'.'** aufweisen müssen
hm*	Dateinamen, die mit hm beginnen und eine Erweiterung haben können oder nicht
h*.	Dateinamen mit einem h an einer beliebigen Position im Dateinamen und mit einer beliebigen Erweiterung, die aber einen **.** aufweisen müssen

? *(Fragezeichen)*	**Ein Zeichen, das Dateien mit folgenden Merkmalen entspricht:**
?.cpp	Dateinamen mit der Erweiterung cpp, die aus nur einem einzigen Zeichen bestehen
hm?.cpp	Dreistellige Dateinamen, die mit hm beginnen und die Erweiterung cpp haben

* ? *(Stern und Fragezeichen)*	**Kombinationen aus Stern und Fragezeichen, die Dateien mit folgenden Merkmalen entsprechen:**
??hm.*	Vierstellige Dateinamen, die mit hm. enden und eine beliebige Erweiterung haben

In einem Pfadnamen für eine Dateispezifikation kann kein Verzeichnis angegeben werden, dessen Name einen Stern (*) oder ein Fragezeichen (?) enthält. Der Client erkennt diese Zeichen nur als Platzhalterzeichen.

Daten zurückschreiben

Mit IBM Spectrum Protect können Sicherungsversionen bestimmter Dateien, einer Gruppe von Dateien mit ähnlichen Namen oder vollständiger Verzeichnisse zurückgeschrieben werden.

Sie können diese Sicherungsversionen zurückschreiben, wenn die ursprünglichen Dateien verloren gegangen oder beschädigt sind. Wählen Sie die zurückzuschreibenden Dateien mithilfe einer Dateispezifikation (Pfad, Name und Erweiterung der Datei), einer Verzeichnisliste oder mithilfe eines Unterverzeichnispfads zu einem Verzeichnis und seinen Unterverzeichnissen aus.

Windows-BetriebssystemeAnmerkung: Wenn Sie ein Verzeichnis zurückschreiben, werden das Datum und die Uhrzeit der Zurückschreibung als Änderungsdatum und Änderungszeit festgelegt und nicht das Datum und die Uhrzeit des Verzeichnisses bei seiner Sicherung. Die Ursache dafür ist, dass IBM Spectrum Protect zuerst die Verzeichnisse zurückschreibt und anschließend die Dateien zu den Verzeichnissen hinzufügt.

Alle Sicherungs- und Zurückschreibungsprozeduren des Clients, auf die in diesem Abschnitt verwiesen wird, gelten auch für den Web-Client. Der Web-Client verfügt jedoch über keinen Profileditor, mit dem Clientoptionen definiert werden können.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeAchtung: Schreiben Sie keine Betriebssystemdateien, wie z. B. Basissystemverzeichnisse, Kernelmodule oder Programmkorrekturen, an ihre ursprüngliche Position zurück, während das Dateisystem ausgeführt wird. Das Betriebssystem könnte blockieren oder ausfallen.

Die folgenden Tasks sind die primären Zurückschreibungstasks:

- Windows-BetriebssystemeDateien und Verzeichnisse zurückschreiben
- Windows-BetriebssystemeWindows-Systemstatus zurückschreiben
- Windows-BetriebssystemeDateien für die automatische Systemwiederherstellung zurückschreiben
- Windows-BetriebssystemeMicrosoft DFS-Baumstruktur und -Dateien zurückschreiben
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeImage zurückschreiben
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDaten über die grafische Benutzerschnittstelle zurückschreiben
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBeispiele für Zurückschreibungsbefehle
- Daten aus einem Sicherungssatz zurückschreiben
- Daten nach Zeitpunkt zurückschreiben
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeNAS-Dateisysteme zurückschreiben
- Windows-BetriebssystemeAnderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeEinen anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen
- Windows-BetriebssystemeDateien von einem anderen Clientknoten zurückschreiben oder abrufen
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDateien von einem anderen Clientknoten zurückschreiben oder abrufen
- Windows-BetriebssystemeDateien auf eine andere Workstation zurückschreiben oder abrufen
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDateien auf eine andere Workstation zurückschreiben oder abrufen
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemePlatte nach Plattenverlust zurückschreiben
- Windows-BetriebssystemeDateibereiche löschen
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDateibereiche löschen
- Windows-BetriebssystemeDaten aus einer VMware-Sicherung zurückschreiben

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDie Veröffentlichung *IBM Spectrum Protect for Space Management for UNIX and Linux* enthält Details über das Zurückschreiben umgelagerter Dateien und die Option restoremigstate.

- Windows-BetriebssystemeDoppelte Dateinamen
  Versuchen Sie, eine Datei zurückzuschreiben oder abzurufen, deren Name mit dem Kurznamen einer vorhandenen Datei identisch ist, tritt eine Dateinamenkollision auf (doppelte Dateinamen vorhanden).

- Windows-BetriebssystemeZurückschreibung mit Namen der allgemeinen Namenskonvention
  Wenn Sie einen UNC-Namen (UNC - Universal Naming Convention, allgemeine Namenskonvention) verwenden, können Sie bestimmte gemeinsam genutzte Dateien in einem separaten Dateibereich zurückschreiben. Dies ist nützlich, wenn ein Benutzer oder Administrator einen Teil von Daten zurückschreiben will, auf den sonst nicht zugegriffen werden könnte.
- Windows-BetriebssystemeZurückschreibung aktiver oder inaktiver Sicherungen
  Ihr Administrator legt fest, wie viele Sicherungsversionen IBM Spectrum Protect für jede Datei auf Ihrer Workstation aufbewahrt. Sind mehrere Versionen einer Datei vorhanden, können ältere Versionen zurückgeschrieben werden, falls die aktuellste Sicherungsversion beschädigt ist.
- Windows-BetriebssystemeDateien und Verzeichnisse zurückschreiben
  Die Dateien, die zurückgeschrieben werden sollen, können durch Suchen und Filtern lokalisiert werden.
- Windows-BetriebssystemeWindows-Systemstatus zurückschreiben
  Der Microsoft Volumeschattenkopie-Dienst (VSS = Volume Shadowcopy Service) wird auf Windows-Clients für Sichern/Archivieren unterstützt. Der Client verwendet VSS, um den Systemstatus zurückzuschreiben. Die Funktion für die Zurückschreibung des Systemstatus ist für Onlinezurückschreibungsoperationen des Systemstatus veraltet.
- Windows-BetriebssystemeDateien für die automatische Systemwiederherstellung zurückschreiben
  Sie können Dateien für die automatische Systemwiederherstellung (Automated System Recovery - ASR) zurückschreiben, um die Datenträgerkonfigurationsdaten und den Systemstatus für das Windows-Betriebssystem wiederherzustellen, wenn ein schwerwiegender System- oder Hardwarefehler auftritt.
- Windows-BetriebssystemeBetriebssystem zurückschreiben, wenn der Computer in Betrieb ist
  Ist Ihr Computer in Betrieb, können Sie das Betriebssystem aus gesicherten Dateien zurückschreiben.
- Computer wiederherstellen, wenn das Windows-Betriebssystem nicht funktioniert
  Hat der Computer einen schwerwiegenden Hardware- oder Softwarefehler, können Sie ein Windows-Betriebssystem mit der automatischen Systemwiederherstellung (Automated System Recovery - ASR) wiederherstellen.
- Windows-BetriebssystemeMicrosoft DFS-Baumstruktur und -Dateien zurückschreiben
  Sollen DFS-Zusammenführungen und die Daten für jede Zusammenführung zurückgeschrieben werden, müssen Sie zunächst die Metadaten der DFS-Zusammenführung und dann jede Zusammenführung separat zurückschreiben.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeImage zurückschreiben
  Einige Punkte sind zu berücksichtigen, bevor Sie mit der Zurückschreibung von Images auf Ihr System beginnen.
- Daten aus einem Sicherungssatz zurückschreiben
  Ihr IBM Spectrum Protect-Administrator kann einen Sicherungssatz (d. h. eine Sammlung Ihrer Dateien, die sich auf dem Server befinden) auf Wechseldatenträgern generieren und diese auf einer Einheit mit einem Format erstellen, das mit der Clienteinheit kompatibel ist.
- Windows-BetriebssystemeNet Appliance-CIFS-Freigaben zurückschreiben
  Das Zurückschreiben der Freigabedefinition erfordert das Zurückschreiben des Stammverzeichnisses des Freigabedateibereichs, das in den meisten Fällen wie folgt durchgeführt werden kann: `dsmc rest \\NetAppFiler\CifsShareName\ -dirsonly`.
- Windows-BetriebssystemeDaten aus einer VMware-Sicherung zurückschreiben
  Es gibt mehrere Möglichkeiten, Daten aus Sicherungen auf einer virtuellen VMware-Maschine zurückzuschreiben. Die Zurückschreibungsmethode ist vom Sicherungstyp und von der Version der Software des Clients für Sichern/Archivieren abhängig, mit der Sie die Zurückschreibung ausführen.
- Windows-BetriebssystemeEinzelne Active Directory-Objekte von Windows zurückschreiben
  Sie können einzelne Active Directory-Objekte zurückschreiben, um die versehentliche Beschädigung oder Löschung von Active Directory-Objekten zu beheben, ohne dass der Active Directory-Server heruntergefahren und erneut gestartet werden muss.
- Daten während einer Übernahme zurückschreiben oder abrufen
  Wenn eine Übernahme des Clients auf dem Sekundärserver stattfindet, können Sie replizierte Daten vom Sekundärserver zurückschreiben oder abrufen.
- Windows-BetriebssystemeAnderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen
  Ein Benutzer kann einem Benutzer auf einem anderen Knoten die Berechtigung zum Zurückschreiben seiner Sicherungsversionen oder zum Abrufen seiner Archivierungskopien erteilen. Auf diese Weise können Sie Dateien mit anderen Benutzern oder anderen Workstations, die Sie mit einem anderen Knotennamen verwenden, gemeinsam nutzen.
- Windows-BetriebssystemeDateien von einem anderen Clientknoten zurückschreiben oder abrufen
  Nachdem andere Benutzer Ihnen den Zugriff auf ihre Dateien auf dem Server erteilt haben, können Sie diese Dateien in Ihr lokales System zurückschreiben oder abrufen.
- Windows-BetriebssystemeDateien auf eine andere Workstation zurückschreiben oder abrufen
  Der Benutzer kann Dateien, die aus der eigenen Workstation gesichert oder archiviert wurden, zurückschreiben oder abrufen, wenn er eine andere Workstation verwendet.
- Windows-BetriebssystemeDateibereiche löschen
  Erteilt Ihnen der IBM Spectrum Protect-Administrator die Berechtigung, können Sie vollständige Dateibereiche auf dem Server löschen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeImage in Datei zurückschreiben
  Wenn Sie ein Image sichern, sichert der Client für Sichern/Archivieren den ersten Sektor des Datenträgers. Bei der Zurückschreibung der Daten wird der erste Sektor jedoch übersprungen, um den ursprünglichen Steuerblock des logischen Datenträgers des Zieldatenträgers beizubehalten.
- AIX-BetriebssystemeLinux-BetriebssystemeGPFS-Dateisystemdaten mit Speicherpools verwalten
  Mithilfe der GPFS-Technologie (GPFS = Global Parallel File Systems) können Sie Ihre Daten mit Speicherpools verwalten. Ein Speicherpool ist eine Sammlung von Platten oder RAIDs mit ähnlichen Eigenschaften, die als eine Gruppe zusammen verwaltet werden.
- Daten nach Zeitpunkt zurückschreiben
  Verwenden Sie eine Zurückschreibung *nach Zeitpunkt*, um Dateien mit dem Stand zurückzuschreiben, den sie an einem bestimmten Datum und zu einer bestimmten Uhrzeit hatten.
- AIX-BetriebssystemeVerschlüsselte AIX-Dateien zurückschreiben
  Wenn Dateien in unformatiertem Format von einem AIX JFS2 EFS (Verschlüsseltes AIX JFS2-Dateisystem) gesichert werden, können Sie

sie nur in dasselbe oder in ein anderes JFS2 EFS zurückschreiben. Sie können nicht in ein anderes Dateisystem oder auf eine andere Plattform zurückgeschrieben werden.

- AIX-BetriebssystemeAIX-Workloadpartitionsdateisysteme zurückschreiben
  Alle Dateien, die von der lokalen Workloadpartition (WPAR) erstellt und von dem in der globalen Workloadpartition installierten Client für Sichern/Archivieren gesichert wurden, können von dem in der globalen Workloadpartition installierten Client zurückgeschrieben werden.
- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeNAS-Dateisysteme zurückschreiben
  NAS-Dateisystemimages werden mithilfe des Web-Clients oder der Befehlszeilenschnittstelle zurückgeschrieben. Die Web-Client-Schnittstelle ist nur für Verbindungen zu einem Server mit IBM Spectrum Protect Version 8.1.1, 8.1.0, 7.1.7 oder einer früheren Version verfügbar.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAktive oder inaktive Sicherungen zurückschreiben
  Ihr Administrator legt fest, wie viele Sicherungsversionen IBM Spectrum Protect für jede Datei auf Ihrer Workstation aufbewahrt.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDaten über die grafische Benutzerschnittstelle zurückschreiben
  In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um Sicherungsversionen von einzelnen Dateien oder Unterverzeichnissen zurückzuschreiben.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeBeispiele für Zurückschreibungsbefehle
  Dieser Abschnitt enthält einige Beispiele für Befehle restore, die für bestimmte Tasks verwendet werden müssen.
- Oracle Solaris-BetriebssystemeSolaris Zettabyte-Dateisysteme (ZFS) zurückschreiben
  ZFS-Dateisysteme (Zettabyte File System) verwenden Speicherpools zum Verwalten von physischen Speichereinheiten.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeZusätzliche Zurückschreibungstasks
  In diesem Abschnitt werden einige weiterführende Hinweise für das Zurückschreiben von Daten erläutert.

Zugehörige Tasks:
Web-Client-Sitzung starten
Windows-Betriebssysteme

Doppelte Dateinamen

Versuchen Sie, eine Datei zurückzuschreiben oder abzurufen, deren Name mit dem Kurznamen einer vorhandenen Datei identisch ist, tritt eine Dateinamenkollision auf (doppelte Dateinamen vorhanden).

Beispiel: Der Datei *abcdef**ghijk**.doc* ist der Kurzname *abcdef~**1**.doc* zugeordnet, und Sie versuchen, eine Datei mit dem expliziten Namen *abcdef~**1**.doc* in dasselbe Verzeichnis zurückzuschreiben oder abzurufen. In diesem Fall tritt eine Kollision auf, weil der Name der zurückzuschreibenden Datei mit dem Kurznamen für *abcdef**ghijk**.doc* identisch ist.

Eine Kollision kann auch dann auftreten, wenn die Dateien in ein leeres Verzeichnis zurückgeschrieben oder abgerufen werden. Beispiel: Die Dateien *abcdef~**1**.doc* und *abcdef**ghijk**.doc* waren möglicherweise ursprünglich als *abcdef**ghijk**.doc* und *abcdef~**2**.doc* in dem Verzeichnis vorhanden. Wenn *abcdef**ghijk**.doc* bei der Zurückschreibung zuerst zurückgeschrieben wird, ordnet das Windows-Betriebssystem ihr den Kurznamen *abcdef~**1**.doc* zu. Wenn Sie *abcdef~**1**.doc* zurückschreiben, treten doppelte Dateinamen auf.

IBM Spectrum Protect handhabt diese Situationen auf der Basis des Werts der Option replace. Mit der Option replace können Sie angeben, ob eine vorhandene Datei überschrieben werden soll oder ob Sie zur Eingabe Ihrer Auswahl aufgefordert werden sollen, wenn Sie Dateien zurückschreiben oder abrufen.

Tritt eine Dateinamenkollision auf, können Sie wie folgt vorgehen:

- Die Datei mit dem Kurzdateinamen an eine andere Position zurückschreiben oder abrufen.
- Die Zurückschreibung oder den Abruf stoppen und den Namen der vorhandenen Datei ändern.
- Die Unterstützung von Kurzdateinamen auf Windows inaktivieren.
- Keine Dateinamen wie *abcdef~**1**.doc* verwenden, die mit der Kurzdateinamenskonvention unverträglich sind.

Zugehörige Verweise:
Replace
Windows-Betriebssysteme

Zurückschreibung mit Namen der allgemeinen Namenskonvention

Wenn Sie einen UNC-Namen (UNC - Universal Naming Convention, allgemeine Namenskonvention) verwenden, können Sie bestimmte gemeinsam genutzte Dateien in einem separaten Dateibereich zurückschreiben. Dies ist nützlich, wenn ein Benutzer oder Administrator einen Teil von Daten zurückschreiben will, auf den sonst nicht zugegriffen werden könnte.

Mit Ausnahme von Laufwerken mit austauschbaren Datenträgern ist der Zugriff auf jeden lokalen Laufwerkbuchstaben mithilfe eines lokalen Namens, der der allgemeinen Namenskonvention entspricht, möglich. Dieser Name besteht aus dem Namen der Workstation und einer Bezeichnung für den Laufwerkbuchstaben. Um beispielsweise auf Laufwerk `c:` für die Workstation `ocean` einen Namen anzugeben, der der allgemeinen Namenskonvention entspricht, Folgendes eingeben:

```
\\ocean\c$
```

Das Zeichen $ *muss* dem Laufwerkbuchstaben angefügt werden.

Um für die Workstation `ocean` und den Freigabepunkt `wave` einen UNC-Namen anzugeben, geben Sie Folgendes ein:

```
\\ocean\wave
```

Beim Zugriff auf Dateien muss der Laufwerkbuchstabe *nur* für Laufwerke mit austauschbaren Datenträgern eingegeben werden.
Windows-Betriebssysteme

Zurückschreibung aktiver oder inaktiver Sicherungen

Ihr Administrator legt fest, wie viele Sicherungsversionen IBM Spectrum Protect für jede Datei auf Ihrer Workstation aufbewahrt. Sind mehrere Versionen einer Datei vorhanden, können ältere Versionen zurückgeschrieben werden, falls die aktuellste Sicherungsversion beschädigt ist.

Die aktuellste Sicherungsversion ist die *aktive* Version. Jede andere Sicherungsversion ist eine *inaktive* Version. Bei jeder Dateisicherung markiert IBM Spectrum Protect die neue Sicherungsversion als die aktive Sicherungsversion, und die letzte aktive Sicherungsversion wird zu einer inaktiven Version. Wenn die maximal zulässige Anzahl inaktiver Versionen erreicht ist, löscht IBM Spectrum Protect die älteste inaktive Version.

Soll eine inaktive Sicherungsversion zurückgeschrieben werden, müssen sowohl aktive als auch inaktive Versionen angezeigt werden. Klicken Sie dazu **Anzeigen** → **Aktive/inaktive Dateien anzeigen** an. Sollen nur die aktiven Versionen angezeigt werden (Standardwert), klicken Sie **Anzeigen** → **Nur aktive Dateien anzeigen** an. Wird versucht, eine aktive und eine inaktive Version einer Datei gleichzeitig zurückzuschreiben, wird nur die aktive Version zurückgeschrieben.

Verwenden Sie in der IBM Spectrum Protect-Befehlszeile die Option inactive, um sowohl aktive als auch inaktive Objekte anzuzeigen.

Zugehörige Verweise:
Inactive
Windows-Betriebssysteme

Dateien und Verzeichnisse zurückschreiben

Die Dateien, die zurückgeschrieben werden sollen, können durch Suchen und Filtern lokalisiert werden.

Beim Filtern werden nur die Dateien angezeigt, die den Filterkriterien der Operation zum Zurückschreiben entsprechen. Dateien, die den Filterkriterien nicht entsprechen, werden nicht angezeigt. Beim Filtern werden Dateien in dem angegebenen Verzeichnis, aber nicht in den Unterverzeichnissen gesucht.

-  WindowsBetriebssystemeDaten über die GUI zurückschreiben
  Sie können Dateien und Verzeichnisse mithilfe der grafischen Benutzerschnittstelle des Clients (Client-GUI) zurückschreiben.
-  WindowsBetriebssystemeBeispiele für das Zurückschreiben von Daten über die Befehlszeile
  Sie können die Beispiele in diesem Abschnitt verwenden, wenn Sie Objekte aus dem IBM Spectrum Protect-Serverspeicher zurückschreiben müssen.

 Windows-Betriebssysteme

Daten über die GUI zurückschreiben

Sie können Dateien und Verzeichnisse mithilfe der grafischen Benutzerschnittstelle des Clients (Client-GUI) zurückschreiben.

Informationen zu diesem Vorgang

Einschränkung: In der GUI des Web-Clients können Netzressourcen für eine Zurückschreibungsoperation nicht durchsucht werden. Es werden keine Freigaben aufgelistet, wenn Sie die Verzweigung Netz einblenden. Eine Zurückschreibung vom Web-Client in eine Netzressource ist möglich, wenn die gesamte Datei verarbeitet wird. Geben Sie das gemeinsam genutzte Dateisystem über die Option domain in der Optionsdatei `dsm.opt` an, beispielsweise `domain all-local \\server\share`. Um die Zurückschreibungsoperation abzuschließen, geben Sie Netzfreigabe im Dialog Zurückschreibungsziel an. Damit werden alle Dateisysteme verarbeitet, die über die Option domain angegeben werden. Sie können die Zurückschreibungsoperation auch über die GUI des Clients ausführen.

Vorgehensweise

1. Klicken Sie im Hauptfenster auf Zurückschreiben. Das Fenster Zurückschreiben wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben einem Objekt in der Baumstruktur klicken. Wählen Sie das Objekt aus, das zurückgeschrieben werden soll. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol Suchen in der Funktionsleiste.
3. Klicken Sie auf das Auswahlfeld für die Objekte, die zurückgeschrieben werden sollen.
4. Um bestimmte Zurückschreibungsoptionen zu ändern, klicken Sie auf die Schaltfläche Optionen. Die geänderten Optionen sind nur während der aktuellen Sitzung wirksam.

5. Klicken Sie auf Zurückschreiben. Das Fenster Zurückschreibungsziel wird angezeigt. Geben Sie die entsprechenden Informationen ein.
6. Klicken Sie auf Zurückschreiben. Im Fenster Task-Liste für die Zurückschreibung wird der Verarbeitungsstatus angezeigt.

Zugehörige Tasks:
Daten über die GUI sichern
Windows-Betriebssysteme

Beispiele für das Zurückschreiben von Daten über die Befehlszeile

Sie können die Beispiele in diesem Abschnitt verwenden, wenn Sie Objekte aus dem IBM Spectrum Protect-Serverspeicher zurückschreiben müssen.

Die folgende Tabelle zeigt die Verwendung einiger Zurückschreibungsbefehle für das Zurückschreiben Ihrer Objekte aus dem IBM Spectrum Protect-Serverspeicher.

Tabelle 1. Beispiele für Zurückschreibungsbefehle

Task	Befehl	Hinweise
Die aktuellste Sicherungsversion der Datei `c:\doc\h1.doc` zurückschreiben, obwohl die Sicherung inaktiv ist.	`dsmc restore c:\doc\h1.doc -latest`	Ist die zurückzuschreibende Datei nicht mehr auf der Workstation des Benutzers vorhanden und wurde nach dem Löschen der Datei eine Teilsicherung ausgeführt, befindet sich keine aktive Sicherungsversion der Datei auf dem Server. In diesem Fall muss mit der Option latest die neueste Sicherungsversion zurückgeschrieben werden. IBM Spectrum Protect schreibt die aktuellste Sicherungsversion zurück, unabhängig davon, ob sie aktiv oder inaktiv ist. Weitere Informationen siehe Latest.
Eine Liste der aktiven und inaktiven Sicherungsversionen von Dateien anzeigen, aus der Sie die zurückzuschreibenden Versionen auswählen können.	`dsmc restore c:\project\* -pick -inactive`	Wird versucht, eine aktive und eine inaktive Version einer Datei gleichzeitig zurückzuschreiben, wird nur die aktive Version zurückgeschrieben. Pick und Inactive enthalten weitere Informationen.
Alle Dateien mit der Dateierweiterung .c aus dem Verzeichnis c:\devel \projecta zurückschreiben.	`dsmc restore c:\devel \projecta\*.c`	Wird kein Ziel angegeben, werden die Dateien an ihre ursprüngliche Position zurückgeschrieben.
Die Datei c:\project\doc\h1.doc in ihr Ursprungsverzeichnis zurückschreiben.	`dsmc restore c:\project\doc\h1.doc`	Wird kein Ziel angegeben, werden die Dateien an ihre ursprüngliche Position zurückgeschrieben.
Die Datei `c:\project\doc\h1.doc` unter einem neuen Namen und in ein neues Verzeichnis zurückschreiben.	`dsmc restore c:\project\doc\h1.doc c:\project\newdoc\h2.doc`	Keine
Die Dateien im Laufwerk e: und allen dessen Unterverzeichnissen zurückschreiben.	`dsmc restore e:\ -subdir=yes`	Sie müssen die Option subdir verwenden, um Verzeichnisattribute/-berechtigungen zurückzuschreiben. Weitere Informationen zur Option subdir befinden sich im Abschnitt Subdir.
Alle Dateien im Verzeichnis c:\mydir mit ihrem Status am 17. August 2002 um 13:00 Uhr zurückschreiben.	`dsmc restore -pitd=17.08.2002 -pitt=13:00:00 c:\mydir\`	Weitere Informationen zu den Optionen pitdate und pittime enthalten die Abschnitte Pitdate und Pittime.

Task	Befehl	Hinweise

Die Datei c:\doc\h2.doc in ihr Ursprungsverzeichnis auf die Workstation mit dem Namen *star* zurückschreiben.	`dsmc restore c:\doc\h2.doc \\star\c$\`
	Um die Datei auf die Workstation "star" zurückzuschreiben, die in "meteor" umbenannt wurde, Folgendes eingeben:
	`dsmc restore \\star\c$\ doc\h2.doc \\meteor\c$\`
	Folgende Eingabe ist auch möglich:
	`dsmc restore \\star\c$\ doc\h2.doc c:\`
	Dieses Beispiel ist gültig, weil die lokale Workstation angenommen wird (in diesem Fall "meteor"), wenn kein Workstationname im Befehl angegeben wird.
		In diesem Handbuch ist die Workstation Teil des Dateinamens. Daher muss ein Ziel angegeben werden, wenn Dateien auf einer Workstation gesichert werden und auf eine andere Workstation zurückgeschrieben werden sollen. Dies gilt auch, wenn auf dieselbe physische Workstation zurückgeschrieben wird, die Workstation jedoch einen neuen Namen hat.

Eine Datei, die ursprünglich von der Diskette "workathome" in Laufwerk a: gesichert wurde, auf die Diskette "extra" in Laufwerk a: zurückschreiben.	`dsmc restore {workathome}\doc\h2.doc a:\doc\h2.doc`	Wird eine Datei auf eine Platte zurückgeschrieben, die eine andere Bezeichnung hat, als die Platte, von der die Datei gesichert wurde, muss der Dateibereichsname (Bezeichnung) der Sicherungsplatte anstelle des Laufwerkbuchstabens verwendet werden.
Die in der Datei c:\filelist.txt angegebenen Dateien in das Verzeichnis d:\dir zurückschreiben.	`dsmc restore -filelist=c:\filelist.txt d:\dir\`	Weitere Informationen zum Zurückschreiben von Dateilisten befinden sich im Abschnitt Filelist.
Alle Teildateien der auf dem IBM Spectrum Protect-Server gespeicherten Gruppensicherung `virtfs\group1` zurückschreiben.	`dsmc restore group {virtfs}\group1`	Weitere Informationen siehe Restore Group.

- Windows-BetriebssystemeBeispiele: Große Datenvolumen zurückschreiben
  Wenn Sie sehr viele Dateien zurückschreiben müssen, können Sie die Leistung verbessern, wenn Sie anstelle der grafischen Benutzerschnittstelle die Befehlszeilenschnittstelle verwenden. Außerdem können Sie die Leistung erhöhen, wenn Sie mehrere restore-Befehle gleichzeitig eingeben.
- Windows-BetriebssystemeStandardzurückschreibung mit Abfrage, Zurückschreibung ohne Abfrage und wiederanlauffähige Zurückschreibung
  In diesem Abschnitt werden die Standardzurückschreibung (klassische Zurückschreibung), die Zurückschreibung ohne Abfrage und die wiederanlauffähige Zurückschreibung beschrieben.

Zugehörige Konzepte:
Befehle verwenden
Zugehörige Verweise:
Restore
Windows-Betriebssysteme

Beispiele: Große Datenvolumen zurückschreiben

Wenn Sie sehr viele Dateien zurückschreiben müssen, können Sie die Leistung verbessern, wenn Sie anstelle der grafischen Benutzerschnittstelle die Befehlszeilenschnittstelle verwenden. Außerdem können Sie die Leistung erhöhen, wenn Sie mehrere restore-Befehle gleichzeitig eingeben.

Informationen zu diesem Vorgang

Sollen beispielsweise alle Dateien im Dateibereich `c:` zurückgeschrieben werden, geben Sie Folgendes ein:

```
dsmc restore c:\* -subdir=yes -replace=all -tapeprompt=no
```

Werden jedoch mehrere Befehle für die Stammverzeichnisse im Dateibereich `c:` eingegeben, können Sie die Dateien schneller zurückschreiben. Zum Beispiel die folgenden Befehle eingeben:

```
dsmc restore c:\users\ -subdir=yes -replace=all -tapeprompt=no
   dsmc restore c:\data1\ -subdir=yes -replace=all -tapeprompt=no
   dsmc restore c:\data2\ -subdir=yes -replace=all -tapeprompt=no
```

Müssen Dateien für mehrere Laufwerke zurückgeschrieben werden, folgende Befehle eingeben:

```
dsmc restore c:\* -subdir=yes -replace=all -tapeprompt=no
   dsmc restore d:\* -subdir=yes -replace=all -tapeprompt=no
   dsmc restore e:\* -subdir=yes -replace=all -tapeprompt=no
```

Sie können auch die Option quiet im Befehl restore verwenden, um Verarbeitungszeit einzusparen. Es werden jedoch keine Informationsnachrichten für einzelne Dateien angezeigt.
Anmerkung: Sind für die Optionen subdir, replace, tapeprompt und quiet bereits die entsprechenden Werte in der Clientoptionsdatei definiert, müssen diese Optionen nicht in den Befehlen angegeben werden.

Werden mehrere Befehle zum Zurückschreiben von Dateien eingegeben, muss ein eindeutiger Teil des Dateibereichs in jedem Befehl restore angegeben werden. Es dürfen keine Überschneidungen bei den Dateispezifikationen in den Befehlen auftreten.

Mit dem Befehl query backup kann eine Liste der Stammverzeichnisse in einem Dateibereich angezeigt werden. Beispiel:

```
dsmc query backup -dirsonly -subdir=no c:\
```

Im Allgemeinen können zwei bis vier restore-Befehle gleichzeitig eingegeben werden. Wie viele Befehle maximal gleichzeitig ausgeführt werden können, ohne die Leistung zu beeinträchtigen, ist abhängig von verschiedenen Faktoren, z. B. von der Netzauslastung und vom verfügbaren Speicher. Befinden sich `\users` und `\data1` beispielsweise auf demselben Band, muss das Zurückschreiben für `\data1` warten, bis das Zurückschreiben für `\users` beendet ist. Befindet sich `\data2` jedoch auf einem anderen Band und stehen mindestens zwei Bandlaufwerke zur Verfügung, kann das Zurückschreiben für `\data2` und für `\users` gleichzeitig beginnen.

Mit welcher Geschwindigkeit Sie die Dateien zurückschreiben können, ist auch davon abhängig, wie viele Bandlaufwerke verfügbar sind und ob der Administrator die Kollokation verwendet, um Dateibereiche möglichst wenig Datenträgern zuzuordnen. Verwendet der Administrator die Kollokation, wird auch die Anzahl der Ladevorgänge für Datenträger mit sequenziellem Zugriff, die für Zurückschreibungsoperationen benötigt werden, reduziert.

Standardzurückschreibung mit Abfrage, Zurückschreibung ohne Abfrage und wiederanlauffähige Zurückschreibung

In diesem Abschnitt werden die Standardzurückschreibung (klassische Zurückschreibung), die Zurückschreibung ohne Abfrage und die wiederanlauffähige Zurückschreibung beschrieben.

-  Windows-BetriebssystemeStandardzurückschreibungsprozess mit Abfrage
  Der Standardzurückschreibungsprozess mit Abfrage ist auch als klassisches Zurückschreiben bekannt. In diesem Abschnitt wird die Standardzurückschreibung mit Abfrage beschrieben.
-  Windows-BetriebssystemeProzess für Zurückschreibung ohne Abfrage
  Beim Zurückschreiben ohne Abfrage wird der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern es wird eine einzelne Zurückschreibungsanforderung an den Server gesendet.
-  Windows-BetriebssystemeWiederanlauffähiger Zurückschreibungsprozess
  Wird der Zurückschreibungsprozess aufgrund eines Stromausfalls oder eines Netzfehlers gestoppt, zeichnet der Server den Punkt auf, an dem dieser Ausfall oder Fehler erfolgte.

Standardzurückschreibungsprozess mit Abfrage

Der Standardzurückschreibungsprozess mit Abfrage ist auch als klassisches Zurückschreiben bekannt. In diesem Abschnitt wird die Standardzurückschreibung mit Abfrage beschrieben.

Die Standardzurückschreibung mit Abfrage arbeitet wie folgt:

- Der Client fragt den Server nach einer Liste mit Dateien ab, die für den Clientdateibereich gesichert wurden, der zurückgeschrieben werden soll.
- Der Server sendet eine Liste der gesicherten Dateien, die den Zurückschreibungsbedingungen entsprechen. Sollen sowohl aktive als auch inaktive Dateien zurückgeschrieben werden, sendet der Server Informationen zu allen gesicherten Dateien an den Client.
- Die vom Server ausgegebene Dateiliste wird im Clientspeicher sortiert, um die Zurückschreibungsreihenfolge der Dateien zu bestimmen und die für die Zurückschreibung erforderlichen Bandladevorgänge zu minimieren.

- Der Client teilt dem Server mit, Dateidaten und Verzeichnisobjekte zurückzuschreiben.
- Die Verzeichnisse und Dateien, die zurückgeschrieben werden sollen, werden vom Server an den Client gesendet.

Prozess für Zurückschreibung ohne Abfrage

Beim Zurückschreiben ohne Abfrage wird der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern es wird eine einzelne Zurückschreibungsanforderung an den Server gesendet.

1. Der Client teilt dem Server mit, dass eine Zurückschreibung ohne Abfrage ausgeführt werden soll, und stellt dem Server die Details zu den Dateibereichen, Verzeichnissen und Dateien zur Verfügung.
2. Der Server verwendet eine separate Tabelle, um die Einträge aufzuzeichnen, die die Zurückschreibung führen.
3. Die zurückzuschreibenden Daten werden an den Client gesendet. Die auf Platte gespeicherten Datei- und Verzeichnisobjekte werden sofort gesendet, da ein Sortieren dieser Daten vor dem Zurückschreiben des Objekts nicht erforderlich ist.
4. Sie können Mehrfachsitzungen verwenden, um die Daten zurückzuschreiben. Befinden sich die Daten auf mehreren Bändern, sind mehrere Mountpunkte auf dem Server verfügbar. Die Kombination der Option resourceutilization und MAXNUMMP ermöglicht Mehrfachsitzungen.

 Wenn Sie eine uneingeschränkte Quellendateispezifikation mit Platzhalterzeichen in den Befehl restore eingeben und keine der folgenden Optionen angeben, verwendet der Client eine Methode *Zurückschreibung ohne Abfrage* zum Zurückschreiben von Dateien und Verzeichnissen vom Server: inactive, latest, pick, fromdate oder todate. Diese Methode wird als *Zurückschreiben ohne Abfrage* bezeichnet, weil der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern eine einzige Zurückschreibungsanforderung an den Server gesendet wird. In diesem Fall gibt der Server die Dateien und Verzeichnisse ohne weitere Aktion durch den Client an den Client zurück. Der Client akzeptiert lediglich die vom Server kommenden Daten und schreibt sie an das im Befehl restore angegebene Ziel zurück.

    Wenn Sie eine uneingeschränkte Quellendateispezifikation mit Platzhalterzeichen in den Befehl restore eingeben und keine der folgenden Optionen angeben, verwendet der Client eine Methode *Zurückschreibung ohne Abfrage* zum Zurückschreiben von Dateien und Verzeichnissen vom Server: inactive, latest, pick, fromdate, todate. Diese Methode wird als *Zurückschreiben ohne Abfrage* bezeichnet, weil der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern eine einzige Zurückschreibungsanforderung an den Server gesendet wird. In diesem Fall gibt der Server die Dateien und Verzeichnisse ohne weitere Aktion durch den Client an den Client zurück. Der Client akzeptiert lediglich die vom Server kommenden Daten und schreibt sie an das im Befehl restore angegebene Ziel zurück.

 Bei Verwendung des IBM Spectrum Protect-GUI-Clients wäre ein Beispiel für einen unbeschränkten Befehl mit Platzhalterzeichen die Auswahl eines Ordners im Fenster 'Baumstruktur zurückschreiben'. Ein Beispiel für einen eingeschränkten Befehl mit Platzhalterzeichen wäre die Auswahl einzelner Dateien aus einem Ordner.

Im Befehlszeilenclient wäre ein Beispiel für einen unbeschränkten Befehl mit Platzhalterzeichen:

```
"/Users/user1/Documents/2004/*"
```

```
/home/mydocs/2004/*
```

```
c:\mydocs\2004\*
```

Ein Beispiel für eine eingeschränkte Dateispezifikation mit Platzhalterzeichen wäre:

```
/Users/user1/Documents/2004/sales.*
```

```
/home/mydocs/2004/sales.*
```

```
c:\mydocs\2004\sales.*
```

Wiederanlauffähiger Zurückschreibungsprozess

Wird der Zurückschreibungsprozess aufgrund eines Stromausfalls oder eines Netzfehlers gestoppt, zeichnet der Server den Punkt auf, an dem dieser Ausfall oder Fehler erfolgte.

Dieser Punkt ist dem Client als *wiederanlauffähige Zurückschreibung* bekannt. Es können mehrere wiederanlauffähige Zurückschreibungssitzungen vorhanden sein. Verwenden Sie den Befehl query restore oder wählen Sie **Wiederanlauffähige Zurückschreibungen** im Menü 'Aktionen' aus, um festzustellen, ob Ihr Client über wiederanlauffähige Zurückschreibungssitzungen in der Serverdatenbank verfügt.

Windows-BetriebssystemeEine wiederanlauffähige Zurückschreibung muss abgeschlossen werden, bevor weitere Sicherungen des Dateisystems versucht werden. Versuchen Sie, die unterbrochene Zurückschreibung zu wiederholen oder den Zieldateibereich zu sichern, schlägt der Versuch fehl, da die ursprüngliche Zurückschreibung nicht abgeschlossen wurde. Sie können die Zurückschreibung an dem Unterbrechungspunkt erneut starten, indem Sie den Befehl restart restore eingeben, oder Sie können die wiederanlauffähige Zurückschreibung löschen, indem Sie den Befehl cancel restore verwenden. Wenn Sie die unterbrochene Zurückschreibung erneut starten, wird mit der ersten Transaktion begonnen. Diese kann aus einer oder aus mehreren Dateien bestehen, die nicht vollständig zurückgeschrieben war oder waren, als die Unterbrechung auftrat. Aus diesem Grund können Sie einige Aufforderungen zum Ersetzen für Dateien aus der unterbrochenen Transaktion empfangen, die bereits zurückgeschrieben wurden.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeEine wiederanlauffähige Zurückschreibung muss abgeschlossen werden, bevor weitere Sicherungen des Dateisystems versucht werden. Versuchen Sie, die unterbrochene Zurückschreibung zu wiederholen oder den Zieldateibereich zu sichern, schlägt der Versuch fehl, da die ursprüngliche Zurückschreibung nicht abgeschlossen wurde. Sie können die Zurückschreibung an dem Unterbrechungspunkt erneut starten, indem Sie den Befehl restart restore eingeben, oder Sie können die wiederanlauffähige Zurückschreibung löschen, indem Sie den Befehl cancel restore verwenden.

Im Dialogfenster **Wiederanlauffähige Zurückschreibungen** in der IBM Spectrum Protect-GUI können Sie die unterbrochene Zurückschreibung auswählen und löschen oder die Zurückschreibung erneut starten. Wenn Sie die unterbrochene Zurückschreibung erneut starten, wird mit der ersten Transaktion begonnen. Diese kann aus einer oder aus mehreren Dateien bestehen, die nicht vollständig zurückgeschrieben war oder waren, als die Unterbrechung auftrat. Aus diesem Grund können Sie einige Aufforderungen zum Ersetzen für Dateien aus der unterbrochenen Transaktion empfangen, die bereits zurückgeschrieben wurden.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Führen Sie folgende Schritte aus, um wiederanlauffähige Zurückschreibungen über die GUI auszuführen:

1. Wählen Sie **Aktionen –> Wiederanlauffähige Zurückschreibungen** in der Hauptanzeige aus.
2. Wählen Sie die wiederanlauffähige Zurückschreibungssitzung aus, die ausgeführt werden soll.
3. Klicken Sie auf die Schaltfläche **Erneut starten** unten auf der Anzeige.

Zugehörige Verweise:
Resourceutilization
Restore
Windows-Betriebssysteme

Windows-Systemstatus zurückschreiben

Der Microsoft Volumeschattenkopie-Dienst (VSS = Volume Shadowcopy Service) wird auf Windows-Clients für Sichern/Archivieren unterstützt. Der Client verwendet VSS, um den Systemstatus zurückzuschreiben. Die Funktion für die Zurückschreibung des Systemstatus ist für Onlinezurückschreibungsoperationen des Systemstatus veraltet.

Informationen zu diesem Vorgang

Es ist nicht mehr möglich, den Systemstatus auf ein System zurückzuschreiben, das noch online ist. Verwenden Sie stattdessen die ASR-basierte Wiederherstellungsmethode zum Zurückschreiben des Systemstatus im Windows PE-Offlinemodus. Weitere Informationen finden Sie in den folgenden Wiki-Artikeln von IBM Spectrum Protect:

- Best Practices for Recovering Windows Server 2012 and Windows 8
- Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1

Wenn Sie versuchen, den Systemstatus mit dem Befehl dsmc restore systemstate über die GUI des Clients für Sichern/Archivieren oder den Web-Client zurückzuschreiben, wird die folgende Nachricht angezeigt:

```
ANS5189E Die Onlinezurückschreibung des Systemstatus ist veraltet. Verwenden Sie die
    Offline-WinPE-Methode für die Ausführung der Zurückschreibung des Systemstatus.
```

Zugehörige Konzepte:
Computer wiederherstellen, wenn das Windows-Betriebssystem nicht funktioniert
Zugehörige Verweise:
Restore Systemstate
Windows-Betriebssysteme

Dateien für die automatische Systemwiederherstellung zurückschreiben

Sie können Dateien für die automatische Systemwiederherstellung (Automated System Recovery - ASR) zurückschreiben, um die Datenträgerkonfigurationsdaten und den Systemstatus für das Windows-Betriebssystem wiederherzustellen, wenn ein schwerwiegender System- oder Hardwarefehler auftritt.

Vorbereitende Schritte

Sie müssen ein Mitglied der Gruppe 'Administratoren' oder 'Sicherungsoperatoren' sein, um ASR-Dateien sichern und zurückschreiben zu können.

Informationen zu diesem Vorgang

Der Client für Sichern/Archivieren schreibt ASR-Daten zurück, wenn der Client für Sichern/Archivieren den Windows-Systemstatus zurückschreibt.

Vorgehensweise

Für die Zurückschreibung von ASR-Dateien auf Windows-Betriebssystemen verwenden Sie den Befehl restore systemstate.
Zugehörige Konzepte:
Computer wiederherstellen, wenn das Windows-Betriebssystem nicht funktioniert
Windows-Betriebssysteme

Betriebssystem zurückschreiben, wenn der Computer in Betrieb ist

Ist Ihr Computer in Betrieb, können Sie das Betriebssystem aus gesicherten Dateien zurückschreiben.

Informationen zu diesem Vorgang

Ist Active Directory installiert, müssen Sie sich im Zurückschreibungsmodus von Active Directory befinden. Wenn Sie eine Betriebssystemwiederherstellung einschließlich Systemstatus ausführen, verwenden Sie die folgende Zurückschreibungsreihenfolge. Führen Sie zwischen den einzelnen Schritten keinen Neustart des Computers durch, selbst wenn Sie dazu aufgefordert werden.

Vorgehensweise

1. Schreiben Sie das Systemlaufwerk zurück. Beispiel: `dsmc restore c:\* -sub=yes -rep=all`.
2. Schreiben Sie den Systemstatus zurück. Beispiel: `dsmc restore systemstate`

Windows-Betriebssysteme

Computer wiederherstellen, wenn das Windows-Betriebssystem nicht funktioniert

Hat der Computer einen schwerwiegenden Hardware- oder Softwarefehler, können Sie ein Windows-Betriebssystem mit der automatischen Systemwiederherstellung (Automated System Recovery - ASR) wiederherstellen.

- Bootfähige WinPE-CD erstellen
  Bevor Sie einen Windows-Computer unter Verwendung der automatischen Systemwiederherstellung (Automated System Recovery, ASR) wiederherstellen können, müssen Sie eine bootfähige CD oder DVD der Windows-Vorinstallationsumgebung (WinPE) erstellen.
- Windows-Betriebssystem mit der automatischen Systemwiederherstellung zurückschreiben
  Sie können das Windows-Betriebssystem eines Computers mit der automatischen Systemwiederherstellung (Automated System Recovery, ASR) zurückschreiben.

Zugehörige Tasks:
Betriebssystem zurückschreiben, wenn der Computer in Betrieb ist
Windows-Betriebssysteme

Bootfähige WinPE-CD erstellen

Bevor Sie einen Windows-Computer unter Verwendung der automatischen Systemwiederherstellung (Automated System Recovery, ASR) wiederherstellen können, müssen Sie eine bootfähige CD oder DVD der Windows-Vorinstallationsumgebung (WinPE) erstellen.

Vorgehensweise

Anweisungen zur Erstellung einer bootfähigen WinPE-CD oder -DVD finden Sie in dem folgenden IBM Spectrum Protect-Wiki-Artikel:

- Best Practices for Recovering Windows Server 2012 and Windows 8
- Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1

Windows-Betriebssysteme

Windows-Betriebssystem mit der automatischen Systemwiederherstellung zurückschreiben

Sie können das Windows-Betriebssystem eines Computers mit der automatischen Systemwiederherstellung (Automated System Recovery, ASR) zurückschreiben.

Vorgehensweise

Anweisungen zum Zurückschreiben eines Windows-Systems unter Verwendung von ASR finden Sie in dem folgenden IBM Spectrum Protect-Wiki-Artikel:

- Best Practices for Recovering Windows Server 2012 and Windows 8
- Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1

Nächste Schritte

Sie können jetzt andere Datenträger zurückschreiben.
Zugehörige Tasks:
Bootfähige WinPE-CD erstellen
Clientoptionsdatei für die automatische Systemwiederherstellung erstellen
Zugehörige Verweise:
Restore
Restore Systemstate
 Windows-Betriebssysteme

Microsoft DFS-Baumstruktur und -Dateien zurückschreiben

Sollen DFS-Zusammenführungen und die Daten für jede Zusammenführung zurückgeschrieben werden, müssen Sie zunächst die Metadaten der DFS-Zusammenführung und dann jede Zusammenführung separat zurückschreiben.

Werden die Metadaten der Zusammenführung nicht zurückgeschrieben, erstellt IBM Spectrum Protect ein Verzeichnis unter dem DFS-Stamm mit dem Namen des Zusammenführungspunkts und schreibt die Daten in dieses Verzeichnis zurück.

Zugehörige Tasks:
Methoden für den Schutz von Microsoft DFS-Dateien
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Image zurückschreiben

Einige Punkte sind zu berücksichtigen, bevor Sie mit der Zurückschreibung von Images auf Ihr System beginnen.

Damit Sie eine Imagezurückschreibung (offline oder online) ausführen können, benötigen Sie die Administratorberechtigung auf dem System.

Beachten Sie die folgende Liste von Hinweisen, bevor Sie ein Image zurückschreiben:

- Durch das Zurückschreiben des Image eines Datenträgers werden die Daten in denselben Zustand zurückgeschrieben, den sie hatten, als die letzte Imagesicherung ausgeführt wurde. Sie müssen absolut sicher sein, dass Sie ein Image zurückschreiben müssen, da Ihr gesamtes aktuelles Dateisystem oder der unformatierte Datenträger durch das Image auf dem Server ersetzt wird.
-  WindowsDie Imagezurückschreibungsoperation überschreibt den Datenträgerkennsatz auf dem Zieldatenträger mit dem Datenträgerkennsatz, der auf dem Quellendatenträger vorhanden war.
- Stellen Sie sicher, dass der Datenträger, auf den Sie das Image zurückschreiben, mindestens so groß ist wie das Image, das zurückgeschrieben wird.
-  LinuxAuf Linux-Systemen verwenden einige Dateisysteme (z. B. ext2, ext3, ext4, btrfs und xfs) eine UUID (Universally Unique Identifier), um sich selbst im Betriebssystem zu identifizieren. Wenn Sie eine Imagesicherung eines solchen Datenträgers erstellen und an eine andere Position zurückschreiben, kann es sein, dass es zwei Datenträger mit derselben UUID gibt. Wenn Sie Ihre Dateisysteme mit einer UUID in /etc/fstab definieren, denken Sie daran, dass der Client für Sichern/Archivieren das zurückgeschriebene Dateisystem unter Umständen wegen eines UUID-Konflikts nicht korrekt anhängen kann. Um diese Situation zu vermeiden, sollten Sie das Image an seine ursprüngliche Position zurückschreiben. Wenn Sie es an eine andere Position zurückschreiben müssen, ändern Sie die UUID des ursprünglichen oder des zurückgeschriebenen Datenträgers, bevor Sie das zurückgeschriebene Dateisystem anhängen. Informationen zur Änderung einer UUID finden Sie in der Linux-Dokumentation. Möglicherweise müssen Sie auch die Datei /etc/fstab manuell bearbeiten, damit der ursprüngliche Datenträger und/oder der zurückgeschriebene Datenträger angehängt werden können.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDas Dateisystem oder der Datenträger, in das bzw. auf den zurückgeschrieben wird, muss denselben Typ wie das Original haben.
-  WindowsDas Dateisystem oder der Datenträger, in das bzw. auf den zurückgeschrieben wird, muss nicht denselben Typ wie das Original haben. Der Datenträger muss nicht einmal formatiert sein. Der Imagezurückschreibungsprozess erstellt das entsprechend formatierte Dateisystem für Sie.
- Stellen Sie sicher, dass der Zieldatenträger für die Zurückschreibung nicht im Gebrauch ist. Der Client sperrt den Datenträger, bevor die Zurückschreibung gestartet wird. Der Client entsperrt den Datenträger, wenn die Zurückschreibung beendet ist. Wird der Datenträger verwendet, wenn der Client versucht, das Dateisystem zu sperren, schlägt die Zurückschreibung fehl.
- Sie können ein Image nicht an eine Position zurückschreiben, auf der das IBM Spectrum Protect-Clientprogramm installiert ist.

- Windows-BetriebssystemeWenn Sie ein Image des Systemlaufwerks erstellt haben, können Sie das Image nicht an dieselben Position zurückschreiben, da der Client keine exklusive Sperre des Systemlaufwerks haben darf. Außerdem kann das Systemimage aufgrund unterschiedlicher Systemkomponentenkonfigurationen in den verschiedenen Komponenten (z. B. Active Directory) inkonsistent sein. Die Konfiguration einiger dieser Komponenten kann die Verwendung verschiedener Datenträger angeben, wobei diese teilweise im Systemlaufwerk, teilweise auf anderen Nicht-Systemlaufwerken installiert sind.
- Wurden fortlaufende Teilsicherungen *und* Imagesicherungen des Dateisystems ausgeführt, können Sie eine Imageteilzurückschreibung des Dateisystems ausführen. Bei dem Prozess werden einzelne Dateien zurückgeschrieben, nachdem das vollständige Image zurückgeschrieben wurde. Die einzelnen zurückgeschriebenen Dateien sind die Dateien, die nach dem ursprünglichen Image gesichert wurden. Wurden Dateien nach der ursprünglichen Sicherung gelöscht, können diese Dateien bei der Teilzurückschreibung wahlweise aus dem Basisimage gelöscht werden.

  Das Löschen von Dateien wird ordnungsgemäß ausgeführt, wenn die Sicherungskopiengruppe des IBM Spectrum Protect-Servers über genügend Versionen für vorhandene und gelöschte Dateien verfügt. Teilsicherungen und -zurückschreibungen können nur für angehängte Dateisysteme und nicht für unformatierte logische Datenträger ausgeführt werden.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSollte ein zurückgeschriebenes Image aus irgendeinem Grund beschädigt sein, können Sie versuchen, es mit dem Tool `fsck` zu reparieren.

  Sie können die Option verifyimage im Befehl restore image verwenden, um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client eine Warnung auf der Konsole und im Fehlerprotokoll aus.

  Befinden sich defekte Sektoren auf dem Zieldatenträger, können Sie die Option imagetofile im Befehl restore image verwenden, um anzugeben, dass das Quellenimage in eine Datei zurückgeschrieben werden soll. Später können Sie ein Datenkopierprogramm Ihrer Wahl verwenden, um das Image von der Datei auf einen Plattendatenträger zu übertragen.

- Windows-BetriebssystemeFalls ein zurückgeschriebenes Image aus irgendeinem Grund beschädigt ist, sollten Sie *chkdsk* ausführen, um nach defekten Sektoren zu suchen und diese zu reparieren (sofern der zurückgeschriebene Datenträger nicht unformatiert (RAW) ist).

  Sie können die Option verifyimage im Befehl restore image verwenden, um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client eine Warnung auf der Konsole und im Fehlerprotokoll aus.

  Befinden sich defekte Sektoren auf dem Zieldatenträger, können Sie die Option imagetofile im Befehl restore image verwenden, um anzugeben, dass das Quellenimage in eine Datei zurückgeschrieben werden soll. Später können Sie ein Datenkopierprogramm Ihrer Wahl verwenden, um das Image von der Datei auf einen Plattendatenträger zu übertragen.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeImage über die GUI zurückschreiben
  Sie können die GUI verwenden, um ein Image Ihres Dateisystems oder unformatierten logischen Datenträgers zurückzuschreiben.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeImage über die Befehlszeile zurückschreiben
  Verwenden Sie den Befehl restore image, um ein Image über den IBM Spectrum Protect-Befehlszeilenclient zurückzuschreiben.

Zugehörige Verweise:
Imagetofile
Verifyimage
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Image über die GUI zurückschreiben

Sie können die GUI verwenden, um ein Image Ihres Dateisystems oder unformatierten logischen Datenträgers zurückzuschreiben.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um ein Image Ihres Dateisystems oder unformatierten logischen Datenträgers zurückzuschreiben:

Vorgehensweise

1. Klicken Sie auf **Zurückschreiben** im Hauptfenster. Das Fenster 'Zurückschreiben' wird angezeigt.
2. Verzeichnisebenen der Verzeichnisbaumstruktur einblenden.
3. Lokalisieren Sie das Objekt in der Baumstruktur mit dem Namen **Image** und erweitern Sie das Objekt. Klicken Sie auf das Auswahlfeld neben dem Image, das Sie zurückschreiben wollen. Detaillierte Informationen über das Objekt erhalten Sie, wenn Sie das Objekt hervorheben und **Sicht → Dateiinformationen...** im Hauptfenster auswählen oder auf die Schaltfläche **Dateiinformationen anzeigen** klicken.
4. **(Optional)** Zum Ausführen einer Imageteilzurückschreibung klicken Sie auf die Schaltfläche **Optionen**, um das Fenster für Zurückschreibungsoptionen aufzurufen. Wählen Sie dann die Option **Image plus Teilsicherung von Verzeichnissen und Dateien** aus. Möchten Sie inaktive Dateien aus Ihrem lokalen Dateisystem löschen, wählen Sie das Kontrollkästchen **Inaktive Dateien von Lokal löschen** aus. Klicken Sie auf die Schaltfläche **OK**.

5. AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeKlicken Sie auf **Zurückschreiben**. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Das Image kann auf den Datenträger mit dem Mountpunkt zurückgeschrieben werden, von dem es ursprünglich gesichert wurde. Alternativ kann ein anderer Datenträger als Zurückschreibungsziel ausgewählt werden.
6. Windows-BetriebssystemeKlicken Sie auf **Zurückschreiben**. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Das Image kann auf den Datenträger mit dem Laufwerkbuchstaben oder Mountpunkt zurückgeschrieben werden, von dem es ursprünglich gesichert wurde. Alternativ kann ein anderer Datenträger als Zurückschreibungsziel ausgewählt werden.
7. Klicken Sie auf die Schaltfläche **Zurückschreiben**, um die Zurückschreibung zu starten. Das Fenster **Taskliste** erscheint, das den Fortschritt der Zurückschreibung anzeigt. Das Fenster 'Zurückschreibungsbericht' zeigt einen ausführlichen Statusbericht an.

Ergebnisse

Die folgenden Hinweise sind zu beachten, wenn Sie eine Imagezurückschreibung über die GUI ausführen:

- Sie können **Sicht → Dateiinformationen** im Hauptfenster auswählen oder auf die Schaltfläche **Dateiinformationen anzeigen** klicken, um die folgenden Statistiken über Dateisystemimages anzuzeigen, die vom Client gesichert wurden:
  - Imagegröße - Dies ist die Größe des Datenträgers, der gesichert wurde.
  - AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeGespeicherte Größe - Dies ist die Größe des Image, das tatsächlich auf dem Server gespeichert wurde. Das auf dem IBM Spectrum Protect-Server gespeicherte Image hat dieselbe Größe wie der Datenträger.
  - Windows-BetriebssystemeGespeicherte Größe - Dies ist die Größe des Image, das tatsächlich auf dem Server gespeichert wurde. Da bei Imagesicherungen nur die belegten Blöcke in einem Dateisystem gesichert werden können, kann die Größe des auf dem IBM Spectrum Protect-Server gespeicherten Image kleiner sein als die Datenträgergröße. Bei Online-Imagesicherungen kann das gespeicherte Image aufgrund der Größe der Cachedateien größer als das Dateisystem sein.
  - Dateisystemtyp
  - Sicherungsdatum und -zeit
  - Die der Imagesicherung zugeordnete Verwaltungsklasse
  - Ob die Imagesicherung eine aktive oder inaktive Kopie ist
- Um bestimmte Zurückschreibungsoptionen zu ändern, klicken Sie auf die Schaltfläche **Optionen**. Die geänderten Optionen sind *nur* während der aktuellen Sitzung wirksam.
- Im Fenster für Zurückschreibungsoptionen können Sie auswählen, ob Sie nur das Image oder zusätzlich die über Teilsicherung gesicherten Verzeichnisse und Dateien zurückschreiben wollen. Wenn Sie **Nur Image** auswählen, wird nur das Image von Ihrer letzten Imagesicherung zurückgeschrieben. Dies ist der Standardwert.

  Haben Sie jedoch Imageteilsicherung nach Datum für einen Datenträger oder Imagesicherungen auf einem über Teilsicherungen gesicherten Datenträger ausgeführt, können Sie die Option **Image plus Teilsicherung von Verzeichnissen und Dateien** auswählen. Wenn Sie **Image plus Teilsicherung von Verzeichnissen und Dateien** auswählen, können Sie auch **Inaktive Dateien von Lokal löschen** auswählen, um inaktive Dateien zu löschen, die in Ihr lokales Dateisystem zurückgeschrieben werden. Haben Sie für das Dateisystem als einzigen Teilsicherungstyp Imageteilsicherung nach Datum ausgeführt, werden keine Dateien gelöscht.

  Wichtig: Sie müssen absolut sicher sein, dass Sie eine Teilzurückschreibung ausführen müssen, da Ihr gesamtes Dateisystem durch das Image auf dem Server ersetzt wird und anschließend die Dateien zurückgeschrieben werden, die Sie mit der Imageteilsicherungsoperation gesichert haben.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Image über die Befehlszeile zurückschreiben

Verwenden Sie den Befehl restore image, um ein Image über den IBM Spectrum Protect-Befehlszeilenclient zurückzuschreiben.

Windows-BetriebssystemeSie können die Option verifyimage im Befehl restore image verwenden, um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt IBM Spectrum Protect eine Warnung auf der Konsole und im Fehlerprotokoll aus.

Windows-BetriebssystemeBefinden sich defekte Sektoren auf dem Zieldatenträger, können Sie die Option imagetofile im Befehl restore image verwenden, um anzugeben, dass das Quellenimage in eine Datei zurückgeschrieben werden soll. Später können Sie ein Datenkopierprogramm Ihrer Wahl verwenden, um das Image von der Datei auf einen Plattendatenträger zu übertragen.

Zugehörige Verweise:
Imagetofile
Verifyimage

Daten aus einem Sicherungssatz zurückschreiben

Ihr IBM Spectrum Protect-Administrator kann einen Sicherungssatz (d. h. eine Sammlung Ihrer Dateien, die sich auf dem Server befinden) auf Wechseldatenträgern generieren und diese auf einer Einheit mit einem Format erstellen, das mit der Clienteinheit kompatibel ist.

Sie können die Daten aus einem Sicherungssatz vom IBM Spectrum Protect-Server zurückschreiben oder aus einem Sicherungssatz, der lokal als Datei oder auf einer Bandeinheit verfügbar ist.

Sie können Sicherungssätze von folgenden Positionen zurückschreiben:

- Vom IBM Spectrum Protect-Server
- Von Wechseldatenträgern auf einer Einheit, die an Ihre Client-Workstation angeschlossen ist
- Von einer Sicherungssatzdatei auf Ihrer Client-Workstation

Sicherungssätze ermöglichen wie in der nachfolgenden Liste beschrieben die sofortige Archivierung und schnelle Wiederherstellung.

Sofortarchivierung
: Diese Fähigkeit erlaubt es einem Administrator, eine Archivierungssammlung aus Sicherungsversionen zu erstellen, die bereits auf dem Server gespeichert sind.

Schnelle Wiederherstellung mit lokalen Sicherungssätzen
: In der Regel werden Zurückschreibungen von normalen Dateisicherungen ausgeführt, die auf dem IBM Spectrum Protect-Server außerhalb von Sicherungssätzen gespeichert sind. Mit dieser Zurückschreibungsmethode können Sie die neueste Sicherungsversion jeder Datei zurückschreiben. Ein Sicherungssatz enthält möglicherweise nicht die neueste Sicherungsversion Ihrer Dateien.

  In manchen Fällen stellt die Zurückschreibung von Daten aus einem Sicherungssatz eine bessere Option als die Zurückschreibung von Daten aus normalen Sicherungsdateien auf dem IBM Spectrum Protect-Server dar. Die Zurückschreibung aus einem Sicherungssatz kann aus folgenden Gründen eine bessere Option sein:

  - Die Zurückschreibung aus einem Sicherungssatz kann schneller sein, da alle für die Zurückschreibung erforderlichen Dateien sich zusammen auf einer kleineren Anzahl von Speicherdatenträgern befinden.
  - Ein Sicherungssatz stellt eine Sammlung von Dateien nach Zeitpunkt dar. Sie können eine zeitpunktgesteuerte Zurückschreibung ausführen, während Sie bei einer normalen Zurückschreibung auf Dateiebene vom Server den aktuellen Stand zurückschreiben.
  - Windows-BetriebssystemeMit einem Sicherungssatzdatenträger können Sie eine ASR-Zurückschreibung ausführen.

  Die Zurückschreibung eines Sicherungssatzes vom IBM Spectrum Protect-Server bietet mehr Zurückschreibungsoptionen als die Zurückschreibung von einem lokalen Sicherungssatz. Dennoch kann die Zurückschreibung aus einem lokalen Sicherungssatz in einigen Fällen Vorteile bieten:

  - Eventuell müssen Sie Ihre Daten zurückschreiben, wenn keine Netzverbindung zum IBM Spectrum Protect-Server besteht. Dies ist bei einer Wiederherstellung nach einem Katastrophenfall möglich.
  - Die lokale Zurückschreibung benötigt möglicherweise weniger Zeit als die Zurückschreibung über eine Netzverbindung zu Ihrem IBM Spectrum Protect-Server.

Ein Sicherungssatz kann vom IBM Spectrum Protect-Server zurückgeschrieben werden, während die Sicherungssatzdatenträger für den Server verfügbar sind, oder sie können für eine lokale Sicherungssatzzurückschreibung auf das Clientsystem übertragen werden. Ein Sicherungssatz kann mit oder ohne Inhaltsverzeichnis (table of contents - TOC) generiert werden und kann Dateidaten oder Imagedaten enthalten.

Windows-BetriebssystemeDer Sicherungssatz kann Systemstatusdaten enthalten.

Ihre Möglichkeiten zum Zurückschreiben von Daten aus Sicherungssätzen sind von der Position des Sicherungssatzes und vom Typ der Daten im Sicherungssatz abhängig. Der Befehlszeilenclient kann einige Daten zurückschreiben, die die GUI nicht zurückschreiben kann. Die GUI ermöglicht Ihnen jedoch das Anzeigen und Auswählen der zurückzuschreibenden Objekte. Im Allgemeinen bieten Sicherungssätze mit Inhaltsverzeichnis, die auf dem Server gespeichert sind, mehr Zurückschreibungsoptionen. In manchen Fällen bieten lokale Sicherungssätze jedoch nützlichere Optionen als die Zurückschreibung vom IBM Spectrum Protect-Server.

Die Einschränkungen, die für das Zurückschreiben von Daten aus Sicherungssätzen über die GUI gelten, sind in der folgenden Tabelle zusammengefasst. Jede innen liegende Zelle stellt eine Kombination aus Datentyp und Position des Sicherungssatzes dar. Für jede Situation gibt die Zelle an, ob Sie die GUI verwenden können, um nur den gesamten Sicherungssatz zurückzuschreiben bzw. um Objekte innerhalb des Sicherungssatzes auszuwählen oder ob Sie nicht die GUI verwenden können, um den Sicherungssatz zurückzuschreiben.

Tabelle 1. Einschränkungen beim Zurückschreiben von Sicherungssätzen über die GUI

	Position des Sicherungssatzes		
Datentyp im Sicherungssatz	**Lokal `location=file` oder `location=tape`)**	**IBM Spectrum Protect-Server (TOC verfügbar)**	**IBM Spectrum Protect-Server (TOC nicht verfügbar)**
Datei	Nur gesamten Sicherungssatz zurückschreiben	Gesamten Sicherungssatz oder ausgewählte Objekte im Sicherungssatz zurückschreiben	Nur gesamten Sicherungssatz zurückschreiben
Image	Zurückschreiben nicht möglich	Gesamten Sicherungssatz oder ausgewählte Objekte im Sicherungssatz zurückschreiben	Zurückschreiben nicht möglich
Systemstatus	Nur gesamten Sicherungssatz zurückschreiben	Gesamten Sicherungssatz oder ausgewählte Objekte im Sicherungssatz zurückschreiben	Nur gesamten Sicherungssatz zurückschreiben

Die Einschränkungen, die für das Zurückschreiben von Daten aus Sicherungssätzen über den Befehlszeilenclient gelten, sind in der folgenden Tabelle zusammengefasst. Jede innen liegende Zelle stellt eine Kombination aus Datentyp und Position des Sicherungssatzes dar. Für jede

Situation listet die Zelle die Befehle zum Zurückschreiben auf, die verwendet werden können. Wenn nicht anders angegeben, können Sie bestimmte Objekte in einem Sicherungssatz sowie den gesamten Sicherungssatz zurückschreiben.

Tabelle 2. Einschränkungen beim Zurückschreiben von Sicherungssätzen über die Befehlszeile

Datentyp im Sicherungssatz	Position des Sicherungssatzes		
	Lokal `location=file` oder `location=tape`)	IBM Spectrum Protect-Server (TOC verfügbar)	IBM Spectrum Protect-Server (TOC nicht verfügbar)

Datei	Befehle:
	
	`restore`
	`restore backupset`
		Befehle:
		
		`restore`
		`restore backupset`
			Befehle:
			
			`restore backupset`

Image	Zurückschreiben nicht möglich	Befehl: `restore image`	Zurückschreiben nicht möglich

Systemstatus	Befehl:
	
	`restore backupset`
		Befehle:
		
		`restore backupset`
		`restore systemstate`
			Befehl:
			
			`restore backupset`

Einschränkung: Beim Zurückschreiben des Systemstatus mit dem Befehl restore backupset können Sie keine einzelnen Objekte angeben. Sie können nur den gesamten Systemstatus zurückschreiben.

- Sicherungssätze zurückschreiben: Hinweise und Einschränkungen
  In diesem Abschnitt sind einige Hinweise und Einschränkungen aufgeführt, die Sie beim Zurückschreiben von Sicherungssätzen beachten müssen.
- Zurückschreibung von Sicherungssätzen
  IBM Spectrum Protect betrachtet einen Sicherungssatz als ein Objekt, das die gesamte Dateistruktur enthält. Sie können den gesamten Sicherungssatz zurückschreiben oder in einigen Fällen Teile des Satzes auswählen. Die Sicherungssatzdatenträger sind selbstbeschreibend und enthalten alle Informationen, die für eine erfolgreiche Zurückschreibung erforderlich sind.
- Sicherungssätze über die GUI zurückschreiben
  Die Client-GUI kann Daten aus einem Sicherungssatz auf dem Server, aus einer lokalen Datei oder von einer lokalen Bandeinheit zurückschreiben. Sie können die GUI verwenden, um einzelne Dateien aus einem Sicherungssatz mit einem Inhaltsverzeichnis vom IBM Spectrum Protect-Server zurückzuschreiben. Dies ist jedoch weder bei lokalen Sicherungssätzen noch bei Sicherungssätzen vom Server ohne Inhaltsverzeichnis möglich.
- Sicherungssätze mit der Befehlszeilenschnittstelle des Clients zurückschreiben
  Die Befehlszeilenschnittstelle des Clients kann Daten aus einem Sicherungssatz auf dem Server, aus einer lokalen Datei oder von einer lokalen Bandeinheit zurückschreiben. Sie können mit der Befehlszeilenschnittstelle des Clients einzelne Dateien aus lokalen Sicherungssätzen und aus Sicherungssätzen ohne Inhaltsverzeichnis zurückschreiben.

Zugehörige Verweise:
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Localbackupset
Query Backupset
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Query Image
Restore
Restore Backupset
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Restore Image
Windows-BetriebssystemeRestore Systemstate

Sicherungssätze zurückschreiben: Hinweise und Einschränkungen

In diesem Abschnitt sind einige Hinweise und Einschränkungen aufgeführt, die Sie beim Zurückschreiben von Sicherungssätzen beachten müssen.

Hinweise für das Zurückschreiben von Sicherungssätzen

Beachten Sie beim Zurückschreiben von Sicherungssätzen die folgenden Hinweise:

- Wenn das zurückzuschreibende Objekt auf einem Clientknoten generiert wurde, dessen Name sich von Ihrem aktuellen Knotennamen unterscheidet, geben Sie in allen Zurückschreibungsbefehlen den ursprünglichen Knotennamen im Parameter filespacename an.
- Ist das Zurückschreiben eines Sicherungssatzes von einem austauschbaren Datenträger nicht möglich, ist zusammen mit dem IBM Spectrum Protect-Administrator zu überprüfen, ob der austauschbare Datenträger auf einer Einheit erstellt wurde, auf der ein kompatibles Format verwendet wurde.
- Wenn Sie den Befehl restore backupset in der Anfangsbefehlszeile mit dem Parameter `-location=tape` oder `-location=file` verwenden, versucht der Client nicht, eine Verbindung zum IBM Spectrum Protect-Server herzustellen.

- Beim Zurückschreiben einer Gruppe aus einem Sicherungssatz:

    - Die gesamte Gruppe bzw. alle Gruppen im virtuellen Dateibereich werden zurückgeschrieben. Wenn sich in einem virtuellen Dateibereich mehrere Gruppen befinden, ist es nicht möglich, durch Angabe des Gruppennamens eine einzige Gruppe zurückzuschreiben. Es ist nicht möglich, durch Angabe eines Dateipfads eine Gruppe teilweise zurückzuschreiben.
    - Geben Sie eine Gruppe über einen der folgenden Werte an:
        - Geben Sie den Namen des virtuellen Dateibereichs mit dem Parameter Dateibereichsname an.
        - Verwenden Sie die Option subdir, um Unterverzeichnisse einzuschließen.
- Eine begrenzte Unterstützung wird für das Zurückschreiben von Sicherungssätzen auf Bandeinheiten bereitgestellt, die an das Clientsystem angeschlossen sind. Sie müssen immer einen nativen Einheitentreiber verwenden, der vom Hersteller der Einheit bereitgestellt wird. Der Einheitentreiber, der von IBM für die Verwendung mit dem IBM Spectrum Protect-Server bereitgestellt wird, kann nicht auf dem Clientsystem zum Zurückschreiben lokaler Sicherungssätze benutzt werden.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeEnthält ein Sicherungssatz Dateien von mehreren Eignern, ist der Sicherungssatz selbst Eigentum der Rootbenutzer-ID und er wird Benutzer-IDs ohne Rootberechtigung nicht angezeigt. In diesem Fall können Benutzer-IDs ohne Rootberechtigung ihre Dateien zurückschreiben, indem sie den Namen des Sicherungssatzes vom IBM Spectrum Protect-Administrator anfordern. Andere Benutzer als Root können nur eigene Dateien zurückschreiben.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeSoll die grafische Benutzerschnittstelle des Clients einen Sicherungssatz von einer lokalen Einheit zurückschreiben, ohne dass eine Serververbindung erforderlich ist, verwenden Sie die Option localbackupset.

Einschränkungen beim Zurückschreiben von Sicherungssätzen

Beachten Sie beim Zurückschreiben von Sicherungssätzen die folgenden Einschränkungen:

- Sicherungssatzdaten, die mit der API gesichert wurden, können weder zurückgeschrieben noch verwendet werden.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeMit dem Befehl restore backupset können Sie keine Imagedaten aus einem Sicherungssatz zurückschreiben. Imagedaten aus einem Sicherungssatz können Sie nur mit dem Befehl restore image zurückschreiben.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeSie können keine Imagedaten aus einem lokalen Sicherungssatz (`location=tape` oder `location=file`) zurückschreiben. Imagedaten aus einem Sicherungssatz können Sie nur vom IBM Spectrum Protect-Server zurückschreiben.

Zurückschreibung von Sicherungssätzen

IBM Spectrum Protect betrachtet einen Sicherungssatz als ein Objekt, das die gesamte Dateistruktur enthält. Sie können den gesamten Sicherungssatz zurückschreiben oder in einigen Fällen Teile des Satzes auswählen. Die Sicherungssatzdatenträger sind selbstbeschreibend und enthalten alle Informationen, die für eine erfolgreiche Zurückschreibung erforderlich sind.

Wenn eine Verbindung zu dem Tivoli Storage Manager-Server der Version 5.4 oder höher besteht, kann Ihr Serveradministrator gestapelte Sicherungssätze erstellen. Diese Sicherungssätze können Daten mehrerer Clientknoten und verschiedene Datentypen für einen bestimmten Clientknoten enthalten. Bei den Datentypen kann es sich um Dateidaten oder Imagedaten handeln.

Windows-BetriebssystemeWenn Sie ein Upgrade von Tivoli Storage Manager Express durchgeführt haben, werden auch einige Anwendungsdaten unterstützt.

Einschränkung: Die Zurückschreibungsverarbeitung von Imagedaten und Anwendungsdaten ist nur verfügbar, wenn die Zurückschreibung vom Server erfolgt. Imagedaten und Anwendungsdaten können Sie nicht aus lokalen Sicherungssätzen auf dem Client zurückschreiben.

Wenn ein Sicherungssatz gestapelt ist, können Sie nur Daten für Ihren eigenen Knoten zurückschreiben. Die Daten aller anderen Knoten werden übersprungen. Wenn Daten aus einem gestapelten Sicherungssatz auf einer lokalen Einheit zurückgeschrieben werden, können Sie nur Daten auf Dateiebene für Ihren eigenen Clientknoten zurückschreiben. Es ist wichtig, dass die Option nodename so eingestellt ist, dass sie für einen der Knoten im Stapelspeicher dem Knotennamen entspricht, der zum Generieren des Sicherungssatzes verwendet wurde.

Wichtig: Aufgrund der Portierbarkeit lokaler Sicherungssätze müssen Sie Ihre lokalen Sicherungssätze auf Wechseldatenträgern durch zusätzliche Maßnahmen sichern. Die Datenträger für Sicherungssätze müssen physisch gesichert werden, weil der Sicherungssatz ohne Authentifizierung beim Server lokal zurückgeschrieben werden kann. Jeder Benutzer hat Zugriff auf alle Daten in dem gestapelten Sicherungssatz; dies bedeutet, dass der Benutzer Zugriff auf Daten habt, die ihm nicht gehören, indem er den Knotennamen ändert oder den Sicherungssatz im unformatierten Format anzeigt. Verschlüsselung oder physischer Schutz der Datenträger sind die einzigen Möglichkeiten zum Schutz der Daten.

Wenn Sie Sicherungssatzdaten vom Server zurückschreiben, können einzelne Dateien, Verzeichnisse oder die gesamten Sicherungssatzdaten in einer einzigen Operation von der GUI oder der Befehlszeile zurückgeschrieben werden. Wenn Sie Sicherungssatzdaten lokal zurückschreiben, kann die GUI nur einen vollständigen Sicherungssatz anzeigen und zurückschreiben. Sie können die Befehlszeile verwenden, um einzelne Dateien oder Verzeichnisse zurückzuschreiben, die in einem Sicherungssatz lokal gespeichert sind.

Sicherungssätze über die GUI zurückschreiben

Die Client-GUI kann Daten aus einem Sicherungssatz auf dem Server, aus einer lokalen Datei oder von einer lokalen Bandeinheit zurückschreiben. Sie können die GUI verwenden, um einzelne Dateien aus einem Sicherungssatz mit einem Inhaltsverzeichnis vom IBM Spectrum Protect-Server zurückzuschreiben. Dies ist jedoch weder bei lokalen Sicherungssätzen noch bei Sicherungssätzen vom Server ohne Inhaltsverzeichnis möglich.

Informationen zu diesem Vorgang

Wichtig: Bevor Sie eine Zurückschreibungsoperation beginnen, beachten Sie, dass Sicherungssätze Daten für mehrere Dateibereiche enthalten können. Wenn Sie ein anderes Ziel als die ursprüngliche Position angeben, werden Daten aus *allen* Dateibereichen an die angegebenen Position zurückgeschrieben.

Führen Sie folgende Schritte aus, um einen Sicherungssatz über die GUI zurückzuschreiben:

1. Mac OS X-BetriebssysemeAIX-BetriebssysteLinux-BetriebssysteOracle Solaris-Betriebssysteme Windows-BetriebssysemeKlicken Sie auf Zurückschreiben im GUI-Hauptfenster. Das Fenster 'Zurückschreiben' wird angezeigt.
2. Lokalisieren Sie das Objekt Sicherungssätze in der Verzeichnisbaumstruktur und erweitern Sie es, indem Sie auf das Pluszeichen (+) daneben klicken.
   - Mac OS X-BetriebssysemeAIX-BetriebssysteLinux-BetriebssysteOracle Solaris-Betriebssysteme Windows-BetriebssysemeSoll der Sicherungssatz von einer lokalen Einheit zurückgeschrieben werden, erweitern Sie das Objekt Lokal. Das Fenster 'Position für Sicherungssatz angeben' wird angezeigt. Wählen Sie im Fenster Dateiname: oder Bandname: in der Liste aus und geben Sie die Position des Band- oder Dateinamens ein. Sie können auch auf die Schaltfläche Durchsuchen klicken, um ein Dateiauswahlfenster zu öffnen und einen Sicherungssatz auszuwählen.
   - Zum Zurückschreiben von Daten aus einem Sicherungssatz auf dem Server müssen Sie zuerst das Objekt Server und anschließend Dateiebene oder Image erweitern, je nachdem, welche Art der Zurückschreibung angefordert wird.
3. Klicken Sie auf das Auswahlfeld, das sich neben dem zurückzuschreibenden Sicherungssatz bzw. neben dem zurückzuschreibenden Verzeichnis oder der zurückzuschreibenden Datei innerhalb des Sicherungssatzes befindet.

   Sie können Dateien innerhalb eines Sicherungssatzes auswählen, wenn der Sicherungssatz sich auf dem Server befindet und über ein Inhaltsverzeichnis verfügt.

4. Klicken Sie auf Zurückschreiben. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Geben Sie die entsprechenden Informationen ein.
5. Klicken Sie auf Zurückschreiben. Im Fenster 'Task-Liste' wird der Verarbeitungsstatus der Zurückschreibung angezeigt.

Anmerkung:

- Wenn das Objekt, das Sie zurückschreiben wollen, Teil eines auf einem Knoten generierten Sicherungssatzes ist und der Knotenname auf dem Server geändert wird, stimmen keine Sicherungssatzobjekte, die vor der Namensänderung generiert wurden, mit dem neuen Knotennamen überein. Stellen Sie sicher, dass der Knotenname derselbe ist wie für den Knoten, für den der Sicherungssatz generiert wurde.
- Mac OS X-BetriebssysemeAIX-BetriebssysteLinux-BetriebssysteOracle Solaris-Betriebssysteme Windows-BetriebssysemeDer Client kann verwendet werden, um einen Sicherungssatz auf einer angeschlossenen Einheit mit oder ohne Serververbindung zurückzuschreiben. Schlägt die Serververbindung fehl, wird eine Eingabeaufforderung angezeigt, um die Zurückschreibung des lokalen Sicherungssatzes fortzusetzen. Außerdem kann der Client über die Option localbackupset angewiesen werden, keine Verbindung zum Server herzustellen.
- Mac OS X-BetriebssysemeAIX-BetriebssysteLinux-BetriebssysteOracle Solaris-Betriebssysteme Windows-BetriebssysemeFür bestimmte lokale Einheiten wie Bandeinheiten (Bandeinheiten gelten nicht für Mac OS X) müssen Einheitentreiber installiert werden, bevor eine Zurückschreibung ausgeführt werden kann. Das Handbuch zur Einheit bietet Unterstützung bei dieser Task. Sie müssen auch die Einheitenadresse kennen, um die Zurückschreibung ausführen zu können.
- Mac OS X-BetriebssysemeAIX-BetriebssysteLinux-BetriebssysteOracle Solaris-Betriebssysteme Windows-BetriebssysemeDie folgenden Features einer Sicherungssatzzurückschreibung vom Server stehen bei einer lokalen Zurückschreibung nicht zur Verfügung:
  1. Mac OS X-BetriebssysemeAIX-BetriebssysteLinux-BetriebssysteOracle Solaris-Betriebssysteme Windows-BetriebssysemeImagezurückschreibung.
  2. Windows-BetriebssysemeZurückschreibung einzelner Systemstatuskomponenten.
  3. Mac OS X-BetriebssysemeAIX-BetriebssysteLinux-BetriebssysteOracle Solaris-Betriebssysteme Windows-BetriebssysemeDie GUI-Anzeige und -Zurückschreibung einzelner Dateien und Verzeichnisse. Die Befehlszeile kann verwendet werden, um ein einzelnes Verzeichnis oder eine einzelne Datei aus einem lokalen Sicherungssatz zurückzuschreiben.
  4. Windows-BetriebssysemeZurückschreibung von Anwendungsdaten, wenn der Server von dem Produkt Tivoli Storage Manager Express migriert wurde.

Sicherungssätze mit der Befehlszeilenschnittstelle des Clients zurückschreiben

Die Befehlszeilenschnittstelle des Clients kann Daten aus einem Sicherungssatz auf dem Server, aus einer lokalen Datei oder von einer lokalen Bandeinheit zurückschreiben. Sie können mit der Befehlszeilenschnittstelle des Clients einzelne Dateien aus lokalen Sicherungssätzen und aus Sicherungssätzen ohne Inhaltsverzeichnis zurückschreiben.

Wenn Sie einen Sicherungssatz über die Befehlszeilenschnittstelle des Clients zurückschreiben wollen, verwenden Sie den Befehl query backupset, um die verfügbaren Sicherungssatzdaten anzuzeigen. Anschließend schreiben Sie die Daten mit Zurückschreibungsbefehlen zurück.

Mit den folgenden Befehlen können Sie Daten aus Sicherungssätzen zurückschreiben:

- restore
- restore backupset
- restore image
- Windows-Betriebssystemerestore systemstate

Verwenden Sie den korrekten Befehl für die Position des Sicherungssatzes und die Daten in dem Sicherungssatz. Weitere Informationen siehe Tabelle 2.

Zugehörige Verweise:
Query Backupset
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeQuery Image
Restore
Restore Backupset
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeRestore Image
Windows-BetriebssystemeRestore Systemstate
Windows-Betriebssysteme

Net Appliance-CIFS-Freigaben zurückschreiben

Das Zurückschreiben der Freigabedefinition erfordert das Zurückschreiben des Stammverzeichnisses des Freigabedateibereichs, das in den meisten Fällen wie folgt durchgeführt werden kann: `dsmc rest \\NetAppFiler\CifsShareName\ -dirsonly`.

Die folgende Ausgabe zeigt an, dass das Stammverzeichnis (und die Freigabedefinition) zurückgeschrieben wurden:

```
Zurückschreiben         0 \\NetAppFiler\CifsShareName\ [Fertig]
```

Wird die CIFS-Freigabedefinition auf dem Net Appliance-Dateiserver gelöscht, ist der Client nicht in der Lage, die Freigabedefinition direkt zurückzuschreiben, da die Freigabe nicht mehr zugänglich ist.

Die Freigabedefinition kann indirekt zurückgeschrieben werden, indem eine temporäre lokale Freigabe erstellt und die Freigabedefinition wie folgt in die temporäre Freigabe zurückgeschrieben wird:

```
 md c:\tempdir  net share tempshare=c:\tempdir
/Anmerkung: "Temporäre Freigabe zum Zurückschreiben einer gelöschten CIFS-Freigabe"
 net use z: \\LocalMachineName\tempshare
 dsmc res \\NetAppFiler\CifsShareName\ z:\ -dirsonly
```

Dadurch wird die ursprüngliche Freigabedefinition (einschließlich der Berechtigungen) auf den Dateiserver zurückgeschrieben.

Ältere Versionen des IBM Spectrum Protect-Servers haben unter Umständen ein Problem, das das Zurückschreiben des Stammverzeichnisses und der CIFS-Freigabedefinition verhindert. Falls dieses Problem auftritt, kann es umgangen werden, indem Sie eine der folgenden Methoden verwenden:

1. Verwenden Sie die Testmarkierung DISABLENQR wie folgt, um das Stammverzeichnis zurückzuschreiben:

   ```
   dsmc res \\NetAppFiler\CifsShareName\ -test=disablenqr  -dirsonly
   ```

2. Verwenden Sie die Befehlszeilenclientoption `-pick` mit dem Befehl restore und wählen Sie das Stammverzeichnis aus:

   ```
   dsmc res \\NetAppFiler\CifsShareName\  -dirsonly -pick
   ```

Zugehörige Tasks:
Net Appliance-CIFS-Freigabedefinition sichern
Linux-Betriebssysteme Windows-Betriebssysteme

Daten aus einer VMware-Sicherung zurückschreiben

Es gibt mehrere Möglichkeiten, Daten aus Sicherungen auf einer virtuellen VMware-Maschine zurückzuschreiben. Die Zurückschreibungsmethode ist vom Sicherungstyp und von der Version der Software des Clients für Sichern/Archivieren abhängig, mit der Sie die Zurückschreibung ausführen.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Linux-Betriebssysteme Windows-BetriebssystemeVollständige VM-Zurückschreibung
Linux-Betriebssysteme Windows-BetriebssystemeMit dem Befehl restore vm können Sie eine vollständige virtuelle Maschine aus einer vollständigen VM-Sicherung zurückschreiben. Wenn Sie eine vollständige VM-Sicherung zurückschreiben, ersetzt das zurückgeschriebene Image die virtuelle Maschine oder eine neue virtuelle Maschine wird erstellt. Bei einer vollständigen VM-Zurückschreibung schreiben Sie alle VMware-Dateien und den Systemstatus auf Windows-Systemen zurück. Wenn Sie Zugriff auf IBM Spectrum Protect Recovery Agent haben, können Sie einzelne Dateien zurückschreiben.
Linux-Betriebssysteme Windows-BetriebssystemeVerwenden Sie, abhängig von der Version des Clients für Sichern/Archivieren, die auf dem VMware-Client ausgeführt wird, die entsprechende Methode für die Zurückschreibung einer VM-Gesamtsicherung:

Versionen des Clients für Sichern/Archivieren vor Version 6.2.2:
Schreiben Sie die vollständige VM-Sicherung mit VMware Consolidated Backup zurück. Weitere Informationen finden Sie im folgenden Abschnitt:

Mit VMware Consolidated Backup erstellte vollständige VM-Sicherungen zurückschreiben

Version 6.2.2 oder höhere Versionen des Clients für Sichern/Archivieren
Schreiben Sie die VM-Gesamtsicherung mit der vStorage-API zurück. Der Client von IBM Spectrum Protect Version 6.2.2 oder höher kann VMware-Gesamtsicherungen zurückschreiben, die mit Versionen des Clients vor Version 6.2.2 erstellt wurden. Weitere Informationen finden Sie im folgenden Abschnitt:

Vollständige VM-Sicherungen zurückschreiben

 Zurückschreibung auf Dateiebene

 Mit dem Befehl restore können Sie einzelne Dateien aus einer VM-Sicherung auf Dateiebene zurückschreiben. Verwenden Sie diese Methode, wenn es nicht möglich ist, ein vollständiges VMware-Image zurückzuschreiben. Sicherungen auf Dateiebene wurden mit Clients für Sichern/Archivieren der Version 7.1 oder früher erstellt.
Für Zurückschreibungen auf Dateiebene gelten die folgenden Einschränkungen:

- Sie können die Zurückschreibung auf Dateiebene nur ausführen, wenn eine Sicherung auf Dateiebene der virtuellen Maschine vorhanden ist.
- Sie können keine vollständige virtuelle Maschine aus Sicherungen auf Dateiebene zurückschreiben, weil der Befehl restore den Windows-Systemstatus nicht erneut erstellt.
- Das Zurückschreiben einzelner Dateien aus einer vollständigen VM-Sicherung einer virtuellen Maschine ist mit dieser Methode nicht möglich.

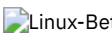
 Verwenden Sie für die Zurückschreibung von Dateien aus einer Sicherung auf Dateiebene die von der Konfiguration der virtuellen Maschine, auf der Sie die Dateien zurückschreiben, abhängige Methode:

Der Client für Sichern/Archivieren ist nicht auf der virtuellen Maschine installiert:
Schreiben Sie die Dateien von dem vStorage-Sicherungsserver zurück, der die virtuelle Maschine gesichert hat.
Der Client für Sichern/Archivieren ist auf der virtuellen Maschine installiert:
Schreiben Sie die Dateien von dem Client für Sichern/Archivieren zurück, der auf der virtuellen Maschine installiert ist.

Weitere Informationen finden Sie im folgenden Abschnitt:

Szenario: VM-Sicherungen auf Dateiebene zurückschreiben

-  Vollständige VM-Sicherungen zurückschreiben
Sie können eine vollständige VMware-Sicherung direkt auf den VMware-Server zurückschreiben, um alle Dateien einer virtuellen VMware-Maschine erneut zu erstellen. Diese Methode ersetzt die veraltete Zurückschreibungsmethode für Sicherungen, die mithilfe der VMware Consolidated Backup-Tools (VCB-Tools) erstellt wurden. Bei dieser Zurückschreibungsmethode müssen Sie nicht das Tool 'VMware Converter' verwenden, bevor Sie die Sicherung auf den VMware-Server zurückschreiben. Das Zurückschreiben einzelner Dateien aus einer vollständigen VM-Sicherung ist mit dieser Zurückschreibungsmethode nicht möglich.
-  Szenarios für die Ausführung des vollständigen VM-Sofortzugriffs (Instant Access) und der vollständigen VM-Sofortzurückschreibung (Instant Restore) über die Befehlszeile des Clients für Sichern/Archivieren
Für Operationen des vollständigen VM-Sofortzugriffs (Instant Access) und der vollständigen VM-Sofortzurückschreibung (Instant Restore) ist eine Lizenz für IBM Spectrum Protect for Virtual Environments erforderlich. Sie können beide Operationen über die Befehlszeile des Clients für Sichern/Archivieren ausführen. Operationen und Optionen für Sofortzugriffs- und Sofortzurückschreibungsoperationen werden nur für virtuelle VMware-Maschinen unterstützt, die auf Servern mit VMware ESXi 5.1 oder höher gehostet werden.
-  Szenario: VM-Sicherungen auf Dateiebene zurückschreiben
Auf Microsoft Windows-Systemen können Sie bestimmte Dateien aus einer Sicherung auf Dateiebene einer virtuellen VMware-Maschine zurückschreiben. Eine Zurückschreibung auf Dateiebene ist nützlich, wenn einzelne Dateien zurückgeschrieben werden sollen, die möglicherweise nicht mehr vorhanden oder beschädigt sind. Sie können diese Methode nicht verwenden, um Dateien zurückzuschreiben, die Teil einer vollständigen VM-Sicherung waren. Bevor Sie Dateien vom Off-Host-Sicherungsserver auf die virtuelle VMware-Maschine zurückschreiben können, muss der Off-Host-Sicherungsserver als Proxy-Server konfiguriert werden.
-  Mit VMware Consolidated Backup erstellte vollständige VM-Sicherungen zurückschreiben
Sie können eine vollständige VMware-Sicherung zurückschreiben, um alle Dateien einer virtuellen VMware-Maschine erneut zu erstellen. Führen Sie folgende Schritte aus, um vollständige VM-Sicherungen zurückzuschreiben, die in IBM Spectrum Protect Version 6.2.0 oder früher mithilfe von VMware Consolidated Backup (VCB) erstellt wurden.

Vollständige VM-Sicherungen zurückschreiben

Sie können eine vollständige VMware-Sicherung direkt auf den VMware-Server zurückschreiben, um alle Dateien einer virtuellen VMware-Maschine erneut zu erstellen. Diese Methode ersetzt die veraltete Zurückschreibungsmethode für Sicherungen, die mithilfe der VMware Consolidated Backup-Tools (VCB-Tools) erstellt wurden. Bei dieser Zurückschreibungsmethode müssen Sie nicht das Tool 'VMware Converter' verwenden, bevor Sie die Sicherung auf den VMware-Server zurückschreiben. Das Zurückschreiben einzelner Dateien aus einer vollständigen VM-Sicherung ist mit dieser Zurückschreibungsmethode nicht möglich.

Vorbereitende Schritte

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Informationen zum Zurückschreiben einer vollständigen VMware-Sicherung, die mithilfe von VCB-Tools in IBM Spectrum Protect Version 6.2.0 oder früher erstellt wurde, finden Sie im Abschnitt "Mit VMware Consolidated Backup erstellte vollständige VM-Sicherungen zurückschreiben".

Vorgehensweise

1. Führen Sie den von der Zielposition der Zurückschreibung abhängigen Schritt aus:
   - Wenn die Zurückschreibung der vollständigen VM-Sicherung die vorhandene virtuelle VMware-Maschine überschreiben wird, löschen Sie die vorhandene virtuelle Maschine.
   - Wenn Sie die vollständige VM-Sicherung auf eine neue virtuelle Maschine zurückschreiben, muss die vorhandene virtuelle Maschine nicht gelöscht werden. Wenn Sie möchten, können Sie die vorhandene virtuelle Maschine löschen. Wenn nicht, fahren Sie mit dem nächsten Schritt fort.
2. Gehen Sie wie folgt vor, um die virtuelle Maschine nach VMware-Sicherungen abzufragen:
   a. Führen Sie auf dem Off-Host-Sicherungsserver den folgenden Befehl aus:

      ```
      dsmc q vm *
      ```

      Mit dem Befehl werden die verfügbaren Sicherungen aufgelistet. Zum Beispiel:

      ```
      Nr.   Sicherungsdatum       Verw.-Klasse   Typ        A/I  Virtuelle Maschine
      ---     -----------        ----------          ----   --- ---------------
        1   12/03/2009 03:05:03   DEFAULT        VSTORFULL  A    vm_guest1
        2   09/02/2010 10:45:09   DEFAULT        VSTORFULL  A    vm_guest11
        3   09/02/2010 09:34:40   DEFAULT        VSTORFULL  A    vm_guest12
        4   09/02/2010 10:10:10   DEFAULT        VSTORFULL  A    vm_guest13
        5   12/04/2009 20:39:35   DEFAULT        VSTORFULL  A    vm_guest14
        6   09/02/2010 11:15:18   DEFAULT        VSTORFULL  A    vm_guest15
        7   09/02/2010 02:52:44   DEFAULT        VSTORFULL  A    vm_guest16
        8   08/05/2010 04:28:03   DEFAULT        VSTORFULL  A    vm_guest17
        9   08/05/2010 05:20:27   DEFAULT        VSTORFULL  A    vm_guest18
       10   08/12/2010 04:06:13   DEFAULT        VSTORFULL  A    vm_guest19
       11   09/02/2010 00:47:01   DEFAULT        VSTORFULL  A    vm_guest7
       12   09/02/2010 01:59:02   DEFAULT        VSTORFULL  A    vm_guest8
       13   09/02/2010 05:20:42   DEFAULT        VSTORFULL  A    vm_guest9
      ANS1900I Rückkehrcode ist 0.
      ANS1901I Höchster Rückkehrcode war 0.
      ```

   b. Ermitteln Sie anhand der vom Abfragebefehl zurückgegebenen Ergebnisse die zurückzuschreibende virtuelle Maschine.
3. Schreiben Sie die vollständige VMware-Sicherung mit dem Befehl restore vm zurück. Soll die Sicherung auf eine virtuelle Maschine mit einem neuen Namen zurückgeschrieben werden, verwenden Sie die Option -vmname. Beispielsweise wird mit dem folgenden Befehl die virtuelle Maschine zurückgeschrieben und ein neuer Name für die zurückgeschriebene virtuelle Maschine angegeben:

   ```
   dsmc restore vm Alter_VM-Name -vmname=Neuer_VM-Name -datastore=Pfad
   ```

4. Nach Beendigung der Zurückschreibung wird die virtuelle Maschine ausgeschaltet. Starten Sie die virtuelle Maschine im VMware vCenter.

Windows-Betriebssysteme

Nächste Schritte

Informationen zur Zurückschreibung von Sicherungen mit Anwendungsschutz finden Sie in Hinweise zu Schattenkopien für das Zurückschreiben einer Sicherung mit Anwendungsschutz von der Einheit zum Versetzen von Daten.

- Windows-BetriebssystemeHinweise zu Schattenkopien für das Zurückschreiben einer Sicherung mit Anwendungsschutz von der Einheit zum Versetzen von Daten
  Wenn Sie bei virtuellen VMware-Maschinen unter Windows versuchen, eine Sicherung mit Anwendungsschutz von der Einheit zum Versetzen von Daten zurückzuschreiben, müssen Sie dabei die Einschränkungen bezüglich Schattenkopien beachten.

Zugehörige Tasks:
Mit VMware Consolidated Backup erstellte vollständige VM-Sicherungen zurückschreiben
Zugehörige Verweise:
Linux-BetriebssystemeWindows-BetriebssystemeQuery VM
Linux-BetriebssystemeWindows-BetriebssystemeRestore VM
INCLUDE.VMSNAPSHOTATTEMPTS
Windows-Betriebssysteme

Szenarios für die Ausführung des vollständigen VM-Sofortzugriffs (Instant Access) und der vollständigen VM-Sofortzurückschreibung (Instant Restore) über die Befehlszeile des Clients für Sichern/Archivieren

Für Operationen des vollständigen VM-Sofortzugriffs (Instant Access) und der vollständigen VM-Sofortzurückschreibung (Instant Restore) ist eine Lizenz für IBM Spectrum Protect for Virtual Environments erforderlich. Sie können beide Operationen über die Befehlszeile des Clients für Sichern/Archivieren ausführen. Operationen und Optionen für Sofortzugriffs- und Sofortzurückschreibungsoperationen werden nur für virtuelle VMware-Maschinen unterstützt, die auf Servern mit VMware ESXi 5.1 oder höher gehostet werden.

Die folgenden Szenarios veranschaulichen die Operationen des vollständigen VM-Sofortzugriffs (Instant Access) und der vollständigen VM-Sofortzurückschreibung (Instant Restore), die Sie ausführen können. Bevor Sie die in den folgenden Abschnitten beschriebenen Operationen ausführen können, müssen Sie mindestens einen Knoten der Einheit zum Versetzen von Daten auf dem vStorage-Sicherungsserver konfigurieren, so dass er die virtuellen Maschinen durch Starten von Hostsicherungs- und -zurückschreibungsoperationen schützen kann. Die Konfigurationsschritte für die Knoten der Einheit zum Versetzen von Daten werden in Knoten der Einheit zum Versetzen von Daten in einer vSphere-Umgebung definieren beschrieben.

Szenario: Sie möchten einen vollständigen VM-Sofortzugriff (Instant Access) ausführen, um die Integrität eines gesicherten Image einer virtuellen VMware-Maschine zu prüfen, ohne die virtuelle Maschine oder die virtuellen Platten tatsächlich auf den ESXi-Host zurückzuschreiben

Zweck dieses Szenarios ist die Bestätigung, dass ein gesichertes Image der virtuellen Maschine für eine erfolgreiche Zurückschreibung eines Systems verwendet werden kann, falls die virtuelle Maschine gelöscht wird oder ihre Platten und Daten beschädigt oder anderweitig unbrauchbar werden.

In diesem Szenario hat ein ESX-Server eine virtuelle Maschine mit dem Namen Orion, die auf ihm ausgeführt wird. Sie wollen überprüfen, ob das vom IBM Spectrum Protect-Server gesicherte Image für die Zurückschreibung dieser virtuellen Maschine verwendet werden kann, wenn die aktuelle virtuelle Maschine ausfällt.

Um eine Sofortzugriffsoperation (Instant Access) für die virtuelle Maschine auszuführen, verwenden Sie den Befehl restore vm mit Optionen für die Bestandsposition, um die Position für die zurückgeschriebene virtuelle Maschine anzugeben. Alle Optionen für die Bestandsposition (z. B. vmname, datacenter, host und datastore) können mit der Sofortzugriffsoption (`-VMRESToretype=INSTANTAccess`) kombiniert werden, um die Position für die zurückgeschriebene virtuelle (Instant Access-)Maschine anzugeben.

Da die virtuelle Maschine 'Orion' im Bestand vorhanden und aktiv ist, müssen Sie einen neuen Namen für eine temporäre virtuelle Maschine angeben. Hierfür fügen Sie den neuen Namen in die Option vmname ein. Außerdem müssen Sie die Option `-VMRESToretype=INSTANTAccess` in die Befehlszeile einfügen, um anzuzeigen, dass dies eine Zurückschreibungsoperation mit Sofortzugriff (Instant Access) ist.

Mit dem folgenden Befehl wird eine virtuelle Maschine mit dem Namen "Orion_verify" vorbereitet, so dass sie für eine Sofortzugriffsoperation verfügbar ist. Sie können diese virtuelle Maschine verwenden, um zu überprüfen, ob ein gesichertes Image zurückgeschrieben werden kann.

```
dsmc restore vm Orion -vmname=Orion_verify  -Host=esxi.example.com
  -datacenter=mydataCenter -VMRESToretype=INSTANTAccess -VMAUTOSTARTvm=YES
```

Die Option `-VMAUTOSTARTvm=YES` zeigt an, dass die virtuelle Maschine gestartet wird, wenn sie zurückgeschrieben worden ist. Die neue virtuelle Maschine wird standardmäßig nicht automatisch gestartet. Mit dieser Standardeinstellung können Sie die virtuelle Maschine neu konfigurieren, bevor Sie sie starten.

Außerdem können Sie die gesicherten Versionen einer virtuellen Maschine mit der Option inactive oder pick auflisten oder mit den Optionen pittime und pitdate eine inaktive oder aktive Sicherung mit einem bestimmten Datum oder einer bestimmten Uhrzeit auswählen. Verwenden Sie beispielsweise den folgenden Befehl, um eine Liste der gesicherten Versionen der virtuellen Maschine Orion anzuzeigen:

```
dsmc restore vm Orion -pick
```

Wenn eine virtuelle Maschine mit der Option `-VMRESToretype=INSTANTAccess` zurückgeschrieben wird, werden die von dieser virtuellen Maschine erstellten temporären Daten in einer VMware-Momentaufnahme gespeichert.

Nach dem Zurückschreiben der temporären virtuellen Maschine (Orion_verify) prüfen Sie die Integrität ihrer Platten und Daten mithilfe von Verifizierungstools. Verwenden Sie ein Dienstprogramm wie chkdsk oder eine andere Anwendung Ihrer Wahl, um die virtuellen Platten und Daten zu überprüfen. Wenn die temporäre virtuelle Maschine die Integritätsprüfungen besteht, können Sie die temporären Ressourcen, die für die Unterstützung der Zurückschreibungsoperation mit Sofortzugriff (Instant Access) erstellt wurden, entfernen.

Szenario: Sie möchten feststellen, ob temporäre virtuelle (Instant Access-) Maschinen vorhanden sind, damit Sie eine Bereinigungsoperation ausführen können, um die zugehörigen Ressourcen freizugeben

Verwenden Sie den Befehl query vm mit einer der folgenden Optionen, die Sie in der Befehlszeile angeben:

```
-VMRESToretype=INSTANTAccess
-VMRESToretype=ALLtype
```

Dabei gilt:

`-VMRESToretype=INSTANTAccess`
: Zeigt alle temporären virtuellen Maschinen an, die im Sofortzugriffsmodus (Instant Access) ausgeführt werden und durch eine `restore vm -VMRESToretype=INSTANTAccess`-Operation erstellt wurden.

`-VMRESToretype=ALLtype`
: Zeigt alle virtuellen Maschinen mit aktiven Sofortzugriffs- (Instant Access) oder Sofortzurückschreibungssitzungen (Instant Restore) an, die mit einem Befehl restore vm gestartet wurden, in dem die Option `-VMRESToretype=INSTANTAccess` oder `VMRESToretype=-INSTANTRestore` verwendet wurde.

Die folgenden Beispiele zeigen die Syntax der verschiedenen Optionen:

```
query vm * -VMREST=INSTANTA
query vm * -VMREST=ALL
```

Sie können in jedem der gezeigten query vm-Befehle eine Option –Detail hinzufügen, um weitere Informationen zu jeder der temporären virtuellen Maschinen anzuzeigen.

```
query vm vmname -VMREST=INSTANTA -Detail
```

Führen Sie den folgenden Befehl aus, um die Ressourcen zu entfernen, die für eine temporäre virtuelle Maschine mit dem Namen "Orion_verify" erstellt wurden:

```
dsmc restore vm Orion –vmname=Orion_verify –VMRESToretype=VMCLeanup
```

Die Option –VMRESToretype=VMCLeanup löscht die temporäre virtuelle Maschine auf dem ESXi-Host, hängt alle angehängten iSCSI-Mounts ab und löscht die iSCSI-Einheitenliste vom ESX-Host. Alle temporären Daten für die temporäre virtuelle Maschine werden aus der VMware-Momentaufnahme gelöscht.

Szenario: Sie möchten eine Sofortzurückschreibungsoperation starten, um eine fehlgeschlagene virtuelle Maschine aus einem von IBM Spectrum Protect erstellten Sicherungsimage auf einen ESX-Host zurückzuschreiben

Der Vorteil einer vollständigen VM-Sofortzurückschreibung (Instant Restore) gegenüber einer klassischen vollständigen VM-Zurückschreibung besteht darin, dass die virtuelle Maschine bei einer Sofortzurückschreibungsoperation für die sofortige Verwendung bereit ist, sobald sie gestartet wurde. Sie müssen nicht warten, bis alle Daten zurückgeschrieben sind, bevor Sie die virtuelle Maschine verwenden können. Während einer Sofortzurückschreibungsoperation (Instant Restore) verwendet die virtuelle Maschine iSCSI-Platten, bis ihre lokalen Platten vollständig zurückgeschrieben sind. Wenn die lokalen Platten zurückgeschrieben sind, wechselt die virtuelle Maschine die Ein-/Ausgabe von den iSCSI-Platten zu den lokalen Platten ohne erkennbare Unterbrechung des Service.

Schreiben Sie eine virtuelle Maschine mit dem Namen Orion mit dem folgenden Befehl zurück:

```
dsmc restore vm Orion –Host=esxi.example.com –datacenter=mydatacenter
  –VMTEMPDAtastore=temp_datastore –VMRESToretype=INSTANTRestore
  –datastore=mydatastore
```

In diesem Befehl sind der Name der virtuellen Maschine, die zurückgeschrieben werden soll, der Host und das Datencenter, die das Ziel der Zurückschreibung sind, sowie der Zurückschreibungstyp (`-VMRESToretype=INSTANTRestore`) angegeben. Die Option VMTEMPDAtastore ist bei Sofortzurückschreibungsoperationen ein obligatorischer Parameter.

Den temporären Datenspeicher verwendet vMotion für die Speicherung der Konfiguration der zurückgeschriebenen virtuellen Maschine während des Sofortzurückschreibungsprozesses. Der Name, den Sie angeben, muss eindeutig sein. Er darf nicht mit dem Namen eines der ursprünglichen Datenspeicher übereinstimmen, die die virtuelle Maschine bei ihrer Sicherung verwendet hat, und er darf nicht mit dem in der optionalen Option –datastore angegebenen Namen übereinstimmen. Wird die Option –datastore nicht verwendet, werden die Dateien der virtuellen Maschine in die Datenspeicher zurückgeschrieben, die bei der Sicherung der virtuellen Maschine verwendet wurden.

Virtuelle Maschinen, die mit Instant Restore (Sofortzurückschreibung) zurückgeschrieben werden, verfügen standardmäßig über Thick Disks. Sie können dieses Verhalten ändern und Thin Disks bereitstellen, indem Sie die Option `-VMDISKProvision=THIN` in die Befehlszeile oder in die Clientoptionsdatei einfügen.

Wichtig: Stellen Sie bei Sofortzurückschreibungsoperationen (Instant Restore) sicher, dass sowohl der temporäre Datenspeicher, den Sie mit der Option vmtempdatastore angeben, als auch der VMware-Datenspeicher (Datastore), der mit der Option datastore im Befehl restore VM angegeben wird, über ausreichenden freien Speicherplatz zum Speichern der zurückzuschreibenden virtuellen Maschine und der Momentaufnahmedatei, die die an den Daten vorgenommenen Änderungen enthält, verfügen. Wenn Sie eine virtuelle Maschine zurückschreiben und Thin oder Thick Provisioning angeben (-vmdiskprovision=thin oder -vmdiskprovision=thick), muss der freie Speicherplatz des Datenspeichers, in den Sie die virtuelle Maschine zurückschreiben, für die Gesamtkapazität der VM-Platte ausreichen und nicht nur für die verwendete Plattenkapazität. Beispiel: Wenn die gesamte Plattenkapazität einer virtuellen Maschine 300 GB beträgt, können Sie diese virtuelle Maschine nicht in einen Datenspeicher mit einer Kapazität kleiner als 300 GB zurückschreiben, selbst wenn nur ein Teil der Gesamtkapazität verwendet wird.

- Windows-BetriebssystemeBereinigungs- und Reparaturszenarios für vollständige VM-Sofortzurückschreibungen
  Wenn eine Sofortzurückschreibungsoperation (Instant Restore) nach dem Einschalten der virtuellen Maschine fehlschlägt, sind manuelle Bereinigungs- und Reparaturschritte erforderlich.

- Windows-BetriebssystemeVom Standard abweichende Fehlerbedingungen beheben
  Probleme mit iSCSI-Einheiten können die Ausführung einer Sofortzugriffs- (Instant Access) oder Sofortzurückschreibungsoperation (Instant Restore) verhindern.

Windows-Betriebssysteme

Bereinigungs- und Reparaturszenarios für vollständige VM-Sofortzurückschreibungen

Wenn eine Sofortzurückschreibungsoperation (Instant Restore) nach dem Einschalten der virtuellen Maschine fehlschlägt, sind manuelle Bereinigungs- und Reparaturschritte erforderlich.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Wenn eine Sofortzurückschreibungsoperation (Instant Restore) fehlschlägt, während Storage vMotion aktiv ist, tritt eine der folgenden Situationen ein:

- Die Sofortzurückschreibungsoperation generiert eine Fehlernachricht.
- Die Sofortzurückschreibungsoperation setzt unendlich aus und die virtuelle Maschine reagiert nicht.

Um die Fehlerursache zu bestimmen, führen Sie eine Detailabfrage der virtuellen Maschine mit dem folgenden Befehl aus:

```
dsmc q vm * -vmrestoretype=instantrestore -detail
```

Suchen Sie in der von diesem Befehl generierten Ausgabe für jede virtuelle Maschine nach der Zeile, die die Worte `Aktion erforderlich` enthält. Führen Sie die Wiederherstellung nach einer fehlgeschlagenen Sofortzurückschreibungsoperation (Instant Restore) mithilfe der folgenden *Aktion erforderlich*-Abschnitte durch (je nach Status von `Aktion erforderlich`).

Aktion erforderlich: Bereinigung

Überprüfen Sie in der Ausgabe des Befehls `query vm * -vmrestoretype=instantrestore -detail`, ob der Status von Storage vMotion 'Erfolgreich' ist (`vMotion-Status: Erfolgreich`) und ob alle Platten der virtuellen Maschine physische Platten sind (`Plattentyp: Physisch`). Dieser Status bestätigt, dass die virtuelle Maschine zurückgeschrieben wurde und dass eine Bereinigung verwaister Komponenten (z. B. iSCSI-Mounts) erforderlich ist.

Dieser Fehler tritt aufgrund einer der folgenden Situationen auf:

- Die Sofortzurückschreibung (Instant Restore) ist fehlgeschlagen und Storage vMotion ist aktiv. VMware vSphere setzt den vMotion-Prozess fort.
- Storage vMotion wurde erfolgreich beendet, aber die automatische Bereinigung der iSCSI-Mounts schlägt fehl.

Für die Bereinigung verwaister Komponenten führen Sie den Befehl restore vm mit dem Parameter -VMRESToretype=VMCLeanup aus. Zum Beispiel:

```
dsmc restore vm ursprünglicher_VM-Name -vmname=neuer_VM-Name -VMRESToretype=VMCLeanup
```

Aktion erforderlich: Reparatur

Überprüfen Sie in der Ausgabe des Befehls `query vm * -vmrestoretype=instantrestore -detail`, ob die iSCSI-Einheit, die an die virtuelle Maschine angeschlossen ist, inaktiv ist (Status ist `Plattenpfad: Inaktiv`).

Dieser Fehler tritt aufgrund einer der drei folgenden Situationen auf:

- Die als Einheit zum Versetzen von Daten verwendete virtuelle Maschine oder die physische Maschine der Einheit zum Versetzen von Daten ist fehlgeschlagen.
- Zwischen der Einheit zum Versetzen von Daten und dem ESX-Host oder zwischen der Einheit zum Versetzen von Daten und dem IBM Spectrum Protect-Server ist ein Netzfehler aufgetreten.
- Der Service 'Data Protection for VMware Recovery Agent' ist fehlgeschlagen.

Die iSCSI-Einheit muss in einen aktiven Zustand versetzt werden, bevor eine andere Operation ausgeführt wird.
Gehen Sie wie folgt vor, um den Versuch einer Wiederherstellung nach einem Fehler der Einheit zum Versetzen von Daten zu unternehmen:

1. Untersuchen Sie die Fehlerursache und starten Sie die Maschine der Einheit zum Versetzen von Daten erneut, wenn sie nicht automatisch startet. Dieser Schritt startet eine automatische Wiederherstellung der angehängten iSCSI-Platten.
2. Überprüfen Sie in der Ausgabe des Befehls `query vm * -vmrestoretype=instantrestore -detail`, ob die Platten der virtuellen Maschine aktiv sind (`Plattenpfad: Aktiv`). Dieser Status bedeutet, dass die virtuelle Maschine zurückgeschrieben wurde und einsatzbereit ist.
3. Starten Sie Storage vMotion in dem vSphere-Client neu und überwachen Sie dessen Fortschritt in der Statusleiste des vSphere-Clients.
4. Wurde die Verarbeitung von Storage vMotion erfolgreich beendet, führen Sie den Befehl restore vm mit dem Parameter -vmrestoretype=VMCLeanup aus, um die iSCSI-Platten zu bereinigen. Beispiel:

```
dsmc restore vm ursprünglicher_VM-Name -vmname=neuer_VM-Name -VMRESToretype=VMCLeanup
```

Gehen Sie wie folgt vor, um den Versuch einer Wiederherstellung nach einem Netzfehler zu unternehmen:

1. Beheben Sie den Netzfehler, so dass die Kommunikation zwischen der Einheit zum Versetzen von Daten und dem ESX-Host sowie zwischen der Einheit zum Versetzen von Daten und dem IBM Spectrum Protect-Server wieder aufgenommen wird.
2. Überprüfen Sie in der Ausgabe des Befehls `query vm * -vmrestoretype=instantrestore -detail`, ob die Platten der virtuellen Maschine aktiv sind (`Plattenpfad: Aktiv`). Dieser Status bedeutet, dass die virtuelle Maschine zurückgeschrieben wurde und einsatzbereit ist.
3. Wenn der Netzfehler keine Zeitlimitüberschreitung in Storage vMotion verursacht hat, ist keine Maßnahme erforderlich.
4. Wenn der Netzfehler eine Zeitlimitüberschreitung in Storage vMotion verursacht hat und die Fehlernachricht anzeigt, dass die Quellenplatte nicht reagiert, starten Sie Storage vMotion im vSphere-Client neu. Wenn die Verarbeitung von Storage vMotion beendet ist, führen Sie den Befehl restore vm mit dem Parameter -vmrestoretype=VMCLeanup aus, um die iSCSI-Platten zu bereinigen. Zum Beispiel:

   ```
   dsmc restore vm ursprünglicher_VM-Name -vmname=neuer_VM-Name -VMRESToretype=VMCLeanup
   ```

Gehen Sie wie folgt vor, um den Versuch einer Wiederherstellung nach einem Fehler des Service 'Data Protection for VMware Recovery Agent' zu unternehmen:

1. Untersuchen Sie die Fehlerursache und starten Sie den Service 'Data Protection for VMware Recovery Agent' erneut, wenn er nicht automatisch startet. Dieser Schritt startet eine automatische Wiederherstellung der angehängten iSCSI-Platten.
2. Überprüfen Sie in der Ausgabe des Befehls `query vm * -vmrestoretype=instantrestore -detail`, ob die Platten der virtuellen Maschine aktiv sind (`Plattenpfad: Aktiv`). Dieser Status bedeutet, dass die virtuelle Maschine zurückgeschrieben wurde und einsatzbereit ist.
3. Wenn der Fehler des Service 'Data Protection for VMware Recovery Agent' keine Zeitlimitüberschreitung in Storage vMotion verursacht hat, ist keine Maßnahme erforderlich.
4. Wenn der Fehler des Service 'Data Protection for VMware Recovery Agent' eine Zeitlimitüberschreitung in Storage vMotion verursacht hat und die Fehlernachricht anzeigt, dass die Quellenplatte nicht reagiert, starten Sie Storage vMotion im vSphere-Client neu. Wenn die Verarbeitung von Storage vMotion beendet ist, führen Sie den Befehl restore vm mit dem Parameter -vmrestoretype=VMCLeanup aus, um die iSCSI-Platten zu bereinigen. Beispiel:

   ```
   dsmc restore vm ursprünglicher_VM-Name -vmname=neuer_VM-Name -VMRESToretype=VMCLeanup
   ```

Vollständige Bereinigung

Wenn Sie einen Fehler nicht beheben können und die virtuelle Maschine und ihre Komponenten entfernen wollen, führen den Befehl restore vm mit dem Parameter -vmrestoretype=VMFULLCLeanup aus. Beispiel:

```
dsmc restore vm ursprünglicher_VM-Name -vmname=neuer_VM-Name -VMRESToretype=VMFULLCLeanup
```

Eine VMFULLCLeanup-Operation erzwingt das Entfernen der virtuellen Maschine und aller ihrer Komponenten ohne Rücksicht auf den Status der virtuellen Maschine. Wenn vMotion eine virtuelle Maschine noch migriert, dürfen Sie keine vollständige Bereinigungsoperation starten.
 Windows-Betriebssysteme

Vom Standard abweichende Fehlerbedingungen beheben

Probleme mit iSCSI-Einheiten können die Ausführung einer Sofortzugriffs- (Instant Access) oder Sofortzurückschreibungsoperation (Instant Restore) verhindern.

Informationen zu diesem Vorgang

Wenn ein ESX-Server nicht auf einen Datenspeicher auf einer iSCSI-Platte zugreifen kann, wird in einer VMware-Nachricht angezeigt, dass ein permanenter Einheitenverlust ("permanent device loss") aufgetreten ist. Sie sollten die Möglichkeit erhalten, den iSCSI-Verbindungsversuch entweder abzubrechen oder zu wiederholen. Wählen Sie die Option zur Wiederholung der Operation aus, um festzustellen, ob der Fehler temporär und eine Fehlerbehebung möglich ist. Schlägt die Wiederholung fehl, führen Sie die folgenden Fehlerbehebungsschritte aus. Wenn diese Fehlerbehebung erfolgreich ist, wiederholen Sie die Sofortzurückschreibungs- (Instant Restore) oder Sofortzugriffsoperation (Instant Access).

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Vorgehensweise

1. Suchen Sie im Task- und Ereignisprotokoll des ESX-Servers nach einem Fehler 'All Paths Down (APD)'. Es kann eine Weile dauern, bis dieser Fehler in den Protokollen erscheint, er muss aber vorhanden sein, damit Sie mit den nächsten Schritten fortfahren können. Wenn Sie nicht warten, bis dieser Fehler angezeigt wird, bevor Sie weitere Fehlerbehebungsschritte ausführen, kann es zu einem Ausfall des ESX-Servers kommen.
2. Schalten Sie die virtuelle Maschine aus.
3. Überprüfen (rescan) Sie den Hostbusadapter (HBA) erneut. Durch eine erneute Überprüfung des Hostbusadapters auf dem ESX-Server wird die ausgefallene Einheit möglicherweise reaktiviert. Wird die erneute Überprüfung des Hostbusadapters durch VMware-

Kernelsperren verhindert, gehen Sie wie folgt vor:

a. Wählen Sie in der vCenter-Schnittstelle den ESX-Host aus.
b. Klicken Sie auf Configuration.
c. Klicken Sie mit der rechten Maustaste auf iSCSI Software Adapter und wählen Sie Properties aus.
d. Klicken Sie auf Static Discovery.
e. Löschen Sie alle statischen Adressen und klicken Sie auf Close.
f. Überprüfen (rescan) Sie den Hostbusadapter (HBA) erneut.

 Windows-Betriebssysteme

Szenario: VM-Sicherungen auf Dateiebene zurückschreiben

Auf Microsoft Windows-Systemen können Sie bestimmte Dateien aus einer Sicherung auf Dateiebene einer virtuellen VMware-Maschine zurückschreiben. Eine Zurückschreibung auf Dateiebene ist nützlich, wenn einzelne Dateien zurückgeschrieben werden sollen, die möglicherweise nicht mehr vorhanden oder beschädigt sind. Sie können diese Methode nicht verwenden, um Dateien zurückzuschreiben, die Teil einer vollständigen VM-Sicherung waren. Bevor Sie Dateien vom Off-Host-Sicherungsserver auf die virtuelle VMware-Maschine zurückschreiben können, muss der Off-Host-Sicherungsserver als Proxy-Server konfiguriert werden.

Vorbereitende Schritte

Sicherungen auf Dateiebene wurden mit Clients für Sichern/Archivieren der Version 7.1 oder früher erstellt.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Wichtig: Führen Sie eine Zurückschreibung auf Dateiebene mit dem Befehl restore aus. Verwenden Sie nicht den Befehl restore vm.
Für dieses Szenario einer Zurückschreibung auf Dateiebene gelten folgende Voraussetzungen:

- Ziel ist das Zurückschreiben von Dateien, die zuvor auf dem IBM Spectrum Protect-Server gesichert wurden.
- Die Dateien wurden auf einer virtuellen VMware-Maschine mit dem Namen Orion und dem Hostnamen orion gesichert. In diesem Szenario tritt ein Fehler in der virtuellen Maschine Orion auf und einige der Dateien müssen zurückgeschrieben werden.
- Die Dateien auf Orion wurden in Dateibereichen gesichert, deren Namen dem Hostnamen des Computers in Kleinbuchstaben entsprechen. Die Dateibereichsnamen entsprechen dem UNC-Format (UNC = Universal Naming Convention, allgemeine Namenskonvention). Zum Beispiel:
  - Dateien, die von Laufwerk C: auf Orion gesichert werden, werden im Dateibereich \\orion\c$ gespeichert.
  - Wenn Orion über ein Laufwerk D: verfügt, werden Dateien, die von diesem Laufwerk gesichert werden, im Dateibereich \\orion\d$ gespeichert.
- In diesem Szenario werden die Dateien aus dem Verzeichnis C:\mydocs, das sich auf Orion befand, in das Verzeichnis C:\restore_temp auf einem anderen Computer zurückgeschrieben. Der Computer, auf den die Dateien zurückgeschrieben werden, kann eine andere virtuelle VMware-Maschine oder ein physischer Computer sein.
- Der Computer, der die Zurückschreibung ausführt, hat einen anderen Hostnamen und einen anderen Knotennamen als die virtuelle Maschine Orion. Während der Zurückschreibung müssen Sie die Quellendateispezifikation im vollständigen UNC-Format angeben und einen der folgenden Parameter verwenden, um auf Orion zuzugreifen:

  -virtualnodename
  Gibt den Clientknoten an, für den eine Sicherung zurückgeschrieben wird. Verwenden Sie diesen Parameter, wenn Sie Dateien auf den Computer zurückschreiben, an dem Sie gerade angemeldet sind.

  -asnodename
  Gibt den Clientknoten an, für den eine Sicherung zurückgeschrieben wird. Verwenden Sie diesen Parameter, wenn Sie Dateien auf einen Computer zurückschreiben, für den Sie über Proxy-Berechtigung verfügen.

Gehen Sie wie folgt vor, um eine Zurückschreibung auf Dateiebene für den Computer Orion auszuführen:

Vorgehensweise

1. Fragen Sie auf dem IBM Spectrum Protect-Server die Dateibereiche ab, die für Orion registriert sind:

   ```
   dsmc query filespace -virtualnode=orion
   ```

2. Führen Sie einen der folgenden Befehle aus, um Dateien für den Dateibereich von Orion zurückzuschreiben:

   Dateien auf den Computer zurückschreiben, an dem Sie gerade angemeldet sind:
   Sie sind momentan an dem Computer mit dem Namen Orion angemeldet. Führen Sie einen der folgenden Befehle aus:
   a. Wenn Ihnen das Kennwort für den Knoten, den Sie zurückschreiben wollen, bekannt ist, verwenden Sie die Option -virtualnodename im Befehl 'restore'. Führen Sie beispielsweise den folgenden Befehl aus, um die Dateien nach Orion zurückzuschreiben:

      ```
      dsmc restore \\orion\c$\mydocs\ c:\restore_temp\ -sub=yes
      -virtualnodename=orion
      ```

b. Wenn Sie über Proxy-Berechtigung verfügen, können Sie Dateien im Namen des Zielknotens zurückschreiben. Proxy-Berechtigung muss vom Agentenknoten aus erteilt werden, das heißt vom Knoten des Computers, von dem die Zurückschreibung ausgeführt wird. Sie müssen das Kennwort des Agentenknotens kennen, so dass Sie auf den Zielknoten zugreifen können. Führen Sie beispielsweise den folgenden Befehl aus, um die Dateien nach Orion zurückzuschreiben:

```
dsmc restore \\orion\c$\mydocs\ c:\restore_temp\ -sub=yes
-asnodename=orion
```

Tabelle 1. Komponenten des Befehls 'restore', wenn Dateien auf denselben Computer zurückgeschrieben werden

Befehlskomponente	Beschreibung
`\\orion\c$\mydocs\`	Quellendateispezifikation auf dem IBM Spectrum Protect-Server. An dieser Position befinden sich die gesicherten Dateien, die Sie zurückschreiben wollen. Die Dateien wurden von der virtuellen Maschine `orion` gesichert, daher muss die Dateispezifikation das UNC-Format aufweisen.
`c:\restore_temp\`	Zieldateispezifikation auf dem Computer, an dem Sie gerade angemeldet sind. Die Dateien werden an diese Position zurückgeschrieben.
`-sub=yes`	Gibt an, dass bei der Zurückschreibungsoperation alle Unterverzeichnisse in der Quellendateispezifikation berücksichtigt werden.
`-virtualnodename=orion`	Informiert den IBM Spectrum Protect-Server darüber, dass die Sicherung auf dem Knoten `orion` ausgeführt wird.
`-asnodename=orion`	Informiert den IBM Spectrum Protect-Server darüber, dass die Sicherung auf dem Knoten `orion` ausgeführt wird.

Dateien auf einen anderen Computer zurückschreiben:

Führen Sie den folgenden Befehl aus, um die Dateien vom IBM Spectrum Protect-Server nicht auf den Computer, an dem Sie gerade angemeldet sind, sondern auf einen anderen Computer zurückzuschreiben. Sie können diesen Befehl nur verwenden, wenn Sie mit Schreibberechtigung für den fernen Computer gemäß Betriebssystemrichtlinien angemeldet sind.

```
dsmc restore \\orion\c$\mydocs\ \\orion\c$\restore_temp\ -sub=yes
-virtualnode=orion
```

Tabelle 2. Komponenten des Befehls 'restore', wenn Dateien auf einen anderen Computer zurückgeschrieben werden

Befehlskomponente	Beschreibung
`\\orion\c$mydocs\`	Gibt die Quellendateispezifikation auf dem IBM Spectrum Protect-Server an. An dieser Position befinden sich die gesicherten Dateien, die Sie zurückschreiben wollen. Die Dateien wurden von der virtuellen Maschine `orion` gesichert, daher muss die Dateispezifikation das UNC-Format aufweisen.
`\\orion\c$\restore_temp\`	Gibt die Zieldateispezifikation auf einem Computer an, an dem Sie nicht gerade angemeldet sind. Sie schreiben die Dateien über das Netz auf die virtuelle Maschine `orion` zurück. Dabei verwenden Sie eine Microsoft-Funktion, die Netzadressen in UNC-Notation identifiziert.
`-sub=yes`	Gibt an, dass bei der Zurückschreibungsoperation alle Unterverzeichnisse in der Quellendateispezifikation berücksichtigt werden.
`-virtualnodename=orion`	Informiert den IBM Spectrum Protect-Server darüber, dass die Sicherung auf dem Knoten `orion` ausgeführt wird.

Zugehörige Konzepte:
Daten aus einer VMware-Sicherung zurückschreiben
Zugehörige Tasks:
Mit VMware Consolidated Backup erstellte vollständige VM-Sicherungen zurückschreiben
Vollständige VM-Sicherungen zurückschreiben
Zugehörige Verweise:
Linux-BetriebssysemeWindows-BetriebssystemeQuery Filespace
Linux-BetriebssysemeWindows-BetriebssystemeRestore
Windows-Betriebssysteme

Mit VMware Consolidated Backup erstellte vollständige VM-Sicherungen zurückschreiben

Sie können eine vollständige VMware-Sicherung zurückschreiben, um alle Dateien einer virtuellen VMware-Maschine erneut zu erstellen. Führen Sie folgende Schritte aus, um vollständige VM-Sicherungen zurückzuschreiben, die in IBM Spectrum Protect Version 6.2.0 oder früher mithilfe von VMware Consolidated Backup (VCB) erstellt wurden.

Vorbereitende Schritte

Informationen zum Zurückschreiben einer vollständigen VMware-Sicherung, die mit IBM Spectrum Protect Version 6.2.2 oder höher erstellt wurde, finden Sie im Abschnitt "Vollständige VM-Sicherungen zurückschreiben".

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Vorgehensweise

1. Führen Sie den von der Zielposition der Zurückschreibung abhängigen Schritt aus:
   - Wenn die Zurückschreibung der vollständigen VM-Sicherung die vorhandene virtuelle VMware-Maschine überschreiben wird, löschen Sie die vorhandene virtuelle Maschine.
   - Wenn Sie die vollständige VM-Sicherung auf eine neue virtuelle Maschine zurückschreiben, muss die vorhandene virtuelle Maschine nicht gelöscht werden. Sie können die vorhandene virtuelle Maschine löschen. Wenn nicht, fahren Sie mit dem nächsten Schritt fort.
2. Gehen Sie wie folgt vor, um die virtuelle Maschine nach vollständigen VMware-Sicherungen abzufragen:
   a. Führen Sie auf dem Off-Host-Sicherungsserver den folgenden Befehl aus:

      ```
      dsmc q vm *
      ```

      Mit dem Befehl werden die verfügbaren Sicherungen aufgelistet. Zum Beispiel:

      ```
      Nr.   Sicherungsdatum       Verw.-Klasse   Typ        A/I  Virtuelle Maschine
      ---     -----------       ----------          ----   --- ---------------
        1   12/03/2009 03:05:03   DEFAULT        VMFULL  A    vm_guest1
        2   09/02/2010 10:45:09   DEFAULT        VMFULL  A    vm_guest11
        3   09/02/2010 09:34:40   DEFAULT        VMFULL  A    vm_guest12
        4   09/02/2010 10:10:10   DEFAULT        VMFULL  A    vm_guest13
        5   12/04/2009 20:39:35   DEFAULT        VMFULL  A    vm_guest14
        6   09/02/2010 11:15:18   DEFAULT        VMFULL  A    vm_guest15
        7   09/02/2010 02:52:44   DEFAULT        VMFULL  A    vm_guest16
        8   08/05/2010 04:28:03   DEFAULT        VMFULL  A    vm_guest17
        9   08/05/2010 05:20:27   DEFAULT        VMFULL  A    vm_guest18
       10   08/12/2010 04:06:13   DEFAULT        VMFULL  A    vm_guest19
       11   09/02/2010 00:47:01   DEFAULT        VMFULL  A    vm_guest7
       12   09/02/2010 01:59:02   DEFAULT        VMFULL  A    vm_guest8
       13   09/02/2010 05:20:42   DEFAULT        VMFULL  A    vm_guest9
      ANS1900I Rückkehrcode ist 0.
      ANS1901I Höchster Rückkehrcode war 0.
      ```

   b. Ermitteln Sie anhand der vom Abfragebefehl zurückgegebenen Ergebnisse die zurückzuschreibende virtuelle Maschine.
3. Schreiben Sie die vollständige VMware-Sicherung mit dem Befehl restore vm zurück. Soll eine virtuelle Maschine nach Zeitpunkt zurückgeschrieben werden, geben Sie die Optionen -pitdate und -pittime an. Zum Beispiel:

   ```
   dsmc restore vm VM-Name Ziel -pitdate=Datum -pittime=hh:mm:ss
   ```

   Hierbei gilt Folgendes:

   VM-Name
   Der Name der virtuellen Maschine, die Sie zurückschreiben wollen.
   Ziel
   Die Verzeichnisposition für die zurückgeschriebene vmdk-Datei.
   -pitdate
   Das Datum, an dem die Sicherung erstellt wurde.
   -pittime
   Die Uhrzeit, zu der die Sicherung erstellt wurde.

4. Nach Beendigung der Zurückschreibung wird die folgende Nachricht zurückgegeben: Geben Sie `J` ein.

   ```
   Virtual Infrastructure Client oder VMware Converter-Tool
   kann verwendet werden, um die virtuelle Maschine für VMware Virtual Center
   Inventory erneut zu definieren.

   Soll der VMware Converter jetzt gestartet werden? (Ja (J)/Nein (N))
   ```

   Tipp: Wenn Sie `N` eingeben, wird zur Befehlszeile zurückgekehrt, ohne dass der VMware Converter geöffnet wird. Sie müssen jedoch das Image konvertieren, damit es zurückgeschrieben werden kann.
5. Gehen Sie wie folgt vor, um das zurückgeschriebene VCB-Image mithilfe des VMware vCenter Converter-Tools in eine virtuelle Maschine auf einem VMWare-Server zu konvertieren:
   a. Öffnen Sie das Converter-Tool über das Windows-Startmenü.

b. Klicken Sie im Converter-Tool auf Maschine konvertieren.
c. Geben Sie in das Feld VM-Datei die Position der zurückgeschriebenen .vmx-Datei ein.
Tipp: Die .vmx-Datei wird in das Verzeichnis zurückgeschrieben, das mit der Option vmbackdir des Befehls `restore vm` angegeben wurde.
d. Führen Sie die übrigen Schritte im Assistenten aus, um die vollständige VM-Sicherung zu konvertieren.
6. Nach Beendigung der Zurückschreibung wird die virtuelle Maschine ausgeschaltet. Starten Sie die virtuelle Maschine im VMware vCenter.

Zugehörige Tasks:
Vollständige VM-Sicherungen zurückschreiben
Zugehörige Verweise:
Linux-BetriebssysemeWindows-BetriebssystemeQuery VM
Linux-BetriebssysemeWindows-BetriebssystemeRestore VM
Windows-Betriebssysteme

Einzelne Active Directory-Objekte von Windows zurückschreiben

Sie können einzelne Active Directory-Objekte zurückschreiben, um die versehentliche Beschädigung oder Löschung von Active Directory-Objekten zu beheben, ohne dass der Active Directory-Server heruntergefahren und erneut gestartet werden muss.

Verwenden Sie auf dem Windows Server-Client den Befehl restore adobjects, um lokale, gelöschte Active Directory-Objekte (Tombstone-Objekte) zurückzuschreiben. Sie können auch einzelne Active Directory-Objekte aus Systemstatussicherungen auf dem IBM Spectrum Protect-Server zurückschreiben.

- Windows-BetriebssystemeTombstone-Objekte reanimieren oder aus einer Systemstatussicherung zurückschreiben
Die Tombstonereanimation ist ein Prozess zum Zurückschreiben eines Objekts, das in Active Directory gelöscht wurde. Wird ein Objekt in Active Directory gelöscht, wird es nicht physisch entfernt, sondern nur als gelöscht markiert. Daher ist es möglich, das Objekt zu reanimieren (zurückzuschreiben).
- Windows-BetriebssystemeActive Directory-Objekte über die GUI und die Befehlszeile zurückschreiben
Um einzelne Active Directory-Objekte zurückzuschreiben, müssen Sie den Client für Sichern/Archivieren auf einem Domänencontroller ausführen und Ihr Benutzerkonto muss ein Mitglied der Gruppe 'Administratoren' sein. Die Active Directory-Objekte werden nicht in der Verzeichnisstruktur angezeigt, wenn Ihr Benutzerkonto kein Mitglied der Gruppe 'Administratoren' ist.
- Windows-BetriebssystemeEinschränkungen und Begrenzungen beim Zurückschreiben von Active Directory-Objekten
Beim Zurückschreiben von Active Directory-Objekten sind einige Einschränkungen und Begrenzungen zu beachten.
- Windows-BetriebssystemeAttribute in Tombstone-Objekten aufbewahren
Um ein Attribut anzugeben, das in dem Tombstone-Objekt aufbewahrt werden soll, lokalisieren Sie zuerst dieses Attribut in dem Active Directory-Schema und aktualisieren Sie dann das Attribut *searchFlags* des Schemaobjekts.
- Windows-BetriebssystemeClientakzeptorservice und Agentenservice für die Verwendung des Web-Clients ändern
Standardmäßig können Sie einzelne Active Directory-Objekte nicht mit dem Web-Client zurückschreiben. Die Web-Client-Services (Clientakzeptor und Agent) werden standardmäßig unter dem lokalen Systemkonto ausgeführt. Das lokale Systemkonto verfügt nicht über die erforderlichen Berechtigungen, um Active Directory-Objekte zurückzuschreiben.

Zugehörige Tasks:
Windows-Systemstatus zurückschreiben
Zugehörige Verweise:
Restore Adobjects
Windows-Betriebssysteme

Tombstone-Objekte reanimieren oder aus einer Systemstatussicherung zurückschreiben

Die Tombstonereanimation ist ein Prozess zum Zurückschreiben eines Objekts, das in Active Directory gelöscht wurde. Wird ein Objekt in Active Directory gelöscht, wird es nicht physisch entfernt, sondern nur als gelöscht markiert. Daher ist es möglich, das Objekt zu reanimieren (zurückzuschreiben).

Beim Reanimieren eines Objekts bleiben nicht alle Objektattribute erhalten. Wenn ein Objekt zu einem Tombstone-Objekt wird, werden viele Attribute automatisch entfernt, und die entfernten Attribute gehen verloren. Es ist jedoch möglich, das Active Directory-Schema zu ändern, um mehr Attribute beim Löschen des Objekts aufzubewahren.

Benutzergruppenlinks werden in Tombstones nicht beibehalten. Beispielsweise gehört das Benutzerkonto keiner Gruppe an, wenn ein Benutzerobjekt reanimiert wird. Alle diese Informationen müssen manuell von dem Active Directory-Administrator erneut erstellt werden.

Wenn ein Active Directory-Objekt aus einer Systemstatussicherung auf dem IBM Spectrum Protect-Server zurückgeschrieben wird, werden praktisch alle seine Attribute und die Gruppenzugehörigkeit zurückgeschrieben. Dies ist die beste Zurückschreibungsoption auf einem Windows Server-Domänencontroller. Wenn ein Objekt vom Server zurückgeschrieben wird, geschieht Folgendes:

- Die Active Directory-Datenbank wird aus einer Systemstatussicherung extrahiert und in ein temporäres Verzeichnis zurückgeschrieben.
- Die zurückgeschriebene Datenbank wird geöffnet.
- Wählen Sie die Objekte aus, die zurückgeschrieben werden sollen. Für jedes Objekt:

    - Wird eine Suche nach dem übereinstimmenden Tombstone ausgeführt. Die GUID (Globally Unique Identifier) des zurückgeschriebenen Objekts wird für die Suche nach dem Tombstone verwendet.
    - Wird der übereinstimmende Tombstone gefunden, wird er reanimiert. In diesem Fall behält das zurückgeschriebene Objekt die ursprüngliche GUID (Globally Unique Identifier) und die SID (Security Identifier).
    - Wird der übereinstimmende Tombstone nicht gefunden, wird ein neues Objekt in der Datenbank erstellt. In diesem Fall hat das neue Objekt eine neue GUID und eine neue SID, die sich vom ursprünglichen Objekt unterscheiden.
- Fehlende Attribute werden aus der Sicherung in das reanimierte oder neu erstellte Objekt kopiert. Vorhandene Attribute, die sich seit der Sicherung geändert haben, werden aktualisiert, damit sie dem Wert in der Sicherung entsprechen. Neue Attribute, die seit der Sicherung hinzugefügt wurden, werden entfernt.
- Die Gruppenzugehörigkeit wird zurückgeschrieben.

Obwohl alle definierbaren Attribute und die Gruppenlinks erneut erstellt werden, sind die zurückgeschriebenen Objekte möglicherweise nicht sofort nach der Zurückschreibungsoperation verfügbar. Ein Active Directory-Administrator muss die zurückgeschriebenen Objekte möglicherweise manuell aktualisieren, um sie verfügbar zu machen. Lesen Sie unbedingt Einschränkungen und Begrenzungen beim Zurückschreiben von Active Directory-Objekten, bevor Sie die Zurückschreibung ausführen.

Zugehörige Konzepte:
Attribute in Tombstone-Objekten aufbewahren
Daten zurückschreiben
Einschränkungen und Begrenzungen beim Zurückschreiben von Active Directory-Objekten
Zugehörige Tasks:
Windows-Systemstatus zurückschreiben
Zugehörige Verweise:
Restore Adobjects
Windows-Betriebssysteme

Active Directory-Objekte über die GUI und die Befehlszeile zurückschreiben

Um einzelne Active Directory-Objekte zurückzuschreiben, müssen Sie den Client für Sichern/Archivieren auf einem Domänencontroller ausführen und Ihr Benutzerkonto muss ein Mitglied der Gruppe 'Administratoren' sein. Die Active Directory-Objekte werden nicht in der Verzeichnisstruktur angezeigt, wenn Ihr Benutzerkonto kein Mitglied der Gruppe 'Administratoren' ist.

Sie können Active Directory-Objekte oder Tombstone-Objekte entweder über die GUI oder über die Befehlszeile zurückschreiben.

Führen Sie folgende Schritte aus, um einzelne Objekte über die GUI zurückzuschreiben:

1. Klicken Sie im IBM Spectrum Protect-Fenster auf Zurückschreiben. Das Fenster 'Zurückschreiben' wird geöffnet.
2. Falls erforderlich, erweitern Sie die Verzeichnisbaumstruktur. Zum Erweitern eines Objekts in der Baumstruktur klicken Sie auf das Pluszeichen (+) neben dem Objekt.
3. Lokalisieren Sie den Active Directory-Knoten in der Verzeichnisbaumstruktur. Erweitern Sie ihn, um Lokale gelöschte Objekte anzuzeigen. Das Objekt 'Server' ist auch verfügbar.
    - Zum Zurückschreiben von Tombstone-Objekten erweitern Sie Lokale gelöschte Objekte, navigieren zu den Tombstone-Objekten, die zurückgeschrieben werden sollen, und wählen die Tombstone-Objekte aus.
    - Gehen Sie wie folgt vor, um Active Directory-Objekte zurückzuschreiben, die auf dem IBM Spectrum Protect-Server gesichert wurden:
        a. Erweitern Sie das Objekt Server. Ein Fenster mit einer Liste von Systemstatussicherungen (mit unterschiedlichen Zeitmarken) auf dem Server wird angezeigt.
        b. Wählen Sie eine Systemstatussicherung in der Liste aus. Die Active Directory-Datenbank dieses Systemstatus wird im Hintergrund zurückgeschrieben und in der Baumstruktur werden Active Directory-Objekte angezeigt.
        c. Navigieren Sie zu den Active Directory-Objekten, die zurückgeschrieben werden sollen, und wählen Sie die Active Directory-Objekte aus.

    Tipp: Zum Anzeigen der Attribute für ein Active Directory-Objekt erweitern Sie jedes Active Directory-Objekt in der Baumstruktur, bis Sie das gewünschte Objekt erreichen. Die Attribute für ein Objekt werden im Anzeigebereich neben der Baumstruktur angezeigt. Sie können ein Active Directory-Objekt auf der Basis seines Namens suchen oder die Baumstruktur filtern.
4. Klicken Sie auf Zurückschreiben, um die Zurückschreibungsoperation zu starten. Das Fenster 'Taskliste' erscheint, das den Fortschritt der Zurückschreibungsoperation anzeigt.

In der Befehlszeile verwenden Sie den Befehl query adobjects für die Abfrage und den Befehl restore adobjects für die Zurückschreibung einzelner Active Directory-Objekte.

Zugehörige Verweise:
Query Adobjects
Restore Adobjects
 Windows-Betriebssysteme

Einschränkungen und Begrenzungen beim Zurückschreiben von Active Directory-Objekten

Beim Zurückschreiben von Active Directory-Objekten sind einige Einschränkungen und Begrenzungen zu beachten.

Beachten Sie die folgenden Einschränkungen beim Zurückschreiben von Objekten:

- Schreiben Sie das Active Directory nur dann als Teil einer Zurückschreibungsoperation für den Systemstatus zurück, wenn es sich um eine vollständige Zurückschreibung des Active Directory bei der Wiederherstellung nach einem Katastrophenfall handelt. Bei diesem Typ der Zurückschreibungsoperation muss der Active Directory-Server gestoppt und erneut gestartet werden.
- Tombstone-Objekte können Sie nicht nach Zeitpunkt zurückschreiben. Eine Zurückschreibung nach Zeitpunkt können Sie für Active Directory-Objekte ausführen, die auf dem Server gesichert wurden.
- Sie können Active Directory-Objekte nicht aus Sicherungssätzen zurückschreiben.

Beachten Sie die folgenden Begrenzungen beim Zurückschreiben von Objekten:

- Für das Zurückschreiben von Active Directory-Objekten vom IBM Spectrum Protect-Server ist temporärer Speicherbereich auf Ihrem lokalen Festplattenlaufwerk erforderlich. Mithilfe der Option stagingdirectory können Sie ein Verzeichnis auf Ihrer lokalen Festplatte für das Speichern temporärer Daten vom Server angeben. Abhängig vom Umfang der temporären Daten, der Netzbandbreite und der Leistung des Clients sowie des Servers kann diese Operation zwischen 20 Sekunden und über eine Stunde in Anspruch nehmen. Möglicherweise tritt eine Verzögerung bei der Aktualisierung des Fensters 'Zurückschreiben' auf, wenn die Active Directory-Baumstruktur angezeigt wird.
- Benutzerkennwörter können nicht standardmäßig zurückgeschrieben werden. Ein zurückgeschriebenes Benutzerobjekt ist inaktiviert, bis der Administrator das Kennwort zurücksetzt und das Konto erneut aktiviert. Zudem muss ein Konto, das aus der Domäne gelöscht und anschließend vom Client für Sichern/Archivieren zurückgeschrieben wurde, nach der Zurückschreibungsoperation manuell mit der Domäne verknüpft werden. Andernfalls können sich die Benutzer auf dem Zielcomputer nicht bei der Domäne anmelden.

  Damit ein Benutzer- oder Computerobjekt nach der Zurückschreibung in vollem Umfang betriebsbereit ist, müssen Sie das Schemaattribut *Unicode-Pwd* wie unter **Attribute in Tombstone-Objekten aufbewahren** beschrieben ändern.

- Das Active Directory-Schema wird bei der Zurückschreibung des Active Directory-Objekts nicht erneut erstellt. Wenn das Schema nach der Sicherung geändert wurde, ist das zurückgeschriebene Objekt eventuell nicht mehr mit dem neuen Schema kompatibel und einige Active Directory-Objekte sind möglicherweise nicht mehr gültig. Der Client gibt eine Warnung aus, wenn einige Attribute nicht zurückgeschrieben werden können.
- Gruppenmaßnahmenobjekte und ihre Verbindungen zu Organisationseinheiten (OU) können nicht zurückgeschrieben werden.
- Lokale Maßnahmen für zurückgeschriebene Active Directory-Objekte werden nicht zurückgeschrieben.
- Schreiben Sie ein Objekt vom IBM Spectrum Protect-Server zurück und ist das Zielobjekt bereits im Active Directory vorhanden, wird das Objekt nicht gelöscht und erneut erstellt, wenn Sie es durch seine Sicherungsversion ersetzen. Das vorhandene Objekt wird als Basis verwendet und seine Attribute werden durch die Sicherungsversion überschrieben. Einige Attribute, beispielsweise die GUID und die SID, bleiben dem vorhandenen Objekt erhalten und werden nicht von der Sicherungsversion überschrieben.
- Wenn mehrere Tombstone-Objekte für denselben Container vorhanden sind, reanimieren Sie diese über die Befehlszeile des Clients für Sichern/Archivieren mithilfe der Objekt-GUID. In diesem Fall reanimiert der Befehlszeilenclient nur das Containerobjekt und nicht seine untergeordneten Objekte. In der GUI des Clients für Sichern/Archivieren kann der gesamte Container für die Reanimation ausgewählt werden.
- Wenn Sie ein Objekt vom IBM Spectrum Protect-Server zurückschreiben, wenn das Active Directory-Liveobjekt vorhanden ist und das Bit für *Löschen verhindern* für das Objekt aktiviert wurde, kann der Client die Attribute des Objekts ändern. Ist jedoch ein Tombstone-Objekt mit demselben Namen, aber einer anderen Objekt-GUID vorhanden, gibt Directory Services den Fehler *Zugriff verweigert* zurück.
- Wenn Sie ein Objekt vom IBM Spectrum Protect-Server zurückschreiben und der Container des Objekts umbenannt wurde, erstellt der Client den Container unter Verwendung des ursprünglichen Namens zum Zeitpunkt der Sicherung erneut. Beim Zurückschreiben eines Tombstone-Objekts schreibt der Client das Objekt in den umbenannten Container zurück, da das Attribut *lastKnownParent* des Tombstone-Objekts mit dem neuen Containernamen aktualisiert wurde.

Zugehörige Konzepte:
Attribute in Tombstone-Objekten aufbewahren
Daten zurückschreiben
Zugehörige Verweise:
Restore Adobjects
Stagingdirectory
Windows-Betriebssysteme

Attribute in Tombstone-Objekten aufbewahren

Um ein Attribut anzugeben, das in dem Tombstone-Objekt aufbewahrt werden soll, lokalisieren Sie zuerst dieses Attribut in dem Active Directory-Schema und aktualisieren Sie dann das Attribut *searchFlags* des Schemaobjekts.

Mit Software von anderen Anbietern (beispielsweise ADSI Edit) können Sie das Attribut *searchFlags* des Schemaobjekts aktualisieren.

Normalerweise sind keine der Bits in der Bitmaske *searchFlags* gesetzt (der Wert ist 0). Setzen Sie *searchFlags* auf 8 (0x00000008), wenn Active Directory das spezielle Attribut in dem Tombstone-Objekt speichern soll, wenn das ursprüngliche Objekt gelöscht wird.

Zugehörige Konzepte:
Daten zurückschreiben
Zugehörige Verweise:
Restore Adobjects

Windows-Betriebssysteme

Clientakzeptorservice und Agentenservice für die Verwendung des Web-Clients ändern

Standardmäßig können Sie einzelne Active Directory-Objekte nicht mit dem Web-Client zurückschreiben. Die Web-Client-Services (Clientakzeptor und Agent) werden standardmäßig unter dem lokalen Systemkonto ausgeführt. Das lokale Systemkonto verfügt nicht über die erforderlichen Berechtigungen, um Active Directory-Objekte zurückzuschreiben.

Führen Sie folgende Schritte aus, um diese Zurückschreibungsoperation im Web-Client zu aktivieren:

1. Ändern Sie den Clientakzeptor- und Agentenservice so, dass bei der Anmeldung bei Windows ein Verwaltungskonto wie *Administrator* verwendet wird.
2. Sie können die Eigenschaften für den Clientakzeptorservice und den Agentenservice (normalerweise als TSM-Clientakzeptor und ferner TSM-Clientagent bezeichnet) in der Systemsteuerung editieren.
3. Ändern Sie den Clientakzeptorservice und den Agentenservice auf der Seite Anmeldeoptionen im IBM Spectrum Protect-Konfigurationsassistenten, wenn Sie den Web-Client konfigurieren.

Wenn der Web-Client bereits konfiguriert ist, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf Start.
2. Klicken Sie auf Systemsteuerung → Verwaltung → Dienste.
3. Wählen Sie den Scheduler-Service aus der Liste der Windows-Dienste aus.
4. Klicken Sie auf die Registerkarte Anmelden.
5. Klicken Sie auf Dieses Konto im Bereich `Anmelden als`.
6. Geben Sie ein Verwaltungskonto ein oder klicken Sie auf Durchsuchen, um das Domänenkonto zu suchen.
7. Geben Sie das Kennwort für das Domänenkonto ein.
8. Klicken Sie auf OK und anschließend auf Starten.

Zugehörige Verweise:
Restore Adobjects

Daten während einer Übernahme zurückschreiben oder abrufen

Wenn eine Übernahme des Clients auf dem Sekundärserver stattfindet, können Sie replizierte Daten vom Sekundärserver zurückschreiben oder abrufen.

Vorbereitende Schritte

Bevor Sie mit dem Zurückschreiben bzw. Abrufen von Daten während einer Übernahme beginnen, müssen Sie Folgendes sicherstellen:

- Die automatisierte Clientübernahme ist auf dem Client konfiguriert.
- Es besteht eine Verbindung zu einem IBM Spectrum Protect-Server, der Clientknoten repliziert. Weitere Informationen zu Übernahmevoraussetzungen finden Sie in Voraussetzungen für die automatisierte Clientübernahme.

Einschränkung: Im Übernahmemodus können Sie keine Daten auf dem Sekundärserver sichern oder archivieren.

Vorgehensweise

Gehen Sie wie folgt vor, um Daten während einer Übernahme zurückzuschreiben oder abzurufen:

1. Überprüfen Sie den Replikationsstatus der Clientdaten auf dem Sekundärserver. Der Replikationsstatus zeigt an, ob die neueste Sicherung auf dem Sekundärserver repliziert wurde.
2. Führen Sie die Zurückschreibung bzw. den Abruf Ihrer Daten wie gewöhnlich mithilfe der Client-GUI oder der Befehlszeilenschnittstelle aus.
   Tipp: Wiederanlauffähige Zurückschreibungsoperationen funktionieren erwartungsgemäß, wenn eine Verbindung zum Sekundärserver besteht. Jedoch können Zurückschreibungsoperationen, die unterbrochen werden, wenn der Primärserver ausfällt, nach der Übernahme des Clients nicht erneut gestartet werden. Sie müssen nach der Übernahme des Clients auf dem Sekundärserver die gesamte Zurückschreibungsoperation erneut ausführen.

Ergebnisse

Wenn die replizierten Daten auf dem Sekundärserver nicht aktuell sind, werden Sie aufgefordert, die Zurückschreibungs- bzw. Abrufoperation fortzusetzen oder zu stoppen.

Geben Sie beispielsweise den folgenden Befehl aus, um das Verzeichnis build.sh über die Befehlszeilenschnittstelle zurückzuschreiben:
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
dsmc res /build.sh
```

Windows-Betriebssysteme

```
dsmc res C:\build.sh
```

Die folgende Ausgabe wird angezeigt:

```
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
  Clientversion 8, Release 1, Stufe 0.0
  Clientdatum/-zeit: 16.11.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016. Alle Rechte vorbehalten.

Knotenname: MY_NODE_NAME
ANS2106I Verbindung zum primären IBM Spectrum Protect-Server 192.0.2.1 ist
fehlgeschlagen.

ANS2107I Es wird versucht, eine Verbindung zum sekundären Server TARGET
unter 192.0.2.9 : 1501 herzustellen.

Knotenname: MY_NODE_NAME
Sitzung hergestellt mit Server TARGET: Windows
  Serverversion 8, Release 1, Stufe 0.0
  Serverdatum/-zeit: 16.11.2016 12:05:35  Letzter Zugriff: 15.11.2016 14:13:32

  Sitzung im Übernahmemodus auf dem sekundären Server aufgebaut
ANS2108I Verbindung zum sekundären Server TARGET hergestellt.
Zurückschreibungsfunktion aufgerufen.

ANS2120W Das vom Server TARGET aufgelistete Datum der letzten Speicheroperation
(16.05.2013 22:38:23) stimmt nicht mit dem vom Client gespeicherten Datum
der letzten Speicheroperation (21.05.2013 21:32:20) überein.
Fortfahren? (Ja (J)/Nein (N))
```

Wenn Sie `N` auswählen, wird die folgende Nachricht angezeigt:

```
ANS1074W  Die Operation wurde vom Benutzer gestoppt.
```

Wenn Sie `J` auswählen, wird die Zurückschreibungsverarbeitung normal fortgesetzt, aber die zurückgeschriebenen Daten sind möglicherweise nicht aktuell.

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Status replizierter Clientdaten bestimmen
Windows-Betriebssysteme

Anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen

Ein Benutzer kann einem Benutzer auf einem anderen Knoten die Berechtigung zum Zurückschreiben seiner Sicherungsversionen oder zum Abrufen seiner Archivierungskopien erteilen. Auf diese Weise können Sie Dateien mit anderen Benutzern oder anderen Workstations, die Sie mit einem anderen Knotennamen verwenden, gemeinsam nutzen.

Informationen zu diesem Vorgang

Sie können auch andere Knoten berechtigen, auf den ASR-Dateibereich (Dateibereich für automatische Systemwiederherstellung) zuzugreifen.

Ein anderer Knoten kann zum Erstellen der ASR-Diskette verwendet werden, sodass die Workstation mit ASR und dem Client für Sichern/Archivieren wiederhergestellt werden kann. Verwenden Sie den anderen Knoten, wenn ein Problem mit der Workstation auftritt und die ASR-Diskette der Workstation nicht verfügbar ist.

Die Berechtigung zum Zurückschreiben oder Abrufen von Dateien wird einem anderen Knoten wie folgt erteilt:

Vorgehensweise

1. Klicken Sie auf **Dienstprogramme** → **Knotenzugriffsliste** im Hauptfenster.
2. Im Fenster **Knotenzugriffsliste** klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Im Fenster **Zugriffsregel hinzufügen** wählen Sie ein Element im Feld **Zugriff erlauben für** aus, um den Typ der Daten anzugeben, auf die der andere Benutzer zugreifen kann. Sie können entweder **Gesicherte Objekte** oder **Archivierte Objekte** auswählen.
4. Geben Sie den Knotennamen des Benutzers im Feld **Zugriff erteilen für Knoten** ein. Geben Sie den Knotennamen der Host-Workstation des Benutzers in das Feld **Zugriff erteilen für Knoten** ein.
5. Geben Sie die Benutzer-ID auf der Host-Workstation in das Feld **Benutzer** ein.
6. Im Feld **Dateibereich und Verzeichnis** wählen Sie den Dateibereich und das Verzeichnis aus, auf den bzw. das der Benutzer zugreifen kann. Sie können jeweils einen Dateibereich und ein Verzeichnis auswählen. Wenn Sie dem Benutzer Zugriff auf einen anderen Dateibereich oder ein anderes Verzeichnis geben wollen, müssen Sie eine andere Zugriffsregel erstellen.

7. Soll der Zugriff des Benutzers auf bestimmte Dateien im Verzeichnis begrenzt werden, geben Sie den Namen oder das Muster für die Dateien auf dem Server, auf die der andere Benutzer zugreifen darf, im Feld **Dateiname** ein. Sie können nur einen Eintrag im Feld **Dateiname** eingeben. Dabei kann es sich um den Namen einer einzelnen Datei oder um ein Muster handeln, das mit einer oder mehreren Dateien übereinstimmt. Es kann ein Platzhalterzeichen als Teil des Musters verwendet werden. Ihr Eintrag muss mit Dateien übereinstimmen, die auf dem Server gespeichert wurden.
8. Wenn Sie Zugriff auf alle Dateien erteilen wollen, die mit der Dateinamenspezifikation innerhalb des ausgewählten Verzeichnisses, einschließlich der Unterverzeichnisse, übereinstimmen, klicken Sie auf **Unterverzeichnisse einschließen**.
9. Klicken Sie auf **OK**, um die Zugriffsregel zu speichern und das Fenster **Zugriffsregel hinzufügen** zu schließen.
10. Die von Ihnen erstellte Zugriffsregel wird im Listenfeld des Fensters **Knotenzugriffsliste** angezeigt. Wenn Sie Ihre Arbeit im Fenster **Knotenzugriffsliste** beendet haben, klicken Sie auf **OK**. Wenn Sie Ihre Änderungen nicht sichern möchten, klicken Sie auf **Abbrechen** oder schließen Sie das Fenster.

Ergebnisse

Beispiel: Um dem Knoten user2 Zugriff auf alle Sicherungsdateien und Unterverzeichnisse unter dem Verzeichnis `d:\user1` zu erteilen, erstellen Sie eine Regel mit den folgenden Werten:

```
Zugriff erlauben für: Gesicherte Objekte
Zugriff erteilen für Knoten: user2
Dateibereich und Verzeichnis: d:\user1
Dateiname: *
Unterverzeichnisse einschließen: Ausgewählt
```

Der Knoten, dem Sie eine Berechtigung erteilen, muss auf Ihrem IBM Spectrum Protect-Server registriert sein.

In der Befehlszeile des Clients verwenden Sie den Befehl set access, um einen anderen Knoten zum Zurückschreiben oder Abrufen Ihrer Dateien zu berechtigen. Sie können auch den Befehl query access verwenden, um Ihre aktuelle Liste einzusehen, und den Befehl delete access, um Knoten aus der Liste zu löschen.

Zugehörige Verweise:
Delete Access
Query Access
Set Access
Windows-Betriebssysteme

Dateien von einem anderen Clientknoten zurückschreiben oder abrufen

Nachdem andere Benutzer Ihnen den Zugriff auf ihre Dateien auf dem Server erteilt haben, können Sie diese Dateien in Ihr lokales System zurückschreiben oder abrufen.

Informationen zu diesem Vorgang

Anhand der folgenden Schritte können Sie Dateibereiche für einen anderen Benutzer auf dem Server anzeigen, die Sicherungsversionen der Dateien für einen anderen Benutzer zurückschreiben oder die Archivierungskopien für einen anderen Benutzer in Ihr lokales Dateisystem abrufen:

Vorgehensweise

1. Klicken Sie auf **Dienstprogramme** im Hauptfenster.
2. Klicken Sie auf **Zugriff auf anderen Knoten**.
3. Geben Sie den Knotennamen der Host-Workstation des Benutzers in das Feld **Knotenname** ein und klicken Sie auf **Definieren**.

Ergebnisse

Werden Befehle verwendet, kann der Knoten mit der Option fromnode angegeben werden. Außerdem müssen Sie den Dateibereichsnamen und nicht den Laufwerkbuchstaben verwenden, um das Laufwerk für Zurückschreiben/Abrufen auszuwählen, auf das zugegriffen werden soll. Schließen Sie den Dateibereichsnamen in geschweifte Klammern ein und geben Sie ihn ebenso wie einen Laufwerkbuchstaben an. Sollen beispielsweise die Dateien aus dem Verzeichnis `\projx` des Knotens cougar im Dateibereich für die D-Platte in Ihr eigenes Verzeichnis `\projx` zurückgeschrieben werden, geben Sie Folgendes ein:

```
dsmc restore -fromnode=cougar  \\cougar\d$\projx\* d:\projx\
```

Verwenden Sie den Befehl query filespace, um eine Liste der Dateibereiche anzuzeigen. Um beispielsweise eine Liste der Dateibereiche von cougar anzuzeigen, geben Sie Folgendes ein:

```
dsmc query filespace -fromnode=cougar
```

Wichtig: Der Client für Sichern/Archivieren kann beim Zurückschreiben von Dateien Dateibereichsinformationen verwenden. Die Dateibereichsinformationen können den Namen des Computers enthalten, von dem die Dateien gesichert wurden. Wenn Sie Dateien von einem anderen Clientknoten zurückschreiben und kein Ziel für die zurückgeschriebenen Dateien angeben, verwendet der Client die Dateibereichsinformationen zum Zurückschreiben der Dateien. In diesem Fall versucht der Client, die Dateien in das Laufwerk auf dem

ursprünglichen Computer zurückzuschreiben. Hat der zurückschreibende Computer Zugriff auf das Laufwerk des ursprünglichen Computers, können Dateien in das ursprüngliche Laufwerk zurückgeschrieben werden. Hat der zurückschreibende Computer keinen Zugriff auf das Laufwerk des ursprünglichen Computers, gibt der Client eine Netzfehlernachricht zurück. Wenn die ursprüngliche Verzeichnisstruktur zurückgeschrieben werden soll, dies jedoch auf einen anderen Computer erfolgen soll, geben Sie beim Zurückschreiben der Dateien nur das Ziellaufwerk an. Dies gilt sowohl für das Zurückschreiben von Dateien von einem anderen Knoten als auch für das Abrufen von Dateien von einem anderen Knoten.

Zugehörige Verweise:
Fromnode
Restore
Retrieve
 Windows-Betriebssysteme

Dateien auf eine andere Workstation zurückschreiben oder abrufen

Der Benutzer kann Dateien, die aus der eigenen Workstation gesichert oder archiviert wurden, zurückschreiben oder abrufen, wenn er eine andere Workstation verwendet.

Die Sicherungsversionen und Archivierungskopien werden nach dem Knoten und nicht nach der Workstation gespeichert. Die Daten werden durch das IBM Spectrum Protect-Kennwort geschützt.

Verwenden Sie zum Zurückschreiben oder Abrufen von Dateien auf eine andere Workstation die Option virtualnodename, um den Knotennamen der Workstation anzugeben, auf der die Dateien gesichert wurden. Sie können die Option virtualnodename verwenden, wenn Sie IBM Spectrum Protect starten, oder Sie können die Option in Ihre Clientoptionsdatei dsm.opt auf der Workstation einfügen. Verwenden Sie nicht Ihre eigene Workstation, geben Sie die Option virtualnodename im Befehl dsm an. Lautet der Knotenname beispielsweise cougar, Folgendes eingeben:

```
start dsm -virtualnodename=cougar
```

Anschließend können Sie Dateien wie an Ihrer ursprünglichen Workstation zurückschreiben oder abrufen.
Sie können die Option virtualnodename auch in Befehlen verwenden. Sollen beispielsweise die Dateien in \projx in Ihr lokales Verzeichnis c:\myfiles zurückgeschrieben werden, geben Sie Folgendes ein:

```
dsmc restore -virtualnodename=cougar \\cougar\d$\projx\*.* c:\myfiles\
```

Sollen die Dateien auf der anderen Workstation nicht in dasselbe Verzeichnis zurückgeschrieben oder abgerufen werden, geben Sie ein anderes Ziel ein.

Dateien auf einen anderen Workstationtyp zurückschreiben oder abrufen

Sie können Dateien von einem Systemtyp auf einen anderen zurückschreiben oder abrufen. Dies wird als *Clientübergreifendes Zurückschreiben* bezeichnet.

Einschränkung: Für den Zugriff auf den Dateibereich der anderen Workstation benötigen Sie die entsprechenden Berechtigungen.

Für NTFS- und ReFS-Laufwerke können längere Datei- und Verzeichnisnamen als für FAT-Laufwerke verwendet werden. Wenn Sie Dateien mit langen Dateinamen in ein FAT-Laufwerk zurückschreiben, geben Sie für jede Datei eine Zieldateispezifikation an.

Verwenden Sie den Windows-Client, um Dateien mit langen Namen in ein NTFS- oder ReFS-Dateisystem zurückzuschreiben, bleiben die langen Namen erhalten, auch wenn die Dateien in einen anderen Laufwerktyp als das Quellenlaufwerk zurückgeschrieben werden.

Zugehörige Tasks:
Anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen
Dateien von einem anderen Clientknoten zurückschreiben oder abrufen
 Windows-Betriebssysteme

Dateibereiche löschen

Erteilt Ihnen der IBM Spectrum Protect-Administrator die Berechtigung, können Sie vollständige Dateibereiche auf dem Server löschen.

Informationen zu diesem Vorgang

Sie können keine einzelnen Sicherungskopien löschen, die auf dem Server aufbewahrt werden. Wenn Sie einen Dateibereich löschen, löschen Sie alle Dateien, sowohl Sicherungskopien als auch Archivierungskopien, die in diesem Dateibereich enthalten sind. Wenn Sie beispielsweise den Dateibereich für Ihr Laufwerk `C` löschen, löschen Sie damit jede Sicherungskopie für jede Datei auf dieser Platte sowie jede Datei, die Sie von dieser Platte archiviert haben.

Achtung: Das Löschen eines Dateibereichs sollte daher nur nach sorgfältiger Überlegung durchgeführt werden.

Sie können Dateibereiche über den GUI-Client oder den Befehlszeilenclient löschen. Zum Löschen von NAS-Dateibereichen (NAS - Network-Attached Storage) verwenden Sie den Web-Client oder den Befehlszeilenclient.

Zum Löschen eines Dateibereichs mit dem GUI-Client führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Wählen Sie im Hauptfenster **Dienstprogramme** → **Dateibereiche löschen** aus.
2. Wählen Sie die Dateibereiche aus, die gelöscht werden sollen.
3. Klicken Sie auf **Löschen**. Der Client fordert Sie zur Bestätigung auf, bevor der Dateibereich gelöscht wird.

Ergebnisse

Sie können einen Dateibereich auch mit dem Befehl delete filespace löschen. Verwenden Sie die Option class im Befehl delete filespace, um NAS-Dateibereiche zu löschen.

Zugehörige Verweise:
Class
Delete Filespace
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Image in Datei zurückschreiben

Wenn Sie ein Image sichern, sichert der Client für Sichern/Archivieren den ersten Sektor des Datenträgers. Bei der Zurückschreibung der Daten wird der erste Sektor jedoch übersprungen, um den ursprünglichen Steuerblock des logischen Datenträgers des Zieldatenträgers beizubehalten.

Wenn Sie ein Image in eine Datei zurückschreiben, wird der vollständige Datenträgerinhalt einschließlich des ersten Sektors in die Datei zurückgeschrieben.

AIX LVM-Datenträger aus ursprünglichen Datenträgergruppen enthalten den Steuerblock des logischen Datenträgers (LVCB = Logical Volume Control Block) im ersten Sektor (512 Byte) des Datenträgers. Der LVCB enthält datenträgerspezifische Metadaten, die von den Anwendungen, die den Datenträger verwenden, beibehalten werden sollten.

Wenn Sie die Datei mit dem Image auf einen LVM-Datenträger aus der ursprünglichen Datenträgergruppe kopieren, müssen Sie den LVCB sowohl in der Datei als auch auf dem Zieldatenträger überspringen. Zu diesem Zweck können Sie den folgenden dd-Befehl verwenden.

```
dd if=<Dateiname> of=/dev/<Datenträger> bs=512 skip=1 seek=1
```

Der Befehl dd setzt die Blockgröße auf 512 Byte, wodurch das Kopieren sehr langsam wird. Es ist besser, einen Wert wie `bs=1m` oder Ähnliches zu verwenden. Alternativ können Imagedaten wie folgt kopiert werden:

1. Sichern Sie den ursprünglichen ersten Sektor in einer Datei:

   ```
   dd if=/dev/<Datenträger> of=firstblk.tmp bs=512 count=1
   ```

2. Kopieren Sie das zurückgeschriebene Image:

   ```
   dd if=<Dateiname> of=/dev/<Datenträger> bs=1m
   ```

3. Schreiben Sie den ursprünglichen ersten Sektor zurück:

   ```
   dd if=firstblk.tmp of=/dev/<Datenträger> bs=512 count=1
   ```

Seit der Einführung großer und skalierbarer Datenträgergruppenformate unter AIX ist es möglich, dass der erste Sektor des logischen Datenträgers keinen LVCB enthält und für die Daten verfügbar ist. Wenn Sie auf Ihrem System große und skalierbare Datenträgergruppen verwenden und den gesamte Datenträger einschließlich des ersten Sektors zurückschreiben müssen, schreiben Sie den Datenträger in eine Datei zurück und kopieren Sie die Datei anschließend auf einen Zieldatenträger. Zu diesem Zweck können Sie den folgenden **dd**-Befehl verwenden.

```
dd if=<Dateiname> of=/dev/<Datenträger> bs=1m
```

Zugehörige Konzepte:
Image über die Befehlszeile zurückschreiben
Zugehörige Tasks:
Image über die GUI zurückschreiben
 AIX-Betriebssysteme  Linux-Betriebssysteme

GPFS-Dateisystemdaten mit Speicherpools verwalten

Mithilfe der GPFS-Technologie (GPFS = Global Parallel File Systems) können Sie Ihre Daten mit Speicherpools verwalten. Ein Speicherpool ist eine Sammlung von Platten oder RAIDs mit ähnlichen Eigenschaften, die als eine Gruppe zusammen verwaltet werden.

Die Gruppe, unter der die Speicherpools zusammen verwaltet werden, ist das Dateisystem. Die automatische Platzierung und Verwaltung von Dateien auf Speicherpoolebene wird von Maßnahmen ausgeführt. Eine Maßnahme ist eine Gruppe von Regeln, die auf der Basis der Dateiattribute den Lebenszyklus von Benutzerdaten beschreibt.

Wenn eine Datei erstellt wird, bestimmt die Platzierungsmaßnahme die ursprüngliche Position der Dateidaten und ordnet die Datei einem Speicherpool zu. Alle Daten, die in diese Datei geschrieben werden, werden in den zugeordneten Speicherpool gestellt. Die

Verwaltungsmaßnahme bestimmt die Dateiverwaltungsoperation wie z. B. Migration und Löschung. Die Dateien innerhalb eines GPFS-Dateisystems werden in Abhängigkeit von den aktivierten Platzierungs- und Umlagerungsmaßnahmen über verschiedene Speicherpools verteilt.

Bei der Zurückschreibung werden die Dateien in den korrekten Speicherpool gestellt. Da der IBM Spectrum Protect-Server die Umlagerungen zwischen den Speicherpools nicht erkennt, werden die Dateien in den Speicherpool gestellt, in dem die Sicherung erfolgt ist. Die Maßnahmensteuerkomponente ersetzt die Dateien auf der Basis von Migrationsmaßnahmen.

Ist eine Speicherpool-ID in den erweiterten Attributen der Datei gespeichert und ist dieser Speicherpool verfügbar, wird die Datei immer in diesen Speicherpool gestellt. Ist der Speicherpool nicht verfügbar, wird die Datei anhand der Platzierungsmaßnahme platziert. Stimmt die Platzierungsmaßnahme nicht mit der Datei überein, wird die Datei in den Systempool gestellt.

GPFS handhabt die Platzierung von Dateien nach einer Zurückschreibung wie folgt:

- Die Datei wird in den Pool gestellt, der ausgewählt werden kann, indem die gesicherten Dateiattribute mit einer Regel RESTORE in Einklang gebracht wird
- Die Datei wird in den Pool gestellt, in der sie war, als sie gesichert wurde
- Die Datei wird auf der Basis der aktuellen Platzierungsmaßnahme platziert
- Die Datei wird in den Systemspeicherpool gestellt

Mit der GPFS-Regel RESTORE können Sie Dateien in Übereinstimmung mit ihren gespeicherten Attributen und nicht mit den aktuellen Dateiattributen bringen. Wenn die Dateiattribute nicht übereinstimmen, versucht GPFS, die Datei bei ihrer Zurückschreibung in der oben beschriebenen Reihenfolge zu platzieren.

Weitere Informationen über die GPFS-Regel RESTORE enthalten die Abschnitte zu Maßnahmen und Regeln in der GPFS-Dokumentation.

Es gelten die folgenden Einschränkungen:

- Das Zurückschreiben von Stubdateien funktioniert nicht mit mehreren Speicherpools bzw. mit Dateien, die über ACLs verfügen
- Das Aufheben von Dateigruppenverbindungen ist nicht zulässig
- Die GPFS-Option ctime sollte auf no (den Standardwert) gesetzt werden, um zu verhindern, dass Dateien nach der GPFS-Dateiumlagerung in einen anderen Speicherpool gesichert werden.

Informationen zur Verwendung von Speicherpools finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Zugehörige Konzepte:
Datenspeicherung in Speicherpools
Zugehörige Informationen:
AIX-BetriebssystemeLinux-BetriebssystemeProduktinformationen zu GPFS
AIX-BetriebssystemeLinux-BetriebssystemeBefehl 'mmbackup': IBM Spectrum Protect-Voraussetzungen
AIX-BetriebssystemeLinux-BetriebssystemeVerwendung der Einschluss- und Ausschlussoptionen von IBM Spectrum Protect in Verbindung mit dem IBM Spectrum Scale-Befehl 'mmbackup'

Daten nach Zeitpunkt zurückschreiben

Verwenden Sie eine Zurückschreibung *nach Zeitpunkt*, um Dateien mit dem Stand zurückzuschreiben, den sie an einem bestimmten Datum und zu einer bestimmten Uhrzeit hatten.

Informationen zu diesem Vorgang

Durch das Zurückschreiben nach Zeitpunkt können die Auswirkungen eines Datenverlusts beseitigt werden, indem die Daten von einem Zeitpunkt vor dem bekannten Datenverlust zurückgeschrieben werden, oder der frühere Status einer Basiskonfiguration kann wiederhergestellt werden.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSie können eine Zurückschreibung nach Zeitpunkt für einen Dateibereich, ein Verzeichnis oder eine Datei ausführen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSie können eine Zurückschreibung nach Zeitpunkt auch für Imagesicherungen ausführen.

Windows-BetriebssystemeSie können eine Zurückschreibung nach Zeitpunkt für Systemstatusdaten, für einen Dateibereich, für ein Verzeichnis oder für eine Datei ausführen. Sie können eine Zurückschreibung nach Zeitpunkt auch für Imagesicherungen ausführen.

Teilsicherungen sind durchzuführen, um eine Zurückschreibung nach Zeitpunkt zu unterstützen. Während einer Teilsicherung benachrichtigt der Client für Sichern/Archivieren den Server, wenn Dateien aus einem Clientdateibereich oder Verzeichnis gelöscht werden. Bei selektiven Sicherungen und Teilsicherungen nach Datum erhält der Server keine Informationen über gelöschte Dateien. Teilsicherungen sollten den möglichen Zurückschreibungsanforderungen entsprechend häufig durchgeführt werden.

Wird eine Zurückschreibung nach Zeitpunkt mit einem Datum und einer Uhrzeit angefordert, die vor der ältesten vom IBM Spectrum Protect-Server verwalteten Version liegen, wird das Objekt nicht in Ihr System zurückgeschrieben. Dateien, die vor dem angegebenen Zeitpunkt von Ihrer Workstation gelöscht wurden, werden nicht zurückgeschrieben.

Anmerkung:

1. Ihr Administrator muss Kopiengruppeneinstellungen definieren, mit denen genügend inaktive Versionen einer Datei aufbewahrt werden, um sicherzustellen, dass diese Datei mit dem Stand eines bestimmten Datums und einer bestimmten Uhrzeit zurückgeschrieben werden kann. Wenn nicht genügend Versionen aufbewahrt werden, kann der Client unter Umständen nicht alle Objekte mit dem Stand des angegebenen Zeitpunkts zurückschreiben.
2. Wird eine Datei oder ein Verzeichnis gelöscht, wird die aktive Sicherungsversion bei der nächsten Ausführung einer Teilsicherung zu einer inaktiven Version, und die ältesten Versionen, die die mit dem Verwaltungsklassenattribut *Versionen gelöschter Daten* angegebene Anzahl überschreiten, werden gelöscht.

Bei der Ausführung einer Zurückschreibung nach Zeitpunkt ist Folgendes zu beachten:

- Der Client schreibt Dateiversionen aus der neuesten Sicherung vor dem angegebenen Datum des Zeitpunkts zurück. Stellen Sie sicher, dass der angegebene Zeitpunkt nicht mit dem Datum und die Uhrzeit identisch ist, an dem bzw. zu der diese Sicherung ausgeführt wurde.
- Liegen das angegebene Datum und die angegebene Uhrzeit für das Objekt, das zurückgeschrieben werden soll, vor dem Datum und der Uhrzeit der ältesten Version, die auf dem Server vorhanden ist, kann der Client dieses Objekt nicht zurückschreiben.
- Bei einer Zurückschreibung nach Zeitpunkt werden Dateien zurückgeschrieben, die nach dem Datum des Zeitpunkts von der Client-Workstation gelöscht wurden, aber keine Dateien, die vor diesem Datum gelöscht wurden.
- Der Client kann keine Datei zurückschreiben, die nach dem Datum und der Uhrzeit des Zeitpunkts erstellt wurde. Wird ein Zurückschreiben nach Zeitpunkt durchgeführt, werden Dateien, die nach dem Datum für den Zeitpunkt auf dem Client erstellt wurden, nicht gelöscht.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Zurückschreibung nach Zeitpunkt über die Client-GUI auszuführen:

1. Klicken Sie auf die Schaltfläche Zurückschreiben im Hauptfenster. Das Fenster Zurückschreiben wird angezeigt.
2. Klicken Sie auf die Schaltfläche Zeitpunkt im Fenster Zurückschreiben. Das Fenster Zurückschreiben nach Zeitpunkt wird angezeigt.
3. Wählen Sie das Auswahlfeld Datum nach Zeitpunkt verwenden aus. Wählen Sie das Datum und die Uhrzeit aus und klicken Sie auf OK. Der angegebene Zeitpunkt wird im Anzeigefeld Zeitpunkt im Fenster Zurückschreiben angezeigt.
4. Zeigen Sie die Objekte an, die zurückgeschrieben werden sollen. Sie können nach einem Objekt anhand des Namens suchen, die Verzeichnisbaumstruktur filtern oder mit den Verzeichnissen in der Verzeichnisbaumstruktur arbeiten.
5. Klicken Sie auf die Auswahlfelder neben den Objekten, die zurückgeschrieben werden sollen.
6. Klicken Sie auf die Schaltfläche Zurückschreiben. Das Fenster Zurückschreibungsziel wird angezeigt. Geben Sie die entsprechenden Informationen ein.
7. Klicken Sie auf die Schaltfläche Zurückschreiben, um die Zurückschreibung zu starten. Im Fenster Task-Liste für die Zurückschreibung wird der Verarbeitungsstatus der Zurückschreibung angezeigt.

Ergebnisse

Anmerkung: Sind keine Sicherungsversionen eines Verzeichnisses für den angegebenen Zeitpunkt vorhanden, können Dateien in diesem Verzeichnis nicht mit der GUI zurückgeschrieben werden. Sie können diese Dateien jedoch mithilfe der Befehlszeile zurückschreiben.

Sie können eine Zurückschreibung nach Zeitpunkt mit dem Befehlszeilenclient starten, indem Sie die Optionen pitdate und pittime in den Befehlen query backup und restore verwenden. Wenn Sie beispielsweise die Optionen pitdate und pittime im Befehl query backup verwenden, legen Sie den Zeitpunkt fest, für den Dateiinformationen zurückgegeben werden. Wenn Sie pitdate und pittime im Befehl restore verwenden, legen die angegebenen Datums- und Zeitwerte den Zeitpunkt fest, für den Dateien zurückgegeben werden. Wird pitdate ohne einen Wert für pittime angegeben, nimmt pittime den Standardwert 23:59:59 an. Wird pittime ohne einen Wert für pitdate angegeben, wird die Option ignoriert.

Zugehörige Konzepte:
Speicherverwaltungsmaßnahmen
Zugehörige Verweise:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeBackup Image
AIX-Betriebssysteme

Verschlüsselte AIX-Dateien zurückschreiben

Wenn Dateien in unformatiertem Format von einem AIX JFS2 EFS (Verschlüsseltes AIX JFS2-Dateisystem) gesichert werden, können Sie sie nur in dasselbe oder in ein anderes JFS2 EFS zurückschreiben. Sie können nicht in ein anderes Dateisystem oder auf eine andere Plattform zurückgeschrieben werden.

Wenn EFS-Dateien im Klartext gesichert werden, können Sie sie standortunabhängig zurückschreiben. Wenn Sie sie in ein JFS2 EFS zurückschreiben, werden sie automatisch nur dann erneut verschlüsselt, wenn für das Verzeichnis, in das sie zurückgeschrieben werden, die AIX-Option "EFS-Vererbung" definiert ist.

Nach dem Zurückschreiben einer in unformatiertem Format gesicherten Datei stellen Sie unter Umständen fest, dass die Datei nicht entschlüsselt werden kann. Der ursprünglich für die Datei verwendete Verschlüsselungsschlüssel ist möglicherweise im Schlüsselspeicher des Benutzers nicht mehr verfügbar. In diesem Fall ist es erforderlich, den zum Zeitpunkt der Sicherung verwendeten Schlüsselspeicher zurückzuschreiben.

Informationen zum Sichern von EFS-Daten finden Sie in Verschlüsseltes AIX JFS2-Dateisystem sichern.

AIX-Workloadpartitionsdateisysteme zurückschreiben

Alle Dateien, die von der lokalen Workloadpartition (WPAR) erstellt und von dem in der globalen Workloadpartition installierten Client für Sichern/Archivieren gesichert wurden, können von dem in der globalen Workloadpartition installierten Client zurückgeschrieben werden.

Es folgen einige Konfigurationsbeispiele für die globale Partition und die Workloadpartition:

```
Globale Partition:

   Systemname: shimla

   Dateisystem: /home /opt

WPAR #1-Konfiguration:

   Name: wpar1

   Dateisystem: /home; Name in globaler WPAR: /wpars/wpar1/home

WPAR #2-Konfiguration:

   Name: wpar2

   Dateisystem: /data; Name in globaler WPAR: /wpars/wpar2/data
```

Es gibt zwei Möglichkeiten, die WPAR-Daten zurückzuschreiben, abhängig von der Methode, die zum Sichern der WPAR-Datendateien verwendet wurde:

- Alle WPAR-Dateisysteme als Dateibereiche innerhalb der globalen Partition zurückschreiben. Mit dem Namen des Dateibereichs muss die Workloadpartition identifiziert werden, zu der der Dateibereich gehört. Alle Daten werden mithilfe eines einzigen Zeitplans auf einem einzigen Knoten verwaltet. Unter Verwendung der zuvor erwähnten Beispielkonfiguration zeigt das folgende Beispiel eine Musterdatei `dsm.sys` mit einer Serverzeilengruppe für alle Systeme, sowohl global als auch lokal:

  ```
  SErvername  shimla

     TCPPort           1500

     TCPServeraddress  server.example.com

     nodename          shimla

     PasswordAccess    generate

     Domain            /wpars/wpar1/home /wpars/wpar2/data /home /opt
  ```

  Verwenden Sie den folgenden Befehl, um jeden einzelnen Dateibereich zurückzuschreiben:

  ```
  dsmc restore /wpars/wpar1/home/*
  dsmc restore /wpars/wpar2/data/*
  dsmc restore /home/*
  dsmc restore /opt/
  ```

- Jedes einzelne WPAR-Dateisystem von einem anderen Knotennamen zurückschreiben, wenn es unter einem anderen Knotennamen gesichert wurde. Jede Workloadpartition muss einen separaten Knotennamen und einen Scheduler haben, der innerhalb der globalen Partition ausgeführt wird. Außerdem müssen drei Scheduler-Services definiert werden, wobei jeder Service entsprechend dem Namen der Serverzeilengruppe eine andere Datei `dsm.opt` verwendet. Diese Methode ermöglicht, dass jede WPAR-Zurückschreibungsoperation unabhängig von den anderen verwaltet wird. Unter Verwendung der zuvor erwähnten Beispielkonfiguration zeigt das folgende Beispiel eine Musterdatei `dsm.sys` mit drei Serverzeilengruppen: eine für `wpar1`, eine für `wpar2` und eine für die globale Partition `shimla`:

  ```
  SErvername  shimla_wpar1
    TCPPort                          1500
    TCPServeraddress          server.example.com
    nodename                         wpar1
    PasswordAccess            generate
    Domain                           /wpars/wpar1/home

  SErvername  shimla_wpar2
    TCPPort                          1500
    TCPServeraddress          server.example.com
    nodename                         wpar2
    PasswordAccess            generate
    Domain                           /wpars/wpar2/data

  SErvername  shimla
    TCPPort                          1500
    TCPServeraddress          server.example.com
  ```

```
nodename                                shimla
PasswordAccess              generate
Domain                                  /home /opt
```

Tabelle 1. Beispielbefehle zum Zurückschreiben von Workloadpartitionen mit der Datei dsm.opt

In der Datei dsm.opt	Beispielbefehl zum Zurückschreiben
servername shimla_wpar1	dsmc restore /wpars/wpar1/home/*
servername shimla_wpar2	dsmc restore /wpars/wpar2/data/*
servername shimla	dsmc restore /home/* dsmc restore /opt/*

 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

NAS-Dateisysteme zurückschreiben

NAS-Dateisystemimages werden mithilfe des Web-Clients oder der Befehlszeilenschnittstelle zurückgeschrieben. Die Web-Client-Schnittstelle ist nur für Verbindungen zu einem Server mit IBM Spectrum Protect Version 8.1.1, 8.1.0, 7.1.7 oder einer früheren Version verfügbar.

Sie können vollständige NAS-Dateisystemimages oder Differenzdateisystemimages zurückschreiben, die zuvor gesichert wurden. Wird ein Differenzimage zurückgeschrieben, schreibt IBM Spectrum Protect automatisch zuerst das vollständige Sicherungsimage und dann das Differenzimage zurück. Es ist nicht erforderlich, dass ein Clientknoten ein NAS-Dateisystem anhängt, um Sicherungs- oder Zurückschreibungsoperationen für dieses Dateisystem auszuführen.

-  AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-BetriebssystemeNAS-Dateisysteme mit dem Web-Client zurückschreiben
  In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um NAS-Dateisysteme mit der Web-Client-GUI zurückzuschreiben.
-  Windows-BetriebssystemeNAS-Dateien und -Verzeichnisse mit dem Web-Client zurückschreiben
  Sie können die Option toc zusammen mit der Option include.fs.nas in Ihrer Clientoptionsdatei verwenden, um anzugeben, ob der Client für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) speichert.
-  AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-BetriebssystemeOptionen und Befehle für die Zurückschreibung von NAS-Dateisystemen über die Befehlszeile
  Dieser Abschnitt enthält einige Beispiele für Optionen und Befehle, die Sie zum Zurückschreiben von NAS-Dateisystemimages über die Befehlszeile verwenden können.

Zugehörige Konzepte:
Übersicht über die Konfiguration des Web-Clients
 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

NAS-Dateisysteme mit dem Web-Client zurückschreiben

In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um NAS-Dateisysteme mit der Web-Client-GUI zurückzuschreiben.

Vorbereitende Schritte

Die Web-Client-Schnittstelle ist nur für Verbindungen zu einem Server mit IBM Spectrum Protect Version 8.1.1, 8.1.0, 7.1.7 oder einer früheren Version verfügbar.

Vorgehensweise

1. Klicken Sie auf die Schaltfläche **Zurückschreiben** im Hauptfenster. Das Fenster 'Zurückschreiben' wird angezeigt.
2. Falls erforderlich, erweitern Sie die Verzeichnisbaumstruktur. Zum Erweitern eines Knotens in der Baumstruktur klicken Sie auf das Pluszeichen (+) neben einem Objekt in der Baumstruktur. Es werden die Knoten angezeigt, die gesichert wurden und für die Ihr Administrator berechtigt ist. Der Anfangsknoten mit dem Namen **Knoten** ist nicht auswählbar. Dieser Knoten wird nur angezeigt, wenn ein NAS-Plug-in auf der Client-Workstation vorhanden ist. NAS-Knoten werden auf derselben Stufe wie der Knoten der Client-Workstation angezeigt. Es werden nur Knoten angezeigt, für die der Administrator berechtigt ist.
3. Erweitern Sie den NAS-Knoten, um das Imageobjekt anzuzeigen.
4. Erweitern Sie das Imageobjekt, um Datenträger anzuzeigen, die Sie zurückschreiben können. Datenträgerobjekte können Sie nicht erweitern.
5. Wählen Sie die Auswahlfelder neben den Datenträgern unter dem Imageobjekt aus, die zurückgeschrieben werden sollen. Wenn Sie ein NAS-Image zurückschreiben wollen, das ein einem bestimmten Datum gesichert wurde, klicken Sie auf die Schaltfläche **Nach Zeitpunkt**. Nach Auswahl eines Datums wird das letzte Objekt angezeigt, das an oder vor diesem Datum gesichert wurde, einschließlich eventueller inaktiver Objekte. Sollen vor der Auswahl von Objekten alle Images (einschließlich aktiver und inaktiver Images) angezeigt werden, wählen Sie in der Menüleiste **Sicht → Aktive/inaktive Dateien anzeigen** aus.
6. Klicken Sie auf **Zurückschreiben**. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Geben Sie die Informationen in das Fenster 'Zurückschreibungsziel' ein. Wenn Sie ein anderes Ziel für die Zurückschreibung auswählen, können Sie jeweils nur einen Datenträger an

ein anderes Ziel zurückschreiben. Sie können NAS-Dateisystemimages auf alle Datenträger auf dem NAS-Dateiserver zurückschreiben, von dem sie gesichert wurden. Sie können Images nicht auf einen anderen NAS-Dateiserver zurückschreiben.

7. Klicken Sie auf **Zurückschreiben**. Im Fenster **Task-Liste** für die NAS-Zurückschreibung werden der Verarbeitungsstatus der Zurückschreibung und die Statusleiste angezeigt. Eine Zahl neben der Statusleiste gibt, falls bekannt, die Größe der Zurückschreibung an. Nach Beendigung der Zurückschreibung zeigt das Fenster 'NAS-Zurückschreibungsbericht' Verarbeitungsdetails an. Wenn Sie die Web-Browser-Sitzung schließen müssen, werden aktuelle NAS-Operationen nach der Trennung der Verbindung fortgesetzt. Sie können die Schaltfläche **Verlassen** im Fenster **Task-Liste** für die NAS-Zurückschreibung verwenden, um die Verarbeitungsüberwachung zu verlassen, ohne die aktuelle Operation zu beenden.
8. (Optional) Um die Verarbeitung einer Operation zu überwachen, wählen Sie Aktionen > IBM Spectrum Protect-Aktivitäten im Hauptfenster aus.

Ergebnisse

Hinweise:

- Workstationsicherungen und ferne Sicherungen (NAS-Sicherungen) schließen sich in einem Zurückschreibungsfenster gegenseitig aus. Wenn ein Element für die Zurückschreibung ausgewählt wurde, muss das nächste Element, das Sie auswählen, denselben Typ aufweisen (entweder NAS oder Nicht-NAS).
- Für NAS-Knoten oder -Images werden keine Details auf der rechten Seite des Zurückschreibungsfensters angezeigt. Um Informationen zu einem NAS-Image anzuzeigen, heben Sie das NAS-Image hervor und wählen Sie Anzeigen > Dateiinformationen im Menü aus.
- Um NAS-Dateibereiche zu löschen, wählen Sie Dienstprogramme > Dateibereiche löschen aus. Sie können sowohl Workstationobjekte als auch ferne Objekte löschen.

Windows-Betriebssysteme

NAS-Dateien und -Verzeichnisse mit dem Web-Client zurückschreiben

Sie können die Option toc zusammen mit der Option include.fs.nas in Ihrer Clientoptionsdatei verwenden, um anzugeben, ob der Client für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) speichert.

Informationen zu diesem Vorgang

Wenn Sie TOC-Informationen speichern, können Sie den Web-Client verwenden, um die gesamte Baumstruktur des Dateisystems zu überprüfen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen. Die Erstellung eines Inhaltsverzeichnisses erfordert, dass Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsimage gebunden wird. Beachten Sie, dass die TOC-Erstellung während der Sicherungsoperation eine zusätzliche Verarbeitung, zusätzliche Netzressourcen, zusätzlichen Speicherpoolspeicher und möglicherweise einen zusätzlichen Mountpunkt erfordert. Wenn Sie keine TOC-Informationen speichern, können Sie über den Serverbefehl RESTORE NODE dennoch einzelne Dateien und Verzeichnisstrukturen zurückschreiben, wenn Sie den vollständig qualifizierten Namen jeder Datei bzw. jedes Verzeichnisses und das Image kennen, in dem das Objekt gesichert wurde.

NAS-Dateien und -Verzeichnisse werden wie folgt zurückgeschrieben:

Vorgehensweise

1. Klicken Sie auf Zurückschreiben im Hauptfenster. Das Fenster 'Zurückschreiben' wird angezeigt.
2. Falls erforderlich, erweitern Sie die Verzeichnisbaumstruktur. Zum Erweitern eines Knotens in der Baumstruktur klicken Sie auf das Pluszeichen (+) neben einem Objekt in der Baumstruktur. Es werden die Knoten angezeigt, die gesichert wurden und für die Ihr Administrator berechtigt ist. Der Anfangsknoten mit dem Namen Knoten ist nicht auswählbar. Dieser Knoten wird nur angezeigt, wenn ein NAS-Plug-in auf der Client-Workstation vorhanden ist. NAS-Knoten werden auf derselben Stufe wie der Knoten der Client-Workstation angezeigt. Es werden nur Knoten angezeigt, für die der Administrator berechtigt ist.
3. Erweitern Sie den NAS-Knoten, um das Objekt Dateiebene anzuzeigen.
4. Erweitern Sie das Objekt Dateiebene, um die zuletzt gesicherten Datenträger, Verzeichnisse und Dateien anzuzeigen. Wenn Sie das Datenträgerobjekt erweitern und vollständige TOC-Informationen für die letzte Sicherung auf dem Server zur Verfügung stehen, wird der Dialog 'Inhaltsverzeichnis laden' angezeigt. Wenn keine vollständigen TOC-Informationen für die letzte Sicherung zur Verfügung stehen, werden unter dem Datenträgerobjekt keine Objekte angezeigt. Im nächsten Schritt wird erklärt, wie Objekte aus anderen Sicherungen als der letzten Sicherung angezeigt werden können. Vollständige TOC-Informationen werden bereitgestellt, wenn Sie eine der folgenden Operationen ausgeführt haben: (1) eine Imagedifferenzsicherung mit TOC-Informationen und die entsprechende Imagegesamtsicherung mit TOC-Informationen oder (2) eine Imagegesamtsicherung mit TOC-Informationen.
5. Klicken Sie auf die Auswahlfelder neben den Dateien oder Verzeichnissen, die Sie zurückschreiben wollen.
    a. Wenn Sie Dateien aus einem NAS-Image zurückschreiben wollen, das an einem bestimmten Datum gesichert wurde, oder wenn Sie Dateien aus älteren Sicherungsversionen anzeigen wollen, heben Sie den zurückzuschreibenden Datenträger hervor, und klicken Sie auf die Schaltfläche Zeitpunkt.
    b. Wenn Sie Das Datum eines Zeitpunkts verwenden in den Fenstern 'Zurückschreiben nach Zeitpunkt' auswählen, werden unter dem Objekt Dateiebene Dateien aus dem Image angezeigt, das an diesem Datum gesichert wurde. Falls es sich um ein Differenzimage handelt, werden außerdem die Dateien aus dem zugehörigen Gesamtimage unter dem Objekt Dateiebene angezeigt.
    c. Wenn Sie im Fenster 'Zurückschreiben nach Zeitpunkt' die Option Ausgewählte Images verwenden anklicken, wird das Fenster 'Ausgewählte Images' angezeigt, über das Sie Images auswählen können. Der Inhalt der ausgewählten Images wird im Objekt Dateiebene angezeigt.

6. Klicken Sie auf Zurückschreiben. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Geben Sie die Informationen in das Fenster 'Zurückschreibungsziel' ein. Wenn Sie ein anderes Ziel für die Zurückschreibung auswählen, können Sie jeweils nur einen Datenträger an ein anderes Ziel zurückschreiben.
7. Klicken Sie auf Zurückschreiben. Im Fenster Task-Liste für die NAS-Zurückschreibung werden der Verarbeitungsstatus der Zurückschreibung und die Statusleiste angezeigt. Eine Zahl neben der Statusleiste gibt, falls bekannt, die Größe der Zurückschreibung an. Nach Beendigung der Zurückschreibung zeigt das Fenster 'NAS-Zurückschreibungsbericht' Verarbeitungsdetails an. Wenn Sie die Web-Browser-Sitzung schließen müssen, werden aktuelle NAS-Operationen nach der Trennung der Verbindung fortgesetzt. Sie können die Schaltfläche Verlassen im Fenster Task-Liste für die NAS-Zurückschreibung verwenden, um die Verarbeitungsüberwachung zu verlassen, ohne die aktuelle Operation zu beenden.
8. (Optional) Um die Verarbeitung einer Operation zu überwachen, wählen Sie Aktionen > IBM Spectrum Protect-Aktivitäten im Hauptfenster aus.

Ergebnisse

Hinweise:

- Workstationsicherungen und ferne Sicherungen (NAS-Sicherungen) schließen sich in einem Zurückschreibungsfenster gegenseitig aus. Wenn ein Element für die Zurückschreibung ausgewählt wurde, muss das nächste Element, das Sie auswählen, denselben Typ aufweisen (entweder Workstation oder NAS).
- Um Informationen zu Objekten in einem NAS-Knoten anzuzeigen, heben Sie das Objekt hervor und wählen Sie Anzeigen > Dateiinformationen im Menü aus.
- Um NAS-Dateibereiche zu löschen, wählen Sie Dienstprogramme > Dateibereiche löschen aus. Sie können sowohl Workstationobjekte als auch ferne Objekte löschen.

Zugehörige Verweise:
Toc
AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Optionen und Befehle für die Zurückschreibung von NAS-Dateisystemen über die Befehlszeile

Dieser Abschnitt enthält einige Beispiele für Optionen und Befehle, die Sie zum Zurückschreiben von NAS-Dateisystemimages über die Befehlszeile verwenden können.

Tabelle 1. NAS-Optionen und -Befehle

Option oder Befehl	Definition	Seite
query node	Zeigt alle Knoten an, für die eine bestimmte Verwaltungsbenutzer-ID die Berechtigung zum Ausführen von Operationen hat. Die Verwaltungsbenutzer-ID sollte mindestens die Clienteignerberechtigung sowohl über den NAS-Knoten als auch den Client-Workstation-Knoten besitzen, der entweder von der Befehlszeile oder vom Web-Client aus verwendet wird.	Query Node
query backup	Verwenden Sie den Befehl query backup mit der Option class, um Informationen zu den Dateisystemimages anzuzeigen, die für einen NAS-Dateiserver gesichert wurden.	Query Backup
query filespace	Verwenden Sie den Befehl query filespace mit der Option ***class***, um eine Liste der Dateibereiche anzuzeigen, die zu einem NAS-Knoten gehören.	Query Filespace
restore nas	Schreibt das Image eines Dateisystems zurück, das zu einem NAS-Dateiserver gehört.	Restore NAS
AIX-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme monitor process	AIX-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeZeigt die aktuellen Sicherungs- und Zurückschreibungsprozesse für alle NAS-Knoten an, für die ein Benutzer mit Verwaltungsaufgaben die Berechtigung hat. Der Benutzer mit Verwaltungsaufgaben kann dann einen Prozess für die Überwachung auswählen.	AIX-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme Monitor Process
cancel process	Zeigt die aktuellen Sicherungs- und Zurückschreibungsprozesse für alle NAS-Knoten an, für die ein Benutzer mit Verwaltungsaufgaben die Berechtigung hat. In der Anzeige kann der Benutzer mit Verwaltungsaufgaben einen Prozess zum Abbrechen auswählen.	Cancel Process
delete filespace	Verwenden Sie delete filespace mit der Option class, um eine Liste der Dateibereiche anzuzeigen, die zu einem NAS-Knoten gehören. In dieser Liste können Sie einen Dateibereich zum Löschen auswählen.	Delete Filespace

AIX-BetriebssysteOracle Solaris-BetriebssystemeUnabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: `/vol/vol0`.

Windows-BetriebssystemeFür eine NAS-Dateisystemspezifikation werden folgende Konventionen verwendet:

Windows-Betriebssysteme

- Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: `/vol/vol0`.
- Für NAS-Dateisystembezeichnungen in der Befehlszeile müssen geschweifte Klammern `{}` als Begrenzer um Dateisystemnamen verwendet werden, zum Beispiel `{/vol/vol0}`.

Anmerkung: Wird eine NAS-Zurückschreibungsoperation mithilfe des Befehlszeilenclients oder des Web-Clients eingeleitet, startet der Server einen Prozess, um die Operation einzuleiten, zu steuern und zu überwachen. Der Fortschritt in der Befehlszeilenschnittstelle des Clients lässt sich erst nach kurzer Zeit feststellen, da der Server eine Ladeoperation und andere erforderliche Tasks ausführen muss, bevor die Datenversetzung erfolgt. Der IBM Spectrum Protect-Befehlszeilenclient zeigt unter Umständen die Nachricht `Unterbrochen...` an, wenn der Ladevorgang erfolgt. Sie können diese Nachricht ignorieren.
Mac OS X-BetriebssysteMac OS X-BetriebssysteAIX-BetriebssysteLinux-BetriebssysteOracle Solaris-Betriebssysteme

Aktive oder inaktive Sicherungen zurückschreiben

Ihr Administrator legt fest, wie viele Sicherungsversionen IBM Spectrum Protect für jede Datei auf Ihrer Workstation aufbewahrt.

Sind mehrere Versionen einer Datei vorhanden, können ältere Versionen zurückgeschrieben werden, falls die aktuellste Sicherungsversion beschädigt ist. Die aktuellste Sicherungsversion ist die *aktive* Version. Jede andere Sicherungsversion ist eine *inaktive* Version.

Bei jeder Dateisicherung markiert IBM Spectrum Protect die neue Sicherungsversion als die aktive Sicherungsversion, und die letzte aktive Sicherungsversion wird zu einer inaktiven Version. Wenn die maximal zulässige Anzahl inaktiver Versionen erreicht ist, löscht IBM Spectrum Protect die älteste inaktive Version.

Soll eine inaktive Sicherungsversion zurückgeschrieben werden, müssen sowohl aktive als auch inaktive Versionen angezeigt werden. Klicken Sie dazu **Anzeigen** → **Aktive/inaktive Dateien anzeigen** an. Sollen nur die aktiven Versionen angezeigt werden (Standardwert), klicken Sie **Anzeigen** → **Nur aktive Dateien anzeigen** an. Wird versucht, mehrere Versionen einer Datei gleichzeitig zurückzuschreiben, wird nur die aktive Version zurückgeschrieben.

Verwenden Sie in der IBM Spectrum Protect-Befehlszeile die Option inactive, um sowohl aktive als auch inaktive Objekte anzuzeigen.

Zugehörige Verweise:
Inactive
Mac OS X-BetriebssysteMac OS X-BetriebssysteAIX-BetriebssysteLinux-BetriebssysteOracle Solaris-Betriebssysteme

Daten über die grafische Benutzerschnittstelle zurückschreiben

In diesem Abschnitt sind die Schritte aufgelistet, die Sie ausführen müssen, um Sicherungsversionen von einzelnen Dateien oder Unterverzeichnissen zurückzuschreiben.

Vorgehensweise

1. Klicken Sie auf **Zurückschreiben** im Hauptfenster. Das Fenster 'Zurückschreiben' wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur. Wählen Sie die Auswahlfelder neben den Dateien oder Verzeichnissen, die zurückgeschrieben werden sollen, aus. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol **Suchen** in der Funktionsleiste.
3. Die Suchkriterien in das Fenster 'Dateien suchen (Zurückschreiben)' eingeben.
4. Klicken Sie auf die Schaltfläche **Suchen**. Das Fenster 'Übereinstimmende Dateien (Zurückschreiben)' wird angezeigt.
5. Klicken Sie auf die Auswahlfelder neben den Dateien, die zurückgeschrieben werden sollen, und schließen Sie das Fenster 'Übereinstimmende Dateien (Zurückschreiben)'.
6. Die Filterkriterien in das Fenster 'Dateien suchen (Zurückschreiben)' eingeben.
7. Klicken Sie auf die Schaltfläche **Filter**. Das Fenster 'Zurückschreiben' zeigt die gefilterten Dateien an.
8. Klicken Sie auf die Auswahlfelder neben den gefilterten Dateien oder Verzeichnissen, die zurückgeschrieben werden sollen.
9. Um bestimmte Zurückschreibungsoptionen zu ändern, klicken Sie auf die Schaltfläche **Optionen**. Die geänderten Optionen sind *nur* während der aktuellen Sitzung wirksam.
10. Klicken Sie auf **Zurückschreiben**. Das Fenster 'Zurückschreibungsziel' wird angezeigt. Geben Sie die Informationen in das Fenster 'Zurückschreibungsziel' ein.
11. Klicken Sie auf **Zurückschreiben**. Im Fenster **Task-Liste** für die Zurückschreibung wird der Verarbeitungsstatus der Zurückschreibung angezeigt.

Ergebnisse

Anmerkung: Beachten Sie unter Mac OS X die folgenden Hinweise, wenn Sie Daten über die GUI zurückschreiben:

1. Wenn die IBM Spectrum Protect-Tools für Administratoren zum Starten des Clients verwendet werden, wird der Client mit der UID null ausgeführt. Dies bedeutet, dass der Root Eigner eines Ordners ist, den Sie als Ziel für die Zurückschreibung erstellen. Sie müssen die Berechtigungen des Ordners ändern, um auf die Dateien zugreifen zu können. Sie können den Eigner des Ordners in einem Terminalfenster mit dem sudo-Befehl **chown** ändern. Weitere Informationen zu dieser Task finden Sie in der Dokumentation zu Ihrem Betriebssystem.
2. Wenn Sie bei einer Dateizurückschreibung für die Option replace den Wert *no* angeben, werden vorhandene Dateien nicht überschrieben, aber vorhandene Verzeichnisse werden überschrieben. Sollen vorhandene Verzeichnisse während einer Zurückschreibungsoperation nicht überschrieben werden, wählen Sie die Schaltfläche **Optionen**, Dropdown-Menü **Alle ausgewählten Dateien und Verzeichnisse** => Option **Nur Dateien** aus.
3. Werden Ordner, die sich nur in der Groß-/Kleinschreibung unterscheiden, von einem UFS- oder HFSX-Dateisystem in ein HFS-Dateisystem zurückgeschrieben, schreibt der Client den Inhalt beider Ordner in einen einzigen Ordner zurück.

 Mac OS X-Betriebssysteme  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Beispiele für Zurückschreibungsbefehle

Dieser Abschnitt enthält einige Beispiele für Befehle restore, die für bestimmte Tasks verwendet werden müssen.

Die folgende Tabelle enthält Beispiele zur Verwendung des Befehls restore zum Zurückschreiben von Objekten aus dem IBM Spectrum Protect-Serverspeicher.

Tabelle 1. Beispiele für Zurückschreibungsbefehle

Task	Befehl	Hinweise
Die aktuellste Sicherungsversion der Datei `/Users/monnett/Documents/h1.doc` zurückschreiben, selbst wenn die Sicherung inaktiv ist.	`dsmc restore /Users/monnett/Documents/h1.doc -latest`	Ist die zurückzuschreibende Datei nicht mehr auf der Workstation des Benutzers vorhanden und wurde nach dem Löschen der Datei eine Teilsicherung ausgeführt, befindet sich keine aktive Sicherungsversion der Datei auf dem Server. In diesem Fall muss mit der Option latest die neueste Sicherungsversion zurückgeschrieben werden. IBM Spectrum Protect schreibt die aktuellste Sicherungsversion zurück, unabhängig davon, ob sie aktiv oder inaktiv ist. Weitere Informationen siehe Latest.
Eine Liste der aktiven und inaktiven Sicherungsversionen von Dateien anzeigen, aus der Sie die zurückzuschreibenden Versionen auswählen können.	`dsmc restore "/Users/monnett/Documents/*"-pick -inactive`	Wird versucht, eine aktive und eine inaktive Version einer Datei gleichzeitig zurückzuschreiben, wird nur die aktive Version zurückgeschrieben. Pick und Inactive enthalten weitere Informationen.
Die Datei `/Users/monnett/Documents/h1.doc` in ihr Ursprungsverzeichnis zurückschreiben.	`dsmc restore /Users/monnett/Documents/h1.doc`	Wird kein Ziel angegeben, werden die Dateien an ihre ursprüngliche Position zurückgeschrieben.
Die Datei `/Users/monnett/Documents/h1.doc` unter einem neuen Namen und in ein neues Verzeichnis zurückschreiben.	`dsmc restore /Users/monnett/Documents/h1.doc /Users/gordon/Documents/h2.doc`	Keine
Die Dateien im Verzeichnis `/Users` und in allen zugehörigen Unterverzeichnissen zurückschreiben.	`dsmc restore /Users/ -subdir=yes`	Beim Zurückschreiben eines bestimmten Pfads und einer bestimmten Datei führt IBM Spectrum Protect eine rekursive Zurückschreibung *aller* Unterverzeichnisse unter diesem Pfad und aller Instanzen der angegebenen Datei, die sich unter *jedem* dieser Unterverzeichnisse befinden, durch. Weitere Informationen zur Option ***subdir*** befinden sich im Abschnitt Subdir.
Alle Dateien im Verzeichnis `/Users/gordon/Documents` in ihrem Status am 17. August 2003 um 13:00 Uhr zurückschreiben.	`dsmc restore -pitd=8/17/2003 -pitt=13:00:00 /Users/gordon/Documents/`	Weitere Informationen zu den Optionen pitdate und pittime enthalten die Abschnitte Pitdate und Pittime.

Task	Befehl	Hinweise
Alle Dateien aus dem Verzeichnis `/Users/mike/Documents`, die mit `.bak` enden, in das Verzeichnis `/Users/mike/projectn/` zurückschreiben.	`dsmc restore "/Users/mike/Documents/*.bak" /Users/mike/projectn/`	Handelt es sich bei dem Ziel um ein Verzeichnis, muss der Begrenzer `(/)` als letztes Zeichen des Ziel angegeben werden. Wird der Begrenzer nicht angegeben und handelt es sich bei der angegebenen Quelle um ein Verzeichnis oder eine Dateispezifikation mit einem Platzhalterzeichen, wird ein Fehler angezeigt. Ist das Verzeichnis `projectn` nicht vorhanden, wird es erstellt.
Die in der Datei `restorelist.txt` angegebenen Dateien an eine andere Position zurückschreiben.	`dsmc restore -filelist=/Users/user2/Documents/restorelist.txt /Users/NewRestoreLocation/`	Weitere Informationen zum Zurückschreiben von Dateilisten befinden sich im Abschnitt Filelist.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeBeispiele: Große Datenvolumen über die Befehlszeile zurückschreiben
  Müssen sehr viele Dateien zurückgeschrieben werden, kann die Leistung verbessert werden, wenn anstelle der grafischen Benutzerschnittstelle der Befehl restore verwendet wird. Außerdem lässt sich die Leistung verbessern, wenn mehrere restore-Befehle gleichzeitig eingegeben werden.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme
  Standardzurückschreibung mit Abfrage, Zurückschreibung ohne Abfrage und wiederanlauffähige Zurückschreibung
  In diesem Abschnitt werden die Standardzurückschreibung (klassische Zurückschreibung), die Zurückschreibung ohne Abfrage und die wiederanlauffähige Zurückschreibung beschrieben.

Zugehörige Verweise:
Restore
Mac OS X-BetriebssystemeMac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Beispiele: Große Datenvolumen über die Befehlszeile zurückschreiben

Müssen sehr viele Dateien zurückgeschrieben werden, kann die Leistung verbessert werden, wenn anstelle der grafischen Benutzerschnittstelle der Befehl restore verwendet wird. Außerdem lässt sich die Leistung verbessern, wenn mehrere restore-Befehle gleichzeitig eingegeben werden.

Sollen beispielsweise alle Dateien im Dateisystem `/home` zurückgeschrieben werden, geben Sie Folgendes ein:

```
dsmc restore /home/ -subdir=yes -replace=all -tapeprompt=no
```

Werden jedoch mehrere Befehle für die Verzeichnisse im Dateibereich `/home` eingegeben, können die Dateien schneller zurückgeschrieben werden.

Es können beispielsweise folgende Befehle eingegeben werden:

```
dsmc restore /home/monnett/ -subdir=yes -replace=all -tapeprompt=no
   dsmc restore /home/gillis/ -subdir=yes -replace=all -tapeprompt=no
   dsmc restore /home/stewart/ -subdir=yes -replace=all -tapeprompt=no
```

Sie können auch die Option quiet in den restore-Befehlen verwenden, um Verarbeitungszeit einzusparen. Es werden jedoch keine Informationsnachrichten für einzelne Dateien angezeigt.

Anmerkung: Wenn Sie die geeigneten Werte für die Optionen subdir, replace, tapeprompt und quiet bereits in Ihrer Clientbenutzeroptionsdatei definiert haben, brauchen Sie diese Optionen nicht in die Befehle einzuschließen.

Werden mehrere Befehle zum Zurückschreiben von Dateien eingegeben, muss ein eindeutiger Teil des Dateibereichs in jedem Befehl restore angegeben werden. Es dürfen keine Überschneidungen bei den Dateispezifikationen in den Befehlen auftreten.

Mit dem Befehl query backup kann eine Liste der Verzeichnisse in einem Dateibereich angezeigt werden. Beispiel:

```
dsmc query backup -dirsonly -subdir=no /Users/
```

Im Allgemeinen können zwei bis vier restore-Befehle gleichzeitig eingegeben werden. Wie viele Befehle maximal gleichzeitig ausgeführt werden können, ohne die Leistung zu beeinträchtigen, ist abhängig von verschiedenen Faktoren, z. B. vom verfügbaren Speicher und von der Netzauslastung.

Mit welcher Geschwindigkeit Sie die Dateien zurückschreiben können, ist auch davon abhängig, wie viele Bandlaufwerke auf dem Server verfügbar sind und ob der Administrator die Kollokation verwendet, um Dateibereiche möglichst wenig Datenträgern zuzuordnen.

Befinden sich `/Users/user1` und `/Users/user2` beispielsweise auf demselben Band, muss das Zurückschreiben für `/Users/user2` warten, bis das Zurückschreiben für `/Users/user1` beendet ist. Befindet sich `/Users/user3` jedoch auf einem anderen Band und stehen mindestens zwei Bandlaufwerke zur Verfügung, kann das Zurückschreiben für `/Users/user3` und für `/Users/user1` gleichzeitig beginnen.

Setzen Sie die ulimit-Systemwerte auf unbegrenzt (-1), wenn Sie sehr große Dateien (2 GB) mit HSM oder dem Client für Sichern/Archivieren zurückschreiben. Der Client kann diese großen Dateien mit ausreichenden Systemressourcen zurückschreiben. Wenn die ulimit-Werte auf niedrigere Werte gesetzt werden, könnten Zurückschreibungsfehler auftreten.

Standardzurückschreibung mit Abfrage, Zurückschreibung ohne Abfrage und wiederanlauffähige Zurückschreibung

In diesem Abschnitt werden die Standardzurückschreibung (klassische Zurückschreibung), die Zurückschreibung ohne Abfrage und die wiederanlauffähige Zurückschreibung beschrieben.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Standardzurückschreibungsprozess mit Abfrage
  Der Standardzurückschreibungsprozess mit Abfrage ist auch als klassisches Zurückschreiben bekannt. In diesem Abschnitt wird die Standardzurückschreibung mit Abfrage beschrieben.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeProzess für Zurückschreibung ohne Abfrage
  Beim Zurückschreiben ohne Abfrage wird der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern es wird eine einzelne Zurückschreibungsanforderung an den Server gesendet.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWiederanlauffähiger Zurückschreibungsprozess
  Wird der Zurückschreibungsprozess aufgrund eines Stromausfalls oder eines Netzfehlers gestoppt, zeichnet der Server den Punkt auf, an dem dieser Ausfall oder Fehler erfolgte.

Standardzurückschreibungsprozess mit Abfrage

Der Standardzurückschreibungsprozess mit Abfrage ist auch als klassisches Zurückschreiben bekannt. In diesem Abschnitt wird die Standardzurückschreibung mit Abfrage beschrieben.

Die Standardzurückschreibung mit Abfrage arbeitet wie folgt:

- Der Client fragt den Server nach einer Liste mit Dateien ab, die für den Clientdateibereich gesichert wurden, der zurückgeschrieben werden soll.
- Der Server sendet eine Liste der gesicherten Dateien, die den Zurückschreibungsbedingungen entsprechen. Sollen sowohl aktive als auch inaktive Dateien zurückgeschrieben werden, sendet der Server Informationen zu allen gesicherten Dateien an den Client.
- Die vom Server ausgegebene Dateiliste wird im Clientspeicher sortiert, um die Zurückschreibungsreihenfolge der Dateien zu bestimmen und die für die Zurückschreibung erforderlichen Bandladevorgänge zu minimieren.
- Der Client teilt dem Server mit, Dateidaten und Verzeichnisobjekte zurückzuschreiben.
- Die Verzeichnisse und Dateien, die zurückgeschrieben werden sollen, werden vom Server an den Client gesendet.

Prozess für Zurückschreibung ohne Abfrage

Beim Zurückschreiben ohne Abfrage wird der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern es wird eine einzelne Zurückschreibungsanforderung an den Server gesendet.

1. Der Client teilt dem Server mit, dass eine Zurückschreibung ohne Abfrage ausgeführt werden soll, und stellt dem Server die Details zu den Dateibereichen, Verzeichnissen und Dateien zur Verfügung.
2. Der Server verwendet eine separate Tabelle, um die Einträge aufzuzeichnen, die die Zurückschreibung führen.
3. Die zurückzuschreibenden Daten werden an den Client gesendet. Die auf Platte gespeicherten Datei- und Verzeichnisobjekte werden sofort gesendet, da ein Sortieren dieser Daten vor dem Zurückschreiben des Objekts nicht erforderlich ist.
4. Sie können Mehrfachsitzungen verwenden, um die Daten zurückzuschreiben. Befinden sich die Daten auf mehreren Bändern, sind mehrere Mountpunkte auf dem Server verfügbar. Die Kombination der Option resourceutilization und MAXNUMMP ermöglicht Mehrfachsitzungen.

Windows-BetriebssystemeWenn Sie eine uneingeschränkte Quellendateispezifikation mit Platzhalterzeichen in den Befehl restore eingeben und keine der folgenden Optionen angeben, verwendet der Client eine Methode *Zurückschreibung ohne Abfrage* zum Zurückschreiben von Dateien und Verzeichnissen vom Server: inactive, latest, pick, fromdate oder todate. Diese Methode wird als *Zurückschreiben ohne Abfrage* bezeichnet, weil der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern eine einzige Zurückschreibungsanforderung an den Server gesendet wird. In diesem Fall gibt der Server die Dateien und Verzeichnisse ohne weitere Aktion durch den Client an den Client zurück. Der Client akzeptiert lediglich die vom Server kommenden Daten und schreibt sie an das im Befehl restore angegebene Ziel zurück.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWenn Sie eine uneingeschränkte Quellendateispezifikation mit Platzhalterzeichen in den Befehl restore eingeben und keine der folgenden Optionen angeben, verwendet der Client eine Methode *Zurückschreibung ohne Abfrage* zum Zurückschreiben von Dateien und Verzeichnissen vom Server: inactive, latest, pick, fromdate, todate. Diese Methode wird als *Zurückschreiben ohne Abfrage* bezeichnet, weil der Server nicht nach jedem zurückzuschreibenden Objekt abgefragt, sondern eine einzige Zurückschreibungsanforderung an den Server gesendet wird. In diesem Fall gibt der Server die Dateien und Verzeichnisse ohne weitere Aktion durch den Client an den Client zurück. Der Client akzeptiert lediglich die vom Server kommenden Daten und schreibt sie an das im Befehl restore angegebene Ziel zurück.

Mac OS X-BetriebssystemeBei Verwendung des IBM Spectrum Protect-GUI-Clients wäre ein Beispiel für einen unbeschränkten Befehl mit Platzhalterzeichen die Auswahl eines Ordners im Fenster 'Baumstruktur zurückschreiben'. Ein Beispiel für einen eingeschränkten Befehl mit Platzhalterzeichen wäre die Auswahl einzelner Dateien aus einem Ordner.

Im Befehlszeilenclient wäre ein Beispiel für einen unbeschränkten Befehl mit Platzhalterzeichen:

Mac OS X-Betriebssysteme

```
"/Users/user1/Documents/2004/*"
```

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
/home/mydocs/2004/*
```

Windows-Betriebssysteme

```
c:\mydocs\2004\*
```

Ein Beispiel für eine eingeschränkte Dateispezifikation mit Platzhalterzeichen wäre:

Mac OS X-Betriebssysteme

```
/Users/user1/Documents/2004/sales.*
```

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
/home/mydocs/2004/sales.*
```

Windows-Betriebssysteme

```
c:\mydocs\2004\sales.*
```

Wiederanlauffähiger Zurückschreibungsprozess

Wird der Zurückschreibungsprozess aufgrund eines Stromausfalls oder eines Netzfehlers gestoppt, zeichnet der Server den Punkt auf, an dem dieser Ausfall oder Fehler erfolgte.

Dieser Punkt ist dem Client als *wiederanlauffähige Zurückschreibung* bekannt. Es können mehrere wiederanlauffähige Zurückschreibungssitzungen vorhanden sein. Verwenden Sie den Befehl query restore oder wählen Sie **Wiederanlauffähige Zurückschreibungen** im Menü 'Aktionen' aus, um festzustellen, ob Ihr Client über wiederanlauffähige Zurückschreibungssitzungen in der Serverdatenbank verfügt.

Windows-BetriebssystemeEine wiederanlauffähige Zurückschreibung muss abgeschlossen werden, bevor weitere Sicherungen des Dateisystems versucht werden. Versuchen Sie, die unterbrochene Zurückschreibung zu wiederholen oder den Zieldateibereich zu sichern, schlägt der Versuch fehl, da die ursprüngliche Zurückschreibung nicht abgeschlossen wurde. Sie können die Zurückschreibung an dem Unterbrechungspunkt erneut starten, indem Sie den Befehl restart restore eingeben, oder Sie können die wiederanlauffähige Zurückschreibung löschen, indem Sie den Befehl cancel restore verwenden. Wenn Sie die unterbrochene Zurückschreibung erneut starten, wird mit der ersten Transaktion begonnen. Diese kann aus einer oder aus mehreren Dateien bestehen, die nicht vollständig zurückgeschrieben war oder waren, als die Unterbrechung auftrat. Aus diesem Grund können Sie einige Aufforderungen zum Ersetzen für Dateien aus der unterbrochenen Transaktion empfangen, die bereits zurückgeschrieben wurden.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeEine wiederanlauffähige Zurückschreibung muss abgeschlossen werden, bevor weitere Sicherungen des Dateisystems versucht werden. Versuchen Sie, die unterbrochene Zurückschreibung zu wiederholen oder den Zieldateibereich zu sichern, schlägt der Versuch fehl, da die ursprüngliche Zurückschreibung nicht abgeschlossen wurde. Sie können die Zurückschreibung an dem Unterbrechungspunkt erneut starten, indem Sie den Befehl restart restore eingeben, oder Sie können die wiederanlauffähige Zurückschreibung löschen, indem Sie den Befehl cancel restore verwenden.

Im Dialogfenster **Wiederanlauffähige Zurückschreibungen** in der IBM Spectrum Protect-GUI können Sie die unterbrochene Zurückschreibung auswählen und löschen oder die Zurückschreibung erneut starten. Wenn Sie die unterbrochene Zurückschreibung erneut starten, wird mit der ersten Transaktion begonnen. Diese kann aus einer oder aus mehreren Dateien bestehen, die nicht vollständig zurückgeschrieben war oder waren, als die Unterbrechung auftrat. Aus diesem Grund können Sie einige Aufforderungen zum Ersetzen für Dateien aus der unterbrochenen Transaktion empfangen, die bereits zurückgeschrieben wurden.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme Führen Sie folgende Schritte aus, um wiederanlauffähige Zurückschreibungen über die GUI auszuführen:

1. Wählen Sie **Aktionen –> Wiederanlauffähige Zurückschreibungen** in der Hauptanzeige aus.
2. Wählen Sie die wiederanlauffähige Zurückschreibungssitzung aus, die ausgeführt werden soll.
3. Klicken Sie auf die Schaltfläche **Erneut starten** unten auf der Anzeige.

Zugehörige Verweise:
Resourceutilization
Restore

Oracle Solaris-Betriebssysteme

Solaris Zettabyte-Dateisysteme (ZFS) zurückschreiben

ZFS-Dateisysteme (Zettabyte File System) verwenden Speicherpools zum Verwalten von physischen Speichereinheiten.

Wie Sie ein ZFS-Dateisystem zurückschreiben, ist davon abhängig, wie das Dateisystem gesichert wurde.

- Wenn Sie alle Dateien und Ordner als separate Objekte gesichert haben, können Sie sie mit einer Zurückschreibung auf Dateiebene zurückschreiben. Beispiel:

  ```
  dsmc restore /tank/myZFS/ -subdir=yes -replace=all
  ```

  Sie dürfen eine Zurückschreibung auf Dateiebene nicht für eine Wiederherstellung nach einem Katastrophenfall ausführen. Auch wenn Sie alle Systemdateien und -ordner erfolgreich aus einer Sicherung zurückschreiben, die von einem Client für Sichern/Archivieren erstellt wurde, kann das zurückgeschriebene System instabil sein oder fehlschlagen.
- Wenn Sie eine vollständige ZFS-Momentaufnahme als einzelne Datei gesichert haben, müssen Sie die Momentaufnahmedatei vom Server in ein temporäres Verzeichnis zurückschreiben. Beispiel:

  ```
  dsmc restore /tmpdir/mySnapshotfile
  ```

  Anschließend können Sie das Dateisystem mithilfe der Oracle Solaris ZFS-Befehle aus der Momentaufnahmedatei zurückschreiben. Beispiel:

  ```
  zfs receive tank/myZFS@mySnapshot < /tmpdir/mySnapshotFile
  ```

  Der Vorteil des Zurückschreibens eines ZFS aus einer Momentaufnahmedatei liegt darin, dass im Notfall das gesamte Dateisystem zurückgeschrieben werden kann.

  Ausführliche Informationen zum Zurückschreiben von Daten auf ZFS-Dateisystemen finden Sie in der bei Oracle erhältlichen Produktdokumentation. Wenn Sie einen ZFS-Root-Pool zurückschreiben, lesen Sie die Abschnitte, in denen die Neuerstellung des Root-Pools und die Wiederherstellung von Root-Pool-Momentaufnahmen beschrieben werden.

Zugehörige Tasks:
Solaris Zettabyte-Dateisysteme (ZFS) sichern
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Zusätzliche Zurückschreibungstasks

In diesem Abschnitt werden einige weiterführende Hinweise für das Zurückschreiben von Daten erläutert.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeEinen anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen
  Sie können andere Benutzer an derselben Workstation oder an einer anderen Workstation dazu berechtigen, Sicherungsversionen Ihrer Dateien zurückzuschreiben oder Archivierungskopien Ihrer Dateien abzurufen.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDateien von einem anderen Clientknoten zurückschreiben oder abrufen
  Nachdem andere Benutzer Ihnen den Zugriff auf ihre Dateien auf dem Server erteilt haben, können Sie diese Dateien in Ihr lokales System zurückschreiben oder abrufen.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDateien auf eine andere Workstation zurückschreiben oder abrufen
  Von einer anderen Workstation können Dateien zurückgeschrieben oder abgerufen werden, die bereits von Ihrer eigenen Workstation gesichert wurden. Sie müssen das IBM Spectrum Protect-Kennwort kennen, das Ihrem Knoten zugeordnet ist.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemePlatte nach Plattenverlust zurückschreiben
  Sie können Ihre Dateien nur wiederherstellen, wenn Sie den Client ausführen können. Steht die Platte, die den Client enthält, nicht zur Verfügung (beispielsweise weil sie gestohlen wurde oder aufgrund eines Hardwarefehlers), muss der Client erneut installiert werden, bevor die Dateien wiederhergestellt werden können. Geht auch die Platte verloren, die das Betriebssystem und die DFV-Software enthält, müssen Sie diese wiederherstellen, bevor Sie eine Verbindung zum IBM Spectrum Protect-Server herstellen können.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDateibereiche löschen
  Erteilt der IBM Spectrum Protect-Administrator einem Benutzer die Berechtigung, kann der Benutzer vollständige Dateibereiche aus dem Server löschen.
- Linux-BetriebssystemeSELinux für das Zurückschreiben von Dateien auf dem Red Hat Enterprise Linux 5-Client aktivieren
  Wenn Sie Benutzer ohne Rootberechtigung sind und versuchen, Dateien auf einem Red Hat Enterprise Linux 5-Client zurückzuschreiben, müssen Sie zuerst SELinux aktivieren.

Mac OS X-BetriebssystemeMac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Einen anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen

Sie können andere Benutzer an derselben Workstation oder an einer anderen Workstation dazu berechtigen, Sicherungsversionen Ihrer Dateien zurückzuschreiben oder Archivierungskopien Ihrer Dateien abzurufen.

Informationen zu diesem Vorgang

Auf diese Weise können mehrere Benutzer oder Workstations, die mit einem anderen Knotennamen verwendet werden, Dateien gemeinsam benutzen. Soll ein Benutzer an einer anderen Workstation dazu berechtigt werden, Ihre Dateien zurückzuschreiben oder abzurufen, muss auf der anderen Workstation einer der UNIX-Clients aktiv und die Workstation muss bei Ihrem Server registriert sein.

 Mac OS X-BetriebssystemeAnmerkung: Mac OS X kann *nur* Mac OS X-Knoten zurückschreiben.

Wie folgt vorgehen, um andere Benutzer zu berechtigen, die eigenen Dateien zurückzuschreiben oder abzurufen:

Vorgehensweise

1. Klicken Sie auf **Dienstprogramme** → **Knotenzugriffsliste** im Hauptfenster. Das Fenster Knotenzugriffsliste wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**. Das Fenster 'Zugriffsregel hinzufügen' wird angezeigt.
3. Im Fenster 'Zugriffsregel hinzufügen' wählen Sie ein Element im Feld 'Zugriff erlauben für' aus, um den Typ der Daten anzugeben, auf die der andere Benutzer zugreifen kann. Sie können entweder gesicherte oder archivierte Objekte auswählen.
4. Geben Sie in das Feld 'Zugriff erteilen für Knoten' den Knotennamen der Host-Workstation des Benutzers ein, der auf Ihre Daten zugreifen darf.
5. Geben Sie in das Feld 'Benutzer' den Namen des Benutzers auf einem Knoten ein, der auf Ihre Daten zugreifen kann.
6. Wählen Sie im Feld 'Dateibereich und Verzeichnis' den Dateibereich und das Verzeichnis aus, auf den bzw. das der Benutzer zugreifen kann. Sie können jeweils einen Dateibereich und ein Verzeichnis auswählen. Wenn Sie dem Benutzer Zugriff auf einen anderen Dateibereich oder ein anderes Verzeichnis geben wollen, müssen Sie eine andere Zugriffsregel erstellen.
7. Soll der Zugriff des Benutzers auf bestimmte Dateien im Verzeichnis begrenzt werden, geben Sie den Namen oder das Muster für den Namen der Dateien auf dem Server, auf die der andere Benutzer zugreifen darf, im Feld Dateiname an. Im Feld 'Dateiname' kann nur ein Eintrag eingegeben werden. Dabei kann es sich um den Namen einer einzelnen Datei oder um ein Muster handeln, das mit einem oder mehreren Dateien übereinstimmt. Es kann ein Platzhalterzeichen als Teil des Musters verwendet werden. Ihr Eintrag muss mit Dateien übereinstimmen, die auf dem Server gespeichert wurden.
8. Für die Java™-GUI: Wenn Sie Zugriff auf alle Dateien erteilen wollen, die mit der Dateinamenspezifikation innerhalb des ausgewählten Verzeichnisses einschließlich der Unterverzeichnisse übereinstimmen, klicken Sie auf **Unterverzeichnisse einschließen**.
9. Klicken Sie auf die Schaltfläche **OK**, um die Zugriffsregel zu sichern und das Fenster 'Zugriffsregel hinzufügen' zu schließen.
10. Die von Ihnen erstellte Zugriffsregel wird im Listenfenster des Fensters 'Knotenzugriffsliste' angezeigt. Nach Beendigung der Arbeit im Fester 'Knotenzugriffsliste' klicken Sie auf die Schaltfläche **OK**. Wenn Sie Ihre Änderungen nicht sichern möchten, klicken Sie auf **Abbrechen** oder schließen Sie das Fenster.

Ergebnisse

In der Befehlszeilenschnittstelle des Clients verwenden Sie den Befehl set access, um einen anderen Knoten zu berechtigen, Ihre Dateien zurückzuschreiben oder abzurufen. Sie können auch den Befehl query access verwenden, um Ihre aktuelle Liste einzusehen, und den Befehl delete access, um Knoten aus der Liste zu löschen.

Zugehörige Verweise:
Delete Access
Query Access
Set Access
 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Dateien von einem anderen Clientknoten zurückschreiben oder abrufen

Nachdem andere Benutzer Ihnen den Zugriff auf ihre Dateien auf dem Server erteilt haben, können Sie diese Dateien in Ihr lokales System zurückschreiben oder abrufen.

Informationen zu diesem Vorgang

Sie können Dateibereiche für einen anderen Benutzer auf dem Server anzeigen, die Sicherungsversionen für einen anderen Benutzer zurückschreiben oder die Archivierungskopien für einen anderen Benutzer in Ihr lokales Dateisystem abrufen:

Vorgehensweise

1. Klicken Sie auf **Dienstprogramme** im Hauptfenster.
2. Klicken Sie auf **Zugriff auf anderen Knoten**. Das Fenster 'Zugriff auf anderen Knoten' wird angezeigt.

3. Geben Sie den Knotennamen der Host-Workstation des Benutzers in das Feld 'Knotenname' ein. Den Benutzernamen in das Feld 'Benutzername' eingeben.
4. Klicken Sie auf die Schaltfläche **Definieren**.

Ergebnisse

Wird mit Befehlen gearbeitet, können mit den Optionen fromnode und fromowner der Knotenname und der Name des Benutzers, der Eigner der Dateien ist, angegeben werden.

Sollen beispielsweise Dateien in eines Ihrer eigenen Dateisysteme zurückgeschrieben werden, die auf einer Workstation mit dem Namen `Knoten1` gesichert wurden und deren Eigner ein Benutzer mit dem Namen `Anne` ist, Folgendes eingeben:

```
dsmc restore -fromn=knoten1 -fromo=anne "/home/proj/*" /home/gillis/
```

Verwenden Sie den Befehl query filespace, um eine Liste von Dateibereichen abzurufen. Soll beispielsweise eine Liste der Dateibereiche, deren Eigner `Anne` ist, für `Knoten1` angezeigt werden, Folgendes eingeben:

```
dsmc query filespace -fromn=knoten1 -fromo=anne
```

Zugehörige Verweise:
Fromnode
Query Filespace
Restore
Retrieve
Mac OS X-Betriebssysteme Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Dateien auf eine andere Workstation zurückschreiben oder abrufen

Von einer anderen Workstation können Dateien zurückgeschrieben oder abgerufen werden, die bereits von Ihrer eigenen Workstation gesichert wurden. Sie müssen das IBM Spectrum Protect-Kennwort kennen, das Ihrem Knoten zugeordnet ist.

Verwenden Sie zum Zurückschreiben oder Abrufen von Dateien auf eine andere Workstation die Option virtualnodename, um den Knotennamen der Workstation anzugeben, auf der die Dateien gesichert wurden. Die Option virtualnodename kann nicht auf den Hostnamen der Workstation gesetzt werden. Sie können die Option virtualnodename verwenden, wenn Sie IBM Spectrum Protect starten, oder Sie können die Option virtualnodename zu Ihrer Clientbenutzeroptionsdatei dsm.opt hinzufügen. Verwenden Sie die Option virtualnodename im Befehl **dsmj**, wenn Sie ausnahmsweise die Workstation eines anderen Benutzers verwenden und die zugehörige Clientbenutzeroptionsdatei nicht aktualisieren wollen.

IBM Spectrum Protect fordert das Kennwort für Ihren ursprünglichen Knoten an. Nach der Eingabe des korrekten Kennworts werden alle Dateisysteme der ursprünglichen Workstation in dem Fenster "Zurückschreiben" oder "Abrufen" angezeigt. Sie können Dateien wie auf Ihrer eigenen Workstation zurückschreiben oder abrufen.

Wichtig: Wird diese Methode verwendet, um auf Dateien zuzugreifen, haben Sie auf alle Dateien Zugriff, die auf Ihrer Workstation gesichert und archiviert wurden. Sie werden als virtueller Root betrachtet.

Die Option virtualnodename kann in einem Befehl verwendet werden. Sollen beispielsweise die Dateien in ***projx*** zurückgeschrieben werden, Folgendes eingeben:

```
dsmc restore -virtualnodename=nodeone "/home/monnett/projx/*"
```

Sollen die Dateien auf der anderen Workstation nicht in dasselbe Verzeichnis zurückgeschrieben oder abgerufen werden, geben Sie ein anderes Ziel ein.

Diese Hinweise gelten sowohl für das Zurückschreiben als auch für das Abrufen von Dateien.

Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Platte nach Plattenverlust zurückschreiben

Sie können Ihre Dateien nur wiederherstellen, wenn Sie den Client ausführen können. Steht die Platte, die den Client enthält, nicht zur Verfügung (beispielsweise weil sie gestohlen wurde oder aufgrund eines Hardwarefehlers), muss der Client erneut installiert werden, bevor die Dateien wiederhergestellt werden können. Geht auch die Platte verloren, die das Betriebssystem und die DFV-Software enthält, müssen Sie diese wiederherstellen, bevor Sie eine Verbindung zum IBM Spectrum Protect-Server herstellen können.

Informationen zu diesem Vorgang

Der Benutzer kann sich gegen diese Verluste schützen, indem er immer die Installationsdatenträger verfügbar hat, mit denen er einen Status des Systems zurückschreiben kann, der es erlaubt, die Verbindung zum Server herzustellen und mit der Wiederherstellung der Daten zu beginnen. Die Installationsdatenträger sollten Folgendes enthalten:

Vorgehensweise

1. Ein startfähiges Betriebssystem, mit dem Basisfunktionen ausgeführt werden können.
2. Ein korrekt konfiguriertes Kommunikationsprogramm, das eine Datenübertragung mit dem Server ermöglicht.
3. Ein Client mit entsprechend angepassten Optionsdateien. Diese Task kann mithilfe der Befehlszeilenschnittstelle des Clients ausgeführt werden.

Ergebnisse

Das verwendete Kommunikationspaket bestimmt, welche Dateien benötigt werden. Die Handbücher zum Betriebssystem und zur DFV-Software helfen bei der Zusammenstellung der Installationsdatenträger.

Ist auf Ihrer Workstation auch der IBM Spectrum Protect for Space Management installiert, müssen die Installationsdatenträger den HSM-Befehlszeilenclient enthalten.

Anmerkung: Der Administrator kann Operationen zum Zurückschreiben planen, was besonders hilfreich sein kann, wenn eine große Anzahl Dateien zurückgeschrieben werden muss.

Zugehörige Konzepte:
AIX-Betriebssysteme Linux-Betriebssysteme Sichern und Zurückschreiben auf speicherverwalteten Dateisystemen
Mac OS X-Betriebssysteme Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Dateibereiche löschen

Erteilt der IBM Spectrum Protect-Administrator einem Benutzer die Berechtigung, kann der Benutzer vollständige Dateibereiche aus dem Server löschen.

Informationen zu diesem Vorgang

Beim Löschen eines Dateibereichs werden alle Dateien und Images, sowohl Sicherungsversionen als auch Archivierungskopien, innerhalb dieses Dateibereichs gelöscht. Wenn Sie beispielsweise den Dateibereich für Ihr Dateisystem `/home/monnet` löschen, löschen Sie damit jede Sicherungskopie für jede Datei in diesem Dateisystem sowie jede Datei, die Sie von diesem Dateisystem archiviert haben. **Das Löschen eines Dateibereichs muss gründlich überlegt werden**. Sie müssen ein berechtigter Benutzer sein, um diese Task auszuführen.

Sie können einzelne Sicherungsversionen löschen, indem Sie den Befehl delete backup verwenden.

Sie können Dateibereiche mithilfe der GUI des Clients für Sichern/Archivieren oder der Clientbefehlszeilenschnittstelle löschen. Verwenden Sie zum Löschen von NAS-Dateibereichen den Web-Client oder die Befehlszeilenschnittstelle des Clients.

Soll ein Dateibereich mit der grafischen Benutzerschnittstelle gelöscht werden, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Wählen Sie **Dienstprogramme** → **Dateibereiche löschen** im Hauptfenster aus.
2. Klicken Sie auf die Auswahlfelder neben den Dateibereichen, die gelöscht werden sollen.
3. Klicken Sie auf die Schaltfläche **Löschen**. Der Client fordert Sie zur Bestätigung auf, bevor der Dateibereich gelöscht wird.

Ergebnisse

Sie können einen Dateibereich auch mit dem Befehl delete filespace löschen. Verwenden Sie die Option ***class*** im Befehl delete filespace, um NAS-Dateibereiche zu löschen.

Zugehörige Verweise:
Class
Delete Backup
Delete Filespace
Linux-Betriebssysteme

SELinux für das Zurückschreiben von Dateien auf dem Red Hat Enterprise Linux 5-Client aktivieren

Wenn Sie Benutzer ohne Rootberechtigung sind und versuchen, Dateien auf einem Red Hat Enterprise Linux 5-Client zurückzuschreiben, müssen Sie zuerst SELinux aktivieren.

Wenn Sie SELinux nicht aktivieren, werden Sie beim Zurückschreiben von Dateien mit geänderten erweiterten Attributen Probleme bekommen.

Daten mit Clients für Sichern/Archivieren archivieren und abrufen

Wenn Sie eine Kopie einer Datei zur Langzeitspeicherung oder Archivierung auf dem IBM Spectrum Protect-Server speichern wollen, verwenden Sie die Funktion *Archivieren*.

Informationen zu diesem Vorgang

Falls die Originaldatei beschädigt wird oder verloren geht, verwenden Sie die Funktion *Abrufen*, um die Archivierungskopie vom Server wiederherzustellen.

- Windows-BetriebssystemeDaten archivieren und abrufen (Windows)
  Sie können selten verwendete Dateien auf dem IBM Spectrum Protect-Server archivieren und bei Bedarf abrufen. Das Archivieren und Abrufen von Dateien ist dem Sichern und Zurückschreiben von Dateien ähnlich.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDaten archivieren und abrufen (UNIX und Linux)
  Sie können selten verwendete Dateien auf dem IBM Spectrum Protect-Server archivieren und bei Bedarf abrufen. Das Archivieren und Abrufen von Dateien ist dem Sichern und Zurückschreiben von Dateien ähnlich. Viele Fenster und Konzepte sind ähnlich.

Windows-Betriebssysteme

Daten archivieren und abrufen (Windows)

Sie können selten verwendete Dateien auf dem IBM Spectrum Protect-Server archivieren und bei Bedarf abrufen. Das Archivieren und Abrufen von Dateien ist dem Sichern und Zurückschreiben von Dateien ähnlich.

Sofern nicht anders angegeben, beziehen sich Verweise auf Windows auf alle unterstützten Windows-Betriebssysteme.

Mit Ausnahme der folgenden Funktionen gelten alle primären Archivierungs- und Abrufprozeduren auch für den Web-Client:

- Profileditor
- Setup-Assistent

Sie können die folgenden primären Archivierungs- und Abruftasks ausführen:

- Daten über die grafische Benutzerschnittstelle archivieren
- Beispiele für das Archivieren von Daten über die Befehlszeile
- Archivierungsdaten löschen
- Archivierungen über die GUI abrufen
- Archivierungskopien über die Befehlszeile abrufen

- Windows-BetriebssystemeDateien archivieren
  Vor dem Archivieren von Dateien müssen die gewünschten Dateien ausgewählt werden. Die Dateien können nach Namen oder nach Beschreibung oder aus einer Verzeichnisbaumstruktur ausgewählt werden.
- Windows-BetriebssystemeArchivierungen abrufen
  Mit der Funktion Abrufen kann eine Archivierungskopie einer Datei oder eines Verzeichnisses wiederhergestellt werden.

Zugehörige Konzepte:
Wann werden Dateien gesichert und wann archiviert?
Zugehörige Tasks:
Web-Client-Sitzung starten
Windows-Betriebssysteme

Dateien archivieren

Vor dem Archivieren von Dateien müssen die gewünschten Dateien ausgewählt werden. Die Dateien können nach Namen oder nach Beschreibung oder aus einer Verzeichnisbaumstruktur ausgewählt werden.

Der Administrator kann Zeitpläne zur automatischen Archivierung bestimmter Dateien auf der Workstation definieren. In den folgenden Abschnitten wird beschrieben, wie Dateien ohne Zeitpläne archiviert werden.

Sie müssen allen archivierten Dateien Archivierungsbeschreibungen zuordnen. Mithilfe einer Archivierungsbeschreibung erhalten die Daten eine aussagekräftige Beschreibung, mit der Dateien und Verzeichnisse später identifiziert werden können. Die Archivierungsbeschreibung darf maximal 254 Zeichen lang sein. Wenn Sie keine Beschreibung eingeben, wird die folgende Standardarchivierungsbeschreibung zugeordnet:

```
   Archivierungsdatum: MM/TT/JJJJ

Hierbei gibt MM/TT/JJJJ das aktuelle Datum an.
```

Wenn Sie die Archivierungsfunktion aus der grafischen Benutzerschnittstelle für Sichern/Archivieren auswählen, wird eine Liste aller bereits verwendeten Archivierungsbeschreibungen angezeigt. Sie können diese Archivierungsbeschreibungen zukünftigen Archivierungen zuordnen.

Bei der Teilsicherung können umgelagerte Dateien zurückgerufen werden, während bei der selektiven Sicherung und Archivierung immer umgelagerte Dateien zurückgerufen werden, sofern Sie nicht die Option skipmigrated verwenden.

- Windows-BetriebssystemeMomentaufnahmesicherung oder -archivierung mit Unterstützung offener Dateien
  Wenn die Unterstützung offener Dateien konfiguriert wurde, führt der Client für Sichern/Archivieren eine Momentaufnahmesicherung oder

-archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder "im Gebrauch") sind.

- Windows-BetriebssystemeDaten über die grafische Benutzerschnittstelle archivieren
  Aus einer Verzeichnisbaumstruktur können bestimmte Dateien oder vollständige Verzeichnisse archiviert werden. Für jede zu archivierende Dateigruppe (Archivierungspaket) kann außerdem eine eindeutige Beschreibung zugeordnet werden.
- Windows-BetriebssystemeBeispiele für das Archivieren von Daten über die Befehlszeile
  Sie können Daten archivieren, wenn Sie Kopien von Dateien für die spätere Verwendung, zu Dokumentationszwecken oder aufgrund gesetzlicher Anforderungen in ihrem aktuellen Status aufbewahren wollen.
- Windows-BetriebssystemeDaten mit dem Clientknoten-Proxy archivieren
  Archivierungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.
- Windows-BetriebssystemeArchivierungsdaten löschen
  Sie können einzelne Archivierungsobjekte aus dem IBM Spectrum Protect-Server löschen, ohne den gesamten Dateibereich löschen zu müssen, zu dem die Objekte gehören.

Zugehörige Konzepte:
Windows-Betriebssysteme Optionen für die Sicherung umgelagerter Dateien: skipmigrated, checkreparsecontent, stagingdirectory
Zugehörige Tasks:
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren
Windows-Betriebssysteme

Momentaufnahmesicherung oder -archivierung mit Unterstützung offener Dateien

Wenn die Unterstützung offener Dateien konfiguriert wurde, führt der Client für Sichern/Archivieren eine Momentaufnahmesicherung oder -archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder "im Gebrauch") sind.

Über die Momentaufnahme wird die Archivierung von einer Kopie des Dateisystems erstellt, die dem Dateisystemstatus zum Zeitpunkt der Erstellung der Momentaufnahme entspricht. Nachfolgende Änderungen am Dateisystem werden bei der Archivierung nicht berücksichtigt. Sie können den Parameter snapshotproviderfs der Option include.fs auf none setzen, um anzugeben, welche Laufwerke keine Unterstützung für offene Dateien verwenden.

Anmerkung:

1. Sie können die Option include.fs verwenden, um Momentaufnahmeoptionen pro Dateisystem festzulegen.
2. Die Unterstützung offener Dateien ist nur für lokale fixierte Datenträger (entweder an Laufwerkbuchstaben oder Datenträgermountpunkte angehängt) verfügbar, die mit FAT-, FAT32-, NTFS- oder ReFS-Dateisystemen formatiert sind. Diese Unterstützung schließt an ein SAN angeschlossene Datenträger ein, die diese Anforderungen erfüllen.
3. Wenn der Client keine Momentaufnahme erstellen kann, findet eine Übernahme in einer Nicht-OFS-Sicherung statt; dieselbe Sicherungsunterstützung, die erfolgen würde, wenn die OFS-Funktion nicht installiert wäre (OFS - Open File Support, Unterstützung offener Dateien).
4. Damit die Unterstützung offener Dateien in einer Clusterumgebung aktiviert wird, sollte für alle Workstations im Cluster die OFS-Funktion konfiguriert sein.
5. Wenn Sie die Funktion zur Unterstützung offener Dateien mit VSS verwenden, fügt der Client dem Pfad des Objekts, das gerade verarbeitet wird, den Datenträgernamen der Momentaufnahme hinzu. Der Datenträgername der Momentaufnahme darf maximal 1024 Byte umfassen. Der vollständige Pfad (Datenträgername der Momentaufnahme plus Objektpfad) darf maximal 8192 Byte umfassen.

Informationen zu Einschränkungen und Problemen bei der Unterstützung offener Dateien erhalten Sie, wenn Sie nach *TSM Client Open File Support (OFS)* (TSM-Client: Unterstützung offener Dateien) auf der IBM® Support-Website suchen.

Zugehörige Konzepte:
Verarbeitungsoptionen
Zugehörige Tasks:
Unterstützung offener Dateien konfigurieren
Windows-Betriebssysteme

Daten über die grafische Benutzerschnittstelle archivieren

Aus einer Verzeichnisbaumstruktur können bestimmte Dateien oder vollständige Verzeichnisse archiviert werden. Für jede zu archivierende Dateigruppe (Archivierungspaket) kann außerdem eine eindeutige Beschreibung zugeordnet werden.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Dateien zu archivieren:

Vorgehensweise

1. Klicken Sie im GUI-Hauptfenster auf Archivieren. Das Fenster Archivieren wird angezeigt.

2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf ein Ordnersymbol in der Baumstruktur klicken. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol Suchen in der Funktionsleiste.
3. Geben Sie im Feld Beschreibung eine Beschreibung für das Archivierungspaket an, akzeptieren Sie die Standardbeschreibung oder wählen Sie eine vorhandene Beschreibung aus.
4. Um bestimmte Archivierungsoptionen zu ändern, klicken Sie auf Optionen. Die geänderten Optionen sind nur während der aktuellen Sitzung wirksam.
5. Klicken Sie auf Archivieren. Im Fenster Archivierungsstatus wird der Status der Archivierungsoperation angezeigt.

 Windows-Betriebssysteme

Beispiele für das Archivieren von Daten über die Befehlszeile

Sie können Daten archivieren, wenn Sie Kopien von Dateien für die spätere Verwendung, zu Dokumentationszwecken oder aufgrund gesetzlicher Anforderungen in ihrem aktuellen Status aufbewahren wollen.

Sie können eine einzelne Datei, eine Dateigruppe oder alle Dateien in einem Verzeichnis oder Unterverzeichnis archivieren. Nach dem Archivieren einer Datei können Sie die Originaldatei von Ihrer Workstation löschen. Dateien können mit dem Befehl archive archiviert werden.

Die folgende Tabelle enthält Beispiele zur Verwendung des Befehls archive zum Archivieren von Objekten.

Tabelle 1. Beispiele für Archivierungsbefehle

Task	Befehl	Hinweise
Alle Dateien im Verzeichnis `c:\plan\proj1` mit der Dateierweiterung `.txt` archivieren.	`dsmc archive c:\plan\proj1\*.txt`	Mithilfe von Platzhalterzeichen können mehrere Dateien gleichzeitig archiviert werden.
Alle Dateien im Verzeichnis `c:\small\testdir` archivieren und die Dateien auf Ihrer Workstation löschen.	`dsmc archive c:\small\testdir\* -deletefiles`	Werden die archivierten Dateien wieder auf der Workstation benötigt, können sie jederzeit abgerufen werden. Weitere Informationen zu der Option deletefiles finden Sie in Deletefiles.
Die Dateien `c:\proj1\h1.doc` und `c:\proj2\h2.doc` archivieren.	`dsmc archive c:\proj1\h1.doc c:\proj2\h2.doc`	Sie können so viele zu archivierende Dateien angeben wie die Ressourcen und Betriebssystembeschränkungen erlauben. Trennen Sie die zu archivierenden Dateien durch ein Leerzeichen. Weitere Informationen zu der Option filelist finden Sie in Filelist.
Eine Liste von Dateien in der Datei `c:\filelist.txt` archivieren.	`dsmc archive -filelist=c:\filelist.txt`	Verwenden Sie die Option filelist, um eine Liste von Dateien zu verarbeiten. Weitere Informationen zu der Option filelist finden Sie in Filelist.
Die Datei `a:\ch1.doc` archivieren und der Archivierung eine Beschreibung zuordnen.	`dsmc archive a:\ch1.doc -description="Kapitel 1, erste Version"`	Wenn Sie keine Beschreibung im Befehl archive angeben, lautet der Standardwert `Archivierungsdatum:`*x*, wobei *x* das aktuelle Systemdatum ist. Weitere Informationen zu der Option description finden Sie in Description.
Alle Dateien im Verzeichnis `d:\proj` und in dessen Unterverzeichnissen archivieren.	`dsmc archive d:\proj\ -subdir=yes`	Weitere Informationen zu der Option subdir finden Sie in Subdir.
Die Option v2archive im Befehl archive verwenden, um nur Dateien im Verzeichnis `c:\relx\dir1` zu archivieren.	`dsmc archive c:\relx\dir1\ -v2archive`	IBM Spectrum Protect archiviert nur Dateien im Verzeichnis `c:\relx\dir1`. Verzeichnisse in diesem Pfad werden nicht verarbeitet. Weitere Informationen zu der Option v2archive finden Sie in V2archive.
Verwenden Sie die Option archmc im Befehl archive, um die verfügbare Verwaltungsklasse für die Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Dateien binden wollen.	`dsmc archive -archmc=RET2YRS c:\plan \proj1\ budget.jan\*`	Weitere Informationen zu der Option archmc finden Sie in Archmc. Weitere Informationen zu Verwaltungsklassen siehe Speicherverwaltungsmaßnahmen.

Task	Befehl	Hinweise
Unter der Annahme, dass eine Momentaufnahme des Laufwerks `C:\` initiiert und die Momentaufnahme als logischer Datenträger `\\florence\c$\snapshots\snapshot.0` angehängt wurde, die Verzeichnisbaumstruktur `c:\dir1\sub1` von der lokalen Momentaufnahme archivieren und auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen `C:\` verwalten.	`dsmc archive c:\dir1\sub1\* -subdir=yes -snapshotroot=\\ florence\c$\snapshots\snapshot.0`	Weitere Informationen finden Sie in Snapshotroot.

- Windows-BetriebssystemeLokale Momentaufnahme einem Serverdateibereich zuordnen (Windows)
  Sie können die Daten in der lokalen Momentaufnahme den realen Dateibereichsdaten zuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

Zugehörige Verweise:
Archive
Windows-Betriebssysteme

Daten mit dem Clientknoten-Proxy archivieren

Archivierungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.

Informationen zu diesem Vorgang

Dies ist nützlich, wenn die für die Durchführung der Archivierung verantwortliche Workstation sich mit der Zeit ändern kann, wie es z. B. bei einem Cluster der Fall ist. Mit der Option asnodename können Daten außerdem von einem anderen System zurückgeschrieben werden als dem, auf dem die Sicherung ausgeführt wurde. Verwenden Sie die Option asnodename mit dem entsprechenden Befehl, um unter dem Zielknotennamen Daten auf dem IBM Spectrum Protect-Server zu sichern, zu archivieren, zurückzuschreiben oder abzurufen.

Tivoli Storage Manager FastBack-Clients werden ebenfalls mit einem Clientknoten-Proxy gesichert.

Um diese Option zu aktivieren, führen Sie folgende Schritte aus:

1. Installieren Sie den Client für Sichern/Archivieren auf allen Knoten in einer gemeinsamen Datenumgebung.
2. Registrieren Sie jeden Knoten beim IBM Spectrum Protect-Server, falls er nicht existiert. Registrieren Sie den einheitlichen Zielknotennamen, damit er von allen Agentenknoten in Ihrer gemeinsamen Datenumgebung gemeinsam genutzt werden kann.
3. Registrieren Sie jeden Knoten in der gemeinsamen Datenumgebung beim IBM Spectrum Protect-Server. Dies ist der Agentenknotenname, der für Authentifizierungszwecke verwendet wird. Daten werden nicht unter Verwendung des Knotennamens gespeichert, wenn die Option asnodename verwendet wird.
4. Der IBM Spectrum Protect-Administrator muss mithilfe des Serverbefehls GRANT PROXYNODE allen Knoten in der gemeinsam genutzten Umgebung Proxy-Berechtigung erteilen, damit sie auf den Zielknotennamen auf dem IBM Spectrum Protect-Server zugreifen können.
5. Verwenden Sie den Verwaltungsclientbefehl QUERY PROXYNODE, um die Clientknoten des berechtigten Benutzers anzuzeigen, denen mit dem Befehl GRANT PROXYNODE die Berechtigung erteilt wurde.

Führen Sie die folgenden Schritte aus, um mit der Option encryptkey=save die Verschlüsselung zu definieren:

Vorgehensweise

1. Geben Sie encryptkey=save in der Optionsdatei an.
2. Sichern Sie mindestens eine Datei mit asnode=ProxyNodeName, um auf jedem Agentenknoten in der Mehrfachknotenumgebung einen lokalen Verschlüsselungsschlüssel zu erstellen.

Ergebnisse

Führen Sie die folgenden Schritte aus, um mit der Option encryptkey=prompt die Verschlüsselung zu definieren:

1. Geben Sie encryptkey=prompt in der Optionsdatei an.
2. Stellen Sie sicher, dass die Benutzer der Agentenknoten in der Mehrfachknotenumgebung denselben Verschlüsselungsschlüssel verwenden.

- Wenn Sie den Verschlüsselungsschlüssel ändern, müssen Sie die vorherigen Schritte wiederholen.
- Verwenden Sie denselben Verschlüsselungsschlüssel für alle Dateien, die in der gemeinsam genutzten Knotenumgebung gesichert wurden.

Führen Sie die folgenden Schritte aus, um den Mehrfachknotenbetrieb von der GUI zu aktivieren:

1. Prüfen Sie, ob der Clientknoten Proxy-Berechtigung für einen Zielknoten hat (oder berechtigt ist, als Zielknoten zu handeln). Verwenden Sie dazu den Verwaltungsclientbefehl QUERY PROXYNODE.
2. Wählen Sie Editieren > Vorgaben aus, um das Vorgabenfenster zu öffnen.
3. Wählen Sie die Registerkarte Allgemein aus und füllen Sie das Feld Wie Knotenname mit dem Namen des für den Proxy berechtigten Zielknotens aus.
4. Klicken Sie auf Anwenden und anschließend auf OK, um das Fenster Vorgaben zu schließen.

Führen Sie die folgenden Schritte aus, um zu bestätigen, dass Ihr Clientknoten jetzt als Zielknoten auf den Server zugreift:

1. Öffnen Sie das Baumstrukturfenster und überprüfen Sie, ob der Zielknotenname, der im Feld Wie Knotenname angegeben ist, angezeigt wird, oder
2. Bestätigen Sie den Zielknotennamen im Feld Zugriff als Knoten im Fenster Verbindungsinformationen.

Um zur Operation mit Einzelknoten zurückzukehren, löschen Sie Wie Knotenname im Feld Zugriff als Knoten auf der Registerkarte Allgemein > Vorgaben.

Hinweise zu einer Sitzung mit Proxy-Berechtigung:

- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise maxnummp und deduplication) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.
- Alle Agentenknoten in der Mehrfachknotenumgebung müssen denselben Plattformtyp haben.
- Verwenden Sie Zielknoten nicht als traditionelle Knoten. Verwenden Sie sie nur für Mehrfachknotenverarbeitung.
- Sie können keine Sicherungen oder Zurückschreibungen von Systemobjekten oder dem Systemstatus ausführen.
- Sie können nicht auf einen anderen Knoten zugreifen (weder von der GUI-Dropdown-Liste noch mithilfe der Option fromnode).
- Sie können die Option clusternode nicht verwenden.
- Sie können keine NAS-Sicherung oder -Zurückschreibung durchführen.

Zugehörige Verweise:
Asnodename
Sitzungseinstellungen und Zeitpläne für eine Proxy-Operation
Windows-Betriebssysteme

Archivierungsdaten löschen

Sie können einzelne Archivierungsobjekte aus dem IBM Spectrum Protect-Server löschen, ohne den gesamten Dateibereich löschen zu müssen, zu dem die Objekte gehören.

Vorbereitende Schritte

Der IBM Spectrum Protect-Administrator muss Ihnen die Berechtigung zum Löschen archivierter Objekte erteilen. Um festzustellen, ob Sie diese Berechtigung haben, wählen Sie Datei > Verbindungsinformationen in der GUI des Clients für Sichern/Archivieren oder im Hauptmenü des Web-Clients aus. Ihr Berechtigungsstatus zum Löschen von Archivierungen wird im Feld `Archivierungsdateien löschen` angezeigt. Wird in diesem Feld `Nein` angezeigt, können Sie archivierte Objekte nur löschen, wenn Ihnen Ihr Administrator die entsprechende Berechtigung erteilt.

Vorgehensweise

Führen Sie die folgenden Schritte im Web-Client oder in der GUI aus, um ein archiviertes Objekt aus dem Server zu löschen. Als Alternative zum Web-Client bzw. zur GUI können Sie archivierte Objekte auch mit dem Befehl delete archive über die Befehlszeile löschen.

1. Wählen Sie Archivierungsdaten löschen im Menü Dienstprogramme aus.
2. Erweitern Sie im Fenster Archivierung löschen die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben einem Objekt klicken, das eingeblendet werden soll. Objekte in der Baumstruktur sind nach der Beschreibung der Archivierungspakete zusammengefasst.
3. Wählen Sie die archivierten Objekte aus, die gelöscht werden sollen.
4. Klicken Sie auf Löschen. Der Client fordert Sie zur Bestätigung auf, bevor die ausgewählten Objekte gelöscht werden. Im Fenster Task-Liste für das Löschen von Archivierungen wird der Löschstatus angezeigt.

Zugehörige Verweise:
Delete Archive
Windows-Betriebssysteme

Archivierungen abrufen

Mit der Funktion Abrufen kann eine Archivierungskopie einer Datei oder eines Verzeichnisses wiederhergestellt werden.

Anmerkung: Wird ein Verzeichnis abgerufen, werden das Änderungsdatum und die Änderungszeit des Verzeichnisses auf das Datum und die Uhrzeit des Abrufs gesetzt, nicht auf das Datum und die Uhrzeit des Verzeichnisses bei seiner Archivierung. Die Ursache dafür ist, dass zuerst die Verzeichnisse abgerufen und anschließend die Dateien zu den Verzeichnissen hinzugefügt werden.

Der Benutzer kann außerdem Archivierungskopien aus der Verzeichnisbaumstruktur abrufen, die Verzeichnisbaumstruktur filtern und Archivierungskopien von Dateien eines anderen Benutzers abrufen. Um eine dieser Aktionen auszuführen, klicken Sie im Hauptfenster der GUI des Clients für Sichern/Archivieren auf die Schaltfläche Abrufen und führen Sie die Anweisungen in der Taskhilfe der GUI aus.

Wichtig: Wenn Sie eine Datei ohne Spezifikationen abrufen und mehrere Versionen der Archivierungskopie auf dem Server vorhanden sind, werden alle Kopien abgerufen. Nachdem die erste Kopie abgerufen ist, wird die zweite Kopie abgerufen. Wenn es auf Ihrer Client-Workstation eine bestehende Kopie gibt, werden Sie zum Ersetzen, Überspringen oder Abbrechen aufgefordert.

- Windows-BetriebssystemeArchivierungen über die GUI abrufen
  Sie können archivierte Dateien über die GUI des Clients für Sichern/Archivieren abrufen.
- Windows-BetriebssystemeArchivierungskopien über die Befehlszeile abrufen
  Eine Datei wird abgerufen, wenn eine Archivierungskopie aus dem Server in die Workstation des Benutzers zurückgestellt werden soll. Dieser Abschnitt enthält einige Beispiele für das Abrufen archivierter Dateien über die Befehlszeile.

Zugehörige Konzepte:
Doppelte Dateinamen
Windows-Betriebssysteme

Archivierungen über die GUI abrufen

Sie können archivierte Dateien über die GUI des Clients für Sichern/Archivieren abrufen.

Vorgehensweise

1. Klicken Sie im Hauptfenster der grafischen Benutzerschnittstelle auf Abrufen. Das Fenster Abrufen wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben dem Objekt, das eingeblendet werden soll, klicken. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol Suchen in der Funktionsleiste.
3. Geben Sie die Suchkriterien in das Fenster Dateien suchen ein.
4. Klicken Sie auf Suchen. Das Fenster Übereinstimmende Dateien wird angezeigt.
5. Klicken Sie auf die Auswahlfelder der Dateien, die abgerufen werden sollen, und schließen Sie das Fenster Übereinstimmende Dateien.
6. Geben Sie die Filterkriterien in das Fenster Dateien suchen ein.
7. Klicken Sie auf Filter. Im Fenster Abrufen werden die gefilterten Dateien angezeigt.
8. Klicken Sie auf die Auswahlfelder der gefilterten Dateien oder Verzeichnissen, die abgerufen werden sollen.
9. Um bestimmte Abrufoptionen zu ändern, klicken Sie auf Optionen. Die geänderten Optionen sind nur während der aktuellen Sitzung wirksam.
10. Klicken Sie auf Abrufen. Das Fenster Abrufziel wird angezeigt. Sie können Dateien in ein anderes Verzeichnis oder Laufwerk abrufen, das von dem Verzeichnis bzw. Laufwerk abweicht, aus dem die Dateien ursprünglich archiviert wurden. Sie können auch den Umfang der übergeordneten Verzeichnisstruktur auswählen, die an der Abrufposition erneut erstellt wird.
11. Klicken Sie auf Abrufen. Im Fenster Abrufstatus wird der Verarbeitungsstatus angezeigt.

Windows-Betriebssysteme

Archivierungskopien über die Befehlszeile abrufen

Eine Datei wird abgerufen, wenn eine Archivierungskopie aus dem Server in die Workstation des Benutzers zurückgestellt werden soll. Dieser Abschnitt enthält einige Beispiele für das Abrufen archivierter Dateien über die Befehlszeile.

Sie können eine einzelne Datei, eine Dateigruppe oder alle Dateien in einem Verzeichnis oder Unterverzeichnis abrufen. Wenn Sie eine Datei abrufen, sendet der IBM Spectrum Protect-Server eine Kopie dieser Datei an Sie. Die archivierte Datei verbleibt im Speicher.

Mit dem Befehl retrieve können Dateien abgerufen werden. Die folgende Tabelle enthält Beispiele zur Verwendung des Befehls retrieve.

Tabelle 1. Beispiele für Befehle zum Abrufen archivierter Dateien

Task	Befehl	Hinweise
Die Datei c:\doc\h2.doc in ihr Ursprungsverzeichnis abrufen.	`dsmc retrieve c:\doc\h2.doc`	Wird kein Ziel angegeben, werden die Dateien an ihre ursprüngliche Position abgerufen.
Die Datei c:\doc\h2.doc unter einem neuen Namen und in ein neues Verzeichnis abrufen.	`dsmc retrieve c:\doc\h2.doc c:\proj2\h3.doc`	Keine
Alle Dateien, die mit einer bestimmten Beschreibung archiviert wurden, in das Verzeichnis retr1 an einer neuen Position abrufen.	`dsmc retrieve c:\* d:\retr1\ -sub=yes -desc="My first archive"`	Keine

Task	Befehl	Hinweise
Alle Dateien im Verzeichnis c:\projecta, die mit den Zeichen .bak enden, in das Verzeichnis c:\projectn abrufen.	`dsmc retrieve c:\projecta\*.bak c:\projectn`	Keine
Die Option pick verwenden, um eine Liste von Archivierungen anzuzeigen, aus denen Sie Dateien zum Abrufen auswählen können.	`dsmc retrieve c:\project\* -pick`	Weitere Informationen zu der Option pick finden Sie in Pick.
Eine Datei, die ursprünglich von der Diskette *workathome* in Laufwerk a: archiviert wurde, auf die Diskette *extra* in Laufwerk a: abrufen.	`dsmc retrieve {workathome}\doc\h2.doc a:\doc\h2.doc`	Wird eine Datei auf eine Platte abgerufen, die eine andere Bezeichnung hat, als die Platte, von der die Datei archiviert wurde, muss der Dateibereichsname (Bezeichnung) der Archivierungsplatte anstelle des Laufwerkbuchstabens verwendet werden.
Die Datei c:\doc\h2.doc in ihr Ursprungsverzeichnis auf der Workstation mit dem Namen *star* abrufen.	`dsmc retrieve c:\doc\h2.doc \\star\c$\` Um die Datei auf die Workstation *star* abzurufen, die in *meteor* umbenannt wurde, Folgendes eingeben: `dsmc retrieve \\star\c$\doc\h2.doc \\meteor\c$\` Folgende Eingabe ist auch möglich: `dsmc retrieve \\star\c$\doc\h2.doc c:\` Dieses Beispiel ist gültig, weil die lokale Workstation angenommen wird (in diesem Fall *meteor*), wenn kein Workstationname im Befehl angegeben wird.	In diesem Handbuch ist die Workstation Teil des Dateinamens. Daher muss ein Ziel angegeben werden, wenn Dateien auf einer Workstation archiviert werden und auf einer anderen Workstation abgerufen werden sollen. Diese Anforderung gilt auch, wenn auf derselben physischen Workstation abgerufen wird, die Workstation jedoch einen neuen Namen hat.

Zugehörige Verweise:
Retrieve
AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme

Daten archivieren und abrufen (UNIX und Linux)

Sie können selten verwendete Dateien auf dem IBM Spectrum Protect-Server archivieren und bei Bedarf abrufen. Das Archivieren und Abrufen von Dateien ist dem Sichern und Zurückschreiben von Dateien ähnlich. Viele Fenster und Konzepte sind ähnlich.

Mit Ausnahme der Prozeduren für den Profileditor gelten alle primären Archivierungs- und Abrufprozeduren in diesem Abschnitt auch für den Web-Client.

Sie können die folgenden primären Archivierungs- und Abruftasks ausführen:

- Daten über die grafische Benutzerschnittstelle archivieren
- Beispiele für das Archivieren von Daten über die Befehlszeile
- Archivierungsdaten löschen
- Daten über die grafische Benutzerschnittstelle abrufen
- Beispiele für das Abrufen von Daten über die Befehlszeile

- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDateien archivieren
  Sollen Dateien archiviert werden, müssen diese explizit zum Archivieren ausgewählt werden. Der Benutzer kann die Dateien auswählen, indem er eine Dateispezifikation verwendet oder indem er die Dateien aus einer Verzeichnisbaumstruktur auswählt.
- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeArchivierungen abrufen
  Eine Datei wird abgerufen, wenn eine Archivierungskopie aus dem Server auf Ihre Workstation zurückgestellt werden soll.

Zugehörige Konzepte:
Daten sichern
Zugehörige Tasks:

Web-Client-Sitzung starten
 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Dateien archivieren

Sollen Dateien archiviert werden, müssen diese explizit zum Archivieren ausgewählt werden. Der Benutzer kann die Dateien auswählen, indem er eine Dateispezifikation verwendet oder indem er die Dateien aus einer Verzeichnisbaumstruktur auswählt.

Der Administrator kann Zeitpläne zur automatischen Archivierung bestimmter Dateien auf der Workstation definieren. In den folgenden Abschnitten ist beschrieben, wie Dateien ohne Zeitpläne archiviert werden.

-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDaten über die grafische Benutzerschnittstelle archivieren
  Dateien oder Dateigruppen können unter Verwendung von Dateinamen archiviert werden. Sie können Dateien, die bestimmten Suchkriterien entsprechen, mithilfe einer Verzeichnisstruktur auswählen.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeBeispiele für das Archivieren von Daten über die Befehlszeile
  Archivierungsservices werden angefordert, um Kopien von Dateien für die spätere Verwendung, zu Dokumentationszwecken oder aufgrund gesetzlicher Anforderungen in ihrem aktuellen Status aufzubewahren. Dieser Abschnitt enthält einige Beispiele für das Archivieren von Daten über die Befehlszeile.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDaten mit dem Clientknoten-Proxy archivieren
  Archivierungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeArchivierungsdaten löschen
  Sie können einzelne Archivierungsobjekte aus dem IBM Spectrum Protect-Server löschen, ohne den gesamten Dateibereich löschen zu müssen, zu dem die Objekte gehören.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeErweiterte Archivierungstasks
  Zugriffsberechtigungen, symbolische Verbindungen und feste Verbindungen sind erweiterte Funktionen, die beim Archivieren von Daten zu berücksichtigen sind.

Zugehörige Tasks:
Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Daten über die grafische Benutzerschnittstelle archivieren

Dateien oder Dateigruppen können unter Verwendung von Dateinamen archiviert werden. Sie können Dateien, die bestimmten Suchkriterien entsprechen, mithilfe einer Verzeichnisstruktur auswählen.

Vorgehensweise

Archivieren Sie Dateien mit der folgenden Prozedur.

1. Klicken Sie auf Archivieren im Hauptfenster.
2. Erweitern Sie im Fenster Archivieren die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben einem Objekt in der Baumstruktur klicken. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol Suchen in der Funktionsleiste.
3. Geben Sie die Suchkriterien in das Fenster Dateien suchen ein.
4. Klicken Sie auf Suchen.
5. Klicken Sie im Fenster Übereinstimmende Dateien auf die Auswahlfelder neben den Dateien, die archiviert werden sollen, und schließen Sie das Fenster Übereinstimmende Dateien.
6. Geben Sie die Filterkriterien in das Fenster Dateien suchen ein.
7. Klicken Sie auf Filter. Im Fenster Archivieren werden die gefilterten Dateien angezeigt.
8. Klicken Sie auf die Auswahlfelder neben den gefilterten Dateien oder Verzeichnissen, die archiviert werden sollen.
9. Geben Sie im Feld Beschreibung eine Beschreibung für das Archivierungspaket an, akzeptieren Sie die Standardbeschreibung oder wählen Sie eine vorhandene Beschreibung aus. Die maximale Länge einer Beschreibung ist 254 Zeichen. Wird eine vorhandene Archivierungsbeschreibung verwendet, werden die ausgewählten Dateien oder Verzeichnisse dem Archivierungspaket hinzugefügt. Alle Archivierungspakete mit derselben Beschreibung werden zum Abrufen, Abfragen und Löschen zusammengefasst.
10. Um bestimmte Archivierungsoptionen zu ändern, klicken Sie auf Optionen. Die geänderten Optionen sind nur während der aktuellen Sitzung wirksam.
11. Klicken Sie auf Archivieren. Im Fenster Task-Liste für die Archivierung wird der Verarbeitungsstatus der Archivierung angezeigt.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Beispiele für das Archivieren von Daten über die Befehlszeile

Archivierungsservices werden angefordert, um Kopien von Dateien für die spätere Verwendung, zu Dokumentationszwecken oder aufgrund gesetzlicher Anforderungen in ihrem aktuellen Status aufzubewahren. Dieser Abschnitt enthält einige Beispiele für das Archivieren von Daten über die Befehlszeile.

Sie können eine einzelne Datei, eine Dateigruppe oder alle Dateien in einem Verzeichnis oder Unterverzeichnis archivieren. Nach dem Archivieren einer Datei können Sie die Originaldatei von Ihrer Workstation löschen.

Die folgende Tabelle enthält Beispiele zur Verwendung des Befehls archive zum Archivieren von Objekten.

Tabelle 1. Beispiele für Archivierungsbefehle

Task	**Befehl**	**Hinweise**
Alle Dateien im Verzeichnis `/home/proj1` mit der Dateierweiterung `.txt` archivieren.	`dsmc archive "/home/proj1/*.txt"`	Mithilfe von Platzhalterzeichen können mehrere Dateien gleichzeitig archiviert werden.
Alle Dateien im Verzeichnis `/home/jones/proj/` archivieren und die Dateien auf Ihrer Workstation löschen.	`dsmc archive /home/jones/proj/ -deletefiles`	Werden die archivierten Dateien wieder auf der Workstation benötigt, können sie jederzeit abgerufen werden. Weitere Informationen zu der Option deletefiles finden Sie in Deletefiles.
Die Dateien `/home/jones/h1.doc` und `/home/jones/test.doc` archivieren.	`dsmc archive /home/jones/h1.doc /home/jones/test.doc`	Geben Sie die Option removeoperandlimit mit dem Befehl archive an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Mit dieser Option können Sie mehr als 20 Dateien in einem einzelnen Befehl angeben. Weitere Informationen zu dieser Option finden Sie in Removeoperandlimit.
Eine Liste von Dateien in der Datei `/home/avi/filelist.txt` archivieren.	`dsmc archive -filelist=/home/avi/filelist.txt`	Verwenden Sie die Option filelist, um eine Liste von Dateien zu verarbeiten. Weitere Informationen finden Sie in Filelist.
Die Datei `/home/jones/ch1.doc` archivieren und der Archivierungskopie eine Beschreibung zuordnen.	`dsmc archive /home/jones/ch1.doc -description="Kapitel 1, erste Version"`	Wenn Sie keine Beschreibung im Befehl archive angeben, lautet der Standardwert `Archivierungsdatum:x`; hierbei gibt `x` das aktuelle Systemdatum an. Weitere Informationen zu der Option description finden Sie in Description.
Alle Dateien im Verzeichnis `/home/jones/proj/` und seinen Unterverzeichnissen archivieren.	`dsmc archive /home/jones/proj/ -subdir=yes`	Weitere Informationen zu der Option subdir finden Sie in Subdir.
Die Option v2archive im Befehl archive verwenden, um nur Dateien im Verzeichnis `/home/relx/dir1` zu archivieren, aber nicht die Verzeichnisse `relx` oder `dir1`.	`dsmc archive "/home/relx/dir1/" -v2archive`	Der Client für Sichern/Archivieren archiviert nur Dateien im Verzeichnis `/home/relx/dir1`. Verzeichnisse in diesem Pfad werden nicht verarbeitet. Weitere Informationen zu der Option v2archive finden Sie in V2archive.
Verwenden Sie die Option archmc im Befehl archive, um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Dateien binden wollen.	`dsmc archive -archmc=ret2yrs /home/plan/proj1/budget.jan`	Weitere Informationen zu der Option archmc finden Sie in Archmc. Weitere Informationen zu Verwaltungsklassen siehe Speicherverwaltungsmaßnahmen.
Unter der Annahme, dass Sie eine Momentaufnahme des Dateisystems `/usr` initiiert und die Momentaufnahme als `/snapshot/day1` angehängt haben, archivieren Sie die Verzeichnisbaumstruktur `/usr/dir1/sub1` aus der lokalen Momentaufnahme und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen `/usr`.	`dsmc archive /usr/dir1/sub1/ -subdir=yes -snapshotroot=/snapshot/day1`	Der Client betrachtet den Wert für snapshotroot als Dateibereichsnamen. Weitere Informationen finden Sie in Snapshotroot.

- Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeLokale Momentaufnahme einem Serverdateibereich zuordnen
  Um Daten in der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind, verwenden Sie die Option snapshotroot.

Zugehörige Verweise:
Archive

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Daten mit dem Clientknoten-Proxy archivieren

Archivierungen mehrerer Knoten, die Speicher gemeinsam benutzen, können zu einem einheitlichen Zielknotennamen auf dem IBM Spectrum Protect-Server konsolidiert werden.

Vorbereitende Schritte

Alle Agentenknoten in der Mehrfachknotenumgebung sollten denselben Plattformtyp aufweisen. Verwenden Sie Zielknoten nicht als traditionelle Knoten. Verwenden Sie sie nur für Mehrfachknotenverarbeitung.

Beachten Sie die folgenden Features einer Sitzung mit Proxy-Berechtigung:

- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise maxnummp und deduplication) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.
- Sie können keine Sicherungen oder Zurückschreibungen von Systemstatus oder Systemservices ausführen.
- Sie können nicht auf einen anderen Knoten zugreifen (weder von der GUI-Dropdown-Liste noch mithilfe der Option fromnode).
- Sie können keine NAS-Sicherung oder -Zurückschreibung ausführen.

Informationen zu diesem Vorgang

Die Konsolidierung archivierter Dateien zu einem einheitlichen Zielknotennamen auf dem Server ist nützlich, wenn die für die Durchführung der Archivierung verantwortliche Workstation sich mit der Zeit ändern kann, wie es z. B. bei einem Xsan oder Cluster der Fall ist. Mit der Option asnodename können Daten außerdem von einem anderen System zurückgeschrieben werden als dem, auf dem die Sicherung ausgeführt wurde. Verwenden Sie die Option asnodename mit dem entsprechenden Befehl, um unter dem Zielknotennamen Daten auf dem IBM Spectrum Protect-Server zu sichern, zu archivieren, zurückzuschreiben oder abzurufen. Diese Unterstützung ist nur mit IBM Spectrum Protect Version 5.3 und höher verfügbar.

Linux-BetriebssystemeTivoli Storage Manager FastBack-Clients werden ebenfalls mit einem Clientknoten-Proxy gesichert.

Die Konfiguration Ihrer Umgebung für Proxy-Operationen besteht aus mehreren Schritten, zu denen das Definieren von Optionen und Befehlen auf dem Client für Sichern/Archivieren und auf dem Server gehören.

Vorgehensweise

Führen Sie die Schritte 1 bis 5 aus, um den Client zu installieren und den Knoten, die Archivierungsprozeduren im Namen eines anderen Knotens ausführen können, Proxy-Berechtigung zu erteilen.

1. Installieren Sie den Client für Sichern/Archivieren auf allen Knoten in einer gemeinsamen Datenumgebung.
2. Registrieren Sie jeden Knoten beim IBM Spectrum Protect-Server, falls er nicht existiert. Registrieren Sie den einheitlichen Zielknotennamen, damit er von allen Agentenknoten in Ihrer gemeinsamen Datenumgebung gemeinsam genutzt werden kann.
3. Registrieren Sie jeden Knoten in der gemeinsamen Datenumgebung beim IBM Spectrum Protect-Server. Dies ist der Agentenknotenname, der für Authentifizierungszwecke verwendet wird. Daten werden nicht unter Verwendung des Knotennamens gespeichert, wenn die Option asnodename verwendet wird.
4. Erteilen Sie mithilfe des Befehls GRANT PROXYNODE allen Knoten in der gemeinsam genutzten Umgebung Proxy-Berechtigung, damit sie auf den Zielknotennamen auf dem IBM Spectrum Protect-Server zugreifen können (IBM Spectrum Protect-Administrator).
5. Verwenden Sie den Verwaltungsclientbefehl QUERY PROXYNODE, um die Clientknoten des berechtigten Benutzers anzuzeigen, denen mit dem Befehl GRANT PROXYNODE die Berechtigung erteilt wurde.

Der Schritt 6 stellt sicher, dass archivierte Dateien auf dem Server verschlüsselt werden.

6. Definieren Sie die Option encryptkey in der Optionsdatei.

   Geben Sie encryptkey=save in der Optionsdatei an, um den Verschlüsselungsschlüssel in der IBM Spectrum Protect-Kennwortdatei zu speichern. Sichern Sie mindestens eine Datei mit asnode=ProxyNodeName, um auf jedem Agentenknoten in der Mehrfachknotenumgebung einen lokalen Verschlüsselungsschlüssel zu erstellen.

   Geben Sie encryptkey=prompt in der Optionsdatei an, wenn die Knotenbenutzer den Verschlüsselungsschlüssel verwalten sollen. Stellen Sie sicher, dass die Benutzer der Agentenknoten in der Mehrfachknotenumgebung denselben Verschlüsselungsschlüssel verwenden.

   Wiederholen Sie diesen Schritt, wenn Sie den Verschlüsselungsschlüssel ändern. Verwenden Sie in der gemeinsam genutzten Umgebung denselben Verschlüsselungsschlüssel für alle Dateien, die gesichert werden.

Führen Sie die Schritte 7 bis 10 aus, um den Mehrfachknotenbetrieb von der grafischen Benutzerschnittstelle (GUI) aus zu aktivieren.

7. Prüfen Sie, ob der Clientknoten Proxy-Berechtigung für einen Zielknoten hat (oder berechtigt ist, als Zielknoten zu handeln). Verwenden Sie dazu den Verwaltungsclientbefehl QUERY PROXYNODE.
8. Wählen Sie Editieren > Vorgaben aus, um das Vorgabenfenster zu öffnen.

9. Wählen Sie die Registerkarte Allgemein aus und füllen Sie das Feld Wie Knotenname mit dem Namen des für den Proxy berechtigten Zielknotens aus.
10. Klicken Sie auf Anwenden und anschließend auf OK, um das Fenster Vorgaben zu schließen.

Führen Sie Schritt 11 aus, um zu bestätigen, dass Ihr Clientknoten jetzt als Zielknoten auf den Server zugreift.

11. Öffnen Sie das Baumstrukturfenster und bestätigen Sie, dass der Zielknotenname, der im Feld Wie Knotenname angegeben ist, angezeigt wird. Sie können auch überprüfen, ob der Zielknotenname im Feld Zugriff als Knoten im Fenster Verbindungsinformationen angezeigt wird.
12. Optional: Um zur Operation mit Einzelknoten zurückzukehren, löschen Sie Wie Knotenname im Feld Zugriff als Knoten auf der Registerkarte Allgemein > Vorgaben.

Zugehörige Verweise:
Asnodename
Sitzungseinstellungen und Zeitpläne für eine Proxy-Operation
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Archivierungsdaten löschen

Sie können einzelne Archivierungsobjekte aus dem IBM Spectrum Protect-Server löschen, ohne den gesamten Dateibereich löschen zu müssen, zu dem die Objekte gehören.

Vorbereitende Schritte

Der IBM Spectrum Protect-Administrator muss Ihnen die Berechtigung zum Löschen archivierter Objekte erteilen. Um festzustellen, ob Sie diese Berechtigung haben, wählen Sie Datei > Verbindungsinformationen in der GUI des Clients für Sichern/Archivieren oder im Hauptmenü des Web-Clients aus. Ihr Berechtigungsstatus zum Löschen von Archivierungen wird im Feld `Archivierungsdateien löschen` angezeigt. Wird in diesem Feld `Nein` angezeigt, können Sie archivierte Objekte nur löschen, wenn Ihnen Ihr Administrator die entsprechende Berechtigung erteilt.

Vorgehensweise

Führen Sie die folgenden Schritte im Web-Client oder in der GUI aus, um ein archiviertes Objekt aus dem Server zu löschen. Als Alternative zum Web-Client bzw. zur GUI können Sie archivierte Objekte auch mit dem Befehl delete archive über die Befehlszeile löschen.

1. Wählen Sie Archivierungsdaten löschen im Menü Dienstprogramme aus.
2. Erweitern Sie im Fenster Archivierung löschen die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben einem Objekt klicken, das eingeblendet werden soll. Objekte in der Baumstruktur sind nach der Beschreibung der Archivierungspakete zusammengefasst.
3. Wählen Sie die archivierten Objekte aus, die gelöscht werden sollen.
4. Klicken Sie auf Löschen. Der Client fordert Sie zur Bestätigung auf, bevor die ausgewählten Objekte gelöscht werden. Im Fenster Task-Liste für das Löschen von Archivierungen wird der Löschstatus angezeigt.

Zugehörige Verweise:
Delete Archive
 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Erweiterte Archivierungstasks

Zugriffsberechtigungen, symbolische Verbindungen und feste Verbindungen sind erweiterte Funktionen, die beim Archivieren von Daten zu berücksichtigen sind.

-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeZugriffsberechtigungen
  Bei der Archivierung einer Datei sichert der Client die der Datei zugeordneten UNIX-Standardzugriffsberechtigungen.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeSymbolische Verbindungen archivieren und abrufen
  Der Client für Sichern/Archivieren verfährt beim Archivieren und Abrufen symbolischer Verbindungen anders als bei regulären Dateien und Verzeichnissen.
-  Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeFeste Verbindungen
  Wenn Sie Dateien archivieren, die fest verbunden sind, archiviert der Client für Sichern/Archivieren jede Instanz der verbundenen Datei.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Zugriffsberechtigungen

Bei der Archivierung einer Datei sichert der Client die der Datei zugeordneten UNIX-Standardzugriffsberechtigungen.

Abhängig vom Betriebssystem werden auch erweiterte Berechtigungen gesichert. Beispielsweise sichert der Client Zugriffssteuerungslisten für Dateien auf einer AIX-Workstation.

Archiviert ein Benutzer eine Datei, für die Lesezugriff besteht, ist der Benutzer der Eigner der archivierten Kopie der Datei. Nur dieser Benutzer kann die archivierte Datei abrufen, es sei denn, einem anderen Benutzer wird der Zugriff auf diese Datei erteilt.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Symbolische Verbindungen archivieren und abrufen

Der Client für Sichern/Archivieren verfährt beim Archivieren und Abrufen symbolischer Verbindungen anders als bei regulären Dateien und Verzeichnissen.

Wie der Client symbolische Verbindungen archiviert und abruft, ist von Optionseinstellungen, von der Verfügbarkeit des Zielverzeichnisses und von der Angabe der Objekte abhängig.

Eine *symbolische Verbindung ist unter UNIX* eine Datei, die einen Zeiger auf eine andere Datei oder ein anderes Verzeichnis enthält. Das Objekt, auf das die symbolische Verbindung zeigt, wird als *Zielobjekt* bezeichnet.

Eine symbolische Verbindung kann entweder als Pfadangabe für das Zielverzeichnis oder als Verzeichnis gesichert werden. Wird die symbolische Verbindung als Verzeichnis gesichert, können auch die Dateien und Ordner im Zielverzeichnis gesichert werden.

Welche Objekte zurückgeschrieben werden, ist von der Art der Sicherung der symbolischen Verbindung, vom Umfang der Zurückschreibung, von der Einstellung der Option followsymbolic und von der Verfügbarkeit des Zielverzeichnisses zum Zeitpunkt der Zurückschreibung abhängig.

Weitere Informationen über die Verarbeitung symbolischer Verbindungen bei der Archivierung enthält die Beschreibung der Option archsymlinkasfile.

Anmerkung: Die hier beschriebene Verarbeitung symbolischer Verbindungen gilt nicht für Mac OS X. Symbolische Verbindungen werden immer als Dateien archiviert und den Zeigern wird nicht gefolgt.

Die folgende Tabelle zeigt Archivierungs- und Abruffunktionen für symbolische Verbindungen und die jeweiligen Aktionen:

Tabelle 1. Verwaltung symbolischer Verbindungen für Archivieren und Abrufen

Funktion	**Aktion**
Archivierung einer Dateiverbindung.	Archiviert die Datei, auf die die symbolische Verbindung zeigt.
Archivierung einer Verzeichnisverbindung.	Archiviert das Verzeichnis und seinen Inhalt.
Archivierung einer Datei mit subdir=yes.	Archiviert die Datei, den Verzeichnispfad und alle Dateien gleichen Namens in der Unterverzeichnisstruktur.
Archivierung eines Verzeichnisses mit subdir=yes.	Archiviert das Verzeichnis, seinen Inhalt und den Inhalt der Unterverzeichnisse.
Archivierung einer symbolischen Verbindung, die auf eine Datei oder ein Verzeichnis zeigt, die bzw. das nicht vorhanden ist.	Archiviert die symbolische Verbindung.
Abrufen einer symbolischen Verbindung, die auf eine Datei zeigt; Datei und Verbindung sind vorhanden.	Die Datei wird ersetzt, wenn replace=y definiert wird.
Abrufen einer symbolischen Verbindung, die auf eine Datei zeigt; die symbolische Verbindung ist nicht mehr vorhanden.	Ruft die Datei in das Verzeichnis ab, in dem sich die symbolische Verbindung befindet, wobei der Dateiname durch den Namen der symbolischen Verbindung ersetzt wird.
Abrufen einer symbolischen Verbindung, die auf ein Verzeichnis zeigt; die symbolische Verbindung und das Verzeichnis sind nicht mehr vorhanden.	In dem Verzeichnis, in dem sich die symbolische Verbindung befindet, wird ein Verzeichnis erstellt, und alle Dateien und Unterverzeichnisse werden in dieses Verzeichnis zurückgeschrieben. Der Name der symbolischen Verbindung wird als Name des neuen Verzeichnisses verwendet.
Abrufen einer symbolischen Verbindung, die auf ein Verzeichnis zeigt; die symbolische Verbindung und das Verzeichnis sind vorhanden.	Das Verzeichnis wird nicht abgerufen, solange die symbolische Verbindung vorhanden ist.

Zugehörige Verweise:
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeArchsymlinkasfile
 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Feste Verbindungen

Wenn Sie Dateien archivieren, die fest verbunden sind, archiviert der Client für Sichern/Archivieren jede Instanz der verbundenen Datei.

Wenn Sie beispielsweise zwei Dateien, die fest verbunden sind, archivieren, archiviert der Client die Dateidaten zweimal.

Wenn Sie fest verbundene Dateien abrufen, stellt der Client die Verbindungen wieder her. Hatten Sie beispielsweise ein Dateipaar mit fester Verbindung und ist nur eine der fest verbundenen Dateien auf Ihrer Workstation, werden beide Dateien beim Abrufen fest verbunden. Bei diesem Verfahren gibt es eine einzige Ausnahme, und zwar, wenn Sie zwei fest verbundene Dateien archivieren und dann die Verbindung zwischen diesen

Dateien auf Ihrer Workstation unterbrechen. Wenn Sie die beiden Dateien vom Server abrufen, respektiert der Client das aktuelle Dateisystem und ruft die feste Verbindung nicht ab.

Tipp: Werden nicht alle fest verbundenen Dateien gleichzeitig archiviert oder abgerufen, können Probleme auftreten. Um sicherzustellen, dass fest verbundene Dateien synchronisiert bleiben, führen Sie die Archivierung und den Abruf fest verbundener Dateien immer gleichzeitig durch.
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Archivierungen abrufen

Eine Datei wird abgerufen, wenn eine Archivierungskopie aus dem Server auf Ihre Workstation zurückgestellt werden soll.

Viele der weiterführenden Überlegungen zum Abrufen von Dateien sind mit den Überlegungen zum Zurückschreiben von Dateien identisch.

Wichtig: Wenn Sie eine Datei ohne Spezifikationen abrufen und mehrere Versionen der Archivierungskopie auf dem Server vorhanden sind, ruft der Client alle Kopien ab. Nachdem die erste Kopie abgerufen ist, wird die zweite Kopie abgerufen. Wenn es auf Ihrer Client-Workstation eine bestehende Kopie gibt, werden Sie zum Ersetzen, Überspringen oder Abbrechen aufgefordert.

- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDaten über die grafische Benutzerschnittstelle abrufen
  Sie können eine archivierte Datei über die grafische Benutzerschnittstelle (GUI) abrufen.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeBeispiele für das Abrufen von Daten über die Befehlszeile
  Sie können eine einzelne Datei, eine Dateigruppe oder alle Dateien in einem Verzeichnis oder Unterverzeichnis abrufen.
- Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeVerwaltungsklassen für die Archivierung
  Der Client für Sichern/Archivieren überprüft die Optionen include in Ihrer Liste der Einschluss-/Ausschlussoptionen um zu bestimmen, welche Verwaltungsklasse Ihren archivierten Dateien zugeordnet werden soll.

Zugehörige Konzepte:
Dateien auf eine andere Workstation zurückschreiben oder abrufen
Zugehörige Tasks:
Einen anderen Benutzer zum Zurückschreiben und Abrufen Ihrer Dateien berechtigen
Dateien von einem anderen Clientknoten zurückschreiben oder abrufen
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Daten über die grafische Benutzerschnittstelle abrufen

Sie können eine archivierte Datei über die grafische Benutzerschnittstelle (GUI) abrufen.

Vorgehensweise

1. Klicken Sie auf Abrufen im Hauptfenster der Client-Java™-GUI. Das Fenster Abrufen wird angezeigt.
2. Erweitern Sie die Verzeichnisbaumstruktur, indem Sie auf das Pluszeichen (+) oder auf das Ordnersymbol neben dem Objekt, das eingeblendet werden soll, klicken. Zum Suchen oder Filtern von Dateien klicken Sie auf das Symbol Suchen in der Funktionsleiste.
3. Geben Sie die Suchkriterien in das Fenster Dateien suchen ein.
4. Klicken Sie auf Suchen. Das Fenster Übereinstimmende Dateien wird angezeigt.
5. Klicken Sie auf die Auswahlfelder neben den Dateien, die abgerufen werden sollen, und schließen Sie das Fenster Übereinstimmende Dateien.
6. Geben Sie die Filterkriterien in das Fenster Dateien suchen ein.
7. Klicken Sie auf Filter. Im Fenster Abrufen werden die gefilterten Dateien angezeigt.
8. Klicken Sie auf die Auswahlfelder der gefilterten Dateien oder Verzeichnissen, die abgerufen werden sollen.
9. Um bestimmte Abrufoptionen zu ändern, klicken Sie auf Optionen. Die geänderten Optionen sind nur während der aktuellen Sitzung wirksam.
10. Klicken Sie auf Abrufen. Das Fenster Abrufziel wird angezeigt. Geben Sie die entsprechenden Informationen in das Fenster Abrufziel ein.
11. Klicken Sie auf Abrufen. Im Fenster Task-Liste wird der Verarbeitungsstatus des Abrufs angezeigt.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Beispiele für das Abrufen von Daten über die Befehlszeile

Sie können eine einzelne Datei, eine Dateigruppe oder alle Dateien in einem Verzeichnis oder Unterverzeichnis abrufen.

Wenn Sie eine Datei abrufen, sendet der IBM Spectrum Protect-Server eine Kopie dieser Datei. Die archivierte Datei verbleibt im Speicher.

Verwenden Sie den Befehl retrieve, um Dateien aus dem Speicher abzurufen und auf Ihrer Workstation zu speichern. Die folgende Tabelle enthält Beispiele zur Verwendung des Befehls retrieve.

Tabelle 1. Beispiele für Befehle zum Abrufen archivierter Dateien

Task	Befehl	Hinweise
Die Datei `/home/jones/h1.doc` in ihr Ursprungsverzeichnis abrufen.	`dsmc retrieve /home/jones/h1.doc`	Wird kein Ziel angegeben, werden die Dateien an ihre ursprüngliche Position abgerufen.
Die Datei `/home/jones/h1.doc` mit einem neuen Namen und in ein anderes Verzeichnis abrufen.	`dsmc retrieve /home/jones/h1.doc /home/smith/h2.doc`	Keine.
Alle Dateien im Verzeichnis `/home/jones`, die mit den Zeichen `.bak` enden, in das Verzeichnis `/home/smith` abrufen.	`dsmc retrieve "/home/jones/*.bak" /home/smith/`	Keine.
Die Datei `/home/jones/ch1.doc` abrufen und eine Beschreibung zuordnen.	`dsmc retrieve /home/jones/ch1.doc -description="Kapitel 1, erste Version"`	Wenn Sie keine Beschreibung im Befehl retrieve angeben, lautet der Standardwert `Abrufdatum:x`; hierbei gibt `x` das aktuelle Systemdatum an.
Die Option pick verwenden, um eine Liste von Archivierungskopien anzuzeigen, aus denen Sie Dateien zum Abrufen auswählen können.	`dsmc retrieve "/home/jones/*" -pick`	Keine.
Eine Liste von Dateien, die in der Datei retrievelist.txt angegeben ist, in ihr Ursprungsverzeichnis abrufen.	`dsmc retrieve -filelist=/home/dir2/retrievelist.txt`	Keine.

Zugehörige Verweise:
Retrieve
Description
Filelist
Pick
Mac OS X-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Verwaltungsklassen für die Archivierung

Der Client für Sichern/Archivieren überprüft die Optionen include in Ihrer Liste der Einschluss-/Ausschlussoptionen um zu bestimmen, welche Verwaltungsklasse Ihren archivierten Dateien zugeordnet werden soll.

Wenn Sie einer Datei nicht mit der Option include eine Verwaltungsklasse zuordnen, ordnet der Client der Datei die Standardverwaltungsklasse zu. Der Client kann eine Datei nur dann archivieren, wenn die ausgewählte Verwaltungsklasse eine Archivierungskopiengruppe enthält.

Sie können die Standardverwaltungsklasse mithilfe der Option archmc überschreiben oder indem Sie in der grafischen Benutzerschnittstelle auf Optionen im Fenster Archivieren und dann auf Einschluss-/Ausschlussliste überschreiben klicken und die Verwaltungsklasse auswählen.

Sie können Einschluss-/Ausschlussanweisungen auch in der Verzeichnisstruktur der Java™-GUI des Clients für Sichern/Archivieren oder des Web-Clients hinzufügen. Anschließend können Sie mithilfe der Funktion Dienstprogramme - Voranzeige für Einschluss/Ausschluss die Voranzeige der Einschluss-/Ausschlussliste aufrufen, bevor Sie Daten an den Server senden.

Zugehörige Konzepte:
Dateien eine Verwaltungsklasse zuordnen
Informationen zu Verwaltungsklassen und Kopiengruppen anzeigen
Zugehörige Verweise:
Preview Archive
Preview Backup

Operationen für Clients für Sichern/Archivieren planen

Sie können Sicherungsoperationen zum Schützen von Clientdaten planen, um sicherzustellen, dass sie regelmäßig ausgeführt werden.

Informationen zu diesem Vorgang

Der Client-Scheduler ist für die Interaktion mit der zentralen Zeitplanung des IBM Spectrum Protect-Servers für die automatische Sicherung Ihrer Daten verfügbar.

- Übersicht über den IBM Spectrum Protect-Scheduler
  Der zentrale IBM Spectrum Protect-Scheduler ermöglicht, dass Clientoperationen zu angegebenen Zeiten automatisch stattfinden.
- Clientrückkehrcodes
  Die Befehlszeilenschnittstelle für Sichern/Archivieren und der Scheduler werden mit einem Rückkehrcode verlassen, der den Erfolg oder das Fehlschlagen der Clientoperation genau wiedergibt.

Übersicht über den IBM Spectrum Protect-Scheduler

Der zentrale IBM Spectrum Protect-Scheduler ermöglicht, dass Clientoperationen zu angegebenen Zeiten automatisch stattfinden.

Zum besseren Verständnis der Zeitplanung mit IBM Spectrum Protect müssen mehrere Begriffe definiert werden:

Zeitplandefinition
: Eine Zeitplandefinition auf dem IBM Spectrum Protect-Server gibt kritische Merkmale einer automatisierten Aktivität an. Hierzu gehören die Art und der Zeitpunkt der Aktion sowie die Häufigkeit, mit der die Aktion stattfinden soll. Für einen Zeitplan können zahlreiche weitere Eigenschaften definiert werden. Informationen zum Befehl DEFINE SCHEDULE finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Zeitplanzuordnung
: Eine Zeitplanzuordnung ist eine Zuordnung zu einer bestimmten Zeitplandefinition für einen Clientknoten. Mehrfachzeitplanzuordnungen ermöglichen, dass einzelne Zeitplandefinitionen von vielen Clientknoten verwendet werden können. Da Zeitplandefinitionen in bestimmten Maßnahmendomänen eingeschlossen sind, können nur Knoten, die für eine bestimmte Maßnahmendomäne definiert sind, Zeitplänen zugeordnet werden, die in dieser Domäne definiert sind.

Geplantes Ereignis
: Ein geplantes Ereignis ist ein bestimmtes Vorkommen, wann ein Zeitplan für einen Knoten ausgeführt wird. Die folgenden Bedingungen müssen erfüllt sein, damit automatisch geplante Ereignisse für einen Client stattfinden:

  - Eine Zeitplandefinition muss für eine bestimmte Maßnahmendomäne vorhanden sein.
  - Eine Zeitplanzuordnung muss für den erforderlichen Knoten, der zu dieser Maßnahmendomäne gehört, vorhanden sein.
  - Der Client-Schedulerprozess muss auf dem Clientsystem aktiv sein.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeBeim Erstellen einer Zeitplandefinition auf dem IBM Spectrum Protect-Server können Sie die folgenden Zeitplanaktionen verwenden: incremental, selective, archive, restore, retrieve, Imagesicherung (gilt nicht für Mac OS X), Imagezurückschreibung (gilt nicht für Mac OS X), command und macro. Die am häufigsten verwendete Aktion ist 'incremental', wobei der Parameter objects nicht definiert wird. Bei dieser Einstellung führt der Client für Sichern/Archivieren eine Domänenteilsicherung aller Dateisysteme aus, die durch die Clientdomänenoption definiert sind. Eine Zeitplandefinition mit der Aktion command bewirkt, dass ein Betriebssystembefehl oder ein Shell-Script ausgeführt werden kann. Wenn Sie Tasks für IBM Spectrum Protect for Data Protection-Clients automatisieren, müssen Sie Zeitplandefinitionen mit der Aktion command verwenden, die die Befehlszeilendienstprogramme für diese Anwendungen aufrufen.

 Windows-BetriebssystemeBeim Erstellen einer Zeitplandefinition auf dem IBM Spectrum Protect-Server können Sie die folgenden Zeitplanaktionen verwenden: incremental, selective, archive, restore, retrieve, imagebackup, imagerestore, command und macro. Die am häufigsten verwendete Aktion ist 'incremental', wobei der Parameter objects nicht definiert wird. Bei dieser Einstellung führt der IBM Spectrum Protect-Client eine Domänenteilsicherung aller Laufwerke durch, die durch die Clientoption domain definiert sind. Eine Zeitplandefinition mit der Aktion command bewirkt, dass ein Betriebssystembefehl oder ein Shell-Script ausgeführt werden kann. Wenn Sie Tasks für IBM Spectrum Protect for Data Protection-Clients automatisieren, müssen Sie Zeitplandefinitionen mit der Aktion command verwenden, die die Befehlszeilendienstprogramme für diese Anwendungen aufrufen.

Der Zeitplan *Startfenster* zeigt den verfügbaren Zeitraum für den Start eines geplanten Ereignisses an. Das Startfenster wird durch die folgenden Zeitplandefinitionsparameter definiert: startdate, starttime, durunits und duration. Die Optionen startdate und starttime definieren den Beginn des Startfensters für das allererste geplante Ereignis. Der Beginn des Startfensters für nachfolgende geplante Ereignisse variiert je nach den Zeitplandefinitonswerten für period und perunit. Die Parameter duration und durunits definieren die Länge des Startfensters. Die Zeitplanaktion muss innerhalb des Startfensters starten. Dies illustrieren die Ergebnisse der folgenden Zeitplandefinition:

```
define schedule standard test1 action=incremental starttime=12:00:00 period=1
perunits=hour dur=30 duru=minutes
```

Ereignis	Fensterstart	Fensterende	Tatsächlicher Start (nur als Beispiel, die Zeiten variieren)
1	12:00:00	12:30:00	12:05:33
2	13:00:00	13:30:00	13:15:02
3	14:00:00	14:30:00	14:02:00
usw.			

Die Variation der tatsächlichen Startzeiten ist ein Ergebnis der vom zentralen IBM Spectrum Protect-Scheduler zur Verfügung gestellten Zufallsgenerierungsfunktion, die hilft, die Last der geplanten Sitzungen auf dem IBM Spectrum Protect-Server zu verteilen.

- Beispiele: Leerzeichen in Dateinamen in Zeitplandefinitionen
  Wenn Sie den Zeitplanparameter objects oder den Zeitplanparameter options mit Dateispezifikationen definieren oder aktualisieren, die Leerzeichen enthalten, müssen Sie alle Dateispezifikationen mit Leerzeichen in Anführungszeichen (") und dann die gesamte Spezifikation in Hochkommas (') einschließen.
- Bevorzugte Startzeiten für bestimmte Knoten
  Gelegentlich wollen Sie vielleicht sicherstellen, dass ein bestimmter Knoten seine geplante Aktivität so nah wie möglich an der definierten Startzeit des Zeitplans beginnt. Diese Notwendigkeit ergibt sich normalerweise, wenn Zeitplanung im Modus mit Bedienerführung verwendet wird.
- Schedulerverarbeitungsoptionen
  Schedulerverarbeitungsoptionen legen fest, welche Operationen beim Starten eines Scheduler-Jobs ausgeführt werden.
- Clientakzeptor-Scheduler-Services gegenüber traditionellen Scheduler-Services
  Sie können den IBM Spectrum Protect-Client so konfigurieren, dass der Schedulerprozess mit dem IBM Spectrum Protect-

Clientakzeptordämon verwaltet wird.
- Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren
  Sie können den IBM Spectrum Protect-Client-Scheduler so konfigurieren, dass er als Systemtask im Hintergrund ausgeführt und automatisch gestartet wird, wenn Ihr System gestartet wird.
- Beispiele: Informationen zu geplanter Arbeit anzeigen
  Zeitpläne können klassisch oder erweitert sein, je nachdem, wie das Intervall bis zur nächsten Ausführung definiert wird.
- Informationen zu beendeter Arbeit anzeigen
  Wenn Sie den Befehl schedule im Vordergrund ausführen, wird die Ausgabe geplanter Befehle auf Ihrem Bildschirm angezeigt.
- Planungsoptionen angeben
  Sie können Planungsoptionen in der Clientoptionsdatei oder in der grafischen Benutzerschnittstelle (GUI) ändern.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeZeitplanungsoptionen für Befehle
  Der Scheduler führt Befehle unter der Benutzer-ID `0` (Root) aus. Einige Befehle müssen möglicherweise jedoch unter einer anderen Benutzer-ID als `0` ausgeführt werden.
- Geplante Befehle aktivieren oder inaktivieren
  Sie können die Option schedcmddisabled verwenden, um die Planung von Befehlen durch den Server zu inaktivieren.
- Windows-BetriebssystemeVom Scheduler-Service verwendete Verarbeitungsoptionen ändern
  Wenn Sie die zentralen Zeitplanungsservices von IBM Spectrum Protect (Scheduler, Clientakzeptor oder ferner Clientagent) konfigurieren, werden einige der von Ihnen angegebenen Verarbeitungsoptionen in der Windows-Registrierung definiert.
- Mehrere Zeitplananforderungen auf einem System verwalten
  In bestimmten Situationen ist es zu bevorzugen, für jedes Clientsystem mehrere geplante Aktivitäten zu haben.

Beispiele: Leerzeichen in Dateinamen in Zeitplandefinitionen

Wenn Sie den Zeitplanparameter objects oder den Zeitplanparameter options mit Dateispezifikationen definieren oder aktualisieren, die Leerzeichen enthalten, müssen Sie alle Dateispezifikationen mit Leerzeichen in Anführungszeichen (") und dann die gesamte Spezifikation in Hochkommas (') einschließen.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDie folgenden Beispiele zeigen, wie Zeitplanparameter object begrenzt werden, wenn Dateispezifikationen Leerzeichen enthalten:

```
objects='"/home/proj1/Some file.doc"'
objects='"/home/proj1/Some file.doc" "/home/Another file.txt" /home/noblanks.txt'
objects='"/home/My Directory With Blank Spaces/"'
objects='"/Users/user1/Documents/Some file.doc"'
objects='"/Users/user1/Documents/Some file.doc"
 "/Users/user5/Documents/Another file.txt" /Users/user3/Documents/noblanks.txt'
objects='"/Users/user1/My Directory With Blank Spaces/"'
```

Diese Syntax stellt sicher, dass eine Dateispezifikation mit Leerzeichen (z. B. /home/proj1/Some file.doc) als Name einer einzigen Datei und nicht als Namen von zwei separaten Dateien (/home/proj1/Some und file.doc) behandelt wird.
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDie folgenden Beispiele zeigen, wie Zeitplanparameter options begrenzt werden, wenn Dateispezifikationen Leerzeichen enthalten:

```
options='-preschedulecmd="/home/me/my files/bin/myscript"
 -postschedulecmd="/home/me/my files/bin/mypostscript" -quiet'
options='-presched="/home/me/my files/bin/precmd" -postsched=finish'
```

Windows-BetriebssystemeDie folgenden Beispiele zeigen, wie Zeitplanparameter object begrenzt werden, wenn Dateispezifikationen Leerzeichen enthalten:

```
objects='"c:\home\proj1\Some file.doc"'
objects='"c:\home\proj1\Some file.doc" "c:\home\Another file.txt"
 c:\home\noblanks.txt'
objects='"c:\home\My Directory With Blank Spaces\"'
objects='"c:\Users\user1\Documents\Some file.doc"'
objects='"c:\Users\user1\Documents\Some file.doc"
 "c:\Users\user5\Documents\ Another file.txt" c:\Users\user3\Documents\noblanks.txt'
objects='"c:\Users\user1\My Directory With Blank Spaces\"'
```

Diese Syntax stellt sicher, dass eine Dateispezifikation mit Leerzeichen (z. B. c:\home\proj1\Some file.doc) als Name einer einzigen Datei und nicht als Namen von zwei separaten Dateien (c:\home\proj1\Some und file.doc) behandelt wird.
Windows-BetriebssystemeDie folgenden Beispiele zeigen, wie Zeitplanparameter options begrenzt werden, wenn Dateispezifikationen Leerzeichen enthalten:

```
options='-preschedulecmd="c:\home\me\my files\bin\myscript"
  -postschedulecmd="c:\home\me\my files\bin\mypostscript" -quiet'
options='-presched="c:\home\me\my files\bin\precmd" -postsched=finish'
```

Weitere Informationen finden Sie auch in der Beschreibung der Parameter objects und options unter den Befehlen DEFINE SCHEDULE und UPDATE SCHEDULE. Die Beschreibungen dieser Befehle und Parameter finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Zugehörige Konzepte:
Eingabezeichenfolgen angeben, die Leerzeichen oder Hochkommas oder Anführungszeichen enthalten

Bevorzugte Startzeiten für bestimmte Knoten

Gelegentlich wollen Sie vielleicht sicherstellen, dass ein bestimmter Knoten seine geplante Aktivität so nah wie möglich an der definierten Startzeit des Zeitplans beginnt. Diese Notwendigkeit ergibt sich normalerweise, wenn Zeitplanung im Modus mit Bedienerführung verwendet wird.

Abhängig von der Anzahl Clientknoten, die dem Zeitplan zugeordnet sind, und von der Position des Knotens in der Bedienerführungsreihenfolge, kann es dazu kommen, dass der Knoten erheblich später angefordert wird als die Startzeit für den Zeitplan beträgt.

In diesem Fall können Sie die folgenden Schritte ausführen:

1. Kopieren Sie den Zeitplan mit einem anderen Namen in einen neuen Zeitplan (oder definieren Sie einen neuen Zeitplan mit den bevorzugten Attributen).
2. Definieren Sie das Prioritätsattribut des neuen Zeitplans so, dass er eine höhere Priorität als der ursprüngliche Zeitplan hat.
3. Löschen Sie die Zuordnung des Knotens zum ursprünglichen Zeitplan und ordnen Sie anschließend den Knoten dem neuen Zeitplan zu.

Nun verarbeitet der IBM Spectrum Protect-Server den neuen Zeitplan zuerst.

Schedulerverarbeitungsoptionen

Schedulerverarbeitungsoptionen legen fest, welche Operationen beim Starten eines Scheduler-Jobs ausgeführt werden.

Sie können die meisten dieser Schedulerverarbeitungsoptionen in der Clientoptionsdatei definieren. Einige dieser Optionen können jedoch auf dem IBM Spectrum Protect-Server für alle Clients definiert werden.

Die folgende Tabelle zeigt, welche Optionen jeweils vom Client und vom Server definiert und welche Option vom Server überschrieben werden. Ein *X* in einer Spalte zeigt an, wo die Option angegeben werden kann.

Option	Clientdefiniert	Serverdefiniert	Globale Überschreibung durch Server
managedservices	X		
maxcmdretries	X		Befehl SET MAXCMDRETRIES
maxschedsessions		X	
postschedulecmd, postnschedulecmd	X		
preschedulecmd, prenschedulecmd	X		
queryschedperiod	X		Befehl SET QUERYSCHEDPERIOD
randomize		X	
retryperiod	X		Befehl SET RETRYPERIOD
schedcmddisabled	X		
schedlogname	X		
schedlogretention	X		
schedmode	X		Befehl SET SCHEDMODES
sessioninitiation	X	X	Befehl UPDATE NODE
tcpclientaddress	X	X (auch auf dem Server definiert, wenn `sessioninit=serveronly` als Teil der Knotendefinition definiert ist)	
tcpclientport	X	X (auch auf dem Server definiert, wenn `sessioninit=serveronly` als Teil der Knotendefinition definiert ist)	

Windows-BetriebssystemeClientdefinierte Optionen sind in der Datei dsm.opt definiert. Der IBM Spectrum Protect-Server kann auch einige Optionen in einer Clientoptionsgruppe oder als Teil der Optionsparameter der Zeitplandefinition definieren. Der IBM Spectrum Protect-Server kann auch einige Optionen global für alle Clients definieren. Standardmäßig wird die Clienteinstellung für diese Optionen berücksichtigt. Wenn auf dem IBM Spectrum Protect-Server die globale Überschreibung gesetzt ist, wird die Clienteinstellung für die Option ignoriert. Das Definieren von Clientoptionen als Teil der Zeitplandefinition ist nützlich, wenn Sie spezifische Optionen für eine geplante Aktion verwenden wollen, die sich

von den normalerweise vom Clientknoten verwendeten Optionseinstellungen unterscheiden oder für jeden Zeitplan, den der Knoten ausführt, verschieden sind.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeClientdefinierte Optionen sind je nach Option und Plattform in der Datei dsm.sys oder dsm.opt definiert. Der IBM Spectrum Protect-Server kann auch einige Optionen in einer Clientoptionsgruppe oder als Teil der Optionsparameter der Zeitplandefinition definieren. Der IBM Spectrum Protect-Server kann auch einige Optionen global für alle Clients definieren. Standardmäßig wird die Clienteinstellung für diese Optionen berücksichtigt. Wenn auf dem IBM Spectrum Protect-Server die globale Überschreibung gesetzt ist, wird die Clienteinstellung für die Option ignoriert. Das Definieren von Clientoptionen als Teil der Zeitplandefinition ist nützlich, wenn Sie spezifische Optionen für eine geplante Aktion verwenden wollen, die sich von den normalerweise vom Clientknoten verwendeten Optionseinstellungen unterscheiden oder für jeden Zeitplan, den der Knoten ausführt, verschieden sind.

Die Option schedmode steuert die Kommunikationsinteraktion zwischen dem IBM Spectrum Protect-Client und -Server. Es gibt zwei Varianten im Planungsmodus: *client polling* (Clientsendeaufruf) und *server prompted* (Serversystemanfrage). Diese Varianten werden in der Dokumentation zum IBM Spectrum Protect-Server erläutert.

- Rückkehrcodes für Zeitpläne in Zeitplanscripts auswerten
  Sie können Umgebungsvariablen verwenden, um den aktuellen IBM Spectrum Protect-Rückkehrcode zu bestimmen, bevor Sie ein Script mithilfe der Clientoption preschedulecmd oder postschedulecmd ausführen.
- Rückkehrcodes von preschedulecmd- und postschedulecmd-Scripts
  In diesem Abschnitt werden die Rückkehrcodes beschrieben, die möglicherweise angezeigt werden, wenn Sie die Optionen preschedulecmd und postschedulecmd verwenden.

Rückkehrcodes für Zeitpläne in Zeitplanscripts auswerten

Sie können Umgebungsvariablen verwenden, um den aktuellen IBM Spectrum Protect-Rückkehrcode zu bestimmen, bevor Sie ein Script mithilfe der Clientoption preschedulecmd oder postschedulecmd ausführen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme IBM Spectrum Protect stellt den aktuellen Wert des Rückkehrcodes in der Umgebungsvariablen mit dem Namen *TSM_PRE_CMD_RC* bereit. Die Variable *TSM_PRE_CMD_RC* ist der aktuelle Wert des IBM Spectrum Protect-Rückkehrcodes, bevor Sie ein Zeitplanscript ausführen. Der Wert der Variablen *TSM_PRE_CMD_RC* ist nicht notwendigerweise mit dem Rückkehrcode identisch, den IBM Spectrum Protect nach der Ausführung des Zeitplanscripts ausgibt. Mit der Variablen *TSM_PRE_CMD_RC* kann in Zeitplanscripts der aktuelle Status des Zeitplans bestimmt werden.

Die Variable *TSM_PRE_CMD_RC* wird mit jeder der folgenden Planungsoptionen definiert: preschedule, prenschedule, postschedule und postnschedule. *TSM_PRE_CMD_RC* hat Einfluss auf die Zeitpläne, in denen die Option ACTION=COMMAND angegeben ist.

Ein Verwendungsbeispiel für die Variable *TSM_PRE_CMD_RC*:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

```
if [[ -n  ${TSM_PRE_CMD_RC} ]] ; then

   if [[ ${TSM_PRE_CMD_RC} == 0 ]] ; then
     echo "The TSM_PRE_CMD_RC is 0"

   elif [[ ${TSM_PRE_CMD_RC} == 4 ]] ; then
     echo "The TSM_PRE_CMD_RC is 4"

   elif [[ ${TSM_PRE_CMD_RC} == 8 ]] ; then
     echo "The TSM_PRE_CMD_RC is 8"


   elif [[ ${TSM_PRE_CMD_RC} == 12 ]] ; then
     echo "The TSM_PRE_CMD_RC is 12"
           else
     echo "The TSM_PRE_CMD_RC is an unexpected value: ${TSM_PRE_CMD_RC}"

   fi

   else
   echo "The TSM_PRE_CMD_RC is not set"
fi
```

Rückkehrcodes von preschedulecmd- und postschedulecmd-Scripts

In diesem Abschnitt werden die Rückkehrcodes beschrieben, die möglicherweise angezeigt werden, wenn Sie die Optionen preschedulecmd und postschedulecmd verwenden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

- Wenn der durch die Option preschedulecmd angegebene Befehl mit einem Rückkehrcode ungleich null endet, nimmt IBM Spectrum Protect an, dass der Befehl fehlgeschlagen ist. In diesem Fall kann weder das geplante Ereignis noch ein postschedulecmd- oder

postnschedulecmd-Befehl ausgeführt werden. Der Verwaltungsbefehl query event mit der Option format=detailed zeigt an, dass das Ereignis mit dem Rückkehrcode 12 fehlgeschlagen ist.

- Wenn der durch die Option postschedulecmd angegebene Befehl mit einem Rückkehrcode ungleich null endet, betrachtet IBM Spectrum Protect den Befehl als fehlgeschlagen. Der Verwaltungsbefehl query event mit der Option format=detailed zeigt an, dass das Ereignis mit dem Rückkehrcode 8 beendet wurde; es sei denn, die geplante Operation wurde mit einem höheren Rückkehrcode beendet. In diesem Fall hat der höhere Rückkehrcode Vorrang. Wenn die geplante Operation mit dem Rückkehrcode 0 oder 4 endet und der Befehl postschedulecmd fehlschlägt, zeigt der Verwaltungsbefehl query event daher an, dass das Ereignis mit dem Rückkehrcode 8 beendet wurde. Wenn die geplante Operation mit dem Rückkehrcode 12 endet, hat dieser Rückkehrcode Vorrang und query event zeigt an, dass das Ereignis mit dem Rückkehrcode 12 fehlgeschlagen ist.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBeim Interpretieren des Rückkehrcodes von einem Befehl betrachtet IBM Spectrum Protect 0 als Erfolg und alles Andere als Fehler. Obwohl dieses Verhalten in der Branche überall akzeptiert wird, kann es nicht zu 100% garantiert werden. Beispiel: Der Befehl widget wurde vielleicht so entwickelt, dass er den Rückkehrcode 3 ausgibt, wenn er erfolgreich ausgeführt wurde. Deshalb ist es möglich, dass der Befehl preschedulecmd oder postschedulecmd unter Umständen mit einem Rückkehrcode ungleich null endet und dennoch erfolgreich ist. Um zu verhindern, dass IBM Spectrum Protect solche Befehle als fehlgeschlagen behandelt, können Sie diese Befehle in ein Script einbetten und das Script so codieren, dass es die Befehlsrückkehrcodes korrekt interpretiert. Das Script wird mit Rückkehrcode 0 beendet, wenn der Befehl erfolgreich war; andernfalls wird es mit einem Rückkehrcode ungleich null beendet. Die Logik für ein Script, das widget ausführt, sieht möglicherweise wie in diesem Beispiel aus:

Windows-BetriebssystemeBeim Interpretieren des Rückkehrcodes von einem Befehl betrachtet IBM Spectrum Protect 0 als Erfolg und alles Andere als Fehler. Obwohl dieses Verhalten in der Branche überall akzeptiert wird, kann es nicht zu 100% garantiert werden. Beispiel: Der Befehl widget.exe wurde eventuell so entwickelt, dass er den Rückkehrcode 3 ausgibt, wenn widget.exe erfolgreich ausgeführt wurde. Deshalb ist es möglich, dass der Befehl preschedulecmd oder postschedulecmd unter Umständen mit einem Rückkehrcode ungleich null endet und dennoch erfolgreich ist. Um zu verhindern, dass IBM Spectrum Protect solche Befehle als fehlgeschlagen behandelt, können Sie diese Befehle in ein Script einbetten und das Script so codieren, dass es die Befehlsrückkehrcodes korrekt interpretiert. Das Script sollte mit Rückkehrcode 0 enden, wenn der Befehl erfolgreich war; andernfalls sollte es mit einem Rückkehrcode ungleich null enden. Die Logik für ein Script, das widget.exe ausführt, sieht möglicherweise wie in diesem Beispiel aus:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

```
run 'widget'
      if lastcc == 3
            exit 0
      else
            exit 1
```

Windows-Betriebssysteme

```
run 'widget.exe'
      if lastcc == 3
            exit 0
      else
            exit 1
```

Zugehörige Verweise:
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme
Postschedulecmd/Postnschedulecmd
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme
Preschedulecmd/Prenschedulecmd

Clientakzeptor-Scheduler-Services gegenüber traditionellen Scheduler-Services

Sie können den IBM Spectrum Protect-Client so konfigurieren, dass der Schedulerprozess mit dem IBM Spectrum Protect-Clientakzeptordämon verwaltet wird.

Der Clientakzeptordämon stellt einen einfachen Zeitgeber zur Verfügung, der den Schedulerprozess nach Bedarf automatisch startet und stoppt. Alternativ dazu hält die traditionelle Methode den IBM Spectrum Protect-Schedulerprozess fortlaufend akitv. Im allgemeinen ist die Verwendung des Clientakzeptordämons zum Verwalten des Schedulers die bevorzugte Methode.

Der folgende Abschnitt enthält einen Vergleich zwischen den vom Clientakzeptordämon (CAD) verwalteten Services und den Methoden der traditionellen Scheduler-Services.

Vom Clientakzeptordämon verwaltete Services

- Werden mithilfe der Option managedservices schedule definiert und mit den Clientakzeptordämonservices (dsmcad) gestartet.
- Der Clientakzeptordämon startet und stoppt den Schedulerprozess für jede geplante Aktion nach Bedarf.
- Erfordern weniger Systemressourcen bei Inaktivität.
- Die IBM Spectrum Protect-Clientoptionen und die Überschreibungsoptionen auf dem IBM Spectrum Protect-Server werden jedes Mal aktualisiert, wenn die Clientakzeptordämonservices eine geplante Sicherung starten.
- Können nicht bei Sicherungen mit SESSIONINITiation=SERVERONly verwendet werden.

Traditionelle IBM Spectrum Protect-Scheduler-Services

- Werden mit dem Befehl `dsmc sched` gestartet.
- Bleiben aktiv, selbst wenn die geplante Sicherung beendet ist.
- Erfordern einen höheren Verbrauch an Systemressourcen bei Inaktivität.
- Die IBM Spectrum Protect-Clientoptionen und die Überschreibungsoptionen auf dem IBM Spectrum Protect-Server werden nur einmal verarbeitet, wenn `dsmc sched` gestartet wird. Wenn Sie eine Option aus einer Clientoptionsgruppe löschen, müssen Sie den Scheduler erneut starten, damit der Scheduler die Löschung registriert.

Tipp: Starten Sie den traditionellen Scheduler regelmäßig, um Systemressourcen freizugeben, die zuvor von Systemaufrufen verwendet wurden.

Client-Scheduler-Prozess für die Ausführung als Hintergrundtask und den automatischen Start beim Systemstart definieren

Sie können den IBM Spectrum Protect-Client-Scheduler so konfigurieren, dass er als Systemtask im Hintergrund ausgeführt und automatisch gestartet wird, wenn Ihr System gestartet wird.

Informationen zu diesem Vorgang

Sie können diese Task unabhängig davon ausführen, ob Sie den Scheduler mit dem Clientakzeptor verwalten oder ob Sie zum Starten des Client-Schedulers die traditionelle Methode verwenden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeWenn Sie einen vom Clientakzeptor verwalteten Zeitplan ausführen, definieren Sie den Clientakzeptorprozess (nicht den Schedulerprozess) für den automatischen Start zur Startzeit. Wenn Sie die traditionelle Methode verwenden, definieren Sie den Schedulerprozess für den automatischen Start zur Startzeit.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeSie können den Clientakzeptor so konfigurieren, dass er als Systemtask im Hintergrund ausgeführt wird und automatisch gestartet wird, wenn Ihr System gestartet wird. Um den Clientakzeptor für die Verwaltung geplanter Sicherungen zu konfigurieren, geben Sie mit der Option managedservices an, ob der Clientakzeptor nur den Scheduler, nur den Web-Client oder sowohl den Scheduler als auch den Web-Client verwaltet. Die Methode zum Definieren des Clientakzeptors als Systemtask ist je nach Plattform unterschiedlich.

Damit der Scheduler automatisch gestartet werden kann, müssen Sie dem Client die Speicherung seines Kennworts ermöglichen, indem Sie die Option passwordaccess auf generate setzen und das Kennwort speichern, indem Sie einen einfachen Clientbefehl wie `dsmc query session` ausführen. Zu Testzwecken können Sie den Scheduler immer im Vordergrund starten, indem Sie `dsmc sched` über eine Eingabeaufforderung ausführen (ohne eine Zeilengruppe `managedservices` zu definieren).

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeUm den Scheduler zur Startzeit automatisch zu starten, verwenden Sie entweder die Methode zur Verwaltung durch den Clientakzeptor oder die traditionelle Methode.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

Methode zur Verwaltung durch den Clientakzeptor

1. Setzen Sie in Ihrer Datei dsm.sys die Option managedservices auf schedule oder schedule webclient.
2. Starten Sie den Clientakzeptor.
   a. AIX-BetriebssystemeOracle Solaris-Betriebssysteme

      Fügen Sie auf AIX- und Solaris-Clients den folgenden Eintrag zur Systemstartdatei (bei den meisten Plattformen /etc/inittab) hinzu:

      ```
      tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # TSM Client
      Acceptor Daemon
      ```

   b.  Linux-Betriebssysteme
      Auf Linux-Clients erstellt das Installationsprogramm ein Startscript für den Clientakzeptor (dsmcad) an der Position /etc/init.d. Der Clientakzeptor (dsmcad) muss gestartet werden, damit er Scheduler-Tasks oder den Web-Client verwalten kann. Führen Sie die folgenden Befehle als Rootbenutzer aus, um den Clientakzeptor zu starten, zu stoppen, erneut zu starten oder seinen Status zu überprüfen:

      ```
      >>-service dsmcad--+-start---+---------------------------------><
                         +-stop----+
                         +-restart-+
                         '-status--'
      ```

      Damit der Clientakzeptor nach einem Systemwiederanlauf automatisch gestartet werden kann, fügen Sie den Service wie folgt über eine Shelleingabeaufforderung hinzu:

      ```
      # chkconfig --add dsmcad
      ```

      Wenn das Betriebssystem Linux den Initialisierungsservice `systemd` ausführt, führen Sie die folgenden Schritte aus, um dsmcad zu starten und zur Systemstartzeit auszuführen:

i. Kopieren Sie die bereitgestellte `systemd`-Einheitendatei /opt/tivoli/tsm/client/ba/bin/dsmcad.service in das Verzeichnis /etc/systemd/system/.
ii. Führen Sie den folgenden Befehl aus, um die `systemd`-Einheitenliste zu aktualisieren:

```
systemctl daemon-reload
```

iii. Führen Sie den folgenden Befehl aus, um den Clientakzeptor zur Systemstartzeit zu starten:

```
systemctl enable dsmcad.service
```

iv. Führen Sie den folgenden Befehl aus, um den Clientakzeptor zu starten:

```
systemctl start dsmcad.service
```

c. Mac OS X-BetriebssystemeUnter Mac OS X muss der Clientakzeptordämon als Starteintrag installiert sein. Ein Systemadministrator muss die IBM Spectrum Protect-Tools für Administratoren verwenden, um den Clientakzeptor zu installieren und zu starten. Um den Clientakzeptor zu starten, zu stoppen oder erneut zu starten, verwenden Sie den folgenden Befehl:

```
>>-sudo /sbin/SystemStarter--+-start---+--dsmcad--------------><
                             +-stop----+
                             '-restart-'
```

3. Setzen Sie in der Datei dsm.sys die Option passwordaccess auf generate.
4. Führen Sie einen Befehl wie `dsmc query sess` aus, um das Kennwort für den Knoten zu speichern.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTraditionelle Methode:
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

1. Legen Sie die Option managedservices fest.
   - AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeAuf AIX-, Linux- und Solaris-Clients müssen Sie die Option entweder vollständig entfernen (standardmäßig wird webclient angenommen) oder auf webclient setzen.
   - Mac OS X-BetriebssystemeSetzen Sie auf Mac OS X-Clients die Option managedservices entweder auf webclient oder auf none. Setzen Sie die Option nicht auf die Einstellung schedule.
2. Fügen Sie unter AIX, Linux und Solaris den folgenden Eintrag zur Systemstartdatei (z. B. /etc/inittab) hinzu, sofern dies unterstützt wird:

```
tsmsched::once:/usr/bin/dsmc sched > /dev/null 2>&1 # TSM scheduler
```

3. Setzen Sie in der Datei dsm.sys die Option passwordaccess auf generate.
4. Führen Sie einen Befehl wie `dsmc query sess` aus, um das Kennwort für den Knoten zu speichern.
5. Um den Client-Scheduler auf Ihrem Clientknoten zu starten und eine Verbindung zum Serverzeitplan herzustellen, müssen Sie den folgenden Befehl eingeben:

   ```
   dsmc schedule
   ```

   Falls sich das aktuelle Verzeichnis nicht in Ihrer Umgebungsvariablen PATH befindet, geben Sie den folgenden Befehl ein:

   ```
   ./dsmc schedule
   ```

   Wenn Sie den Client-Scheduler starten, ist dieser kontinuierlich aktiv, bis Sie das Fenster schließen, den Prozess beenden oder sich vom System abmelden.

   Geben Sie folgenden Befehl ein, damit der Befehl schedule im Hintergrund ausgeführt wird und der Client-Scheduler auch nach einer Abmeldung vom System aktiv bleibt:

   ```
   nohup dsmc schedule 2> /dev/null &
   ```

Windows-BetriebssystemeAuf Windows-Plattformen werden der Scheduler und der Clientakzeptor als Dienst ausgeführt. Sie können diese Dienste entweder mit dem Setup-Assistenten oder mit dem Konfigurationsdienstprogramm für den IBM Spectrum Protect-Client-Service dsmcutil.exe erstellen und verwalten.

Windows-Betriebssysteme

- Um den Setup-Assistenten zu starten, wählen Sie Dienstprogramme > Setup-Assistent in der GUI für Sichern/Archivieren aus; wählen Sie dann die Option Hilfe zum Konfigurieren für den entsprechenden Service aus. Folgen Sie den Bedienerführungen, um den Service zu installieren, zu konfigurieren und zu starten.
- Um das Konfigurationsdienstprogramm für den Client-Service zu starten, öffnen Sie ein Fenster mit Eingabeaufforderung und geben Sie den folgenden Befehl aus, um zu dem Verzeichnis zu wechseln, das die Datei dsmcutil.exe enthält:

  ```
  cd /d "c:\Programme\tivoli\tsm\baclient"
  ```

  Verwenden Sie dsmcutil, um den Clientakzeptorservice oder den Scheduler-Service zu verwalten. Die vollständige Dokumentation zur Verwendung von dsmcutil können Sie durch Eingabe von `dsmcutil help` anzeigen.

Windows-BetriebssystemeDer Client-Scheduler kann vom Clientakzeptor verwaltet werden. Wenn die Scheduler-Services für die Ausführung mit der Verwaltung durch den Clientakzeptor definiert werden, müssen zwei Services erstellt werden: der Scheduler-Service und der Clientakzeptorservice. Wenn Sie den Clientakzeptorservice mit dsmcutil.exe installieren, müssen Sie mit dem Parameter /cadschedname: angeben, welchen Scheduler-Service der Clientakzeptor verwaltet. Wenn Sie den Scheduler mit dem Setup-Assistenten installieren, können Sie das Kontrollkästchen Scheduler mit Clientakzeptor verwalten auswählen, wodurch automatisch beide Services erstellt und zugeordnet werden.

Windows-BetriebssystemeBeim Konfigurationsdienstprogramm für den Client-Service können Sie eine der beiden folgenden Methoden verwenden:

Windows-Betriebssysteme

Methode zur Verwaltung durch den Clientakzeptor

1. Setzen Sie in Ihrer Clientoptionsdatei (dsm.opt) die Option managedservices entweder auf schedule oder auf schedule webclient.
2. Setzen Sie in Ihrer Clientoptionsdatei (dsm.opt) die Option passwordaccess auf generate.
3. Erstellen Sie den Scheduler-Service:

   ```
   dsmcutil inst /name:"TSM-Client-Scheduler" /node:tsmclient1
   /password:secret /autostart:no /startnow:no
   ```

4. Erstellen Sie den Clientakzeptor und ordnen Sie den Scheduler-Service dem Clientakzeptor zu:

   ```
   dsmcutil inst CAD /name:"TSM-Clientakzeptor" /cadschedname:
   "TSM-Client-Scheduler" /node:tsmclient1 /password:secret /autostart:yes
   ```

5. Starten Sie den Clientakzeptorservice manuell:

   ```
   net start "TSM-Clientakzeptor"
   ```

Traditionelle Methode

1. Entfernen Sie in Ihrer Clientoptionsdatei (dsm.opt) entweder die Option managedservices vollständig (ihre Standardeinstellung ist webclient) oder setzen Sie sie auf webclient.
2. Setzen Sie in Ihrer Clientoptionsdatei (dsm.opt) die Option passwordaccess auf generate.
3. Erstellen Sie den Scheduler-Service:

   ```
   dsmcutil inst /name:"TSM-Client-Scheduler" /node:tsmclient1
   /password:secret /autostart:yes
   ```

Windows-BetriebssystemeUm die Zuverlässigkeit des Client-Scheduler-Service unter Windows zu verbessern, definieren Sie die Services so, dass sie nach einem Fehler automatisch wiederhergestellt werden. Gehen Sie dazu wie folgt vor:

Windows-Betriebssysteme

- Starten Sie die Windows-Verwaltungskonsole für Dienste (Services). Hierzu wählen Sie Start > Einstellungen > Systemsteuerung > Verwaltung > Dienste aus.
- Klicken Sie mit der rechten Maustaste auf den Dienst TSM-Client-Scheduler und wählen Sie die Option Eigenschaften aus.
- Klicken Sie auf die Registerkarte Wiederherstellen.
- Definieren Sie die Wiederherstellungsaktion für 'Erster Fehler', 'Zweiter Fehler' und 'Weitere Fehler' als Dienst neu starten.

Windows-BetriebssystemeWenn Sie den Scheduler mit dem Clientakzeptor verwalten, müssen Sie die Wiederherstellungseigenschaften für den Dienst TSM-Clientakzeptor definieren, die Wiederherstellungseinstellungen für den Dienst TSM-Client-Scheduler für den ersten Fehler, den zweiten Fehler und weitere Fehler jedoch als Keine Aktion durchführen übernehmen. Dieselben Wiederherstellungseinstellungen können auch definiert werden, um die Zuverlässigkeit des TSM-Journalservice zu verbessern.

Zugehörige Verweise:
Cadlistenonport

Beispiele: Informationen zu geplanter Arbeit anzeigen

Zeitpläne können klassisch oder erweitert sein, je nachdem, wie das Intervall bis zur nächsten Ausführung definiert wird.

Bei klassischen Zeitplänen kann der Zeitraum so klein wie eine Stunde sein. Bei erweiterten Plänen können Aktionen an bestimmten Tagen ausgeführt werden.

Um die für Ihren Clientknoten definierten Zeitpläne anzuzeigen, geben Sie Folgendes ein: AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

```
dsmc query schedule
```

Der Client für Sichern/Archivieren zeigt detaillierte Informationen zur gesamten für Ihren Clientknoten geplanten Arbeit an. In Tabelle 1 wird die Beispielausgabe des Befehls query schedule für klassische Zeitpläne angezeigt.

Tabelle 1. Beispielausgabe des Befehls 'query schedule' für klassische Zeitpläne

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
 Zeitplanname: DAILY_INC
        Beschreibung: Tägliche Systemsicherung
     Zeitplanstil: Klassisch
                Aktion: Teilsicherung
                Optionen: QUIET
                 Objekte:
              Priorität: 1
Nächste Ausführung: 30 Minuten
                  Dauer: 4 Stunden
                  Periode: 1 Tag
           Wochentag: Jeden Tag
                     Monat:
       Tag im Monat:
    Woche im Monat:
                Verfällt: Nie

  Zeitplan: WEEKLY_INC
        Beschreibung: Wöchentliche Sicherung für Projektdateien
     Zeitplanstil: Klassisch
                Aktion: Teilsicherung
                Optionen: QUIET
                 Objekte: /proj
              Priorität: 1
Nächste Ausführung: 60 Minuten
                  Dauer: 8 Stunden
                  Periode: 7 Tage
           Wochentag: Freitag
                     Monat:
       Tag im Monat:
    Woche im Monat:
                Verfällt: Nie
```

 Windows-Betriebssysteme

```
 Zeitplanname: DAILY_INC
        Beschreibung: Tägliche Systemsicherung
     Zeitplanstil: Klassisch
                Aktion: Teilsicherung
                Optionen: QUIET
                 Objekte:
              Priorität: 1
Nächste Ausführung: 30 Minuten
                  Dauer: 4 Stunden
                  Periode: 1 Tag
           Wochentag: Jeden Tag
                     Monat:
       Tag im Monat:
    Woche im Monat:
                Verfällt: Nie

  Zeitplan: WEEKLY_INC
        Beschreibung: Wöchentliche Sicherung für Projektdateien
     Zeitplanstil: Klassisch
                Aktion: Teilsicherung
                Optionen: QUIET
                 Objekte: e: f:
              Priorität: 1
Nächste Ausführung: 60 Minuten
                  Dauer: 8 Stunden
                  Periode: 7 Tage
           Wochentag: Freitag
                     Monat:
       Tag im Monat:
    Woche im Monat:
                Verfällt: Nie
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDer Zeitplan mit dem Namen **WEEKLY_INC** startet eine wöchentliche Teilsicherung im Dateisystem `/proj`.

 Windows-BetriebssystemeDer Zeitplan mit dem Namen **WEEKLY_INC** startet eine wöchentliche Teilsicherung in den Laufwerken `e:` und `f:`.

Der Zeitplan mit dem Namen **DAILY_INC** startet eine tägliche Teilsicherung. Die nächste Teilsicherung beginnt in 30 Minuten. Da keine Objekte aufgelistet sind, führt der Client die Teilsicherung in Ihrer Standarddomäne aus. Der Zeitplan hat kein Verfallsdatum.

Damit der Status geplanter Ereignisse genauer bestimmt werden kann, enthält die Ausgabe von query schedule für einen erweiterten Zeitplan auf Clients von IBM Spectrum Protect Version 5.3 und höher neue Felder. Diese Felder werden immer angezeigt, selbst wenn es sich um einen klassischen Zeitplan oder eine Clientsitzung der Version 5.3 mit einem Server vor Version 5.3 handelt; die neuen Felder sind dann aber leer. Beachten Sie, dass bei einem Client einer älteren Version (vor Version 5.3) der Server den Zeitraum als unendlich und den Wochentag als unzulässigen Tag zurückmeldet. In Tabelle 2 wird die Beispielausgabe des Befehls query schedule für erweiterte Zeitpläne angezeigt.

Tabelle 2. Beispielausgabe des Befehls 'query schedule' für erweiterte Zeitpläne

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
Zeitplanname: QUARTERLY_FULL
           Beschreibung: Vierteljährliche Gesamtsicherung
        Zeitplanstil: Erweitert
                      Aktion: Selektive Sicherung
                  Optionen: subdir=yes
                   Objekte: /* /Volumes/fs2/*
                 Priorität: 5
  Nächste Ausführung: 1744 Stunden und 26 Minuten
                    Dauer: 1 Tag
                    Periode:
              Wochentag: Freitag
                        Monat: März, Juni, September, Dezember
         Tag im Monat: Jeden Tag
       Woche im Monat: Letzte
                  Verfällt: Nie
```

Windows-Betriebssysteme

```
Zeitplanname: QUARTERLY_FULL
           Beschreibung: Vierteljährliche Gesamtsicherung
        Zeitplanstil: Erweitert
                      Aktion: Selektive Sicherung
                  Optionen: subdir=yes
                   Objekte: \* \volumes\fs2\*
                 Priorität: 5
  Nächste Ausführung: 1744 Stunden und 26 Minuten
                    Dauer: 1 Tag
                    Periode:
              Wochentag: Freitag
                        Monat: März, Juni, September, Dezember
         Tag im Monat: Jeden Tag
       Woche im Monat: Letzte
                  Verfällt: Nie
```

Informationen zu beendeter Arbeit anzeigen

Wenn Sie den Befehl schedule im Vordergrund ausführen, wird die Ausgabe geplanter Befehle auf Ihrem Bildschirm angezeigt.

Die Ausgabe wird außerdem in die Datei dsmsched.log im Installationsverzeichnis gestellt, wenn Sie den Verzeichnis- und Dateinamen nicht mit der Option schedlogname ändern.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWenn der Befehl schedule im Hintergrund ausgeführt wird, wird die Ausgabe geplanter Befehle in die Datei dsmsched.log im aktuellen Verzeichnis oder in den vom Benutzer angegebenen Pfad und Dateinamen übertragen. Die Datei dsmsched.log kann keine symbolische Verbindung sein.

Mac OS X-BetriebssystemeAnmerkung: Unter Mac OS X befindet sich das Protokoll standardmäßig an einer der folgenden Positionen:

```
~/Library/Logs/tivoli/tsm
/Library/Logs/tivoli/tsm
```

Windows-BetriebssystemeWenn der Befehl schedule als Service ausgeführt wird, wird die Ausgabe geplanter Befehle im Anwendungsereignisprotokoll angezeigt. Die Ausgabe wird außerdem in die Datei dsmsched.log im aktuellen Verzeichnis gestellt, wenn Sie den Pfad- und Dateinamen nicht mit der Option schedlogname ändern. Die Ausführlichkeit der Informationen ist abhängig davon, ob die Option *verbose* oder die Option *quiet* in der Datei `dsm.opt` definiert ist. Der Scheduler-Service übergibt auch Nachrichten an das Windows-Ereignisprotokoll.

Wenn die geplante Arbeit beendet ist, im Planungsprotokoll überprüfen, ob die Arbeit erfolgreich ausgeführt wurde.

Wenn ein geplanter Befehl verarbeitet wird, enthält das Planungsprotokoll folgenden Eintrag:

```
Geplantes Ereignis Ereignisname erfolgreich ausgeführt
```

Falls das geplante Ereignis nicht erfolgreich ausgeführt wird, erhalten Sie eine Nachricht wie die Folgende:

```
ANS1512E Geplantes Ereignis Ereignisname fehlgeschlagen. Rückkehrcode = Code.
```

Der Client gibt an, ob IBM Spectrum Protect den geplanten Befehl, der zu dem *Ereignisnamen* gehört, erfolgreich ausgegeben hat (action=command). Erfolg oder Misserfolg des Befehls wird nicht überprüft. Der Status des Befehls kann durch Auswertung des Rückkehrcodes vom geplanten Befehl im Planungsprotokoll bestimmt werden. Vor dem Eintrag für den Rückkehrcode des Befehls im Planungsprotokoll steht folgender Text:

```
Befehl beendet. Der Rückkehrcode lautet:
```

Das Planungsprotokoll kann unendlich groß werden, wenn Sie es nicht mit der Option schedlogretention bereinigen oder mit der Option schedlogmax eine Maximalgröße angeben.

- Beispiele: Ereignisprotokolle
  Der Scheduler-Service protokolliert Informationen im Anwendungsereignisprotokoll und stellt für jedes Ereignis im Protokoll eine Ereignis-ID zur Verfügung. Dieser Abschnitt enthält Beispiele für Ereignisse, die im Anwendungsereignisprotokoll protokolliert werden.

Zugehörige Konzepte:
Planungsoptionen angeben

Planungsoptionen angeben

Sie können Planungsoptionen in der Clientoptionsdatei oder in der grafischen Benutzerschnittstelle (GUI) ändern.

Gibt der Administrator jedoch einen Wert für diese Optionen an, überschreibt dieser Wert die Angabe des Benutzers in der Clientdatei.

Zugehörige Konzepte:
Planungsoptionen
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

Zeitplanungsoptionen für Befehle

Der Scheduler führt Befehle unter der Benutzer-ID `0` (Root) aus. Einige Befehle müssen möglicherweise jedoch unter einer anderen Benutzer-ID als `0` ausgeführt werden.

In diesem Fall kann Ihr IBM Spectrum Protect-Administrator mit der Serveroption schedcmduser Zeitpläne für Befehle definieren, die unter einer anderen Benutzer-ID als der Benutzer-ID des Schedulers ausgeführt werden.

Die Option schedcmduser gibt den Namen eines gültigen Benutzers auf dem System an, auf dem ein geplanter Befehl ausgeführt wird. Diese Option kann nur vom IBM Spectrum Protect-Serveradministrator definiert werden. Wenn diese Option angegeben wird, wird der Befehl mit der Berechtigung des angegebenen Benutzers ausgeführt. Andernfalls wird der Befehl mit der Berechtigung des Schedulers ausgeführt.

```
>>-SCHEDCMDUser----Benutzername--------------------------------><
```

Benutzername
Gibt den Namen eines gültigen Benutzers auf dem System an, auf dem ein geplanter Befehl ausgeführt wird.

Anmerkung: Die Option schedcmduser beeinflusst *nicht* die Benutzer-ID, die für Befehle vor und nach dem Zeitplan verwendet wird. Befehle vor und nach dem Zeitplan werden immer als Root (Benutzer-ID 0) ausgeführt.

Geplante Befehle aktivieren oder inaktivieren

Sie können die Option schedcmddisabled verwenden, um die Planung von Befehlen durch den Server zu inaktivieren.

Befehle werden mithilfe der Option action=*command* im Serverbefehl DEFINE SCHEDULE geplant.

Durch die Option schedcmddisabled werden die Befehle preschedulecmd und postschedulecmd nicht inaktiviert. Sie können jedoch preschedulecmd oder postschedulecmd mit einem Leerzeichen oder einer Nullzeichenfolge angeben, um die Zeitplanung dieser Befehle zu inaktivieren.

Mithilfe der Option schedrestretrdisabled können Sie verhindern, dass der IBM Spectrum Protect-Serveradministrator Planungsoperationen für Zurückschreibung oder Abruf ausführt.

Mithilfe der Option srvprepostscheddisabled können Sie verhindern, dass der IBM Spectrum Protect-Serveradministrator bei der Ausführung geplanter Operationen Befehle ausführt, die vor bzw. nach der Ausführung des Zeitplans ausgeführt werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme
Mithilfe der Option srvprepostsnapdisabled können Sie verhindern, dass der IBM Spectrum Protect-Serveradministrator bei der Ausführung geplanter Operationen für Image-Momentaufnahmesicherungen Befehle vor und nach der Momentaufnahme ausführt.

Zugehörige Verweise:
Schedcmddisabled
Schedrestretrdisabled
Srvprepostscheddisabled
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme
Srvprepostsnapdisabled
 Windows-Betriebssysteme

Vom Scheduler-Service verwendete Verarbeitungsoptionen ändern

Wenn Sie die zentralen Zeitplanungsservices von IBM Spectrum Protect (Scheduler, Clientakzeptor oder ferner Clientagent) konfigurieren, werden einige der von Ihnen angegebenen Verarbeitungsoptionen in der Windows-Registrierung definiert.

Die folgenden Optionen können ebenfalls in der Clientoptionsdatei (dsm.opt) angegeben werden.

- nodename
- httpport
- tcpserveraddress
- tcpport
- webports

Wenn der Client-Scheduler als Vordergrundprozess mit dem Befehl dsmc sched ausgeführt wird, werden die Optionen in der Clientoptionsdatei verwendet. Wenn der Scheduler jedoch als Windows-Dienst ausgeführt wird, werden stattdessen die Optionen in der Registrierung verwendet. Wenn Sie den Scheduler-Service verwenden und eine Option in der Datei dsm.opt ändern, müssen Sie den entsprechenden Wert in der Registrierung ebenfalls aktualisieren.

Zum Aktualisieren des Werts in der Windows-Registrierung:

Verwenden Sie den Setup-Assistenten in der Client-GUI. Weitere Informationen finden Sie in Scheduler konfigurieren.
Alternativ dazu können Sie das Dienstprogramm dsmcutil verwenden, um den Wert in der Registrierung zu ändern. Beispiel: `dsmcutil update scheduler /name: <Servicename> /node: <Name für neuen Knoten> /password: <Kennwort für neuen Knoten>`.
Anmerkung: Nach dem Aktualisieren der Registrierung müssen Sie den Scheduler-Service erneut starten, damit die Änderungen wirksam werden. Wenn Sie eine vom Clientakzeptordämon verwaltete Zeitplanung verwenden, ist dies nicht notwendig, da der Scheduler für jede Sicherung vom Clientakzeptordämon erneut gestartet wird.

Mehrere Zeitplananforderungen auf einem System verwalten

In bestimmten Situationen ist es zu bevorzugen, für jedes Clientsystem mehrere geplante Aktivitäten zu haben.

Informationen zu diesem Vorgang

Normalerweise können Sie dies erreichen, indem Sie einem Knoten mehrere Zeitplandefinitionen zuordnen. Dies ist die Standardmethode für die Ausführung mehrerer Zeitpläne auf einem System.

Sie müssen sicherstellen, dass sich die Zeitplanfenster für die einzelnen Zeitpläne nicht überlappen. Ein einzelner Client-Schedulerprozess ist nicht in der Lage, mehrere geplante Aktionen gleichzeitig auszuführen, d. h., bei einer Überlappung wird der zweite zu startende Zeitplan ausgelassen, wenn der erste Zeitplan nicht bis zum Ende des Startfensters des zweiten Zeitplans beendet ist.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAngenommen, die meisten Dateisysteme auf Ihrem Clientsystem müssen täglich und ein Dateisystem mit kritischen Daten muss stündlich gesichert werden. In diesem Fall müssten Sie für die Handhabung dieser Anforderung zwei Zeitpläne definieren. Um einen Konflikt zwischen dem stündlichen und dem täglichen Datensicherungszeitplan zu vermeiden muss die *Startzeit* der beiden Zeitpläne variiert werden.

Windows-BetriebssystemeAngenommen, die meisten Laufwerke auf Ihrem Clientsystem müssen täglich und ein Laufwerk mit kritischen Daten muss stündlich gesichert werden. In diesem Fall müssten Sie für die Handhabung dieser Anforderung zwei Zeitpläne definieren. Um einen Konflikt zwischen dem stündlichen und dem täglichen Datensicherungszeitplan zu vermeiden muss die *Startzeit* der beiden Zeitpläne variiert werden.

In bestimmten Fällen ist es notwendig, mehrere Schedulerprozesse auf einem System auszuführen. Mehrfachprozesse erfordern eine separate Optionsdatei für jeden Prozess und müssen folgende Informationen aufweisen:

- Definieren Sie für jeden Prozess einen eindeutigen Knotennamen.
- Geben Sie für jeden Prozess eindeutige Zeitplan- und Fehlerprotokolle an.
- Im Modus mit Bedienerführung müssen Sie die Option tcpclientport verwenden, um für jeden Prozess einen eindeutigen Anschluss anzugeben.

Windows-BetriebssystemeAnmerkung: Wenn der Scheduler als Dienst ausgeführt wird, überschreiben die Verarbeitungsoptionen, die in der Windows-Registrierung angegeben werden, dieselben Optionen, die in der Clientoptionsdatei angegeben werden.

Die Vorteile bei der Verwendung mehrerer Zeitplanprozesse:

- Sie können mehrere geplante Sicherungen gleichzeitig ausführen.
- Mithilfe der Clientoptionsdatei oder der Überschreibungsoptionen auf dem IBM Spectrum Protect-Server können Sie für jeden gestarteten Zeitplan unterschiedliche Sicherungskriterien angeben.

Die Nachteile bei der Verwendung mehrerer Zeitplanprozesse:

- Für jeden Knotennamen auf dem IBM Spectrum Protect-Server wird ein eindeutiger Dateibereich erstellt.
- Beim Zurückschreiben der Daten müssen Sie denselben Knotennamen verwenden, der der Sicherung zugeordnet ist.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAuf UNIX- und Linux-Plattformen können entweder mit der vom Clientakzeptordämon verwalteten Methode oder mit der traditionellen Methode der Ausführung des

Schedulers mehrere Zeitplanprozesse ausgeführt werden. In beiden Fällen gibt es bestimmte Konfigurationsvoraussetzungen:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

- Jeder Prozess muss mit einem anderen Knotennamen ausgeführt werden.
- Für jeden Schedulerprozess müssen Sie mehrere Zeilengruppen in der Datei dsm.sys erstellen. In jeder Zeilengruppe müssen Sie einen eindeutigen Knotennamen definieren und eindeutige Werte für die Optionen errorlogname und schedlogname angeben. Sie können für jede Zeilengruppe aber auch angepasste domain-, include- und exclude-Anweisungen definieren.
- Setzen Sie in Ihrer Datei dsm.sys die Option passwordaccess in jeder Zeilengruppe auf 'generate'. Das Kennwort muss für jeden Knotennamen, der einen Schedulerprozess ausführt, generiert werden, indem ein Befehl wie z. B.`dsmc query sess` ausgeführt wird.
- Ist bei der Ausführung die Option schedmode auf *prompt* gesetzt, sollten Sie einen eindeutigen tcpclientport-Wert für jede Zeilengruppe definieren.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSie müssen jeden Befehl bzw. jede Instanz `dsmc sched` mit der Option -servername starten, um in dsm.sys auf den eindeutigen Zeilengruppennamen zu verweisen. Bei dsmcad ist es erforderlich, für jede Instanz von dsmcad die Umgebungsvariable DSM_CONFIG zu definieren, um auf die eindeutige Optionsdatei zu verweisen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDas folgende Beispiel zeigt die Konfiguration zweier Zeitplanprozesse, die vom Clientakzeptordämon verwaltet werden, in der Datei dsm.sys. Bitte beachten Sie, dass Sie vollständige Pfadangaben für die Namen der Protokolldateien verwenden müssen, um zu vermeiden, dass die Dateien in das Stammverzeichnis geschrieben werden:

```
servername tsm1_sched1
        nodename        aixsvt01_sched1
        tcpserv         firebat
        tcpclientport    1507
        passwordaccess  generate
        domain          /svt1
        schedmode       prompted
        schedlogname    /tsm/dsmsched1.log
        errorlogname    /tsm/dsmerror1.log
        managedservices schedule

servername tsm1_sched2
  nodename        aixsvt01_sched2
  tcpserv         firebat
  tcpclientport   1508
  passwordaccess  generate
  domain          /svt1
  schedmode       prompted
  schedlogname    /tsm/dsmsched2.log
  errorlogname    /tsm/dsmerror2.log
  managedservices schedule
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeInhalt von /test/dsm.opt1:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
servername tsm1_sched1
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeInhalt von /test/dsm.opt2:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
servername tsm1_sched2
```

Mac OS X-BetriebssystemeÖffnen Sie zwei Shellbefehlsfenster:

Mac OS X-Betriebssysteme

- In Shellbefehlsfenster 1 geben Sie Folgendes ein:

  ```
  export DSM_CONFIG=/test/dsm.opt1
  sudo dsmcad
  ```

- In Shellbefehlsfenster 2 geben Sie Folgendes ein:

  ```
  export DSM_CONFIG=/test/dsm.opt2
  sudo dsmcad
  ```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme**Anmerkung:** Sie sollten diese Befehle in ein Shell-Script eingeben, falls Sie beabsichtigen, die dsmcad-Prozesse direkt von /etc/inittab zu starten, damit die korrekte Variable DSM_CONFIG definiert werden kann, bevor dsmcad gestartet wird.

Windows-BetriebssystemeSie müssen für jeden Zeitplanprozess einen separaten Service erstellen. Wenn Sie den Scheduler mit dem Clientakzeptordämon verwalten, ist für jeden Zeitplan ein Clientakzeptordämonservice und ein Zeitplanungsservice erforderlich. Das folgende Beispiel zeigt die Einstellung zweier Zeitplanprozesse, die vom Clientakzeptordämon verwaltet werden:

```
dsmcutil inst /name:"TSM-Client-Scheduler1"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt1"
/node:tsmcli_sched1 /password:secret /autostart:no /startnow:no

dsmcutil inst CAD /name:"TSM-Clientakzeptor1"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt1"
/cadschedname:"TSM-Client-Scheduler1" /node:tsmcli_sched1 /password:secret
/autostart:yes
dsmcutil inst /name:"TSM-Client-Scheduler2"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt2"
/node:tsmcli_sched2 /password:secret /autostart:no /startnow:no

dsmcutil inst CAD /name:"TSM-Clientakzeptor2"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt2"
/cadschedname:"TSM-Client-Scheduler2" /node:tsmcli_sched2 /password:secret
/autostart:yes
```

 Windows-BetriebssystemeFür jede Zeitplaninstanz sind eindeutige Optionsdateien erforderlich, die zum Zeitpunkt der Serviceerstellung identifiziert werden müssen:

Optionsdatei Nr. 1 (c:\program files\tivoli\tsm\baclient\dsm.opt1)

```
tcps             tsmserv1.example.com
nodename         tsmcli_sched1
passwordaccess   generate
schedlogname     "c:\program files\tivoli\tsm\baclient\dsmsched1.log"
errorlogname     "c:\program files\tivoli\tsm\baclient\dsmerror1.log"
schedmode        prompted
tcpclientport    1507
domain           h:
   managedservices schedule
```

Optionsdatei Nr. 2 (c:\program files\tivoli\tsm\baclient\dsm.opt2)

```
tcps             tsmserv1.example.com
nodename         tsmcli_sched2
passwordaccess   generate
schedlogname     "c:\program files\tivoli\tsm\baclient\dsmsched2.log"
errorlogname     "c:\program files\tivoli\tsm\baclient\dsmerror2.log"
schedmode        prompted
tcpclientport    1508
domain           i:
   managedservices schedule
```

Zugehörige Konzepte:
Vom Scheduler-Service verwendete Verarbeitungsoptionen ändern

Clientrückkehrcodes

Die Befehlszeilenschnittstelle für Sichern/Archivieren und der Scheduler werden mit einem Rückkehrcode verlassen, der den Erfolg oder das Fehlschlagen der Clientoperation genau wiedergibt.

Scripts, Stapeldateien und andere Automatisierungsfunktionen können den Rückkehrcode von der Befehlszeilenschnittstelle aus verwenden. Bei Operationen, bei denen der IBM Spectrum Protect-Scheduler verwendet wird, werden die Rückkehrcodes in der Ausgabe des Verwaltungsbefehls QUERY EVENT angezeigt.

Im Allgemeinen bezieht sich der Rückkehrcode auf die Nachricht mit der höchsten Wertigkeit während der Clientoperation.

- Ist die Nachricht mit der höchsten Wertigkeit eine Informationsnachricht (ANSnnnnI), lautet der Rückkehrcode 0.
- Ist die Nachricht mit der höchsten Wertigkeit eine Warnung (ANSnnnnW), lautet der Rückkehrcode 8.
- Ist die Nachricht mit der höchsten Wertigkeit eine Fehlernachricht (ANSnnnnE oder ANSnnnnS), lautet der Rückkehrcode 12.

Eine Ausnahme von den genannten Regeln tritt auf, wenn Warnungen oder Fehlernachrichten anzeigen, dass einzelne Dateien nicht verarbeitet werden konnten. Der Rückkehrcode für Dateien, die nicht verarbeitet werden können, ist 4. Überprüfen Sie die Datei dsmerror.log, um die Ursache der Fehler festzustellen, die während der Clientoperationen auftreten. Fehler, die während geplanter Ereignisse auftreten, werden in der Datei dsmsched.log aufgezeichnet.

Tabelle 1 enthält eine Beschreibung der Rückkehrcodes und ihrer Bedeutung.

Tabelle 1. Clientrückkehrcodes und ihre Bedeutung

Code	Erläuterung
0	Alle Operationen wurden erfolgreich abgeschlossen.

Code	Erläuterung
4	Die Operation wurde erfolgreich abgeschlossen, einige Dateien wurden jedoch nicht verarbeitet. Es sind keine anderen Fehler oder Warnungen aufgetreten. Dieser Rückkehrcode kommt häufig vor. Dateien werden aus verschiedenen Gründen nicht verarbeitet; die folgende Liste enthält die häufigsten Gründe. • Die Datei entspricht einem Eintrag in einer Ausschlussliste. Ausgeschlossene Dateien generieren Protokolleinträge nur während selektiver Sicherungen. • Die Datei wurde von einer anderen Anwendung verwendet, und der Client konnte nicht auf die Datei zugreifen. • An der Datei wurden während der Operation so viele Änderungen vorgenommen, die aufgrund des Attributs für die Kopiennummerierung nicht zulässig sind. Siehe Attribut 'Kopiennummerierung'.
8	Die Operation wurde mit mindestens einer Warnung abgeschlossen. Bei geplanten Ereignissen lautet der Status `Beendet`. Überprüfen Sie die Datei dsmerror.log (und für geplante Ereignisse die Datei dsmsched.log) auf ausgegebene Warnungen, um ihre Auswirkungen auf die Operation zu bestimmen.
Windows-Betriebssysteme 12	Windows-BetriebssystemeDie Operation wurde mit mindestens einer Fehlernachricht (außer Fehlernachrichten für übersprungene Dateien) abgeschlossen. Bei geplanten Ereignissen lautet der Status `Fehlgeschlagen`. Überprüfen Sie die Datei dsmerror.log (und für geplante Ereignisse die Datei dsmsched.log) auf ausgegebene Fehlernachrichten, um ihre Auswirkungen auf die Operation zu bestimmen. Im Allgemeinen bedeutet dieser Rückkehrcode, dass der Fehler schwerwiegend genug war, um die erfolgreiche Beendigung der Operation zu verhindern. Beispielsweise gibt ein Fehler, der die Verarbeitung eines vollständigen Laufwerks verhindert, den Rückkehrcode 12 aus.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme 12	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie Operation wurde mit mindestens einer Fehlernachricht (außer Fehlernachrichten für übersprungene Dateien) abgeschlossen. Bei geplanten Ereignissen lautet der Status `Fehlgeschlagen`. Überprüfen Sie die Datei dsmerror.log (und für geplante Ereignisse die Datei dsmsched.log) auf ausgegebene Fehlernachrichten, um ihre Auswirkungen auf die Operation zu bestimmen. Im Allgemeinen bedeutet dieser Rückkehrcode, dass der Fehler schwerwiegend genug war, um die erfolgreiche Beendigung der Operation zu verhindern. Beispielsweise gibt ein Fehler, der die Verarbeitung eines vollständigen Dateisystems verhindert, den Rückkehrcode 12 aus.
Sonstige	Bei geplanten Operationen, bei denen ein Befehl ausgeführt wird, wird der Rückkehrcode des ausgeführten Befehls zurückgegeben. Ist der Rückkehrcode 0, lautet der Status der geplanten Operation `Beendet`. Hat der Rückkehrcode einen anderen Wert als 0, lautet der Status `Fehlgeschlagen`. Einige Befehle geben möglicherweise einen anderen Rückkehrcode als Null zurück, wenn die Operation erfolgreich ausgeführt wurde. Für diese Befehle können Sie den Status `Fehlgeschlagen` vermeiden, wenn Sie den Befehl in ein Script *verpacken*, das den Befehl startet, das Ergebnis interpretiert und beendet wird. Das Script sollte den Rückkehrcode 0 ausgeben, wenn der Befehl erfolgreich war, oder einen Rückkehrcode ungleich null, wenn der Befehl fehlgeschlagen ist. Bitten Sie dann Ihren IBM Spectrum Protect-Serveradministrator, die Zeitplandefinition so zu ändern, dass Ihr Script anstelle des Befehls ausgeführt wird.

Der Rückkehrcode für ein Clientmakro ist der höchste der Rückkehrcodes, die für die einzelnen Befehle ausgegeben werden, aus denen das Makro besteht. Ein Makro besteht beispielsweise aus den folgenden Befehlen:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
selective "/home/devel/*" -subdir=yes
incremental "/home/devel/TestDriver/*" -subdir=yes
archive "/home/plan/proj1/*" -subdir=yes
```

Windows-Betriebssysteme

```
selective c:\MyTools\* -subdir=yes
incremental c:\MyPrograms\TestDriver\* -subdir=yes
archive e:\TSM\* -subdir=yes
```

Wenn der erste Befehl mit dem Rückkehrcode 0, der zweite Befehl mit dem Rückkehrcode 8 und der dritte Befehl mit dem Rückkehrcode 4 beendet wird, ist der Rückkehrcode für das Makro 8.

Weitere Informationen zum Befehl QUERY EVENT finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Zugehörige Konzepte:
Zeitplanungsoptionen für Befehle

Speicherverwaltungsmaßnahmen

Speicherverwaltungsmaßnahmen sind vom Administrator definierte Regeln für die Verwaltung der Sicherungen und Archivierungen auf dem Server.

Ihre Daten werden diesen Maßnahmen zugeordnet (oder an sie gebunden); wenn die Daten dann gesichert oder archiviert werden, werden sie gemäß den Maßnahmenbedingungen verwaltet. Zu den Maßnahmekriterien gehören eine Maßnahmendomäne, eine Maßnahmengruppe, eine Verwaltungsklasse und eine Kopiengruppe.

Maßnahmen legen Folgendes fest:

- Ob eine Datei für Sicherungs- oder Archivierungsservices ausgewählt werden kann.
- Wie viele Sicherungsversionen aufbewahrt werden.
- Wie lange inaktive Sicherungsversionen und Archivierungskopien aufbewahrt werden.
- Wo die Kopien im Speicher aufbewahrt werden.
- Für Teilsicherungen legen Maßnahmen außerdem Folgendes fest:
  - Wie oft eine Datei gesichert werden kann.
  - Ob eine Datei geändert werden muss, bevor sie erneut gesichert wird.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeWenn der IBM Spectrum Protect for Space Management-Client installiert ist, definiert Ihr Administrator auch Regeln, die festlegen, ob Dateien für die Umlagerung aus Ihren lokalen Dateisystemen in den Speicher auswählbar sind.

In diesem Abschnitt wird Folgendes erläutert:

- Maßnahmekriterien (Maßnahmendomänen, Maßnahmengruppen, Kopiengruppen und Verwaltungsklassen)
- Wie Maßnahmen angezeigt werden
- Wie Ihre Daten Maßnahmen zugeordnet werden

- Maßnahmendomänen und Maßnahmengruppen
  Eine *Maßnahmendomäne* ist eine Gruppe von Clients mit ähnlichen Sicherungs- und Archivierungsanforderungen.
- Verwaltungsklassen und Kopiengruppen
  Eine *Verwaltungsklasse* ist eine Gruppe von Sicherungs- und Archivierungskopiengruppen, die bestimmte Speicherverwaltungsanforderungen zum Sichern und Archivieren von Daten enthält.
- Informationen zu Verwaltungsklassen und Kopiengruppen anzeigen
  Sie können Maßnahmeninformationen mit der Befehlszeilenschnittstelle oder mit einer grafischen Benutzerschnittstelle anzeigen.
- Verwaltungsklasse für Dateien auswählen
  Entspricht die Standardverwaltungsklasse den Sicherungs- und Archivierungsanforderungen für alle Dateien auf der Workstation des Benutzers, muss der Benutzer die Dateien dieser Verwaltungsklasse nicht zuordnen. Die Zuordnung erfolgt automatisch beim Sichern oder Archivieren der Dateien.
- Dateien eine Verwaltungsklasse zuordnen
  Eine Verwaltungsklasse definiert, wann Dateien bei einer Sicherung berücksichtigt werden, wie lange sie auf dem Server aufbewahrt werden und wie viele Versionen einer Datei der Server aufbewahren soll.
- Verwaltungsklasse für archivierte Dateien überschreiben
  Wenn Sie eine Datei archivieren, können Sie die zugeordnete Verwaltungsklasse mit der grafischen Benutzerschnittstelle (GUI) überschreiben oder indem Sie die Option archmc im Befehl archive verwenden.
- Verwaltungsklasse für Verzeichnisse auswählen
  Entspricht die Verwaltungsklasse in Ihrer aktiven Maßnahmengruppe mit der längsten Einstellung für "Einzige Version aufbewahren" (RETONLY) Ihren Sicherungsanforderungen für Verzeichnisse, ist es möglicherweise nicht notwendig, dieser Verwaltungsklasse Verzeichnisse zuzuordnen. Die Zuordnung der Verwaltungsklasse erfolgt automatisch bei der Sicherung Ihrer Verzeichnisse.
- Verwaltungsklassen an Dateien binden
  Durch das *Binden* wird eine Datei einer Verwaltungsklasse zugeordnet.
- Sicherungsversionen von Dateien erneut binden
  Beim *erneuten Binden* wird eine Datei oder das Image eines logischen Datenträgers einer neuen Verwaltungsklasse zugeordnet.
- Aufbewahrungszeitraum
  IBM Spectrum Protect stellt einen *Aufbewahrungszeitraum für Sicherung* und einen *Aufbewahrungszeitraum für Archivierung* zur Verfügung, die die Sicherungs- und Archivierungsdaten schützen sollen, wenn es eine Datei nicht erneut an eine geeignete Verwaltungsklasse binden kann.
- Ereignisgesteuerte Maßnahme für Aufbewahrungsschutz
  Alle Verwaltungsklassen mit einer Archivierungskopiengruppe müssen einen Aufbewahrungszeitraum angeben, z. B. die Anzahl Tage, die ein archiviertes Objekt auf dem Server gespeichert wird, bevor es gelöscht wird.

Maßnahmendomänen und Maßnahmengruppen

Eine *Maßnahmendomäne* ist eine Gruppe von Clients mit ähnlichen Sicherungs- und Archivierungsanforderungen.

Maßnahmendomänen enthalten eine oder mehrere Maßnahmengruppen. Ein Administrator verwendet Maßnahmendomänen für die logische Verwaltung einer Gruppe von Clientknoten.

Eine Maßnahmendomäne kann beispielsweise Folgendes enthalten:

- Eine Abteilung, z. B. Buchhaltung.
- Einen physischen Standort, wie z. B. ein bestimmtes Gebäude oder Stockwerk.
- Ein lokales Netz, wie z. B. alle Clients, die einem bestimmten Dateiserver zugeordnet sind.

IBM Spectrum Protect enthält eine Standardmaßnahmendomäne mit dem Namen *Standard*. Der Clientknoten ist am Anfang eventuell der Standardmaßnahmendomäne zugeordnet. Der Administrator kann jedoch zusätzliche Maßnahmendomänen definieren, wenn weitere Benutzergruppen mit eindeutigen Sicherungs- und Archivierungsanforderungen vorhanden sind.

Eine *Maßnahmengruppe* besteht aus mindestens einer Verwaltungsklasse. Eine Maßnahmendomäne kann viele Maßnahmengruppen enthalten. Der Administrator verwendet eine Maßnahmengruppe, um verschiedene Verwaltungsklassen auf der Basis von Geschäfts- und Benutzeranforderungen zu implementieren. Es kann nur jeweils eine Maßnahmengruppe aktiv sein. Sie wird als *aktive Maßnahmengruppe* bezeichnet. Jede Maßnahmengruppe enthält eine *Standardverwaltungsklasse* und eine beliebige Anzahl zusätzlicher Verwaltungsklassen.

Verwaltungsklassen und Kopiengruppen

Eine *Verwaltungsklasse* ist eine Gruppe von Sicherungs- und Archivierungskopiengruppen, die bestimmte Speicherverwaltungsanforderungen zum Sichern und Archivieren von Daten enthält.

Ein Administrator kann separate Verwaltungsklassen für die Sicherungs- und Archivierungsanforderungen unterschiedlicher Daten definieren, wie z. B.:

- Geschäftskritische Systemdaten
- Anwendungsdaten, die sich häufig ändern
- Berichtsdaten, die monatlich über die Verwaltung überprüft werden
- Rechtliche Hinweise, die ohne zeitliche Begrenzung aufbewahrt werden müssen und viel Plattenspeicherplatz erfordern

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAnmerkung: Wenn IBM Spectrum Protect for Space Management installiert ist, können auch spezifische Anforderungen für die Umlagerung von Dateien in Speicher enthalten sein.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme Die meisten Änderungen von Speicherverwaltungsmaßnahmen betreffen Verwaltungsklassen. Alle Dateien und Verzeichnisse, die Sie sichern, und alle Dateien, die Sie archivieren, sind wie folgt einer Verwaltungsklasse zugeordnet (oder an sie *gebunden*):

- Sind Ihre Daten keiner Verwaltungsklasse zugeordnet, verwendet IBM Spectrum Protect die Standardverwaltungsklasse in der aktiven Maßnahmengruppe.
- Beim Sichern von Verzeichnissen können Sie eine Verwaltungsklasse mit einer Anweisung *include* oder mit der Option dirmc angeben. Wird keine Verwaltungsklasse angegeben, verwendet IBM Spectrum Protect diejenige Verwaltungsklasse in der aktiven Maßnahmengruppe, die die längste Aufbewahrungsdauer für einzige Version angibt. Erfüllen mehrere Verwaltungsklassen dieses Kriterium, verwendet IBM Spectrum Protect die letzte gefundene Verwaltungsklasse in alphabetischer Reihenfolge.
- Für das Archivieren von Verzeichnissen können Sie eine Verwaltungsklasse mit der Anweisung *include.archive* oder mit der Option archmc angeben. Wird keine Verwaltungsklasse angegeben, ordnet der Server dem Archivierungverzeichnis die Standardverwaltungsklasse zu. Hat die Standardverwaltungsklasse keine Archivierungskopiengruppe, ordnet der Server die Verwaltungsklasse zu, die derzeit über die Archivierungskopiengruppe mit dem kürzesten Aufbewahrungszeitraum verfügt.

Sie können *include*-Anweisungen in Ihrer Einschluss-/Ausschlussliste verwenden, um Dateien Verwaltungsklassen zuzuordnen. In Ihrer Clientoptionsdatei können Sie mit der Option dirmc Verzeichnisse einer Verwaltungsklasse zuordnen.

Innerhalb einer Verwaltungsklasse befinden sich die spezifischen Sicherungs- und Archivierungsanforderungen in den *Kopiengruppen*. Kopiengruppen definieren die spezifischen Speicherverwaltungsattribute, die beschreiben, wie der Server gesicherte oder archivierte Daten verwaltet. Zu den Kopiengruppen gehören *Sicherungskopiengruppen* und *Archivierungskopiengruppen*. Eine Verwaltungsklasse kann eine Sicherungskopiengruppe und/oder eine Archivierungskopiengruppe oder keine Kopiengruppe enthalten.

Eine *Sicherungskopiengruppe* enthält Attribute, mit denen während der Sicherung Folgendes bestimmt wird:

- Wie viele Tage vergehen müssen, bis eine Datei wieder gesichert wird.
- Wie eine Datei während einer Sicherung verarbeitet wird, wenn sie im Gebrauch ist.

Sie enthält außerdem Attribute, mit denen die Sicherungsversionen der Dateien auf dem Server verwaltet werden. Diese Attribute steuern Folgendes:

- Auf welchem Datenträgertyp der Server Sicherungsversionen Ihrer Dateien und Verzeichnisse speichert.
- Wie viele Sicherungsversionen Ihrer Dateien und Verzeichnisse der Server aufbewahrt.
- Wie lange der Server Sicherungsversionen Ihrer Dateien und Verzeichnisse aufbewahrt.
- Wie lange der Server inaktive Sicherungsversionen aufbewahrt.
- Wie lange die letzte verbliebene inaktive Version einer Datei aufbewahrt wird.

Eine *Archivierungskopiengruppe* enthält Attribute, die Folgendes steuern:

- Ob eine Datei archiviert wird, die im Gebrauch ist.
- Auf welchem Datenträgertyp der Server Archivierungskopien Ihrer Dateien speichert.
- Wie lange der Server Archivierungskopien der Dateien aufbewahrt.

Zugehörige Konzepte:
Verwaltungsklasse für Dateien auswählen
Aufbewahrungszeitraum

Informationen zu Verwaltungsklassen und Kopiengruppen anzeigen

Sie können Maßnahmeninformationen mit der Befehlszeilenschnittstelle oder mit einer grafischen Benutzerschnittstelle anzeigen.

Klicken Sie in einer grafischen Benutzerschnittstelle auf **Maßnahmeninformationen anzeigen** im Menü 'Dienstprogramme'. Im Fenster **Maßnahmeninformationen** werden die verfügbaren Verwaltungsklassen angezeigt. In einer Befehlszeile verwenden Sie den Befehl query mgmtclass, um die verfügbaren Verwaltungsklassen anzuzeigen. Mit der Option detail erhalten Sie weitere Informationen.

Tabelle 1 zeigt die Standardwerte für die Sicherungs- und Archivierungskopiengruppen in der Standardverwaltungsklasse.

Tabelle 1. Standardattributwerte in der Standardverwaltungsklasse

Attribut	**Standardwert für Sicherung**	**Standardwert für Archivierung**
Name der Kopiengruppe	Standard	Standard
Kopienart	Sichern	Archivieren
Kopienhäufigkeit	0 Tage	CMD (Befehl)
Versionen bestehender Daten	2 Versionen	Nicht zutreffend
Versionen gelöschter Daten	1 Version	Nicht zutreffend
Extraversionen aufbewahren	30 Tage	Nicht zutreffend
Einzige Version aufbewahren	60 Tage	Nicht zutreffend
Kopiennummerierung	Gemeinsam statisch	Gemeinsam statisch
Kopienmodus	Geändert	Absolut
Kopienziel	Backuppool	Archivepool
Version aufbewahren	Nicht zutreffend	365 Tage
LAN-unabhängig	Ziel	No
Deduplizierung aktiviert	No	No

- Attribut 'Kopiengruppenname'
  Das Attribut *Kopiengruppenname* ist der Name der Kopiengruppe. Der Standardwert für die Sicherung und Archivierung ist *Standard*.
- Attribut 'Kopienart'
  Das Attribut *Kopienart* ist die Art der Kopiengruppe. Der Wert für Sicherungen lautet immer *Sichern*, der Wert für Archivierungen immer *Archivieren*.
- Attribut 'Kopienhäufigkeit'
  Das Attribut *Kopienhäufigkeit* ist die Mindestanzahl Tage, die zwischen aufeinanderfolgenden Teilsicherungen vergehen muss. Verwenden Sie dieses Attribut während einer vollständigen Teilsicherung.
- Attribut 'Versionen bestehender Daten'
  Das Attribut *Versionen bestehender Daten* gibt die maximale Anzahl verschiedener Sicherungsversionen an, die für Dateien und Verzeichnisse aufbewahrt werden.
- Attribut 'Versionen gelöschter Daten'
  Das Attribut *Versionen gelöschter Daten* gibt die maximale Anzahl verschiedener Sicherungsversionen an, die für gelöschte Dateien und Verzeichnisse aufbewahrt werden.
- Attribut 'Extraversionen aufbewahren'
  Das Attribut *Extraversionen aufbewahren* gibt an, wie viele Tage alle Sicherungsversionen außer der aktuellsten Sicherungsversion aufbewahrt werden.
- Attribut 'Einzige Version aufbewahren'
  Das Attribut *Einzige Version aufbewahren* gibt die Anzahl Tage an, während der die letzte inaktive Version einer Datei oder eines Verzeichnisses aufbewahrt wird.
- Attribut 'Kopiennummerierung'
  Das Attribut Kopiennummerierung legt fest, ob eine Datei während einer Sicherung oder Archivierung im Gebrauch sein kann und welche Maßnahmen zu ergreifen sind, wenn dies der Fall ist.
- Parameter für den Kopienmodus
  Der Parameter für den Kopienmodus legt fest, ob eine Datei oder ein Verzeichnis für die Teilsicherung unabhängig davon berücksichtigt wird, ob sie bzw. es sich seit der letzten Sicherung geändert hat.
- Attribut 'Kopienziel'
  Das Attribut *Kopienziel* gibt das Ziel an, an dem Sicherungen oder Archivierungen gespeichert werden.
- Attribut 'Version aufbewahren'
  Das Attribut *Version aufbewahren* gibt die Anzahl Tage an, die eine archivierte Datei im Speicher aufbewahrt wird.
- Attribut 'Daten deduplizieren'
  Das Attribut *Daten deduplizieren* gibt an, ob während der Sicherungs- und Archivierungsverarbeitung redundante Daten an den IBM Spectrum Protect-Server übertragen werden.

Attribut 'Kopiengruppenname'

Das Attribut *Kopiengruppenname* ist der Name der Kopiengruppe. Der Standardwert für die Sicherung und Archivierung ist *Standard*.

Attribut 'Kopienart'

Das Attribut *Kopienart* ist die Art der Kopiengruppe. Der Wert für Sicherungen lautet immer *Sichern*, der Wert für Archivierungen immer *Archivieren*.

Attribut 'Kopienhäufigkeit'

Das Attribut *Kopienhäufigkeit* ist die Mindestanzahl Tage, die zwischen aufeinanderfolgenden Teilsicherungen vergehen muss. Verwenden Sie dieses Attribut während einer vollständigen Teilsicherung.

Die Kopienhäufigkeit arbeitet mit dem Parameter mode zusammen. Gelten beispielsweise `frequency=0` und `mode=modified`, wird eine Datei oder ein Verzeichnis nur gesichert, wenn sie bzw. es sich seit der letzten Teilsicherung geändert hat. Gelten `frequency=0` und `mode=absolute`, wird ein Objekt bei jeder Teilsicherung gesichert. Gelten `frequency=0` und `mode=absolute`, haben Änderungen und die Anzahl Tage seit der letzten Sicherung keinen Einfluss auf die aktuelle Sicherungsoperation. Das Attribut für die Häufigkeit (frequency) wird bei selektiven Sicherungen nicht überprüft.

Bei Archivierungskopiengruppen lautet die Einstellung für die Kopienhäufigkeit immer CMD (Befehl). Beim Archivieren eines Objekts gibt es keine Einschränkungen bezüglich der Häufigkeit.

 AIX-Betriebssysteme  Windows-BetriebssystemeBei einer journalbasierten Sicherung wird die Kopienhäufigkeit ignoriert.

 Windows-Betriebssysteme Journalbasierte Teilsicherungen unterscheiden sich von traditionellen vollständigen Teilsicherungen, weil IBM Spectrum Protect keine nicht standardmäßigen Kopienhäufigkeiten (außer 0) erzwingt.

Attribut 'Versionen bestehender Daten'

Das Attribut *Versionen bestehender Daten* gibt die maximale Anzahl verschiedener Sicherungsversionen an, die für Dateien und Verzeichnisse aufbewahrt werden.

Wird eine Verwaltungsklasse ausgewählt, die mehrere Sicherungsversionen zulässt, wird die aktuellste Version als *aktive* Version bezeichnet. Alle anderen Versionen werden als *inaktive* Versionen bezeichnet. Beträgt die maximal zulässige Anzahl der Versionen 5 und wird bei einer Sicherung eine sechste Version erstellt, wird die älteste Version aus dem Serverspeicher gelöscht.

Attribut 'Versionen gelöschter Daten'

Das Attribut *Versionen gelöschter Daten* gibt die maximale Anzahl verschiedener Sicherungsversionen an, die für gelöschte Dateien und Verzeichnisse aufbewahrt werden.

Dieser Parameter wird ignoriert, bis Sie die Datei oder das Verzeichnis löschen.

Wenn Sie die Datei oder das Verzeichnis löschen, wird die aktive Sicherungsversion bei der nächsten Teilsicherung zu einer inaktiven Version. Der IBM Spectrum Protect-Server löscht die ältesten Versionen, die die durch diesen Parameter angegebene Anzahl überschreiten.

Das Verfallsdatum für die übrigen Versionen richtet sich nach den Parametern *Extraversionen aufbewahren* und *Einzige Version aufbewahren*.

Attribut 'Extraversionen aufbewahren'

Das Attribut *Extraversionen aufbewahren* gibt an, wie viele Tage alle Sicherungsversionen außer der aktuellsten Sicherungsversion aufbewahrt werden.

Die aktuellste Version ist die aktive Version, die nie gelöscht wird. Wird *Keine Begrenzung* angegeben, werden Extraversionen aufbewahrt, bis die Anzahl der Sicherungsversionen den Wert des Parameters *Versionen bestehender Daten* oder *Versionen gelöschter Daten* überschreitet. In diesem Fall wird die älteste Extraversion sofort gelöscht.

Attribut 'Einzige Version aufbewahren'

Das Attribut *Einzige Version aufbewahren* gibt die Anzahl Tage an, während der die letzte inaktive Version einer Datei oder eines Verzeichnisses aufbewahrt wird.

Wird *Keine Begrenzung* angegeben, wird die letzte Version unbegrenzt aufbewahrt.

Nach dem Löschen einer Datei aus dem Clientsystem wird dieser Parameter bei der nächsten Teilsicherung wirksam. Alle nachfolgenden Aktualisierungen dieses Parameters wirken sich nicht auf Dateien aus, die bereits inaktiv sind. Beispiel: Ist dieser Parameter auf 10 Tage gesetzt, wenn eine Datei während einer Teilsicherung inaktiviert wird, wird die Datei nach 10 Tagen vom Server gelöscht.

Attribut 'Kopiennummerierung'

Das Attribut Kopiennummerierung legt fest, ob eine Datei während einer Sicherung oder Archivierung im Gebrauch sein kann und welche Maßnahmen zu ergreifen sind, wenn dies der Fall ist.

Dieses Attribut kann einen der folgenden Werte aufweisen:

- Statisch. Eine Datei oder ein Verzeichnis darf während einer Sicherung oder Archivierung nicht geändert werden. Wird das Objekt während eines Sicherungs- oder Archivierungsversuchs geändert, wird es nicht gesichert oder archiviert.
- Gemeinsam statisch. Eine Datei oder ein Verzeichnis darf während der Sicherung oder Archivierung nicht geändert werden. Der Client wiederholt einen Sicherungs- oder Archivierungsversuch abhängig von dem für die Option changingretries in Ihrer Optionsdatei angegebenen Wert maximal vier Mal. Wird das Objekt bei jedem Sicherungs- oder Archivierungsversuch geändert, wird es nicht gesichert oder archiviert.
- Dynamisch. Eine Datei oder ein Verzeichnis wird beim ersten Versuch gesichert oder archiviert, auch wenn sie bzw. es sich während der Sicherung oder Archivierung ändert.
- Gemeinsam dynamisch. Eine Datei oder ein Verzeichnis wird gesichert oder archiviert, auch wenn sie bzw. es sich während der Sicherung oder Archivierung ändert. Der Client wiederholt einen Sicherungs- oder Archivierungsversuch maximal vier mal. Die Anzahl der Versuche ist von dem Wert abhängig, der für die Option changingretries in Ihrer Optionsdatei angegeben ist. Die Datei wird beim letzten Versuch gesichert oder archiviert, auch wenn sie sich ändert.

  Bei einer Verwaltungsklasse, die die Sicherung oder Archivierung einer im Gebrauch befindlichen Datei gestattet, wird die Sicherungsversion oder Archivierungskopie im Serverspeicher möglicherweise als Kopie mit grober Übereinstimmung gespeichert. Eine *Kopie mit grober Übereinstimmung* ist eine Sicherungsversion oder Archivierungskopie, die den aktuellen Inhalt einer Datei nicht korrekt wiedergibt. Sie kann einige, jedoch nicht alle Änderungen enthalten. Ist dies nicht akzeptabel, muss eine Verwaltungsklasse ausgewählt werden, die eine Sicherungsversion oder Archivierungskopie nur dann erstellt, wenn sich die Datei während der Sicherung oder Archivierung nicht ändert. Wenn Sie die statische Durchnummerierung verwenden, können Anwendungen eine Datei nicht mit Schreibzugriff öffnen, während die Datei gesichert wird.

  Wird eine Dateikopie mit grober Übereinstimmung zurückgeschrieben oder abgerufen, ist die Datei möglicherweise unbrauchbar. Sie sollten die Durchnummerierung "Dynamisch" oder "Gemeinsam dynamisch" beim Sichern von Dateien nur verwenden, wenn Sie sicher sind, dass die Zurückschreibung der Kopie mit grober Übereinstimmung verwendbar ist.

  Wichtig: Bei der Auswahl einer Verwaltungsklasse, die eine Kopiengruppe mit der Durchnummerierung "Gemeinsam dynamisch" oder "Dynamisch" enthält, muss mit besonderer Vorsicht vorgegangen werden.

Zugehörige Konzepte:
Windows-BetriebssystemeUnterstützung offener Dateien für Sicherungsoperationen
Zugehörige Tasks:
Windows-BetriebssystemeUnterstützung offener Dateien konfigurieren
Zugehörige Verweise:
Snapshotproviderimage

Parameter für den Kopienmodus

Der Parameter für den Kopienmodus legt fest, ob eine Datei oder ein Verzeichnis für die Teilsicherung unabhängig davon berücksichtigt wird, ob sie bzw. es sich seit der letzten Sicherung geändert hat.

Bei der Ausführung selektiver Sicherungen überprüft der Client den Parameter für den Modus nicht.

Der Wert für diesen Parameter kann eine der folgenden Einstellungen sein:

geändert
: Das Objekt wird bei der Teilsicherung nur dann berücksichtigt, wenn es sich seit der letzten Sicherung geändert hat. Ein Objekt wird als geändert betrachtet, wenn eine der folgenden Bedingungen zutrifft:

  - Abweichung des Datums oder der Uhrzeit der letzten Änderung.
  - Größenabweichung.
  - Windows-BetriebssystemeAbweichung der Attribute, mit Ausnahme des Archivierungsattributs.
  - Wenn sich nur die Metadaten (wie beispielsweise Zugriffsberechtigungen) ändern, sichert der Client unter Umständen nur die Metadaten.
  - AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Eignerabweichung.

absolut
: Das Objekt wird bei der Teilsicherung berücksichtigt, unabhängig davon, ob es sich seit der letzten Sicherung geändert hat. Bei Archivierungskopiengruppen lautet der Modus immer Absolut, d. h., ein Objekt wird unabhängig davon archiviert, ob es sich seit der letzten Archivierungsanforderung geändert hat.

Attribut 'Kopienziel'

Das Attribut *Kopienziel* gibt das Ziel an, an dem Sicherungen oder Archivierungen gespeichert werden.

Das Ziel kann ein Speicherpool mit Platteneinheiten oder ein Speicherpool mit Einheiten, die austauschbare Datenträger (z. B. Band) unterstützen, sein.

Attribut 'Version aufbewahren'

Das Attribut *Version aufbewahren* gibt die Anzahl Tage an, die eine archivierte Datei im Speicher aufbewahrt wird.

Nach Ablauf der angegebenen Anzahl an Tagen für die archivierte Kopie einer Datei wird sie aus dem Serverspeicher gelöscht.

Attribut 'Daten deduplizieren'

Das Attribut *Daten deduplizieren* gibt an, ob während der Sicherungs- und Archivierungsverarbeitung redundante Daten an den IBM Spectrum Protect-Server übertragen werden.

Zugehörige Konzepte:
Clientseitige Datendeduplizierung
Zugehörige Verweise:
Deduplication
Enablededupcache
Ausschlussoptionen

Verwaltungsklasse für Dateien auswählen

Entspricht die Standardverwaltungsklasse den Sicherungs- und Archivierungsanforderungen für alle Dateien auf der Workstation des Benutzers, muss der Benutzer die Dateien dieser Verwaltungsklasse nicht zuordnen. Die Zuordnung erfolgt automatisch beim Sichern oder Archivieren der Dateien.

Wenn für Dateien eine andere Verwaltungsklasse ausgewählt wird, müssen folgende Fragen beachtet werden:

- Enthält die Verwaltungsklasse eine Sicherungskopiengruppe?

  Wird versucht, eine Datei zu sichern, die einer Verwaltungsklasse ohne Sicherungskopiengruppe zugeordnet ist, wird die Datei nicht gesichert.

- Enthält die Verwaltungsklasse eine Archivierungskopiengruppe?

  Es ist nicht möglich, eine Datei zu archivieren, die einer Verwaltungsklasse ohne Archivierungskopiengruppe zugeordnet ist.

- Enthält die Sicherungskopiengruppe Attribute, die eine ausreichend häufige Sicherung der Dateien gewährleisten?

  Kopienmodus und -häufigkeit legen gemeinsam fest, wie oft eine Datei bei Teilsicherungen gesichert wird. Diese Attribute werden bei einer selektiven Sicherung nicht überprüft.

- Welche Nummerierungsmethode wird von der Kopiengruppe verwendet?

  Die Nummerierungsmethode bestimmt das Verhalten von IBM Spectrum Protect, wenn sich eine Datei während ihrer Sicherung ändert.

- Sind in der Sicherungskopiengruppe eine angemessene Anzahl Sicherungsversionen angegeben?
- Ist in der Archivierungskopiengruppe ein angemessener Aufbewahrungszeitraum für Archivierungskopien angegeben?

Zugehörige Konzepte:
Attribut 'Kopiennummerierung'

Dateien eine Verwaltungsklasse zuordnen

Eine Verwaltungsklasse definiert, wann Dateien bei einer Sicherung berücksichtigt werden, wie lange sie auf dem Server aufbewahrt werden und wie viele Versionen einer Datei der Server aufbewahren soll.

Der Serveradministrator wählt eine Standardverwaltungsklasse aus. Der Benutzer kann eine eigene Verwaltungsklasse angeben, um die Standardverwaltungsklasse außer Kraft zu setzen.

Soll Verzeichnissen eine andere Verwaltungsklasse als die Standardverwaltungsklasse zugeordnet werden, verwenden Sie die Option dirmc in Ihrer Optionsdatei.

Sie können eine Verwaltungsklasse für eine Datei oder Dateigruppe zuordnen, indem Sie eine Anweisung include in Ihrer Optionsdatei verwenden. Sie können auch eine Verwaltungsklasse zuordnen, indem Sie eine Anweisung include in der Einschluss-/Ausschlussdatei verwenden, die durch die Option inclexcl angegeben ist. Bei dem Namen der Verwaltungsklasse muss die Groß-/Kleinschreibung nicht berücksichtigt werden.

Soll mithilfe des Befehlszeilenclients allen Dateien im Verzeichnis `costs` die Verwaltungsklasse `budget` zugeordnet werden, geben Sie Folgendes ein:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

```
include /home/proj2/costs/* budget
```

 Windows-Betriebssysteme

```
include c:\adsm\proj2\costs\* budget
```

Soll eine Verwaltungsklasse mit dem Namen `managall` angegeben werden, die für alle Dateien verwendet werden soll, denen Sie nicht explizit eine Verwaltungsklasse zuordnen, geben Sie Folgendes ein:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

```
include /.../* managall
```

 Windows-Betriebssysteme

```
include ?:\...\* managall
```

Die folgenden Beispiele zeigen, wie Dateien eine Verwaltungsklasse zugeordnet wird:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
exclude /.../*.sno
include /home/winter/.../*.ice      mcweekly
include /home/winter/december/*.ice mcdaily
include /home/winter/january/*.ice  mcmonthly
include /home/winter/february/white.sno
```

 Windows-Betriebssysteme

```
exclude ?:\...\*.sno
include c:\winter\...\*.ice      mcweekly
include c:\winter\december\*.ice mcdaily
include c:\winter\january\*.ice  mcmonthly
include c:\winter\february\white.sno
```

Folgende Verarbeitungsschritte werden durchgeführt:

1. Die Datei white.sno im Verzeichnis february im Verzeichnis winter wird gemäß den folgenden Regeln für die Verarbeitung von unten nach oben gesichert. Da Sie in dieser Anweisung keine Verwaltungsklasse angegeben haben, wird der Datei die Standardverwaltungsklasse zugeordnet.
2. Allen Dateien mit der Erweiterung `ice` im Verzeichnis january wird die Verwaltungsklasse `mcmonthly` zugeordnet.
3. Allen Dateien mit der Erweiterung `ice` im Verzeichnis december wird die Verwaltungsklasse `mcdaily` zugeordnet.
4. Allen übrigen Dateien mit der Erweiterung `ice` in einem beliebigen Verzeichnis unter dem Verzeichnis winter wird die Verwaltungsklasse `mcweekly` zugeordnet.
5. Alle Dateien mit der Erweiterung `sno` in allen Verzeichnissen werden von der Sicherung ausgeschlossen. Die Ausnahme zu dieser Regel ist white.sno im Verzeichnis february, das sich im Verzeichnis winter befindet.

Soll eine eigene Standardverwaltungsklasse `Verwaltungsklassenname` für Dateien angegeben werden, die nicht explizit eingeschlossen werden, stellen Sie die folgende Anweisung an den Anfang Ihrer Einschlussliste:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

```
include /.../* Verwaltungsklassenname
```

 Windows-Betriebssysteme

```
include ?:\...\* Verwaltungsklassenname
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeWenn eine Datei mithilfe der grafischen Benutzerschnittstelle archiviert wird, kann eine andere Verwaltungsklasse ausgewählt werden, um die der Datei zugeordnete Verwaltungsklasse außer Kraft zu setzen.

Zugehörige Verweise:
Dirmc
Einschlussoptionen

Verwaltungsklasse für archivierte Dateien überschreiben

Wenn Sie eine Datei archivieren, können Sie die zugeordnete Verwaltungsklasse mit der grafischen Benutzerschnittstelle (GUI) überschreiben oder indem Sie die Option archmc im Befehl archive verwenden.

Die Überschreibung der Verwaltungsklasse mit der GUI ist äquivalent zu der Verwendung der Option archmc im Befehl archive. In der grafischen Benutzerschnittstelle müssen Sie die Schaltfläche **Optionen** in der Archivierungsbaumstruktur drücken, um die Verwaltungsklasse zu überschreiben und eine andere Verwaltungsklasse auszuwählen.

Geben Sie in der Befehlszeile den folgenden Befehl ein, um der Datei `budget.jan` die Verwaltungsklasse **ret2yrs** zuzuordnen:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

```
dsmc archive -archmc=ret2yrs /home/jones/budget.jan
```

 Windows-Betriebssysteme

```
dsmc archive -archmc=ret2yrs c:\plan\proj1\budget.jan
```

Verwaltungsklasse für Verzeichnisse auswählen

Entspricht die Verwaltungsklasse in Ihrer aktiven Maßnahmengruppe mit der längsten Einstellung für "Einzige Version aufbewahren" (RETONLY) Ihren Sicherungsanforderungen für Verzeichnisse, ist es möglicherweise nicht notwendig, dieser Verwaltungsklasse Verzeichnisse zuzuordnen. Die Zuordnung der Verwaltungsklasse erfolgt automatisch bei der Sicherung Ihrer Verzeichnisse.

Wenn mehrere Verwaltungsklassen mit der längsten Einstellung für RETONLY vorhanden sind, wählt der IBM Spectrum Protect-Client die Verwaltungsklasse aus, deren Name in alphabetischer Reihenfolge an letzter Stelle steht.

Entspricht die Standardverwaltungsklasse nicht Ihren Anforderungen, müssen Sie eine Verwaltungsklasse mit einem angemessenen Aufbewahrungszeitraum auswählen, der durch den Parameter Einzige Version aufbewahren angegeben wird. Beispiel: Wenn die Verwaltungsklasse Daten direkt auf Band sichert, Sie aber Ihre Verzeichnissicherungen auf Platte haben möchten, müssen Sie eine andere Verwaltungsklasse auswählen. Verzeichnisse sollten Sie mindestens so lange aufbewahren wie die Dateien, die diesen Verzeichnissen zugeordnet sind.

Verwenden Sie für Sicherungsverzeichnisse die Option dirmc, um die Verwaltungsklasse anzugeben, an die die Verzeichnisse gebunden werden.

Verwenden Sie für Archivierungsverzeichnisse die Option archmc im Befehl archive.

Sie können die folgenden Methoden verwenden, um die verfügbaren Verwaltungsklassen und deren Attribute anzuzeigen:

- GUI- oder Web-Client: Wählen Sie Maßnahmeninformationen anzeigen im Menü Dienstprogramme aus.
- Befehlszeilenclient: Führen Sie den Befehl `dsmc query mgmtclass -detail` aus.

Anmerkung: Wenn während der Verfallsverarbeitung auf dem IBM Spectrum Protect-Server ein archiviertes Verzeichnis für den Verfall auswählbar ist, prüft der Server, ob es für vorhandene archivierte Dateien erforderlich ist, dass das archivierte Verzeichnis bestehen bleibt. Ist dies der Fall, verfällt das archivierte Verzeichnis nicht und der Client für Sichern/Archivieren aktualisiert das Einfügedatum im archivierten Verzeichnis, um sicherzustellen, dass das Verzeichnis nicht verfällt, bevor die Dateien in ihm verfallen.

Verwaltungsklassen an Dateien binden

Durch das *Binden* wird eine Datei einer Verwaltungsklasse zugeordnet.

Wenn eine Datei zum ersten Mal gesichert wird, bindet sie IBM Spectrum Protect entweder an die Standardverwaltungsklasse oder an die in der Einschluss-/Ausschlussliste angegebene Verwaltungsklasse.

Wenn die Sicherungskopiengruppe der Verwaltungsklasse die Aufbewahrung mehrerer Sicherungsversionen der Datei angibt und wenn mehrere Sicherungen angefordert werden, verfügt der Server immer über eine aktive Sicherungsversion (die aktuelle Version) und mindestens eine inaktive Sicherungsversion der Datei. Alle Sicherungsversionen einer Datei werden an dieselbe Verwaltungsklasse gebunden und gemäß den Attributen in der Sicherungskopiengruppe verwaltet.

Wenn eine Datei zum ersten Mal archiviert wird, bindet sie IBM Spectrum Protect an die Standardverwaltungsklasse, an die in der Einschluss-/Ausschlussliste angegebene Verwaltungsklasse oder an eine Verwaltungsklasse, die angegeben wird, wenn die Archivierungsoptionen während einer Archivierung geändert werden.

Archivierte Dateien werden nicht erneut an eine andere Verwaltungsklasse gebunden. Wenn Sie die Verwaltungsklasse für eine Datei mit einer Anweisung include.archive, mit der Option archmc oder über die GUI des Clients für Sichern/Archivieren ändern, bleiben zuvor archivierte Kopien der Datei an die Verwaltungsklasse gebunden, die bei ihrer Archivierung angegeben wurde.

Wird eine Datei auf dem Clientsystem gelöscht, werden die inaktiven Objekte dieser Datei nicht erneut gebunden.

Informationen zur Zuordnung von Dateien und Verzeichnissen zu Verwaltungsklassen finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Sicherungsversionen von Dateien erneut binden

Beim *erneuten Binden* wird eine Datei oder das Image eines logischen Datenträgers einer neuen Verwaltungsklasse zugeordnet.

Sicherungsversionen von Dateien werden unter folgenden Bedingungen erneut an eine andere Verwaltungsklasse gebunden. In jedem Fall werden die Dateien (aktive und inaktive) erst bei der nächsten Sicherung erneut gebunden.

- Um die Verwaltungsklasse einer Datei zu ändern, wird eine andere Verwaltungsklasse in einer Include-Anweisung angegeben. Die Sicherungen werden gemäß der alten Verwaltungsklasse verwaltet, bis eine neue Sicherung durchgeführt wird.
- Der Administrator löscht die Verwaltungsklasse aus der aktiven Maßnahmengruppe des Benutzers. Die Standardverwaltungsklasse wird zum Verwalten der Sicherungsversionen verwendet, wenn die Datei erneut gesichert wird.
- Der Administrator ordnet den Clientknoten einer anderen Maßnahmendomäne zu, deren aktive Maßnahmengruppe keine Verwaltungsklasse mit demselben Namen enthält. Die Standardverwaltungsklasse für die neue Maßnahmendomäne wird zum Verwalten der Sicherungsversionen verwendet.

Informationen zur Zuordnung von Dateien und Verzeichnissen zu Verwaltungsklassen finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

Aufbewahrungszeitraum

IBM Spectrum Protect stellt einen *Aufbewahrungszeitraum für Sicherung* und einen *Aufbewahrungszeitraum für Archivierung* zur Verfügung, die die Sicherungs- und Archivierungsdaten schützen sollen, wenn es eine Datei nicht erneut an eine geeignete Verwaltungsklasse binden kann.

Der Aufbewahrungszeitraum für Sicherung wird in folgenden Fällen verwendet:

- Der Benutzer ändert die Verwaltungsklasse einer Datei, aber weder die Standardverwaltungsklasse noch die neue Verwaltungsklasse enthält eine Sicherungskopiengruppe.
- Die Verwaltungsklasse, an die eine Datei gebunden ist, ist nicht mehr vorhanden, und die Standardverwaltungsklasse enthält keine Sicherungskopiengruppe.

Der in der Maßnahmendomäne definierte Aufbewahrungszeitraum für Sicherung startet, wenn eine Teilsicherung ausgeführt wird. Der Standardwert ist 30 Tage. Der Administrator kann diesen Zeitraum jedoch verlängern oder verkürzen.

Wenn der IBM Spectrum Protect-Server eine Datei mithilfe des Aufbewahrungszeitraums für Sicherung verwaltet, werden keine neuen Sicherungsversionen der Datei erstellt. Alle vorhandenen Sicherungsversionen der Datei verfallen 30 Tage (bzw. die in der Maßnahmendomäne angegebene Anzahl Tage) nach dem Tag, an dem sie als inaktiv markiert wurden.

Archivierungskopien werden niemals erneut gebunden, da jede Archivierungsoperation eine andere Archivierungskopie erstellt. Archivierungskopien bleiben an den Verwaltungsklassennamen gebunden, der angegeben wurde, als sie vom Benutzer archiviert wurden. Ist die Verwaltungsklasse, an die eine Archivierungskopie gebunden ist, nicht mehr vorhanden, oder enthält sie keine Archivierungskopiengruppe mehr, verwendet der Server die Standardverwaltungsklasse. Wenn Sie später die Standardverwaltungsklasse ändern oder ersetzen, verwendet der Server die aktualisierte Standardverwaltungsklasse, um die Archivierungskopie zu verwalten. Enthält die Standardverwaltungsklasse keine Archivierungskopiengruppe, verwendet der Server den für die Maßnahmendomäne angegebenen Aufbewahrungszeitraum für Archivierung.

Ereignisgesteuerte Maßnahme für Aufbewahrungsschutz

Alle Verwaltungsklassen mit einer Archivierungskopiengruppe müssen einen Aufbewahrungszeitraum angeben, z. B. die Anzahl Tage, die ein archiviertes Objekt auf dem Server gespeichert wird, bevor es gelöscht wird.

Eine ereignisgesteuerte Maßnahme bietet die Option, dass der Aufbewahrungszeitraum entweder zu dem Zeitpunkt beginnt, an dem das Objekt archiviert wird, oder zu einem späteren Zeitpunkt, wenn ein Aktivierungsereignis für dieses Objekt an den Server gesendet wird.

Mit dem Kopiengruppenwert `RETINIT=CREATE` wird der Aufbewahrungszeitraum für Daten gestartet, wenn die Datei archiviert wird. Mit dem Kopiengruppenwert `RETINIT=EVENT` wird der Aufbewahrungszeitraum für Daten gestartet, wenn der Server benachrichtigt wird, dass das Ereignis eingetreten ist.

Das folgende Beispiel veranschaulicht dieses Konzept:

Der Benutzer verfügt über zwei Dateien, create.file und event.file. Dem Benutzer stehen zwei Verwaltungsklassen zur Verfügung: CREATE mit `RETINIT=CREATE` und EVENT mit `RETINIT=EVENT`. Beide Verwaltungsklassen haben einen Aufbewahrungszeitraum von 60 Tagen. Der Benutzer archiviert beide Dateien am selben Tag:

```
dsmc archive create.file -archmc=CREATE
  dsmc archive event.file -archmc=EVENT
```

Zehn Tage später gibt der Benutzer den Befehl set event `-type=hold` für die Datei create.file aus, damit die Datei nicht gelöscht werden kann. Am selben Tag gibt der Benutzer set event `-type=activate` für die Datei event.file aus. Zu diesem Zeitpunkt sind für create.file 50 Tage Aufbewahrungszeitraum übrig, und für event.file 60 Tage. Wird keine andere Aktion ausgeführt, bleibt `create.file` für immer auf dem Server und event.file verfällt 70 Tage nach dem Erstellen (60 Tage nach Eintreten des Ereignisses). Der Benutzer gibt jedoch 20 Tage nach der ursprünglichen Archivierung den Befehl set event *-type=release* für die Datei create.file aus. Dreißig Tage ihres Aufbewahrungszeitraums sind vergangen, sodass die Datei in 30 Tagen verfällt (durch die Sperre wird der Aufbewahrungszeitraum nicht erweitert).

Informationen zum Kopiengruppenwert RETINIT finden Sie in der Dokumentation zum IBM Spectrum Protect-Server.

- Dateien auf einem Datenaufbewahrungsserver archivieren
  Bis zu diesem Punkt gibt es keinen Unterschied zwischen der Archivierung auf einem normalen Server und einem Datenaufbewahrungsserver.

Zugehörige Verweise:
Set Event

Optionen und Befehle des Clients für Sichern/Archivieren

Verwenden Sie die Clientoptionen, um die Verarbeitung des Clients für Sichern/Archivieren an Ihre Anforderungen anzupassen. Verwenden Sie die Befehlszeilenschnittstelle (CLI - Command-Line Interface) des Clients als Alternative zu der grafischen Benutzerschnittstelle (GUI - Graphical User-Interface). Referenzinformationen für die Clientoptionen und die Clientbefehle sowie ergänzende Informationen werden bereitgestellt.

- Syntaxdiagramme lesen
  Folgen Sie beim Lesen eines Syntaxdiagramms für die Befehlseingabe der Linie. Lesen Sie von links nach rechts und von oben nach unten.
- Verarbeitungsoptionen
  Sie können Standardwerte für die Verarbeitung von Clientoptionen verwenden oder die Verarbeitungsoptionen so anpassen, dass sie Ihren spezifischen Erfordernissen entsprechen. Dieser Abschnitt enthält eine Übersicht über Verarbeitungsoptionen und einen Optionsreferenzabschnitt, der detaillierte Informationen zu jeder Option bereitstellt.
- Befehle verwenden
  Der Client für Sichern/Archivieren verfügt über eine Befehlszeilenschnittstelle, die Sie alternativ zur grafischen Benutzerschnittstelle verwenden können. Dieser Abschnitt enthält Informationen zum Starten und Beenden einer Clientbefehlssitzung und Anweisungen zur Eingabe von Befehlen.
-  Windows-BetriebssystemeIBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service
  Die folgenden Client-Services können installiert werden, wenn Sie den Client für Sichern/Archivieren installieren oder das IBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service nach der Installation des Clients für Sichern/Archivieren verwenden:

Zugehörige Konzepte:
IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Zugehörige Tasks:
Clients für Sichern/Archivieren konfigurieren
Daten mit Clients für Sichern/Archivieren sichern und zurückschreiben
Daten mit Clients für Sichern/Archivieren archivieren und abrufen

Syntaxdiagramme lesen

Folgen Sie beim Lesen eines Syntaxdiagramms für die Befehlseingabe der Linie. Lesen Sie von links nach rechts und von oben nach unten.

- Das Symbol ►►——— zeigt den Anfang eines Syntaxdiagramms an.
- Das Symbol ———► am Ende einer Zeile zeigt an, dass das Syntaxdiagramm in der nächsten Zeile fortgesetzt wird.
- Das Symbol ►——— am Anfang einer Zeile zeigt an, dass das Syntaxdiagramm aus der vorherigen Zeile fortgesetzt wird.
- Das Symbol ———►◄ zeigt das Ende eines Syntaxdiagramms an.

Syntaxelemente, wie z. B. ein Schlüsselwort oder eine Variable, können sich an folgenden Positionen befinden:

- In der Linie (erforderliches Element)
- Oberhalb der Linie (Standardelement)
- Unterhalb der Linie (optionales Element)

Symbole

Geben Sie diese Symbole *exakt* so ein, wie sie im Syntaxdiagramm dargestellt werden.

- * Stern
- *{ }* Geschweifte Klammern
- *:* Doppelpunkt
- , Komma
- = Gleichheitszeichen
- - Bindestrich
- *()* Runde Klammern
- . Punkt
- Leerzeichen
- " Anführungszeichen
- ' Einfaches Anführungszeichen (Hochkomma)

Variablen

Kursiv dargestellte Elemente in Groß-/Kleinschreibung (z. B. *<Variablenname>* geben Variablen an. In diesem Beispiel können Sie einen *<Variablennamen>* angeben, wenn Sie den Befehl **Befehlsname** eingeben.

```
>>-Befehlsname--<Variablenname>--------------------------------><
```

Wiederholung

Ein nach links zurückweisender Pfeil bedeutet, dass Sie das Element wiederholen können. Ein Zeichen innerhalb des Pfeils bedeutet, dass Sie die wiederholten Elemente durch dieses Zeichen voneinander trennen müssen.

```
   .-,-----------.
   V             |
>>---wiederholen-+-----------------------------------------------><
```

Eine Fußnote (1) neben dem Pfeil gibt an, wie oft Sie das Element wiederholen können.

```
   .-,-----------------.
   V  (1)              |
>>---------wiederholen-+---------------------------------------><
```

Anmerkungen:

1. Geben Sie wiederholen maximal 5 Mal an.

Erforderliche Auswahlmöglichkeiten

Sind zwei oder mehr Elemente übereinander angeordnet und befindet sich eines von ihnen in der Linie, *müssen* Sie eines der Elemente angeben.

In diesem Beispiel müssen Sie A, B oder C auswählen.

```
>>-Befehlsname--+-A-+-------------------------------------------><
                +-B-+
                '-C-'
```

Optionale Auswahlmöglichkeiten

Steht ein Element *unterhalb* der Linie, ist es optional. Im ersten Beispiel können Sie A oder gar nichts auswählen.

```
>>-Befehlsname--+---+-------------------------------------------><
                '-A-'
```

Sind zwei oder mehr Elemente unterhalb der Linie untereinander angeordnet, sind alle Elemente optional. Im zweiten Beispiel können Sie A, B, C oder gar nichts auswählen.

```
>>-Befehlsname--+---+-------------------------------------------><
                +-A-+
                +-B-+
                '-C-'
```

Wiederholbare Auswahlmöglichkeiten

Mehrere übereinander angeordnete Elemente gefolgt von einem nach links zurückweisenden Pfeil bedeuten, dass Sie mehrere Elemente auswählen können oder in einigen Fällen ein einzelnes Element wiederholen können.

Im vorliegenden Beispiel können Sie eine beliebige Kombination aus A, B oder C auswählen.

```
                .-,-----.
                V       |
>>-Befehlsname----+-A-+-+---------------------------------------><
                  +-B-+
                  '-C-'
```

Standardwerte

Standardwerte stehen oberhalb der Linie. Der Standardwert wird ausgewählt, wenn er nicht überschrieben wird. Sie können den Standardwert auch explizit auswählen. Wenn der Standardwert überschrieben werden soll, geben Sie eine der unterhalb der Linie aufgeführten Optionen an.

In diesem Beispiel ist A der Standardwert. Wählen Sie B oder C aus, um A zu überschreiben.

```
                .-A-.
>>-Befehlsname--+---+-----------------------------------------><
                +-B-+
                '-C-'
```

Verarbeitungsoptionen

Sie können Standardwerte für die Verarbeitung von Clientoptionen verwenden oder die Verarbeitungsoptionen so anpassen, dass sie Ihren spezifischen Erfordernissen entsprechen. Dieser Abschnitt enthält eine Übersicht über Verarbeitungsoptionen und einen Optionsreferenzabschnitt, der detaillierte Informationen zu jeder Option bereitstellt.

- Übersicht über die Verarbeitungsoptionen
  IBM Spectrum Protect verwendet *Verarbeitungsoptionen*, um die Übertragung, die Sicherungs- und Archivierungsverarbeitung und andere Verarbeitungstypen zu steuern.
- Übertragungsoptionen
  Mithilfe von Übertragungsoptionen können Sie angeben, wie Ihr Clientknoten mit dem IBM Spectrum Protect-Server kommuniziert. Dieser Abschnitt enthält Informationen über die Typen von Übertragungsoptionen, die verwendet werden können.
- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeServeroptionen
  Mit der Option servername in der Datei dsm.sys können Sie eine Gruppe von Optionen (Zeilengruppen) beginnen, mit denen die Verbindung zum IBM Spectrum Protect-Server hergestellt wird.
- Verarbeitungsoptionen für Sichern und Archivieren
  Sie können Clientoptionen zur Steuerung einiger Aspekte der Sicherungs- und Archivierungsverarbeitung angeben.
- Verarbeitungsoptionen für Zurückschreiben und Abrufen
  Sie können Clientoptionen zur Steuerung einiger Aspekte der Zurückschreibungs- und Abrufverarbeitung verwenden.
- Planungsoptionen
  In diesem Abschnitt sind die Optionen beschrieben, die Sie zum Steuern der zentralen Zeitplanung verwenden können. Der Client für Sichern/Archivieren verwendet Planungsoptionen nur, wenn der Scheduler aktiv ist.
- Optionen für Format und Sprache
  Mit Optionen für Format und Sprache können Sie unterschiedliche Datums-, Uhrzeit- und Zahlenformate für verschiedene Sprachen auswählen.
- Befehlsverarbeitungsoptionen
  In diesem Abschnitt sind die Optionen beschrieben, die Sie mit den Befehlen des Clients für Sichern/Archivieren verwenden können.
- Berechtigungsoptionen
  Über Berechtigungsoptionen wird der Zugriff auf den IBM Spectrum Protect-Server gesteuert.
- Fehlerverarbeitungsoptionen
  Fehlerverarbeitungsoptionen geben den Namen der Fehlerprotokolldatei sowie die Behandlung der Einträge in der Protokolldatei durch den Client für Sichern/Archivieren an.
- Transaktionsverarbeitungsoptionen
  Transaktionsverarbeitungsoptionen steuern, wie Transaktionen zwischen dem IBM Spectrum Protect-Client und -Server verarbeitet werden.
- Web-Client-Optionen
  Zum Konfigurieren des IBM Spectrum Protect-Web-Clients werden verschiedene Optionen des Clients für Sichern/Archivieren verwendet.
- Optionen in Befehlen verwenden
  Sie können einige der Optionen in Ihrer Clientoptionsdatei (dsm.opt) überschreiben, indem Sie sie mit den entsprechenden Befehlen des Clients für Sichern/Archivieren eingeben.
- Clientoptionsreferenz
  Die folgenden Abschnitte enthalten detaillierte Informationen über die einzelnen IBM Spectrum Protect-Verarbeitungsoptionen.

Zugehörige Konzepte:
Optionen in Befehlen verwenden
Zugehörige Verweise:
Syntaxdiagramme lesen

Übersicht über die Verarbeitungsoptionen

IBM Spectrum Protect verwendet *Verarbeitungsoptionen*, um die Übertragung, die Sicherungs- und Archivierungsverarbeitung und andere Verarbeitungstypen zu steuern.

Windows-BetriebssystemeSie können Verarbeitungsoptionen in der Clientoptionsdatei (dsm.opt) oder in der Befehlszeile angeben.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSie können Verarbeitungsoptionen in der Clientsystemoptionsdatei (dsm.sys), in der Clientbenutzeroptionsdatei (dsm.opt) oder in der Befehlszeile angeben.

Sie können folgende Optionstypen definieren:

- Optionen für die Datenübertragung
- Windows-BetriebssystemeKnotenoptionen
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeServer- und Knotenoptionen
- Verarbeitungsoptionen für Sichern und Archivieren
- Verarbeitungsoptionen für Zurückschreiben und Abrufen
- Planungsoptionen
- Windows-BetriebssystemeOptionen für Format und Sprache
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFormatoptionen
- Befehlsverarbeitungsoptionen
- Berechtigungsoptionen
- Fehlerverarbeitungsoptionen
- Transaktionsverarbeitungsoptionen
- Web-Client-Optionen
- Diagnoseoptionen

Der Client für Sichern/Archivieren umfasst außerdem eine Gruppe von Clientbefehlsoptionen, die Sie nur in der Befehlszeile mit bestimmten Befehlen eingeben können. Sie können einige der Optionen in Ihrer Optionsdatei überschreiben, indem Sie sie mit den entsprechenden Befehlen für Sichern/Archivieren eingeben.

Windows-BetriebssystemeAnmerkung: Einige der Verarbeitungsoptionen, die der zentrale Scheduler von IBM Spectrum Protect verwendet, werden bei der Konfiguration der Zeitplanungsservices in der Windows-Registrierung definiert. Diese Optionen können auch in der Clientoptionsdatei angegeben werden. Wenn der Scheduler als Dienst ausgeführt wird, überschreiben die Verarbeitungsoptionen, die in der Registrierung angegeben werden, dieselben Optionen, die in der Clientoptionsdatei angegeben werden.

Zugehörige Konzepte:
Optionen mit einem Befehl eingeben

Zugehörige Tasks:
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Clientsystemoptionsdatei erstellen und ändern
Windows-BetriebssystemeClientoptionsdatei erstellen und ändern

Übertragungsoptionen

Mithilfe von Übertragungsoptionen können Sie angeben, wie Ihr Clientknoten mit dem IBM Spectrum Protect-Server kommuniziert. Dieser Abschnitt enthält Informationen über die Typen von Übertragungsoptionen, die verwendet werden können.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeFür UNIX und Linux verwenden Sie eines der folgenden Übertragungsprotokolle:

- TCP/IP
- AIX-BetriebssystemeLinux-BetriebssystemeShared Memory (AIX, Linux)

Windows-BetriebssystemeFür alle Windows-Clients verwenden Sie eines der folgenden Protokolle:

Windows-Betriebssysteme

- TCP/IP
- Benannte Pipes
- Shared Memory

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Geben Sie das Übertragungsprotokoll mit der Option commmethod an.

Bitten Sie Ihren IBM Spectrum Protect-Administrator um Hilfe bei der Festlegung Ihrer Übertragungsoptionen.

- TCP/IP-Optionen
  Zur Verwendung des TCP/IP-Übertragungsprotokolls müssen Sie die Option tcpserveraddress in Ihre Clientoptionsdatei einschließen.
- Windows-BetriebssystemeOption für benannte Pipes
  Dieser Abschnitt enthält Informationen über die Datenübertragungsoption namedpipename.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeOptionen für Shared Memory
  Dieser Abschnitt enthält Informationen über die Shared Memory-Optionen, die Sie verwenden können.

Zugehörige Verweise:
Commmethod

TCP/IP-Optionen

Zur Verwendung des TCP/IP-Übertragungsprotokolls müssen Sie die Option tcpserveraddress in Ihre Clientoptionsdatei einschließen.

Die anderen TCP/IP-Optionen haben Standardwerte, die Sie ggf. ändern können. Dieser Abschnitt enthält Informationen über die Typen von Übertragungsoptionen, die verwendet werden können.

Tabelle 1. TCP/IP-Optionen

Option	Beschreibung
httpport	Gibt eine TCP/IP-Anschlussadresse für den Web-Client an.
lanfreetcpport	Gibt die Nummer des TCP/IP-Anschlusses an, an dem der IBM Spectrum Protect-Speicheragent empfangsbereit ist.
lanfreetcpserveraddress	Gibt die TCP/IP-Adresse für den IBM Spectrum Protect-Speicheragenten an.
tcpbuffsize	Gibt die Größe des internen TCP/IP-Kommunikationspuffers in Kilobyte an.
Windows-Betriebssystemetcpnodelay	Windows-BetriebssystemeGibt an, ob der Server oder Client die Verzögerung beim Senden aufeinanderfolgender kleiner Pakete im Netz inaktiviert.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemetcpnodelay	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeGibt an, ob der Server oder Client die Verzögerung beim Senden aufeinanderfolgender kleiner Pakete im Netz inaktiviert. Diese Option ist für alle UNIX-Clients gültig.
tcpadminport	Gibt eine separate TCP/IP-Anschlussnummer an, an der der Server Anforderungen für Verwaltungsclientsitzungen erwartet. Dies ermöglicht sichere Verwaltungssitzungen innerhalb eines privaten Netzes.
tcpcadaddress	Gibt eine TCP/IP-Adresse für dsmcad an.
tcpport	Gibt die TCP/IP-Anschlussadresse für einen IBM Spectrum Protect-Server an.
tcpserveraddress	Gibt die TCP/IP-Adresse für einen IBM Spectrum Protect-Server an.
tcpwindowsize	Gibt die Größe (in Kilobyte) des TCP/IP-Schiebefensters für Ihren Clientknoten an.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemewebports	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAktiviert die Verwendung des Web-Clients außerhalb einer Firewall, indem die TCP/IP-Anschlussnummer angegeben wird, die vom Clientakzeptordämon und dem Web-Client-Agentenservice (Web-Client-Agentenservice gilt nicht für Mac OS X) für die Kommunikation mit der Web-GUI verwendet wird.
Windows-Betriebssystemewebports	Windows-BetriebssystemeAktiviert die Verwendung des Web-Clients außerhalb einer Firewall, indem die TCP/IP-Anschlussnummer angegeben wird, die vom Clientakzeptorservice und dem Web-Client-Agentenservice für die Kommunikation mit dem Web-Client verwendet wird.

Zugehörige Verweise:
Nfstimeout
Windows-Betriebssysteme

Option für benannte Pipes

Dieser Abschnitt enthält Informationen über die Datenübertragungsoption namedpipename.

Tabelle 1. Datenübertragungsoption für benannte Pipes

Option	Beschreibung
namedpipename Namedpipename	Gibt den Namen einer benannten Pipe an, die für die Übertragung zwischen einem Client und dem IBM Spectrum Protect-Server in derselben Windows-Serverdomäne verwendet werden soll.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Optionen für Shared Memory

Dieser Abschnitt enthält Informationen über die Shared Memory-Optionen, die Sie verwenden können.

Tabelle 1. Übertragungsoptionen für Shared Memory

Option	Beschreibung
lanfreeshmport Lanfreeshmport	Gibt die eindeutige Zahl an, die vom Client und vom Speicheragenten verwendet wird, um den für die Datenübertragung verwendeten gemeinsam benutzten Speicherbereich (Shared Memory) zu identifizieren.

Option	Beschreibung
lanfreeshmport Shmport	Gibt die eindeutige Zahl an, die vom Client und vom Server verwendet wird, um den für die Datenübertragung verwendeten gemeinsam benutzten Speicherbereich (Shared Memory) zu identifizieren.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

Serveroptionen

Mit der Option servername in der Datei dsm.sys können Sie eine Gruppe von Optionen (Zeilengruppen) beginnen, mit denen die Verbindung zum IBM Spectrum Protect-Server hergestellt wird.

Sie können mehrere Zeilengruppen in der Datei dsm.sys definieren, um eine Verbindung zu verschiedenen Servern herstellen zu können. Unter jeder servername-Zeilengruppe müssen alle Clientoptionszeilengruppen aufgelistet sein, die erforderlich sind, um die Kommunikation mit einem Server herzustellen. Die Zeilengruppenliste kann auch andere Optionen für Sicherungs- und Archivierungsoperationen enthalten.

Wenn Ihre Clientsystemoptionsdatei nur eine Zeilengruppe enthält, richtet Ihr Clientknoten alle Serviceanforderungen an den in dieser Zeilengruppe angegebenen Server.

Wenn Ihre Clientsystemoptionsdatei mehrere Zeilengruppen enthält, können Sie mit der Option defaultserver einen Standardserver angeben. Wenn Sie keinen Standardserver angeben, stellt IBM Spectrum Protect eine Verbindung zu dem Server her, den Sie in der ersten Zeilengruppe Ihrer Datei dsm.sys angeben.

Fügen Sie die Option defaultserver am Anfang der Datei dsm.sys vor allen Serverzeilengruppen ein. Weitere Informationen enthält Defaultserver.

Geben Sie mit der Option servername in der Clientbenutzeroptionsdatei (dsm.opt) oder in der Befehlszeile einen Server an, an den Sicherungs- und Archivierungsserviceanforderungen gerichtet werden sollen. Damit wird der in der Datei `dsm.sys` angegebene Standardserver überschrieben.

Anmerkung: Den in der Clientsystemoptionsdatei angegebenen Umlagerungsserver können Sie nicht überschreiben.

Tabelle 1 zeigt eine dsm.sys-Beispieldatei.

Tabelle 1. Beispiel einer Clientsystemoptionsdatei

Beispieldatei dsm.sys

`DEFAULTServer server2`
 	
`SErvername server1`
`NODename node1`
`COMMMethod TCPip`
`TCPPort 1500`
`TCPServeraddress node.domain.company.com`
`PASSWORDAccess generate`
`GRoups system adsm`
`USERs ashton stewart kaitlin`
`INCLExcl /adm/adsm/backup1.excl`
 	
`SErvername server2`
`COMMMethod SHAREdmem`
`shmport 1520`
`PASSWORDAccess prompt`
`GRoups system adsm`
`USERs danielle derek brant`
`INCLExcl /adm/adsm/backup2.excl`

Verarbeitungsoptionen für Sichern und Archivieren

Sie können Clientoptionen zur Steuerung einiger Aspekte der Sicherungs- und Archivierungsverarbeitung angeben.

Tabelle 1. Verarbeitungsoptionen für Sichern und Archivieren

Option	Beschreibung
 AIX-Betriebssysteme  Linux-Betriebssysteme afmskipuncachedfiles	AIX-BetriebssystemeLinux-BetriebssystemeVerwenden Sie die Option afmskipuncachedfiles, um anzugeben, ob bei General Parallel File System (GPFS™) nicht zwischengespeicherte und genutzte Dateien in Active File Management-Dateigruppen bei Sicherungs-, Archivierungs- und Umlagerungsoperationen verarbeitet werden.
archmc	Verwenden Sie die Option archmc im Befehl archive, um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Dateien binden wollen.

Option	Beschreibung
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme archsymlinkasfile	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt an, ob der Client einer symbolischen Verbindung folgen und die Datei oder das Verzeichnis, auf die bzw. das sie verweist, archivieren soll, oder ob nur die symbolische Verbindung archiviert werden soll.
asnodename	Mit der Option asnodename können Agentenknoten Daten im Namen eines anderen Knotens (des Zielknotens) sichern oder zurückschreiben. Diese Option ermöglicht gleichzeitig ablaufende Operationen von mehreren Knoten, um Daten auf demselben Zielknoten und in demselben Dateibereich parallel zu speichern.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme automount	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeVerwenden Sie diese Option zusammen mit der Option domain, um alle Auto-Mount-Dateisysteme anzugeben, die der Client zu folgenden Zeitpunkten anzuhängen versucht: • Wenn der Client für Sichern/Archivieren gestartet wird • Wenn die Sicherung gestartet wird • Wenn der Client für Sichern/Archivieren während der Sicherung ein Auto-Mount-Dateisystem erreicht
autofsrename	Gibt an, ob ein vorhandener Dateibereich auf einem Unicode-aktivierten Server umbenannt werden soll, damit für die aktuelle Operation ein Unicode-aktivierter Dateibereich erstellt werden kann.
Windows-Betriebssysteme backmc	Windows-BetriebssystemeGibt die Verwaltungsklasse an, die auf den Unterbefehl backup fastback für Aufbewahrungszwecke anzuwenden ist.
changingretries	Gibt an, wie oft der Client einen Sicherungs- oder Archivierungsversuch wiederholt, wenn die Datei im Gebrauch ist.
Windows-Betriebssysteme class	Windows-BetriebssystemeGibt an, ob die NAS- oder Clientobjekte während einer Operation query backup, query filespace oder delete filespace aufgelistet werden sollen.
compressalways	Die Option compressalways gibt an, ob die Komprimierung eines Objekts fortgesetzt wird, wenn es während der Komprimierung größer wird. Diese Option ist mit der Option compression zu verwenden.
compression	Die Option compression komprimiert Dateien, bevor sie an den Server gesendet werden. Die Komprimierung der Dateien reduziert den erforderlichen Datenspeicherplatz für Sicherungsversionen und Archivierungskopien der Dateien.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-Betriebssysteme createnewbase Createnewbase	AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme Die Option createnewbase erstellt eine Basismomentaufnahme und verwendet sie als Quelle für die Ausführung einer vollständigen Teilsicherung. Mit dieser Option wird die Sicherung aller Dateien sichergestellt, die möglicherweise während der Teilsicherung unter Verwendung der Momentaufnahmedifferenz übersprungen wurden.
deduplication Deduplication	Gibt an, ob redundante Daten auf der Clientseite entfernt werden sollen, wenn der Client während der Sicherungs- oder Archivierungsverarbeitung Daten an den IBM Spectrum Protect-Server überträgt.
dedupcachepath Dedupcachepath	Gibt die Position an, an der die Cachedatenbank für die clientseitige Datendeduplizierung erstellt wird, wenn die Option enablededupcache=yes bei der Sicherungs- oder Archivierungsverarbeitung definiert ist.
dedupcachesize Dedupcachesize	Legt die maximale Größe der Cachedatei für die Datendeduplizierung fest.
enablededupcache Enablededupcache	Gibt an, ob der Cache für die clientseitige Datendeduplizierung aktiviert werden soll, sodass der Client für Sichern/Archivieren die geänderten Daten aus dem Cache erhält.

Option	Beschreibung
deletefiles	Verwenden Sie die Option deletefiles im Befehl archive, um Dateien von Ihrer Workstation zu löschen, nachdem Sie sie archiviert haben. AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeWindows-BetriebssystemeDiese Option kann auch im Befehl restore image und mit der Option incremental verwendet werden, um Dateien aus dem zurückgeschriebenen Image zu löschen, falls sie nach der Erstellung des Image gelöscht wurden.
Beschreibung	Die Option description ordnet Dateien eine Beschreibung zu oder gibt eine Beschreibung für diese Dateien an, wenn der Client Operationen zum Archivieren, Löschen, Abrufen, Abfragen der Archivierung oder Abfragen des Sicherungssatzes ausführt.
detail	Mit der Option detail können Sie, abhängig vom Befehl, mit dem sie verwendet wird, Informationen zu Verwaltungsklassen, Dateibereichen, Sicherungen und Archivierungen auflisten.
 Linux-Betriebssysteme  AIX-Betriebssysteme Windows-Betriebssysteme diffsnapshot	Linux-BetriebssystemeAIX-Betriebssysteme  Windows-Betriebssysteme Verwenden Sie die Option diffsnapshot, um zu bestimmen, ob der Client eine Differenzmomentaufnahme erstellt.
dirmc	Gibt die Verwaltungsklasse an, die für Verzeichnisse verwendet werden soll. Wenn Sie diese Option nicht angeben, verwendet der Client die Verwaltungsklasse in der aktiven Maßnahmengruppe Ihrer Maßnahmendomäne mit dem längsten Aufbewahrungszeitraum.
dirsonly	Nur Verzeichnisse sichern, zurückschreiben, archivieren, abrufen oder abfragen.
diskcachelocation	Gibt die Position an, an der die Plattencachedatenbank erstellt wird, wenn die Option memoryefficient=diskcachemethod bei einer Teilsicherung definiert ist.
 AIX-Betriebssysteme  Linux-Betriebssysteme Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme domain	 AIX-Betriebssysteme  Linux-Betriebssysteme Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeGibt die Dateisysteme an, die für eine Teilsicherung in Ihre Standardclientdomäne aufgenommen werden sollen.
 Windows-Betriebssysteme domain	 Windows-BetriebssystemeGibt die Laufwerke an, die für eine Teilsicherung in Ihre Standardclientdomäne aufgenommen werden sollen.
 AIX-Betriebssysteme  Linux-Betriebssysteme Oracle Solaris-Betriebssysteme domain.image	 AIX-Betriebssysteme  Linux-Betriebssysteme Oracle Solaris-BetriebssystemeGibt die angehängten Dateisysteme und unformatierten logischen Datenträger an, die Sie für eine Imagesicherung in Ihre Clientdomäne einbeziehen wollen. Diese Option gilt nur für AIX, Linux x86_64, Linux on POWER und Solaris.
 Windows-Betriebssysteme domain.image	 Windows-BetriebssystemeGibt die Dateisysteme und unformatierten logischen Datenträger an, die Sie für eine Imagesicherung in Ihre Clientdomäne einbeziehen wollen. Diese Option ist für alle Windows-Clients gültig.
 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme Windows-Betriebssysteme domain.nas	 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme Windows-BetriebssystemeGibt die Datenträger an, die für NAS-Imagesicherungen in Ihre Standarddomäne einbezogen werden sollen.
Linux-Betriebssysteme  Windows-Betriebssysteme domain.vmfull Domain.vmfull	 Linux-Betriebssysteme  Windows-BetriebssystemeGibt die virtuellen Maschinen an, die bei vollständigen Imagesicherungen für virtuelle VMware-Maschinen berücksichtigt werden sollen.
 AIX-Betriebssysteme efsdecrypt	 AIX-BetriebssystemeGibt an, ob Dateien, die von einem AIX Encrypted File System (EFS) verschlüsselt werden, in verschlüsseltem oder entschlüsseltem Format gelesen werden.
enablearchiveretentionprotection	Ermöglicht dem Client, eine Verbindung zu einem Datenaufbewahrungsserver herzustellen.

Option	Beschreibung
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme enablelanfree Enablelanfree	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeWindows-BetriebssystemeGibt an, ob ein verfügbarer LAN-unabhängiger Pfad zu einer an ein Speicherbereichsnetz (SAN) angeschlossenen Speichereinheit aktiviert werden soll.
Windows-Betriebssysteme exclude exclude.backup exclude.file exclude.file.backup	Windows-BetriebssystemeMit diesen Optionen können Sie eine Datei oder Dateigruppe von den Sicherungsservices ausschließen.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme exclude exclude.backup exclude.file exclude.file.backup	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMit diesen Optionen können Sie eine Datei oder Dateigruppe von den Sicherungsservices und von den Speicherverwaltungsservices (wenn der HSM-Client installiert ist) ausschließen. Die Option exclude.backup schließt Dateien nur von der normalen Sicherung aus, nicht von HSM.
encryptiontype	Wählen Sie die 256-Bit-AES- oder 128-Bit-AES-Datenverschlüsselung aus. Die 256-Bit-AES-Datenverschlüsselung bietet die stärkste Datenverschlüsselung.
encryptkey	Gibt an, ob das Kennwort für den Verschlüsselungsschlüssel lokal gesichert werden soll, wenn der Client eine Operation Sichern/Archivieren ausführt, oder ob der Benutzer zur Eingabe des Kennworts für den Verschlüsselungsschlüssel aufgefordert werden soll.
exclude.archive	Schließt eine dem Muster entsprechende Datei oder Dateigruppe nur von den Archivierungsservices aus.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme exclude.attribute.symlink	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSchließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt (Aliasnamen gelten für Mac OS X), nur von der Sicherungsverarbeitung aus.
exclude.compression	Schließt Dateien von der Komprimierungsverarbeitung aus, wenn die Option compression auf *yes* gesetzt ist. Diese Option gilt für Sicherungen und Archivierungen.
exclude.dir	Schließt ein Verzeichnis, seine Dateien sowie alle zugehörigen Unterverzeichnisse und ihre Dateien von der Sicherungsverarbeitung aus.
exclude.encrypt	Schließt die angegebenen Dateien von der Verschlüsselungsverarbeitung aus.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme exclude.fs	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSchließt Dateibereiche aus, die mit einem Muster übereinstimmen. Diese Option ist für alle UNIX-Clients gültig.
AIX-BetriebssystemeOracle Solaris-Betriebssysteme exclude.fs.nas	AIX-BetriebssystemeOracle Solaris-BetriebssystemeBei Verwendung im Befehl backup nas werden Dateisysteme auf dem NAS-Dateiserver von der Imagesicherung ausgeschlossen. Diese Option ist nur für AIX- und Solaris-Clients gültig.
Windows-Betriebssysteme exclude.fs.nas	Windows-BetriebssystemeBei Verwendung im Befehl backup nas werden Dateisysteme auf dem NAS-Dateiserver von der Imagesicherung ausgeschlossen.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme exclude.image	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeSchließt angehängte Dateisysteme und unformatierte logische Datenträger, die dem angegebenen Muster entsprechen, von den Imagegesamtsicherungsoperationen aus. Diese Option ist nur für AIX-, Solaris- und alle Linux-Clients gültig.
Windows-Betriebssysteme exclude.image	Windows-BetriebssystemeSchließt angehängte Dateisysteme und unformatierte logische Datenträger, die dem angegebenen Muster entsprechen, von den Imagegesamtsicherungsoperationen aus. Imageteilsicherungsoperationen sind von exclude.image nicht betroffen.

Option	Beschreibung
Linux-BetriebssystemeWindows-Betriebssysteme fbbranch	Linux-BetriebssystemeWindows-BetriebssystemeGibt die Filialen-ID des fernen FastBack-Servers an, der gesichert oder archiviert werden soll.
Linux-BetriebssystemeWindows-Betriebssysteme fbclientname	Linux-BetriebssystemeWindows-BetriebssystemeGibt den Namen eines oder mehrerer FastBack-Clients an, die vom Sicherungsproxy gesichert werden sollen.
Linux-BetriebssystemeWindows-Betriebssysteme fbpolicyname	Linux-BetriebssystemeWindows-BetriebssystemeGibt den Namen einer oder mehrerer Tivoli Storage Manager FastBack-Maßnahmen an, die vom Sicherungsproxy gesichert werden sollen.
Linux-BetriebssystemeWindows-Betriebssysteme fbreposlocation	Linux-BetriebssystemeWindows-BetriebssystemeGibt die Position des Tivoli Storage Manager FastBack-Repositorys an, zu dem der IBM Spectrum Protect-Client-Proxy die Verbindung herstellt, um die Befehle MOUNT DUMP, MOUNT ADD und MOUNT DEL auszugeben.
Linux-BetriebssystemeWindows-Betriebssysteme fbserver	Linux-BetriebssystemeWindows-BetriebssystemeGibt den Hostnamen der FastBack-Server-Workstation oder der FastBack Disaster Recovery Hub-Workstation an, die Eigner des durch die Option fbreposlocation angegebenen Repositorys ist.
Linux-BetriebssystemeWindows-Betriebssysteme fbvolumename	Linux-BetriebssystemeWindows-BetriebssystemeGibt den Namen eines oder mehrerer Tivoli Storage Manager FastBack-Datenträger an, die vom Sicherungs-Proxy gesichert werden sollen.
filelist	Gibt eine Liste von Dateien an, die für den Befehl verarbeitet werden sollen. Der Client öffnet die angegebene Dateiliste und verarbeitet die darin aufgelisteten Dateien gemäß dem Befehl.
filesonly	Nur Dateien sichern, zurückschreiben, abrufen oder abfragen.
groupname	Verwenden Sie diese Option im Befehl backup group, um den vollständig qualifizierten Namen des Hauptmembers einer Gruppe anzugeben.
ieobjtype Ieobjtype	Gibt einen Objekttyp für eine Operation für clientseitige Datendeduplizierung an. Diese Option wird mit den Optionen include.dedup und exclude.dedup verwendet.
AIX-Betriebssysteme imagegapsize	AIX-BetriebssystemeGibt die Mindestgröße der leeren Bereiche auf einem Datenträger an, die Sie während der Sicherung überspringen wollen. Diese Option ist für AIX JFS2-Clients gültig.
Windows-Betriebssysteme imagegapsize	Windows-BetriebssystemeGibt die Mindestgröße der leeren Bereiche auf einem Datenträger an, die Sie während der Sicherung überspringen wollen. Diese Option ist für alle Windows-Clients gültig.
inclexcl	Gibt den Pfad und den Dateinamen einer Einschluss-/Ausschlussoptionsdatei an.
include include.backup include.file	Mit diesen Optionen können Sie Dateien einschließen oder Verwaltungsklassen für die Sicherungsverarbeitung zuordnen.
include.archive	Schließt Dateien für die Archivierungsverarbeitung ein oder ordnet Verwaltungsklassen zu.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme include.attribute.symlink	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSchließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt (Aliasnamen gelten für Mac OS X), innerhalb einer größeren Gruppe von ausgeschlossenen Dateien nur bei der Sicherungsverarbeitung ein.
include.compression	Schließt Dateien für die Komprimierungsverarbeitung ein, wenn Sie die Option compression auf *yes* setzen. Diese Option gilt für Sicherungen und Archivierungen.
include.encrypt	Schließt die angegebenen Dateien in die Verschlüsselungsverarbeitung ein. Standardmäßig führt der Client keine Verschlüsselungsverarbeitung durch.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme include.fs	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMit der Option include.fs können Sie steuern, wie der Client Ihren Dateibereich für die Teilsicherung verarbeitet.

Option	Beschreibung
Windows-Betriebssysteme include.fs	Windows-BetriebssystemeVerwenden Sie die Option include.fs, um Verarbeitungsoptionen für ein Dateisystem anzugeben. Verwenden Sie die Option include.fs, um anzugeben, welche Laufwerke die Unterstützung offener Dateien verwenden, und um zu steuern, wie Teilsicherungen für komplette Dateibereiche verarbeitet werden.
AIX-BetriebssystemeOracle Solaris-Betriebssysteme include.fs.nas	AIX-BetriebssystemeOracle Solaris-BetriebssystemeVerwenden Sie die Option include.fs.nas, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Sie können auch angeben, ob der Client während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Verwenden Sie dazu die Option toc mit der Option include.fs.nas in Ihrer Datei dsm.sys. Weitere Informationen finden Sie in Toc. Diese Option ist nur für AIX- und Solaris-Clients gültig.
Windows-Betriebssysteme include.fs.nas	Windows-BetriebssystemeVerwenden Sie die Option include.fs.nas, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Sie können auch angeben, ob der Client während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Verwenden Sie dazu die Option toc mit der Option include.fs.nas in Ihrer Clientoptionsdatei (dsm.opt). Weitere Informationen finden Sie in Toc.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme include.image	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeGibt ein Dateisystem oder einen logischen Datenträger an, das/der für die Verarbeitung der Imagesicherung eingeschlossen werden soll. Diese Option stellt außerdem einen Weg zur Verfügung, um eine explizite Verwaltungsklassenzuordnung für ein angegebenes Dateisystem oder einen logischen Datenträger anzugeben. Der Befehl 'backup image' ignoriert alle anderen Einschlussoptionen. Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig.
Windows-Betriebssysteme include.image	Windows-BetriebssystemeGibt ein Dateisystem oder einen logischen Datenträger an, das/der für die Verarbeitung der Imagesicherung eingeschlossen werden soll. Diese Option stellt außerdem einen Weg zur Verfügung, um eine explizite Verwaltungsklassenzuordnung für ein angegebenes Dateisystem oder einen logischen Datenträger anzugeben. Der Befehl backup image ignoriert alle anderen Include-Optionen. Verwenden Sie die Option include.fs, um anzugeben, welche Laufwerke die Unterstützung offener Dateien verwenden, und um zu steuern, wie Teilsicherungen für komplette Dateibereiche verarbeitet werden.
Windows-Betriebssysteme include.systemstate	Windows-BetriebssystemeOrdnet Verwaltungsklassen für die Sicherung des Windows-Systemstatus zu. Der Standardwert ist, das Systemobjekt an die Standardverwaltungsklasse zu binden.
incrbydate	Verwenden Sie diese Option im Befehl incremental , um eine Teilsicherung nach Datum anzufordern.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme incremental	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeVerwenden Sie diese Option im Befehl restore image , um sicherzustellen, dass Änderungen des Basisimage auch auf das zurückgeschriebene Image angewendet werden. Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig.
Windows-Betriebssysteme incremental	Windows-BetriebssystemeVerwenden Sie diese Option im Befehl restore image , um sicherzustellen, dass Änderungen des Basisimage auch auf das zurückgeschriebene Image angewendet werden.
Windows-Betriebssysteme incrthreshold	Windows-BetriebssystemeDie Option incrthreshold gibt den Schwellenwert für die Anzahl Verzeichnisse in einem Journaldateibereich an, für die aktive Objekte auf dem Server, aber keine äquivalenten Objekte auf der Workstation vorhanden sein können.
memoryefficientbackup	Gibt einen Speicher sparenden Sicherungsalgorithmus für Teilsicherungen an, wenn diese Option im Befehl incremental verwendet wird.

Option	Beschreibung
mode	Die Option mode ist in den folgenden Befehlen wie folgt zu verwenden:  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssystemebackup image  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme Angeben, ob eine selektive Imagesicherung oder eine Imageteilsicherung von Clientdateisystemen ausgeführt werden soll.  AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssystemebackup nas  AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-BetriebssystemeAngeben, ob eine vollständige oder eine differenzielle Imagesicherung von NAS-Dateisystemen ausgeführt werden soll. backup group Angeben, ob eine vollständige oder differenzielle Gruppensicherung einer Liste von Dateien ausgeführt werden soll, die sich in einem oder mehreren Dateibereichen befinden.  Linux-Betriebssystemebackup vm  Linux-BetriebssystemeAngeben, ob eine selektive Sicherung oder eine Teilsicherung von VMware-Systemen ausgeführt werden soll.  Windows-Betriebssystemebackup vm  Windows-BetriebssystemeAngeben, ob eine vollständige oder eine Teilsicherung einer virtuellen VMware-Maschine ausgeführt werden soll, wenn vmbackuptype=fullvm gilt und wenn Sie IBM Spectrum Protect for Virtual Environments installiert haben.
 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme Windows-Betriebssysteme monitor	AIX-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeGibt an, ob Sie eine Imagesicherung von Dateisystemen, die zu einem NAS-Dateiserver gehören, überwachen wollen.
 Mac OS X-Betriebssysteme noprompt	Mac OS X-BetriebssystemeUnterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group, delete archive, expire und set event angezeigt wird.
 AIX-Betriebssysteme  Linux-Betriebssysteme Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme noprompt	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeWindows-BetriebssystemeUnterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group, delete archive, expire, restore image und set event angezeigt wird.
 AIX-Betriebssysteme  Linux-Betriebssysteme nojournal	AIX-BetriebssystemeLinux-BetriebssystemeVerwenden Sie diese Option im Befehl incremental, um anzugeben, dass statt der standardmäßigen ournalgestützten Sicherung die traditionelle vollständige Teilsicherung ausgeführt werden soll.
 Windows-Betriebssysteme nojournal	Windows-BetriebssystemeVerwenden Sie diese Option im Befehl incremental, um anzugeben, dass statt der standardmäßigen ournalgestützten Sicherung die traditionelle vollständige Teilsicherung ausgeführt werden soll.
Windows-Betriebssysteme optfile	Windows-BetriebssystemeGibt die Clientoptionsdatei an, die Sie verwenden wollen, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme optfile	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt die Clientbenutzeroptionsdatei an, die Sie verwenden wollen, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.
AIX-BetriebssystemeLinux-Betriebssysteme postsnapshotcmd	AIX-BetriebssystemeLinux-BetriebssystemeWährend einer momentaufnahmebasierten Sicherung können Sie mit dieser Option eine Anwendung manuell öffnen, nachdem die Momentaufnahme erstellt wurde. Diese Option ist nur für momentaufnahmebasierte AIX-JFS2- oder Linux-LVM-Operationen gültig.

Option	Beschreibung
Windows-Betriebssysteme postsnapshotcmd	Windows-BetriebssystemeWährend einer Online-Imagesicherung oder einer Operation mit Unterstützung offener Dateien (Open File Support - OFS) können Sie mit dieser Option eine Anwendung manuell öffnen, nachdem der Momentaufnahmeprovider eine Momentaufnahme gestartet hat. Diese Option ist nur gültig, wenn die OFS-Unterstützung oder Online-Imageunterstützung aktiviert ist.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme preservelastaccessdate	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeWindows-BetriebssystemeVerwenden Sie diese Option während einer Sicherungs- oder Archivierungsoperation, um anzugeben, ob das Datum des letzten Zugriffs auf angegebene Dateien nach einer Sicherungs- oder Archivierungsoperation auf seinen ursprünglichen Wert zurückgesetzt werden soll. Standardmäßig setzt der Client das Datum des letzten Zugriffs auf gesicherte oder archivierte Dateien nicht auf den ursprünglichen Wert vor der Sicherungs- oder Archivierungsoperation zurück.
AIX-BetriebssystemeLinux-Betriebssysteme presnapshotcmd	AIX-BetriebssystemeLinux-BetriebssystemeWährend einer momentaufnahmebasierten Sicherung können Sie mit dieser Option eine Anwendung manuell in den Wartemodus versetzen, bevor die Momentaufnahme erstellt wird. Diese Option ist nur für momentaufnahmebasierte AIX-JFS2- oder Linux-LVM-Operationen gültig.
Windows-Betriebssysteme presnapshotcmd	Windows-BetriebssystemeWährend einer Online-Imagesicherung oder einer Operation mit Unterstützung offener Dateien (Open File Support - OFS) können Sie mit dieser Option eine Anwendung manuell in den Wartemodus versetzen, bevor der Momentaufnahmeprovider eine Momentaufnahme startet. Diese Option ist nur gültig, wenn die OFS-Unterstützung oder Online-Imageunterstützung aktiviert ist.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme removeoperandlimit	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt an, dass der Client die Beschränkung auf 20 Operanden entfernt. Geben Sie die Option removeoperandlimit mit dem Befehl incremental, selective oder archive an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt.
Windows-Betriebssysteme resetarchiveattribute	Windows-BetriebssystemeGibt an, ob der Client das Windows-Archivierungsattribut für Dateien zurücksetzt, die erfolgreich auf dem IBM Spectrum Protect-Server gesichert wurden. Diese Option ist für alle Windows-Clients gültig.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme skipacl	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt an, ob die ACL-Verarbeitung vollständig übersprungen werden soll.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme skipaclupdatecheck	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt an, ob Kontrollsummen- und Größenvergleiche vor und nach einer Sicherung und während einer Teilsicherung ausgeführt werden sollen.
Windows-Betriebssysteme skipntpermissions	Windows-BetriebssystemeGibt an, ob Windows-Sicherheitsinformationen gesichert, archiviert, abgerufen oder zurückgeschrieben werden sollen.
Windows-Betriebssysteme skipntsecuritycrc	Windows-BetriebssystemeGibt an, ob während nachfolgender Sicherungen die Sicherheits-CRC-Prüfung für den Berechtigungsvergleich berechnet werden soll. Verwenden Sie diese Option für alle Windows-Clients.
AIX-BetriebssystemeLinux-Betriebssysteme Windows-Betriebssysteme snapdiff	AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme Gibt eine Teilsicherung der Dateien an, die von NetApp als geändert aufgelistet wurden, anstatt den Datenträger auf Dateien zu untersuchen, die sich geändert haben. Verwenden Sie diese Option bei der Teilsicherung von vollständigen NAS-Datenträgern.

Option	Beschreibung
  snapshotcachesize	 Nur für Linux und AIX: Verwenden Sie diese Option, um eine entsprechende Momentaufnahmengröße anzugeben, damit alle ursprünglichen Datenblöcke während der Dateiänderung und -löschung gespeichert werden können. Eine Momentaufnahmengröße von 100 Prozent gewährleistet eine gültige Momentaufnahme. Der Standardwert ist 100 Prozent.
 snapshotproviderfs	 Verwenden Sie die Option snapshotproviderfs, um momentaufnahmebasierte Dateisicherungs- und Dateiarchivierungsoperationen zu aktivieren und einen Momentaufnahmeprovider anzugeben. Sie müssen Root sein, um eine momentaufnahmebasierte Dateisicherungs- oder Dateiarchivierungsoperation auszuführen. Wenn Sie kein Rootbenutzer sind, schlägt die Operation mit einer Fehlernachricht fehl.
 snapshotproviderfs	 Verwenden Sie die Option snapshotproviderfs , um Dateisicherungs- und Dateiarchivierungsoperationen auf Momentaufnahmebasis zu aktivieren und einen Momentaufnahmeprovider anzugeben.
  snapshotproviderimage	 Verwenden Sie die Option snapshotproviderimage, um momentaufnahmebasierte Imagesicherung zu aktivieren und einen Momentaufnahmeprovider anzugeben. Sie müssen Root sein, um eine momentaufnahmebasierte Imagesicherungsoperation auszuführen. Wenn Sie kein Rootbenutzer sind, schlägt die Operation mit einer Fehlernachricht fehl.
 snapshotproviderimage	 Verwenden Sie die Option snapshotproviderimage, um eine momentaufnahmebasierte Online-Imagesicherung zu aktivieren und einen Momentaufnahmeprovider anzugeben.
 snapshotroot	 Verwenden Sie die Option snapshotroot im Befehl incremental, selective oder archive mit einer Anwendung eines unabhängigen Softwareanbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.
    snapshotroot	  Verwenden Sie die Option snapshotroot im Befehl incremental, selective oder archive mit einer Anwendung eines unabhängigen Softwareanbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind. Diese Option ist für alle UNIX- und Linux-Clients gültig.
subdir	Gibt an, ob Unterverzeichnisse eines benannten Verzeichnisses eingeschlossen werden sollen.
tapeprompt	Gibt an, ob der Client auf einen Bandladevorgang, der für einen Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufprozess erforderlich ist, warten soll, oder ob eine Bedienerführung für die Auswahl angezeigt werden soll.
   toc	   Verwenden Sie die Option toc mit dem Befehl backup nas oder der Option include.fs.nas, um anzugeben, ob der Client für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Wenn Sie TOC-Informationen speichern, können Sie den Serverbefehl QUERY TOC verwenden, um den Inhalt einer Dateisystemsicherung zu bestimmen, sowie den Serverbefehl RESTORE NODE, um einzelne Dateien oder Verzeichnisstrukturen zurückzuschreiben. Sie können auch den Web-Client verwenden, um die gesamte Baumstruktur des Dateisystems zu untersuchen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen.
type	Verwenden Sie die Option type im Befehl query node, um den Typ des abzufragenden Knotens anzugeben.

Option	Beschreibung
v2archive	Verwenden Sie die Option v2archive im Befehl archive, um anzugeben, dass nur Dateien auf dem Server archiviert werden sollen. Der Client verarbeitet keine Verzeichnisse, die in dem Pfad der Quellendateispezifikation vorhanden sind.
virtualfsname (gilt nicht für Mac OS X)	Verwenden Sie diese Option im Befehl backup group, um den Namen des Containers für die Gruppe anzugeben, mit der die Operation ausgeführt werden soll.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme virtualmountpoint	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeDefiniert einen virtuellen Mountpunkt für ein Dateisystem, wenn Dateien für die Sicherung berücksichtigt werden sollen, die mit einem bestimmten Verzeichnis innerhalb dieses Dateisystems beginnen.
Linux-BetriebssystemeWindows-Betriebssysteme vmchost	Linux-BetriebssystemeWindows-BetriebssystemeWird mit den Befehlen backup VM, restore VM und query VM verwendet, um den Hostnamen des VMware VirtualCenter oder des ESX-Servers anzugeben, an das/den die Befehle gerichtet sind.
Linux-BetriebssystemeWindows-Betriebssysteme vmcpw	Linux-BetriebssystemeWindows-BetriebssystemeWird mit den Befehlen backup VM, restore VM und query VM verwendet, um das Kennwort des VirtualCenter- oder ESX-Benutzers anzugeben, das mit der Option vmcuser angegeben ist.
Linux-BetriebssystemeWindows-Betriebssysteme vmcuser	Linux-BetriebssystemeWindows-BetriebssystemeWird mit den Befehlen backup VM, restore VM und query VM verwendet, um den Benutzernamen des VMware VirtualCenter oder des ESX-Servers anzugeben, an das/den die Befehle gerichtet sind.
Linux-BetriebssystemeWindows-Betriebssysteme vmmaxvirtualdisks	Linux-BetriebssystemeWindows-BetriebssystemeWird mit dem Befehl backup VM verwendet, um die maximale Größe von Platten virtueller VMware-Maschinen (VMDKs) anzugeben, die in eine Sicherungsoperation eingeschlossen werden sollen.
Linux-BetriebssystemeWindows-Betriebssysteme vmskipmaxvirtualdisks	Linux-BetriebssystemeWindows-BetriebssystemeWird mit dem Befehl backup VM verwendet, um anzugeben, wie die Sicherungsoperation Platten virtueller VMware-Maschinen (VMDKs) verarbeitet, die die maximale Plattengröße überschreiten. In Version 7.1.3 und früheren Versionen hatte die Option vmskipmaxvirtualdisks den Namen vmskipmaxvmdks.
Linux-BetriebssystemeWindows-Betriebssysteme	Linux-BetriebssystemeWindows-Betriebssysteme

Windows-BetriebssystemeDie folgenden Optionen sind Optionen des Clients für Sichern/Archivieren, die nur für umgelagerte Dateien von IBM Spectrum Protect HSM for Windows gelten.

Windows-Betriebssysteme

- Restorecheckstubaccess
- Restoremigstate
- Skipmigrated

Zugehörige Konzepte:
Windows-Betriebssysteme Optionen für die Sicherung umgelagerter Dateien: skipmigrated, checkreparsecontent, stagingdirectory
Windows-Betriebssysteme Optionen für die Zurückschreibung umgelagerter Dateien: restorecheckstubaccess, restoremigstate

Verarbeitungsoptionen für Zurückschreiben und Abrufen

Sie können Clientoptionen zur Steuerung einiger Aspekte der Zurückschreibungs- und Abrufverarbeitung verwenden.

In Tabelle 1 sind die verfügbaren Verarbeitungsoptionen für Zurückschreiben und Abrufen aufgelistet.

Tabelle 1. Verarbeitungsoptionen für Zurückschreiben und Abrufen

Option	Beschreibung
Windows-Betriebssystemeasrmode	Windows-BetriebssystemeVerwenden Sie diese Option mit den Befehlen restore und restore systemstate, um anzugeben, ob eine Zurückschreibungsoperation im ASR-Systemwiederherstellungsmodus ausgeführt wird. Diese Option wird nur im Kontext von Zurückschreibungsbefehlen verwendet, die in der Datei asr.sif durch den Befehl backup asr generiert werden. Diese Option darf außerhalb des Kontexts des ASR-Wiederherstellungsmodus nicht verwendet werden.

Option	Beschreibung
Windows-Betriebssystemebackupsetname	Windows-BetriebssystemeDie Option backupsetname gibt entweder den Namen des Sicherungssatzes an oder den Namen der Datei oder der Bandeinheit, die den Sicherungssatz enthält. Diese Option wird zusammen mit der Option location verwendet.
dirsonly	Qualifiziert die Operation (Sichern, Archivieren, Zurückschreiben, Abrufen), sodass nur Verzeichnisse verarbeitet werden.
disablenqr	Gibt an, ob der Client für Sichern/Archivieren die Methode zur Zurückschreibung ohne Abfrage verwenden kann, um Dateien und Verzeichnisse vom Server zurückzuschreiben.
filelist	Gibt eine Datei an, die eine Liste der Dateien enthält, die von dem angegebenen Befehl verarbeitet werden sollen.
filesonly	Qualifiziert die Operation (Sichern, Archivieren, Zurückschreiben, Abrufen), sodass nur Dateien verarbeitet werden.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemefollowsymbolic	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt an, ob Dateien in symbolische Verbindungen zurückgeschrieben werden sollen oder ob eine symbolische Verbindung als virtueller Mountpunkt verwendet werden soll.
fromdate	Mit der Option fromdate können Sie in Verbindung mit der Option fromtime ein Datum mit Uhrzeit angeben, ab dem Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
fromnode	Ermöglicht, dass ein Knoten Befehle für einen anderen Knoten ausführen kann. Ein Benutzer auf einem anderen Knoten muss Ihnen mit dem Befehl set access die Berechtigung zum Abfragen, Zurückschreiben oder Abrufen von Dateien oder Images für diesen anderen Knoten erteilen.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemefromowner	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDateibereiche für einen alternativen Eigner anzeigen. Außerdem einen alternativen Eigner angeben, von dem Dateien zurückgeschrieben oder abgerufen werden sollen.
fromtime	Mit der Option fromtime können Sie in Verbindung mit der Option fromdate eine Anfangszeit angeben, ab der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
ifnewer	Ersetzt eine vorhandene Datei nur dann durch die neueste Sicherungsversion, wenn die Sicherungsversion aktueller als die vorhandene Datei ist.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssystemeimagetofile	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeVerwenden Sie die Option imagetofile im Befehl restore image, um anzugeben, dass Sie das Quellenimage in eine Datei zurückschreiben wollen. Es kann erforderlich sein, das Image in eine Datei zurückzuschreiben, wenn der Zieldatenträger defekte Sektoren enthält oder die Imagedaten bearbeitet werden sollen. Diese Option ist für AIX-, Linux- und Solaris-Clients gültig.
Windows-Betriebssystemeimagetofile	Windows-BetriebssystemeVerwenden Sie die Option imagetofile im Befehl restore image, um anzugeben, dass Sie das Quellenimage in eine Datei zurückschreiben wollen. Es kann erforderlich sein, das Image in eine Datei zurückzuschreiben, wenn der Zieldatenträger defekte Sektoren enthält oder die Imagedaten bearbeitet werden sollen.
inactive	Zeigt bei Verwendung mit der Option pick eine Liste aktiver und inaktiver Dateien an.
latest	Die letzte Sicherungsversion einer Datei zurückschreiben, unabhängig davon, ob sie aktiv oder inaktiv ist.
localbackupset	Gibt an, ob die GUI des Clients für Sichern/Archivieren die anfängliche Anmeldung am Server umgeht, um einen lokalen Sicherungssatz auf einer eigenständigen Workstation zurückzuschreiben.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssystememakesparsefile (gilt nicht für Mac OS X)	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeVerwenden Sie die Option makesparsefile im Befehl restore oder retrieve, um anzugeben, wie Dateien mit freien Bereichen erneut erstellt werden.

Option	Beschreibung
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystememonitor	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeGibt an, ob Sie eine Imagezurückschreibung eines oder mehrerer zu einem NAS-Dateiserver gehörenden Dateisysteme überwachen wollen.
Mac OS X-Betriebssystemenoprompt	Mac OS X-BetriebssystemeUnterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group, delete archive, expire und set event angezeigt wird.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemenoprompt	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeUnterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group, delete archive, expire, restore image und set event angezeigt wird.
Windows-Betriebssystemeoptfile	Windows-BetriebssystemeGibt die Clientoptionsdatei an, die Sie verwenden wollen, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemeoptfile	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeGibt die Clientbenutzeroptionsdatei an, die Sie verwenden wollen, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.
pick	Erstellt eine Liste der Sicherungsversionen, Images oder Archivierungskopien, die der eingegebenen Dateispezifikation entsprechen. Aus der Liste können die zu verarbeitenden Versionen ausgewählt werden. Fügen Sie die Option inactive ein, um sowohl aktive als auch inaktive Objekte anzuzeigen.
pitdate	Sie können mit der Option pitdate in Verbindung mit der Option pittime einen Zeitpunkt definieren, für den die aktuellsten Sicherungsversionen angezeigt oder zurückgeschrieben werden sollen.
pittime	Sie können mit der Option pittime in Verbindung mit der Option pitdate einen Zeitpunkt definieren, für den die aktuellsten Sicherungsversionen angezeigt oder zurückgeschrieben werden sollen.
preservepath	Gibt an, wie viel vom Quellenpfad als Teil des Zielverzeichnispfades wiederherzustellen ist, wenn Dateien an eine neue Position zurückgeschrieben oder abgerufen werden.
replace	Gibt an, ob eine vorhandene Datei überschrieben werden soll oder ob Sie zur Eingabe Ihrer Auswahl aufgefordert werden sollen, wenn Sie Dateien zurückschreiben oder abrufen.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemeshowmembers (gilt nicht für Mac OS X)	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeZeigt alle Member einer Gruppe an.
subdir	Gibt an, ob Sie Unterverzeichnisse eines benannten Verzeichnisses einschließen wollen.
tapeprompt	Gibt an, ob der Client für Sichern/Archivieren auf das Laden eines für eine Zurückschreibung oder einen Abruf erforderlichen Bands warten soll oder ob Sie zur Eingabe Ihrer Auswahl aufgefordert werden sollen.
todate	Mit der Option todate können Sie in Verbindung mit der Option totime ein Enddatum mit einer Endzeit angeben, bis zu dem Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
totime	Mit der Option totime können Sie in Verbindung mit der Option todate ein Enddatum und eine Endzeit angeben, bis zu der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
type	Verwenden Sie die Option type im Befehl query node, um den Typ des abzufragenden Knotens anzugeben.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssystemeverifyimage	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeVerwenden Sie die Option verifyimage im Befehl restore image, um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client eine Warnung auf der Konsole und im Fehlerprotokoll aus.

Option	Beschreibung
Windows-Betriebssystemeverifyimage	Windows-BetriebssystemeVerwenden Sie die Option verifyimage im Befehl restore image, um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client eine Warnung auf der Konsole und im Fehlerprotokoll aus.

Die folgenden Optionen sind Optionen des Clients für Sichern/Archivieren, die für umgelagerte Dateien von IBM Spectrum Protect HSM for Windows gelten. Weitere Informationen zu diesen Optionen finden Sie in den Abschnitten des IBM® Knowledge Center unter http://www.ibm.com/support/knowledgecenter/SSERFH_8.1.2/hsmwin/welcome.html.

- Checkreparsecontent
- Restorecheckstubaccess
- Restoremigstate
- Skipmigrated

Die folgenden Optionen sind Optionen des Clients für Sichern/Archivieren, die für umgelagerte Dateien von IBM Spectrum Protect for Space Management gelten. Weitere Informationen zu diesen Optionen finden Sie in den Abschnitten des IBM Knowledge Center unter http://www.ibm.com/support/knowledgecenter/SSERBH_8.1.2/hsmul/welcome.html.

- Restoremigstate
- Skipmigrated

Planungsoptionen

In diesem Abschnitt sind die Optionen beschrieben, die Sie zum Steuern der zentralen Zeitplanung verwenden können. Der Client für Sichern/Archivieren verwendet Planungsoptionen nur, wenn der Scheduler aktiv ist.

In Tabelle 1 sind die verfügbaren Planungsoptionen aufgelistet.

Tabelle 1. Planungsoptionen

Option	Beschreibung
cadlistenonport	Gibt an, ob Empfangsports für den Clientakzeptor geöffnet werden sollen, wenn der Clientakzeptor zum Verwalten von Zeitplänen im Abfragemodus verwendet wird.
managedservices	Gibt an, ob der Clientakzeptor den Web-Client und/oder den Scheduler verwaltet.
maxcmdretries	Gibt an, wie oft der Client-Scheduler einen geplanten Befehl, der bei der Ausführung fehlgeschlagen ist, maximal zu wiederholen versucht.
Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWindows-Betriebssysteme postschedulecmd/postnschedulecmd	Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWindows-BetriebssystemeGibt einen Befehl an, der nach Ausführung eines Zeitplans verarbeitet werden soll.
Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWindows-Betriebssysteme preschedulecmd/prenschedulecmd	Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWindows-BetriebssystemeGibt einen Befehl an, der vor Ausführung eines Zeitplans verarbeitet werden soll.
queryschedperiod	Gibt die Anzahl Stunden an, die der Client-Scheduler zwischen den Versuchen, geplante Arbeit auf dem Server abzufragen, wartet.
retryperiod	Gibt die Anzahl Minuten an, die der Client-Scheduler zwischen den Versuchen, einen geplanten Befehl, der fehlgeschlagen ist, zu verarbeiten oder zwischen fehlgeschlagenen Versuchen, Ergebnisse an den Server zu melden, wartet.
Windows-Betriebssystemerunasservice	Windows-BetriebssystemeErzwingt die Fortsetzung der Clientbefehlsverarbeitung, auch wenn sich das Konto, das den Client gestartet hat, abmeldet. Verwenden Sie diese Option für alle Windows-Clients.
schedcmddisabled	Gibt an, ob die Zeitplanung generischer Befehle, die von Ihrem IBM Spectrum Protect-Administrator angegeben werden, inaktiviert werden soll.

Option	Beschreibung
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme schedcmduser (nur serverdefiniert)	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDer Scheduler führt Befehle unter der UID 0 aus; es kann jedoch einige Benutzer geben, die eine andere Benutzer-ID haben. In diesem Fall kann Ihr IBM Spectrum Protect-Administrator mithilfe dieser Option Zeitpläne definieren and zulassen, dass diese Zeitpläne unter einer anderen UID als 0 ausgeführt werden. Die IBM Spectrum Protect-Client-API unterstützt diese Option nicht.
schedlogmax Schedlogmax	Gibt die maximale Größe des Planungsprotokolls und des Web-Client-Protokolls in Megabyte an.
schedlogname Schedlogname	Gibt den Pfad und den Namen der Datei an, in der die Planungsprotokolldaten gespeichert werden sollen.
schedlogretention	Gibt die Anzahl Tage an, die Einträge im Planungsprotokoll und im Web-Client-Protokoll aufbewahrt werden sollen, und gibt an, ob bereinigte Einträge gesichert werden sollen.
schedmode	Gibt an, welcher Planungsmodus verwendet werden soll, Ausführung bei Clientsendeaufruf (*polling*) oder servergesteuerte Ausführung (*prompted*).
schedrestretrdisabled	Gibt an, ob verhindert werden soll, dass der IBM Spectrum Protect-Serveradministrator Planungsoperationen für Zurückschreibung oder Abruf ausführt.
sessioninitiation	Verwenden Sie die Option sessioninitiation, um zu steuern, ob der Server oder der Client Sitzungen durch eine Firewall einleiten soll. Standardwert ist, dass der Client Sitzungen einleiten kann.
srvprepostscheddisabled	Gibt an, ob verhindert werden soll, dass der IBM Spectrum Protect-Serveradministrator bei der Ausführung geplanter Operationen Befehle vor und nach dem Zeitplan ausführt.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeWindows-Betriebssysteme srvprepostsnapdisabled	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeWindows-BetriebssystemeGibt an, ob verhindert werden soll, dass der IBM Spectrum Protect-Serveradministrator bei der Ausführung geplanter Operationen für Image-Momentaufnahmesicherungen Befehle vor und nach der Momentaufnahme ausführt.
tcpclientaddress	Gibt eine TCP/IP-Adresse an, wenn Ihr Clientknoten über mehrere Adressen verfügt und der Server eine Verbindung zu einer anderen Adresse herstellen soll als der, mit der die erste Verbindung zum Server hergestellt wurde. Der Server verwendet diese Adresse, wenn er die Operation mit Zeitplanung über Serversystemanfrage beginnt. Details siehe schedmode prompted (Schedmode).
tcpclientport	Gibt eine TCP/IP-Anschlussnummer für den Server an, mit der eine Verbindung zum Client hergestellt wird, wenn der Server die Operation mit Zeitplanung über Serversystemanfrage beginnt. Details siehe schedmode prompted (Schedmode).

Optionen für Format und Sprache

Mit Optionen für Format und Sprache können Sie unterschiedliche Datums-, Uhrzeit- und Zahlenformate für verschiedene Sprachen auswählen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMit Formatoptionen können Sie unterschiedliche Formate für Datum, Uhrzeit und Zahlen auswählen.

Tabelle 1. Optionen für Format und Sprache

Option	Beschreibung
dateformat	Gibt das Format für das Anzeigen von Datumsangaben an.
Windows-Betriebssystemelanguage	Windows-BetriebssystemeGibt die Sprache an, die für Nachrichten verwendet wird.
numberformat	Gibt das Format für das Anzeigen von Zahlen an.
timeformat	Gibt das Format für das Anzeigen von Zeitangaben an.

Befehlsverarbeitungsoptionen

In diesem Abschnitt sind die Optionen beschrieben, die Sie mit den Befehlen des Clients für Sichern/Archivieren verwenden können.

Mit Optionen zur Befehlsverarbeitung können Sie einige Aspekte der Formatierung der Daten auf Ihrer Terminalanzeige steuern.

Tabelle 1. Befehlsverarbeitungsoptionen

Option	Beschreibung
quiet	Begrenzt die Anzahl der Nachrichten, die während der Verarbeitung auf dem Bildschirm angezeigt werden. Diese Option kann vom Server überschrieben werden.
scrolllines	Gibt die Anzahl Datenzeilen an, die gleichzeitig auf dem Bildschirm angezeigt werden. Verwenden Sie diese Option nur, wenn scrollprompt auf yes gesetzt ist.
scrollprompt	Gibt an, ob der Client für Sichern/Archivieren nach dem Anzeigen der Anzahl Datenzeilen, die Sie mit der Option scrolllines angegeben haben, stoppen und warten soll, oder ob durch alle Zeilen geblättert und am Ende der Datenliste gestoppt werden soll.
setwindowtitle	Gibt an, ob der IBM Spectrum Protect-Servername und der Host-Server-Name im Titel des Befehlsfensters für den Verwaltungsclient angezeigt werden sollen.
verbose	Gibt an, dass Verarbeitungsdaten auf Ihrem Bildschirm angezeigt werden sollen. Die Alternative dazu ist quiet. Diese Option kann vom Server überschrieben werden.

Berechtigungsoptionen

Über Berechtigungsoptionen wird der Zugriff auf den IBM Spectrum Protect-Server gesteuert.

In Tabelle 1 sind die verfügbaren Berechtigungsoptionen aufgelistet.

Tabelle 1. Berechtigungsoptionen

Option	Beschreibung
AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme autodeploy	AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeGibt an, ob Sie eine automatische Implementierung des Clients aktivieren oder inaktivieren wollen, wenn ein Neustart erforderlich ist.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemegroups	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeGibt die Gruppen auf Ihrer Workstation an, die Sie berechtigen wollen, IBM Spectrum Protect-Services vom Server anzufordern.
password	Gibt das IBM Spectrum Protect-Kennwort an.
passwordaccess	Gibt an, ob Sie bei jedem Start des Clients ein generiertes Kennwort verwenden oder ein Kennwort eingeben wollen.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme passworddir	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeGibt das Verzeichnis an, in dem Sie das automatisch generierte Kennwort für Ihren Clientknoten speichern wollen. Der Verschlüsselungsschlüssel und das Kennwort werden in der Datei TSM.sth verschlüsselt und gespeichert.
revokeremoteaccess	Beschränkt den Zugriff eines Administrators mit Clientzugriffsberechtigung auf Ihre Workstation durch den Web-Client.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemeusers	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeErteilt bestimmten Benutzern auf Ihrer Workstation die Berechtigung zum Anfordern von Services von einem Server.

Fehlerverarbeitungsoptionen

Fehlerverarbeitungsoptionen geben den Namen der Fehlerprotokolldatei sowie die Behandlung der Einträge in der Protokolldatei durch den Client für Sichern/Archivieren an.

In Tabelle 1 sind die verfügbaren Fehlerverarbeitungsoptionen aufgelistet.

Tabelle 1. Fehlerverarbeitungsoptionen

Option	Beschreibung

Option	Beschreibung
errorlogmax	Gibt die maximale Größe des Fehlerprotokolls in Megabyte an.
errorlogname Errorlogname	Gibt den vollständig qualifizierten Pfad und Dateinamen der Datei an, in der Informationen zu Fehlern gespeichert werden sollen, die während der Verarbeitung auftreten.
errorlogretention	Gibt an, wie viele Tage Fehlerprotokolleinträge aufbewahrt werden sollen, bevor sie bereinigt werden, und zeigt an, ob die bereinigten Einträge gesichert werden sollen.

Transaktionsverarbeitungsoptionen

Transaktionsverarbeitungsoptionen steuern, wie Transaktionen zwischen dem IBM Spectrum Protect-Client und -Server verarbeitet werden.

In Tabelle 1 sind die verfügbaren Transaktionsverarbeitungsoptionen aufgelistet.

Tabelle 1. Transaktionsverarbeitungsoptionen

Option	Beschreibung
collocatebyfilespec	Gibt an, ob der Client für Sichern/Archivieren nur eine einzige Serversitzung verwenden soll, um Objekte zu senden, die von einer einzigen Dateispezifikation generiert wurden. Durch das Setzen der Option collocatebyfilespec auf *yes* wird das Durchsetzen von Dateien von unterschiedlichen Dateispezifikationen eliminiert, indem der Client auf eine Serversitzung pro Dateispezifikation begrenzt wird. Wenn Sie Daten auf Band speichern, werden Dateien für jede Dateispezifikation deshalb zusammen auf einem Band gespeichert (sofern auf Grund erhöhter Kapazität kein weiteres Band erforderlich ist).
commrestartduration	Gibt die maximale Anzahl Minuten an, die der Client nach einem Übertragungsfehler versuchen soll, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen.
commrestartinterval	Gibt die Anzahl Sekunden an, die der Client nach einem Übertragungsfehler zwischen Versuchen, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen, warten soll.
diskbuffsize	Gibt die maximale Platten-E/A-Puffergröße (in Kilobyte) an, die der Client beim Lesen von Dateien verwenden kann.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme largecommbuffers	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeDiese Option wurde ersetzt durch die Option diskbuffsize. Derzeit wird largecommbuffers vom Client für Sichern/Archivieren noch akzeptiert, um den Übergang zu der neuen Option zu erleichtern. Der von largecommbuffers angegebene Wert wird jedoch zugunsten der Einstellung für diskbuffsize ignoriert. Wichtig: Verwenden Sie largecommbuffers nicht mehr, da diese Option in zukünftigen Releases des Clients möglicherweise nicht akzeptiert wird.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemenfstimeout	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeGibt die Wartezeit des Servers auf einen Statussystemaufruf für ein NFS-Dateisystem in Sekunden an, bevor eine Zeitlimitüberschreitung auftritt.
Windows-Betriebssysteme resourceutilization	Windows-BetriebssystemeMit der Option resourceutilization in Ihrer Clientoptionsdatei dsm.opt können Sie den Umfang der Ressourcen steuern, die der IBM Spectrum Protect-Server und -Client während der Verarbeitung verwenden können.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme resourceutilization	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeMit der Option resourceutilization in Ihrer Datei dsm.sys können Sie den Umfang der Ressourcen steuern, die der IBM Spectrum Protect-Server und -Client während der Verarbeitung verwenden können.
txnbytelimit	Gibt die Anzahl Kilobyte an, die das Clientprogramm puffert, bevor es eine Transaktion an den Server sendet.
Windows-Betriebssystemeusedirectory	Windows-BetriebssystemeBietet einen bequeme Möglichkeit, die Client-DFV-Konfiguration zu vereinfachen, indem die in der Clientoptionsdatei definierten Parameter für commmethod überschrieben werden und stattdessen das Active Directory nach der Übertragungsmethode und dem Server abgefragt wird.

Web-Client-Optionen

Zum Konfigurieren des IBM Spectrum Protect-Web-Clients werden verschiedene Optionen des Clients für Sichern/Archivieren verwendet.

In Tabelle 1 sind die verfügbaren Web-Client-Optionen aufgelistet.

Tabelle 1. Web-Client-Optionen

Option	Beschreibung
httpport	Gibt eine TCP/IP-Anschlussadresse für den Web-Client an.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystememanagedservices	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt an, ob der Clientakzeptordämon den Web-Client und/oder den Scheduler verwaltet.
Windows-Betriebssystememanagedservices	Windows-BetriebssystemeGibt an, ob der Clientakzeptorservice den Web-Client und/oder den Scheduler verwaltet.
revokeremoteaccess	Beschränkt den Administratorzugriff auf eine Workstation über den Web-Client.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemewebports	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAktiviert die Verwendung des Web-Clients außerhalb einer Firewall, indem die TCP/IP-Anschlussnummer angegeben wird, die vom Clientakzeptordämon und dem Web-Client-Agentenservice für die Kommunikation mit dem Web-Client verwendet wird.
Windows-Betriebssystemewebports	Windows-BetriebssystemeAktiviert die Verwendung des Web-Clients außerhalb einer Firewall, indem die TCP/IP-Anschlussnummer angegeben wird, die vom Clientakzeptorservice und dem Web-Client-Agentenservice für die Kommunikation mit dem Web-Client verwendet wird.

Optionen in Befehlen verwenden

Sie können einige der Optionen in Ihrer Clientoptionsdatei (dsm.opt) überschreiben, indem Sie sie mit den entsprechenden Befehlen des Clients für Sichern/Archivieren eingeben.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSie können einige Optionen in Ihrer Datei dsm.sys oder Clientbenutzeroptionsdatei (dsm.opt) überschreiben, indem Sie sie mit den entsprechenden Befehlen des Clients für Sichern/Archivieren eingeben.

Der Client verarbeitet die Optionen in folgender Reihenfolge (Vorrangstellung):

1. Auf dem Server definierte Optionen mit vom Server erzwungenen Clientoptionen. Der Server überschreibt die Clientwerte.
2. Optionen, die lokal in die Befehlszeile eingegeben werden.
3. Optionen, die unter Verwendung der Optionsparameter für einen Zeitplan auf dem Server definiert werden.
4. Optionen, die lokal in die Optionsdatei eingegeben werden.
5. Vom Server empfangene Optionen mit Clientoptionsgruppen, die nicht wie vom Server erzwungen definiert werden. Der Server überschreibt die Clientwerte *nicht*, wenn dies nicht erzwungen wird.
6. Standardoptionswerte.

- Optionen mit einem Befehl eingeben
  Sie müssen die allgemeinen Regeln für die Eingabe von Optionen mit einem Befehl befolgen.
- Ausschließlich in der Anfangsbefehlszeile gültige Optionen
  Eine Untergruppe von Clientoptionen ist nur in der Anfangsbefehlszeile gültig. Viele dieser Optionen bauen die Laufzeitumgebung auf, wie z. B. die Optionen commmethod und optfile. Optionen in dieser Kategorie sind im Dialog-, Makro- oder Schedulermodus nicht gültig. Sie generieren einen Fehler und führen dazu, dass die Verarbeitung gestoppt wird.
- Clientoptionen, die vom IBM Spectrum Protect-Server definiert werden können
  Einige Clientoptionen können vom IBM Spectrum Protect-Server definiert werden.

Optionen mit einem Befehl eingeben

Sie müssen die allgemeinen Regeln für die Eingabe von Optionen mit einem Befehl befolgen.

- Einen Befehl, einen Bindestrich (–), den Optionsnamen, ein Gleichheitszeichen (=) und den Optionswert oder -parameter eingeben. Auf beiden Seiten des Gleichheitszeichens (=) dürfen keine Leerzeichen sein.

  Die folgenden Beispiele zeigen diese Syntax für verschiedene Clients:

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

  ```
  dsmc archive -description="Jahresende 1999" /home/
  ```

  Windows-Betriebssysteme

  ```
  dsmc archive -description="Projekt A" c:\devel\proj1\*
  ```

- Bei Optionen, die über keine Parameter verfügen, müssen ein Befehl, ein Bindestrich (–) und der Optionsname eingegeben werden. Beispiel:

```
dsmc incremental -quiet
```

Anmerkung: Verwenden Sie einen führenden Bindestrich (-), um anzuzeigen, dass der folgende Text der Name einer Option ist. Wenn ein Objektname mit einem Bindestrich beginnt, müssen Sie ihn entweder in Hochkommas (') oder in Anführungszeichen (") einschließen. Die meisten Betriebssystem-Befehlszeilenprozessoren entfernen die Hochkommas bzw. Anführungszeichen, bevor die Befehlszeilenargumente an die IBM Spectrum Protect-Clientanwendung übergeben werden. In diesen Fällen müssen Sie Escapezeichen oder doppelte Hochkommas bzw. Anführungszeichen verwenden, damit der Client den Objektnamen in Hochkommas/Anführungszeichen empfangen kann. Im Schleifenmodus schließen Sie solche Objekte entweder in Hochkommas (') oder in Anführungszeichen (") ein.

- Den Optionsnamen oder eine Abkürzung des Optionsnamens eingeben. Für die Option latest kann beispielsweise `-lat` oder `-latest` angegeben werden. Die Großbuchstaben in der Optionssyntax zeigen die Mindestabkürzung für den betreffenden Optionsnamen an.
- Optionen vor oder hinter den Befehlsparametern eingeben. Sie können beispielsweise die Option subdir vor oder hinter einer Dateispezifikation eingeben: AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

```
dsmc selective -subdir=yes "/home/devel/proj1/*"
dsmc selective "/home/devel/proj1/*" -subdir=yes
```

Windows-Betriebssysteme

```
dsmc selective -subdir=yes c:\devel\proj1\*
dsmc selective c:\devel\proj1\* -subdir=yes
```

- Wenn Sie mehrere Optionen in einem Befehl eingeben, müssen Sie sie durch eine Leerstelle trennen.
- Schließen Sie den Wert in Anführungszeichen (" ") ein, wenn der von Ihnen eingegebene Optionswert ein Leerzeichen enthält. Zum Beispiel: AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

```
dsmc archive -description="Projekt A" "/home/devel/proj1/*"
```

Windows-Betriebssysteme

```
dsmc archive -description="Projekt A" c:\devel\proj1\*
```

- Die meisten Optionen, die Sie in der Befehlszeile eingeben, überschreiben den in der Vorgabendatei definierten Wert. Wenn Sie jedoch die Option domain mit dem Befehl incremental verwenden, wird die Angabe zu der in Ihrer Clientoptionsdatei angegebenen Domäne hinzugefügt, statt den aktuellen Wert zu überschreiben.
- AIX-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBei AIX, Solaris, Linux on z und Mac beträgt die maximale Anzahl Zeichen für einen Dateinamen 255. Die maximale Länge der Kombination aus Dateiname und Pfadname ist 1024 Zeichen. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthalten könnte, variieren kann.
- Linux-BetriebssystemeBei Linux beträgt die maximale Länge für einen Dateinamen 255 Byte. Die maximale Länge der Kombination aus Dateiname und Pfadname beträgt 4096 Byte. Diese Länge entspricht dem vom Betriebssystem unterstützten Wert für PATH_MAX. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, aus denen ein Pfad- und Dateiname besteht, variieren kann. Die tatsächliche Begrenzung ist die Anzahl Byte in den Pfad- und Dateikomponenten, die einer gleichen Anzahl Zeichen entsprechen kann, aber nicht muss.

  Linux-BetriebssystemeBei Linux beträgt die maximale Länge, die Sie für eine Kombination aus Pfad- und Dateiname angeben können, für Archivierungs- oder Abrufoperationen weiterhin 1024 Byte.

- Windows-BetriebssystemeDie maximale Anzahl Byte für einen Dateinamen und einen Dateipfad beträgt zusammen 6255. Der Dateiname selbst darf jedoch 255 Byte nicht überschreiten und der Pfad, der zur Datei führt, darf 6000 Byte nicht überschreiten. Darüber hinaus sind Verzeichnisnamen (einschließlich des Verzeichnisbegrenzers) innerhalb eines Pfads auf 255 Byte begrenzt. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthalten könnte, variieren kann.
- Mac OS X-BetriebssystemeFür Mac OS X: Die maximale Länge eines Dateinamens ist auf 504 Byte (nicht Zeichen) begrenzt. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthält, variieren kann.

Ausschließlich in der Anfangsbefehlszeile gültige Optionen

Eine Untergruppe von Clientoptionen ist nur in der Anfangsbefehlszeile gültig. Viele dieser Optionen bauen die Laufzeitumgebung auf, wie z. B. die Optionen commmethod und optfile. Optionen in dieser Kategorie sind im Dialog-, Makro- oder Schedulermodus nicht gültig. Sie generieren einen Fehler und führen dazu, dass die Verarbeitung gestoppt wird.

In Tabelle 1 sind die Optionen aufgelistet, die nur in der Anfangsbefehlszeile gültig sind.

Tabelle 1. Optionen, die nur in der Anfangsbefehlszeile gültig sind

Optionen, die in der Anfangsbefehlszeile gültig sind	

Optionen, die in der Anfangsbefehlszeile gültig sind	
• Windows-Betriebssystemeasrmode • Windows-Betriebssystemebackupregistry • commmethod • Windows-Betriebssystemecomputername • deduplication • diskbuffsize • editor • enablededupcache • AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme enablelanfree • errorlogmax • errorlogname • errorlogretention • Windows-Betriebssystemeincrthreshold • AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme lanfreecommmethod • AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme lanfreeshmport • AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme lanfreetcpport • maxcmdretries • Windows-Betriebssystemenamedpipename • AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme nfstimeout • nodename • optfile • password • postschedulecmd/postnschedulecmd (kann in die Zeitplandefinition eingeschlossen werden) • Windows-Betriebssystemepostsnapshotcmd	• preschedulecmd/prenschedulecmd (kann in die Zeitplandefinition eingeschlossen werden) • Windows-Betriebssystemepresnapshotcmd • queryschedperiod • resourceutilization • retryperiod • Windows-Betriebssystemerunasservice • schedlogmax • schedlogname • schedlogretention • schedmode • AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemeservername • sessioninitiation • setwindowtitle • tcpbuffsize • tcpcadaddress • tcpclientaddress • tcpclientport • Windows-Betriebssystemetcpport • Windows-Betriebssystemetcpserveraddress • tcpwindowsize • txnbytelimit • Windows-Betriebssystemeusedirectory • virtualnodename

Clientoptionen, die vom IBM Spectrum Protect-Server definiert werden können

Einige Clientoptionen können vom IBM Spectrum Protect-Server definiert werden.

In Tabelle 1 sind die Optionen aufgelistet, die vom Server definiert werden können.

Tabelle 1. Optionen, die vom IBM Spectrum Protect-Server definiert werden können

Optionen, die vom IBM Spectrum Protect-Server definiert werden können	

Optionen, die vom IBM Spectrum Protect-Server definiert werden können	
• AIX-BetriebssystemeLinux-BetriebssystemeAfmskipuncachedfiles • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeArchsymlinkasfile • Windows-BetriebssystemeCasesensitiveaware • Changingretries • Collocatebyfilespec • Compressalways • Compression • Deduplication • Dirmc • Disablenqr • Diskcachelocation • Domain • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeWindows-BetriebssystemeDomain.image • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeDomain.nas • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeEncryptiontype • Encryptkey • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeAusschlussoptionen • Inclexcl • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeEinschlussoptionen • maxcandprocs • maxmigrators • Memoryefficientbackup • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeNfstimeout • Postschedulecmd/Postnschedulecmd • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemePostsnapshotcmd • Preschedulecmd/Prenschedulecmd • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemePreservelastaccessdate • AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemePresnapshotcmd	• Queryschedperiod • Quiet • Windows-Betriebssysteme Resetarchiveattribute • Resourceutilization • Retryperiod • Schedmode • Scrolllines • Scrollprompt • AIX-Betriebssysteme Linux-BetriebssystemeSnapshotcachesize • AIX-Betriebssysteme Windows-Betriebssysteme Snapshotproviderfs • AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme Snapshotproviderimage • AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeStagingdirectory • Subdir • Tapeprompt • Txnbytelimit • Verbose • Linux-Betriebssysteme Windows-BetriebssystemeVmchost • Linux-Betriebssysteme Windows-BetriebssystemeVmcuser • Linux-Betriebssysteme Windows-Betriebssysteme Vmprocessvmwithindependent • Linux-Betriebssysteme Windows-Betriebssysteme Vmprocessvmwithprdm

Anmerkung:

1. Siehe die Produktdokumentation zu IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server im IBM® Knowledge Center unter http://www.ibm.com/support/knowledgecenter/SSERBW/welcome.

Zugehörige Tasks:
Clientoperationen über Clientoptionsgruppen steuern

Clientoptionsreferenz

Die folgenden Abschnitte enthalten detaillierte Informationen über die einzelnen IBM Spectrum Protect-Verarbeitungsoptionen.

Die Informationen zu jeder Option umfassen Folgendes:

- Beschreibung
- Syntaxdiagramm
- Detaillierte Beschreibung der Parameter
- Beispiele für die Verwendung der Option in der Clientoptionsdatei (falls zutreffend)
- Beispiele für die Verwendung der Option in der Befehlszeile (falls zutreffend)

Optionen mit dem Befehlszeilenbeispiel **Nicht zutreffend** können nicht in der Befehlszeile oder mit geplanten Befehlen verwendet werden.

Mac OS X-BetriebssystemeAnmerkung:

1. Schließen Sie einen Optionswert nicht in Hochkommas oder Anführungszeichen ein, es sei denn, der Wert ist eine Dateispezifikation, die Leerzeichen oder Platzhalterzeichen enthält. Die folgende Option ist beispielsweise ungültig:

   ```
   passwordaccess  "generate"
   ```

2. AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeAlle Optionen in der Datei dsm.sys mit Ausnahme der Option defaultserver müssen innerhalb einer Serverzeilengruppe eingefügt werden. Eine Serverzeilengruppe ist eine Gruppe von Optionsanweisungen in dsm.sys, die mit einer Option SERVERName beginnt und entweder bei der nächsten Option SERVERName oder am Dateiende endet.

- Absolute
  Mit der Option absolute im Befehl incremental können Sie eine Sicherung aller Dateien und Verzeichnisse erzwingen, die der Dateispezifikation oder domain entsprechen, auch wenn die Objekte sich seit der letzten Teilsicherung nicht geändert haben.
- Windows-BetriebssystemeAdlocation
  Sie können die Option adlocation in den Befehlen query adobjects oder restore adobjects verwenden, um anzugeben, ob die Active Directory-Objekte aus dem lokalen Container für gelöschte Active Directory-Objekte oder aus einer Systemstatussicherung auf dem IBM Spectrum Protect-Server abgefragt oder zurückgeschrieben werden sollen.
- AIX-BetriebssystemeLinux-BetriebssystemeAfmskipuncachedfiles
  Die Option afmskipuncachedfiles gibt an, ob bei General Parallel File System (GPFS) nicht zwischengespeicherte und genutzte Dateien in Active File Management-Dateigruppen bei Sicherungs-, Archivierungs- und Umlagerungsoperationen verarbeitet werden.
- Archmc
  Verwenden Sie die Option archmc im Befehl archive, um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Dateien und Verzeichnisse binden wollen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeArchsymlinkasfile
  Die Option archsymlinkasfile gibt an, ob der Client für Sichern/Archivieren einer symbolischen Verbindung folgt und die Datei oder das Verzeichnis archiviert, auf die/das die Verbindung zeigt, oder ob nur die symbolische Verbindung archiviert wird. Diese Option ist im Befehl archive zu verwenden.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAsnodename
  Mit der Option asnodename können Agentenknoten Daten im Namen eines anderen Knotens (des Zielknotens) sichern oder zurückschreiben. Auf diese Weise sind gleichzeitig ablaufende Operationen von mehreren Knoten möglich, um Daten auf demselben Zielknoten und in demselben Dateibereich parallel zu speichern.
- Windows-BetriebssystemeAsnodename
  Mit der Option asnodename kann ein Agentenknoten Daten im Namen eines Zielknotens sichern, archivieren, zurückschreiben, abrufen und abfragen.
- Windows-BetriebssystemeAsrmode
  Verwenden Sie die Option asrmode mit den Befehlen restore und restore systemstate, um anzugeben, ob eine Zurückschreibungsoperation im ASR-Systemwiederherstellungsmodus ausgeführt wird.
- Auditlogging
  Verwenden Sie die Option auditlogging, um ein Prüfprotokoll zu generieren, das für jede Datei, die während einer Teilsicherungsoperation, einer selektiven Sicherungsoperation, einer Archivierungs-, Zurückschreibungs- oder Abrufoperation verarbeitet wird, einen Eintrag enthält.
- Auditlogname
  Die Option auditlogname gibt den Pfad und den Namen der Datei an, in der Prüfprotokollinformationen gespeichert werden sollen. Diese Option wird angewendet, wenn die Prüfprotokollierung aktiviert ist.
- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme
  Windows-BetriebssystemeAutodeploy
  Verwenden Sie die Option autodeploy, um eine automatische Implementierung des Clients zu aktivieren oder zu inaktivieren, wenn ein Neustart erforderlich ist.
- Autofsrename
  Mit der Option autofsrename wird ein vorhandener, nicht Unicode-fähiger Dateibereich auf dem IBM Spectrum Protect-Server umbenannt, sodass für die aktuelle Operation ein Unicode-fähiger Dateibereich mit dem ursprünglichen Namen erstellt werden kann.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAutomount
  Die Option automount fügt durch Anhängen ein Auto-Mount-Dateisystem in die Domäne ein. Diese Option ist mit der Option domain zu verwenden.
- Linux-BetriebssystemeWindows-BetriebssystemeBackmc
  Die Option backmc gibt die Verwaltungsklasse an, die für Aufbewahrungszwecke auf den Befehl backup fastback angewendet werden soll.
- Backupsetname
  Die Option backupsetname gibt den Namen eines Sicherungssatzes auf dem IBM Spectrum Protect-Server an.
- Basesnapshotname
  Die Option basesnapshotname gibt die Momentaufnahme an, die als Basismomentaufnahme verwendet werden soll, wenn Sie eine Momentaufnahmedifferenzsicherung (snapdiff) eines NetApp-Dateiserverdatenträgers ausführen. Wenn Sie diese Option angeben, müssen Sie auch die Option snapdiff verwenden. Andernfalls tritt ein Fehler auf. Wenn basesnapshotname nicht angegeben wird, wählt die Option useexistingbase die jüngste Momentaufnahme auf dem Dateiserverdatenträger als Basismomentaufnahme aus.
- Cadlistenonport
  Die Option cadlistenonport gibt an, ob ein Empfangsport für den Clientakzeptor geöffnet werden soll.
- Windows-BetriebssystemeCasesensitiveaware
  Die Option casesensitiveaware gibt an, ob der Windows-Client für Sichern/Archivieren versucht, Datei- und Verzeichnisobjekte herauszufiltern, bei denen Namenskonflikte vorliegen, die durch unterschiedliche Groß-/Kleinschreibung verursacht werden.

- Changingretries
  Mit der Option changingretries wird angegeben, wie oft der Client den Versuch, eine im Gebrauch befindliche Datei zu sichern oder zu archivieren, wiederholen soll. Diese Option ist in den Befehlen archive, incremental und selective zu verwenden.
-  AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeWindows-BetriebssystemeClass
  Die Option class gibt an, ob bei Verwendung der Befehle delete filespace, query backup und query filespace eine Liste der NAS- oder der Clientobjekte angezeigt werden soll.
-  Windows-BetriebssystemeClientview
  Die Option clientview ist für Benutzer verfügbar, die ein Upgrade vom IBM® Tivoli Storage Manager Express-Sicherungsclient auf den Enterprise-Client für Sichern/Archivieren durchgeführt haben.
-  Windows-BetriebssystemeClusterdisksonly
  Die Option clusterdisksonly gibt an, ob der Client für Sichern/Archivieren die ausschließliche Sicherung von Clusterplatten in bestimmten Umgebungen zulässt.
-  Windows-BetriebssystemeClusternode
  Die Option clusternode gibt an, wie der Client für Sichern/Archivieren Clusterlaufwerke verwaltet.
- Collocatebyfilespec
  Verwenden Sie die Option collocatebyfilespec, um anzugeben, ob der Client für Sichern/Archivieren nur eine Serversitzung verwenden soll, um Objekte zu senden, die von einer einzigen Dateispezifikation generiert wurden.
- Commmethod
  Mit der Option commmethod wird die verwendete Übertragungsmethode für die Konnektivität der Client/Server-Übertragung angegeben.
- Commrestartduration
  Mit der Option commrestartduration wird die maximale Anzahl Minuten angegeben, die der Client nach einem Übertragungsfehler zwischen Versuchen, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen, warten soll.
- Commrestartinterval
  Mit der Option commrestartinterval wird die Anzahl Sekunden angegeben, die der Client nach einem Übertragungsfehler zwischen Versuchen, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen, warten soll.
- Compressalways
  Die Option compressalways gibt an, ob die Komprimierung eines Objekts fortgesetzt wird, wenn es während der Komprimierung größer wird.
- Compression
  Die Option compression komprimiert Dateien, bevor sie an den Server gesendet werden.
- Console
  Verwenden Sie die Option console im Befehl query systeminfo, um Informationen an der Konsole auszugeben.
- Createnewbase
  Die Option createnewbase erstellt eine Basismomentaufnahme und verwendet sie als Quelle für die Ausführung einer vollständigen Teilsicherung.
- Datacenter
  Gibt die Zielposition des Datencenters an, das die zurückgeschriebenen Maschinendaten enthalten soll.
- Datastore
  Gibt das Datenspeicherziel an, das während der VMware-Zurückschreibungsoperation verwendet werden soll.
- Dateformat
  Mit der Option dateformat wird das Format angegeben, das für die Anzeige oder Eingabe von Datumsangaben verwendet werden soll.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
   Windows-BetriebssystemeDedupcachepath
  Verwenden Sie die Option dedupcachepath, um die Position anzugeben, an der die Cachedatenbank für die clientseitige Datendeduplizierung erstellt wird.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
   Windows-BetriebssystemeDedupcachesize
  Verwenden Sie die Option dedupcachesize, um die maximale Größe der Cachedatei für die Datendeduplizierung festzulegen. Wenn die Cachedatei ihre maximale Größe erreicht, wird der Inhalt des Cache gelöscht und neue Einträge werden hinzugefügt.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
   Windows-BetriebssystemeDeduplication
  Verwenden Sie die Option deduplication, um anzugeben, ob die clientseitige Entfernung redundanter Daten bei der Übertragung von Daten an IBM Spectrum Protect während der Sicherungs- und Archivierungsverarbeitung aktiviert sein soll.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDefaultserver
  Verwenden Sie die Option defaultserver, um den Namen des IBM Spectrum Protect-Servers anzugeben, zu dem zwecks Sicherungs-/Archivierungsservices der Kontakt hergestellt werden soll, falls mehrere Server in der Datei dsm.sys definiert sind.
- Deletefiles
  Verwenden Sie die Option deletefiles im Befehl archive, um Dateien von Ihrer Workstation zu löschen, nachdem Sie sie archiviert haben.
- Description
  Die Option description ordnet Dateien beim Ausführen von Archivieren, Archivierung löschen, Abrufen, Archivierung abfragen oder Sicherungssatz abfragen eine Beschreibung zu oder gibt eine Beschreibung für diese Dateien an.
- Detail
  Verwenden Sie die Option detail, um abhängig vom Befehl, mit dem sie verwendet wird, Angaben zu Verwaltungsklasse, Dateibereich, Sicherung und Archivierung sowie zusätzliche Informationen anzuzeigen.
- Diffsnapshot
  Die Option diffsnapshot legt fest, ob der Client für Sichern/Archivieren die Differenzmomentaufnahme erstellt, wenn eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausgeführt wird.

- Diffsnapshotname
  Mit der Option diffsnapshotname können Sie angeben, welche Differenzmomentaufnahme auf dem Datenträger des Ziel-Dateiservers während einer Momentaufnahmedifferenzsicherung verwendet werden soll. Diese Option wird nur angegeben, wenn Sie auch diffsnapshot=latest angeben.
- Dirmc
  Mit der Option dirmc wird die Verwaltungsklasse angegeben, die für Verzeichnisse verwendet werden soll.
- Dirsonly
  Mit der Option dirsonly werden *nur* Verzeichnisse verarbeitet. Der Client verarbeitet keine Dateien.
- Disablenqr
  Die Option disablenqr gibt an, ob der Client für Sichern/Archivieren die Methode zur Zurückschreibung ohne Abfrage verwenden kann, um Dateien und Verzeichnisse vom Server zurückzuschreiben.
- Diskbuffsize
  Die Option diskbuffsize gibt die maximale Platten-E/A-Puffergröße (in Kilobyte) an, die der Client beim Lesen von Dateien verwenden kann. Die Option diskbuffsize ersetzt die Option largecommbuffers.
- Diskcachelocation
  Die Option diskcachelocation gibt die Position an, an der die Plattencachedatenbank erstellt wird, wenn die Option memoryefficientbackup=diskcachemethod bei einer Teilsicherung definiert ist.
- Domain
  Die Option domain gibt an, welche Objekte Sie bei Teilsicherungen einschließen wollen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeDomain.image
  Die Option domain.image gibt an, welche Objekte Sie bei einer Imagesicherung in Ihre Clientdomäne einschließen wollen.
- AIX-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeDomain.nas
  Die Option domain.nas gibt die Datenträger an, die bei Ihren NAS-Imagesicherungen berücksichtigt werden sollen.
- Linux-Betriebssysteme Windows-BetriebssystemeDomain.vmfull
  Die Option domain.vmfull gibt die Imagegesamtsicherungsoperationen für virtuelle Maschinen eingeschlossen werden sollen.
- Linux-BetriebssystemeDontload
  Linux x86_64-Clients können mit der Option dontload das Laden bestimmter Plugin-Bibliotheken beim Starten des Clients für Sichern/Archivieren unterdrücken.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDynamicimage
  Verwenden Sie die Option dynamicimage im Befehl backup image oder mit der Option include.image, um anzugeben, dass Sie eine dynamische Imagesicherung ausführen wollen.
- AIX-BetriebssystemeEfsdecrypt
  Mit der Option efsdecrypt können Sie steuern, ob Dateien, die von einem verschlüsselten AIX-Dateisystem (AIX-EFS) verschlüsselt wurden, in verschlüsseltem oder in entschlüsseltem Format gelesen werden sollen.
- Windows-BetriebssystemeEnable8dot3namesupport
  Die Option enable8dot3namesupport gibt an, ob der Client 8.3-Kurznamen für Dateien, die auf NTFS-Dateisystemen Langnamen haben, sichert und zurückschreibt.
- Enablearchiveretentionprotection
  Mit der Option enablearchiveretentionprotection kann der Client eine Verbindung zum IBM Spectrum Protect for Data Retention-Server herstellen. Dieser stellt sicher, dass Archivierungsobjekte erst dann auf dem Server gelöscht werden, wenn auf Richtlinien basierende Aufbewahrungskriterien für dieses Objekt erfüllt wurden.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeEnablededupcache
  Mit der Option enablededupcache geben Sie an, ob bei der clientseitigen Datendeduplizierung ein Cache verwendet werden soll. Die Verwendung eines lokalen Cache kann den Datenaustausch im Netz zwischen dem IBM Spectrum Protect-Server und dem Client reduzieren.
- Enableinstrumentation
  Standardmäßig werden Instrumentierungsdaten automatisch vom Client für Sichern/Archivieren und von der IBM Spectrum Protect-API erfasst, um Leistungsengpässe während der Sicherungs- und Zurückschreibungsverarbeitung zu identifizieren. Um die Instrumentierung zu inaktivieren oder später zu aktivieren, verwenden Sie die Option enableinstrumentation.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeEnablelanfree
  Die Option enablelanfree gibt an, ob ein verfügbarer LAN-unabhängiger Pfad zu einer an ein Speicherbereichsnetz (SAN) angeschlossenen Speichereinheit aktiviert werden soll.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeEncryptiontype
  Verwenden Sie die Option encryptiontype, um den Algorithmus für die Datenverschlüsselung anzugeben.
- Encryptkey
  Der Client für Sichern/Archivieren unterstützt die Option zum Verschlüsseln von Dateien, die auf dem IBM Spectrum Protect-Server gesichert oder archiviert werden. Diese Option wird mit der Option include.encrypt aktiviert.
- Errorlogmax
  Die Option errorlogmax gibt die maximale Größe des Fehlerprotokolls in Megabyte an. Der Standardname des Fehlerprotokolls lautet dsmerror.log.
- Errorlogname
  Diese Option gibt den vollständig qualifizierten Pfad und Dateinamen der Datei an, die die Fehlernachrichten enthält.
- Errorlogretention
  Die Option errorlogretention legt fest, wieviele Tage Fehlerprotokolleinträge aufbewahrt werden sollen, bevor sie bereinigt werden, und ob die bereinigten Einträge in anderen Dateien gespeichert werden sollen.

- Ausschlussoptionen
  Verwenden Sie die Ausschlussoptionen, um Objekte von Sicherungs-, Image- oder Archivierungsservices auszuschließen.
- Linux-BetriebssysteWindows-BetriebssystemeFbbranch
  Verwenden Sie die Option fbbranch mit dem Befehl backup fastback oder archive fastback.
- Linux-BetriebssysteWindows-BetriebssystemeFbclientname
  Verwenden Sie die Option fbclientname mit dem Befehl backup fastback oder archive fastback.
- Linux-BetriebssysteWindows-BetriebssystemeFbpolicyname
  Verwenden Sie die Option fbpolicyname mit dem Befehl backup fastback oder archive fastback.
- Linux-BetriebssysteWindows-BetriebssystemeFbreposlocation
  Verwenden Sie die Option fbreposlocation mit dem Befehl backup fastback oder archive fastback.
- Linux-BetriebssysteWindows-BetriebssystemeFbserver
  Verwenden Sie die Option fbserver mit dem Befehl backup fastback oder archive fastback.
- Linux-BetriebssysteWindows-BetriebssystemeFbvolumename
  Verwenden Sie die Option fbvolumename mit dem Befehl backup fastback oder archive fastback.
- Filelist
  Verwenden Sie die Option filelist, um eine Liste von Dateien zu verarbeiten.
- Filename
  Verwenden Sie die Option filename im Befehl query systeminfo, um den Namen einer Datei anzugeben, in der Informationen gespeichert werden sollen.
- Filesonly
  Mit der Option filesonly wird die Verarbeitung beim Sichern, Zurückschreiben, Abrufen oder Abfragen *nur* auf Dateien beschränkt.
- AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssystemeFollowsymbolic
  Bei einer Sicherungsoperation gibt die Option followsymbolic an, ob Sie eine symbolische Verbindung als virtuellen Mountpunkt verwenden wollen. Bei einer Zurückschreibungs- oder Abrufoperation gibt die Option followsymbolic an, wie der Client für Sichern/Archivieren ein Verzeichnis zurückschreibt, dessen Name mit einer symbolischen Verbindung auf dem Zieldateisystem für die Zurückschreibung übereinstimmt.
- Forcefailover
  Mit der Option forcefailover kann eine sofortige Übernahme des Clients auf dem Sekundärserver stattfinden.
- Fromdate
  Mit der Option fromdate können Sie in Verbindung mit der Option fromtime ein Datum mit Uhrzeit angeben, ab dem Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
- Fromnode
  Mit der Option fromnode kann ein Knoten Befehle für einen anderen Knoten ausführen. Ein Benutzer auf einem anderen Knoten muss mit dem Befehl set access die Berechtigung zum Abfragen, Zurückschreiben oder Abrufen von Dateien für diesen anderen Knoten erteilen.
- AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeFromowner
  Die Option fromowner gibt einen alternativen Eigner an, von dem Sicherungsversionen oder archivierte Dateien oder Images zurückgeschrieben werden sollen. Der Eigner muss einem anderen Benutzer eine Zugriffsberechtigung für die Dateien oder Images erteilen.
- Fromtime
  Mit der Option fromtime können Sie in Verbindung mit der Option fromdate eine Anfangszeit angeben, ab der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
- Groupname
  Verwenden Sie die Option groupname im Befehl backup group, um den Namen für eine Gruppe anzugeben. Operationen können nur mit neuen Gruppen oder der zurzeit aktiven Version einer Gruppe ausgeführt werden.
- AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeGroups (veraltet)
  Diese Option ist veraltet.
- Host
  Die Option 'host' gibt die Position des ESX-Zielservers an, auf dem die neue virtuelle Maschine während einer VMware-Zurückschreibungsoperation erstellt wird.
- Httpport
  Mit der Option httpport wird eine TCP/IP-Anschlussadresse für den Web-Client angegeben.
- Hsmreparsetag
  Die Option hsmreparsetag gibt eine eindeutige Analysekennung an, die von einem auf Ihrem System installierten HSM-Produkt erstellt wird.
- AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-Betriebssysteme
  Windows-BetriebssystemeIeobjtype
  Verwenden Sie die Option ieobjtype, um einen Objekttyp für eine clientseitige Operation für die Datendeduplizierung innerhalb von Einschluss-/Ausschlussanweisungen anzugeben.
- Ifnewer
  Mit der Option ifnewer wird eine vorhandene Datei nur dann durch die letzte Sicherungsversion ersetzt, wenn die Sicherungsversion neuer ist als die vorhandene Datei.
- AIX-BetriebssysteWindows-BetriebssystemeImagegapsize
  Verwenden Sie die Option imagegapsize im Befehl backup image, in der Optionsdatei oder mit der Option include.image, um die Mindestgröße der leeren Bereiche auf einem Datenträger anzugeben, die Sie während der Imagesicherung überspringen wollen.
- AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteWindows-BetriebssystemeImagetofile
  Verwenden Sie die Option imagetofile im Befehl restore image, um anzugeben, dass Sie das Quellenimage in eine Datei zurückschreiben wollen.

- Inactive
  Verwenden Sie die Option inactive, um sowohl aktive als auch inaktive Objekte anzuzeigen.
- Inclexcl
  Die Option inclexcl gibt den Pfad und Dateinamen der Einschluss-/Ausschlussoptionsdatei an.
- Einschlussoptionen
  Die Einschlussoptionen geben Objekte an, die Sie für Sicherungs- und Archivierungsservices eingeschlossen werden sollen.
- Incrbydate
  Verwenden Sie die Option incrbydate im Befehl incremental, um neue und geänderte Dateien zu sichern, deren Änderungsdatum nach dem Datum der letzten auf dem Server gespeicherten Teilsicherung liegt (sofern die Dateien nicht von der Sicherung ausgeschlossen sind).
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeIncremental
  Verwenden Sie die Option incremental im Befehl restore image, um sicherzustellen, dass am Basisimage vorgenommene Änderungen auch auf das zurückgeschriebene Image angewendet werden.
- Windows-BetriebssystemeIncrthreshold
  Die Option incrthreshold gibt den Schwellenwert für die Anzahl Verzeichnisse in einem Journaldateibereich an, für die aktive Objekte auf dem Server, aber keine äquivalenten Objekte auf der Workstation vorhanden sein können.
- Instrlogmax
  Die Option instrlogmax gibt die maximale Größe des Instrumentierungsprotokolls (dsminstr.log) in MB an. Während der Sicherungs- oder Zurückschreibungsverarbeitung werden Leistungsdaten für den Client in der Datei dsminstr.log erfasst, wenn die Option enableinstrumentation auf *yes* gesetzt ist.
- Instrlogname
  Die Option instrlogname gibt den Pfad und den Namen der Datei an, in der Leistungsdaten gespeichert werden sollen, die der Client für Sichern/Archivieren erfasst.
- Windows-BetriebssystemeJournalpipe
  Die Option journalpipe gibt den Namen der Pipe eines Journaldämonsitzungsmanagers an, zu dem die Sicherungsclients eine Verbindung herstellen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeLanfreecommmethod
  Die Option lanfreecommmethod gibt das Übertragungsprotokoll zwischen dem IBM Spectrum Protect-Client und dem Speicheragenten an. Dadurch wird die Verarbeitung zwischen dem Client und der an SAN angeschlossenen Speichereinheit aktiviert.
- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeLanfreeshmport
  Verwenden Sie die Option lanfreeshmport, wenn `lanfreecommmethod=SHAREdmem` für die Übertragung zwischen dem Client für Sichern/Archivieren und dem Speicheragenten angegeben wird. Dadurch wird die Verarbeitung zwischen dem Client und der an SAN angeschlossenen Speichereinheit aktiviert.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeLanfreetcpport
  Die Option lanfreetcpport gibt die Nummer des TCP/IP-Anschlusses an, an dem der IBM Spectrum Protect-Speicheragent empfangsbereit ist.
- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme
  Windows-BetriebssystemeLanfreessl
  Verwenden Sie die Option lanfreessl, um Secure Sockets Layer (SSL) für eine sichere Client- und Speicheragentenkommunikation zu aktivieren. Diese Option wird nicht mehr unterstützt, wenn Sie die Verbindung zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeLanfreetcpserveraddress
  Die Option lanfreetcpserveraddress gibt die TCP/IP-Adresse für den IBM Spectrum Protect-Speicheragenten an.
- Windows-BetriebssystemeLanguage
  Mit der Option language wird die Landessprache für die angezeigten Clientnachrichten angegeben.
- Latest
  Verwenden Sie die Option latest, um die neueste Sicherungsversion einer Datei zurückzuschreiben, auch wenn die Sicherung inaktiv ist.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
  Windows-BetriebssystemeLocalbackupset
  Die Option localbackupset gibt an, ob die GUI des Clients für Sichern/Archivieren die anfängliche Anmeldung beim IBM Spectrum Protect-Server umgeht, um einen lokalen Sicherungssatz auf einer eigenständigen Workstation zurückzuschreiben.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMakesparsefile
  Verwenden Sie die Option makesparsefile im Befehl restore oder retrieve, um anzugeben, wie Dateien mit freien Bereichen erneut erstellt werden.
- Managedservices
  Die Option managedservices gibt an, ob der IBM Spectrum Protect-Clientakzeptorservice den Scheduler und/oder den Web-Client verwaltet.
- Maxcmdretries
  Mit der Option maxcmdretries kann angegeben werden, wie oft der Client-Scheduler auf Ihrer Workstation einen geplanten Befehl, der bei der Ausführung fehlgeschlagen ist, maximal wiederholt.
- Mbobjrefreshthresh
  Die Option mbobjrefreshthresh (Aktualisierungsschwellenwert für Megablockobjekte) gibt eine Zahl an, die einen Schwellenwert definiert. Wenn die Anzahl der IBM Spectrum Protect-Objekte, die zum Beschreiben eines 128-MB-Megablocks benötigt werden, diesen Wert überschreitet, wird der gesamte Megablock aktualisiert und die Objekte, mit denen dieser Bereich in vorherigen Sicherungen dargestellt wurde, verfallen.
- Mbpctrefreshthresh
  Die Option mbpctrefreshthresh (Aktualisierungsschwellenwert für Megablockprozentsatz) gibt eine Zahl an, die einen Schwellenwert definiert. Wenn der Prozentsatz der IBM Spectrum Protect-Objekte, die zum Beschreiben eines 128-MB-Megablocks benötigt werden,

diesen Wert überschreitet, wird der gesamte Megablock aktualisiert und die Objekte, mit denen dieser Bereich in vorherigen Sicherungen dargestellt wurde, verfallen.

- Memoryefficientbackup
  Mit der Option memoryefficientbackup wird der Speichersparalgorithmus für die Verwendung bei der Verarbeitung von Gesamtsicherungen für Dateibereiche angegeben.
- Mode
  Mit der Option 'mode' können Sie den Sicherungsmodus angeben, der bei bestimmten Sicherungsoperationen verwendet werden soll.
-  AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeWindows-BetriebssystemeMonitor
  Die Option monitor gibt an, ob eine Imagesicherung oder -zurückschreibung von Dateisystemen, die zu einem NAS-Dateiserver gehören, überwacht werden soll.
-  Windows-BetriebssystemeMyprimaryserver
  Die Option myprimaryserver gibt den Namen des Primärservers an, mit dem sich der Client im Übernahmemodus beim Sekundärserver anmeldet.
- Myreplicationserver
  Die Option myreplicationserver gibt an, welche Zeilengruppe des Sekundärservers der Client im Fall einer Übernahme verwendet.
-  Windows-BetriebssystemeNamedpipename
  Die Option namedpipename gibt den Namen der benannten Pipe an, die für die Übertragung zwischen einem Client und einem Server in derselben Windows-Serverdomäne verwendet werden soll.
-  AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeWindows-BetriebssystemeNasnodename
  Die Option nasnodename gibt den Knotennamen des NAS-Dateiservers bei der Verarbeitung von NAS-Dateisystemen an. Der Client fordert Sie zur Eingabe einer Administrator-ID auf.
-  AIX-Betriebssysteme  Linux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeNfstimeout
  Die Option nfstimeout gibt die Wartezeit des Clients auf einen Statussystemaufruf für ein NFS-Dateisystem in Sekunden an, bevor eine Zeitlimitüberschreitung auftritt.
- Nodename
  Verwenden Sie die Option nodename in Ihrer Clientoptionsdatei, um Ihre Workstation beim Server zu identifizieren. Für mehrere Betriebssysteme auf der Workstation können verschiedene Knotennamen verwendet werden.
-  Windows-BetriebssystemeNojournal
  Verwenden Sie die Option nojournal im Befehl incremental, um anzugeben, dass statt der standardmäßigen journalbasierten Sicherung eine traditionelle vollständige Teilsicherung ausgeführt werden soll.
-  AIX-BetriebssystemeNojournal
  Verwenden Sie die Option nojournal im Befehl incremental, um anzugeben, dass statt der standardmäßigen journalbasierten Sicherung eine traditionelle vollständige Teilsicherung ausgeführt werden soll.
- Noprompt
  Die Option noprompt unterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group, delete archive, expire, restore image und set event angezeigt wird.
- Nrtablepath
  Die Option nrtablepath gibt die Position der Knotenreplikationstabelle auf dem Client an. Der Client für Sichern/Archivieren verwendet diese Tabelle für die Speicherung von Informationen zu jeder Sicherungs- oder Archivierungsoperation auf dem IBM Spectrum Protect-Server.
- Numberformat
  Mit der Option numberformat wird das Format angegeben, das zum Anzeigen von Zahlen verwendet werden soll.
- Optfile
  Die Option optfile gibt die Clientoptionsdatei an, die verwendet werden soll, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.
- Password
  Die Option password gibt ein Kennwort für IBM Spectrum Protect an.
- Passwordaccess
  Mit der Option passwordaccess kann angegeben werden, ob Ihr Kennwort automatisch generiert oder als Benutzereingabeaufforderung definiert werden soll.
-  AIX-Betriebssysteme  Linux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemePassworddir
  Die Option passworddir gibt die Verzeichnisposition an, in der eine verschlüsselte Kennwortdatei gespeichert werden soll.
- Pick
  Die Option pick erstellt eine Liste der Sicherungsversionen oder Archivierungskopien, die mit der von Ihnen eingegebenen Dateispezifikation übereinstimmen.
- Pitdate
  Verwenden Sie die Option pitdate mit der Option pittime, um einen Zeitpunkt zu definieren, für den die letzte Version Ihrer Sicherungen angezeigt oder zurückgeschrieben werden soll.
- Pittime
  Verwenden Sie die Option pittime mit der Option pitdate, um einen Zeitpunkt zu definieren, für den die letzte Version Ihrer Sicherungen angezeigt oder zurückgeschrieben werden soll.
-  AIX-Betriebssysteme  Linux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
   Windows-BetriebssystemePostschedulecmd/Postnschedulecmd
  Die Option postschedulecmd/postnschedulecmd gibt einen Befehl an, den das Clientprogramm verarbeitet, nachdem ein Zeitplan ausgeführt wurde.
-  AIX-Betriebssysteme  Linux-BetriebssystemeWindows-BetriebssystemePostsnapshotcmd
  Mit der Option postsnapshotcmd können Sie Shellbefehle oder Scripts des Betriebssystems ausführen, nachdem der Client für Sichern/Archivieren während einer Sicherungsoperation auf Momentaufnahmebasis eine Momentaufnahme gestartet hat.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemePreschedulecmd/Prenschedulecmd
  Mit der Option preschedulecmd wird ein Befehl angegeben, den das Clientprogramm vor der Ausführung eines Zeitplans verarbeitet.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemePreservelastaccessdate
  Mit der Option preservelastaccessdate können Sie angeben, ob eine Sicherungs- oder Archivierungsoperation die letzte Zugriffszeit ändert.
- Preservepath
  Mit der Option preservepath wird angegeben, wie viel vom Quellenpfad als Teil des Zielverzeichnispfades wiederherzustellen ist, wenn Dateien an eine neue Position zurückgeschrieben oder abgerufen werden.
- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemePresnapshotcmd
  Mit der Option presnapshotcmd können Sie Betriebssystembefehle ausführen, bevor der Client für Sichern/Archivieren eine Momentaufnahme startet.
- Queryschedperiod
  Mit der Option queryschedperiod kann die Anzahl Stunden festgelegt werden, die der Client-Scheduler zwischen den Versuchen, den Server nach geplanter Arbeit abzufragen, warten soll.
- Querysummary
  Die Option querysummary stellt Statistikdaten zu Dateien, Verzeichnissen und Objekten bereit, die von den Befehlen query backup oder query archive zurückgegeben werden.
- Quiet
  Mit der Option quiet wird die Anzahl der Nachrichten, die während der Verarbeitung auf dem Bildschirm angezeigt werden, begrenzt.
- Quotesareliteral
  Die Option quotesareliteral gibt an, ob Hochkommas (') oder Anführungszeichen (") in der eigentlichen Bedeutung interpretiert werden, wenn sie in einer Dateilistenspezifikation in einer Option filelist angegeben werden.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeRemoveoperandlimit
  Die Option removeoperandlimit gibt an, dass der Client die Beschränkung auf 20 Operanden entfernt.
- Replace
  Die Option replace gibt an, ob vorhandene Dateien auf Ihrer Workstation überschrieben werden sollen oder ob Sie zur Eingabe Ihrer Auswahl aufgefordert werden sollen, wenn Sie Dateien zurückschreiben oder abrufen.
- Replserverguid
  Die Option replserverguid gibt die global eindeutige ID (GUID) an, die verwendet wird, wenn der Client während der Übernahme eine Verbindung zum Sekundärserver herstellt. Mit der GUID wird der Sekundärserver validiert, um sicherzustellen, dass es sich um den erwarteten Server handelt.
- Replservername
  Die Option replservername gibt den Namen des Sekundärservers an, zu dem der Client während einer Übernahme eine Verbindung herstellt.
- Replsslport
  Die Option replsslport gibt den SSL-fähigen TCP/IP-Anschluss des Sekundärservers an. Die Option replsslport wird verwendet, wenn der Client während einer Übernahme eine Verbindung zum Sekundärserver herstellt. Diese Option wird nicht mehr unterstützt, wenn Sie die Verbindung zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen.
- Repltcpport
  Die Option repltcpport gibt den TCP/IP-Anschluss des Sekundärservers an, der verwendet werden soll, wenn der Client während einer Übernahme eine Verbindung zum Sekundärserver herstellt.
- Repltcpseveraddress
  Die Option repltcpseveraddress gibt die TCP/IP-Adresse des Sekundärservers an, die verwendet werden soll, wenn der Client während einer Übernahme eine Verbindung zum Sekundärserver herstellt.
- Windows-BetriebssystemeResetarchiveattribute
  Verwenden Sie die Option resetarchiveattribute, um anzugeben, ob der Client für Sichern/Archivieren das Windows-Archivierungsattribut für Dateien zurücksetzt, die erfolgreich auf dem IBM Spectrum Protect-Server gesichert wurden.
- Resourceutilization
  Mit der Option resourceutilization in Ihrer Optionsdatei können Sie den Umfang der Ressourcen steuern, die der IBM Spectrum Protect-Server und -Client während der Verarbeitung verwenden können.
- Retryperiod
  Mit der Option retryperiod wird die Wartezeit (in Minuten) des Client-Schedulers zwischen den Versuchen, einen geplanten Befehl, der fehlgeschlagen ist, auszuführen oder zwischen fehlgeschlagenen Versuchen, Ergebnisse an den Server zu melden, angegeben. Verwenden Sie diese Option nur, wenn der Scheduler aktiv ist.
- Revokeremoteaccess
  Die Option revokeremoteaccess schränkt den Zugriff eines Administrators mit Clientzugriffsberechtigung auf eine Client-Workstation, auf der der Web-Client aktiv ist, ein.
- Windows-BetriebssystemeRunasservice
  Mit der Option runasservice wird die Fortsetzung der Clientbefehlsverarbeitung erzwungen, auch wenn sich das Konto, das den Client gestartet hat, abmeldet.
- Schedcmddisabled
  Die Option schedcmddisabled gibt an, ob die Zeitplanung von Befehlen durch die Serveroption action=command im Serverbefehl define schedule inaktiviert werden soll.
- Schedcmdexception
  Die Option schedcmdexception wird in Kombination mit der Option schedcmddisabled verwendet, um die Planung von Befehlen durch die Serveroption action=command im Serverbefehl DEFINE SCHEDULE zu inaktivieren, mit Ausnahme bestimmter Befehlszeichenfolgen.
- Schedgroup
  Mit der Option schedgroup wird ein Zeitplan einer Gruppe zugeordnet.

- Schedlogmax
  Die Option schedlogmax gibt die maximale Größe des Planungsprotokolls (dsmsched.log) und des Web-Client-Protokolls (dsmwebcl.log) in Megabyte an.
- Schedlogname
  Die Option schedlogname gibt den Pfad und den Namen der Datei an, in der Planungsprotokollinformationen gespeichert werden sollen.
- Schedlogretention
  Mit der Option schedlogretention kann die Aufbewahrungsdauer in Tagen für Einträge im Planungsprotokoll (dsmsched.log) und im Web-Client-Protokoll (dsmwebcl.log) festgelegt werden und ob bereinigte Einträge in einer anderen Datei gespeichert werden sollen.
- Schedmode
  Mit der Option schedmode kann angegeben werden, ob der Modus Polling (Clientsendeaufruf: der Clientknoten fragt den Server regelmäßig nach geplanter Arbeit) oder der Modus Prompted (Servergesteuerte Ausführung: der Server stellt eine Verbindung zum Clientknoten her, wenn eine geplante Operation gestartet werden muss) verwendet werden soll.
- Schedrestretrdisabled
  Die Option schedrestretrdisabled gibt an, ob die Ausführung von Zurückschreibungs- oder Abrufplanungsoperationen inaktiviert werden soll.
- Scrolllines
  Mit der Option scrolllines wird die Anzahl Datenzeilen angegeben, die gleichzeitig auf dem Bildschirm angezeigt werden.
- Scrollprompt
  Die Option scrollprompt gibt an, ob der Client für Sichern/Archivieren nach dem Anzeigen der Anzahl Datenzeilen, die Sie in der Option scrolllines angegeben haben, stoppen und warten soll oder ob er alle Zeilen durchblättern und am Ende der Datenliste stoppen soll.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeServername
  In Ihrer Datei dsm.sys gibt die Option servername den Namen an, den Sie für die Identifikation eines Servers und am Anfang einer Zeilengruppe mit Optionen für diesen Server verwenden wollen. Es können mehrere Server benannt und Optionen für sie angegeben werden.
- Sessioninitiation
  Verwenden Sie die Option sessioninitiation, um zu steuern, ob der Server oder der Client Sitzungen durch eine Firewall einleiten soll. Standardwert ist, dass der Client Sitzungen einleitet. Sie können diese Option im Befehl schedule verwenden.
- Setwindowtitle
  Verwenden Sie die Option setwindowtitle, um den Titel des Befehlsfensters für den Verwaltungsclient während der Verarbeitung zu ändern.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeShmport
  Die Option shmport gibt die TCP/IP-Anschlussadresse eines Servers an, wenn gemeinsam genutzter Speicher verwendet wird. Alle Übertragungen mit gemeinsam genutztem Speicher starten mit einer TCP/IP-Verbindung.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeShowmembers
  Verwenden Sie die Option showmembers, um alle Member einer Gruppe anzuzeigen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeSkipacl
  Mit der Option skipacl können Sie ACL-Daten während einer Sicherungs- oder Archivierungsoperation einschließen oder ausschließen (ACL = Access Control List, Zugriffssteuerungsliste). ACL-Daten werden standardmäßig eingeschlossen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeSkipaclupdatecheck
  Die Option skipaclupdatecheck inaktiviert Kontrollsummen- und Größenvergleiche von ACL-Daten.
- Windows-BetriebssystemeSkipmissingsyswfiles
  Verwenden Sie die Option skipmissingsyswfiles, um anzugeben, ob der Client für Sichern/Archivieren bestimmte fehlende VSS Writer-Dateien überspringt und die Systemstatussicherung fortsetzt.
- Windows-BetriebssystemeSkipntpermissions
  Die Option skipntpermissions übergeht die Verarbeitung der Sicherheitsinformationen für Windows-Dateisysteme.
- Windows-BetriebssystemeSkipntsecuritycrc
  Die Option skipntsecuritycrc steuert die Berechnung der zyklischen Blockprüfung (CRC = Cyclic Redundancy Check) für einen Vergleich der Windows NTFS- oder ReFS-Sicherheitsinformationen während der folgenden Operationen: Teilsicherung, selektive Sicherung, Archivierung, Zurückschreibung oder Abruf.
- Windows-BetriebssystemeSkipsystemexclude
  Verwenden Sie die Option skipsystemexclude, um anzugeben, wie Ausschlussanweisungen für bestimmte Betriebssystemdateien, die der IBM Spectrum Protect for Virtual Environments-Client standardmäßig überspringt, verarbeitet werden sollen.
- Linux-Betriebssysteme Windows-BetriebssystemeSnapdiff
  Die Verwendung der Option snapdiff mit dem Befehl incremental optimiert den Teilsicherungsprozess. Der Befehl führt eine Teilsicherung der Dateien aus, die von NetApp als geändert zurückgemeldet wurden, und durchsucht nicht den gesamten Datenträger nach geänderten Dateien.
- Linux-Betriebssysteme Windows-BetriebssystemeSnapdiffchangelogdir
  Die Option snapdiffchangelogdir definiert die Position, an der der Client persistente Änderungsprotokolle speichert, die für Momentaufnahmedifferenzsicherungsoperationen verwendet werden.
- Linux-Betriebssysteme Windows-BetriebssystemeSnapdiffhttps
  Geben Sie die Option snapdiffhttps an, um eine sichere HTTPS-Verbindung für die Kommunikation mit einem NetApp-Dateiserver während einer Momentaufnahmedifferenzsicherung zu verwenden.
- AIX-Betriebssysteme Linux-BetriebssystemeSnapshotcachesize
  Verwenden Sie die Option snapshotcachesize, um eine angemessene Cachegröße zum Erstellen der Momentaufnahme anzugeben.
- AIX-Betriebssysteme Windows-BetriebssystemeSnapshotproviderfs
  Verwenden Sie die Option snapshotproviderfs, um Dateisicherungs- und Dateiarchivierungsoperationen auf Momentaufnahmebasis zu aktivieren und einen Momentaufnahmeprovider anzugeben.

- AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeSnapshotproviderimage
  Verwenden Sie die Option snapshotproviderimage, um Imagesicherung auf Momentaufnahmebasis zu aktivieren und einen Momentaufnahmeprovider anzugeben.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeSnapshotroot
  Verwenden Sie die Option snapshotroot im Befehl incremental, selective oder archive mit einer Anwendung eines unabhängigen Softwareanbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.
- Srvoptsetencryptiondisabled
  Die Option srvoptsetencryptiondisabled ermöglicht es dem Client, die Verschlüsselungsoptionen in einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server zu ignorieren.
- Srvprepostscheddisabled
  Die Option srvprepostscheddisabled gibt an, ob verhindert werden soll, dass die vom IBM Spectrum Protect-Administrator angegebenen Befehle vor und nach dem Zeitplan bei der Ausführung geplanter Operationen auf dem Clientsystem ausgeführt werden.
- Linux-BetriebssystemeWindows-BetriebssystemeSrvprepostsnapdisabled
  Die Option srvprepostsnapdisabled gibt an, ob verhindert werden soll, dass die vom IBM Spectrum Protect-Administrator angegebenen Befehle vor und nach der Momentaufnahme bei der Ausführung geplanter Sicherungsoperationen für Image-Momentaufnahmen ausgeführt werden.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeSsl
  Verwenden Sie die Option ssl, um Secure Sockets Layer (SSL) für eine sichere Client- und Serverkommunikation zu aktivieren. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Versionen kommuniziert, legt der Client fest, ob SSL aktiviert wird. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.2 und höher kommuniziert, wird SSL immer verwendet und mithilfe dieser Option gesteuert, ob Objektdaten verschlüsselt werden oder nicht. Aufgrund von Leistungsaspekten ist es möglicherweise sinnvoll, die Objektdaten nicht zu verschlüsseln.
- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme
  Windows-BetriebssystemeSslacceptcertfromserv
  Mithilfe der Option sslacceptcertfromserv können Sie steuern, ob der Client für Sichern/Archivieren oder die API-Anwendung das öffentliche SSL-Zertifikat des IBM Spectrum Protect-Servers akzeptiert und als vertrauenswürdig anerkennt, wenn das erste Mal eine Verbindung zwischen ihnen hergestellt wird. Diese Option gilt nur für das erste Herstellen der Verbindung zwischen dem Client für Sichern/Archivieren oder der API-Anwendung und dem IBM Spectrum Protect-Server. Wenn das öffentliche SSL-Zertifikat akzeptiert wird, werden zukünftige Änderungen an dem Zertifikat nicht automatisch akzeptiert; sie müssen manuell in den Client für Sichern/Archivieren importiert werden. Mit dieser Option können Sie die Verbindung nur zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen.
- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme
  Windows-BetriebssystemeSsldisablelegacytls
  Verwenden Sie die Option ssldisablelegacytls, um die Verwendung von SSL-Protokollen mit einer niedrigeren Stufe als TLS 1.2 nicht zuzulassen.
- Sslfipsmode
  Die Option sslfipsmode gibt an, ob der Client den FIPS-Modus (FIPS = Federal Information Processing Standards) für die SSL-Übertragung (SSL = Secure Sockets Layer) mit dem Server verwendet. Der Standardwert ist No.
- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme
  Windows-BetriebssystemeSslrequired
  Die Option sslrequired gibt die Bedingungen an, unter denen SSL erforderlich ist, wenn sich der Client beim IBM Spectrum Protect-Server oder bei den Speicheragenten anmeldet. Um SSL zu aktivieren, damit die Kommunikation zwischen Client und Server sowie Client und Speicheragent sicher ist, müssen Sie die Clientoption ssl auf yes setzen. Bei der Kommunikation mit dem IBM Spectrum Protect-Server der Version 8.1.2 und höher ist diese Option nicht mehr gültig, da SSL immer verwendet wird.
- AIX-BetriebssystemeWindows-BetriebssystemeStagingdirectory
  Die Option stagingdirectory definiert die Position, an der der Client alle Daten speichert, die er zum Ausführen seiner Operationen generiert. Die Daten werden gelöscht, wenn die Verarbeitung abgeschlossen ist.
- Subdir
  Die Option subdir gibt an, ob Unterverzeichnisse benannter Verzeichnisse bei der Verarbeitung berücksichtigt werden sollen.
- Windows-BetriebssystemeSystemstatebackupmethod
  Mit der Option systemstatebackupmethod können Sie angeben, welche Sicherungsmethode für die Sicherung des System Writer-Abschnitts der Systemstatusdaten verwendet werden soll. Die von Ihnen ausgewählte Methode wird bei der Sicherung der Systemstatusdaten verwendet.
- Tapeprompt
  Die Option tapeprompt gibt an, ob der Client für Sichern/Archivieren auf auf einen Bandladevorgang warten soll, der für eine Sicherung, Archivierung, Zurückschreibung oder einen Abruf erforderlich ist, oder ob eine Bedienerführung für die Auswahl angezeigt werden soll.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
  Windows-BetriebssystemeTcpadminport
  Verwenden Sie die Option tcpadminport, um eine separate TCP/IP-Anschlussnummer anzugeben, an der der Server Anforderungen für Verwaltungsclientsitzungen erwartet. Dies ermöglicht sichere Verwaltungssitzungen innerhalb eines privaten Netzwerks.
- Tcpbuffsize
  Die Option tcpbuffsize gibt die Größe des internen TCP/IP-Kommunikationspuffers an, der verwendet wird, um Daten zwischen dem Clientknoten und dem Server zu übertragen. Ein größerer Puffer kann die Übertragungsleistung verbessern, benötigt jedoch mehr Speicher.
- Tcpcadaddress
  Die Option tcpcadaddress gibt eine TCP/IP-Adresse für dsmcad an. Normalerweise wird diese Option nicht benötigt. Verwenden Sie diese

Option nur, wenn Ihr Clientknoten mehrere TCP/IP-Adressen hat oder wenn TCP/IP nicht die Standardübertragungsmethode ist.

- Tcpclientaddress
  Mit der Option tcpclientaddress kann eine TCP/IP-Adresse angegeben werden, wenn der Clientknoten des Benutzers über mehrere Adressen verfügt und der Server eine Verbindung zu einer anderen Adresse herstellen soll, als die, mit der die erste Verbindung zum Server hergestellt wurde.
- Tcpclientport
  Mit der Option tcpclientport wird eine TCP/IP-Anschlussnummer für den Server angegeben, mit der eine Verbindung zum Client hergestellt wird, wenn der Server die Operation mit Zeitplanung über Serversystemanfrage beginnt.
- Tcpnodelay
  Die Option tcpnodelay gibt an, ob der Client die Verzögerung beim Senden aufeinanderfolgender kleiner Pakete im Netz pro Transaktion inaktiviert.
- Tcpport
  Die Option tcpport gibt eine TCP/IP-Anschlussadresse für den IBM Spectrum Protect-Server an. Diese Adresse kann beim Administrator erfragt werden.
- Tcpserveraddress
  Die Option tcpserveraddress gibt die TCP/IP-Adresse für den IBM Spectrum Protect-Server an. Sie können diese Serveradresse beim Administrator erfragen.
- Tcpwindowsize
  Mit der Option tcpwindowsize können Sie die Größe in Kilobyte angeben, die Sie für das TCP/IP-Schiebefenster für Ihren Clientknoten verwenden wollen.
- Timeformat
  Mit der Option timeformat wird das Format angegeben, in dem die Systemzeit angezeigt oder eingegeben werden soll.
-  AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeWindows-BetriebssystemeToc
  Verwenden Sie die Option toc mit dem Befehl backup nas oder der Option include.fs.nas, um anzugeben, ob der Client für Sichern/Archivieren für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) speichern soll.
- Todate
  Mit der Option todate können Sie in Verbindung mit der Option totime ein Enddatum und eine Endzeit angeben, bis zu der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.
- Totime
  Mit der Option totime können Sie in Verbindung mit der Option todate ein Enddatum und eine Endzeit angeben, bis zu der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen. Der Client für Sichern/Archivieren ignoriert diese Option, wenn Sie die Option todate nicht angeben.
- Txnbytelimit
  Mit der Option txnbytelimit wird die Anzahl Kilobyte angegeben, die das Clientprogramm puffert, bevor eine Transaktion an den Server gesendet wird.
- Type
  Verwenden Sie die Option type im Befehl query node, um den Typ des abzufragenden Knotens anzugeben. Verwenden Sie diese Option im Befehl set event, um eine Löschsperre zu aktivieren oder freizugeben bzw. um den Aufbewahrungszeitraum zu starten.
- Updatectime
  Überprüfen Sie mithilfe der Option updatectime das Attribut für die Änderungszeit (ctime) während einer Teilsicherungsoperation.
-  Windows-BetriebssystemeUsedirectory
  Die Option usedirectory fragt im Active Directory die Übertragungsmethode und den Server ab, zu dem eine Verbindung hergestellt werden soll.
- Useexistingbase
  Die Option useexistingbase wird verwendet, wenn Sie Momentaufnahmen sichern, die sich auf NetApp-Dateiserverdatenträgern befinden. Die Option useexistingbase gibt an, dass die jüngste Momentaufnahme, die sich auf dem zu sichernden Datenträger befindet, als Basismomentaufnahme während einer Momentaufnahmedifferenzsicherung verwendet werden soll.
- Usereplicationfailover
  Die Option usereplicationfailover gibt an, ob die automatisierte Clientübernahme auf einem Clientknoten stattfindet.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeUsers (veraltet)
  Diese Option ist veraltet.
- V2archive
  Verwenden Sie die Option v2archive im Befehl archive, um anzugeben, dass nur Dateien auf dem Server archiviert werden sollen.
- Verbose
  Mit der Option verbose können Sie angeben, dass Sie detaillierte Verarbeitungsinformationen auf Ihrem Bildschirm anzeigen wollen. Dies ist der Standardwert.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-BetriebssystemeVerifyimage
  Verwenden Sie die Option verifyimage im Befehl restore image, um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll.
- Virtualfsname
  Verwenden Sie die Option virtualfsname im Befehl backup group, um den Namen des virtuellen Dateibereichs für die Gruppe anzugeben, mit dem die Operation ausgeführt werden soll. Die Angabe für virtualfsname darf nicht mit einem vorhandenen Dateibereichsnamen übereinstimmen.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeVirtualmountpoint
  Die Option virtualmountpoint definiert einen virtuellen Mountpunkt für ein Dateisystem, wenn Dateien für die Sicherung berücksichtigt werden sollen, die mit einem bestimmten Verzeichnis innerhalb dieses Dateisystems beginnen.
- Virtualnodename
  Die Option virtualnodename gibt den Knotennamen Ihrer Workstation an, wenn Sie Dateien auf einer anderen Workstation

zurückschreiben oder abrufen wollen.

- Windows-BetriebssystemeVmautostartvm
  Mit der Option vmautostartvm in Verbindung mit dem Befehl restore VM vmrestoretype=instantaccess können Sie angeben, ob die virtuelle Maschine, die während der Sofortzugriffsverarbeitung erstellt wird, automatisch eingeschaltet wird.
- Linux-BetriebssystemeWindows-BetriebssystemeVmbackdir
  Die Option vmbackdir gibt die temporäre Plattenposition an, an der der Client Steuerdateien speichert, die während VM-Gesamtsicherungs- und -Zurückschreibungsoperationen für virtuelle Maschinen erstellt werden.
- Linux-BetriebssystemeWindows-BetriebssystemeVmbackuplocation
  Verwenden Sie die Option vmbackuplocation mit dem Befehl backup vm oder restore vm, um die Sicherungsposition für Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen anzugeben.
- Linux-BetriebssystemeWindows-BetriebssystemeVmbackupmailboxhistory
  Die Option vmbackupmailboxhistory gibt an, ob die Mailbox-History automatisch mit der VM-Sicherung hochgeladen wird, wenn IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server auf einer virtuellen Maschine erkannt wird.
- Linux-BetriebssystemeWindows-BetriebssystemeVmbackuptype
  Verwenden Sie die Option vmbackuptype mit dem Befehl backup VM oder restore VM, um den Typ der Sicherung oder Zurückschreibung der virtuellen Maschine anzugeben, der ausgeführt werden soll. Sie können diese Option auch in query VM-Befehlen verwenden, um die Abfrageergebnisse zu filtern, sodass nur virtuelle Maschinen angezeigt werden, die mit einem bestimmten Sicherungstyp gesichert wurden. Beispiele finden Sie in der Beschreibung des Befehls query VM.
- Linux-BetriebssystemeWindows-BetriebssystemeVmchost
  Verwenden Sie die Option vmchost im Befehl backup VM, restore VM oder query VM, um den Hostnamen des VMware VirtualCenter- oder ESX-Servers anzugeben, der gesichert, zurückgeschrieben oder abgefragt werden soll.
- Linux-BetriebssystemeWindows-BetriebssystemeVmcpw
  Verwenden Sie die Option vmcpw im Befehl backup VM, restore VM oder query VM, um das Kennwort für die VMware VirtualCenter- oder ESX-Benutzer-ID anzugeben, die mit der Option vmcuser angegeben wird.
- Vmctlmc
  Diese Option gibt die Verwaltungsklasse an, die beim Sichern von Steuerdateien für virtuelle Maschinen verwendet werden soll.
- Linux-BetriebssystemeWindows-BetriebssystemeVmcuser
  Verwenden Sie die Option vmcuser im Befehl backup VM, restore VM oder query VM, um den Benutzernamen des VMware VirtualCenter- oder ESX-Servers anzugeben, der gesichert, zurückgeschrieben oder abgefragt werden soll.
- Linux-BetriebssystemeWindows-BetriebssystemeVmdatastorethreshold
  Verwenden Sie die Option vmdatastorethreshold, um den Prozentsatz für den Schwellenwert der Speicherbelegung für jeden VMware-Datenspeicher einer virtuellen Maschine zu definieren.
- Linux-BetriebssystemeWindows-BetriebssystemeVmdefaultdvportgroup
  Mit dieser Option können Sie die Portgruppe angeben, die NICs (Netzschnittstellenkarten) während restore vm-Operationen für eine virtuelle Maschine verwenden sollen, die bei ihrer Sicherung mit einer verteilten virtuellen Portgruppe verbunden war, ohne dass der Zielhost der Zurückschreibungsoperation eine ähnliche verteilte virtuelle Portgruppe enthält.
- Linux-BetriebssystemeWindows-BetriebssystemeVmdefaultdvswitch
  Mit dieser Option können Sie den verteilten virtuellen Switch (dvSwitch) angeben, der die Portgruppe enthält, die Sie mit der Option vmdefaultdvportgroup definieren. Die Option bleibt ohne Wirkung, wenn nicht auch die Option vmdefaultdvportgroup angegeben wird.
- Linux-BetriebssystemeWindows-BetriebssystemeVmdefaultnetwork
  Mit dieser Option können Sie ein Netz angeben, das NICs (Netzschnittstellenkarten) während einer restore vm-Operation für eine virtuelle Maschine verwenden sollen, die bei ihrer Sicherung mit einer verteilten virtuellen Portgruppe verbunden war, ohne dass für den Zielhost der Zurückschreibungsoperation verteilte Switch-Portgruppen konfiguriert sind.
- Windows-BetriebssystemeVmdiskprovision
  Mit der Option vmdiskprovision können Sie eine Bereitstellungsmaßnahme für die virtuelle Plattendatei angeben, die für die Zurückschreibung von Daten virtueller VMware-Maschinen verwendet wird. Diese Option ist nur für restore vm-Operationen mit der Angabe `vmrestoretype=instantrestore` gültig.
- Vmenabletemplatebackups
  Die Option vmenabletemplatebackups gibt an, ob der Client virtuelle VMware-Schablonenmaschinen sichert, wenn er virtuelle Maschinen auf einem vCenter-Server schützt. Virtuelle VMware-Schablonenmaschinen können nicht gesichert werden, wenn sie sich auf einem ESXi-Host befinden, weil ESXi Schablonen nicht unterstützt.
- Windows-BetriebssystemeVmexpireprotect
  Verwenden Sie diese Option, um Momentaufnahmen virtueller Maschinen zu schützen, sodass sie nicht verfallen können, während eine Sofortzurückschreibungs- oder Sofortzugriffsoperation für virtuelle VMware-Maschinen oder eine Zurückschreibung auf Dateiebene für eine virtuelle VMware-Maschine aktiv ist. Verwenden Sie diese Option, um Momentaufnahmen virtueller Maschinen zu schützen, sodass sie nicht verfallen können, während eine Sofortzurückschreibungs- oder Sofortzugriffsoperation für virtuelle Hyper-V-Maschinen oder eine Zurückschreibung auf Dateiebene für eine virtuelle Hyper-V-Maschine aktiv ist.
- Vmiscsiadapter
  Diese Option gibt an, welcher iSCSI-Adapter auf dem ESX-Host für Sofortzurückschreibungsoperationen und Sofortzugriffsoperationen für virtuelle VMware-Maschinen verwendet werden soll.
- Windows-BetriebssystemeVmiscsiserveraddress
  Verwenden Sie die Option vmiscsiserveraddress mit dem Befehl restore VM, um den Hostnamen oder die IP-Adresse des iSCSI-Servers anzugeben, der die iSCSI-Ziele für Sofortzurückschreibungs- und Sofortzugriffsoperationen bereitstellt.
- Vmlimitperdatastore
  Die Option vmlimitperdatastore gibt die Anzahl virtueller Maschinen (VMs) und virtueller Platten in einem Datenspeicher an, die während einer optimierten Sicherungsoperation parallel verarbeitet werden können.
- Vmlimitperhost
  Die Option vmlimitperhost gibt die Anzahl virtueller Maschinen (VMs) und virtueller Platten in einem Host an, die während einer

optimierten Sicherungsoperation parallel verarbeitet werden können.

- Windows-BetriebssystemeVmlist
  Die Option vmlist ist für Hyper-V-Sicherungsoperationen veraltet. Um eine oder mehrere virtuelle Hyper-V-Maschinen (VMs) in Data Protection for Microsoft Hyper-V-Sicherungsoperation einzuschließen, verwenden Sie die Option domain.vmfull oder geben Sie die VMs bei der Ausführung des Befehls backup vm an.
- Vmmaxbackupsessions
  Die Option vmmaxbackupsessions gibt die maximale Anzahl IBM Spectrum Protect-Serversitzungen zum Versetzen von VM-Daten auf den Server an, die in eine optimierte Sicherungsoperation eingeschlossen werden können.
- Vmmaxparallel
  Die Option vmmaxparallel dient zum Konfigurieren optimierter Sicherungen mehrerer virtueller Maschinen mithilfe einer einzigen Instanz des Clients für Sichern/Archivieren. Diese Option gibt die maximale Anzahl virtueller Maschinen an, die gleichzeitig auf dem IBM Spectrum Protect-Server gesichert werden können.
- Windows-BetriebssystemeVmmaxpersnapshot
  Mithilfe der Option vmmaxpersnapshot können Sie die maximale Anzahl virtueller Maschinen (VMs) angeben, die in eine Hyper-V-Momentaufnahme eingeschlossen werden sollen. Die VMs in der Momentaufnahme werden auf dem IBM Spectrum Protect-Server gesichert.
- Vmmaxrestoresessions
  Die Option vmmaxrestoresessions gibt die maximale Anzahl IBM Spectrum Protect-Serversitzungen an, die in eine optimierte Zurückschreibungsoperation für eine virtuelle Maschine (VM) eingeschlossen werden können.
- Vmmaxrestoreparalleldisks
  Die Option vmmaxrestoreparalleldisks ermöglicht einem IBM Spectrum Protect-Client die gleichzeitige Zurückschreibung mehrerer virtueller Platten.
- Windows-BetriebssystemeVmmaxsnapshotretry
  Verwenden Sie die Option vmmaxsnapshotretry, um die maximale Anzahl Wiederholungen einer Momentaufnahmeoperation für eine virtuelle Maschine (VM) anzugeben, wenn die erste Momentaufnahmeoperation mit einer wiederherstellbaren Bedingung fehlschlägt.
- Vmmaxvirtualdisks
  Die Option vmmaxvirtualdisks gibt die maximale Größe von Platten virtueller VMware-Maschinen (VMDKs) an, die in eine Sicherungsoperation eingeschlossen werden sollen.
- Linux-BetriebssystemeWindows-BetriebssystemeVmmc
  Verwenden Sie die Option vmmc, um die Sicherungen virtueller Maschinen mit einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zu speichern. Für Sicherungen virtueller VMware-Maschinen ist die Option vmmc nur gültig, wenn die Option vmbackuptype=fullvm festgelegt ist.
- Vmmountage
  Verwenden Sie die Option vmmountage mit dem Befehl restore VM "*" -vmrestoretype=mountcleanupall, um die Dauer in Stunden anzugeben, während der eine VM-Zurückschreibung auf Dateiebene aktiv sein muss, damit sie bereinigt wird.
- Linux-BetriebssystemeWindows-BetriebssystemeVmnoprdmdisks
  Diese Option ermöglicht dem Client die Zurückschreibung von Konfigurationsinformationen für die pRDM-Datenträger, die einer virtuellen VMware-Maschine zugeordnet sind, auch wenn die LUNs, die den Datenträgern zugeordnet wurden, nicht gefunden werden. Da pRDM-Datenträger in einer VM-Momentaufnahme nicht enthalten sind, können nur die Konfigurationsinformationen und nicht die Daten zurückgeschrieben werden, die sich auf den Datenträgern befanden.
- Linux-BetriebssystemeWindows-BetriebssystemeVmnovrdmdisks
  Diese Option ermöglicht dem Client die Zurückschreibung von Konfigurationsinformationen und Daten für die vRDM-Datenträger, die einer virtuellen VMware-Maschine zugeordnet sind, auch wenn die LUNs, die den Datenträgern zugeordnet wurden, nicht gefunden werden.
- Linux-BetriebssystemeWindows-BetriebssystemeVmpreferdagpassive
  Die Option vmpreferdagpassive gibt an, ob eine aktive Kopie oder eine passive Kopie einer Datenbank gesichert werden soll, die zu einer Microsoft Exchange Server-Datenbankverfügbarkeitsgruppe (DAG) gehört.
- Linux-BetriebssystemeWindows-BetriebssystemeVmprocessvmwithindependent
  Mit dieser Option können Sie steuern, ob vollständige VMware VM-Sicherungen verarbeitet werden, wenn die Maschine mit einer oder mit mehreren unabhängigen Plattendatenträgern bereitgestellt wird.
- Vmprocessvmwithphysdisks
  Mithilfe der Option vmprocessvmwithphysdisks können Sie steuern, ob Hyper-V-RCT-Sicherungen einer virtuellen Maschine (VM) verarbeitet werden, wenn für die VM eine oder mehrere physische Platten (Durchgriffsplatten) bereitgestellt werden.
- Linux-BetriebssystemeWindows-BetriebssystemeVmprocessvmwithprdm
  Mit dieser Option können Sie steuern, ob vollständige VMware VM-Sicherungen verarbeitet werden, wenn die virtuelle Maschine über mindestens einen RDM-Datenträger (RDM = raw device mapping) verfügt, der im Modus für physische Kompatibilität (pRDM) bereitgestellt wird.
- Windows-BetriebssystemeVmrestoretype
  Verwenden Sie die Option vmrestoretype mit dem Befehl query VM oder restore VM, um den Typ der auszuführenden oder abzufragenden Zurückschreibungsoperation anzugeben.
- Windows-BetriebssystemeLinux-BetriebssystemeVmskipctlcompression
  Mit der Option vmskipctlcompression können Sie bei VM-Sicherungen angeben, ob Steuerdateien (*.ctl) während einer VM-Sicherung komprimiert werden. Die Option hat keinen Einfluss auf die Komprimierung von Datendateien (*.dat).
- Vmskipmaxvirtualdisks
  Die Option vmskipmaxvirtualdisks gibt an, wie die Sicherungsoperation Platten virtueller VMware-Maschinen (VMDKs) verarbeitet, die die maximale Plattengröße überschreiten.
- Vmskipmaxvmdks
  Die Option vmskipmaxvmdks gibt an, wie die Sicherungsoperation Platten virtueller VMware-Maschinen (VMDKs) verarbeitet, die die maximale Plattengröße überschreiten.

- Vmskipphysdisks
  Mithilfe der Option vmskipphysdisks können Sie Konfigurationsinformationen für physische Platten (Durchgriffsplatten), die einer virtuellen Hyper-V-Maschine zugeordnet sind, zurückschreiben, wenn die Nummern logischer Einheiten (LUNs), die den Datenträgern auf den physischen Platten zugeordnet sind, verfügbar sind.
-  Windows-BetriebssystemeVmstoragetype
  Verwenden Sie die Option vmstoragetype mit dem Befehl restore VM, um den Typ der Speichereinheit anzugeben, von der die Momentaufnahme mit IBM Spectrum Protect Recovery Agent bereitgestellt wird.
-  Linux-Betriebssysteme  Windows-BetriebssystemeVmtagdatamover
  Verwenden Sie die Option vmtagdatamover, um Tagging-Unterstützung auf dem Client für Sichern/Archivieren (Einheit zum Versetzen von Daten) zu aktivieren. Wenn diese Option aktiviert ist, verwaltet der Client Sicherungen virtueller Maschinen in VMware-Bestandsobjekten gemäß den Datenschutztags, die über das IBM Spectrum Protect vSphere-Client-Plug-in des vSphere-Web-Clients oder mithilfe von Tools wie VMware vSphere PowerCLI Version 5.5 R2 oder höher definiert werden.
-  Linux-Betriebssysteme  Windows-BetriebssystemeVmtagdefaultdatamover
  Verwenden Sie die Option vmtagdefaultdatamover, um virtuelle Maschinen zu schützen, die in einem Zeitplan definiert sind und denen keine Kategorie und kein Tag `Data Mover` zugeordnet ist bzw. die keine derartige Kategorie und keinen derartigen Tag geerbt haben.
-  Windows-BetriebssystemeVmtempdatastore
  Verwenden Sie die Option vmtempdatastore mit dem Befehl restore VM, um einen temporären Datenspeicher auf dem ESX-Host für eine Sofortzurückschreibungsoperation zu definieren.
- Vmverifyifaction
  Mit dieser Option können Sie die Aktion angeben, die ausgeführt werden soll, wenn die Einheit zum Versetzen von Daten Integritätsprobleme mit den jüngsten CTL- und Bitmapdateien für eine virtuelle Maschine erkennt.
- Vmverifyiflatest
  Diese Option ist nur für Sicherungsoperationen von virtuellen VMware-Maschinen gültig, die im Modus der immer inkrementellen Teilsicherung ausgeführt werden (d. h. ein Befehl backup vm mit der Angabe -mode=IFIncremental). Wenn die Option vmverifyiflatest aktiviert ist, führt die Einheit zum Versetzen von Daten eine Integritätsprüfung der CTL- und Bitmapdateien durch, die während der letzten Sicherung auf dem Server erstellt wurden, falls die letzte Sicherung eine immer inkrementelle Teilsicherung war.
-  Linux-Betriebssysteme  Windows-BetriebssystemeVmvstortransport
  Die Option vmvstortransport gibt die bevorzugte Transportreihenfolge (Hierarchie) an, die beim Sichern oder Zurückschreiben von virtuellen VMware-Maschinen verwendet werden soll. Wenn Sie einen bestimmten Transport mit dieser Option nicht einschließen, wird dieser Transport ausgeschlossen und nicht für die Übertragung von Daten verwendet.
-  Windows-BetriebssystemeVssaltstagingdir
  Die Option vssaltstagingdir gibt den vollständig qualifizierten Pfad an, der den Systemausschlusscache und temporäre Daten für VSS-Momentaufnahmeoperationen enthält.
-  Windows-BetriebssystemeVssusesystemprovider
  Die Option vssusesystemprovider gibt an, ob der Windows-Systemprovider verwendet wird oder ob Windows den am besten geeigneten Provider auswählt.
-  Linux-Betriebssysteme  Windows-BetriebssystemeVmtimeout
  VMTIMEOut gibt die maximale Wartezeit in Sekunden an, bevor eine VM-Sicherungsoperation (backup vm) abgebrochen wird, wenn die Option INCLUDE.VMTSMVSS für die Bereitstellung von Anwendungsschutz verwendet wird. Um diese Option verwenden zu können, muss die IBM Spectrum Protect for Virtual Environments-Lizenz installiert sein.
- Webports
  Die Option webports ermöglicht die Verwendung des Web-Clients außerhalb einer Firewall.
- Wildcardsareliteral
  Die Option wildcardsareliteral gibt an, ob Fragezeichen (?) und Sterne (*) in der eigentlichen Bedeutung interpretiert werden, wenn sie in einer Dateilistenspezifikation in einer Option filelist angegeben werden.

Absolute

Mit der Option absolute im Befehl incremental können Sie eine Sicherung aller Dateien und Verzeichnisse erzwingen, die der Dateispezifikation oder domain entsprechen, auch wenn die Objekte sich seit der letzten Teilsicherung nicht geändert haben.

Diese Option überschreibt den Parameter mode für Sicherungskopiengruppen der Kopiengruppe in der Verwaltungsklasse. Sie hat weder Einfluss auf den Parameter frequency noch auf andere Sicherungskopiengruppenparameter. Exclude-Anweisungen werden von dieser Option nicht überschrieben. Daher können Objekte, die von der Sicherung ausgeschlossen sind, nicht für eine Sicherung ausgewählt werden, auch wenn die Option absolute angegeben ist.

Wichtig: Bevor Sie die Option absolute verwenden, lesen Sie die folgenden Informationen zu den Auswirkungen, die diese Option auf Sicherungs- und IBM Spectrum Protect-Serveroperationen haben kann:

- Sicherungen benötigen mehr Serverspeicher und Datenbankressourcen.
- Sicherungen erfordern mehr Netzbandbreite.
- Die Ausführung von Serveroperationen (z. B. Bestandsverfall, Speicherpoolsicherung, Speicherpoolumlagerung, Wiederherstellung und Knotenreplikation) nimmt mehr Zeit in Anspruch. Die Datendeduplizierung kann einige dieser Auswirkungen mindern, sie verhindert jedoch nicht die erforderliche Verarbeitung zur Wiederherstellung der deduplizierten Daten zurück in ihre ursprüngliche Form, wenn der Speicherpool in Speicher ohne Deduplizierung umgelagert oder gesichert wird.

Diese Option ist nur als Befehlszeilenparameter für den Befehl incremental gültig, wenn Sie folgende Operationen ausführen:

- Vollständige oder partielle progressive Teilsicherungen von Dateisystemen oder Plattenlaufwerken.

- Momentaufnahmedifferenzsicherungen, wenn außerdem createnewbase=yes angegeben ist.

Um eine Gesamtsicherung eines Dateisystems zu erzwingen, in dem die journalbasierte Sicherung verwendet wird, geben Sie die Optionen nojournal und absolute im Befehl incremental an.

Windows-BetriebssystemeBei einer Domänenteilsicherung, für die systemstate als Teil der Domäne angegeben ist, erzwingt die Option absolute keine Gesamtsicherung von Systemstatusobjekten. Sie müssen systemstatebackupmethod full zur Clientoptionsdatei hinzufügen, um die Erstellung einer Gesamtsicherung von Systemstatusobjekten bei einer Domänenteilsicherung zu erzwingen.

Damit die Option absolute für geplante Teilsicherungen verwendet werden kann, muss der IBM Spectrum Protect-Serveradministrator einen separaten Sicherungszeitplan erstellen, der die Option absolute im Parameter options des Zeitplans enthält.

Unterstützte Clients

Diese Option ist für alle Clients als Befehlszeilenparameter für den Befehl incremental gültig. Diese Option kann nicht einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server hinzugefügt werden.

Syntax

```
>>-ABSolute-----------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
dsmc incr -absolute "/Users/sparky/source/*.c"
```

Windows-Betriebssysteme

```
dsmc incr -absolute c:\foo\*.c
```

Windows-Betriebssysteme

Adlocation

Sie können die Option adlocation in den Befehlen query adobjects oder restore adobjects verwenden, um anzugeben, ob die Active Directory-Objekte aus dem lokalen Container für gelöschte Active Directory-Objekte oder aus einer Systemstatussicherung auf dem IBM Spectrum Protect-Server abgefragt oder zurückgeschrieben werden sollen.

Unterstützte Clients

Diese Option ist für unterstützte Windows Server-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
                .-local--.
>>-ADLOCation--+--------+---------------------------------------><
                '-server-'
```

Parameter

server
: Gibt an, dass die Active Directory-Objekte aus einer Systemstatussicherung auf dem IBM Spectrum Protect-Server abgefragt oder zurückgeschrieben werden sollen. Für alle unterstützten Windows Server-Clients gültig.

local
: Gibt an, dass die Active Directory-Objekte aus dem lokalen Container für gelöschte Active Directory-Objekte abgefragt oder zurückgeschrieben werden sollen. Dies ist der Standardwert.

Beispiel

Befehlszeile:

```
query adobjects "cn=Jim Smith" -adlocation=server
```

AIX-BetriebssystemeLinux-Betriebssysteme

Afmskipuncachedfiles

Die Option afmskipuncachedfiles gibt an, ob bei General Parallel File System (GPFS) nicht zwischengespeicherte und genutzte Dateien in Active File Management-Dateigruppen bei Sicherungs-, Archivierungs- und Umlagerungsoperationen verarbeitet werden.

GPFS Active File Management sowie die Dateistatus *nicht zwischengespeichert* und *genutzt* sind in Produktinformationen zu GPFS erläutert.

Die Ausführung von HSM auf GPFS-Dateisystemen, die Active File Management-Dateigruppen verwenden, ist in Anleitung für die Integration von IBM Spectrum Scale AFM mit IBM Spectrum Protect beschrieben.

Definieren Sie `afmskipuncachedfiles=yes`, wenn Sie Dateien aus einem Dateisystem sichern, archivieren oder umlagern, das Active File Management-Dateigruppen enthält.

Einschränkung: Wenn Active File Management im LU-Modus (LU = Local Update) ausgeführt wird, muss die Option afmskipuncachedfiles in der Cachedateigruppe auf No gesetzt werden.

Unterstützte Clients

Diese Option ist für Clients für Sichern/Archivieren gültig, die auf AIX- und Linux-Systemen ausgeführt werden.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys vor allen Serverzeilengruppen ein.

Syntax

```
                          .-NO--.
>>-AFMSKIPUNCACHEDFILES--+-----+-------------------------------><
                          '-YES-'
```

Parameter

NO
: Der Active File Management-Dateistatus wird bei Sicherungs-, Archivierungs- und Umlagerungsoperationen ignoriert. Umlagerungsoperationen für nicht zwischengespeicherte oder genutzte Dateien schlagen fehl und führen zur Fehlernachricht ANS9525E. Sicherungs- und Archivierungsoperationen für nicht zwischengespeicherte Dateien erfordern Active File Management-Abrufoperationen. Die Abrufoperationen können beträchtlichen Datenaustausch im Netz zwischen der Active File Management-Ausgangsposition und dem Cache verursachen. Dieser Parameter ist der Standardwert.

YES
: Nicht zwischengespeicherte oder genutzte Dateien in Active File Management-Dateigruppen werden bei der Sicherungs-, Archivierungs- und Umlagerungsverarbeitung übersprungen.

Archmc

Verwenden Sie die Option archmc im Befehl archive, um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Dateien und Verzeichnisse binden wollen.

Wenn Sie eine Datei archivieren, können Sie die zugeordnete Verwaltungsklasse überschreiben, indem Sie die Option archmc im Befehl archive angeben oder den Web-Client verwenden. Das Überschreiben der Verwaltungsklasse mit dem Web-Client ist äquivalent zur Verwendung der Option archmc im Befehl archive.

Wenn Sie die Option archmc nicht verwenden, bindet der Server archivierte Verzeichnisse an die Standardverwaltungsklasse. Hat die Standardverwaltungsklasse keine Archivierungskopiengruppe, bindet der Server archivierte Verzeichnisse an die Verwaltungsklasse mit dem kürzesten Aufbewahrungszeitraum.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDiese Option ist für alle UNIX- und Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

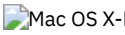
```
>>-ARCHMc = -Verwaltungsklasse--------------------------------><
```

Parameter

Verwaltungsklasse
: Gibt den Namen einer verfügbaren Verwaltungsklasse in der aktiven Maßnahmengruppe der Maßnahmendomäne an. Diese Verwaltungsklasse überschreibt die Standardverwaltungsklasse und alle include-Anweisungen für die Dateien und Verzeichnisse, die Sie archivieren.

Beispiele

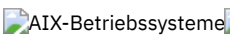
Befehlszeile:



```
dsmc archive -archmc=ret2yrs /Users/van/Documents/budget.jan
```

```
dsmc archive -archmc=ret2yrs /home/plan/proj1/budget.jan
```

```
dsmc archive -archmc=ret2yrs c:\plan\proj1\budget.jan\*
```



Archsymlinkasfile

Die Option archsymlinkasfile gibt an, ob der Client für Sichern/Archivieren einer symbolischen Verbindung folgt und die Datei oder das Verzeichnis archiviert, auf die/das die Verbindung zeigt, oder ob nur die symbolische Verbindung archiviert wird. Diese Option ist im Befehl archive zu verwenden.

Unterstützte Clients

Diese Option ist für alle UNIX-Clients mit Ausnahme von Mac OS X gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

```
                      .-Yes-.
>>-ARCHSYMLinkasfile--+-----+-----------------------------------><
                      '-No--'
```

Parameter

Yes
: Gibt an, dass der Client einer symbolischen Verbindung folgt und die zugehörige Datei oder das zugehörige Verzeichnis archiviert. Dies ist der Standardwert.

No
: Gibt an, dass der Client die symbolische Verbindung archiviert und nicht die zugehörige Datei oder das zugehörige Verzeichnis.

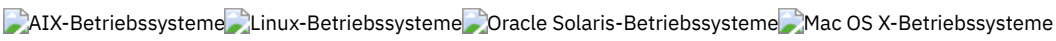
Beispiele

Optionsdatei:

archsymlinkasfile no

Befehlszeile:

-archsyml=no



Asnodename

Mit der Option asnodename können Agentenknoten Daten im Namen eines anderen Knotens (des Zielknotens) sichern oder zurückschreiben. Auf diese Weise sind gleichzeitig ablaufende Operationen von mehreren Knoten möglich, um Daten auf demselben Zielknoten und in demselben Dateibereich parallel zu speichern.

Ihrem Clientknoten muss über den Befehl grant proxynode vom Verwaltungsclient des IBM Spectrum Protect-Servers Zugriff auf den Zielknoten erteilt werden und Sie müssen ein Root sein, um die Option asnodename zu verwenden.

Wenn der IBM Spectrum Protect-Administrator einem Knoten die Proxy-Berechtigung erteilt und Sie die Option asnodename für diesen Knoten verwenden, können Sie alle Dateien abfragen und zurückschreiben, als ob Sie über Rootberechtigung verfügen würden.

Ein Agentenknoten ist ein Clientknoten, dem die Berechtigung erteilt wurde, Clientoperationen im Namen eines Zielknotens auszuführen.

Ein Zielknoten ist ein Clientknoten, der einem oder mehreren Agentenknoten die Berechtigung erteilt, in seinem Namen Clientoperationen auszuführen.

Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise maxnummp und deduplication) sowie Zeitpläne, die auf dem Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.

Beispielsweise können Sie den folgenden Befehl verwenden, um gemeinsam genutzte Daten für den Dateibereich zu sichern, der unter dem Knotennamen MyCluster gespeichert ist:

```
/cluster1/mydata
```

```
dsmc incremental /Users -asnodenodename=MyCluster
```

Sie können die Option asnodename auch verwenden, um Daten zurückzuschreiben, die unter einem anderen Knotennamen auf dem Server gespeichert sind. Sie können nur Daten zurückschreiben, deren Eigner Sie sind.

Die Option asnodename unterscheidet sich wie folgt von der Option nodename:

- Bei Verwendung der Option nodename müssen Sie das Kennwort für den von Ihnen angegebenen Knotennamen eingeben.
- Bei Verwendung der Option asnodename müssen Sie das Kennwort für Ihren Clientagentenknoten angeben, um auf die Daten zugreifen zu können, die für den Zielknoten gespeichert sind.

Einschränkungen: Sie können die Option asnodename nicht mit -fromnode verwenden und Sie können mit asnodename keine NAS-Sicherung ausführen. Außerdem kann asnodename für Clustersysteme verwendet werden, auch wenn keine spezifische Cluster-Software unterstützt wird.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys *innerhalb* einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte **Allgemein** des Profileditors definieren.

Syntax

```
>>-ASNODEname- --Zielknoten-----------------------------------><
```

Parameter

Zielknoten
: Gibt den Knotennamen auf dem IBM Spectrum Protect-Server an, unter dem Daten gesichert oder zurückgeschrieben werden sollen.

Beispiele

Optionsdatei:
: asnodename mycluster

Befehlszeile:
: -asnodename=mycluster

Diese Option ist im interaktiven Modus nicht gültig, aber sie kann im Abschnitt Optionen einer Zeitplandefinition definiert werden.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSitzungseinstellungen und Zeitpläne für eine Proxy-Operation
  Eine Proxy-Operation tritt auf, wenn ein Agentenknoten die Option `asnodename` *`Name_des_Zielknotens`* verwendet, um Operationen in Namen des angegebenen Zielknotens auszuführen.

Windows-Betriebssysteme

Asnodename

Mit der Option asnodename kann ein Agentenknoten Daten im Namen eines Zielknotens sichern, archivieren, zurückschreiben, abrufen und abfragen.

Ein *Agentenknoten* ist ein Clientknoten, dem der IBM Spectrum Protect-Administrator die Berechtigung zum Ausführen von Clientoperationen im Namen eines *Zielknotens* erteilt. Der Zielknoten ist der Clientknoten, für den der Agentenknoten die Aktionen ausführt. Der Administrator erteilt diese Berechtigung mit dem Befehl grant proxynode auf dem IBM Spectrum Protect-Server.

Agentenknoten können verwendet werden, um die Arbeitslast der Sicherung der Datenträger eines Computers über mehrere Clientsysteme zu verteilen. Jedes System, das an der Sicherung beteiligt ist, verwendet einen eigenen Agentenknotennamen. Die Sicherungsdaten werden jedoch in einem gemeinsamen Dateibereich gespeichert, dessen Eigner der Zielknoten ist.

Beispiel: Angenommen, Sie planen die Sicherung von vier Datenträgern, die zu einem Knoten mit dem Namen SCORPIO gehören, aber die Sicherungsoperation dauert zu lange. Sie können einen Teil der Arbeitslast auf drei weitere Maschinen verteilen: TAURUS, ARIES und LEO. SCORPIO und die drei anderen Maschinen sichern jeweils einen Datenträger von SCORPIO. Jeder Knoten, der an der Sicherung beteiligt ist, verwendet seinen eigenen Agentenknotennamen, um eine Verbindung zum Server herzustellen, und jeder Knoten gibt einen eindeutigen Wert für die Option asnodename an. Verwenden Sie keinen Computernamen oder Clusternamen als Wert für die Option asnodename. Die folgende Tabelle veranschaulicht eine Beispielkonfiguration.

Tabelle 1. Definition des Werts für die Option asnodename, um Sicherungen zu verteilen.

Hostname	Wert der Option NODENAME	Wert der Option ASNODENAME	Gesicherter Datenträger	Name des Serverdateibereichs
SCORPIO	SCORPIO	TARGET_SCORPIO	\\scorpio\r$	\\target_scorpio\r$
TAURUS	TAURUS	TARGET_SCORPIO	\\scorpio\s$	\\target_scoprio\s$
ARIES	ARIES	TARGET_SCORPIO	\\scorpio\t$	\\target_scorpio\t$
LEO	LEO	TARGET_SCORPIO	\\scorpio\u$	\\target_scorpio\u$

Zum Erstellen der Beziehungen zwischen dem Zielknoten und den Proxy-Knoten muss der IBM Spectrum Protect-Serveradministrator die folgenden Aktionen ausführen:

1. Die Knoten SCORPIO, TAURUS, ARIES, LEO und TARGET_SCORPIO registrieren.
2. Den Knoten SCORPIO, TAURUS, ARIES und LEO die Proxy-Berechtigung für den Knoten TARGET_SCORPIO erteilen.

Wenn Sie Daten ohne die Option asnodename sichern oder archivieren, werden die gesicherten Daten in einem Dateibereich auf dem Server gespeichert, der dem UNC-Namen des Laufwerks entspricht, auf dem sich die ursprünglichen Daten befinden.

Wenn Sie die Option asnodename zum Sichern von Daten im Namen eines Zielknotens verwenden, werden die Daten in einem Dateibereich gespeichert, dessen Eigner der Zielknoten ist. Im Dateibereichsnamen wird jedoch nicht der Hostname, sondern der Name des Zielknotens verwendet. Wenn TAURUS beispielsweise die Daten auf dem Laufwerk S von SCORPIO sichert und der Wert der Option asnodename auf `–asnodename=target_scorpio` gesetzt ist, werden die Sicherungsdaten in einem Dateibereich mit dem Namen \\target_scorpio\s$ gespeichert. Der Eigner des Dateibereichs ist der Knoten TARGET_SCORPIO.

Das Standardverhalten beim Zurückschreiben oder Abrufen von Daten ist das Zurückschreiben oder Abrufen der Daten an eine Position, die dem Dateibereichsnamen entspricht.

Wenn in dem vorangehenden Beispiel der Knoten SCORPIO die Option `–asnodename=target_scorpio` verwendet, um Daten aus \\target_scorpio\s$ zurückzuschreiben, versucht der Client, die Daten in das Laufwerk S eines Computers mit dem Namen TARGET_SCORPIO zurückzuschreiben. Diese Operation führt nicht zu dem erwarteten Ergebnis, da in der Beispielkonfiguration kein Computer mit dem Namen TARGET_SCORPIO vorhanden ist.

Im folgenden Beispiel wird der Befehl restore auf dem Knoten SCORPIO eingegeben. Der Befehl schreibt alle Dateien und Unterverzeichnisse aus dem Verzeichnis Users\andy\education im Dateibereich \\target_scorpio\s$ auf das Laufwerk S des Computers mit dem Namen SCORPIO zurück:

```
dsmc restore \\target_scorpio\s$\users\andy\education\* s:\
  -subdir=yes -asnodename=target_scorpio
```

Die folgenden Hinweise gelten, wenn Sie einen Proxy-Knoten verwenden, um Daten auf anderen Knoten zu sichern oder zurückzuschreiben:

- Eine Proxy-Operation verwendet die Einstellungen für den Zielknoten (beispielsweise maxnummp und deduplication) sowie Zeitpläne, die auf dem IBM Spectrum Protect-Server definiert sind. Die Einstellungen und Zeitpläne für den Agentenknoten auf dem IBM Spectrum Protect-Server werden ignoriert.
- Sie können asnodename nicht mit dem Befehl backup nas verwenden.
- Sie können asnodename nicht mit der Option fromnode verwenden.
- Wenn Sie asnodename zum Sichern und Zurückschreiben von Datenträgern in Clusterkonfigurationen verwenden, darf clusternode yes nicht verwendet werden.
- Sie können asnodename nicht zum Sichern oder Zurückschreiben des Systemstatus verwenden.
- Wenn ein Agentenknoten Daten aus einem Sicherungssatz zurückschreibt, wird das Systemstatusobjekt in dem Sicherungssatz nicht zurückgeschrieben.

- Sie können asnodename mit dem Befehl backup image verwenden; Sie müssen den Datenträger jedoch mit dem UNC-Namen angeben. Sie können nicht den Laufwerkbuchstaben verwenden.
- Wenn Sie denselben asnodename-Wert verwenden, um Dateien von verschiedenen Maschinen zu sichern, müssen Sie den Überblick darüber behalten, welche Dateien oder Datenträger von jedem System gesichert werden, damit Sie sie an die korrekte Position zurückschreiben können.
- In einer Umgebung mit mehreren Knoten sollten alle Agentenknoten denselben Plattformtyp aufweisen.
- Verwenden Sie Zielknoten nicht als traditionelle Knoten, insbesondere wenn Sie die Dateien verschlüsseln, bevor Sie sie auf dem Server sichern.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.opt ein. Sie können diese Option auf der Registerkarte Allgemein des Profileditors definieren.

Syntax

```
>>-ASNODEname- --Zielknoten-----------------------------------><
```

Parameter

Zielknoten
: Gibt den Knotennamen auf dem IBM Spectrum Protect-Server an, unter dem Daten gesichert oder zurückgeschrieben werden sollen.

Beispiele

Optionsdatei:
```
asnodename target_scorpio
```
Befehlszeile:
: Dieser Befehl sichert das gesamte Laufwerk F: im Serverdateibereich mit dem Namen \\target_scorpio\f$.

```
dsmc incremental f: -asnodename=target_scorpio
```

Diese Option ist im interaktiven Modus nicht gültig, aber sie kann im Abschnitt Optionen einer Zeitplandefinition definiert werden.

- Windows-BetriebssystemeSitzungseinstellungen und Zeitpläne für eine Proxy-Operation
  Eine Proxy-Operation tritt auf, wenn ein Agentenknoten die Option `asnodename Name_des_Zielknotens` verwendet, um Operationen in Namen des angegebenen Zielknotens auszuführen.

Windows-Betriebssysteme

Asrmode

Verwenden Sie die Option asrmode mit den Befehlen restore und restore systemstate, um anzugeben, ob eine Zurückschreibungsoperation im ASR-Systemwiederherstellungsmodus ausgeführt wird.

Diese Option wird nur im Kontext von restore-Befehlen verwendet, die in der Datei asr.sif vom Befehl backup asr generiert werden.

Unterstützte Clients

Diese Option ist für unterstützte Windows-Clients gültig, die in einer Windows-Vorinstallationsumgebung (WinPE) ausgeführt werden. Sowohl BIOS- als auch UEFI-Bootarchitekturen werden unterstützt.

Syntax

```
>>-ASRMODE = -+-----+-------------------------------------------><
              +-No--+
              '-Yes-'
```

Parameter

No
: Gibt an, dass der Client die Zurückschreibungsoperation nicht im ASR-Systemwiederherstellungsmodus ausführt.

Yes

Gibt an, dass der Client die Zurückschreibungsoperation im ASR-Wiederherstellungsmodus ausführt. Dies ist der Standardwert für Windows-Clients während der ASR-Wiederherstellung. Diese Clients werden während der ASR-Wiederherstellung in Windows-Vorinstallationsumgebung (WinPE) ausgeführt.

Beispiele

Befehlszeile:

```
restore systemstate -asrmode=yes
restore systemstate -asrmode=yes -inactive -pick
```

Diese Option ist für eine interaktive Sitzung gültig, kann aber nicht geändert werden, indem die Option eingegeben wird, während die interaktive Sitzung aktiv ist.

Auditlogging

Verwenden Sie die Option auditlogging, um ein Prüfprotokoll zu generieren, das für jede Datei, die während einer Teilsicherungsoperation, einer selektiven Sicherungsoperation, einer Archivierungs-, Zurückschreibungs- oder Abrufoperation verarbeitet wird, einen Eintrag enthält.

Das Prüfprotokoll kann so konfiguriert werden, dass es entweder eine Basisversion oder eine inklusivere (vollständige) Version an Informationen erfasst.

Die Basisversion der Prüfprotokollierungsfunktion erfasst die Informationen, die sich im Planungsprotokoll befinden und zeichnet die Informationen auf, dass eine Datei während einer Teilsicherungsoperation, einer selektiven Sicherungsoperation, einer Archivierungs-, Zurückschreibungs- oder Abrufoperation gesichert, archiviert, aktualisiert, zurückgeschrieben, abgerufen, gelöscht und übersprungen wurde oder abgelaufen oder fehlgeschlagen ist. Darüber hinaus erfasst die Basisversion der Prüfprotokollierung den Eingabebefehl für die durch den Befehlszeilenclient für Sichern/Archivieren oder den Scheduler-Client ausgeführten Befehle.

Die vollständige Version der Prüfprotokollierung zeichnet für jede Datei, die vom Client für Sichern/Archivieren verarbeitet wird, eine Aktion auf. Zusätzlich zu all den Ereignissen, die von der Basisversion der Prüfprotokollierung aufgezeichnet wird, zeichnet die vollständige Version der Prüfprotokollierung Informationen über eine Datei auf, die ausgeschlossen wurde oder während einer fortlaufenden Teilsicherungsoperation nicht gesendet wurde, weil sich die Datei nicht geändert hat.

Nachfolgend wird ein Beispiel der Nachrichten aufgezeigt, die ausgegeben werden, wenn das Prüfprotokoll so konfiguriert wird, dass es die Basisversion der Informationen erfasst:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

```
21.04.07 15:25:05 ANS1650I Befehl:
  sel /home/spike/test/*
21.04.07 15:25:05 ANS1651I Gesichert:
  /home/spike/test/file.txt
21.04.07 15:25:05 ANS1652I Archiviert:
  /home/spike/test/file.txt
21.04.07 15:25:05 ANS1653I Aktualisiert:
  /home/spike/test/file.txt
21.04.07 15:25:05 ANS1654E Fehlgeschlagen:
  /home/spike/test/file.txt
21.04.07 15:25:05 ANS1655I Zurückgeschrieben:
  /home/spike/test/file.txt
21.04.07 15:25:05 ANS1656I Abgerufen:
  /home/spike/test/file.txt
21.04.07 15:25:05 ANS1657I Abgelaufen:
  /home/spike/test/file.txt
21.04.07 15:25:05 ANS1658I Gelöscht:
  /home/spike/test/file.txt
21.04.07 15:25:05 ANS1659I Übersprungen:
  /home/spike/test/file.txt
```

 Windows-Betriebssysteme

```
21.04.07 15:25:05 ANS1650I Befehl:
  sel c:\test\file.txt
21.04.07 15:25:05 ANS1651I Gesichert:
  \\spike\c$\test\file.txt
21.04.07 15:25:05 ANS1652I Archiviert:
  \\spike\c$\test\file.txt
21.04.07 15:25:05 ANS1653I Aktualisiert:
  \\spike\c$\test\file.txt
21.04.07 15:25:05 ANS1654E Fehlgeschlagen:
  \\spike\c$\test\file.txt
21.04.07 15:25:05 ANS1655I Zurückgeschrieben:
  \\spike\c$\test\file.txt
21.04.07 15:25:05 ANS1656I Abgerufen:
  \\spike\c$\test\file.txt
21.04.07 15:25:05 ANS1657I Abgelaufen:
  \\spike\c$\test\file.txt
```

```
21.04.07 15:25:05 ANS1658I Gelöscht:
  \\spike\c$\test\file.txt
21.04.07 15:25:05 ANS1659I Übersprungen:
  \\spike\c$\test\file.txt
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie folgenden Nachrichten können ausgegeben werden, wenn das Prüfprotokoll so konfiguriert wird, dass es die vollständige Version der Informationen erfasst (zusätzlich zu all den Nachrichten, die für die Basisversion der Prüfprotokollierung ausgegeben werden):

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
21.04.07 15:25:05 ANS1660I Ausgeschlossen:
  /home/spike/test/file.txt
21.04.07 15:25:05 ANS1661I Unverändert:
  /home/spike/test/file.txt
```

Windows-BetriebssystemeNachfolgend wird ein Beispiel der Nachrichten gezeigt, die ausgegeben werden, wenn das Prüfprotokoll so konfiguriert wird, dass es die vollständige Version der Informationen erfasst (zusätzlich zu all den Nachrichten, die für die Basisversion der Prüfprotokollierung ausgegeben werden):

Windows-Betriebssysteme

```
21.04.07 15:25:05 ANS1660I Ausgeschlossen:
  \\spike\c$\test\file.txt
21.04.07 15:25:05 ANS1661I Unverändert:
  \\spike\c$\test\file.txt
```

Das Prüfprotokoll ist kein Ersatz oder Vertreter für das Standardfehlerprotokoll (`dsmerror.log`) oder für das Planungsprotokoll (`dsmsched.log`). Tritt ein Fehler auf, der die Verarbeitung einer Datei verhindert, wird eine Nachricht in das Prüfprotokoll geschrieben, die besagt, dass ein Fehler aufgetreten ist. Die Nachricht gibt jedoch nicht die Art des Fehlers an. Zur Fehlerdiagnose muss trotzdem noch das Standardfehlerprotokoll verwendet werden.

Die Prüfprotokolleinträge enthalten nur eine Zeitmarke und den Objektnamen. Es gibt keine Angaben, um zwischen Dateien und Verzeichnissen unterscheiden zu können, oder Informationen über die Größe eines Objekts.

Mac OS X-BetriebssystemeDer Client für Sichern/Archivieren unter Mac OS X erstellt das Prüfprotokoll als Unicode-Datei (UTF-16).

Windows-BetriebssystemeBei Verwendung des Windows-Clients für Sichern/Archivieren werden alle Objektnamen im UNC-Format geschrieben. Der Windows-Client für Sichern/Archivieren erstellt das Prüfprotokoll als Unicode-Datei.

Standardmäßig lautet der Name des Prüfprotokolls `dsmaudit.log`; es ist in demselben Verzeichnis enthalten wie das Fehlerprotokoll `dsmerror.log`. Der Name und die Position des Prüfprotokolls können mithilfe der Option auditlogname konfiguriert werden. Es gibt keine Parameter, um die Größe des Prüfprotokolls zu steuern oder das Prüfprotokoll zu bereinigen. Die Option auditlogname kann nicht als Option in einer Clientoptionsgruppe des IBM Spectrum Protect-Servers definiert werden.

Mac OS X-BetriebssystemeDer Befehl auditlogging wird mit Sicherungsbefehlen unterstützt, die mit Objekten auf Dateiebene interagieren, z. B. backup groups.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDer Befehl auditlogging wird nicht mit Sicherungsbefehlen unterstützt, die mit Objekten auf Imageebene interagieren, z. B. backup image oder restore image. Der Befehl auditlogging wird mit Sicherungsbefehlen unterstützt, die mit Objekten auf Dateiebene interagieren, z. B. backup groups.

Windows-BetriebssystemeDer Befehl auditlogging wird nicht mit Sicherungsbefehlen unterstützt, die mit Objekten auf Imageebene interagieren, z. B. backup image oder restore image. Der Befehl auditlogging wird mit Sicherungsbefehlen unterstützt, die mit Objekten auf Dateiebene interagieren, z. B. backup groups und backup systemstate.

Haben Sie die Prüfprotokollierung für eine Operation aktiviert und ist das Schreiben in das Prüfprotokoll nicht möglich (wenn beispielsweise die Platte voll ist, auf der das Prüfprotokoll gespeichert ist), wird die Prüfprotokollierung für den Rest der Operation inaktiviert und der Rückkehrcode für die Operation wird unabhängig vom Ergebnis der Operation auf 12 gesetzt.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Datei dsm.opt ein.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

```
                .-off---.
```

```
>>-AUDITLOGGing--+-------+-------------------------------------><
                +-basic-+
                '-full--'
```

Parameter

off
: Gibt an, dass die Prüfprotokollierungseinrichtung nicht aktiviert ist. Dies ist der Standardwert.

basic
: Gibt an, dass das Prüfprotokoll eine Basisebene an Informationen erfasst.

full
: Gibt an, dass das Prüfprotokoll eine umfassendere Ebene an Informationen erfasst.

Beispiele

Eine Teilsicherung mit aktivierter Prüfprotokollierung ausführen.

Befehlszeile:

```
dsmc i -auditlogging=basic
```

Eine Liste von Dateien mit der umfassendsten Protokollierungsstufe sichern, sodass eine separate Anwendung wie ein Perl-Script die Ergebnisse überprüfen kann.

 Windows-Betriebssysteme

```
dsmc i -filelist=file.lst -auditlogging=full
  -auditlogname="c:\Programme\tivoli\tsm\baclient\
  temp_audit001.log"
```

Auditlogname

Die Option auditlogname gibt den Pfad und den Namen der Datei an, in der Prüfprotokollinformationen gespeichert werden sollen. Diese Option wird angewendet, wenn die Prüfprotokollierung aktiviert ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 Windows-BetriebssystemeFügen Sie diese Option in die Datei dsm.opt ein.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

```
>>-AUDITLOGName--Dateispezifikation----------------------------><
```

Parameter

Dateispezifikation
: Gibt den Pfad und den Namen der Datei an, in der der Client für Sichern/Archivieren Prüfprotokolldaten speichern soll.

  Wird nur ein Dateiname angegeben, wird die Datei im aktuellen Verzeichnis gespeichert. Standardwert ist das Installationsverzeichnis mit dem Dateinamen dsmaudit.log. Die Datei dsmaudit.log kann keine symbolische Verbindung sein.

   Windows-BetriebssystemeIm UNC-Format (Universal Naming Convention) muss der Pfad einen Laufwerkbuchstaben enthalten. Im folgenden Beispiel enthält der Pfad den Laufwerkbuchstaben D$: \\computer7\D$\logs\tsmaudit.log.

Beispiele

Eine Teilsicherung mit aktivierter Prüfprotokollierung ausführen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeBeispielsausgabe
:  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeNachfolgend wird ein Beispiel für eine Ausführung und Ausgabedatei aufgeführt:

```
> dsmc inc /SMSVT/mfs1 -auditlogging=full
  -auditlogname=/home/cliv3/audit.log
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
  Clientversion 8, Release 1, Stufe 0.0
  Clientdatum/-zeit: 16.11.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016.
    Alle Rechte vorbehalten.

Knotenname: NAXOS_CLUSTER
Sitzung hergestellt mit Server
  ODINHSMSERV: AIX-RS/6000
  Serverversion 8, Release 1, Stufe 0.0
  Serverdatum/-zeit: 16.11.2016 12:05:35
  Letzter Zugriff: 15.11.2016   12:01:57

Teilsicherung von Datenträger '/SMSVT/mfs1'
Verzeichnis-->               4.096 /SMSVT
  /mfs1/ [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test0 [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test1 [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test2 [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test3 [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test4 [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test5 [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test6 [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test7 [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test8 [Gesendet]
Normale Datei-->            32.768 /SMSVT
  /mfs1/test9 [Gesendet]
Erfolgreiche Teilsicherung von '/SMSVT/mfs1'

Gesamtzahl geprüfter Objekte:                   11
Gesamtzahl gesicherter Objekte:                 11
Gesamtzahl aktualisierter Objekte:               0
Gesamtzahl erneut gebundener Objekte:            0
Gesamtzahl gelöschter Objekte:                   0
Gesamtzahl verfallener Objekte:                  0
Gesamtzahl fehlgeschlagener Objekte:             0
Gesamtzahl übertragener Byte:                320,31 KB
Datenübertragungszeit:                         0,01 Sek.
Datenübertragungsgeschwindigkeit im Netz:  17.141,84 KB/Sek.
Datenübertragungsgeschwindigkeit Gesamt:      297,43 KB/Sek.
Objekte komprimiert um:                          0%
Verarbeitungszeit:                        00:00:01
```

Nachfolgend wird der Inhalt des Prüfprotokolls aufgeführt:

```
03.07.07   12:05:14 ANS1650I Befehl:
  inc /SMSVT/mfs1
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test0
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test1
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test2
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test3
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test4
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test5
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test6
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test7
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test8
03.07.07   12:05:15 ANS1651I Gesichert:
  /SMSVT/mfs1/test9
```

Windows-BetriebssystemeOptionsdatei:

Windows-BetriebssystemeDas Prüfprotokoll in einem anderen Pfad als dem Standardpfad speichern.

```
auditlogname c:\mypath\myaudit.log
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeEine Liste von Dateien mit der umfassendsten Protokollierungsstufe sichern, sodass eine separate Anwendung wie ein Perl-Script die Ergebnisse überprüfen kann:

```
dsmc i -filelist=file.lst -auditlogging=full
  -auditlogname="c:\Programme\tivoli\tsm\baclient\
  temp_audit001.log"
```

Windows-BetriebssystemeBeispielsausgabe

Windows-BetriebssystemeNachfolgend wird ein Beispiel für eine Ausführung und Ausgabedatei aufgeführt:

```
C:\Programme\Tivoli\TSM\baclient>dsmc i
   c:\test\* -sub=yes -auditlogging=full
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
  Clientversion 8, Release 1, Stufe 0.0
  Clientdatum/-zeit: 16.11.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016.
    Alle Rechte vorbehalten.

Knotenname: PATMOS
Sitzung hergestellt mit Server PATMOS_5331: Windows
  Serverversion 8, Release 1, Stufe 0.0
  Serverdatum/-zeit: 16.11.2016 12:05:35
  Letzter Zugriff: 15.11.2016 15:52:06

Teilsicherung von Datenträger 'c:\test\*'
Normale Datei-->         1.048.576 \\patmos\c$\test
  \dir1\file1 [Gesendet]
Normale Datei-->         1.048.576 \\patmos\c$\test
  \dir1\file2 [Gesendet]
Normale Datei-->             1.024 \\patmos\c$\test
  \dir1\file3 [Gesendet]
Normale Datei-->         1.048.576 \\patmos\c$\test
  \dir2\file1 [Gesendet]
Normale Datei-->         1.048.576 \\patmos\c$\test
  \dir2\file2 [Gesendet]
Normale Datei-->             1.024 \\patmos\c$\test
  \dir2\file3 [Gesendet]
Erfolgreiche Teilsicherung von '\\patmos\c$\test\*'

Gesamtzahl geprüfter Objekte:                  12
Gesamtzahl gesicherter Objekte:                 6
Gesamtzahl aktualisierter Objekte:              0
Gesamtzahl erneut gebundener Objekte:           0
Gesamtzahl gelöschter Objekte:                  0
Gesamtzahl verfallener Objekte:                 0
Gesamtzahl fehlgeschlagener Objekte:            0
Gesamtzahl übertragener Byte:              400,85 KB
Datenübertragungszeit:                       0,00 Sek.
Datenübertragungsgeschwindigkeit im Netz:    0,00 KB/Sek.
Datenübertragungsgeschwindigkeit Gesamt:   382,85 KB/Sek.
Objekte komprimiert um:                        91%
Verarbeitungszeit:                      00:00:01
ANS1900I Rückkehrcode ist 0.
ANS1901I Höchster Rückkehrcode war 0.
```

Nachfolgend wird der Inhalt des Prüfprotokolls aufgeführt:

```
21.04.2007 15:52:25 ANS1650I Befehl:
  i c:\test\*
21.04.07 15:52:26 ANS1661I Unverändert:
  \\patmos\c$\test
21.04.07 15:52:26 ANS1661I Unverändert:
  \\patmos\c$\test\dir1
21.04.07 15:52:26 ANS1661I Unverändert:
  \\patmos\c$\test\dir2
21.04.07 15:52:26 ANS1661I Unverändert:
  \\patmos\c$\test\file1
21.04.07 15:52:26 ANS1661I Unverändert:
  \\patmos\c$\test\file2
21.04.07 15:52:26 ANS1661I Unverändert:
  \\patmos\c$\test\file3
21.04.07 15:52:26 ANS1651I Gesichert:
  \\patmos\c$\test\dir1\file1
21.04.07 15:52:26 ANS1651I Gesichert:
```

```
  \\patmos\c$\test\dir1\file2
21.04.07 15:52:26 ANS1651I Gesichert:
  \\patmos\c$\test\dir1\file3
21.04.07 15:52:26 ANS1651I Gesichert:
  \\patmos\c$\test\dir2\file1
21.04.07 15:52:26 ANS1651I Gesichert:
  \\patmos\c$\test\dir2\file2
21.04.07 15:52:26 ANS1651I Gesichert:
  \\patmos\c$\test\dir2\file3
```

Autodeploy

Verwenden Sie die Option autodeploy, um eine automatische Implementierung des Clients zu aktivieren oder zu inaktivieren, wenn ein Neustart erforderlich ist.

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist für AIX-, Linux-, Mac- und Solaris-Clients gültig.

 Windows-BetriebssystemeDiese Option ist für Windows-Clients gültig.

Optionsdatei

Sie können diese Option definieren, indem Sie sie in Ihre Clientoptionsdatei einfügen. Sie können sie auch über die Java-GUI definieren. Klicken Sie hierfür auf Editieren > Clientvorgaben und wählen Sie die entsprechende Option auf der Registerkarte Allgemein aus.

 Windows-Betriebssysteme

Syntax

```
                .-Yes------.
>>-AUTODEPLOY--+----------+-------------------------------------><
                +-No-------+
                '-NOReboot-'
```

 Windows-Betriebssysteme

Parameter

Yes
: Gibt an, dass der Client vom Server automatisch implementiert wird. Yes ist der Standardwert.
Wichtig:

- Wenn Sie autodeploy auf yes setzen, können Sie den Neustart nicht inaktivieren, wenn für die Beendigung der Implementierung ein Neustart der Client-Workstation erforderlich ist. Die Client-Workstation wird erneut gestartet. Wenn es wichtig ist, dass die Workstation nicht automatisch erneut gestartet wird, müssen Sie autodeploy auf noreboot setzen. Dann wird die Implementierung abgebrochen, falls ein Neustart erforderlich ist. Der aktuelle Client ist nicht betroffen.
- Ist ein Neustart erforderlich, initialisiert der Deployment Manager einen Neustart für den Client. Anschließend wird der Deployment Manager beendet. Möglicherweise wird der Neustart jedoch vom Benutzer abgebrochen oder unterbrochen. Da der Deployment Manager bereits beendet ist, wird keine Nachricht bezüglich des fehlgeschlagenen Neustarts an den Server gesendet. Das Implementierungsergebnis lautet dennoch 'erfolgreich'. Sie müssen den Computer erneut starten, sodass die neue Clientimplementierung abgeschlossen wird.

No
: Gibt an, dass der Client vom Server nicht automatisch implementiert wird.

NOReboot
: Gibt an, dass der Deployment Manager den Client-Computer niemals automatisch erneut startet, selbst dann nicht, wenn ein Neustart erforderlich ist. Wenn ein Neustart erforderlich ist, kann eine automatische Implementierung auf vielen Maschinen mit dem Parameter NOReboot dazu führen, dass möglicherweise zahlreiche Clients nur teilweise aktualisiert werden.

  Um dieses Problem abzumildern, versucht der Deployment Manager festzustellen, ob ein Neustart erforderlich ist. Ist ein Neustart erforderlich, bricht der Deployment Manager die Implementierung vor der Installation des neuen Clients ab. Auf diese Weise ist sichergestellt, dass der Client-Computer noch über einen funktionierenden Client für Sichern/Archivieren verfügt und dass die Implementierung des neuen Clients erneut geplant werden kann.

  In seltenen Fällen kann der Deployment Manager den Neustart nicht feststellen. Dies ist beispielsweise der Fall, wenn Clientprozesse von einem Script gestartet werden. In diesen Fällen wird die Installation des neuen Clients fortgesetzt; jedoch ist ein manueller Neustart des Client-Computers erforderlich.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

Syntax

```
                .-Yes-.
>>-AUTODEPLOY--+-----+-----------------------------------------><
                '-No--'
```

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

Parameter

Yes
: Gibt an, dass der Client vom Server automatisch implementiert wird. Yes ist der Standardwert.

No
: Gibt an, dass der Client vom Server nicht automatisch implementiert wird.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Optionsdatei:

```
autodeploy no
```

Befehlszeile:

Nicht zutreffend.

Windows-Betriebssysteme

Optionsdatei:

```
autodeploy noreboot
```

Befehlszeile:

Nicht zutreffend.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Wichtig: Verwenden Sie schedmode prompted mit der Option autodeploy, um die sofortige Verarbeitung des Clientimplementierungszeitplans durch den Scheduler zu aktivieren.
Zugehörige Konzepte:
Automatische Implementierung des Clients für Sichern/Archivieren

Autofsrename

Mit der Option autofsrename wird ein vorhandener, nicht Unicode-fähiger Dateibereich auf dem IBM Spectrum Protect-Server umbenannt, sodass für die aktuelle Operation ein Unicode-fähiger Dateibereich mit dem ursprünglichen Namen erstellt werden kann.

Mac OS X-BetriebssystemeWenn Sie autofsrename yes in Ihrer Clientoptionsdatei angeben und der Serverwert für autofsrename auf client gesetzt ist, generiert der IBM Spectrum Protect-Server einen eindeutigen Namen durch Anhängen von `_OLD` an den Dateibereichsnamen, den Sie in der aktuellen Operation angeben. Beispielsweise benennt der Server den Dateibereich `Jaguar` in `Jaguar_OLD` um. Ist der neue Dateibereichsname zu lang, ersetzt das Suffix die letzten Zeichen des Dateibereichsnamens. Beispielsweise wird der Dateibereichsname `mylongfilesystemname` wie folgt umbenannt:

```
mylongfilesystem_OLD
```

Mac OS X-BetriebssystemeIst der neue Dateibereich bereits auf dem Server vorhanden, benennt der Server den neuen Dateibereich in `Jaguar_OLDx` um, wobei `x` eine eindeutige Zahl ist.

Mac OS X-BetriebssystemeDer Server erstellt neue Unicode-fähige Dateibereiche, die nur die in der aktuellen Operation angegebenen Daten enthalten. Beispiel: Angenommen, `Jaguar` ist der Name Ihrer Startplatte und Sie archivieren alle `.log`-Dateien im Verzeichnis `/Users/user5/Documents`. Bevor die Archivierung stattfindet, benennt der Server den Dateibereich in `Jaguar_OLD` um. Bei der Archivierung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen `Jaguar` gestellt. Der neue Unicode-fähige Dateibereich enthält nun nur das Verzeichnis `/Users/user5/logs` und die Dateien `*.log`, die in der Operation angegeben wurden. Der Server speichert alle Daten aus nachfolgenden vollständigen und partiellen Teilsicherungen, selektiven Sicherungen und Archivierungen in den neuen Unicode-fähigen Dateibereichen.

Mac OS X-BetriebssystemeBeispiel: Angenommen, `Jaguar` ist der Name Ihrer Startplatte und Sie archivieren alle `.log`-Dateien im Verzeichnis `/Users/user5/Documents`. Bevor die Archivierung stattfindet, benennt der Server den Dateibereich in `Jaguar_OLD` um. Bei der Archivierung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen `Jaguar` gestellt. Der neue Unicode-fähige Dateibereich enthält nun nur das Verzeichnis `/Users/user5/logs` und die Dateien `*.log`, die in der Operation angegeben

wurden. Alle Daten aus nachfolgenden vollständigen und partiellen Teilsicherungen, selektiven Sicherungen und Archivierungen werden in den neuen Unicode-fähigen Dateibereichen gespeichert.

Wenn Sie `autofsrename yes` in Ihrer Clientoptionsdatei angeben und der Serverwert für autofsrename auf `client` gesetzt ist, generiert der IBM Spectrum Protect-Server einen eindeutigen Namen durch Anhängen von `_OLD` an den Dateibereichsnamen, den Sie in der aktuellen Operation angeben. Beispielsweise benennt der Server den Dateibereich `\\Ihr-Knotenname\h$` in `\\Ihr-Knotenname\h$_OLD` um. Ist der neue Dateibereichsname zu lang, werden die letzten Zeichen des Dateibereichsnamens wie folgt durch das Suffix ersetzt:

```
\\Ihr_Knotenname_OLD
```

Ist der neue Dateibereichsname bereits auf dem Server vorhanden, benennt der Server den neuen Dateibereich in `\\Ihr-Knotenname_OLDx` um, wobei `x` eine eindeutige Zahl ist.

Der Server erstellt neue Unicode-fähige Dateibereiche, die nur die in der aktuellen Operation angegebenen Daten enthalten. Sollen beispielsweise Dateien von Ihrer Platte `H:` mit dem Namen `\\Ihr-Knoten\h$` archiviert werden, geben Sie den folgenden Archivierungsbefehl ein:

```
arc h:\logs\*.log
```

Bevor die Archivierung stattfindet, benennt der Server den Dateibereich in `\\Ihr-Knoten\h$_OLD` um. Bei der Archivierung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen `\\Ihr-Knoten\h$` gestellt. Der neue Unicode-fähige Dateibereich enthält nun nur das Verzeichnis `\logs` und die Dateien `*.log`, die in der Operation angegeben wurden. Alle Daten aus nachfolgenden vollständigen und partiellen Teilsicherungen, selektiven Sicherungen und Archivierungen werden in den neuen Unicode-fähigen Dateibereichen gespeichert.

Die umbenannten Dateibereiche verbleiben als stabilisierte Dateibereiche auf dem Server. *Diese Dateibereiche enthalten alle Originaldaten, die Sie zurückschreiben können, solange sie sich auf dem Server befinden.*

Anmerkung: Wenn ein vorhandener Dateibereich während der Unicode-Konvertierung umbenannt wird, gelten die für den Dateibereich definierten Zugriffsregeln weiterhin für den ursprünglichen Dateibereich. Für den neuen Unicode-Dateibereich müssen neue Zugriffsregeln definiert werden.

Führen Sie nach der Installation eine vollständige Teilsicherung aus und benennen Sie alle vorhandenen Dateibereiche um, die nicht Unicode-fähig sind. Sichern Sie die darin enthaltenen Dateien und Verzeichnisse unter den neuen Unicode-fähigen Dateibereichen. Diese Operation erfordert mehr Verarbeitungszeit und Speicher auf dem Server.

Dateibereiche, die nicht Unicode-fähig sind, können im Zeichensatz der Ländereinstellung angezeigt werden, in der die Dateien gesichert wurden. Eine Workstation mit anderen länderspezifischen Angaben ist möglicherweise nicht in der Lage, diese Dateibereiche anzuzeigen oder Daten aus diesen Dateibereichen zurückzuschreiben. Unicode-fähige Dateibereiche, die in bestimmten länderspezifischen Angaben gesichert werden, sind in allen anderen länderspezifischen Angaben sichtbar, sofern auf der Workstation die entsprechenden Schriftarten installiert sind.

Zum Zurückschreiben oder Abrufen aus einem Dateibereich, der nicht Unicode-fähig ist, müssen Sie die Quelle auf dem Server und das Ziel auf dem Client angeben. Siehe

Der Server kann die Option autofsrename definieren und die Einstellung für autofsrename auf dem Client überschreiben.

Unterstützte Clients

Diese Option ist nur für Mac OS X gültig. Der Server kann die Option autofsrename definieren und die Einstellung für autofsrename auf dem Client überschreiben. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Diese Option ist für alle Windows-Clients gültig. Der Server kann die Option autofsrename definieren und die Einstellung für autofsrename auf dem Client überschreiben. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Allgemein im Dropdown-Listenfeld Nicht-Unicode-Dateibereiche beim Sichern/Archivieren umbenennen im Profileditor definieren.

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Allgemein im Dropdown-Listenfeld Nicht-Unicode-Dateibereiche beim Sichern/Archivieren umbenennen im Profileditor angeben.

Syntax

Parameter

Yes
: Gibt an, dass der IBM Spectrum Protect-Server automatisch alle Dateibereiche, die nicht Unicode-fähig sind, in der aktuellen Sicherungs- oder Archivierungsoperation umbenennt.

No
: Gibt an, dass der Server Dateibereiche, die nicht Unicode-fähig sind, in der aktuellen Sicherungs- oder Archivierungsoperation nicht umbenennt.

Prompt
: Gibt an, dass Sie angeben müssen, ob die Dateibereiche, die nicht Unicode-fähig sind, in der aktuellen Operation umbenannt werden sollen. Dies ist der Standardwert.

Hinweise:

- Diese Option wird nur angewendet, wenn der Server die Option autofsrename auf `client` setzt.
- Wenn der Client-Scheduler ausgeführt wird, wird standardmäßig keine Bedienerführung angezeigt. Bei der nächsten interaktiven Sitzung werden Sie über eine Bedienerführung gefragt, ob der Dateibereich umbenannt werden soll.
- Der Client zeigt die Bedienerführung *nur* einmal pro Dateibereich an. Wird an der Bedienerführung `no` angegeben, kann der Client die Dateibereiche später nicht mehr umbenennen. Der IBM Spectrum Protect-Administrator kann die Dateibereiche jedoch auf dem Server umbenennen.
- Mac OS X-Betriebssysteme Windows-BetriebssystemeWerden Dateien in einem Dateibereich gesichert, der nicht Unicode-fähig ist, überspringt der Unicode-fähige Client die Dateien und Verzeichnisse mit Namen, die Zeichen aus einer Zeichenumsetztabelle enthalten, die von den aktuellen länderspezifischen Angaben abweichen.
- Mac OS X-Betriebssysteme Windows-BetriebssystemeWurden Dateien und Verzeichnisse mit Namen, die Zeichen aus einer anderen Zeichenumsetztabelle als den aktuellen länderspezifischen Angaben enthalten, zuvor mit einem Client gesichert, der nicht Unicode-fähig war, können sie verfallen. Der Unicode-fähige Client lässt diese Dateien verfallen, wenn Sie den Dateibereich nicht in einen Unicode-fähigen Dateibereich migrieren. Sie können diese Dateien in einem Unicode-fähigen Dateibereich sichern und archivieren.

Beispiele

Optionsdatei:

```
autofsrename yes
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Automount

Die Option automount fügt durch Anhängen ein Auto-Mount-Dateisystem in die Domäne ein. Diese Option ist mit der Option domain zu verwenden.

Verwenden Sie diese Option, um alle Auto-Mount-Dateisysteme anzugeben, die der Client für Sichern/Archivieren zu folgenden Zeitpunkten anzuhängen versucht:

- Beim Start des Clients
- Beim Start der Sicherung
- Wenn der Client während der Sicherung ein Auto-Mount-Dateisystem erreicht hat

Hängen Sie das Dateisystem an, bevor der Client eine Sicherung dieses Dateisystems ausführt. Wenn das Dateisystem immer vor der Ausführung der Sicherung angehängt wird, ist es nicht erforderlich, explizit ein Auto-Mount-Dateisystem in der Option automount anzugeben. Sie sollten dieses Dateisystem jedoch der Option automount hinzufügen, um sicherzustellen, dass das Dateisystem zu allen oben aufgeführten Zeitpunkten angehängt wurde. Die Auto-Mount-Dateisysteme werden erneut angehängt, wenn sie zwischenzeitlich während einer Sicherung abgehängt wurden.

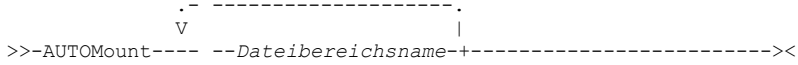
Unterstützte Clients

Diese Option ist für alle UNIX-Plattformen außer Mac OS X gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax



Parameter

Dateibereichsname
: Gibt mindestens ein vollständig qualifiziertes Auto-Mount-Dateisystem an, das angehängt und in die Domäne eingefügt wird.

Beispiele

Optionsdatei:
: automount /home/Fred /home/Sam

Befehlszeile:
: Nicht zutreffend.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Backmc

Die Option backmc gibt die Verwaltungsklasse an, die für Aufbewahrungszwecke auf den Befehl backup fastback angewendet werden soll.

Verwenden Sie die Option backmc mit dem Befehl backup fastback.

Wenn Sie ein Objekt mehrmals sichern und für jede Sicherung eine andere Verwaltungsklasse angeben, werden alle Sicherungsversionen des Objekts erneut an die letzte angegebene Verwaltungsklasse gebunden.

Unterstützte Clients

 LinuxBetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

 WindowsBetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile oder im Scheduler angeben.

Syntax

```
>>-BACKMc=--Name der Verwaltungsklasse------------------------><
```

Parameter

Name der Verwaltungsklasse
: Gibt den Namen der Verwaltungsklasse an.

Beispiele

Befehlszeile:
```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=server1 -backmc=ret2yrs
```

Backupsetname

Die Option backupsetname gibt den Namen eines Sicherungssatzes auf dem IBM Spectrum Protect-Server an.

Sie können die Option backupsetname in den folgenden Befehlen verwenden:

- query backup
- query filespace
-  Windows-Betriebssystemequery image
- AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssystemequery image
-  Windows-Betriebssystemequery systemstate
-  Windows-Betriebssystemerestore image
-  AIX-Betriebssysteme  Linux-BetriebssystemeOracle Solaris-Betriebssystemerestore image

Anmerkung: Die folgenden Befehle akzeptieren den Parameter backupsetname zur Angabe einer Position. Der Parameter backupsetname zur Angabe einer Position verhält sich anders als die Option backupsetname. Den Beschreibungen der Befehle können Sie entnehmen, wie der Parameter backupsetname zur Angabe einer Position sich auf jeden dieser Befehle auswirkt:

- query backupset
- restore

- restore backupset

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist für alle UNIX- und Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Windows-BetriebssystemeDiese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Syntax

```
>>-BACKUPSETName--Name des Sicherungssatzes-------------------><
```

Parameter

Name des Sicherungssatzes
: Gibt den Namen des Sicherungssatzes auf dem IBM Spectrum Protect-Server an. Platzhalterzeichen sind nicht zulässig.

Beispiele

Befehlszeile:

Mac OS X-Betriebssysteme

```
dsmc query backup /Volumes/bkSets/file.1
  -backupsetname=YEAR_END_ACCOUNTING.12345678
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc query backup /usr/projects -subdir=yes
  -backupsetname=YEAR_END_ACCOUNTING.12345678
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
dsmc restore image /home/proj
  -backupsetname=ACCOUNTING_2007.12345678
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

```
dsmc query image -backupsetname=WEEKLY_BSET.21435678
```

Windows-Betriebssysteme

```
dsmc query backup c:\* -subdir=yes
  -backupsetname=weekly_accounting_data.32145678
```

Windows-Betriebssysteme

```
dsmc restore image e:
  -backupsetname=weekly_backup_data.12345678
```

Linux-BetriebssystemeWindows-Betriebssysteme

Basesnapshotname

Die Option basesnapshotname gibt die Momentaufnahme an, die als Basismomentaufnahme verwendet werden soll, wenn Sie eine Momentaufnahmedifferenzsicherung (snapdiff) eines NetApp-Dateiserverdatenträgers ausführen. Wenn Sie diese Option angeben, müssen Sie auch die Option snapdiff verwenden. Andernfalls tritt ein Fehler auf. Wenn basesnapshotname nicht angegeben wird, wählt die Option useexistingbase die jüngste Momentaufnahme auf dem Dateiserverdatenträger als Basismomentaufnahme aus.

Wenn die angegebene Momentaufnahme nicht gefunden wird, wird ein Fehler gemeldet und die Sicherungsoperation schlägt fehl.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Diese Option kann in der Clientoptionsdatei oder in der Befehlszeile angegeben werden.

Syntax

```
>>-BASESNAPSHOTName-- --Momentaufnahmename--------------------><
```

Parameter

Momentaufnahmename
Gibt den Namen einer vorhandenen Momentaufnahme an, die als Basismomentaufnahme verwendet werden soll. Der angegebene Name kann der Name einer Momentaufnahme wie vol1_snap oder der Name einer geplanten NetApp-Sicherung wie beispielsweise nightly.*x* sein, wobei *x* für die Folgenummer steht (dabei ist nightly.0 die älteste Momentaufnahme).
Sie können auch ein Muster mit Platzhalterzeichen für die Auswahl einer Momentaufnahme verwenden. Gültige Platzhalterzeichen sind:

*
: Ein Stern (*) entspricht beliebigen Zeichen.

?
: Ein Fragezeichen (?) entspricht einem einzelnen Zeichen.

Die Platzhalterzeichen sind nützlich, wenn Ihre Momentaufnahmenamen einem Muster entsprechen, z. B. wenn sie das Datum oder die Uhrzeit enthalten. Eine am 12. November 2012 um 11:10:00 Uhr erstellte Momentaufnahme könnte beispielsweise als `UserDataVol_121103111000_snapshot` gespeichert werden. Die jüngste Momentaufnahme, die dem Muster entspricht, wird als vorhandene Basis ausgewählt. Wenn beispielsweise die beiden gespeicherten Momentaufnahmen `UserDataVol_121103111000_snapshot` und `UserDataVol_121103231000_snapshot` vorhanden sind, wird `UserDataVol_121103231100_snapshot` ausgewählt, weil diese Momentaufnahme 12 Stunden jünger als die andere Momentaufnahme ist.

```
-basesnapshotname="UserDataVol_*_snapshot"
```

Fragezeichen sind für geplante Sicherungen, die einem konsistenten Namensmuster folgen, gut geeignet. Mit der folgenden Syntax wird die jüngste Sicherung "nightly" als Momentaufnahme ausgewählt, die als vorhandene Basis verwendet werden soll.

```
-basenameshotname="nightly.?"
```

Beispiele

Optionsdatei:

```
basesnapshotname nightly.?

basesnapshotname volum_base_snap
```

Befehlszeile:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff
  -useexistingbase -basesnapshotname="nightly.?"
```

Zugehörige Verweise:
Useexistingbase

Cadlistenonport

Die Option cadlistenonport gibt an, ob ein Empfangsport für den Clientakzeptor geöffnet werden soll.

Wenn ein Empfangsport offen ist, kann er alle eingehenden Verbindungen akzeptieren. Der Port wird jedoch nicht verwendet, wenn der Clientakzeptor nur den Scheduler verwaltet und der Scheduler im Abfragemodus ausgeführt wird. Mit dieser Option können Sie verhindern, dass der Akzeptor den nicht verwendeten Port öffnet.

Die Standardeinstellung für diese Option ist yes. Verwenden Sie cadlistenonport no nur, wenn managedservices schedule und schedmode polling verwendet werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                    .-Yes-.
>>-CADLISTENONPort--+-----+-------------------------------------><
                    '-No--'
```

Parameter

Yes
: Gibt an, dass der Clientakzeptor einen Empfangsport öffnet. Dieser Parameter ist der Standardwert.

No
: Gibt an, dass der Clientakzeptor keinen Empfangsport öffnet. Verwenden Sie diese Einstellung, wenn Sie den Clientakzeptor nur zur Verwaltung des Schedulers im Abfragemodus verwenden.

  Diese Einstellung bewirkt die effektive Inaktivierung anderer Clientfunktionen, die vom Clientakzeptor abhängig sind, wie beispielsweise Sicherungs- und Zurückschreibungsoperationen des Web-Clients, Operationen der IBM Spectrum Protect for Virtual Environments: Data Protection for VMware vSphere-GUI sowie Sicherungs- und Zurückschreibungsoperationen von IBM Spectrum Protect Snapshot.

Beispiel

Optionsdatei:
: cadlistenonport no

Befehlszeile:
: Nicht zutreffend.

Zugehörige Verweise:
Managedservices
Schedmode
Windows-Betriebssysteme

Casesensitiveaware

Die Option casesensitiveaware gibt an, ob der Windows-Client für Sichern/Archivieren versucht, Datei- und Verzeichnisobjekte herauszufiltern, bei denen Namenskonflikte vorliegen, die durch unterschiedliche Groß-/Kleinschreibung verursacht werden.

Bei NTFS- und ReFS-Datenträgern muss die Groß-/Kleinschreibung beachtet werden und es ist möglich, Dateinamen mit unterschiedlicher Groß-/Kleinschreibung zu speichern. Im Betriebssystem Windows muss die Groß-/Kleinschreibung zwar nicht beachtet werden, aber Anwendungen wie Windows Services for UNIX (SFU) verwenden POSIX-Konventionen und erlauben Dateinamen, bei denen die Groß-/Kleinschreibung beachtet werden muss. SFU ist normalerweise in Windows-Betriebssystemen wie Windows Powered OS und Windows Storage Server enthalten. Diese Betriebssysteme werden in der Regel auf Hardware implementiert (z. B. NAS-Hardware), die als dedizierter Dateiserver in einer heterogenen Umgebung fungiert.

Sind UNIX-Clients vorhanden, die Dateien auf NTFS- oder ReFS-Datenträgern in diesen Windows-Dateiserverumgebungen speichern, verwenden Sie die Option casesensitiveaware. Wird diese Option in diesen Umgebungen nicht verwendet, treten während der Sicherungs- und Archivierungsoperationen unvorhersehbare Ergebnisse auf, wenn Konflikte bezüglich der Groß-/Kleinschreibung bei Dateinamen festgestellt werden. Für homogene Windows-Dateiserverumgebungen ist die Option casesensitiveaware nicht erforderlich.

Beispiel: Es liegt eine Gruppe von Objekten mit den Namen 'MyWork.xls', 'MYWORK.xls' und 'mywork.xls' vor. Da im Betriebssystem Windows die Groß-/Kleinschreibung nicht beachtet werden muss, können Anwendungen nicht zwischen den beiden Objekten 'mywork.xls' und 'MyWork.xls' unterscheiden.

Aus diesem Grund kann der Windows-Client für Sichern/Archivieren die Zurückschreibungsintegrität solcher Objekte nicht garantieren. Wenn ein Namenskonflikt bezüglich der Groß-/Kleinschreibung auftritt, kann der Client für Sichern/Archivieren nur die Zurückschreibungsintegrität der ersten Datei in einer alphabetischen Sortierung garantieren. Für ein auf ASCII basierendes Betriebssystem wie Windows bedeutet dies, dass Großbuchstaben in einer alphabetischen Sortierung vor Kleinbuchstaben erscheinen, sodass 'MyWork.xls' vor 'mywork.xls' stehen würde.

In diesem Beispiel würde bei Verwendung der Option casesensitiveaware nur 'MyWork.xls' verarbeitet. Für `'mywork.xls'` wird eine Fehlernachricht ausgegeben und sie wird übersprungen. Ist 'mywork.xls' ein Verzeichnis, würde die Unterverzeichnisstruktur 'mywork.xls' übersprungen. In allen Fällen werden Nachrichten in das lokale Fehlerprotokoll geschrieben und an der IBM Spectrum Protect-Serverkonsole ausgegeben, um die exakten Dateinamen der Objekte anzugeben, die übersprungen werden.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                          .-No--.
>>-CASESENSITIVEAware--+-----+---------------------------------><
                          '-Yes-'
```

Parameter

yes
: Gibt an, dass der Client versucht, Objektnamen zu identifizieren, die sich nur in der Groß-/Kleinschreibung unterscheiden, und Objekte herauszufiltern, bei denen Konflikte bezüglich der Groß-/Kleinschreibung vorliegen und für die eine korrekte Zurückschreibung nicht garantiert werden kann.

no
: Gibt an, dass der Client nicht versucht, Objektnamen zu identifizieren, die sich nur in der Groß-/Kleinschreibung unterscheiden. Dies ist der Standardwert.

Changingretries

Mit der Option changingretries wird angegeben, wie oft der Client den Versuch, eine im Gebrauch befindliche Datei zu sichern oder zu archivieren, wiederholen soll. Diese Option ist in den Befehlen archive, incremental und selective zu verwenden.

Diese Option ist nur dann zu verwenden, wenn für die Kopiennummerierung (ein Attribut in der Kopiengruppe einer Verwaltungsklasse) Gemeinsam statisch oder Gemeinsam dynamisch angegeben wird.

Ist eine Datei bei der Durchnummerierung Gemeinsam statisch während einer Operation geöffnet, wird die Operation so oft wiederholt, wie Sie angeben. Ist die Datei bei jedem Versuch geöffnet, wird die Operation nicht durchgeführt.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeIst eine Datei bei der Durchnummerierung Gemeinsam dynamisch während einer Operation geöffnet, wird die Operation so oft wiederholt, wie Sie angeben. Die Sicherung oder Archivierung wird beim letzten Versuch durchgeführt, unabhängig davon, ob die Datei geöffnet ist.

 Windows-BetriebssystemeIst eine Datei bei der Durchnummerierung Gemeinsam dynamisch während einer Operation geöffnet, wird die Operation so oft wiederholt, wie Sie angeben. Die Sicherung oder Archivierung wird beim letzten Versuch durchgeführt, unabhängig davon, ob die Datei geöffnet ist. Mit der Unterstützung offener Dateien können Dateien gesichert werden, die gesperrt oder im Gebrauch sind.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDiese Option ist für alle UNIX- und Linux-Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

 Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Sichern im Feld Anzahl Wiederholungen, wenn Datei im Gebrauch ist des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Sichern im Feld Anzahl Wiederholungen, wenn Datei im Gebrauch ist des Profileditors definieren.

Syntax

```
>>-CHAngingretries- Anzahl Wiederholungen---------------------><
```

Parameter

Anzahl Wiederholungen
: Gibt an, wie oft ein Sicherungs- oder Archivierungsversuch wiederholt wird, wenn die Datei im Gebrauch ist. Der Wertebereich ist 0 bis 4; Standardwert ist 4.

Beispiele

Optionsdatei:
: changingretries 3

Befehlszeile:
: -cha=3

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Class

Die Option class gibt an, ob bei Verwendung der Befehle delete filespace, query backup und query filespace eine Liste der NAS- oder der Clientobjekte angezeigt werden soll.

Wenn Sie z. B. eine Liste der Dateibereiche anzeigen wollen, die zu einem NAS-Knoten gehören, geben Sie folgenden Befehl ein:

```
query filespace -class=nas
```

Unterstützte Clients

 AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist nur für AIX-, Linux- und Oracle Solaris-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

 Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Syntax

```
            .-client-.
>>-CLASS = -+--------+-----------------------------------------><
            '-nas----'
```

Parameter

client
: Gibt an, dass Sie eine Liste der Dateibereiche für einen Clientknoten anzeigen wollen. Dies ist der Standardwert.

nas
: Gibt an, dass Sie eine Liste der Dateibereiche für einen NAS-Knoten anzeigen wollen.

Beispiele

Keine. Sie können diese Option nur in der Befehlszeile angeben.

Befehlszeile:
: `q backup -nasnodename=Knotenname -class=nas`

Windows-Betriebssysteme

Clientview

Die Option clientview ist für Benutzer verfügbar, die ein Upgrade vom IBM® Tivoli Storage Manager Express-Sicherungsclient auf den Enterprise-Client für Sichern/Archivieren durchgeführt haben.

Um diese Option verwenden zu können, muss eine Verbindung zu einem Tivoli Storage Manager-Server mit Version 5.4 oder höher bestehen. Mit der Option clientview können Sie entweder die Express-Sicht oder die Standardsicht der Client-GUI (GUI = grafische Benutzerschnittstelle) auswählen.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.opt ein. Zum Umschalten in die Express-Sicht führen Sie Folgendes aus:

1. Wählen Sie in der GUI des Clients für Sichern/Archivieren Editieren > Vorgaben in der Menüleiste aus.
2. Klicken Sie auf der Registerkarte Allgemein des Profileditors im Feld Clientsicht auf Express.
3. Klicken Sie auf OK, um Ihre Änderungen zu sichern.

Zum Umschalten in die Standardsicht führen Sie Folgendes aus:

1. Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Einstellungen ändern.
2. Klicken Sie auf der Registerkarte Allgemein des Profileditors im Feld Clientsicht auf Standard.
3. Klicken Sie auf OK, um Ihre Änderungen zu sichern.

Syntax

```
                .-standard-.
>>-CLIENTVIEW = -+----------+----------------------------------><
                '-express--'
```

Parameter

standard
: Gibt an, dass die Standard- oder Enterprise-Sicht der GUI des Clients für Sichern/Archivieren verwendet werden soll. Die Standardsicht enthält die erweiterten Funktionen der GUI des Clients für Sichern/Archivieren. Dies ist der Standardwert.

express
: Gibt an, dass die Express-Sicht der GUI des Clients für Sichern/Archivieren verwendet werden soll. Die Express-Sicht enthält dieselben Funktionen wie die GUI des Express-Sicherungsclients.

 Windows-Betriebssysteme

Clusterdisksonly

Die Option clusterdisksonly gibt an, ob der Client für Sichern/Archivieren die ausschließliche Sicherung von Clusterplatten in bestimmten Umgebungen zulässt.

Der Client für Sichern/Archivieren lässt die ausschließliche Sicherung von Clusterplatten zu, wenn der Client in den folgenden Umgebungen ausgeführt wird:

- In einem Microsoft Cluster Server (MSCS)
- Wenn Failover-Cluster-Unterstützung auf einem unterstützten Windows-Server eingesetzt wird
- In einer VCS-Umgebung (VERITAS Cluster Server), wenn Sie clusternode yes angeben

Bisher ließ der Client für Sichern/Archivieren nur Sicherungen und Zurückschreibungen von Daten auf Clusterlaufwerken zu, die als Laufwerkbuchstabe bereitgestellt wurden.

Es ist üblich, dass Clusterlaufwerke als Datenträgermountpunkte bereitgestellt werden. Windows-Server-Betriebssysteme erlauben es dem Benutzer, die Begrenzung von 26 Laufwerkbuchstaben zu überschreiten, indem die Definition von Datenträgermountpunkten auf einem Cluster-Server zugelassen wird. Der Client kann Daten auf Clusterplatten schützen, die in Computern mit einem Windows Server-Betriebssystem als Laufwerkbuchstabe bereitgestellt werden. Der Client kann auch Daten auf Clusterplatten schützen, die als Datenträgermountpunkte bereitgestellt werden. Der Client für Sichern/Archivieren kann automatisch feststellen, ob ein Datenträger, der einen Datenträgermountpunkt verwendet, ein Clusterdatenträger ist.

Wenn Sie clusterdisksonly yes angeben, trennt der Client für Sichern/Archivieren weiterhin lokale Laufwerke von Clusterlaufwerken, wenn er die Domänenoption ALL-LOCAL auswertet. Wenn clusterdisksonly no angegeben wird, müssen Sie die Sicherungsdomänen explizit definieren. Wenn clusterdisksonly no angegeben wird, übergeht der Client für Sichern/Archivieren außerdem die Aufzählung der Clusterressourcen, um festzustellen, welche Ressourcen Clusterlaufwerke darstellen.

Unterstützte Clients

Diese Option ist für alle unterstützten Windows Server-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                      .-Yes-.
>>-CLUSTERDISKSOnly--+-----+-----------------------------------><
                      '-No--'
```

Parameter

Yes
: Gibt an, dass der Client nur die Verarbeitung von Clusterlaufwerken zulässt. 'Yes' ist der Standardwert.

No
: Gibt an, dass der Client die Verarbeitung aller Platten zulässt, wenn clusternode yes definiert ist.

Beispiele

Szenario 1: Einen Knoten sichern, der die lokalen Laufwerke (keine Clusterlaufwerke) und die Systemstatusinformationen verwaltet

Hierbei handelt es sich um den Knoten, der für die Wiederherstellung des physischen Systems zuständig ist, falls ein Hardwarefehler auftreten sollte. Es gibt keine Clusterlaufwerke, die als Datenträgermountpunkte bereitgestellt werden.

Optionsdatei:

```
CLUSTERNODE NO (Standardwert)
CLUSTERDISKSONLY YES (Standardwert)
DOMAIN ALL-LOCAL (Standardwert)
EXCLUDE c:\...\file.txt
```

Szenario 1b: Einen Knoten sichern, der die lokalen Laufwerke (keine Clusterlaufwerke) und die Systemstatusinformationen verwaltet, und die Aufzählung der Clusterressourcen übergehen

Dieses Szenario ist dem Szenario 1 ähnlich. Es kann eingesetzt werden, wenn der Startvorgang des Clients für Sichern/Archivieren zu viel Zeit in Anspruch nimmt. Während der Initialisierung des Clients für Sichern/Archivieren werden alle Clusterressourcen aufgezählt, um festzustellen, welche Ressourcen Clusterplatteneinheiten darstellen. Diese Verarbeitung kann mit der Angabe clusterdisksonly no übersprungen werden.

Optionsdatei:

```
CLUSTERNODE NO (Standardwert)
CLUSTERDISKSONLY NO
DOMAIN C: D: (lokale Laufwerke müssen explizit aufgezählt werden)
EXCLUDE c:\...\file.txt
```

Szenario 2: Einen Knoten sichern, der die Clusterlaufwerke in einer Clusterressourcengruppe verwaltet, und die Aufzählung der Clusterressourcen übergehen

Dieses Szenario kann eingesetzt werden, wenn der Startvorgang des Clients für Sichern/Archivieren zu viel Zeit in Anspruch nimmt. Während der Initialisierung des Clients für Sichern/Archivieren werden alle Clusterressourcen aufgezählt, um festzustellen, welche Ressourcen Clusterplatteneinheiten darstellen. Diese Verarbeitung kann mit der Angabe clusterdisksonly no übersprungen werden.

Optionsdatei:

```
CLUSTERNODE YES
CLUSTERDISKSONLY NO
DOMAIN f: g:
EXCLUDE f:\...\file.txt
```

Szenario 3: Einen Knoten sichern, der die Clusterlaufwerke in einer Clusterressourcengruppe verwaltet, und dabei Datenträgermountpunkte als Clusterressourcen verwenden

In diesem Szenario wird vorausgesetzt, dass der Knoten für die Sicherung einer Clusterressourcengruppe verantwortlich ist, die über zwei Laufwerke, f: und f:\mnt, verfügt. Es gibt Clusterlaufwerke, die als Datenträgermountpunkte bereitgestellt werden (Windows Server-Betriebssysteme). Stellen Sie sicher, dass Sie für die Domäne mit Teilsicherungsverarbeitung nur die Datenträger in einer Clusterressourcengruppe definieren. Wenn Sie mehrere Clusterressourcengruppen haben, ordnen Sie einen eindeutigen Clientknoten für die Verwaltung jeder Clusterressourcengruppe zu.

Optionsdatei

```
CLUSTERNODE YES
CLUSTERDISKSONLY YES
DOMAIN f: f:\mnt
EXCLUDE f:\mnt\...\file.txt
```

Tabelle 1 enthält eine Liste der Kombinationen von clusternode und clusterdisksonly.

Tabelle 1. Kombinationen von clusternode und clusterdisksonly

Clusternode	Clusterdiskonly	Verwendung
no	yes	Dies ist das Standardverhalten, wenn keine Angabe erfolgt; da die Option clusterdisksonly auf clusterdisksonly yes gesetzt ist, wird die Clusterplattenzuordnungstabelle erstellt. Diese Kombination wird zum Sichern lokaler Laufwerke verwendet.
yes	yes	Dies ist die Standardeinstellung für die Ausführung in einem Clusterknoten zur Sicherung von Clusterplatten, einschließlich Platten, die als Mountpunkte verfügbar sind. Die Clusterplattenzuordnungstabelle wird erstellt.
yes	no	Für Clients, die unter Windows Server-Betriebssystemen ausgeführt werden, dürfen Sie clusterdisksonly no nur angeben, wenn Sie die Aufzählung der Clusterdatenträger aus Gründen der Leistung übergehen wollen.

 Windows-Betriebssysteme

Clusternode

Die Option clusternode gibt an, wie der Client für Sichern/Archivieren Clusterlaufwerke verwaltet.

 Windows-BetriebssystemeDer Client für Sichern/Archivieren verwaltet Clusterlaufwerke in den folgenden Umgebungen:

- Microsoft Cluster Server (MSCS)
- Failover-Cluster-Unterstützung (Clustering mit Übernahme) in Windows Server-Systemen
- VERITAS Cluster Server (VCS)

Ist clusternode yes festgelegt, sind nur gemeinsam genutzte Clusterlaufwerke für die Sicherungs- und Archivierungsverarbeitung verfügbar. Wenn Sie clusternode yes definieren, ist der Knotenname standardmäßig der Clustername.

 Windows-BetriebssystemeZum Sichern der lokalen Laufwerke oder des Windows Server-Systemstatus müssen Sie clusternode no festlegen.

Anmerkung: Sie müssen clusternode yes für alle von IBM Spectrum Protect verwalteten Clusteroperationen definieren. Wird die Option clusternode für einen bestimmten IBM Spectrum Protect-Clusterknotennamen nicht konsistent verwendet, wird das verschlüsselte Kennwort für den Clusterknotennamen möglicherweise ungültig und der Benutzer wird beim nächsten Aufruf des IBM Spectrum Protect-Programms zur erneuten Eingabe des Kennworts aufgefordert.

Verwenden Sie die Option optfile, um die richtige (Cluster-)Datei dsm.opt für alle IBM Spectrum Protect-Programme aufzurufen, damit bei Clusteroperationen die korrekte Funktionalität sichergestellt ist. Weitere Informationen finden Sie in der Beschreibung der Option optfile.

 Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für Clients mit dem Betriebssystem Windows Server gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                .-No--.
>>-CLUSTERnode--+-----+---------------------------------------><
                '-Yes-'
```

Parameter

 WindowsBetriebssystemeYes
 WindowsBetriebssystemeGibt an, dass der Client Clusterlaufwerke in den folgenden Umgebungen verwalten soll:

- MSCS
- Failover-Cluster-Unterstützung (Clustering mit Übernahme) in Windows Server-Systemen
- VCS

No
Gibt an, dass Sie lokale Festplatten sichern wollen. Dies ist der Standardwert.

Beispiele

Optionsdatei:
cluster no

Befehlszeile:
-cluster=yes

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Collocatebyfilespec

Verwenden Sie die Option collocatebyfilespec, um anzugeben, ob der Client für Sichern/Archivieren nur eine Serversitzung verwenden soll, um Objekte zu senden, die von einer einzigen Dateispezifikation generiert wurden.

Durch das Setzen der Option collocatebyfilespec auf yes wird versucht, das Durchsetzen von Dateien von unterschiedlichen Dateispezifikationen zu eliminieren, indem der Client auf eine Serversitzung pro Dateispezifikation begrenzt wird. Wenn Sie Daten auf Band speichern, werden Dateien für jede Dateispezifikation deshalb zusammen auf einem Band gespeichert (sofern auf Grund erhöhter Kapazität kein weiteres Band erforderlich ist).

Hinweise:

- Verwenden Sie die Option collocatebyfilespec nur, wenn der Speicherpool direkt auf Band geht. Wenn Sie diese Option für einen Plattenspeicherpool verwenden, könnte dies den Lastausgleich und somit das Leistungsverhalten negativ beeinflussen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDiese Option ist für alle UNIX- und Linux-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                          .-No--.
>>-COLlocatebyfilespec--+-----+--------------------------------><
                          '-Yes-'
```

Parameter

Yes
: Gibt an, ob der Client nur eine Serversitzung verwenden soll, um Objekte zu senden, die von einer einzigen Dateispezifikation generiert wurden. Wenn Sie Daten auf Band speichern, werden Dateien für jede Dateispezifikation deshalb zusammen auf einem Band gespeichert, sofern auf Grund erhöhter Kapazität kein weiteres Band erforderlich ist. Als Ergebnis kann sich die Leistung beim Zurückschreiben erhöhen.

No
: Gibt an, dass der Client (abhängig von der Ausführungsdynamik und der Einstellung der Option resourceutilization auf 3 oder höher) mehrere Serversitzungen verwenden kann, um die Dateien von einer Dateispezifikation zu senden. Dies ist der Standardwert.

  Als Ergebnis kann sich die Leistung beim Sichern erhöhen. Wenn die Dateien auf Band gesichert werden, werden sie auf mehreren Bändern gespeichert. Im Allgemeinen sind die in der Dateispezifikation angegebenen Dateien trotzdem zusammenhängend.

Beispiele

Optionsdatei:
collocatebyfilespec yes
Befehlszeile:
-collocatebyfilespec=yes

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Commmethod

Mit der Option commmethod wird die verwendete Übertragungsmethode für die Konnektivität der Client/Server-Übertragung angegeben.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Übertragung des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung des Profileditors definieren.

AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-Betriebssysteme

Syntax

```
              .-TCPip-----.
>>-COMMMethod-+-----------+-------------------------------------><
              +-SHAREdmem-+
              '-V6TCPIP---'
```

Windows-Betriebssysteme

Syntax

```
              .-TCPip------.
>>-COMMMethod-+------------+-----------------------------------><
              +-SHAREdmem--+
              +-V6TCPIP----+
              '-NAMedpipes-'
```

Parameter

TCPip
: Die Übertragungsmethode Transmission Control Protocol/Internet Protocol (TCP/IP). Dies ist der Standardwert.

V6Tcpip
: Gibt an, dass abhängig von der Systemkonfiguration und den Ergebnissen einer DNS-Suche (Domain Name Service - Domänennamensservice) entweder TCP/IP V4 oder V6 verwendet werden soll. Es muss eine gültige DNS-Umgebung verfügbar sein.

Windows-BetriebssystemeNAMedpipes
: Windows-BetriebssystemeDie Interprozesskommunikationsmethode, bei der Nachrichtendatenströme zwischen einem Client und einem Server fließen können. Verwenden Sie diese Übertragungsmethode für einen IBM Spectrum Protect-Server, der auf derselben Workstation wie der Client aktiv ist.

AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssystemeSHAREdmem
: AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssystemeVerwenden Sie die Shared-Memory-Übertragungsmethode, wenn der Client und der Server auf demselben System ausgeführt werden. Dies ermöglicht eine bessere Leistung als das TCP/IP-Protokoll.

  AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssystemeDiese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

  Wenn Sie diese Übertragungsmethode unter AIX angeben, kann der Client als Root oder Nicht-Root angemeldet sein, solange der Server als Root ausgeführt wird. Wird der Server nicht als Root ausgeführt, muss die Benutzer-ID, die den Client ausführt, mit der Benutzer-ID, die den Server ausführt, übereinstimmen.

  Wichtig: Bei Verwendung von commmethod sharedmem unter Linux wird möglicherweise die Fehlernachricht `ANR8294W Shared Memory-Sitzung kann nicht initialisiert werden` auf der Konsole des Servers oder Speicheragenten ausgegeben. Standardmäßig ist Linux nicht mit genügend Systemressourcen konfiguriert, um die Nachrichtenwarteschlangen zu erstellen. Sie müssen den Kernelparameter `MSGMNI` auf 128 erhöhen (der Standardwert ist 16). Sie können diesen Parameter ändern, indem Sie den folgenden Befehl ausführen:

  ```
  echo 128 > /proc/sys/kernel/msgmni
  ```

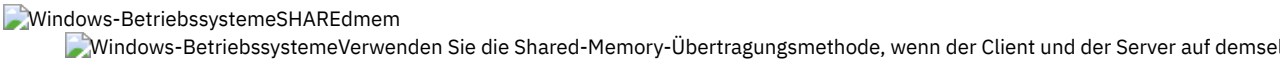
  Damit dieser Parameter auch nach einem Warmstart für das System permanent beibehalten wird, können Sie stattdessen die folgende Zeile der Datei `/etc/sysctl.conf` hinzufügen und dann einen Warmstart für das System durchführen:

  ```
  kernel.msgmni=128
  ```

  Um die aktuelle ipc-Einstellungen anzuzeigen, führen Sie diesen Befehl aus:

```
ipcs -l
```

Schauen Sie sich jetzt den Wert `max queues system wide` an. Der Standardwert ist 16.


Windows-BetriebssystemeSHAREdmem
Windows-BetriebssystemeVerwenden Sie die Shared-Memory-Übertragungsmethode, wenn der Client und der Server auf demselben System ausgeführt werden. Dies ermöglicht eine bessere Leistung als das TCP/IP-Protokoll.
Anmerkung: Die Verwendung dieser Übertragungsmethode erfordert, dass der Client und der Server unter demselben Windows-Konto ausgeführt werden.

Beispiele

Optionsdatei:

Nur TCP/IP V4 verwenden.

```
commmethod tcpip
```

Sowohl TCP/IP V4 als auch V6 verwenden, abhängig von der Systemkonfiguration und den Ergebnissen einer DNS-Suche.

```
commmethod V6Tcpip
```

Anmerkung: Der Befehl 'dsmc schedule' kann nicht verwendet werden, wenn SCHEDMODe prompt und commmethod V6Tcpip angegeben sind.

Befehlszeile:

-commm=tcpip

-commm=V6Tcpip

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Commrestartduration

Mit der Option commrestartduration wird die maximale Anzahl Minuten angegeben, die der Client nach einem Übertragungsfehler zwischen Versuchen, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen, warten soll.

Anmerkung: Ein geplantes Ereignis wird fortgesetzt, wenn der Client die Verbindung zum Server wiederherstellt, bevor der Wert für commrestartduration abläuft; dies ist selbst dann der Fall, wenn das Startfenster des Ereignisses abgelaufen ist.

Sie können die Optionen commrestartduration und commrestartinterval in ausgelasteten oder nicht stabilen Netzumgebungen verwenden, um Verbindungsfehler zu verringern.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Übertragung im Abschnitt Allgemeine Optionen des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung im Abschnitt Allgemeine Optionen des Profileditors definieren.

Syntax

```
>>-COMMRESTARTDuration- Minuten--------------------------------><
```

Parameter

Minuten

Die maximale Anzahl Minuten, die der Client nach einem Übertragungsfehler versuchen soll, die Verbindung zu einem Server wiederherzustellen. Der Wertebereich ist 0 bis 9999; Standardwert ist 60.

Beispiele

Optionsdatei:

commrestartduration 90

Befehlszeile:

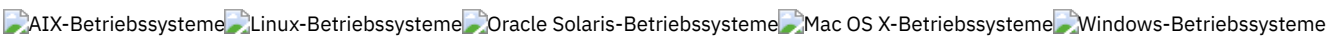
Nicht zutreffend.

Commrestartinterval

Mit der Option commrestartinterval wird die Anzahl Sekunden angegeben, die der Client nach einem Übertragungsfehler zwischen Versuchen, die Verbindung zum IBM Spectrum Protect-Server wiederherzustellen, warten soll.

Anmerkung: Verwenden Sie diese Option nur, wenn für commrestartduration ein Wert größer als Null definiert ist.

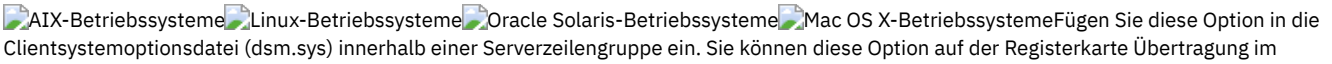
Sie können die Optionen commrestartduration und commrestartinterval in ausgelasteten oder nicht stabilen Netzumgebungen verwenden, um Verbindungsfehler zu verringern.



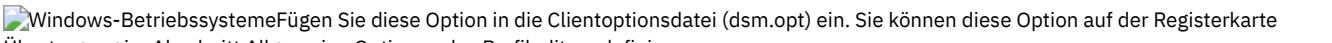
Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei



Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Übertragung im Abschnitt Allgemeine Optionen des Profileditors definieren.



Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung im Abschnitt Allgemeine Optionen des Profileditors definieren.

Syntax

```
>>-COMMRESTARTInterval- Sekunden-------------------------------><
```

Parameter

Sekunden

Die Anzahl Sekunden, die der Client nach einem Übertragungsfehler zwischen den Versuchen, die Verbindung zu einem Server wiederherzustellen, warten soll. Der Wertebereich ist 0 bis 65535; Standardwert ist 15.

Beispiele

Optionsdatei:

commrestartinterval 30

Befehlszeile:

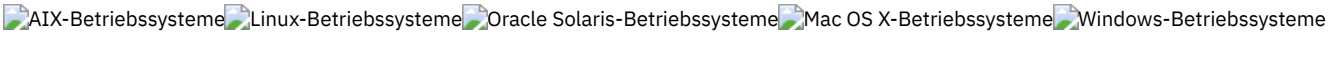
Nicht zutreffend.

Compressalways

Die Option compressalways gibt an, ob die Komprimierung eines Objekts fortgesetzt wird, wenn es während der Komprimierung größer wird.

Verwenden Sie diese Option mit der Option compression und in den Befehlen archive, incremental und selective.

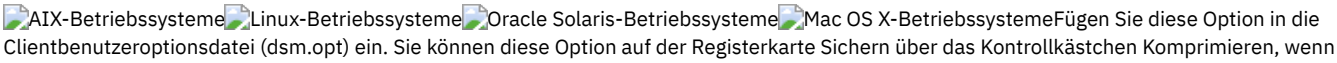
Die Option compressalways wird ignoriert, wenn die clientseitige Deduplizierung aktiviert ist.



Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei



Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Sichern über das Kontrollkästchen Komprimieren, wenn Objekt anwächst im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Sichern über das Kontrollkästchen Komprimieren, wenn Objekt anwächst im Profileditor definieren.

Syntax

```
                    .-Yes-.
>>-COMPRESSAlways--+-----+-------------------------------------><
                    '-No--'
```

Parameter

Yes
: Die Komprimierung der Datei wird fortgesetzt, auch wenn die Datei durch die Komprimierung größer wird. Dies ist der Standardwert.

No
: Objekte des Clients für Sichern/Archivieren werden dekomprimiert erneut gesendet, wenn sie während der Komprimierung größer werden. Das API-Verhalten ist von der Anwendung abhängig. Anwendungssicherungen können fehlschlagen.

Beispiele

Optionsdatei:
: compressalways yes

Befehlszeile:
: -compressa=no

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Compression

Die Option compression komprimiert Dateien, bevor sie an den Server gesendet werden.

Die Komprimierung der Dateien reduziert den erforderlichen Datenspeicherplatz für Sicherungsversionen und Archivierungskopien der Dateien. Das Komprimieren kann sich jedoch auf den IBM Spectrum Protect-Durchsatz auswirken. Bei einem schnellen Prozessor und einer langsamen Netzverbindung ist die Komprimierung von Vorteil, bei einem langsamen Prozessor und einer schnellen Netzverbindung nicht.

Verwenden Sie die Option compression in den Befehlen archive, incremental und selective.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDer Befehl backup image verwendet den Wert der Option compression, der in der Datei dsm.sys angegeben ist. Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Diese Option kann auch auf dem Server definiert werden; sie überschreibt dann den Clientwert.

Windows-BetriebssystemeDer Befehl backup image verwendet den Wert der Option compression, der in der Datei dsm.opt angegeben ist. Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Diese Option kann auch auf dem Server definiert werden; sie überschreibt dann den Clientwert.

Der Client für Sichern/Archivieren sichert eine Datei mit freien Bereichen als reguläre Datei, wenn die Clientkomprimierung inaktiviert ist. Legen Sie compression yes fest, um die Dateikomprimierung bei der Sicherung von Dateien mit freien Bereichen zu aktivieren und dadurch die Netzübertragungszeit zu verringern und den Serverspeicherbereich zu vergrößern.

Wenn Sie compressalways yes festlegen, wird die Komprimierung fortgesetzt, selbst wenn die Dateigröße zunimmt. Soll die Komprimierung gestoppt werden, wenn die Dateigröße zunimmt, und soll die Datei dekomprimiert erneut gesendet werden, müssen Sie compressalways no festlegen.

Wenn Sie compression yes festlegen, können Sie die Komprimierungsverarbeitung auf folgende Weise steuern:

- Windows-BetriebssystemeVerwenden Sie die Option exclude.compression in Ihrer Clientoptionsdatei (dsm.opt), um bestimmte Dateien oder Dateigruppen von der Komprimierungsverarbeitung auszuschließen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeVerwenden Sie die Option exclude.compression in Ihrer Clientsystemoptionsdatei (dsm.sys), um bestimmte Dateien oder Dateigruppen von der Komprimierungsverarbeitung auszuschließen.
- Windows-BetriebssystemeVerwenden Sie die Option include.compression in Ihrer Clientoptionsdatei (dsm.opt), um Dateien innerhalb einer großen Gruppe ausgeschlossener Dateien für die Komprimierungsverarbeitung einzuschließen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeVerwenden Sie die Option include.compression in Ihrer Clientsystemoptionsdatei (dsm.sys), um Dateien innerhalb einer großen Gruppe ausgeschlossener Dateien für die Komprimierungsverarbeitung einzuschließen.

Mit dieser Option kann die Komprimierung nur dann gesteuert werden, wenn Ihr Administrator angibt, dass Ihr Clientknoten Dateien komprimieren kann, bevor sie an den Server gesendet werden.

Der Komprimierungstyp, den der Client verwendet, wird durch die Kombination von Komprimierung und clientseitiger Datendeduplizierung bestimmt, die während der Sicherungs- oder Archivierungsverarbeitung verwendet wird. Die folgenden Komprimierungstypen werden verwendet:

LZ4
: Eine schnellere und effizientere Komprimierungsmethode, die der Client verwendet, wenn vom Client deduplizierte Daten an einen LZ4-kompatiblen Containerspeicherpool auf dem IBM Spectrum Protect-Server gesendet werden. Der Server muss Version 7.1.5 oder höher haben und Containerspeicherpools verwenden. Die clientseitige LZ4-Komprimierung wird nur verwendet, wenn die clientseitige Datendeduplizierung aktiviert ist.

LZW
: Ein traditioneller Komprimierungstyp, den der Client in den folgenden Situationen verwendet:

  - Vom Client deduplizierte Daten werden an traditionelle (Nicht-Container) Speicherpools auf dem Server gesendet.
  - Für die Clientdaten wird keine clientseitige Datendeduplizierung ausgeführt. (Gilt nicht für Data Protection for VMware und Data Protection for Microsoft Hyper-V, bei denen nur vom Client deduplizierte Daten komprimiert werden können.)
  - Für die Clientdaten wird nur eine traditionelle serverseitige Datendeduplizierung ausgeführt. (Gilt nicht für Data Protection for VMware und Data Protection for Microsoft Hyper-V, bei denen nur vom Client deduplizierte Daten komprimiert werden können.)

Keine
: Das Objekt wird vom Client nicht komprimiert. Das Objekt wird nicht komprimiert, da die Option compression auf *no* gesetzt ist oder die Option während der Sicherungs- oder Archivierungsverarbeitung nicht angegeben wird. Auch wenn das Objekt nicht vom Client komprimiert wird, kann es vom Server komprimiert werden.

Sie müssen den Komprimierungstyp nicht definieren. Er wird vom Client für Sichern/Archivieren während der Sicherungs- oder Archivierungsverarbeitung bestimmt.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Sichern über das Kontrollkästchen Objekte komprimieren im Profileditor definieren.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte `Sichern` über das Kontrollkästchen Objekte komprimieren im Profileditor definieren.

Syntax

```
                .-No--.
>>-COMPRESSIon--+-----+-----------------------------------------><
                '-Yes-'
```

Parameter

No
: Dateien werden nicht komprimiert, bevor sie an den Server gesendet werden. Dies ist der Standardwert.

Yes
: Dateien werden komprimiert, bevor sie an den Server gesendet werden.

Beispiele

Optionsdatei:
: compression yes

Befehlszeile:
: -compressi=no

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Verweise:
Deduplication
Ausschlussoptionen
Einschlussoptionen

Console

Verwenden Sie die Option console im Befehl query systeminfo, um Informationen an der Konsole auszugeben.

- DSMOPTFILE - Der Inhalt der Datei dsm.opt
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDSMSYSFILE - Inhalt der Datei dsm.sys
- ENV - Umgebungsvariablen
- ERRORLOG - IBM Spectrum Protect-Fehlerprotokolldatei
- FILE - Attribute für den angegebenen Dateinamen.
- Windows-BetriebssystemeFILESNOTTOBACKUP - Aufzählung des Windows-Registerschlüssels:

  ```
  HKEY_LOCAL_MACHINE\
     SYSTEM\
        CurrentControlSet\
           BackupRestore\
              FilesNotToBackup
  ```

  Dieser Schlüssel gibt diejenigen Dateien an, die von Sicherungsprodukten nicht gesichert werden sollen. Der Befehl query inclexcl zeigt an, dass diese Dateien vom Betriebssystem ausgeschlossen sind.
- INCLEXCL - Stellt eine Liste der Einschluss/Ausschlussanweisungen in der Reihenfolge zusammen, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden.
- Windows-BetriebssystemeKEYSNOTTORESTORE - Aufzählung des Windows-Registerschlüssels:

  ```
  HKEY_LOCAL_MACHINE\
     SYSTEM\
        ControlSet001\
           BackupRestore\
              KeysNotToRestore
  ```

  Dieser Schlüssel gibt diejenigen Windows-Registerschlüssel an, die von Sicherungsprodukten nicht zurückgeschrieben werden sollen.
- Windows-BetriebssystemeMSINFO - Windows-Systeminformationen (Ausgabe von MSINFO32.EXE).
- OPTIONS - Optionen
- Windows-BetriebssystemeOSINFO - Name und Version des Clientbetriebssystems
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeOSINFO - Name und Version des Clientbetriebssystems (umfasst ULIMIT-Informationen für UNIX und Linux).
- POLICY - Speicherauszug der Maßnahmengruppe
- Windows-BetriebssystemeREGISTRY - Windows IBM Spectrum Protect-bezogene Windows-Registry-Einträge.
- SCHEDLOG - Inhalt des IBM Spectrum Protect-Planungsprotokolls (normalerweise dsmsched.log).
- Windows-BetriebssystemeSFP - Liste der Dateien, die durch Windows-Systemdateischutz geschützt sind, und für jede Datei die Anzeige, ob diese Datei vorhanden ist. Diese Dateien werden als Teil des Systemobjekts SYSFILES gesichert.
- Windows-BetriebssystemeSFP=*Dateiname* - Zeigt an, ob die angegebene Datei (*Dateiname*) durch den Windows-Systemdateischutz geschützt ist. Zum Beispiel:

  ```
  SFP=C:\WINNT\SYSTEM32\MSVCRT.DLL
  ```

- Windows-BetriebssystemeSYSTEMSTATE - Informationen zum Windows-Systemstatus
- AIX-BetriebssystemeCLUSTER - AIX-Clusterinformationen
- Windows-BetriebssystemeCLUSTER - Windows-Clusterinformationen

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Syntax

```
>>-CONsole---------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
query systeminfo dsmoptfile errorlog -console
```

Linux-BetriebssystemeWindows-Betriebssysteme

Createnewbase

Die Option createnewbase erstellt eine Basismomentaufnahme und verwendet sie als Quelle für die Ausführung einer vollständigen Teilsicherung.

Einige Dateien werden möglicherweise nicht gesichert, wenn der Befehl zur Ausführung einer Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausgeführt wird. Werden die Dateien übersprungen, können Sie mit der Option createnewbase eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausführen, um diese Dateien zu sichern. Der Abschnitt Snapdiff enthält eine Liste mit Gründen, die angeben, warum eine Datei möglicherweise nicht gesichert wird, wenn der Befehl zur Ausführung einer Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausgeführt wird.

Ein Grund, dass eine Datei während der Sicherungsverarbeitung übersprungen werden kann, liegt darin, dass der Dateiname von NetApp Data ONTAP nicht unterstützt wird. NetApp Data ONTAP-Version 8.0 und Versionen vor Version 7.3.3 unterstützen nur Dateinamen, die sich innerhalb des 7-Bit-ASCII-Zeichensatzes befinden. NetApp Data ONTAP-Version 7.3.3 und Versionen höher als 8.0.0 unterstützen Unicode-Dateinamen. Wenn Sie für NetApp Data ONTAP ein Upgrade von einer Version, die keine Unicode-Dateinamen unterstützt, auf eine Version durchgeführt haben, die Unicode-Dateinamen unterstützt, führen Sie eine vollständige Teilsicherung mit der Option createnewbase=migrate aus.

Unterstützte Clients

Diese Option ist für die folgenden Clients gültig:

- Windows-BetriebssystemeAlle Windows-Clients
- Linux-BetriebssystemeLinux x86_64-Clients

Geben Sie die Option createnewbase in der Befehlszeile ein. Geben Sie diese Option mit der Option snapdiff an.

Syntax

```
                  .-No------.
>>-Createnewbase--+---------+---------------------------------><
                  +-Yes-----+
                  +-IGNore--+
                  '-MIGRate-'
```

Parameter

No
: Gibt an, dass eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausgeführt wird. Wenn der Client für Sichern/Archivieren feststellt, dass der NetApp Data ONTAP-Dateiserver von einer Version, die keine Unicode-Dateinamen unterstützt, auf einen Dateiserver migriert wurde, der Unicode-Dateinamen unterstützt, wird eine Warnung im Fehlerprotokoll und im IBM Spectrum Protect-Serveraktivitätenprotokoll aufgezeichnet. Die Warnung gibt an, dass eine vollständige Teilsicherung ausgeführt werden muss, und protokolliert den Rückkehrcode 8, auch wenn die Operation erfolgreich ausgeführt wurde.
Dieser Parameter ist der Standardwert.

Yes
: Gibt an, dass eine vollständige Teilsicherung ausgeführt wird, indem eine neue Basismomentaufnahme erstellt und diese für die Ausführung einer scanbasierten Teilsicherung verwendet wird. Verwenden Sie diese Option, um alle Dateiänderungen zu sichern, die von der Momentaufnahmedifferenz-API möglicherweise nicht festgestellt wurden.
Wird die Operation erfolgreich beendet, endet der Befehl mit dem Rückkehrcode 0.
Geben Sie die Option createnewbase=yes nicht für einen Zeitplan an, mit dem eine tägliche Momentaufnahmedifferenzsicherung ausgeführt wird. Erstellen Sie stattdessen einen separaten monatlichen Zeitplan, der über die Option createnewbase=yes verfügt.

IGNore
: Gibt an, dass eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausgeführt wird, wenn der Client für Sichern/Archivieren feststellt, dass für den NetApp Data ONTAP-Dateiserver ein Upgrade zur Unterstützung von Unicode-Dateinamen durchgeführt wurde.
Die Option ignore unterscheidet sich vom Parameter no, da mit der Option ignore die Warnung unterdrückt wird. Stattdessen wird im Fehlerprotokoll und im IBM Spectrum Protect-Aktivitätenprotokoll eine Informationsnachricht aufgezeichnet, die angibt, dass eine vollständige Teilsicherung ausgeführt werden soll.
Wird der Befehl erfolgreich beendet, wird der Code 0 zurückgegeben.
Verwenden Sie die Option ignore, wenn Sie für den NetApp Data ONTAP-Dateiserver ein Upgrade zur Unterstützung von Unicode durchgeführt, aber noch keine vollständige Teilsicherung ausgeführt haben. Diese Option wird nur verwendet, wenn der Client für Sichern/Archivieren festgestellt hat, dass der Dateiserver migriert und noch keine vollständige Teilsicherung ausgeführt wurde. Zu allen anderen Zeiten wird die Option ignoriert.

MIGRate
: Gibt an, dass eine Basismomentaufnahme erstellt und eine scanbasierte Teilsicherung ausgeführt wird, wenn für den NetApp Data ONTAP-Dateiserver ein Upgrade auf eine Version durchgeführt wurde, die Unicode-Dateinamen unterstützt. Die Option migrate unterscheidet sich von der Option yes, da die Option migrate eine Basismomentaufnahme nur erstellt, wenn der Client erkennt, dass die Version des NetApp Data ONTAP-Dateiservers aktualisiert wurde. Mit der Option yes wird bei jeder Ausführung des Befehls eine Basismomentaufnahme erstellt.
Nach der Ausführung der Teilsicherung werden keine zusätzlichen migrationsbezogenen Nachrichten im Fehlerprotokoll oder im Aktivitätenprotokoll des IBM Spectrum Protect-Servers aufgezeichnet. Wird die Operation ausgeführt, wird der Befehl mit dem

Rückkehrcode 0 beendet.
Verwenden Sie die Option migrate, wenn Sie für den NetApp Data ONTAP-Dateiserver ein Upgrade zur Unterstützung von Unicode durchgeführt, aber noch keine vollständige Teilsicherung ausgeführt haben. Die Option migrate wird ignoriert, wenn für den NetApp Data ONTAP-Dateiserver kein Upgrade durchgeführt wurde.

Beispiele

Befehlszeile:

```
dsmc incremental -snapdiff -createnewbase=yes /net/home1
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Datacenter

Gibt die Zielposition des Datencenters an, das die zurückgeschriebenen Maschinendaten enthalten soll.

Verwenden Sie diese Option in Befehlen restore vm.

Werden Ordner innerhalb des Virtual Center verwendet, um Datencenter zu organisieren, muss der Ordnername in die Datencenterspezifikation (durch einen Schrägstrich getrennt) eingeschlossen werden.

Erfolgt die Zurückschreibung über einen ESX-Server anstelle eines Virtual Center, sollte die Option '-datacenter=ha-datacenter' verwendet werden.

Die Standardzielposition ist das Datencenter, in dem die virtuelle Maschine zum Zeitpunkt der Sicherung gespeichert wurde.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Beispiele

Eine virtuelle Maschine in das Datencenter 'USEast' zurückschreiben, das sich unter einem Ordner mit dem Namen 'Production' im Virtual Center befindet.

```
dsmc restore vm my_vm -datacenter=Production/USEast
```

Die Sicherung einer virtuellen Maschine, die im Virtual Center erstellt wurde, unter Verwendung eines ESX-Servers zurückschreiben.

```
restore vm my_vm -datacenter=ha-datacenter
```

Die virtuelle Maschine in das Datencenter 'USWest' zurückschreiben.

```
restore vm my_vm -datacenter=USWEst
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Datastore

Gibt das Datenspeicherziel an, das während der VMware-Zurückschreibungsoperation verwendet werden soll.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Beispiel

Die virtuelle Maschine in einen Datenspeicher mit dem Namen `ds8k_prod1` zurückschreiben:

```
restore vm my_vm -datastore=ds8k_prod1
```

Dateformat

Mit der Option dateformat wird das Format angegeben, das für die Anzeige oder Eingabe von Datumsangaben verwendet werden soll.

 WindowsBetriebssystemeVerwenden Sie diese Option, wenn Sie das standardmäßige Datumsformat für die Sprache des von Ihnen verwendeten Nachrichtenrepositorys ändern wollen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme
Der Client für Sichern/Archivieren und der Verwaltungsclient erhalten standardmäßig Formatinformationen aus der Ländereinstellungsdefinition, die beim Starten des Clients aktiv ist. Ausführliche Informationen zur Definition der länderspezifischen Angaben können der Dokumentation auf dem lokalen System entnommen werden.

Anmerkung:

1. Die Option dateformat betrifft nicht den Web-Client. Der Web-Client verwendet das Datumsformat der Ländereinstellung, die im Browser aktiv ist. Ist im Browser eine Ländereinstellung aktiv, die nicht unterstützt wird, verwendet der Web-Client das Datumsformat für amerikanisches Englisch.
2. Wenn Sie das Datumsformat ändern und mit der Option schedlogretention das Planungsprotokoll bereinigen, entfernt der Client während der Protokollbereinigung alle Einträge im Planungsprotokoll mit einem anderen Datumsformat. Wenn Sie das Datumsformat ändern und das Fehlerprotokoll mit der Option errorlogretention bereinigen, entfernt der Client während der Protokollbereinigung alle Einträge im Fehlerprotokoll mit einem anderen Datumsformat. Bei einer Änderung des Datumsformats müssen das Planungs- und das Fehlerprotokoll kopiert werden, wenn Protokolleinträge mit einem anderen Datumsformat aufbewahrt werden sollen.

Sie können die Option dateformat mit den folgenden Befehlen verwenden.

- delete archive
- delete backup
- expire
- query archive
- Windows-Betriebssystemequery asr
- query backup
- query filespace
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemequery image
- Windows-Betriebssystemequery image
- Windows-Betriebssystemequery systemstate
- restore
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemerestore image
- Windows-Betriebssystemerestore image
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemerestore nas
- Windows-Betriebssystemerestore nas
- retrieve
- Windows-Betriebssystemerestore registry
- set event

Wenn Sie die Option dateformat in einem Befehl angeben, muss sie vor den Optionen fromdate, pitdate und todate stehen.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Regionale Einstellungen in der Dropdown-Liste Datumsformat im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Regionale Einstellungen in der Dropdown-Liste Datumsformat im Profileditor definieren.

Syntax

```
>>-DATEformat-- --Formatnummer---------------------------------><
```

Parameter

Formatnummer
Zeigt das Datum in einem der folgenden Formate an. Die Nummer für das Datumsformat auswählen, das verwendet werden soll:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme0
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDas durch die Ländereinstellung festgelegte Datumsformat verwenden (gilt nicht für Mac OS X).

AIX-BetriebssystemeOracle Solaris-BetriebssystemeFür AIX und Solaris: Dies ist der Standardwert, wenn das durch die Ländereinstellung festgelegte Datumsformat aus Ziffern und Trennzeichen besteht.

1
MM/TT/JJJJ

AIX-BetriebssystemeOracle Solaris-BetriebssystemeFür AIX und Solaris: Dies ist der Standardwert, wenn das durch die Ländereinstellung festgelegte Datumsformat nicht aus Ziffern und Trennzeichen besteht.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeDies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

- Amerikanisches Englisch
- Traditionelles Chinesisch
- Koreanisch

2
TT-MM-JJJJ

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeDies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

- Brasilianisches Portugiesisch
- Italienisch

3
JJJJ-MM-TT

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeDies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

- Japanisch
- Vereinfachtes Chinesisch
- Polnisch

4
TT.MM.JJJJ

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeDies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

- Deutsch
- Französisch
- Spanisch
- Tschechisch
- Russisch

5
JJJJ.MM.TT

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeDies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

- Ungarisch

6
JJJJ/MM/TT

7
TT/MM/JJJJ

Beispiele

Optionsdatei:
dateformat 3
Befehlszeile:
-date=3

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Weitere Hinweise zur Angabe von Datums- und Zeitformaten

Das Datums- oder Zeitformat, das Sie mit dieser Option angeben, muss verwendet werden, wenn Optionen verwendet werden, deren Eingabe aus Datums- und Zeitangaben besteht. Beispiele sind: totime, fromtime, todate, fromdate und pittime.

Wenn Sie beispielsweise die Option timeformat als `TIMEFORMAT 4` angeben, muss der Wert, den Sie für die Option fromtime oder totime angeben, als Zeit angegeben werden, wie z. B. `12:24:00pm`. Die Angabe `13:24:00` wäre nicht gültig, da `TIMEFORMAT 4` als Angabe für die Stunde eine ganze Zahl, die kleiner-gleich 12 ist, erfordert. Wenn in einer Option für die Stunde Werte bis zu 24 angegeben und Kommas als Trennzeichen verwendet werden sollen, müssen Sie `TIMEFORMAT 2` angeben.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-Betriebssysteme

Datums- und Zeitformate in der Konfigurationsdatei für die Systemländereinstellung konfigurieren

Sie können Datums- und Zeitformate angeben, indem Sie diese in der Ländereinstellungsdatei des Systems konfigurieren. Wenn Sie Datums- und Zeitformate in der Ländereinstellungsdatei angeben, müssen diese mithilfe einer Untermenge von Formatkennungen definiert werden, die Zahlen erstellen und von der Funktion `strftime()` der Programmiersprache C unterstützt werden. Sie können Datums- und Zeitformate in den Konfigurationseinstellungen für Ihre Ländereinstellung mithilfe der folgenden Kennungen definieren.

Datumskennungen

- `%Y` - das Jahr, angegeben mit 4 Ziffern, z. B. 2011
- `%y` - das Jahr, Angabe nur der letzten beiden Ziffern, z. B. 11 (nicht 2011)
- `%m` - der Monat, angegeben als Dezimalzahl (1-12)
- `%d` - der Tag des Monats (1-31)

In den Datumskennungen können Sie nur eine einzige Jahreskennung angeben. Sie dürfen `%Y` und `%y` nicht gleichzeitig angeben. Der Modifikator E (Großbuchstabe E) kann vor Datumskennungen stehen, um das Alternativformat der Ländereinstellung für das Jahr, den Monat oder den Tag zu erstellen. Wenn kein Alternativformat vorhanden ist, wird der Modifikator E ignoriert. Trennen Sie die Kennungen durch ein einzelnes 7-Bit-ASCII-Zeichen voneinander. Häufig verwendete Trennzeichen umfassen Doppelpunkte (:), Kommas (,), Punkte (.), Bindestriche (-) und Schrägstriche (/). Sie dürfen keine Mehrbytezeichen als Trennzeichen verwenden.

Zeitkennungen

- `%H` - die Stunde, angegeben im 24-Stunden-Format (00-23)
- `%I` - die Stunde, angegeben im 12-Stunden-Format (00-12)
- `%M` - die Minuten nach der Stunde (00-59)
- `%S` - die Sekunden nach der Minute (00-59)
- `%p` - fügt den Anzeiger AM (vor 12 Uhr mittags) oder PM (nach 12 Uhr mittags) ein.

In den Zeitkennungen können Sie nur eine einzige Stundenkennung angeben. Sie dürfen `%I` und `%H` nicht gleichzeitig angeben.

Der Modifikator O (Großbuchstabe O) kann vor Zeitkennungen stehen, um das Alternativformat der Ländereinstellung für die Stunde, die Minuten oder die Sekunden zu erstellen. Der Modifikator O darf nicht vor der Kennung `%p` stehen. Trennen Sie die Kennungen durch ein einzelnes 7-Bit-ASCII-Zeichen voneinander. Häufig verwendete Trennzeichen umfassen Doppelpunkte (:), Kommas (,) oder Punkte (.). Sie dürfen keine Mehrbytezeichen als Trennzeichen verwenden. Zwischen der Kennung `%p` und dem Trennzeichen, das vor oder hinter der Kennung steht, dürfen Sie kein Trennzeichen angeben.

Beispiele für in den Ländereinstellungen konfigurierte Zeitformate

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeUm ein bestimmtes Zeitformat zu definieren, editieren Sie die Konfigurationsdatei für die Ländereinstellung und ändern Sie die Zeile `t_fmt` gemäß den Anforderungen. Das ausgewählte Zeitformat gilt sowohl für die Ausgabe als auch für die Eingabe. Nachdem die Konfigurationsdatei für die Ländereinstellung editiert wurde, muss der Befehl localedef ausgeführt werden, um die endgültige Ländereinstellungsdatei zu erstellen.

Tabelle 1. Mustereinstellungen für das Zeitformat in der Konfigurationsdatei für die Ländereinstellung (Zeile t_fmt)

Beispiel	**Ergebnis**
"%H:%M:%S"	Zeigt die Zeit im Format *hh:mm:ss* an; *hh* liegt im Bereich von 0 bis 23.
"%H,%M,%S"	Zeigt die Zeit im Format *hh,mm,ss* an; *hh* liegt im Bereich von 0 bis 23.
"%I,%M,13p"	Zeigt die Zeit im Format *hh,mm,ssA/P* an, wobei *hh* (Stunde) den Bereich 1 bis 12 aufweist und *A/P* die Abkürzung für ante-meridian (vormittags, AM in Englisch) oder post-meridian (nachmittags, PM in Englisch) ist.

Beispiele für in den Ländereinstellungen konfigurierte Datumsformate

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeUm ein bestimmtes Datumsformat zu definieren, editieren Sie die Konfigurationsdatei und ändern Sie die Zeile `d_fmt` gemäß Ihren Anforderungen. Das ausgewählte Datumsformat gilt sowohl für die Ausgabe als auch für die Eingabe.

Tabelle 2. Mustereinstellungen für das Datumsformat in der

Konfigurationsdatei für die Ländereinstellung (Zeile d_fmt)

Beispiel	Ergebnis
"%m/%d/%y"	Zeigt das Datum im Format MM/TT/JJ an.
"%d.%m.%Y"	Zeigt das Datum im Format TT.MM.JJJJ an.

Dedupcachepath

Verwenden Sie die Option dedupcachepath, um die Position anzugeben, an der die Cachedatenbank für die clientseitige Datendeduplizierung erstellt wird.

Diese Option wird ignoriert, wenn die Option enablededupcache=no während der Sicherung- oder Archivierungsverarbeitung definiert wird.

Unterstützte Clients

Diese Option ist für alle Client gültig. Diese Option ist auch für die IBM Spectrum Protect-API gültig.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeFügen Sie diese Option in die Systemoptionsdatei (dsm.sys) ein. Sie können diese Option im Feld Position des Deduplizierungscache des Profileditors definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option im Textfeld Deduplizierung > Position des Deduplizierungscache des Profileditors definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax

```
>>-DEDUPCACHEPath--Pfad----------------------------------------><
```

Parameter

Pfad
: Gibt die Position an, an der die Cachedatenbank für die clientseitige Datendeduplizierung erstellt wird, wenn die Option enablededupcache auf yes gesetzt wird. Die Standardposition für die Erstellung der Cachedatei für die Datendeduplizierung ist das Installationsverzeichnis des Clients für Sichern/Archivieren oder der API.

  Windows-BetriebssystemeIm UNC-Format (Universal Naming Convention) muss der Pfad einen Laufwerkbuchstaben enthalten. In dem folgenden Beispiel für das UNC-Format enthält der Pfad den Laufwerkbuchstaben D$: \\computer7\D$\stgmgr\dedupecache.

Beispiele

Optionsdatei:
: AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssystemededupcachepath /volumes/temp
  Windows-Betriebssystemededupcachepath c:\logs\dedup\

Befehlszeile:
: Nicht zutreffend.

Zugehörige Verweise:
Enablededupcache

Dedupcachesize

Verwenden Sie die Option dedupcachesize, um die maximale Größe der Cachedatei für die Datendeduplizierung festzulegen. Wenn die Cachedatei ihre maximale Größe erreicht, wird der Inhalt des Cache gelöscht und neue Einträge werden hinzugefügt.

Unterstützte Clients

Diese Option ist für alle Client gültig. Diese Option ist auch für die IBM Spectrum Protect-API gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Systemoptionsdatei (dsm.sys) ein. Sie können diese Option im Feld Deduplizierung > Deduplizierungscache > Maximale Größe des Profileditors definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option im Feld Deduplizierung > Deduplizierungscache > Maximale Größe des Profileditors definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax

```
>>-DEDUPCACHESize--Größe des Deduplizierungscache--------------><
```

Parameter

Größe des Deduplizierungscache
: Gibt die maximale Größe der Cachedatei für die Datendeduplizierung in Megabyte an. Der Wertebereich ist 1 - 2048; der Standardwert ist 256.

Beispiele

Optionsdatei:
: dedupcachesize 1024

Befehlszeile:
: Nicht zutreffend.

Zugehörige Verweise:
Deduplication

Deduplication

Verwenden Sie die Option deduplication, um anzugeben, ob die clientseitige Entfernung redundanter Daten bei der Übertragung von Daten an IBM Spectrum Protect während der Sicherungs- und Archivierungsverarbeitung aktiviert sein soll.

Die Datendeduplizierung ist inaktiviert, wenn die Option enablelanfree festgelegt ist. Vom Client für Sichern/Archivieren verschlüsselte Dateien sind von der clientseitigen Datendeduplizierung ausgeschlossen. Dateien aus verschlüsselten Dateisystemen sind ebenfalls ausgeschlossen.

Für die Unterstützung der clientseitigen Datendeduplizierung müssen die folgenden Bedingungen erfüllt sein:

- Die clientseitige Datendeduplizierung für den Knoten ist auf dem Server aktiviert.
- Der Zielspeicherpool für die Daten muss ein Speicherpool sein, der für die Datendeduplizierung aktiviert ist. Der Speicherpool muss über den Einheitentyp "Datei" verfügen.
- Eine Datei kann von der clientseitigen Datendeduplizierungsverarbeitung ausgeschlossen werden (standardmäßig sind alle Dateien eingeschlossen).
- Der Server kann die maximale Transaktionsgröße für die Datendeduplizierung durch Definieren der Option CLIENTDEDUPTXNLIMIT auf dem Server begrenzen. Weitere Informationen zu der Option finden Sie in der IBM Spectrum Protect-Serverdokumentation.
- Die Datei muss größer als 2 KB sein.

Unterstützte Clients

Diese Option ist für alle Clients gültig und kann auch von der IBM Spectrum Protect-API verwendet werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option definieren, indem Sie das Kontrollkästchen Deduplizierung > Deduplizierung aktivieren des Profileditors auswählen. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option definieren, indem Sie das Kontrollkästchen Deduplizierung > Deduplizierung aktivieren des Profileditors auswählen. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax

```
                .-No--.
>>-DEDUPLication--+-----+--------------------------------------><
```

```
'-Yes-'
```

Parameter

No
: Gibt an, dass Sie die clientseitige Datendeduplizierung für die Sicherungs- und Archivierungsverarbeitung nicht aktivieren wollen. 'No' ist der Standardwert.

Yes
: Gibt an, dass Sie die clientseitige Datendeduplizierung für die Sicherungs- und Archivierungsverarbeitung aktivieren wollen.

Beispiele

Optionsdatei:
: deduplication yes

Befehlszeile:
: -deduplication=yes

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Verweise:
Einschlussoptionen
Ausschlussoptionen
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

Defaultserver

Verwenden Sie die Option defaultserver, um den Namen des IBM Spectrum Protect-Servers anzugeben, zu dem zwecks Sicherungs-/Archivierungsservices der Kontakt hergestellt werden soll, falls mehrere Server in der Datei dsm.sys definiert sind.

Standardmäßig stellt die Sicherung/Archivierung den Kontakt zu dem Server her, der in der ersten Zeilengruppe in der Datei dsm.sys definiert ist. Diese Option wird nur verwendet, wenn die Option servername nicht in der Clientbenutzeroptionsdatei (dsm.opt) angegeben ist.

Wenn der Client für die hierarchische Speicherverwaltung (HSM-Client) auf Ihrer Workstation installiert ist und kein Umlagerungsserver mit der Option migrateserver angegeben wird, können Sie mit dieser Option den Server angeben, in den Dateien umgelagert werden sollen. Weitere Informationen enthält die Produktdokumentation zu IBM Spectrum Protect for Space Management im IBM Knowledge Center unter http://www.ibm.com/support/knowledgecenter/SSERBH/welcome.

Unterstützte Clients

Diese Option ist für alle UNIX-Clients gültig.

Optionsdatei

Fügen Sie diese Option *am Anfang* der Datei dsm.sys *vor* allen Serverzeilengruppen ein.

Syntax

```
>>-DEFAULTServer-- --Servername--------------------------------><
```

Parameter

Servername
: Gibt den Namen des Standardservers an, auf dem Sie Dateien sichern oder archivieren. Der Server, auf den Dateien von Ihren lokalen Dateisystemen umgelagert werden, kann mit dieser Option ebenfalls angegeben werden.

Beispiele

Optionsdatei:
: defaults server_a

Befehlszeile:
: Nicht zutreffend.

Deletefiles

Verwenden Sie die Option deletefiles im Befehl archive, um Dateien von Ihrer Workstation zu löschen, nachdem Sie sie archiviert haben.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeDiese Option kann auch im Befehl restore image und mit der Option incremental verwendet werden, um Dateien aus dem zurückgeschriebenen Image zu löschen, falls sie nach der Erstellung des Image gelöscht wurden. Das Löschen von Dateien wird ordnungsgemäß ausgeführt, wenn die Sicherungskopiengruppe des IBM Spectrum Protect-Servers über genügend Versionen für vorhandene und gelöschte Dateien verfügt.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-DELetefiles-----------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

Mac OS X-Betriebssysteme

```
dsmc archive "/Users/dgordon/Documents/*.c" -deletefiles
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
dsmc archive "/home/foo/*.c" -deletefiles
dsmc restore image /local/data -incremental -deletefiles
```

Windows-Betriebssysteme

```
dsmc archive c:\foo\*.c -deletefiles
dsmc rest image c: -incre -deletefiles
```

Description

Die Option description ordnet Dateien beim Ausführen von Archivieren, Archivierung löschen, Abrufen, Archivierung abfragen oder Sicherungssatz abfragen eine Beschreibung zu oder gibt eine Beschreibung für diese Dateien an.

Soll beispielsweise die Datei budget.jan archiviert und ihr die Beschreibung "2002 Budget für Proj 1" zugeordnet werden, geben Sie Folgendes ein: AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc archive -des="2003 Budget für Proj 1" /home/plan/
proj1/budget.jan
```

Windows-Betriebssysteme

```
dsmc archive -des="2003 Budget für Proj 1" c:\plan\proj1\
budget.jan
```

Anmerkung:

1. Die maximale Länge einer Beschreibung ist 254 Zeichen.
2. Schließen Sie den Wert in Anführungszeichen (" ") ein, wenn der von Ihnen eingegebene Optionswert ein Leerzeichen enthält.

Die Option description kann in den folgenden Befehlen verwendet werden:

- archive
- delete archive
- query archive
- query backupset
- retrieve

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-DEScription = - --Beschreibung------------------------------><
```

Parameter

Beschreibung

Ordnet der Datei, die archiviert wird, eine Beschreibung zu. Wenn Sie keine Beschreibung im Befehl archive angeben, lautet der Standardwert Archivierungsdatum:x; hierbei gibt x das aktuelle Systemdatum an. Bitte beachten Sie, dass das Datum immer 10 Zeichen lang ist. Wenn Ihr Datumsformat nur zwei Stellen für das Jahr verwendet, sind am Ende des Datums zwei Leerzeichen. Beispiel: Eine Standardbeschreibung mit einer vierstelligen Jahreszahl könnte so aussehen: "Archivierungdatum: 03.05.2002". Dieselbe Standardbeschreibung mit einer zweistelligen Jahreszahl würde so aussehen: "`Archivierungdatum: 03.05.02 `" (beachten Sie die beiden Leerzeichen am Ende). Wenn Sie Dateien mit der zweistelligen Jahreszahlbeschreibung abrufen, können Sie die Zeichenfolge der Option -description auf eine der beiden folgenden Arten eingeben:

```
-description="Archivierungsdatum: 03.05.02  "
 oder
-description="Archivierungsdatum: 03.05.02*"
```

Werden mit dem Befehl archive mehrere Dateien archiviert, gilt die eingegebene Beschreibung für jede Datei. Soll beispielsweise eine Dateigruppe archiviert und jeder Datei dieselbe Beschreibung, *Projekt X*, zugeordnet werden, Folgendes eingeben:

```
dsmc archive -description="Projekt X" "/Users/van/Documents/*.x"
```




```
   dsmc archive -description="Projekt X" "/home/allproj/.*"
```

```
   dsmc archive -description="Projekt X" c:\allproj\*.x
```

Mithilfe der Beschreibung können dann alle Dateien abgerufen werden.

Beispiele

Befehlszeile:

```
dsmc archive "/Users/van/Documents/*.prj" -des="2003 Budget für Proj 1"
```




```
dsmc archive "/home/foo/*.prj" -des="2003 Budget für Proj 1"
dsmc query backupset -loc=server -descr="Mein Laptop"
```

```
dsmc archive -des="2003 Budget für Proj 1" c:\foo\ *.prj
```

Detail

Verwenden Sie die Option detail, um abhängig vom Befehl, mit dem sie verwendet wird, Angaben zu Verwaltungsklasse, Dateibereich, Sicherung und Archivierung sowie zusätzliche Informationen anzuzeigen.

Verwenden Sie die Option detail im Befehl query mgmtclass, um ausführliche Informationen zu allen Verwaltungsklassen in Ihrer aktiven Maßnahmengruppe anzuzeigen. Wird die Option detail nicht verwendet, werden nur der Name der Verwaltungsklasse und eine Kurzbeschreibung auf dem Bildschirm angezeigt. Wird die Option detail angegeben, werden Informationen zu Attributen in jeder Kopiengruppe in allen Verwaltungsklassen auf dem Bildschirm angezeigt. Eine Verwaltungsklasse kann eine Sicherungskopiengruppe und/oder eine Archivierungskopiengruppe oder keine Kopiengruppe enthalten.






Ein Unicode-fähiger Dateibereich wird unter Umständen nicht korrekt angezeigt, wenn der Server den Unicode-Namen nicht anzeigen kann. In diesem Fall müssen Sie die Dateibereichskennung (fsID) des Dateibereichs verwenden, um diese Dateibereiche auf dem Server zu identifizieren. Verwenden Sie die Option detail in den Befehlen delete filespace und query filespace, um die FSID eines Dateibereichs festzustellen. Die FSID wird auch im Dateiinformationsdialog der GUIs des Clients für Sichern/Archivieren und des Web-Clients angezeigt.

Verwenden Sie die Option detail in den Befehlen query backup und query archive, um die folgenden Attribute für die von Ihnen angegebene Datei anzuzeigen:

- Datum der letzten Änderung
- Datum des letzten Zugriffs

- Komprimierung
- Verschlüsselungstyp
- Clientseitige Datendeduplizierung
- Ob der HSM-Client die Datei umgelagert oder vorumgelagert hat

Windows-BetriebssystemeVerwenden Sie die Option detail im Befehl query adobjects, um ausführliche Informationen zu Active Directory-Objekten einschließlich aller ihrer Attribute anzuzeigen.

Windows-BetriebssystemeVerwenden Sie die Option detail im Befehl query adobjects, um ausführliche Informationen zu Active Directory-Objekten einschließlich aller ihrer Attribute anzuzeigen.

Linux-BetriebssystemeWindows-BetriebssystemeVerwenden Sie die Option detail im Befehl query vm, um folgende Statistikdaten anzuzeigen:

- Die durchschnittliche Anzahl IBM Spectrum Protect-Objekte, die für die Beschreibung eines einzelnen Megablocks benötigt wird. Dabei werden alle Megablöcke in einer Sicherung berücksichtigt.
- Die durchschnittliche Anzahl IBM Spectrum Protect-Objekte, die für die Beschreibung eines einzelnen Megablocks für alle Megablöcke in einem Dateibereich benötigt wird.
- Das Verhältnis des von der Überwachung geänderter Blöcke dokumentierten Datenvolumens im Vergleich zu dem Datenvolumen, das in einer bestimmten Sicherung tatsächlich gesichert wurde.
- Das Verhältnis des von der Überwachung geänderter Blöcke dokumentierten Datenvolumens im Vergleich zu dem Datenvolumen, das bei allen Sicherungen in diesem Dateibereich tatsächlich gesichert wurde.
- Die Anzahl der Sicherungen, die seit der Erstellung der letzten Gesamtsicherung von den Produktionsplatten erstellt wurden.

Die für query vm zurückgegebenen Werte können Ihnen bei der Optimierung der heuristischen Verfahren helfen (siehe die Optionen Mbobjrefreshthresh und Mbpctrefreshthresh), um den Werteauslöser für die Aktualisierung von Megablöcken zu optimieren.

Verwenden Sie die Option detail in den folgenden Befehlen:

- delete filespace
- incremental
- Windows-Betriebssystemequery adobjects
- query archive
- query backup
- query filespace
- query inclexcl
- query mgmtclass
- Windows-Betriebssystemequery systemstate
- Linux-BetriebssystemeWindows-Betriebssystemequery vm

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option wird nicht in der Clientoptionsdatei definiert. Sie fügen sie in die Befehlszeile ein, wenn Sie einen der Befehle eingeben, die diese Option unterstützen. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-DETail-----------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc query mgmtclass -detail
```

```
dsmc query filespace -detail
```

```
dsmc query backup file1 -detail
```

Windows-Betriebssysteme

```
dsmc query systemstate -detail
```

Linux-BetriebssystemeWindows-Betriebssysteme

```
dsmc query vm -detail
```

Linux-BetriebssystemeWindows-Betriebssysteme

Diffsnapshot

Die Option diffsnapshot legt fest, ob der Client für Sichern/Archivieren die Differenzmomentaufnahme erstellt, wenn eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausgeführt wird.

Wird die Differenzmomentaufnahme nicht vom Client erstellt, wird die letzte auf dem Datenträger gefundene Momentaufnahme als Differenzmomentaufnahme und als Quelle für die Sicherungsoperation verwendet.

Der Standardwert ist die Erstellung der Differenzmomentaufnahme. Diese Option wird ignoriert, wenn die Option snapdiff zum ersten Mal verwendet wird. Bei der ersten Verwendung der Option snapdiff für einen Datenträger muss eine Momentaufnahme erstellt und als Quelle für eine vollständige Teilsicherung verwendet werden. Vom Client für Sichern/Archivieren erstellte Momentaufnahmen werden nach Beendigung der nächsten Teilsicherung unter Verwendung der Momentaufnahmedifferenz vom Client gelöscht.

Linux-BetriebssystemeMomentaufnahmen können mit dem Network Appliance FilerView-Tool erstellt werden. Verwenden Sie den Parameter latest, wenn der Client die neueste Momentaufnahme verwenden soll, die mit dieser oder einer anderen Methode erstellt wurde. Momentaufnahmen, die mit Methoden außerhalb von IBM Spectrum Protect erstellt werden, werden nie vom Client gelöscht.

Windows-BetriebssystemeMomentaufnahmen können mit dem Network Appliance FilerView-Tool erstellt werden. Verwenden Sie den Parameter latest, wenn der Client die neueste Momentaufnahme verwenden soll, die erstellt wurde. Namen von Momentaufnahmen, die sich nur durch die Groß-/Kleinschreibung unterscheiden, funktionieren nicht ordnungsgemäß mit der Option snapdiff, unabhängig davon, mit welcher Methode benannte Momentaufnahmen erstellt werden. Vom Client erstellte Momentaufnahmen haben nicht das Problem mit der Groß-/Kleinschreibung. Momentaufnahmen, die mit Methoden außerhalb von IBM Spectrum Protect erstellt werden, werden nie vom Client gelöscht.

Unterstützte Clients

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

Syntax

```
                .-create-.
>>-DIFFSNAPSHOT--+--------+-----------------------------------><
                '-latest-'
```

Parameter

create
: Gibt an, dass Sie eine neue, persistente Momentaufnahme erstellen wollen, die als Quellenmomentaufnahme verwendet wird. Dies ist der Standardwert.

latest
: Gibt an, dass Sie die neueste Momentaufnahme, die auf dem Dateiserver gefunden wird, als Quellenmomentaufnahme verwenden wollen.

Beispiele

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeEine Teilsicherung unter Verwendung der Momentaufnahmedifferenz für das über NFS-Mount angehängte Dateisystem `/vol/vol1` ausführen, das sich auf dem Dateiserver `homestore.example.com` befindet. Dabei ist `/net/home1` der Mountpunkt von `/vol/vol1`.

Linux-Betriebssysteme
```
incremental -snapdiff -diffsnapshot=latest /net/home1
```

Der Wert latest der Option -diffsnapshot bedeutet, dass bei der Operation die letzte Momentaufnahme (die aktive Momentaufnahme) verwendet wird.

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeEine Teilsicherung mit der Option snapdiff auf der Basis einer Momentaufnahme ausführen, die von dem gemeinsam genutzten Netzbereich `//homestore.example.com/vol/vol1` erstellt wurde, der als Laufwerk `H:` angehängt ist. Dabei ist `homestore.example.com` ein Dateiserver.

Windows-Betriebssysteme
```
incremental -snapdiff H:
```

Windows-BetriebssystemeEine Teilsicherung mit der Option snapdiff auf der Basis einer Momentaufnahme ausführen, die von dem gemeinsam genutzten Netzbereich `//homestore.example.com/vol/vol1` erstellt wurde, der als Laufwerk `H:` angehängt ist. Dabei ist `homestore.example.com` ein Dateiserver.Der Wert `LATEST` der Option -diffsnapshot bedeutet, dass bei der Operation die letzte Momentaufnahme (die aktive Momentaufnahme) für Datenträger `H:` verwendet wird.

Windows-Betriebssysteme`incremental -snapdiff H: -diffsnapshot=latest`

Linux-Betriebssysteme Windows-Betriebssysteme

Diffsnapshotname

Mit der Option diffsnapshotname können Sie angeben, welche Differenzmomentaufnahme auf dem Datenträger des Ziel-Dateiservers während einer Momentaufnahmedifferenzsicherung verwendet werden soll. Diese Option wird nur angegeben, wenn Sie auch diffsnapshot=latest angeben.

Wird diese Option nicht angegeben, wird bei der Angabe von diffsnapshot=latest die jüngste vorhandene Momentaufnahme auf dem Dateiserverdatenträger ausgewählt und als Differenzmomentaufnahme verwendet.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Diese Option kann in der Clientoptionsdatei oder in der Befehlszeile angegeben werden.

Syntax

```
>>-DIFFSNAPSHOTName-- --Momentaufnahmename---------------------><
```

Parameter

Momentaufnahmename
Gibt den Namen einer vorhandenen Momentaufnahme an, die als Differenzmomentaufnahme verwendet werden soll.
Sie können auch ein Muster mit Platzhalterzeichen für die Auswahl einer Momentaufnahme verwenden. Gültige Platzhalterzeichen sind:

*
Ein Stern (*) entspricht beliebigen Zeichen.

?
Ein Fragezeichen (?) entspricht einem einzelnen Zeichen.

Die jüngste Momentaufnahme, die dem Platzhaltermuster entspricht, wird als Differenzmomentaufnahme ausgewählt.

Beispiele

Optionsdatei:

```
diffsnapshotname volume_base_snap

diffsnapshotname nightly.?
```

Befehlszeile:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff
  -useexistingbase -basenameshotname="nightly.?"
  -diffsnapshot=latest -diffsnapshotname="nightly.?"
```

Zugehörige Verweise:
Useexistingbase
Basesnapshotname

Dirmc

Mit der Option dirmc wird die Verwaltungsklasse angegeben, die für Verzeichnisse verwendet werden soll.

Wenn Sie diese Option nicht für die Zuordnung zwischen einer Verwaltungsklasse und Verzeichnissen angeben, verwendet das Clientprogramm die Verwaltungsklasse in der aktiven Maßnahmengruppe Ihrer Maßnahmendomäne mit dem längsten Aufbewahrungszeitraum. Wählen Sie eine Verwaltungsklasse für einzelne Verzeichnisse aus, durch die Verzeichnisse mindestens so lange aufbewahrt werden wie die ihnen zugeordneten Dateien.

Wenn Sie eine Verwaltungsklasse mit dieser Option angeben, sind alle Verzeichnisse, die in einer Sicherungsoperation angegeben werden, an diese Verwaltungsklasse gebunden.

Die Option dirmc gibt die Verwaltungsklasse für gesicherte Verzeichnisse an; bei archivierten Verzeichnissen bleibt sie ohne Wirkung. Verwenden Sie die Option archmc im Befehl archive, um die verfügbare Verwaltungsklasse für Ihre Maßnahmendomäne anzugeben, an die Sie Ihre archivierten Verzeichnisse und Dateien binden wollen. Wenn Sie die Option archmc nicht verwenden, bindet der Server archivierte Verzeichnisse an die Standardverwaltungsklasse. Hat die Standardverwaltungsklasse keine Archivierungskopiengruppe, bindet der Server archivierte Verzeichnisse an die Verwaltungsklasse mit dem kürzesten Aufbewahrungszeitraum.

Wichtig: Nur erweiterte Attribute und ACLs werden in Speicherpools gespeichert. Die Verzeichnisinformationen über die erweiterten Attribute und ACLs hinaus verbleiben in der Datenbank. Auf Windows-Systemen belegen Verzeichnisse Speicherbereich im Speicherpool.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Sichern im Abschnitt Verzeichnis für Verwaltungsklasse im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Sichern im Abschnitt Verzeichnis für Verwaltungsklasse im Profileditor definieren.

Syntax

```
>>-DIRMc-- --Verwaltungsklassenname----------------------------><
```

Parameter

Verwaltungsklassenname
: Gibt den Namen der Verwaltungsklasse an, die Verzeichnissen zugeordnet werden soll. Der Client verwendet den von Ihnen angegebenen Verwaltungsklassennamen für alle Verzeichnisse, die Sie sichern. Wenn Sie diese Option nicht angeben, wird den Verzeichnissen vom Client die Verwaltungsklasse mit dem längsten Aufbewahrungszeitraum zugeordnet.

Beispiele

Optionsdatei:
: dirm managdir

Befehlszeile:
: Nicht zutreffend.

Dirsonly

Mit der Option dirsonly werden *nur* Verzeichnisse verarbeitet. Der Client verarbeitet keine Dateien.

Die Option dirsonly ist in den folgenden Befehlen zu verwenden:

- archive
- incremental
- query archive
- query backup
- restore
- restore backupset
- retrieve
- selective

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-DIrsonly---------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssystemedsmc query backup -dirsonly "/Users/*"

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedsmc query backup -dirsonly "*"

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssystemedsmc query backup -dirsonly c:*

Disablenqr

Die Option disablenqr gibt an, ob der Client für Sichern/Archivieren die Methode zur Zurückschreibung ohne Abfrage verwenden kann, um Dateien und Verzeichnisse vom Server zurückzuschreiben.

Wenn Sie die Option disablenqr auf no (Standardwert) setzen, kann der Client den Zurückschreibungsprozess ohne Abfrage verwenden.

Wenn Sie die Option disablenqr auf yes setzen, kann der Client nur den Standardzurückschreibungsprozess (auch als "klassische Zurückschreibung" bekannt) verwenden.

Anmerkung: Es gibt keine Option bzw. keinen Wert, mit dem angegeben werden kann, dass der Client nur die Zurückschreibungsmethode ohne Abfrage verwenden darf.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.opt ein.

Syntax

```
                .-No--.
>>-DISABLENQR--+-----+-----------------------------------------><
                '-Yes-'
```

Parameter

No
: Gibt an, dass der Client die Methode zur Zurückschreibung ohne Abfrage verwenden kann. Dies ist der Standardwert.

Yes
: Gibt an, dass der Client nur die Standardzurückschreibungsmethode verwendet. Die Methode zur Zurückschreibung ohne Abfrage ist nicht zulässig.

Beispiele

Optionsdatei:

```
disablenqr yes
```

Befehlszeile:

```
-disablenqr=yes
```

Diskbuffsize

Die Option diskbuffsize gibt die maximale Platten-E/A-Puffergröße (in Kilobyte) an, die der Client beim Lesen von Dateien verwenden kann. Die Option diskbuffsize ersetzt die Option largecommbuffers.

Windows-BetriebssystemeDie optimale Umlagerungsclientleistung beim Sichern oder Archivieren kann normalerweise erreicht werden, wenn der Wert dieser Option maximal dem Wert für das Vorauslesen von Dateien entspricht, der für das Clientdateisystem angegeben ist. Für einen größeren Puffer ist mehr Hauptspeicher erforderlich und die Leistung erhöht sich eventuell nicht.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDie optimale Umlagerungsclientleistung beim Sichern, beim Archivieren oder bei HSM kann normalerweise erreicht werden, wenn der Wert dieser Option

maximal dem Wert für das Vorauslesen von Dateien entspricht, der für das Clientdateisystem angegeben ist. Für einen größeren Puffer ist mehr Hauptspeicher erforderlich und die Leistung erhöht sich eventuell nicht.

Wichtig: Verwenden Sie die Standardeinstellung, solange die Mitarbeiter der IBM® Unterstützungsfunktion keine anderen Anweisungen erteilen.
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

```
>>-DISKBuffsize-- --Größe----------------------------------------><
```

Parameter

 Windows-BetriebssystemeGröße
 Windows-BetriebssystemeGibt die maximale Platten-E/A-Puffergröße (in Kilobyte) an, die der Client beim Lesen von Dateien verwendet. Der Wertebereich ist 16 bis 1023; Standardwert ist 32.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeGröße
 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeGibt die maximale Platten-E/A-Puffergröße (in Kilobyte) an, die der Client beim Lesen von Dateien verwendet. Der Wertebereich ist 16 bis 1023; Standardwert ist 32. Für AIX: Ist enablelanfree no festgelegt, lautet die Standardeinstellung für diskbuffsize 256.

Beispiele

Optionsdatei:
diskbuffsize 64
Befehlszeile:
Nicht zutreffend.

Diskcachelocation

Die Option diskcachelocation gibt die Position an, an der die Plattencachedatenbank erstellt wird, wenn die Option memoryefficientbackup=diskcachemethod bei einer Teilsicherung definiert ist.

Sie können die Option diskcachelocation in Ihrer Optionsdatei oder mit der Option include.fs angeben. Ist die Option diskcachelocation in der Optionsdatei vorhanden, wird ihr Wert für alle Dateisysteme verwendet, für die keine Option include.fs zusammen mit der Option diskcachelocation angegeben ist.

Der Plattencache ist eine temporäre Datei, die nach der Ausführung des Befehls incremental gelöscht wird. Verwenden Sie diese Option für die Auswahl einer der folgenden Angaben:

1. Eine Speicherposition mit mehr freiem Plattenspeicherplatz, wenn Sie bei Verwendung von memoryefficientbackup=diskcachemethod die Nachricht erhalten, dass die Plattencachedatei nicht erstellt werden kann, da nicht genügend Plattenspeicherplatz verfügbar ist.
2. Eine Speicherposition auf einem anderen physischen Datenträger, um Konkurrenzsituationen beim Plattenzugriff zu verhindern und somit die Leistung zu verbessern

Wichtig: Verwenden Sie aus Leistungsgründen kein fernes Laufwerk für diskcachelocation!

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDer tatsächlich erforderliche Plattenspeicherplatz für die Plattencachedatei, die bei Teilsicherungen des Plattencaches erstellt wird, ist von der Anzahl der Dateien und Verzeichnisse abhängig, die in die Sicherung eingeschlossen werden, sowie von der durchschnittlichen Länge der zu sichernden Dateien und Verzeichnisse. Für UNIX und Linux beträgt der Schätzwert 1 Byte pro Zeichen im Pfadnamen. Für Mac OS X beträgt der Schätzwert 4 Byte pro Zeichen im Pfadnamen. Beispiel: Es müssen 1 000 000 Dateien und Verzeichnisse gesichert werden und die durchschnittliche Pfadlänge beträgt 200 Zeichen. In diesem Fall belegt die Datenbank etwa 200 MB für UNIX- und Linux-Clients und 800 MB für Mac OS X-Clients. Ein anderes Schätzverfahren für Planungszwecke besteht darin, die Anzahl der Dateien und Verzeichnisse mit der Länge des längsten Pfads zu multiplizieren, um eine maximale Datenbankgröße zu ermitteln.

 Windows-BetriebssystemeDer tatsächlich erforderliche Plattenspeicherplatz für die Plattencachedatei, die bei Teilsicherungen des Plattencaches erstellt wird, ist von der Anzahl der Dateien und Verzeichnisse abhängig, die in die Sicherung eingeschlossen werden, sowie von

der durchschnittlichen Länge der zu sichernden Dateien und Verzeichnisse. Der Schätzwert beträgt 2 Byte pro Zeichen im Pfadnamen. Beispiel: Es müssen 1 000 000 Dateien und Verzeichnisse gesichert werden und die durchschnittliche Pfadlänge beträgt 200 Zeichen. In diesem Fall belegt die Datenbank etwa 400 MB. Ein anderes Schätzverfahren für Planungszwecke besteht darin, die Anzahl der Dateien und Verzeichnisse mit der Länge des längsten Pfads zu multiplizieren, um eine maximale Datenbankgröße zu ermitteln.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBeim Sichern eines über HSM verwalteten Dateisystems wird eine zweite Plattencachedatei für die Liste der umgelagerten Dateien erstellt. Für beide Plattencachedateien zusammen - die bei Teilsicherungen des Plattencaches erstellte Plattencachedatei und die bei Sicherungen von über HSM verwalteten Dateisystemen erstellte Plattencachedatei - können mehr als 400 MB Plattenspeicherplatz pro Million zu sichernder Dateien erforderlich sein. Die Plattencachedatei kann sehr groß werden. Auf dem Dateisystem, das für die Plattencachedatei verwendet wird, muss Unterstützung für große Dateien aktiviert sein.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein.

Syntax

```
>>-DISKCACHELocation-- --Pfad----------------------------------><
```

Parameter

Pfad
: Gibt die Position an, an der die Plattencachedatenbank erstellt wird, wenn memoryefficientbackup=diskcachemethod festgelegt ist. Standardmäßig wird die Plattencachedatei im Stammverzeichnis des Dateibereichs erstellt, der gerade verarbeitet wird.

  Windows-BetriebssystemeIm UNC-Format (Universal Naming Convention) muss der Pfad einen Laufwerkbuchstaben enthalten. In dem folgenden Beispiel für das UNC-Format enthält der Pfad den Laufwerkbuchstaben D$: \\computer7\D$\temp\diskcache.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeOptionsdatei:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
diskcachelocation /home
diskcachelocation /Volumes/hfs2
```

Windows-BetriebssystemeOptionsdatei:
Windows-Betriebssysteme

```
diskcachelocation c:\temp
diskcachelocation c:\tivoli\data
```

Befehlszeile:
: Nicht zutreffend.

Domain

Die Option domain gibt an, welche Objekte Sie bei Teilsicherungen einschließen wollen.

Domänenobjekte werden nur gesichert, wenn Sie den Befehl incremental ohne Dateispezifikation starten.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDer Client für Sichern/Archivieren verwendet den Wert von 'domain' in den folgenden Situationen, um festzustellen, welche Dateisysteme während einer Teilsicherung zu verarbeiten sind:

- Wenn Sie eine Teilsicherung mithilfe des Befehls incremental ausführen und nicht angeben, welche Dateisysteme verarbeitet werden sollen.
- Wenn Ihr IBM Spectrum Protect-Administrator einen Zeitplan für eine Teilsicherung für Sie definiert, aber nicht angibt, welche Dateisysteme verarbeitet werden sollen.
- Wenn Sie die Aktion Domäne sichern in der GUI des Clients für Sichern/Archivieren auswählen.

Windows-BetriebssystemeDer Client für Sichern/Archivieren verwendet den Wert von 'domain' in den folgenden Situationen, um festzustellen, welche Laufwerke während einer Teilsicherung zu verarbeiten sind:

- Wenn Sie eine Teilsicherung mithilfe des Befehls incremental ausführen und nicht angeben, welche Laufwerke verarbeitet werden sollen.
- Wenn Ihr IBM Spectrum Protect-Administrator einen Zeitplan für eine Teilsicherung für Sie definiert, aber nicht angibt, welche Laufwerke verarbeitet werden sollen.
- Wenn Sie die Aktion Domäne sichern in der GUI des Clients für Sichern/Archivieren auswählen.

Sie können die Option domain an den folgenden Positionen definieren:

- In einer Optionsdatei.
- In der Befehlszeile, wenn sie mit einem Clientbefehl eingegeben wird.
- In einer Clientoptionsgruppe, die auf dem Server mit dem Befehl define clientopt definiert wird.
- Als Option in einem geplanten Befehl, der auf dem Server mit dem Befehl define schedule definiert wird.

Enthält eine dieser Quellen eine Domänendefinition, sichert der Client die entsprechende Domäne. Sind Domänen in mehreren Quellen angegeben, sichert der Client alle angegebenen Domänen. Dasselbe Domänenobjekt kann mehrfach definiert werden; die Auswirkungen unterscheiden sich jedoch nicht von der einmaligen Definition. Wenn Sie keine Domäne angeben, sichert der Client die Standarddomäne, wie unter dem Parameter all-local beschrieben.

Sie können Objekte aus der Domäne ausschließen, indem Sie den Ausschlussoperator (-) vor dem Objekt angeben. Wenn ein Objekt in einer Domänendefinition ausgeschlossen ist, wird dieses Objekt von der Domäne ausgeschlossen, auch wenn es in einer anderen Definition eingeschlossen ist. Sie können den Domänenausschlussoperator (-) keinem Domänenschlüsselwort voranstellen, das mit all- beginnt.

Wenn eine Domänenanweisung mindestens ein Objekt ausschließt und keine Domänenanweisung Objekte einschließt, ist das Ergebnis eine leere Domäne (nichts wird gesichert). Sie müssen die Objekte, die in der Domäne eingeschlossen sein sollen, angeben, wenn Objekte durch Domänenanweisungen ausgeschlossen werden.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeBeispiel 1: In diesem Beispiel werden mit einer Domänenanweisung alle lokalen Dateisysteme außer /fs1 gesichert:

```
domain all-local -/fs1
```

Beispiel 2: In diesem Beispiel werden mit mehreren Domänenanweisungen alle lokalen Dateisysteme außer /fs1 gesichert:

```
domain all-local domain -/fs1
```

Beispiel 3: In diesem Beispiel wird /fs1 während einer Sicherungsoperation ausgeschlossen. Wenn keine andere Domänenanweisung verwendet wird, hat dies eine leere Domäne zur Folge. Nichts wird gesichert.

```
domain -/fs1
```

Windows-BetriebssystemeBeispiel 1: In diesem Beispiel werden mit einer Domänenanweisung alle lokalen Dateisysteme außer dem Systemstatus gesichert:

```
domain all-local -systemstate
```

Beispiel 2: In diesem Beispiel werden mit mehreren Domänenanweisungen alle lokalen Dateisysteme außer dem Systemstatus gesichert:

```
domain all-local domain -systemstate
```

Beispiel 3: In diesem Beispiel wird der Systemstatus von einer Sicherungsoperation ausgeschlossen. Wenn keine andere Domänenanweisung verwendet wird, hat dies eine leere Domäne zur Folge. Nichts wird gesichert.

```
domain -systemstate
```

Wenn Sie den Befehl 'incremental' mit einer Dateispezifikation starten, ignoriert der Client alle Domänendefinitionen und sichert nur die Dateispezifikation.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeSie können einen virtuellen Mountpunkt in Ihre Clientdomäne einschließen.

AIX-BetriebssystemeLinux-BetriebssystemeWichtig: Wenn Sie GPFS für AIX oder GPFS für Linux x86_64 in einem Cluster mit mehreren Knoten ausführen und alle Knoten ein angehängtes GPFS-Dateisystem gemeinsam nutzen, verarbeitet der Client dieses Dateisystem als lokales Dateisystem. Der Client sichert während einer Teilsicherung das Dateisystem auf jedem Knoten. Um diese Situation zu vermeiden, können Sie eine der folgenden Tasks ausführen:

- Konfigurieren Sie explizit die Anweisung 'domain' in der Clientbenutzeroptionsdatei (dsm.opt), sodass die Dateisysteme, die auf diesem Knoten gesichert werden sollen, aufgelistet werden.
- AIX-BetriebssystemeLinux-BetriebssystemeDefinieren Sie die Option exclude.fs in der Clientsystemoptionsdatei so, dass das GPFS-Dateisystem von den Sicherungsservices ausgeschlossen ist.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

Auto-Mount-Dateisysteme

Ist die Option domain auf all-local gesetzt und wird eine Sicherung ausgeführt, werden vom automatischen Mountprogramm verarbeitete Dateien und Schleifendateisysteme nicht gesichert.

Ist die Option domain auf all-local gesetzt, wenn Sie ein Dateisystem sichern, werden alle Unterverzeichnisse, die Mountpunkte für ein Auto-Mount-Dateisystem (AutoFS) sind, von einer Sicherungsoperation ausgeschlossen. Alle Dateien, die auf dem Server für das Auto-Mount-Unterverzeichnis vorhanden sind, verfallen.

Wenn eine Sicherung ausgeführt wird und die Option domain auf all-lofs gesetzt ist, werden alle expliziten Schleifendateisysteme (LOFS - Loopback File Systems) gesichert und alle Auto-Mount-Dateisysteme ausgeschlossen. Setzen Sie für Schleifeneinheiten und lokale Dateisysteme, die vom automatischen Mountprogramm verarbeitet werden, die Option domain auf all-auto-lofs.

Verwenden Sie die Option automount mit den Domänenparametern all-auto-nfs und all-auto-lofs, um mindestens ein Auto-Mount-Dateisystem anzugeben, das angehängt und der Domäne hinzugefügt werden soll. Wenn Sie die Option automount angeben, werden Auto-Mount-Dateisysteme erneut angehängt, falls sie während der Ausführung des Befehls incremental in den Offlinestatus versetzt wurden.

Virtuelle Mountpunkte können nicht mit Auto-Mount-Dateisystemen verwendet werden.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme
Linux-BetriebssystemeWichtig: Bei einigen Linux-Distributionen sind Mountpunkte oder -zuordnungen für Auto-Mount-Dateisysteme (AutoFS) möglicherweise in der aktuellen Mounttabelle nicht aufgelistet. Demzufolge werden die Auto-Mount-Dateisysteme, die während der Sicherungs- oder Archivierungsverarbeitung abgehängt werden, möglicherweise nicht korrekt verarbeitet und als Teil einer falschen Domäne gespeichert (beispielsweise als Teil der Domäne all-local, all-nfs oder all-lofs, abhängig vom tatsächlichen Dateisystemtyp). Aus diesem Grund müssen Sie in derartigen Linux-Distributionsumgebungen die entsprechende Einstellung für die Option automount angeben, damit Ihre Einstellung für die Option 'domain' zu jedem Zeitpunkt korrekt verarbeitet wird.

Mac OS X-BetriebssystemeFür Mac OS X werden Auto-Mount-Dateisysteme nicht unterstützt. Wenn ein Auto-Mount-Dateisystem Teil einer Domänenanweisung ist, schlägt die Sicherung fehl und im Auto-Mount-Dateisystem werden keine Dateien verarbeitet. Sichern Sie das Auto-Mount-Dateisystem auf dem Hostsystem und schreiben Sie es von dort zurück. Führen Sie die Sicherung bzw. die Zurückschreibung des Auto-Mount-Dateisystems nicht über eine Netzverbindung aus.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Optionsdatei, dsm.opt, ein. Sie können diese Option auf der Registerkarte Sichern im Abschnitt Domäne für Sicherung im Profileditor definieren.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Fügen Sie diese Option in die Optionsdatei, dsm.opt oder dsm.sys, ein. In der Datei dsm.sys müssen Sie diese Option innerhalb einer Serverzeilengruppe einfügen. Sie können diese Option auf der Registerkarte Sichern im Abschnitt Domäne für Sicherung im Profileditor definieren.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

Syntax

```
          .-------------------.
          V .-all-local-----. |
>>-DOMain----+---------------+-+-------------------------------><
             +-Domäne--------+
             +- -Domäne------+
             +-all-lofs------+
             +-all-nfs-------+
             +-all-auto-nfs--+
             '-all-auto-lofs-'
```

Windows-Betriebssysteme

Syntax

```
          .-------------------.
          V .-all-local-----. |
>>-DOMain----+---------------+-+-------------------------------><
             +-Objekt--------+
             +- -Objekt------+
             +-systemstate---+
             '- -systemstate-'
```

Parameter

all-local
Windows-Betriebssysteme

Alle lokalen Datenträger auf dem System und den Windows-Systemstatus sichern. Dies ist die Standardeinstellung. Lokale Datenträger werden als Datenträger definiert, die mit einem unterstützten Dateisystem (ReFS, NTFS, FAT32 oder FAT) auf einer DAS-Einheit formatiert sind, einschließlich Speicher mit SAN-Anschluss und mit iSCSI-Anschluss.Verzeichnisse, die mit dem Windows-Befehl subst Laufwerkbuchstaben zugeordnet werden, werden bei einer Sicherung berücksichtigt, wenn sich das zugeordnete Verzeichnis auf einer lokalen Platte befindet.

Windows-BetriebssystemeDie folgenden Datenträgertypen werden nicht berücksichtigt, wenn all-local angegeben wird:

- An das Netz angeschlossene Datenträger, einschließlich CIFS-Freigaben, die Laufwerkbuchstaben zugeordnet werden.
- Austauschbare Datenträger, einschließlich CD-/DVD-Laufwerken, USB-Thumb-Drives und Diskettenlaufwerken. Einige Festplatten mit USB-Anschluss werden in die Domäne all-local aufgenommen, wenn Windows sie nicht als austauschbare Speichereinheit klassifiziert.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeSichert alle lokalen Dateisysteme außer LOFS-Dateisystemen und LOFS durch das automatische Mountprogramm. Dieser Parameter ist der Standardwert. Das Verzeichnis /tmp ist nicht eingeschlossen.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme*Domäne*
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDefiniert die Dateisysteme, die in Ihre Standardclientdomäne einzuschließen sind.

Wenn Sie *domain* im Befehl incremental verwenden, werden diese Dateisysteme zusätzlich zu den Dateisystemen verarbeitet, die in Ihrer Standardclientdomäne angegeben sind.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme-*Domäne*
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDefiniert die Dateisysteme, die von Ihrer Standardclientdomäne auszuschließen sind.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemeall-lofs
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSichert alle Schleifendateisysteme mit Ausnahme der durch das automatische Mountprogramm bearbeiteten Dateisysteme. Dieser Parameter wird nicht unter Mac OS X unterstützt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemeall-nfs
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSichert alle Netzdateisysteme mit Ausnahme der durch das automatische Mountprogramm bearbeiteten Dateisysteme. Dieser Parameter wird nicht unter Mac OS X unterstützt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemeall-auto-nfs
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSichert alle Netzdateisysteme (jedoch nicht die lokalen Dateisysteme), die vom automatischen Mountprogramm verarbeitet werden. Dieser Parameter wird nicht unter Mac OS X unterstützt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemeall-auto-lofs
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSichert alle Schleifeneinheiten und lokalen Dateisysteme, die durch ein automatisches Mountprogramm bearbeitet werden. Dieser Parameter wird nicht unter Mac OS X unterstützt.

Objekt
Gibt die Domänenobjekte an, die in die Domäne eingeschlossen werden sollen.

Ein Objektname muss in Anführungszeichen eingeschlossen werden, wenn er Leerzeichen enthält.

-Objekt
Gibt die Domänenobjekte an, die von der Domäne ausgeschlossen werden sollen.

Ein Objektname muss in Anführungszeichen eingeschlossen werden, wenn er Leerzeichen enthält.

Windows-Betriebssystemesystemstate
Windows-BetriebssystemeDen Windows-Systemstatus sichern. Die Domäne systemstate ist in der Domäne all-local eingeschlossen.

Windows-Betriebssysteme -systemstate
Windows-BetriebssystemeDen Systemstatus von der Sicherungsverarbeitung ausschließen.

Beispiele

Optionsdatei:

Eine Optionsdatei kann mehrere Anweisungen domain enthalten. Jede der domain-Anweisungen stellt jedoch ein Beispiel für eine einzige Anweisung in einer Optionsdatei dar.

Mac OS X-Betriebssysteme

```
domain all-local
domain all-local -/Volumes/volume2
domain all-local '-/Volumes/Macintosh HD'
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
domain /tst /datasave /joe
"domain all-local"
domain ALL-LOCAL -/home
domain ALL-NFS -/mount/nfs1
```

Windows-Betriebssysteme

```
domain
c: d: e:
domain c: systemstate
domain ALL-LOCAL -systemstate
domain ALL-LOCAL -c:
domain ALL-LOCAL -\\florence\e$
```

In einer einzigen Domänenanweisung können ein oder mehrere Objekte für die Domäne aufgelistet sein. Sie können mehrere Domänenanweisungen verwenden. Aus den folgenden beiden Beispielen aus zwei Optionsdateien ergibt sich dieselbe Domäne:

Beispiel 1

```
...
domain fs1
domain all-local
domain -fs3
...
```

Beispiel 2

```
...
domain all-local fs1 -fs3
...
```

Befehlszeile:

Mac OS X-Betriebssysteme

```
-domain="/ /Volumes/volume2"
-domain="all-local -/Volumes/volume2"
```

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
-domain="/fs1 /fs2"
-domain=/tmp
-domain="ALL-LOCAL -/home"
```

Windows-Betriebssysteme

```
-domain="c: d:"
-domain="ALL-LOCAL -c: -systemstate"
```

Interaktion zwischen Domänendefinitionen

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDomänen können in mehreren Quellen definiert sein und das Ergebnis ist die Summe aller Domänendefinitionen. Als Beispiel für die Interaktion zwischen Domänendefinitionen sehen Sie im Folgenden, wie Domänendefinitionen aus mehreren Quellen zu verschiedenen Ergebnissen bei der Sicherung führen. In der Tabelle ist *FS* gefolgt von einer Zahl (z. B. FS1) ein Dateisystem. Diese Tabelle zeigt nur Befehle, die in die Befehlszeile eingegeben werden. Für geplante Befehle ist die Spalte für die Befehlszeile nicht relevant und die Optionen für den geplanten Befehl müssen beachtet werden.

Windows-BetriebssystemeDomänen können in mehreren Quellen definiert sein und das Ergebnis ist die Summe aller Domänendefinitionen. Als Beispiel für die Interaktion zwischen Domänendefinitionen sehen Sie im Folgenden, wie Domänendefinitionen aus mehreren Quellen zu verschiedenen Ergebnissen bei der Sicherung führen. In der Tabelle ist *FS* gefolgt von einer Zahl (z. B. FS1) ein Laufwerk. Diese Tabelle zeigt nur Befehle, die in die Befehlszeile eingegeben werden. Für geplante Befehle ist die Spalte für die Befehlszeile nicht relevant und die Optionen für den geplanten Befehl müssen beachtet werden.

Tabelle 1. Interaktion zwischen Domänendefinitionen aus mehreren Quellen

Optionsdatei	**Befehlszeile:**	**Clientoptionsgruppe**	**Mit dem Befehl incremental gesicherte Objekte**
`domain FS1`	`incremental -domain=FS2`	`domain FS3`	FS1 FS2 FS3
`domain FS1`	`incremental`	`domain FS3`	FS1 FS3
	`incremental -domain=FS2`		FS2
	`incremental -domain=FS2`	`domain FS3`	FS2 FS3
	`incremental`	`domain FS3`	FS3
	`incremental`		all-local

Optionsdatei	Befehlszeile:	Clientoptionsgruppe	Mit dem Befehl incremental gesicherte Objekte
`domain all-local`	`incremental`	`domain FS3`	all-local + FS3
`domain all-local` `domain -FS1`	`incremental`		all-local, aber nicht FS1
`domain -FS1`	`incremental`		Keine
`domain FS1 FS3`	`incremental`	`domain -FS3`	FS1
`domain all-local`	`incremental`	`domain -FS3`	all-local, aber nicht FS3
	`incremental FS1 -` `domain=all-local`		FS1
	`incremental FS1`	`domain all-local`	FS1
`domain -FS1`	`incremental FS1`		FS1

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Domain.image

Die Option domain.image gibt an, welche Objekte Sie bei einer Imagesicherung in Ihre Clientdomäne einschließen wollen.

Windows-BetriebssystemeUnformatierte logische Datenträger müssen explizit genannt werden.

Wenn Sie im Befehl backup image kein Dateisystem angeben, werden die Dateisysteme gesichert, die Sie mit der Option domain.image angeben.

Wenn Sie ein Dateisystem im Befehl backup image angeben, wird die Option domain.image ignoriert.

Verwenden Sie in Ihrer Clientoptionsdatei nicht die Option domain.image zur Angabe von Dateisystemen und geben Sie kein Dateisystem im Befehl backup image an, wird eine Nachricht ausgegeben und keine Sicherung durchgeführt.

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist für AIX, Linux x86_64, Linux on POWER und Solaris gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

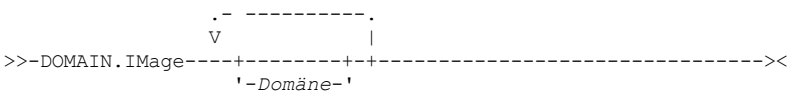
Diese Option ist für alle unterstützten Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option im Feld Sichern > Domäne für Sicherung im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option im Feld Sichern > Domäne für Sicherung im Profileditor definieren.

Syntax



Parameter

Domäne
: Definiert die Dateisysteme oder die unformatierten logischen Datenträger, die in Ihre Standardclientimagedomäne eingeschlossen werden sollen.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeOptionsdatei:
: AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemedomain.image /fs1 /fs2

Windows-BetriebssystemeOptionsdatei:
: Windows-Betriebssystemedomain.image d: e: f: domain.image f:\mnt\raw\rawmnt1 f:\mnt\fs\fsmnt1

Befehlszeile:
: Nicht zutreffend.

AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Domain.nas

Die Option domain.nas gibt die Datenträger an, die bei Ihren NAS-Imagesicherungen berücksichtigt werden sollen.

Sie können all-nas angeben, um alle angehängten Dateisysteme auf dem NAS-Dateiserver zu berücksichtigen. Ausgenommen sind hierbei die mit der Option exclude.fs.nas ausgeschlossenen Dateisysteme.

Der Client für Sichern/Archivieren verwendet Ihre Domäne für NAS-Imagesicherungen, wenn Sie den Befehl backup nas ausführen und nicht angeben, welche Datenträger zu verarbeiten sind.

AIX-BetriebssystemeOracle Solaris-BetriebssystemeWenn Sie diese Option in Ihrer Clientsystemoptionsdatei (dsm.sys) verwenden, definiert die Option domain.nas Ihre Standarddomäne für NAS-Imagesicherungen. Wenn Sie eine Imagesicherung des NAS-Dateisystems mithilfe des Befehls backup nas ausführen, fügt der Client die in der Befehlszeile angegebenen Datenträger den Datenträgern hinzu, die in Ihrer Datei dsm.sys definiert sind. Beispiel: Wenn Sie `domain.nas nas1/vol/vol0 nas1/vol/vol1` in Ihrer Datei dsm.sys angeben und `dsmc backup nas -nasnodename=nas1 /vol/vol2` in die Befehlszeile eingeben, sichert der Client die Datenträger `vol/vol0`, `vol/vol1` und `vol/vol2` auf dem Knoten `nas1`.

AIX-BetriebssystemeOracle Solaris-BetriebssystemeWenn Sie die Option domain.nas in der Datei dsm.opt auf all-nas setzen, sichert der Client alle angehängten Datenträger auf dem NAS-Dateiserver. Wenn Sie bei einer Sicherung eine Dateispezifikation verwenden und die Option domain.nas in der Datei dsm.sys auf all-nas setzen, hat die Angabe all-nas Vorrang.

Windows-BetriebssystemeWenn Sie diese Option in Ihrer Clientsystemoptionsdatei (dsm.opt) verwenden, definiert die Option domain.nas Ihre Standarddomäne für NAS-Imagesicherungen.

Windows-BetriebssystemeWenn Sie eine Imagesicherung des NAS-Dateisystems mithilfe des Befehls backup nas ausführen, fügt der Client die in der Befehlszeile angegebenen Datenträger den Datenträgern hinzu, die in Ihrer Datei dsm.opt definiert sind. Beispiel: Wenn Sie `domain.nas nas1/vol/vol0 nas1/vol/vol1` in Ihrer Datei dsm.opt angeben und `dsmc backup nas -nasnodename=nas1 /vol/vol2` in die Befehlszeile eingeben, sichert der Client die Datenträger `vol/vol0`, `vol/vol1` und `vol/vol2` auf dem Knoten `nas1`.

Windows-BetriebssystemeWenn Sie die Option domain.nas in der Datei dsm.opt auf all-nas setzen, sichert der Client alle angehängten Datenträger auf dem NAS-Dateiserver. Wenn Sie bei einer Sicherung eine Dateispezifikation verwenden und die Option domain.nas in der Datei dsm.opt auf all-nas setzen, hat die Angabe all-nas Vorrang.

Unterstützte Clients

AIX-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist nur für AIX- und Solaris-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                .- -----------.
                V .-all-nas-. |
>>-DOMAIN.Nas----+---------+-+--------------------------------><
                  '-Domäne--'
```

Parameter

Domäne
: Definiert die Datenträger, die Sie verarbeiten wollen. Es ist nicht möglich, Datenträger durch Angabe des Operators Bindestrich (-) auszuschließen.

all-nas
: Verarbeitet alle angehängten Datenträger auf dem NAS-Dateiserver. Ausgenommen sind hierbei die mit der Option exclude.fs.nas ausgeschlossenen Datenträger. Dies ist der Standardwert. Enthält die Datei dsm.opt keine Anweisung domain.nas und werden keine Datenträger in der Befehlszeile angegeben, sichert der Client alle angehängten Datenträger auf dem NAS-Server.

Beispiele

Optionsdatei:

domain.nas nas1/vol/vol0 nas1/vol/vol1
domain.nas all-nas

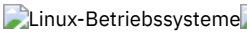
Befehlszeile:
Nicht zutreffend.

Domain.vmfull

Die Option domain.vmfull gibt die Imagegesamtsicherungsoperationen für virtuelle Maschinen eingeschlossen werden sollen.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Diese Option gilt sowohl für Platten virtueller VMware-Maschinen als auch für Platten virtueller Microsoft Hyper-V-Maschinen.



Domain.vmfull für virtuelle VMware-Maschinen

Für Sicherungen virtueller VMware-Maschinen arbeitet die Option domain.vmfull mit der Option vmchost zusammen. Die Option vmchost gibt den vCenter-Server oder ESX-Server an, der die virtuellen Maschinen enthält, die Sie schützen wollen. Mit den Parametern von domain.vmfull wird eine Operation auf eine Untergruppe der virtuellen Maschinen beschränkt, die auf dem durch vmchost angegebenen System ausgeführt werden.

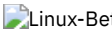
Sie können die zu verarbeitenden virtuellen Maschinen mit einer der folgenden Methoden angeben:

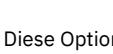
- Verwenden Sie die Option VM= und geben Sie den Namen einer virtuellen Maschine an.
- Geben Sie eine durch Kommas getrennte Liste mit den Namen der virtuellen Maschinen an.
- Verwenden Sie eine Syntax mit Platzhalterzeichen, um die virtuellen Maschinen zu verarbeiten, die dem Namensmuster entsprechen.
- Verwenden Sie einen der folgenden Parameter auf Domänenebene:
  - all-vm
  - all-windows
  - schedule-tag
  - vmhost
  - vmfolder
  - vmhostcluster
  - vmdatastore
  - vmresourcepool
  - vmhostfolder
  - vmdatacenter

Wenn Sie Parameter auf Domänenebene verwenden, werden virtuelle Maschinen, die in der Domäne erstellt werden, automatisch eingeschlossen, wenn die nächste Sicherung stattfindet. Wenn Sie beispielsweise den Parameter vmfolder verwenden, um alle in einem Ordner enthaltenen virtuellen Maschinen zu sichern, werden alle neuen virtuellen Maschinen, die diesem Ordner hinzugefügt werden, bei der nächsten Sicherung berücksichtigt. Dies gilt auch für die mit einem Muster abgeglichenen Namen, die in einer Syntax mit Platzhalterzeichen eingeschlossen sind.

Die mit der Option domain.vmfull angegebenen virtuellen Maschinen werden nur verarbeitet, wenn der Befehl backup vm ohne Angabe einer virtuellen Maschine oder eine Liste virtueller Maschinen in die Befehlszeile eingegeben wird.

Unterstützte Clients

 Diese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

 Diese Option kann für unterstützte Windows-Clients verwendet werden.

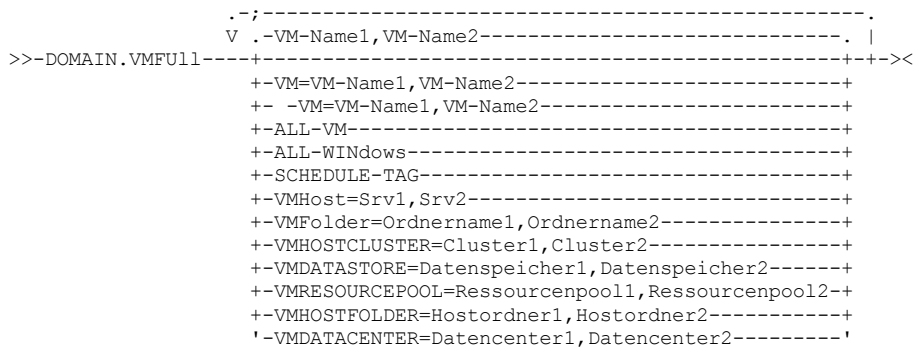
Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Definieren Sie diese Option in den Clientoptionen, über die Befehlszeile oder mithilfe der Registerkarte VM-Sicherung im Profileditor. Einschränkung: Die folgenden Parameter können nicht im Profileditor definiert werden. Schließen Sie diese Einstellung in die Optionsdatei oder in die Befehlszeile ein, wenn Sie einen Befehl backup vm ausführen:

- *VM-Name*:vmdk=*VM-Plattenkennsatz*
- schedule-tag
- vmresourcepool
- vmhostfolder
- vmdatacenter

Syntax für virtuelle VMware-Maschinen



Syntaxregeln: Mehrere Schlüsselwörter müssen jeweils durch ein Semikolon voneinander getrennt werden. Schließen Sie hinter den Semikolons keine Leerzeichen ein. Mehrere Namen virtueller Maschinen oder Domänen müssen durch Kommas und ohne Leerzeichen getrennt werden. Beispiele finden Sie bei vm=VM-Name. Die Regel für mehrere Namen virtueller Maschinen oder Domänen gilt nicht, wenn Sie das Schlüsselwort "Schedule-Tag" verwenden.

Parameter

VM-Name
: Gibt den Namen der virtuellen Maschine an, die verarbeitet werden soll. Der Name ist der Anzeigename der virtuellen Maschine. Sie können eine Liste mit Hostnamen virtueller Maschinen angeben. Trennen Sie die Namen jeweils durch ein Komma voneinander (`vm1,vm2,vm5`).

vm=*VM-Name*
: Das Schlüsselwort vm= gibt an, dass die nächste Gruppe von Werten eine Liste mit Namen virtueller Maschinen ist. Das Schlüsselwort vm= ist der Standardwert und ist nicht erforderlich.
In diesem Beispiel ist vm= nicht angegeben und die Maschinennamen sind durch Kommas getrennt.

```
domain.vmfull my_vm1,my_vm2
```

Wenn Sie mehrere Schlüsselwörter angeben, z. B. vm= und vmfolder=, müssen die Werte, auf die sich die Schlüsselwörter beziehen, durch Semikolons und ohne Zwischenleerschritte getrennt werden:

```
domain.vmfull vm=my_vm1;vm=my_vm2
domain.vmfull vm=my_vm1;vmfolder=folder1;vmfolder=folder2
```

Für die Auswahl von Namen virtueller Maschinen, die einem Muster entsprechen, können Platzhalterzeichen verwendet werden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem beliebigen einzelnen Zeichen. Zum Beispiel:

- Alle Dateien ausschließen, deren Hostname die Zeichenfolge "test" enthält: `-vm=*test*`
- Alle virtuellen Maschinen mit Namen wie den folgenden einschließen: "test20", "test25", "test29", "test2A": `vm=test2?`

Sie können eine virtuelle Maschine von einer Sicherungsoperation ausschließen, indem Sie den Ausschlussoperator (-) vor dem Schlüsselwort vm= angeben. Beispielsweise wird -vm für den Ausschluss einer bestimmten Maschine oder mehrerer Maschinen von einer Sicherung auf Domänenebene (z. B. ALL-Windows, ALL-VM und VMFolder) verwendet. Ist "vm1" der Name einer virtuellen Maschine im Ordner mit dem Namen "accountingDept", können Sie alle virtuellen Maschinen im dem Ordner sichern, aber die virtuelle Maschine "vm1" von der Sicherung ausschließen. Definieren Sie die folgende Option:

```
domain.vmfull VMFolder=accountingDept;-vm=vm1
```

Sie können mit dem Ausschlussoperator (-) keine Domäne ausschließen (z. B. ALL-VM, ALL-Windows oder VMFolder). Der Ausschlussoperator funktioniert nur auf der Ebene der Namen der virtuellen Maschinen.

VM-Name:vmdk=*VM-Plattenkennsatz*
: Das Schlüsselwort `:vmdk=` gilt nur für virtuelle VMware-Maschinen. Für die Verwendung dieses Schlüsselworts ist eine Lizenz für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware erforderlich.

Diese Option wird in der Regel verwendet, um Platten von der Sicherung auszuschließen (siehe Syntax :-vmdk). Sie können auch Platten virtueller Maschine einschließen, indem Sie die Option INCLUDE.VMDISK verwenden, oder Platten virtueller Maschine ausschließen, indem Sie die Option EXCLUDE.VMDISK verwenden.

Die virtuellen Platten in einer virtuellen Maschine verfügen über Plattenkennsätze, die jede virtuelle Platte eindeutig identifizieren. Mit dem Schlüsselwort :vmdk= geben Sie die Kennsätze der virtuellen Platten an, die bei einer VM-Sicherungsoperation (Backup VM) berücksichtigt werden sollen. Wenn Sie :vmdk= und einen Plattenkennsatz nicht angeben, werden alle virtuellen Platten in der virtuellen Maschine gesichert.

Beispiel: Es gibt eine virtuelle Maschine mit dem Namen "my_vm_example". Diese virtuelle Maschine verfügt über vier Platten (`Hard Disk 1, Hard Disk 2, Hard Disk 3, Hard Disk 4`). Sollen nur 'Hard Disk 2' und 'Hard Disk 3' bei einer Sicherung berücksichtigt werden,

fügen Sie das Schlüsselwort :vmdk= und den Plattenkennsatz für diese Platten hinzu. Da die Plattenkennsätze Leerzeichen enthalten, müssen die Parameter zwischen Anführungszeichen stehen. Beispiel:

```
domain.vmfull "my_vm_example:vmdk=Hard Disk 2:vmdk=Hard Disk 3"
```

Mit dem folgenden Beispiel werden 'Hard Disk 1' und 'Hard Disk 2' auf VM1 sowie 'Hard Disk 3' und 'Hard Disk 4' auf VM2 gesichert. Ein Komma wird als Trennzeichen für die Informationen der virtuellen Maschinen verwendet.

```
domain.vmfull "vm1:vmdk=Hard Disk 1:vmdk=Hard Disk 2",
  "vm2:vmdk=Hard Disk 3:vmdk=Hard Disk 4"
```

Wie bei dem Schlüsselwort -vm= können Sie auch bei :vmdk= den Ausschlussoperator (-) verwenden, um Platten von einer Sicherungsoperation auszuschließen.

Verwenden Sie folgende Syntax, um eine virtuelle Maschine (vm1) zu sichern und die Platten 'Hard Disk 3' und 'Hard Disk 4' auszuschließen:

```
domain.vmfull "vm1:-vmdk=Hard Disk 3:-vmdk=Hard Disk 4"
```

Sollen zwei virtuelle Maschinen (vm1 und vm2) gesichert und die beiden ersten Platten auf jeder Maschine ausgeschlossen werden, verwenden Sie folgende Syntax:

```
domain.vmfull "vm1:-vmdk=Hard Disk 1:-vmdk=Hard Disk 2",
  "vm2:-vmdk=Hard Disk 1:-vmdk=Hard Disk 2"
```

Sie können eine oder mehrere Platten in einer Anweisung domain.vmfull einschließen. Sie können eine oder mehrere Platten in einer Anweisung domain.vmfull ausschließen. Sie können das Einschließen und Ausschließen von Platten in einer Anweisung kombinieren. Die folgende Anweisung ist beispielsweise gültig:

```
domain.vmfull
    "vm1:vmdk=Hard Disk 1:-vmdk=Hard Disk 2:vmdk=Hard Disk 3:vmdk:Hard Disk 4"
```

Wenn eine Einschlussanweisung vorhanden ist, werden alle anderen Platten in der virtuellen Maschine von einer Sicherungsoperation ausgeschlossen, sofern die anderen Platten nicht auch in einer Einschlussanweisung angegeben sind. Mit der folgenden Anweisung werden beispielsweise alle Festplatten (Hard Disks) in vm1 ausgeschlossen, außer 'Hard Disk 1':

```
domain.vmfull "vm1:vmdk=Hard Disk 1"
```

Mit jedem der folgenden Beispiele wird 'Hard Disk 4' von einer Sicherung von vm1 ausgeschlossen:

```
domain.vmfull "vm1:vmdk=Hard Disk 1:vmdk=Hard Disk 2:vmdk=Hard Disk 3"
domain.vmfull "vm1:-vmdk=Hard Disk 4"
```

all-vm
: Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option vmchost angegeben ist.

all-windows
: Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option vmchost angegeben ist. Die virtuellen Maschinen müssen außerdem über den Gastbetriebssystemtyp Windows verfügen.

schedule-tag
: Für geplante Sicherungen virtueller VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center-Server definiert sind, der in der Option vmchost angegeben ist.

  Der IBM Spectrum Protect-Serveradministrator kann diese Option einer Zeitplandefinition hinzufügen, um anzugeben, dass der Zeitplan mit der Kategorie und dem Tag `Schedule (IBM Spectrum Protect)` kompatibel ist. Virtuelle Maschinen in VMware-Objekten, denen der Tag `Schedule` zugeordnet ist, werden gemäß dem Zeitplan gesichert.

  Voraussetzung: Damit die Option -domain.vmfull für das Tagging kompatibel ist, darf sie außer dem Parameter Schedule-Tag in der Zeitplandefinition keine weiteren Parameter auf Domänenebene enthalten. Andernfalls wird der Tag `Schedule (IBM Spectrum Protect)` ignoriert. Bei der Option muss die Groß-/Kleinschreibung nicht beachtet werden und die Option darf keine Leerzeichen enthalten. Die Anführungszeichen, die den Parameter Schedule-Tag einschließen, sind optional. Virtuelle Maschinen in VMware-Containern, die mit Tags versehen sind, die inkompatible Zeitpläne angeben, werden nicht gesichert.

  Weitere Informationen zum Tag `Schedule` finden Sie in "Unterstützte Datenschutztags". .

vmhost=*Hostname*
: Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option vmchost angegeben ist. Der angegebene Hostname muss mit dem vollständig qualifizierten Hostnamen oder der IP-Adresse übereinstimmen, der/die in der vCenter-Serveransicht Hosts und Cluster angegeben ist.

  Alle diesem Host hinzugefügten virtuellen Maschinen werden bei der Sicherungs- und Zurückschreibungsverarbeitung automatisch berücksichtigt. Die virtuellen Maschinen müssen darüber hinaus auf dem ESX-Server ausgeführt werden, der durch den Hostnamen angegeben ist, damit sie berücksichtigt werden. Sie dürfen nicht ausgeschaltet sein.

Dieser Parameter kann mehrere durch Kommas getrennte ESX-Server umfassen. Wenn das Virtual Center mehrere ESX-Server enthält, kann mit dieser Option nicht der ESX-Server bestimmt werden, auf dem eine Momentaufnahme erstellt wird. Der ESX-Server, auf dem eine Momentaufnahme erstellt wird, wird durch den VMware VirtualCenter-Web-Service bestimmt.

Wenn Sie eine direkte Verbindung zu einem ESXi- oder ESX-Host herstellen, ist die Option vmchost nur gültig, wenn vmhost der Server ist, zu dem Sie eine Verbindung herstellen. Andernfalls wird eine Warnung an die Konsole gesendet und in der Datei dsmerror.log aufgezeichnet; sie wird auch als Serverereignisnachricht aufgezeichnet.

Wenn die Option vmenabletemplatebackups auf yes gesetzt ist und VM-Schablonen Teil der Domäne sind, werden sie bei der Sicherung berücksichtigt.
Einschränkung: VMware-Schablonen für virtuelle Maschinen können nicht gesichert werden, wenn sie sich auf einem ESX- oder ESXi-Host befinden, weil ESX- und ESXi-Hosts Schablonen nicht unterstützen.

vmfolder=*Ordnername*
Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option vmchost angegeben ist. Die virtuellen Maschinen müssen sich außerdem in dem VMware-Ordner befinden, der durch den Ordnernamen angegeben ist. Der Ordnername kann mehrere VMware-Ordner umfassen, die durch Kommas getrennt sind.

vmhostcluster=*Host-Cluster-Name*
Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option vmchost angegeben ist. Die virtuellen Maschinen müssen darüber hinaus auf dem ESX-Host-Cluster ausgeführt werden, der durch den Host-Cluster-Namen angegeben ist. Sollen mehrere Host-Cluster-Namen angegeben werden, trennen Sie die Clusternamen durch Kommas: `VMHOSTCLUSTER=cluster1,cluster2`.

Wenn die Option vmenabletemplatebackups auf yes gesetzt ist und VM-Schablonen Teil der Domäne sind, werden sie bei der Sicherung berücksichtigt. Ein VMware-Host-Cluster ist nicht verfügbar, wenn Sie eine direkte Verbindung zu einem ESXi- oder ESX-Host herstellen. Wenn Sie eine direkte Verbindung zu einem ESXi-/ESX-Host herstellen und eine Domäne verarbeitet wird, die einen Host-Cluster enthält, wird eine Warnung an die Konsole gesendet und in der Datei dsmerror.log aufgezeichnet; sie wird auch als Serverereignisnachricht aufgezeichnet.

vmdatastore=*Datenspeichername*
Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center- oder ESX-Server definiert sind, der in der Option vmchost angegeben ist. Die konfigurierte Datenspeicherposition für eine virtuelle Maschine muss dem durch *Datenspeichername* angegebenen Datenspeichernamen entsprechen. Der Datenspeichername kann mehrere durch Kommas getrennte Datenspeicher umfassen: `VMDATASTORE=datastore1,datastore2`

Die Platte (vmdk-Dateien) virtueller Maschinen kann sich in mehreren Datenspeichern befinden, es gibt jedoch nur eine Standarddatenspeicherposition. Diese Standarddatenspeicherposition ist in der Konfiguration der virtuellen Maschine definiert und ist immer mit der Position der Konfigurationsdatei der virtuellen Maschine (.vmx-Datei) identisch. Wird eine Maschine mithilfe eines Domänenschlüsselworts für die Sicherung ausgewählt, werden die Konfigurationsdatei der virtuellen Maschine und alle Platten der virtuellen Maschine in die Sicherung eingeschlossen, einschließlich der Platten, die sich nicht in dem als Domäne angegebenen Datenspeicher, sondern in einem anderen Datenspeicher befinden.

vmresourcepool=*Name_des_Ressourcenpools*
Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center-Server definiert sind, der in der Option vmchost angegeben ist. Die virtuellen Maschinen müssen auch in dem VMware-Ressourcenpool vorhanden sein, der durch den Ressourcenpoolnamen angegeben ist. Der Name des Ressourcenpools kann mehrere durch Kommas getrennte Namen von Ressourcenpools umfassen, beispielsweise: `VMRESOURCEPOOL=Ressourcenpool1, Ressourcenpool2`

vmhostfolder=*Name_des_Hostordners*
Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center-Server definiert sind, der in der Option vmchost angegeben ist. Die virtuellen Maschinen müssen sich außerdem in dem VMware-Hostordner befinden, der durch den Hostordnernamen angegeben ist. Der Name des Hostordners kann mehrere durch Kommas getrennte Namen von VMware-Hostordnern umfassen, beispielsweise: `VMHOSTFOLDER=Hostordner1,Hostordner2`

vmdatacenter=*Datencentername*
Für virtuelle VMware-Maschinen. Mit dieser Option werden alle virtuellen Maschinen verarbeitet, die für den Virtual Center-Server definiert sind, der in der Option vmchost angegeben ist. Die virtuellen Maschinen müssen sich außerdem in dem VMware-Datencenter befinden, das durch den Datencenternamen angegeben ist. Der Datencentername kann mehrere durch Kommas getrennte Namen von Datencentern umfassen, beispielsweise: `VMDATACENTER=Datencenter1,Datencenter2`

Tipp: Wenn Sie mehr als einen Containertyp angeben, beispielsweise `vmfolder=Ordner1` und `vmhostcluster=Cluster2`, werden alle virtuellen Maschinen, die in `Ordner1` und `Cluster2` enthalten sind, geschützt. Die virtuellen Maschinen müssen nicht sowohl in `Ordner1` als auch in `Cluster2` vorhanden sein.

Sie können die virtuellen Maschinen wie in diesem Beispiel gezeigt angeben:
`domain.vmfull=vmfolder=Ordner1;vmhostcluster=Cluster2`

Beispiele für virtuelle VMware-Maschinen

Optionsdatei:
Alle virtuellen Maschinen in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull    all-vm
```

Alle virtuellen Maschinen mit Ausnahme der Maschinen mit dem Namenssuffix _test in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull all-vm;-vm=*_test
```

Alle virtuellen Maschinen mit dem Betriebssystem Windows in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull all-windows
```

Alle virtuellen Maschinen in den Cluster-Servern 1, 2 und 3 in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmhostcluster=cluster1,cluster2,cluster3
```

Alle Daten virtueller Maschinen in dem Datenspeicher `datastore1` in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmdatastore=datastore1
```

Alle virtuellen Maschinen in VM-Gesamtsicherungsoperationen einschließen, jedoch die virtuellen Maschinen testvm1 und testmvm2 ausschließen.

```
domain.vmfull all-vm;-VM=testvm1,testvm2
```

Die virtuellen Maschinen, die in den VM-Ordnern mit den Namen lab1 und lab2 definiert sind, in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmfolder=lab1,lab2
```

Alle virtuellen Maschinen auf den ESX-Hosts mit den Namen "brovar", "doomzoo" und "kepler" in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmhost=brovar.example.com,
  doomzoo.example.com,kepler.example.com
```

Alle virtuellen Maschinen in den VMware-Ressourcenpools `Ressourcenpool_A` und `Ressourcenpool_B` in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmresourcepool=Ressourcenpool_A,Ressourcenpool_B
```

Die virtuellen Maschinen, die in den VMware-Hostordnern mit den Namen `Hostordner1` und `Hostordner2` definiert sind, in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmhostfolder=Hostordner1,Hostordner2
```

Alle virtuellen Maschinen im VMware-Datencenter `dc1` in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull vmdatacenter=dc1
```

 Windows-Betriebssysteme

Domain.vmfull für virtuelle Microsoft Hyper-V-Maschinen

Verwenden Sie für Sicherungen virtueller Hyper-V-Maschinen die Option domain.vmfull, um anzugeben, welche virtuellen Hyper-V-Maschinen verarbeitet werden, wenn Sie einen Befehl backup vm ausführen, ohne Namen virtueller Hyper-V-Maschinen anzugeben.

Sie können die zu verarbeitenden VMs mit einer der folgenden Methoden angeben:

- Verwenden Sie die Option VM= und geben Sie den Namen einer virtuellen Maschine an.
- Geben Sie eine durch Kommas getrennte Liste mit den Namen der virtuellen Maschinen an.
- Verwenden Sie eine Syntax mit Platzhalterzeichen, um die virtuellen Maschinen zu verarbeiten, die dem Namensmuster entsprechen.
- Verwenden Sie die Option *VM-Name*:vhdx=, um die VM-Festplatte (VHDX) anzugeben, die in die Hyper-V-RCT-Sicherungsoperation für eine VM eingeschlossen oder von ihr ausgeschlossen werden soll.
- Verwenden Sie den Parameter all-vm auf Domänenebene. Sie können auch eine oder mehrere virtuelle Maschinen mithilfe des Schlüsselworts `VM=` einschließen oder VMs mithilfe der Syntax `-VM=` ausschließen.

Die mit der Option domain.vmfull angegebenen virtuellen Maschinen werden nur verarbeitet, wenn der Befehl backup vm ohne Angabe einer virtuellen Maschine oder eine Liste virtueller Maschinen in die Befehlszeile eingegeben wird.

Achtung: Bei Microsoft Hyper-V-Operationen ist all-vm der einzige gültige Parameter auf Domänenebene für die Option domain.vmfull. Sie können auch virtuelle Maschinen mit dem Schlüsselwort `VM=` einschließen oder mit der Syntax `-VM=` ausschließen.

Unterstützte Clients

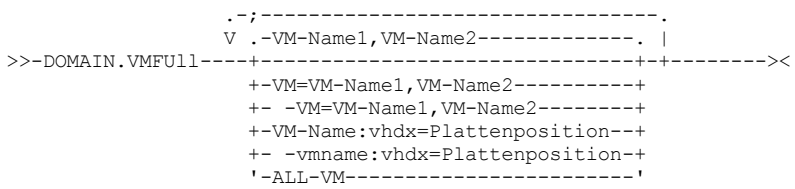
Diese Option kann für unterstützte Windows-Clients verwendet werden. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Definieren Sie diese Option in den Clientoptionen, über die Befehlszeile oder mithilfe der Registerkarte VM-Sicherung im Profileditor.

Einschränkung: Der Parameter *VM-Name*:vhdx=*VHDX-Position* kann nicht im Profileditor festgelegt werden. Schließen Sie diese Einstellung in die Optionsdatei oder in die Befehlszeile ein, wenn Sie einen Befehl backup vm ausführen:

Syntax für virtuelle Microsoft Hyper-V-Maschinen



Syntaxregeln: Mehrere Schlüsselwörter müssen jeweils durch ein Semikolon voneinander getrennt werden. Hinter den Semikolons dürfen keine Leerzeichen stehen. Mehrere Maschinen- oder Domänennamen müssen durch Kommas und ohne Leerzeichen getrennt werden. Beispiele finden Sie bei `vm=VM-Name`.

Parameter

VM-Name
: Definiert den Namen der virtuellen Maschine, die verarbeitet werden soll. Sie können eine Liste mit Hostnamen virtueller Maschinen angeben. Trennen Sie die Namen jeweils durch ein Komma voneinander (`vm1,VM2,Vm5`). Bei den Namen muss die Groß-/Kleinschreibung beachtet werden und die Groß-/Kleinschreibung muss mit der Schreibweise übereinstimmen, die auf dem Hyper-V-Host in der Sicht Hyper-V-Manager > Virtuelle Maschinen angezeigt wird.

vm=*VM-Name*
: Das Schlüsselwort vm= gibt an, dass die nächste Gruppe von Werten eine Liste mit Namen virtueller Maschinen ist. Das Schlüsselwort vm= ist der Standardwert und ist nicht erforderlich.
In diesem Beispiel ist vm= nicht angegeben und die Maschinennamen sind durch Kommas getrennt.

```
domain.vmfull my_vm1,my_vm2
```

Wenn Sie mehrere Schlüsselwörter angeben, wie beispielsweise vm= und -vm=, müssen die Werte, auf die sich die Schlüsselwörter beziehen, durch Semikolons und ohne Zwischenleerschritte getrennt werden:

```
domain.vmfull vm=my_vm1;vm=my_vm2
domain.vmfull -vm=my_vm3;-vm=my_vm4
```

Für die Auswahl von Namen virtueller Maschinen, die einem Muster entsprechen, können Platzhalterzeichen verwendet werden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem beliebigen einzelnen Zeichen. Zum Beispiel:

- Alle Dateien ausschließen, deren Hostname die Zeichenfolge "test" enthält: `-vm=*test*`
- Alle virtuellen Maschinen mit Namen wie den folgenden einschließen: "test20", "test25", "test29", "test2A":

  ```
  vm=test2?
  ```

Sie können eine virtuelle Maschine von einer Sicherungsoperation ausschließen, indem Sie den Ausschlussoperator (-) vor dem Schlüsselwort vm= angeben. Beispielsweise wird -vm für den Ausschluss einer bestimmten Maschine oder mehrerer Maschinen von einer Sicherung auf Domänenebene (wie beispielsweise ALL-VM) verwendet. Wenn "vm1" der Name einer virtuellen Maschine ist, können Sie alle virtuellen Maschinen in der Domäne sichern, die virtuelle Maschine "vm1" jedoch von der Sicherung ausschließen. Definieren Sie die folgende Option:

```
domain.vmfull all-vm;-vm=vm1
```

Sie können mit dem Ausschlussoperator (-) keine Domäne ausschließen, beispielsweise ALL-VM. Der Ausschlussoperator funktioniert nur auf der Ebene der Namen der virtuellen Maschinen.

VM-Name:vhdx=*VHDX-Position*
: Diese Option gibt die Position der Festplatte der virtuellen Maschine (VHDX) an, die in Hyper-V-RCT-Sicherungsoperationen für virtuelle Maschinen unter dem Betriebssystem Windows Server 2016 eingeschlossen werden soll.
Die Variable *VM-Name* gibt den Namen der zu sichernden virtuellen Maschine an. Für die Auswahl von Namen virtueller Maschinen, die einem Muster entsprechen, können Platzhalterzeichen verwendet werden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem beliebigen einzelnen Zeichen.
Das Schlüsselwort :vhdx=*Plattenposition* gibt die Position der Platte der virtuellen Maschine an, die in die Sicherungsoperation eingeschlossen werden soll. Die Plattenposition, die durch die Variable *Plattenposition* angegeben wird, muss mit "SCSI" oder "IDE" beginnen, gefolgt von der Controllernummer und der Einheitenpositionsnummer. Beispiel:

```
domain.vmfull "vm1:VHDX=IDE 1 0"
domain.vmfull "vm*:VHDX=SCSI 0 1"
domain.vmfull "vm?:VHDX=SCSI 0 1"
```

Sie können eine virtuelle Maschine von Sicherungsoperationen ausschließen, indem Sie den Ausschlussoperator (-) vor dem Schlüsselwort vhdx= angeben. Verwenden Sie beispielsweise -vhdx=, um eine VM-Platte von der Sicherungsoperation für eine virtuelle Maschine

auszuschließen. Beispiel:

```
domain.vmfull "vm1:-VHDX=IDE 1 0"
```

Wenn Sie mehrere einzuschließende oder auszuschließende Platten virtueller Maschinen angeben, müssen das Schlüsselwort vhdx= bzw. -vhdx= und die zugehörigen Werte durch Doppelpunkte ohne Zwischenleerschritte voneinander getrennt werden. Beispiel:

```
domain.vmfull "vm1:vhdx=IDE 1 0:vhdx=SCSI 0 1"
```

Wenn Sie mehrere Namen virtueller Maschinen und Platten virtueller Maschinen angeben, müssen der VM-Name und die zugehörigen Werte durch Semikolons ohne Zwischenleerschritte voneinander getrennt werden. Beispiel:

```
domain.vmfull "vm1:VHDX=IDE 1 0:VHDX=SCSI 0 1;vm2:VHDX=IDE 1 0:VHDX=SCSI 0 1"
domain.vmfull "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1;vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

all-vm
: Diese Option gibt an, dass bei einer Operation backup vm alle virtuellen Hyper-V-Maschinen verarbeitet werden, die dem Hyper-V-Host bekannt sind.

Beispiele für virtuelle Microsoft Hyper-V-Maschinen

Optionsdatei:
: Alle virtuellen Maschinen in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull   all-vm
```

Alle virtuellen Maschinen mit Ausnahme der Maschinen mit dem Namenssuffix _test in VM-Gesamtsicherungsoperationen einschließen.

```
domain.vmfull all-vm;-vm=*_test
```

Alle virtuellen Maschinen in VM-Gesamtsicherungsoperationen einschließen, jedoch die virtuellen Maschinen testvm1 und testmvm2 ausschließen.

```
domain.vmfull all-vm;-VM=testvm1,testvm2
```

IDE-Platten (mit Controller 1 und Plattenposition 0) und SCSI-Platten (mit Controller 0 und Plattenposition 1) in Hyper-V-RCT-Sicherungsoperationen für die virtuellen Maschinen `vm1` und `vm2` einschließen.

```
domain.vmfull "vm1:VHDX=IDE 1 0:VHDX=SCSI 0 1;vm2:VHDX=IDE 1 0:VHDX=SCSI 0 1"
```

Einschränkung: Sie können die Option all-vm nicht zusammen mit der Option *VM-Name:*-vhdx= in der Optionsdatei oder in der Befehlszeile verwenden.

 Linux-Betriebssysteme

Dontload

Linux x86_64-Clients können mit der Option dontload das Laden bestimmter Plugin-Bibliotheken beim Starten des Clients für Sichern/Archivieren unterdrücken.

Das Paket TIVsm_BAhdw.x86_64, das in Verteilungen von Linux x86_64 bereitgestellt wird, enthält Software, die zur Unterstützung von Momentaufnahmeteilsicherungen für NetAPP- und N-Series-Dateiserver benötigt wird. Wenn dieses Paket auf einem Linux x86_64-System installiert wird, das zur Ausführung von Operationen einer Einheit zum Versetzen von Daten für eine virtuelle Maschine verwendet wird, haben die Dateien in diesem Paket zur Folge, dass alle VMware-Sicherungsoperationen fehlschlagen. Wenn diese Fehler auftreten, wird die folgende Nachricht angezeigt:

```
ANS8811E

VMware-Operationen können nicht ausgeführt werden, wenn das Hardware-Plug-in-Produkt TIVsm-BAhdw installiert
und geladen ist. Deinstallieren Sie das Hardwareprodukt TIVsm-BAhdw oder definieren Sie die Option DONTLOAD
PIHDW in der Optionsdatei, um zu verhindern, dass das Hardware-Plug-in geladen wird.
```

Verwenden Sie diese Option, um das Laden der Plug-in-Bibliothek in den Arbeitsspeicher (RAM) beim Starten des Clients zu verhindern. Alternativ können Sie das Paket TIVsm_BAhdw deinstallieren, falls es nicht für Momentaufnahmeoperationen benötigt wird.

Unterstützte Clients

Diese Option ist nur für Linux x86_64-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

```
>>-DONTLoad----PIHDW-----------------------------------------><
```

Parameter

PIHDW
: Gibt an, dass das Hardware-Plug-in (TIVsm-BAhdw) beim Starten des Clients nicht in den Arbeitsspeicher (RAM) geladen wird. Verwenden Sie diese Option bei Clients für Sichern/Archivieren, bei denen das Hardware-Plug-in installiert ist, um zu verhindern, dass das Plug-in Fehler verursacht, wenn Sicherungs-/Archivierungsoperationen auf virtuellen VMware-Maschinen ausgeführt werden. Für die Option dontload gibt es keinen Standardwert.
Um festzustellen, ob das Plug-in installiert ist, geben Sie den folgenden Befehl ein und prüfen Sie die Ausgabe.

```
rpm -q -a | grep TIV
```

Falls die Ausgabe ein Paket enthält, das mit der Angabe "TIVsm-BAhdw" (gefolgt von einer Versionszeichenfolge) beginnt, ist das Paket für das Hardware-Plug-in installiert.

Beispiele

Optionsdatei:

```
DONTLoad PIHDW
```

Befehlszeile:
: Nicht zutreffend. Verwenden Sie diese Option nicht in der Befehlszeile.

Zugehörige Verweise:
Backup VM
Restore VM
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Dynamicimage

Verwenden Sie die Option dynamicimage im Befehl backup image oder mit der Option include.image, um anzugeben, dass Sie eine dynamische Imagesicherung ausführen wollen.

Unterstützte Clients

Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie die Anweisung include.image mit dem Wert dynamicimage in die Serverzeilengruppe Ihrer Systemoptionsdatei dsm.sys ein. Sie können diese Option auch mithilfe des Profileditors setzen.

Syntax

```
>>-DYNAMICImage-- --Wert--------------------------------------><
```

Parameter

Wert
: Gibt einen der folgenden Werte an:

yes
: Verwenden Sie diese Option nur, wenn der Datenträger nicht abgehängt und mit Lesezugriff erneut angehängt werden kann. Der Client sichert den Datenträger unverändert, ohne erneutes schreibgeschütztes Anhängen. Die Sicherung kann beschädigt werden, wenn Anwendungen auf den Datenträger schreiben, während die Sicherung ausgeführt wird. Führen Sie in diesem Fall fsck nach einer Zurückschreibung aus und hängen Sie das Dateisystem manuell an, um wieder Zugriff auf den Datenträger zu erlangen. Diese Option ist für AIX-, Solaris- und alle Linux-Clients gültig.
Anmerkung: Diese Option ist für AIX JFS2-Dateisysteme nicht zulässig.

no
: Verwenden Sie diese Option, wenn Sie keine dynamische Imagesicherung ausführen wollen. Dies ist der Standardwert. Das Standardverhalten hängt von der Plattform und dem Dateisystemtyp ab. Für Plattformen und Dateisysteme, die Momentaufnahmen unterstützen, namentlich AIX JFS2-Dateisysteme und LINUX LVM-Dateisysteme, ist der Standardwert die Imagesicherung auf Momentaufnahmebasis. Für alle anderen UNIX-Plattformen und Dateisystemen ist der Standardwert die statische Imagesicherung.

Beispiele

Optionsdatei:

```
include.image /kalafs1 dynamicimage=yes
```

Befehlszeile im Sicherungsimage:

```
dynamicimage=yes
```

 AIX-Betriebssysteme

Efsdecrypt

Mit der Option efsdecrypt können Sie steuern, ob Dateien, die von einem verschlüsselten AIX-Dateisystem (AIX-EFS) verschlüsselt wurden, in verschlüsseltem oder in entschlüsseltem Format gelesen werden sollen.

Der Standardwert der Option efsdecrypt ist no, d. h., die verschlüsselten oder unformatierten Daten werden gesichert. Wenn Sie yes angeben, werden die Dateien im Klartext gesichert. Dies bedeutet, dass sie als normale Dateien gesichert werden, als ob sie in unverschlüsseltem Format im Dateisystem gespeichert wären.

Wichtig: Immer, wenn Sie eine Sicherung ausführen, die auf einem EFS verschlüsselte Dateien einschließt, müssen Sie sicherstellen, dass Sie die korrekte Spezifikation der Option efsdecrypt verwenden. Falls sich der Optionswert efsdecrypt zwischen zwei Teilsicherungen ändert, werden alle verschlüsselten Dateien auf EFS-Dateisystemen erneut gesichert, selbst wenn sie sich seit der letzten Sicherung nicht geändert haben. Wenn Sie z. B. eine Teilsicherung verschlüsselter Dateien ausführen, die zuvor als "unformatiert" gesichert wurden, müssen Sie sicherstellen, dass für efsdecrypt der Wert no angegeben wird. Wenn Sie für efsdecrypt den Wert yes angeben, werden alle Dateien im Klartext erneut gesichert, selbst wenn sie unverändert sind. Verwenden Sie diese Option also mit Vorsicht.

Anmerkung: Dies ist eine globale Option, die auf die gesamte Sicherung angewendet wird. Es sind zwei separate Aufrufe des Clients erforderlich, um einige verschlüsselte Dateien als unformatierte Daten und andere als Klartext zu sichern.

Unterstützte Clients

Diese Option ist für AIX-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys oder in die Clientbenutzeroptionsdatei (dsm.opt) ein. In der Datei dsm.sys müssen Sie diese Option innerhalb einer Serverzeilengruppe einfügen.

Syntax

```
                .-No--.
>>-EFSDecrypt--+-----+-----------------------------------------><
                '-Yes-'
```

Parameter

No
: Verschlüsselte Dateien werden in verschlüsseltem oder unformatiertem Datenformat gelesen, und die Verschlüsselung und Komprimierung von IBM Spectrum Protect ist zwangsweise unterbrochen. Dies ist der Standardwert.

Yes
: Verschlüsselte Dateien werden in entschlüsseltem Format oder Klartextformat gelesen.

Beispiele

Optionsdatei:

```
EFSDecrypt yes
```

Befehlszeile:

```
-EFSDecrypt=no
```

 Windows-Betriebssysteme

Enable8dot3namesupport

Die Option enable8dot3namesupport gibt an, ob der Client 8.3-Kurznamen für Dateien, die auf NTFS-Dateisystemen Langnamen haben, sichert und zurückschreibt.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Eine Datei mit einem langen Dateinamen hat möglicherweise keinen 8.3-Kurznamen, wenn die Generierung von Kurznamen auf dem Windows-System inaktiviert ist. Diese Option ist nur für NTFS-Dateisysteme wirksam.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte 'Allgemein' des Profileditors definieren.

Syntax

```
                            .-No--.
>>-ENABLE8DOT3NAMESupport--+-----+-----------------------------><
                            '-Yes-'
```

Parameter

No
: 8.3-Kurznamen für Dateien mit langen Dateinamen werden nicht gesichert oder zurückgeschrieben. Dies ist der Standardwert.

Yes
: 8.3-Kurznamen für Dateien mit langen Dateinamen werden gesichert und zurückgeschrieben.

  Jeder Kurzname belegt bis zu 14 zusätzliche Byte in der Serverdatenbank. Obwohl dies eine kleine Zahl ist, kann es bei einer großen Anzahl Dateien mit 8.3-Kurznamen auf einer großen Anzahl von Windows-Systemen zu einer Vergrößerung der IBM Spectrum Protect-Serverdatenbank kommen.

Wichtig: Ziehen Sie Ihren IBM Spectrum Protect-Serveradministrator zu Rate, bevor Sie diese Option verwenden.

Bei der ersten Sicherung, die mit dieser Option ausgeführt wird, werden alle Dateien mit 8.3-Kurznamen auf dem IBM Spectrum Protect-Server selbst dann aktualisiert, wenn sich die Dateien sonst nicht geändert haben. Grund hierfür ist, dass der Client die 8.3-Kurznamen den aktiven Sicherungsversionen hinzufügt.

Ist diese Option für Zurückschreibung aktiviert, versucht der Client, den 8.3-Kurznamen für die zurückgeschriebenen Dateien festzulegen, selbst wenn die Generierung von Kurznamen auf dem Windows-System inaktiviert ist. Der Client muss unter einem Windows-Konto ausgeführt werden, das die Berechtigung SE_RESTORE_NAME besitzt, damit diese Option wirksam wird. Wenden Sie sich an Ihren Systemadministrator, wenn Sie Fragen zu Benutzereintragsberechtigungen haben.

Beim Zurückschreiben wird der 8.3-Kurzname einer Datei nicht zurückgeschrieben, wenn ein anderes Objekt in demselben Verzeichnis bereits denselben 8.3-Kurznamen hat. In diesem Fall wird die Datei zurückgeschrieben und es wird eine Informationsnachricht protokolliert, die angibt, dass der Kurzname nicht gesetzt werden konnte. Wenn die Datei mit ihrem Originalkurznamen zurückgeschrieben werden muss, müssen Sie den Konflikt mit der vorhandenen Datei auflösen und anschließend die Zurückschreibung erneut versuchen.

Wichtig: Dieser Parameter kann in einigen Fällen zu unerwarteten Ergebnissen führen. Beispiel: Wenn sich der Kurzname einer Datei zwischen der letzten Sicherung der Datei und dem Zeitpunkt der Zurückschreibung ändert und es einen Link oder einen Registry-Eintrag gibt, der sich auf den neueren Kurznamen bezieht, werden durch das Zurückschreiben der Datei mit dem älteren Kurznamen die Verweise auf den neueren Kurznamen ungültig.

Beispiele

Optionsdatei:
```
enable8dot3namesupport yes
```
Befehlszeile:
```
-enable8dot3namesupport=yes
```

Enablearchiveretentionprotection

Mit der Option enablearchiveretentionprotection kann der Client eine Verbindung zum IBM Spectrum Protect for Data Retention-Server herstellen. Dieser stellt sicher, dass Archivierungsobjekte erst dann auf dem Server gelöscht werden, wenn auf Richtlinien basierende Aufbewahrungskriterien für dieses Objekt erfüllt wurden.

Diese Option wird ignoriert, wenn der Client eine Verbindung mit einem Server herstellt, der nicht für Aufbewahrungsschutz aktiviert ist. Lautet die Option no (der Standardwert) und wird ein Versuch unternommen, eine Verbindung zum Datenaufbewahrungsserver herzustellen, wird die Verbindung zurückgewiesen.

Der Datenaufbewahrungsserver ist speziell für diese Aufgabe konfiguriert, d. h., die normale Sicherungs- oder Zurückschreibungsverarbeitung wird vom Server zurückgewiesen. Ist ein Client mit einem Datenaufbewahrungsserver verbunden, sind die folgenden Befehle nicht verfügbar. Wenn Sie versuchen, diese Befehle zu verwenden, wird eine Nachricht angezeigt, die besagt, dass sie mit diesem Server nicht gültig sind.

- incremental
- backup (alle Unterbefehle)
- selective
- restore (alle Unterbefehle mit Ausnahme von restore backupset -location=file oder -location=tape)
  Anmerkung: Bei restore backupset -location=file oder -location=tape wird keinerlei Verbindung zu einem Server (außer dem virtuellen Server) hergestellt und somit wird der Befehl unter keinen Umständen blockiert.
- restart restore
- delete backup
- delete group
- expire
- Alle Abfragen *außer*
  - query access
  - query archive
  - query filespace
  - query inclexcl
  - query managementclass
  - query node
  - query options
  - query schedule
  - query session
  - query systeminfo
  - query tracestatus

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 Windows-BetriebssystemeDiese Option ist nur in der Clientoptionsdatei (dsm.opt) gültig und nicht in einer Clientoptionsgruppe des Servers. Sie ist auch nicht in der Befehlszeile gültig.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDiese Option ist nur in der Datei dsm.sys *innerhalb* einer Serverzeilengruppe gültig und nicht in einer Clientoptionsgruppe des Servers. Sie ist auch nicht in der Befehlszeile gültig.

Syntax

```
                                        .-No--.
>>-ENABLEARCHIVERETENTIONProtection--+-----+--------------------><
                                        '-Yes-'
```

Parameter

No
: Die Verbindung zum Datenaufbewahrungsserver wird zurückgewiesen. Dies ist der Standardwert.

Yes
: Der Client stellt eine Verbindung zu einem Datenaufbewahrungsserver her.

Enablededupcache

Mit der Option enablededupcache geben Sie an, ob bei der clientseitigen Datendeduplizierung ein Cache verwendet werden soll. Die Verwendung eines lokalen Cache kann den Datenaustausch im Netz zwischen dem IBM Spectrum Protect-Server und dem Client reduzieren.

Wenn Sie eine Sicherungs- oder Archivierungsoperation mit aktiviertem Cache für die Datendeduplizierung ausführen, wird die Spezifikation der gesicherten oder archivierten Datenbereiche in der Cachedatenbank gespeichert. Bei der nächsten Ausführung einer Sicherung oder Archivierung fragt der Client den Cache für die Datendeduplizierung ab und ermittelt die Datenbereiche, die bereits zuvor auf dem Server gespeichert wurden. Datenbereiche, die mit Datenbereichen auf dem Server identisch sind, werden nicht erneut an den Server gesendet.

Wenn der Server und der Cache nicht synchronisiert sind, wird der Cache entfernt und ein neuer Cache erstellt.

Zu jedem Zeitpunkt kann nur jeweils ein Prozess auf den verteilten Cache für die Datendeduplizierung zugreifen. Parallele Sicherungsinstanzen auf einer Workstation, die denselben Server und Speicherpool verwenden, müssen entweder eindeutige Knotennamen oder eindeutige Cachespezifikationen benutzen. Auf diese Weise können alle Instanzen lokale Caches verwenden und die clientseitige Datendeduplizierung optimieren.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Auch die IBM Spectrum Protect-API unterstützt diese Option.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option mit dem Kontrollkästchen Deduplizierung > Deduplizierungscache aktivieren im Profileditor definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option mit dem Kontrollkästchen Deduplizierung > Deduplizierungscache aktivieren im Profileditor definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax

```
                    .-Yes*-.
>>-ENABLEDEDUPCache--+------+-----------------------------------><
                    '-No---'
```

Parameter

Yes
: Gibt an, dass Sie den Cache für die Datendeduplizierung aktivieren wollen. Ist die Datendeduplizierung nicht aktiviert, ist diese Einstellung nicht gültig. Yes ist der Standardwert für den Client für Sichern/Archivieren. No ist der Standardwert für die IBM Spectrum Protect-API.

No
: Gibt an, dass Sie den Cache für die Datendeduplizierung nicht aktivieren wollen.

Beispiele

Optionsdatei:
```
enablededupcache no
```
Befehlszeile:
```
-enablededupcache=no
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Verweise:
Deduplication
Dedupcachepath
Dedupcachesize

Enableinstrumentation

Standardmäßig werden Instrumentierungsdaten automatisch vom Client für Sichern/Archivieren und von der IBM Spectrum Protect-API erfasst, um Leistungsengpässe während der Sicherungs- und Zurückschreibungsverarbeitung zu identifizieren. Um die Instrumentierung zu inaktivieren oder später zu aktivieren, verwenden Sie die Option enableinstrumentation.

Wenn diese Option aktiviert ist, müssen Sie nicht darauf warten, dass Sie vom IBM Kundendienst aufgefordert werden, Leistungsdaten zu erfassen, wenn ein Problem auftritt. Stattdessen können die Daten bei jeder Ausführung einer Sicherungs- oder Zurückschreibungsoperation erfasst werden. Diese Funktion kann nützlich sein, da Sie das Problem nicht reproduzieren müssen, um Leistungsdaten zu erfassen. Die Informationen werden bereits vom Client erfasst.

Diese Option ersetzt die Optionen -TESTFLAG=instrument:detail, -TESTFLAG=instrument:API und -TESTFLAG=instrument:detail/API, die in vorherigen Versionen des Clients und der API verwendet werden.

Für jeden Prozess werden die folgenden Typen von Leistungsinstrumentierungsdaten erfasst:

- Die Aktivitätsnamen für jeden Thread (wie beispielsweise `File I/O`, `Data Verb`, `Compression` und `Transaction`), die durchschnittliche abgelaufene Zeit pro Aktivität und die Häufigkeit der Aktivität.
- Die Gesamtzeit der Aktivität für jeden Thread.
- Der Befehl, der ausgegeben wurde, und die Optionen, die verwendet wurden.
- Die Zusammenfassung des Sicherungs-, Zurückschreibungs- oder Abfragebefehls.

Standardmäßig werden die Leistungsdaten in der Instrumentierungsprotokolldatei (dsminstr.log) in dem Verzeichnis gespeichert, das mit der Umgebungsvariablen DSM_LOG (oder der Umgebungsvariablen DSMI_LOG für API-abhängige Produkte wie z. B. IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server und IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server) angegeben wird. Wenn Sie die Umgebungsvariable DSM_LOG nicht definiert haben, wird die Instrumentierungsprotokolldatei im aktuellen Verzeichnis gespeichert (das Verzeichnis, in dem der Befehl dsmc ausgegeben wurde).

Sie können wahlweise den Namen und die Position der Instrumentierungsprotokolldatei mit der Option instrlogname ändern. Sie können auch die Größe der Protokolldatei steuern, indem Sie die Option instrlogmax angeben.

Leistungsdaten werden nicht für die GUI des Clients für Sichern/Archivieren oder die GUI des Web-Clients erfasst.

Leistungsdaten werden für die folgenden Produkte erfasst, wenn die Option enableinstrumentation in der Clientoptionsdatei angegeben wird:

- Geplante Sicherungsoperationen auf Dateiebene mit dem Client für Sichern/Archivieren
- Sicherungen mit IBM Spectrum Protect for Virtual Environments: Data Protection for VMware
- Sicherungen mit IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- Sicherungen mit IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server
- Sicherungen mit IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server

Leistungsdaten werden auch während der Archivierungs- und Abrufverarbeitung erfasst.

Unterstützte Clients

Diese Option ist für alle Clients und die IBM Spectrum Protect-API gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Tipp: Diese Option ist standardmäßig aktiviert. Daher müssen Sie diese Option normalerweise nicht in die Clientoptionsdatei einfügen, es sei denn, die Option muss inaktiviert werden.

Syntax

```
                          .-Yes-.
>>-ENABLEINSTRUMENTATION--+-----+------------------------------><
                          '-No--'
```

Parameter

Yes
: Gibt an, dass während der Ausführung von Sicherungs- und Zurückschreibungsoperationen Leistungsdaten erfasst werden sollen. Der Standardwert ist Yes. Er bedeutet, dass Leistungsdaten auch dann erfasst werden, wenn diese Option nicht angegeben wird.

  Standardmäßig werden die Leistungsdaten in der Instrumentierungsprotokolldatei (dsminstr.log) in dem Verzeichnis gespeichert, das mit der Umgebungsvariablen DSM_LOG angegeben wird. Wenn Sie die Umgebungsvariable DSM_LOG nicht definiert haben, wird die Instrumentierungsprotokolldatei im aktuellen Verzeichnis gespeichert (das Verzeichnis, in dem der Befehl dsmc ausgegeben wurde). Ist die Datei nicht vorhanden, erstellt der Client die Datei und fügt der Datei Leistungsdaten hinzu.

No
: Gibt an, dass während der Ausführung von Sicherungs- und Zurückschreibungsoperationen keine Leistungsdaten erfasst werden sollen. Ist das Instrumentierungsprotokoll vorhanden, werden der Datei keine weiteren Daten hinzugefügt.

Beispiele

Optionsdatei:

```
enableinstrumentation yes
```

Befehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
dsmc sel /home/mydir/* -subdir=yes -enableinstrumentation=yes
```

Windows-Betriebssysteme

```
dsmc sel c:\mydir\* -subdir=yes -enableinstrumentation=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Tasks:
Clientinstrumentierungsdaten erfassen
API-Instrumentierungsdaten erfassen
Zugehörige Verweise:

Instrlogmax
Instrlogname
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Enablelanfree

Die Option enablelanfree gibt an, ob ein verfügbarer LAN-unabhängiger Pfad zu einer an ein Speicherbereichsnetz (SAN) angeschlossenen Speichereinheit aktiviert werden soll.

Ein LAN-unabhängiger Pfad ermöglicht die Verarbeitung von Sicherungen, Zurückschreibungen, Archivierungen und Abrufen zwischen dem Client für Sichern/Archivieren und der an ein SAN angeschlossenen Speichereinheit.

Zur Unterstützung der LAN-unabhängigen Datenversetzung müssen Sie das ProgrammIBM Spectrum Protect for SAN Storage Agent auf der Client-Workstation installieren und konfigurieren.

Anmerkung:

1. Wenn Sie die Option enablelanfree in die Clientoptionsdatei (dsm.opt) stellen, während einer Operation jedoch Null (0) Byte über das SAN übertragen wurden, müssen Sie sicherstellen, dass Sie die Daten an eine Verwaltungsklasse binden, die für LAN-unabhängig aktiviert ist.
2. Weitere Informationen über das Zurückschreiben von Sicherungssätzen in einer SAN-Umgebung enthält .
3. Wenn ein LAN-unabhängiger Pfad aktiviert ist, überschreiben die Einstellungen des SAN-Speicheragenten die Clientoptionen tcpserveraddress, tcpport und ssl. Mit dieser Überschreibungsaktion soll sichergestellt werden, dass der Client und der Speicheragent dieselben Serverkommunikationsoptionen verwenden.

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist nur für AIX-, Linux x86_64-, Linux on POWER- und Oracle Solaris-Clients gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch durch Auswahl des Kontrollkästchens LAN-unabhängig aktivieren auf der Registerkarte Allgemein des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auch durch Auswahl des Kontrollkästchens LAN-unabhängig aktivieren auf der Registerkarte Allgemein des Profileditors definieren.

Syntax

```
                  .-No--.
>>-ENABLELanfree--+-----+---------------------------------------><
                  '-Yes-'
```

Parameter

Yes
: Gibt an, dass Sie einen verfügbaren LAN-unabhängigen Pfad zu einer an ein Speicherbereichsnetz (SAN) angeschlossenen Speichereinheit aktivieren wollen.

No
: Gibt an, dass Sie einen LAN-unabhängigen Pfad zu einer an ein Speicherbereichsnetz (SAN) angeschlossenen Speichereinheit nicht aktivieren wollen. Dies ist der Standardwert.

Beispiele

Optionsdatei:
```
enablelanfree yes
```
Befehlszeile:
```
-enablelanfree=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Encryptiontype

Verwenden Sie die Option encryptiontype, um den Algorithmus für die Datenverschlüsselung anzugeben.

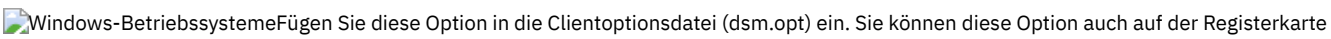
Die Option encryptiontype wirkt sich nur auf Sicherungs- und Archivierungsoperationen aus. Die Daten, die Sie einschließen, werden in verschlüsselter Form gespeichert; die Verschlüsselung hat keine Auswirkungen auf das gesendete oder empfangene Datenvolumen. Während der Zurückschreibungs- und Abrufoperationen werden die verschlüsselten Daten mit dem entsprechenden Verschlüsselungsalgorithmus entschlüsselt. Die Einstellung dieser Option spielt dabei keine Rolle.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch auf der Registerkarte Berechtigung des Profileditors definieren. Der Server kann dies überschreiben.



Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auch auf der Registerkarte Berechtigung im Profileditor definieren. Der Server kann dies überschreiben.

Syntax

```
                    .-AES128-.
>>-ENCRYPTIONType--+--------+-----------------------------------><
                    '-AES256-'
```

Parameter

AES128
: 128-Bit-AES-Datenverschlüsselung. 128-Bit-AES ist der Standardwert.

AES256
: 256-Bit-AES-Datenverschlüsselung. Die 256-Bit-AES-Datenverschlüsselung bietet die stärkste Datenverschlüsselung, die für Sicherungs- und Archivierungsoperationen verfügbar ist.

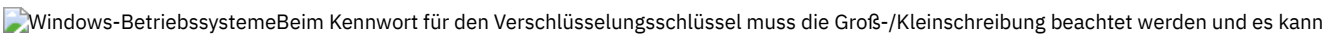
Beispiele

Optionsdatei:
```
encryptiontype aes128
```
Befehlszeile:
: Nicht zutreffend.

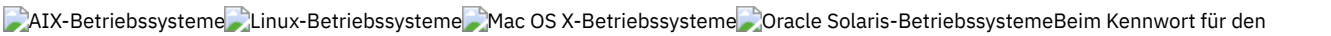
Encryptkey

Der Client für Sichern/Archivieren unterstützt die Option zum Verschlüsseln von Dateien, die auf dem IBM Spectrum Protect-Server gesichert oder archiviert werden. Diese Option wird mit der Option include.encrypt aktiviert.

Alle Dateien, die mit dem Muster in der Spezifikation include.encrypt übereinstimmen, werden verschlüsselt, bevor die Daten an den Server gesendet werden. Es gibt drei Optionen zum Steuern des Schlüssels, mit dem die Dateien verschlüsselt werden (prompt, save und generate). Alle drei Optionen können entweder mit dem Client für Sichern/Archivieren oder mit der IBM Spectrum Protect-API verwendet werden.



Beim Kennwort für den Verschlüsselungsschlüssel muss die Groß-/Kleinschreibung beachtet werden und es kann maximal 63 der folgenden Zeichen enthalten:



Beim Kennwort für den Verschlüsselungsschlüssel muss die Groß-/Kleinschreibung beachtet werden und es kann maximal 64 der folgenden Zeichen enthalten:

A-Z
: Alle Buchstaben von A bis Z in Groß- oder Kleinschreibung. Sie können keine Zeichen in der Landessprache angeben.

0-9
: Alle Zahlen von 0 bis 9

+
: Plus

.
: Punkt

_
: Unterstreichung

-
Silbentrennungsstrich

&
Et-Zeichen

Anmerkung:

1. Die API verfügt über eine alternative Methode für die Angabe von encryptkey=generate; die vorherige Option enableclientencryptkey=yes kann ebenfalls angegeben werden, um das Generieren der Verschlüsselungsverarbeitung anzufordern.
2. Die API-Option enableclientencryptkey=yes wird noch immer unterstützt; daher ist es möglich, beim Verwenden der API eine unzulässige Kombination von Optionen anzugeben. Beispiel: enableclientencryptkey=yes und encryptkey=prompt oder encryptkey=save.
3. Wenn sich widersprechende Werte angegeben werden, gibt die API eine Fehlernachricht zurück.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAchtung: Bei Verwendung der Option 'prompt' wird Ihr Verschlüsselungsschlüssel nicht in der IBM Spectrum Protect-Kennwortdatei unter UNIX gesichert. Wenn Sie den Schlüssel vergessen, können Ihre Daten nicht wiederhergestellt werden.
Windows-BetriebssystemeAchtung: Bei Verwendung der Option 'prompt' wird Ihr Verschlüsselungsschlüssel nicht in der Windows-Registrierungsdatenbank gespeichert. Wenn Sie den Schlüssel vergessen, können Ihre Daten nicht wiederhergestellt werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Berechtigung im Abschnitt Kennwort für Verschlüsselungsschlüssel des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Berechtigung im Abschnitt Kennwort für Verschlüsselungsschlüssel des Profileditors definieren.

Syntax

```
                .-save-----.
>>-ENCRYPTKey--+----------+-----------------------------------><
               +-prompt---+
               '-generate-'
```

Parameter

save
Das Kennwort für den Verschlüsselungsschlüssel wird in der Kennwortdatei des Clients für Sichern/Archivieren gespeichert. Es wird eine Bedienerführung für ein anfängliches Kennwort für den Verschlüsselungsschlüssel ausgegeben und nach der anfänglichen Bedienerführung wird das in der Kennwortdatei gespeicherte Kennwort für den Verschlüsselungsschlüssel für die Sicherungen und Archivierungen der Dateien verwendet, die mit der Spezifikation include.encrypt übereinstimmen. Der Schlüssel wird bei Zurückschreibungs- und Abrufoperationen aus der Kennwortdatei abgerufen.

Windows-BetriebssystemeDas Kennwort kann maximal 63 Byte umfassen.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeDas Kennwort kann maximal 64 Byte umfassen.

Wird für eine API-Anwendung die Option save angegeben, muss das anfängliche Schlüsselkennwort von der Anwendung, die die API verwendet, im Funktionsaufruf dsmInitEx zur Verfügung gestellt werden. Die API selbst gibt keine Bedienerführung an den Benutzer aus, sondern verlässt sich darauf, dass die Anwendung den Benutzer, falls notwendig, durch Bedienerführung zur Eingabe auffordert.

Dieser Parameter ist der Standardwert.

Anmerkung: Es gelten die folgenden Einschränkungen:

- Diese Option kann nur verwendet werden, wenn zusätzlich passwordaccess generate angegeben ist.
- Der Rootbenutzer oder ein berechtigter Benutzer muss das anfängliche Kennwort für den Verschlüsselungsschlüssel angeben.

prompt
Die Verwaltung des Kennworts für den Verschlüsselungsschlüssel wird vom Benutzer zur Verfügung gestellt. Der Benutzer muss das Kennwort für den Verschlüsselungsschlüssel angeben, wenn der Client eine Sicherung oder Archivierung startet. Eine Bedienerführung für dasselbe Kennwort wird ausgegeben, wenn die verschlüsselte Datei zurückgeschrieben oder abgerufen wird.

Windows-BetriebssystemeDieses Kennwort kann maximal 63 Byte umfassen.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDieses Kennwort kann maximal 64 Byte umfassen.

Wird für eine API-Anwendung die Option prompt angegeben, muss das Schlüsselkennwort von der Anwendung, die die API verwendet, im Funktionsaufruf dsmInitEx zur Verfügung gestellt werden. Die API selbst gibt keine Bedienerführung an den Benutzer aus, sondern verlässt sich darauf, dass die Anwendung den Benutzer, falls notwendig, durch Bedienerführung zur Eingabe auffordert.

generate
Ein Kennwort für den Verschlüsselungsschlüssel wird dynamisch generiert, wenn der Client eine Sicherung oder Archivierung startet. Dieses generierte Schlüsselkennwort wird für die Sicherungen der Dateien verwendet, die mit der Spezifikation include.encrypt übereinstimmen. Das generierte Schlüsselkennwort wird in verschlüsselter Form auf dem IBM Spectrum Protect-Server aufbewahrt. Das Schlüsselkennwort wird an den Client zurückgegeben, damit die Datei in Zurückschreibungs- und Abrufoperationen entschlüsselt werden kann.

Beispiele

Optionsdatei:

```
encryptkey prompt
```

Befehlszeile:
Nicht zutreffend.

Errorlogmax

Die Option errorlogmax gibt die maximale Größe des Fehlerprotokolls in Megabyte an. Der Standardname des Fehlerprotokolls lautet dsmerror.log.

Der Protokollumlauf wird durch die Option errorlogmax gesteuert. Wenn errorlogmax auf null (0) gesetzt ist, ist die Größe des Protokolls unbegrenzt. Es gibt keinen "Umlauf" protokollierter Einträge, wodurch auch keine älteren protokollierten Einträge überschrieben werden. Wenn errorlogmax nicht auf null gesetzt ist, überschreiben die neuesten Protokolleinträge die ältesten Protokolleinträge, sobald die Protokolldatei ihre maximale Größe erreicht.

Die Protokollbereinigung wird durch die Option errorlogretention gesteuert. Für bereinigte Protokolle wird kein Umlauf durchgeführt. Stattdessen werden Protokolleinträge, deren Alter die mit der Option errorlogretention angegebene Anzahl von Tagen übersteigt, aus der Protokolldatei entfernt.

Wenn Sie vom Protokollumlauf (Option errorlogmax) zur Protokollbereinigung (Option errorlogretention) wechseln, werden alle vorhandenen Protokolleinträge aufbewahrt, und das Protokoll wird mit den neuen Kriterien von errorlogretention bereinigt. Bereinigte Protokolleinträge werden in einer Datei mit dem Namen dsmerlog.pru gespeichert.

Wenn Sie von der Protokollbereinigung (Option errorlogretention) zum Protokollumlauf (Option errorlogmax) wechseln, werden alle Sätze im vorhandenen Protokoll in die Protokolldatei dsmerlog.pru kopiert, das vorhandene Protokoll wird geleert und die Protokollierung beginnt dann mit den neuen Protokollumlaufbedingungen.

Wenn Sie lediglich den Wert der Option errorlogmax ändern, wird das vorhandene Protokoll erweitert oder gekürzt, um der neuen Größe zu entsprechen. Wird der Wert verkleinert, werden die ältesten Einträge gelöscht, um die Datei auf die neue Größe zu verkleinern.

Wird weder errologmax noch errorlogretention angegeben, kann das Fehlerprotokoll uneingeschränkt wachsen. Sie müssen den Protokollinhalt manuell verwalten, um zu verhindern, dass das Protokoll die Plattenressourcen verbraucht. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option errorlogretention ausgeben, wird das Protokoll mit dem angegebenen Wert für die Aufbewahrungsdauer bereinigt. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option errorlogmax ausgeben, wird das vorhandene Protokoll als bereinigtes Protokoll behandelt. Das heißt, der Inhalt der Datei dsmerror.log wird in eine Datei mit dem Namen dsmerlog.pru kopiert, in dsmerror.log werden neue Protokolleinträge erstellt und es findet ein Protokollumlauf statt, wenn das Protokoll seine maximale Größe erreicht.

Anmerkung: Wenn Sie für errorlogmax einen Wert ungleich null angeben (wodurch der Protokollumlauf aktiviert wird), können Sie nicht die Option errorlogretention verwenden, um bereinigte Protokolle zu erstellen. Für Protokolle kann entweder eine Bereinigung oder ein Umlauf durchgeführt werden, aber nicht beides.
Mit der Option errorlogmax erstellte Protokolle enthalten einen Protokollkopfsatz, der Informationen wie in dem folgenden Beispieldatensatz enthält:

```
LOGHEADERREC 661  104857600 IBM Spectrum Protect 8.1.0 Fri Dec 9 06:46:53 2011
```

Beachten Sie, dass die Datums- und Zeitmarkenangaben im Text von LOGHEADERREC nicht mithilfe der Einstellungen übersetzt oder formatiert werden, die in den Optionen dateformat und timeformat angegeben sind.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme Sie können diese Option auch auf der Registerkarte Clientvorgaben in der grafischen Benutzerschnittstelle definieren. Wählen Sie hierfür Umlauf für Fehlerprotokolldatei aktivieren aus und geben Sie einen Wert ungleich null für die maximale Größe der Protokolldatei an. Geben Sie für die maximale Größe null an, um den Umlauf der Protokolldatei zu verhindern. Wenn die maximale Größe auf null gesetzt ist, bleibt die Option Umlauf für Fehlerprotokolldatei aktivieren wirkungslos. Es findet kein Protokollumlauf statt, wenn die maximale Größe auf null gesetzt ist.

Syntax

```
>>-ERRORLOGMAX-- --Größe----------------------------------------><
```

Parameter

Größe
: Gibt die maximale Größe für die Protokolldatei in Megabyte an. Der Wertebereich ist 0 bis 2047. Der Standardwert ist 0, wodurch der Protokolldateiumlauf inaktiviert und die Größe der Protokolldatei unbeschränkt wird.

Beispiele

Optionsdatei:
```
errorlogmax 2000
```
Befehlszeile:
```
-errorlogmax=2000
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Errorlogname

Diese Option gibt den vollständig qualifizierten Pfad und Dateinamen der Datei an, die die Fehlernachrichten enthält.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDer Wert für diese Option überschreibt die Umgebungsvariable `DSM_LOG`. Die Dateien `dsmwebcl.log` und `dsmsched.log` werden in demselben Verzeichnis erstellt wie die Fehlerprotokolldatei, die Sie mit der Option errorlogname angeben.

 Mac OS X-BetriebssystemeFür Mac OS X ist die Standardposition eine der folgenden Positionen:

```
~/Library/Logs/tivoli/tsm/
/Library/Logs/tivoli/tsm/
```

 Mac OS X-Betriebssystemedsmerror.log kann keine symbolische Verbindung sein.

 Windows-BetriebssystemeDer Wert für diese Option überschreibt die Umgebungsvariable `DSM_LOG`. Die Dateien `dsmwebcl.log` und `dsmsched.log` werden in demselben Verzeichnis erstellt wie die Fehlerprotokolldatei, die Sie mit der Option errorlogname angeben.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Allgemein über die Schaltfläche Fehlerprotokoll auswählen im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Allgemein über die Schaltfläche Fehlerprotokoll auswählen im Profileditor definieren.

Syntax

```
>>-ERRORLOGName-- --Dateispezifikation-------------------------><
```

Parameter

Dateispezifikation
: Der vollständig qualifizierte Pfad und Name der Datei, in der Fehlerprotokollinformationen gespeichert werden sollen. Wenn ein Teil des von Ihnen angegebenen Pfads nicht vorhanden ist, versucht der Client, ihn zu erstellen.

   AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDie Datei dsmerror.log kann keine symbolische Verbindung sein.

Beispiele

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeOptionsdatei:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme`errorlogname /tmp/tsmerror.log`

 Windows-BetriebssystemeOptionsdatei:

 Windows-Betriebssysteme`errorlogname c:\temp\dsmerror.log`

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeBefehlszeile:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme`-errorlogname=/tmp/tsmerror.log`

 Windows-BetriebssystemeBefehlszeile:

 Windows-Betriebssysteme`-errorlogname=c:\temp\dsmerror.log`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

 Windows-BetriebssystemeDie Position der Protokolldatei, die mit dem Konfigurationsdienstprogramm für den Client-Service oder dem Clientkonfigurationsassistenten angegeben wird, überschreibt die in der Clientoptionsdatei (dsm.opt) angegebene Position.

Errorlogretention

Die Option errorlogretention legt fest, wieviele Tage Fehlerprotokolleinträge aufbewahrt werden sollen, bevor sie bereinigt werden, und ob die bereinigten Einträge in anderen Dateien gespeichert werden sollen.

Das Fehlerprotokoll wird bereinigt, wenn der erste Fehler in das Protokoll geschrieben wird, nachdem eine Clientsitzung gestartet wurde. Wenn als einzige Sitzung der Client-Scheduler täglich ununterbrochen aktiv ist, wird das Fehlerprotokoll möglicherweise nicht erwartungsgemäß bereinigt. Stoppen Sie die Sitzung und starten Sie sie erneut, damit der Scheduler das Fehlerprotokoll bereinigen kann.

Wenn Sie von der Protokollbereinigung (Option errorlogretention) zum Protokollumlauf (Option errorlogmax) wechseln, werden alle Sätze im vorhandenen Protokoll in die Protokolldatei dsmerlog.pru kopiert, das vorhandene Protokoll wird geleert und die Protokollierung beginnt dann mit den neuen Protokollumlaufbedingungen.

Wenn Sie vom Protokollumlauf (Option errorlogmax) zur Protokollbereinigung (Option errorlogretention) wechseln, werden alle vorhandenen Protokolleinträge aufbewahrt, und das Protokoll wird mit den neuen Kriterien von errorlogretention bereinigt. Bereinigte Protokolleinträge werden in einer Datei mit dem Namen dsmerlog.pru gespeichert.

Wird weder errologmax noch errorlogretention angegeben, kann das Fehlerprotokoll uneingeschränkt wachsen. Sie müssen den Protokollinhalt manuell verwalten, um zu verhindern, dass das Protokoll die Plattenressourcen verbraucht. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option errorlogretention ausgeben, wird das Protokoll mit dem angegebenen Wert für die Aufbewahrungsdauer bereinigt. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option errorlogmax ausgeben, wird das vorhandene Protokoll als bereinigtes Protokoll behandelt. Das heißt, der Inhalt der Datei dsmerror.log wird in eine Datei mit dem Namen dsmerlog.pru kopiert, in dsmerror.log werden neue Protokolleinträge erstellt und es findet ein Protokollumlauf statt, wenn das Protokoll seine maximale Größe erreicht.

Anmerkung: Wenn Sie die Option errorlogretention angeben, um bereinigte Protokolle zu erstellen, können Sie die Option errorlogmax nicht angeben. Für Protokolle kann entweder eine Bereinigung oder ein Umlauf durchgeführt werden, aber nicht beides.
AIX-Betriebssysteme  Linux-BetriebssystemeOracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

AIX-BetriebssystemeLinux-BetriebssysteMac OS X-BetriebssysteOracle Solaris-BetriebssysteWindows-Betriebssysteme
Sie können diese Option auch auf der Registerkarte Clientvorgaben in der grafischen Benutzerschnittstelle definieren. Wählen Sie hierfür Alte Einträge bereinigen aus und geben Sie einen Wert für Einträge bereinigen, die älter sind als an. Durch Auswahl der Option Bereinigte Einträge sichern werden die bereinigten Protokolleinträge in der Protokolldatei dsmerlog.pru gespeichert.

Syntax

```
                        .-N----.  .-D-.
>>-ERRORLOGRetention--+------+--+---+-------------------------><
                      '-Tage-'  '-S-'
```

Parameter

N oder Tage
: Gibt die Wartezeit vor dem Bereinigen des Fehlerprotokolls an.

  N
  : Das Fehlerprotokoll nicht bereinigen. Das Fehlerprotokoll kann unendlich groß werden. Dies ist der Standardwert.

  Tage
  : Die Anzahl Tage, die Protokolldateieinträge aufbewahrt werden sollen, bevor das Protokoll bereinigt wird. Der Wertebereich ist 0 bis 9999.

D oder S
: Gibt an, ob bereinigte Einträge gesichert werden sollen. Ein Leerzeichen oder ein Komma eingeben, um diesen Parameter vom vorherigen zu trennen.

  D
  : Die Fehlerprotokolleinträge löschen, wenn das Protokoll bereinigt wird. Dies ist der Standardwert.

  S
  : Die Fehlerprotokolleinträge sichern, wenn das Protokoll bereinigt wird.

    Die bereinigten Einträge werden aus dem Fehlerprotokoll in die Datei dsmerlog.pru kopiert, die sich in demselben Verzeichnis wie die Datei dsmerror.log befindet.

Beispiele

Optionsdatei:

Protokolleinträge in der Datei dsmerror.log, die älter als 365 Tage sind, bereinigen und die bereinigten Einträge in dsmerlog.pru speichern.

```
errorlogretention 365 S
```

Befehlszeile:

```
-errorlogr=365,S
```

Optionsdatei:

Protokolleinträge in der Datei dsmerror.log, die älter als 365 Tage sind, bereinigen und die bereinigten Einträge nicht speichern.

```
errorlogretention 365 D
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Ausschlussoptionen

Verwenden Sie die Ausschlussoptionen, um Objekte von Sicherungs-, Image- oder Archivierungsservices auszuschließen.

Windows-BetriebssystemeBeispielsweise können Sie die folgenden Informationstypen ausschließen:

- Alle temporären Dateien
- Alle lokalen Caches von Netzdateien
- Alle Dateien, die kompilierten Objektcode enthalten, den Sie auf einfache Weise mit anderen Methoden erneut erstellen können
- Ihre Betriebssystemdateien

AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeBeispielsweise können Sie die folgenden Informationstypen ausschließen:

- Alle temporären Dateien
- Alle lokalen Caches von Netzdateien
- Alle Dateien, die kompilierten Objektcode enthalten, den Sie auf einfache Weise mit anderen Methoden erneut erstellen können
- Ihre Betriebssystemdateien

Sie können bestimmte Dateien von der Verschlüsselungsverarbeitung während einer Sicherung ausschließen.

Windows-BetriebssystemeSie können Dateien mit Fernzugriff ausschließen, indem Sie UNC-Namen (d. h. Namen, die der allgemeinen Namenskonvention entsprechen) in Ihrer Ausschlussanweisung angeben.

Anmerkung:

1. Windows-BetriebssystemeWenn Sie eine Datei ausschließen, die zuvor eingeschlossen war, werden vorhandene Sicherungsversionen bei der nächsten Teilsicherung inaktiv.
2. AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMit Ausnahme von exclude.fs werden vorhandene Sicherungsversionen bei der nächsten Teilsicherung inaktiv, wenn Sie eine Datei ausschließen, die zuvor eingeschlossen war.
3. Windows-BetriebssystemeBei den Exclude-Anweisungen muss die Groß-/Kleinschreibung nicht beachtet werden.
4. Auf dem Server können Ausschlussoptionen mit der Option inclexcl definiert werden.
5. Windows-BetriebssystemeWie bei anderen Einschluss-/Ausschlussanweisungen können Sie mithilfe der Option inclexcl eine Datei angeben, die Unicode-Format haben und Ausschlussanweisungen mit Dateinamen in Unicode enthalten kann.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeSchließen Sie alle Systemdateien oder Images aus, die bei ihrer Wiederherstellung das Betriebssystem beschädigen könnten. Schließen Sie außerdem das Verzeichnis mit den IBM Spectrum Protect-Clientdateien aus.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSoll ein vollständiges Verzeichnis mit dem Namen `/any/test` ausgeschlossen werden, geben Sie Folgendes ein:

Windows-BetriebssystemeSoll ein vollständiges Verzeichnis mit dem Namen `any\test` ausgeschlossen werden, geben Sie Folgendes ein:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
exclude.dir /any/test
```

Windows-Betriebssysteme

```
exclude.dir c:\any\test
```

Windows-BetriebssystemeSollen Unterverzeichnisse unter dem Verzeichnis `any` ausgeschlossen werden, deren Name mit `test` beginnt, geben Sie Folgendes ein:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSollen Unterverzeichnisse unter dem Verzeichnis `/any/` ausgeschlossen werden, deren Name mit `test` beginnt, geben Sie Folgendes ein:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
exclude.dir /any/test*
```

Windows-Betriebssysteme

```
exclude.dir c:\any\test*
```

Windows-BetriebssystemeAnmerkung: Wenn Sie eine Ausschlussanweisung ohne Angabe eines Laufwerkbuchstabens definieren, z. B. `exclude.dir code`, wird das Verzeichnis `code` auf allen Laufwerken von der Verarbeitung ausgeschlossen.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Optionen auf der Registerkarte Einschluss/Ausschluss im Abschnitt Einschluss-/Ausschlussoptionen definieren im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Optionen in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Optionen auf der Registerkarte Einschluss/Ausschluss im Abschnitt Einschluss-/Ausschlussoptionen definieren im Profileditor definieren.

Syntax

```
>>-Optionen-- --Muster----------------------------------------><
```

Windows-Betriebssystemeexclude, exclude.backup, exclude.file, exclude.file.backup
Windows-BetriebssystemeMit diesen Optionen können Sie eine Datei oder Dateigruppe von den Sicherungsservices ausschließen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemeexclude, exclude.backup, exclude.file, exclude.file.backup

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMit diesen Optionen können Sie eine Datei oder Dateigruppe von den Sicherungsservices und von den Speicherverwaltungsservices (wenn der HSM-Client installiert ist) ausschließen. Die Option exclude.backup schließt Dateien nur von der normalen Sicherung aus, nicht von HSM.

exclude.archive

Schließt eine dem Muster entsprechende Datei oder Dateigruppe *nur* von den Archivierungsservices aus.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemeexclude.attribute.symlink

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSchließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt (Aliasnamen gelten für Mac OS X), nur von der Sicherungsverarbeitung aus.

Mac OS X-BetriebssystemeAnmerkung: Bei Mac OS X sind Aliasnamen ausgeschlossen.

exclude.compression

Schließt Dateien von der Komprimierungsverarbeitung aus, wenn die Option compression auf yes gesetzt ist. Diese Option gilt für Sicherungen und Archivierungen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme exclude.dedup

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeSchließt Dateien von der clientseitigen Datendeduplizierung aus. Zum Steuern einer clientseitigen Operation für die Datendeduplizierung können Sie ieobjtype als Wert der Option exclude.dedup angeben.
Gültige Parameter für ieobjtype sind:

- File
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeImage
- Windows-BetriebssystemeSYSTEMState
- Windows-BetriebssystemeAsr

Der Standardwert ist File.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemeexclude.dir

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSchließt ein Verzeichnis, seine Dateien sowie alle zugehörigen Unterverzeichnisse und ihre Dateien von der Sicherungsverarbeitung aus. Beispiel: Die Anweisung `exclude.dir /test/dan/data1` schließt das Verzeichnis `/test/dan/data1`, dessen Dateien und Unterverzeichnisse sowie die Dateien in den Unterverzeichnissen aus.

Wenn Sie ein zuvor eingeschlossenes Verzeichnis ausschließen, kennzeichnet der Server vorhandene Sicherungsversionen der darin enthaltenen Dateien und Verzeichnisse während der nächsten Teilsicherung als verfallen. Verwenden Sie diese Option, um einen Abschnitt Ihrer Daten auszuschließen, die keine zugrunde liegende Dateien für die Sicherung aufweisen.

Anmerkung: Vermeiden Sie die Ausführung einer selektiven Sicherung oder einer partiellen Teilsicherung für eine einzelne Datei innerhalb eines ausgeschlossenen Verzeichnisses. Bei der nächsten Ausführung einer Teilsicherung verfallen alle Dateien, die auf diese Art gesichert wurden.

Windows-Betriebssystemeexclude.dir

Windows-BetriebssystemeSchließt ein Verzeichnis, seine Dateien sowie alle zugehörigen Unterverzeichnisse und ihre Dateien von der Sicherungsverarbeitung aus. Beispiel: Die Anweisung `exclude.dir c:\test\dan\data1` schließt das Verzeichnis `c:\test\dan\data1`, dessen Dateien und Unterverzeichnisse sowie die Dateien in den Unterverzeichnissen aus.

Wenn Sie ein zuvor eingeschlossenes Verzeichnis ausschließen, kennzeichnet der Server vorhandene Sicherungsversionen der darin enthaltenen Dateien und Verzeichnisse während der nächsten Teilsicherung als verfallen. Verwenden Sie diese Option, um einen Abschnitt Ihrer Daten auszuschließen, die keine zugrunde liegende Dateien für die Sicherung aufweisen.

Anmerkung: Vermeiden Sie die Ausführung einer selektiven Sicherung oder einer partiellen Teilsicherung für eine einzelne Datei innerhalb eines ausgeschlossenen Verzeichnisses. Bei der nächsten Ausführung einer Teilsicherung verfallen alle Dateien, die auf diese Art gesichert wurden.
Anmerkung: Wenn Sie eine Ausschlussanweisung ohne Angabe eines Laufwerkbuchstabens definieren, z. B. `exclude.dir code`, wird das Verzeichnis `code` auf allen Laufwerken von der Verarbeitung ausgeschlossen.

exclude.encrypt

Schließt die angegebenen Dateien von der Verschlüsselungsverarbeitung aus. Diese Option hat keine Auswirkungen darauf, ob Dateien von der Sicherungs- oder Archivierungsverarbeitung ausgeschlossen werden, sondern nur, ob sie von der Komprimierungsverarbeitung ausgeschlossen werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemeexclude.fs

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSchließt Dateisysteme, die mit dem angegebenen Muster übereinstimmen, von Sicherungsoperationen, Imageteilsicherungsoperationen und Archivierungsoperationen aus. Wenn Dateien aus den ausgeschlossenen Dateisystemen jemals gesichert wurden, findet kein erneutes Binden für die Verwaltungsklasse und keine Verfallsverarbeitung für gelöschte Dateien statt. Vorhandene Sicherungsversionen verbleiben jedoch auf dem Server und unterliegen den Einstellungen zugeordneter Verwaltungsklassen. Die Dateien, die zuvor von den ausgeschlossenen Dateisystemen archiviert wurden, verbleiben als Archivierungskopien auf dem Server.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie Option exclude.fs verhindert NICHT die Sicherung oder Archivierung virtueller Mountpunkte, die Unterverzeichnisse des ausgeschlossenen Dateisystems sind.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeVerwenden Sie exclude.image, um Dateisysteme von Imagegesamtsicherungsoperationen auszuschließen.

AIX-BetriebssystemeOracle Solaris-Betriebssystemeexclude.fs.nas
AIX-BetriebssystemeOracle Solaris-BetriebssystemeBei Verwendung im Befehl backup nas werden Dateisysteme auf dem NAS-Dateiserver von der Imagesicherung ausgeschlossen. Der NAS-Knotenname muss vor dem Dateisystemnamen stehen, z. B.: `netappsj1/vol/vol1`. Um den Ausschluss auf alle NAS-Knoten anzuwenden, müssen Sie den NAS-Knotennamen durch ein Platzhalterzeichen ersetzen, z. B.: `*/vol/vol1`. Der Befehl backup nas ignoriert alle anderen Ausschlussanweisungen einschließlich der Anweisungen exclude.fs und exclude.dir. Diese Option ist *nur* für AIX- und Solaris-Clients gültig.

Windows-Betriebssystemeexclude.fs.nas
Windows-BetriebssystemeBei Verwendung im Befehl backup nas werden Dateisysteme auf dem NAS-Dateiserver von der Imagesicherung ausgeschlossen. Der NAS-Knotenname muss vor dem Dateisystemnamen stehen, z. B.: `netappsj1/vol/vol1`. Um den Ausschluss auf alle NAS-Knoten anzuwenden, müssen Sie den NAS-Knotennamen durch ein Platzhalterzeichen ersetzen, z. B.: `*/vol/vol1`. Der Befehl backup nas ignoriert alle anderen Ausschlussanweisungen einschließlich Anweisungen exclude.dir. Diese Option ist für alle Windows-Clients gültig.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemeexclude.image
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Schließt angehängte Dateisysteme und unformatierte logische Datenträger, die dem angegebenen Muster entsprechen, von den Imagegesamtsicherungsoperationen aus. Diese Option ist nur für AIX-, Solaris- und alle Linux-Clients gültig.Verwenden Sie exclude.fs, um Dateisysteme von Imageteilsicherungsoperationen auszuschließen.
Einschränkung: Diese Option gilt nicht für Mac OS X.

Windows-Betriebssysteme

Tabelle 1. Systemservicekomponenten und zugehörige Schlüsselwörter

Komponente	**Schlüsselwort**
Intelligenter Hintergrundübertragungsdienst	BITS
Ereignisprotokoll	EVENTLOG
Removable Storage Management	RSM
Clusterdatenbank	CLUSTERDB
Ferner Speicherservice	RSS
Terminal Server-Lizenzierung	TLS
Windows Management Instrumentation (WMI)	WMI
IIS-Metabasis (IIS = Internet Information Services, Internetinformationsservices)	IIS
DHCP-Datenbank	DHCP
Wins-Datenbank	WINSDB

Parameter

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMuster
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt die Datei oder Dateigruppe an, die ausgeschlossen werden soll.
Anmerkung: Für NAS-Dateisysteme: Sie müssen den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Ausschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, bezieht sich das identifizierte Dateisystem auf den NAS-Knotennamen, der in der Clientsystemoptionsdatei (dsm.sys) oder in der Befehlszeile angegeben ist.

Wenn das Muster mit einem einfachen oder doppelten Anführungszeichen beginnt oder eingebettete Leerzeichen oder Gleichheitszeichen enthält, muss der Wert in einfache (') oder doppelte (") Anführungszeichen eingeschlossen werden. Die Anführungszeichen am Anfang und am Ende müssen identisch sein.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeFür die Option exclude.image ist das Muster der Name eines angehängten Dateisystems oder eines unformatierten logischen Datenträgers.

Windows-BetriebssystemeMuster
Windows-BetriebssystemeGibt die Datei oder Dateigruppe an, die ausgeschlossen werden soll.
Anmerkung: Für NAS-Dateisysteme: Sie müssen den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Ausschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, bezieht sich das identifizierte Dateisystem auf den NAS-Knotennamen, der in der Clientoptionsdatei (dsm.opt) oder in der Befehlszeile angegeben ist.

Wenn das Muster mit einem einfachen oder doppelten Anführungszeichen beginnt oder eingebettete Leerzeichen oder Gleichheitszeichen enthält, muss der Wert in einfache (') oder doppelte (") Anführungszeichen eingeschlossen werden. Die Anführungszeichen am Anfang und am Ende müssen identisch sein.

- Für die Option exclude.image ist das Muster der Name eines Dateisystems oder eines unformatierten logischen Datenträgers.

Beispiele

Optionsdatei:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
exclude /unix/
exclude /.../core
exclude /home/jones/proj1/*
exclude.archive /.../core
exclude.backup /home/jones/proj1/devplan/
exclude.dir /home/jones/tmp
exclude.backup /users/home1/file1
exclude.image /usr/*/*
exclude.encrypt /users/home2/file1
exclude.compression /home/gordon/proj1/*
exclude.fs.nas  netappsj/vol/vol0
exclude.attribute.symlink /.../*
exclude.dedup /Users/Administrator/Documents/Important/.../*
```

Windows-Betriebssysteme

```
exclude ?:\...\swapper.dat
exclude "*:\ea data. sf"
exclude ?:\io.sys
exclude ?:\...\spart.par
exclude c:\*\budget.fin
exclude c:\devel\*
exclude.dir c:\home\jodda
exclude.archive c:\home\*.obj
exclude.encrypt c:\system32\mydocs\*
exclude.compression c:\test\file.txt

exclude.fs.nas  netappsj/vol/vol0
exclude.dedup c:\Users\Administrator\Documents\Important\...\*
exclude.dedup e:\*\* ieobjtype=image
exclude.dedup ALL ieobjtype=systemstate
exclude.dedup ALL ieobjtype=ASR
```

Befehlszeile:

Nicht zutreffend.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie Verarbeitung symbolischer Verbindungen und Aliasnamen steuern
  Der Client für Sichern/Archivieren behandelt symbolische Verbindungen und Aliasnamen (Aliasnamen gelten nur für Mac OS X) als tatsächliche Dateien und sichert sie. Die Datei, auf die durch die symbolische Verbindung verwiesen wird, wird jedoch nicht gesichert. In einigen Fällen können symbolische Verbindungen problemlos erneut erstellt werden und müssen nicht gesichert werden.
- Steuerung der Komprimierungsverarbeitung
  In diesem Abschnitt sind einige Hinweise aufgeführt, die Sie beachten sollten, wenn bestimmte Dateien oder Dateigruppen während einer Sicherungs- oder Archivierungsoperation von der Komprimierungsverarbeitung ausgeschlossen werden sollen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
  Windows-BetriebssystemeVerarbeitung von NAS-Dateisystemen
  Mithilfe der Option exclude.fs.nas können Sie Dateisysteme von der NAS-Imagesicherungsverarbeitung ausschließen.
- Linux-BetriebssystemeWindows-BetriebssystemeAusschlussoptionen für virtuelle Maschinen
  Einschluss- und Ausschlussoptionen für virtuelle Maschinen wirken sich auf das Verhalten von Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen aus. Diese Optionen werden vor allen Befehlszeilenoptionen verarbeitet. Daher können Optionen in der Befehlszeile Optionen überschreiben, die in den Einschluss- oder Ausschlussoptionen für virtuelle Maschinen angegebenen sind. Informationen zu den Optionen finden Sie in der jeweiligen Optionsbeschreibung.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme

Die Verarbeitung symbolischer Verbindungen und Aliasnamen steuern

Der Client für Sichern/Archivieren behandelt symbolische Verbindungen und Aliasnamen (Aliasnamen gelten nur für Mac OS X) als tatsächliche Dateien und sichert sie. Die Datei, auf die durch die symbolische Verbindung verwiesen wird, wird jedoch nicht gesichert. In einigen Fällen können symbolische Verbindungen problemlos erneut erstellt werden und müssen nicht gesichert werden.

Darüber hinaus kann durch das Sichern dieser symbolischen Verbindungen die Sicherungsverarbeitungszeit zunehmen und ein wesentlicher Bereich des Speichers auf dem IBM Spectrum Protect-Server eingenommen werden. Sie können die Option exclude.attribute.symlink verwenden, um eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen handelt, von der Sicherungsverarbeitung auszuschließen. Falls notwendig, können Sie mithilfe der Option include.attribute.symlink symbolische Verbindungen innerhalb einer breiten Gruppe ausgeschlossener Dateien für die Sicherungsverarbeitung einschließen.

Sollen beispielsweise alle symbolischen Verbindungen von der Sicherungsverarbeitung ausgeschlossen werden, mit Ausnahme derjenigen, die sich unter dem Verzeichnis `/home/spike` befinden, geben Sie die folgenden Anweisungen in Ihre Datei dsm.sys ein:

```
exclude.attribute.symlink  /.../*
include.attribute.symlink /home/spike/.../*
```

Zugehörige Verweise:
Einschlussoptionen

Steuerung der Komprimierungsverarbeitung

In diesem Abschnitt sind einige Hinweise aufgeführt, die Sie beachten sollten, wenn bestimmte Dateien oder Dateigruppen während einer Sicherungs- oder Archivierungsoperation von der Komprimierungsverarbeitung ausgeschlossen werden sollen.

- Denken Sie daran, dass der Client für Sichern/Archivieren die Dateien, die verarbeitet werden, mit den in den Einschluss-/Ausschlussanweisungen angegebenen Mustern vergleicht, wobei in der Optionsdatei von unten nach oben gelesen wird.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDer Client verarbeitet exclude.fs, exclude.dir und andere Einschluss-/Ausschlussanweisungen zuerst. Danach berücksichtigt der Client alle Anweisungen exclude.compression. Wenn beispielsweise folgende Einschluss-/Ausschlussliste eingegeben wird:

  ```
  exclude /home/jones/proj1/*.*
  exclude.compression /home/jones/proj1/file.txt
  include /home/jones/proj1/file.txt
  ```

  Der Client prüft die Anweisungen (von unten nach oben gelesen) und stellt fest, dass die Datei `/home/jones/proj1/file.txt` ein Kandidat für die Sicherung, jedoch kein Kandidat für die Komprimierungsverarbeitung ist.

- Windows-BetriebssystemeDer Client verarbeitet exclude.dir und andere Einschluss-/Ausschlussanweisungen zuerst. Danach berücksichtigt der Client alle Anweisungen exclude.compression. Wenn beispielsweise folgende Einschluss-/Ausschlussliste eingegeben wird:

  ```
  exclude c:\test\*.*
  exclude.compression c:\test\file.txt
  include c:\test\file.txt
  ```

  Der Client prüft die Anweisungen (von unten nach oben gelesen) und stellt fest, dass die Datei `c:\test\file.txt` ein Kandidat für die Sicherung, jedoch kein Kandidat für die Komprimierungsverarbeitung ist.

- Die Komprimierungsverarbeitung von Einschluss-/Ausschlussdateien ist nur für die Sicherungs- und Archivierungsverarbeitung gültig. Die Option exclude.compression hat keine Auswirkungen darauf, ob Dateien von der Sicherungs- oder Archivierungsverarbeitung ausgeschlossen werden, sondern nur, ob sie von der Komprimierungsverarbeitung ausgeschlossen werden.

Zugehörige Verweise:
Compression
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Verarbeitung von NAS-Dateisystemen

Mithilfe der Option exclude.fs.nas können Sie Dateisysteme von der NAS-Imagesicherungsverarbeitung ausschließen.

Linux-BetriebssystemeWindows-BetriebssystemeAnmerkung: Die Option exclude.fs.nas gilt nicht für eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz.

Für eine NAS-Dateisystemspezifikation werden folgende Konventionen verwendet:

- NAS-Knoten stellen einen eindeutigen Knotentyp dar. Der Name des NAS-Knotens identifiziert einen NAS-Dateiserver und seine Daten eindeutig für den Client für Sichern/Archivieren. Sie können den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Ausschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, gilt das angegebene Dateisystem für alle NAS-Dateiserver.
- Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: `/vol/vol0`.

Geben Sie beispielsweise folgende Ausschlussanweisung an, um `/vol/vol1` auf allen NAS-Knoten von den Sicherungsservices auszuschließen:

```
exclude.fs.nas */vol/vol1
```

Linux-BetriebssystemeWindows-Betriebssysteme

Ausschlussoptionen für virtuelle Maschinen

Einschluss- und Ausschlussoptionen für virtuelle Maschinen wirken sich auf das Verhalten von Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen aus. Diese Optionen werden vor allen Befehlszeilenoptionen verarbeitet. Daher können Optionen in der Befehlszeile Optionen überschreiben, die in den Einschluss- oder Ausschlussoptionen für virtuelle Maschinen angegebenen sind. Informationen zu den Optionen finden Sie in der jeweiligen Optionsbeschreibung.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

- Linux-BetriebssystemeWindows-BetriebssystemeExclude.vmdisk
  Mit der Option EXCLUDE.VMDISK wird eine Platte einer virtuellen Maschine von Sicherungsoperationen ausgeschlossen.

Zugehörige Verweise:
Exclude.vmdisk
Linux-BetriebssystemeWindows-Betriebssysteme

Fbbranch

Verwenden Sie die Option fbbranch mit dem Befehl backup fastback oder archive fastback.

Die Option fbbranch gibt die Filialen-ID des fernen FastBack-Servers an, der gesichert oder archiviert werden soll. Die Option fbbranch ist nur erforderlich, wenn der Client für Sichern/Archivieren auf dem FastBack Disaster Recovery Hub installiert ist oder wenn ein dedizierter Proxy eine Verbindung zu einem replizierten FastBack Disaster Recovery Hub-Repository herstellt. Geben Sie die Option fbbranch nicht an, wenn der Client für Sichern/Archivieren auf dem FastBack-Server installiert ist.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

Linux-BetriebssystemeKeine. Sie können diese Option nur in der Befehlszeile angeben. Diese Option kann auch auf dem Server definiert oder vom Server überschrieben werden.

Windows-BetriebssystemeKeine. Sie können diese Option nur in der Befehlszeile angeben. Diese Option kann auch auf dem Server definiert oder vom Server überschrieben werden.

Syntax

```
>>-FBBranch=--Filialen-ID--------------------------------------><
```

Parameter

Filialen-ID
Gibt die Filialen-ID des FastBack-Servers an. Der Wert ist Teil der Disaster Recovery-Konfiguration des FastBack-Servers.

Beispiele

Befehlszeile:

```
-FBBranch=oracle
```

Auf einem Client für Sichern/Archivieren, der auf dem FastBack Disaster Recovery Hub installiert ist:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=myFbServer
  -fbbranch=oracle
```

Befehlszeile:

Auf einem Client für Sichern/Archivieren, der eine Verbindung zu einem Repository auf einem fernen FastBack Disaster Recovery Hub herstellt:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=server1
  -Fbreposlocation=\\myDrHub.company.com\REP
  -fbbranch=oracle
```

Wenn die Option fbbranch auf einer Workstation des Clients für Sichern/Archivieren angegeben wird, die auf dem FastBack-Server installiert ist, wird die Option fbbranch ignoriert.

Linux-BetriebssystemeWindows-Betriebssysteme

Fbclientname

Verwenden Sie die Option fbclientname mit dem Befehl backup fastback oder archive fastback.

Mit der Option fbclientname können Sie den Namen eines Clients oder mehrere durch Kommas getrennte Namen von Clients in FastBack angeben, die vom Sicherungsproxy gesichert oder archiviert werden sollen. Die Werte für die Option fbclientname sind ungültig, wenn mehrere Maßnahmen in der Option fbpolicyname angegeben sind.

Sie können keine Leerzeichen in den Werten der Option fbclientname angeben.

Wenn Sie keine Werte für die Option fbvolumename angeben, werden alle Datenträger von allen FastBack-Clients in der angegebenen Maßnahme gesichert. Wenn Sie mehrere FastBack-Clients in der Option fbclientname angeben, können Sie keine Werte für die Option fbvolumename angeben.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

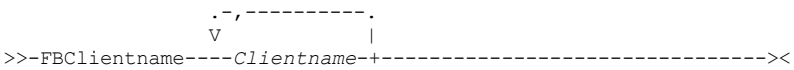
Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

Linux-BetriebssystemeKeine. Sie können diese Option nur in der Befehlszeile angeben.

Windows-BetriebssystemeKeine. Sie können diese Option nur in der Befehlszeile angeben. Diese Option kann auch auf dem Server definiert oder vom Server überschrieben werden.

Syntax



Parameter

Clientname
: Gibt den/die Namen eines oder mehrerer FastBack-Clients an. Sie können bis zu 10 FastBack-Clientnamen angeben.

Wichtig:

Wenn Sie den Befehl archive fastback oder backup fastback angeben:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBCLientName angegeben werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Sie müssen immer die Option FBReposLocation für Linux angeben.

Beispiele

Linux-BetriebssystemeBefehlszeile:
Linux-Betriebssysteme

```
dsmc backup fastback -fbpolicyname=Policy1
  -fbclientname=fbclient1,fbclient2
  -fbserver=myFbServer
  -fbreposlocation=/mnt/FBLocation
```

Sichert alle Datenträger für die FastBack-Clients fbclient1 und fbclient2, die sich in der Maßnahme Policy1 befinden.

Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme

```
dsmc backup fastback -fbpolicyname=Policy1
  -fbclientname=fbclient1,fbclient2
  -fbserver=myFbServer
  -fbreposlocation=\\myFbServer.company.com\REP
```

Sichert alle Datenträger für die FastBack-Clients fbclient1 und fbclient2, die sich in der Maßnahme Policy1 befinden.

Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme

```
dsmc backup fastback -fbpolicyname=Policy1
  -fbclientname=fbclient1
  -fbvolume=c:,f: -fbserver=myFbServer
  -fbreposlocation=\\myFbServer.company.com\REP
```

Sichert die Datenträger C:\ und F:\ für den FastBack-Client fbclient1, der sich in der Maßnahme Policy1 befindet.

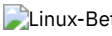

Windows-BetriebssystemeBefehlszeile:


Windows-Betriebssysteme

```
dsmc backup fastback -fbpolicyname=Policy1
  -fbclientname=fbWindowsClient,fbLinuxClient
  -fbserver=myFbServer
  -fbreposlocation=\\myFbServer.company.com\REP
```

Sichert alle Datenträger für den FastBack-Client `fbWindowsClient`, der sich in der Maßnahme Policy1 befindet.

Die Datenträger für den Linux FastBack-Client `fbLinuxClient` werden nicht vom Windows-Client für Sichern/Archivieren gesichert. Zum Sichern oder Archivieren der Datenträger eines Linux FastBack-Clients müssen Sie den Linux-Client für Sichern/Archivieren verwenden.


Linux-Betriebssysteme 
Windows-Betriebssysteme

Fbpolicyname

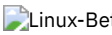
Verwenden Sie die Option fbpolicyname mit dem Befehl backup fastback oder archive fastback.

Mit der Option fbpolicyname können Sie den Namen einer Maßnahme oder mehrere durch Kommas getrennte Namen von Maßnahmen in FastBack angeben, die vom Sicherungsproxy gesichert oder archiviert werden sollen. Sie müssen mindestens einen Maßnahmennamen angeben. Mehrere Maßnahmennamen können Sie über eine durch Kommas begrenzte Liste von Maßnahmen angeben. Es gibt keinen Standardwert.

Wenn mindestens ein FB-Maßnahmenname Leerzeichen enthält, müssen Sie die Namen in Anführungszeichen einschließen. Hier ein Beispiel: "FB Policy NAME1, FBPolicy Name 2".

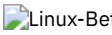
Wenn Sie keine Werte für die Optionen fbclientname und fbvolumename angeben, werden alle Datenträger von allen FastBack-Clients in den angegebenen Maßnahmen gesichert. Wenn Sie mehrere Maßnahmen in der Option fbpolicyname angeben, können Sie keine Werte für die Optionen fbclientname und fbvolumename angeben.


WindowsWenn eine Maßnahmenspezifikation sowohl Windows als auch Linux FastBack-Clients enthält, werden nur die Windows-Datenträger vom Windows-Client für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gesichert oder archiviert.


LinuxWenn eine Maßnahmenspezifikation sowohl Windows als auch Linux FastBack-Clients enthält, werden nur die Linux-Datenträger vom Linux-Client für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gesichert oder archiviert.

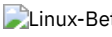
Bei Ausgabe des Befehls dsmc sollte mindestens eine Momentaufnahme für die zu archivierenden oder zu sichernden FastBack-Maßnahmen im FastBack-Repository vorhanden sein.

Unterstützte Clients


LinuxDiese Option ist für Linux x86_64-Clients gültig.


WindowsDiese Option ist für alle Windows-Clients gültig.

Optionsdatei


LinuxKeine. Sie können diese Option nur in der Befehlszeile angeben.


WindowsKeine. Sie können diese Option nur in der Befehlszeile angeben. Diese Option kann auch auf dem Server definiert oder vom Server überschrieben werden.

Syntax

```
                .-,-------------.
                V               |
>>-FBPolicyname----Maßnahmenname-+----------------------------><
```

Parameter

Maßnahmenname
: Gibt die Namen der FastBack-Maßnahmen an. Sie können bis zu 10 FastBack-Maßnahmennamen angeben.

Wichtig:

Wenn Sie den Befehl archive fastback oder backup fastback angeben:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBCLientName angegeben werden. Sie müssen genau einen Wert für FBClientName angeben. Der Wert kann nicht übergangen werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Sie müssen immer die Option FBReposLocation für Linux angeben.

Beispiele

Befehlszeile:

```
dsmc backup fastback -fbpolicyname=Policy1,Policy2,Policy3
  -fbserver=myFbServer
  -fbreposlocation=\\myFbServer.company.com\REP
```

Sichert alle Datenträger für alle FastBack-Clients, die sich in den Maßnahmen Policy1, Policy2 und Policy3 befinden.

Zum Angeben von Maßnahmennamen mit Leerzeichen schließen Sie diese in Anführungszeichen ein, z. B.:

```
-fbpolicyname="Policy 1,Policy2,Policy3"
```

Linux-BetriebssysemeWindows-Betriebssysteme

Fbreposlocation

Verwenden Sie die Option fbreposlocation mit dem Befehl backup fastback oder archive fastback.

Die Option fbreposlocation gibt die Position des Tivoli Storage Manager FastBack-Repositorys an, zu dem der Proxy des Clients für Sichern/Archivieren eine Verbindung herstellen soll, um Tivoli Storage Manager FastBack-Shellbefehle auszugeben, die zum Bereitstellen der entsprechenden Momentaufnahmen erforderlich sind.

Linux-BetriebssystemeDiese Option ist auf Linux-Systemen erforderlich. Es gibt keine Standardposition.

Linux-BetriebssystemeWenn Sie die Option fbreposlocation für eine Momentaufnahme auf dem FastBack-Server angeben, müssen Sie das Format Servername@WORKGROUP verwenden.

Linux-BetriebssystemeFür die Angabe der FastBack-Repository-Position auf dem FastBack Disaster Recovery Hub gibt es zwei Möglichkeiten:

- Geben Sie die vollständige Repository-Position über die Option `-fbreposlocation=\\DR_Hub\rep_server` an. Wenn Sie dieses Format verwenden, ist DR_Hub der Name der FastBack Disaster Recovery Hub-Maschine und rep_server ist der Name des replizierten FastBack-Server-Repositorys auf dem DR Hub.
- Geben Sie die Repository-Position über eine Kombination der Optionen -fbreposlocation= und -fbbranch an. Wenn Sie dieses Format verwenden, geben Sie die Position des DR Hub-Repositorys über die Option `-fbreposlocation=DR_Hub@WORKGROUP` und den Namen des replizierten FastBack-Server-Repositorys auf dem DR Hub über die Option -fbranch an.

Windows-BetriebssystemeAuf Windows-Systemen ist die Angabe der Option fbreposlocation nicht erforderlich, wenn der Client für Sichern/Archivieren auf einem DR Hub-Server oder der FastBack-Server-Workstation installiert ist. Ist der Client für Sichern/Archivieren auf einem dedizierten Client-Proxy installiert, ist die Option fbreposlocation für die Repository-Position erforderlich.

Windows-BetriebssystemeWenn Sie die Option fbreposlocation für den FastBack Disaster Recovery Hub angeben, geben Sie nur das Basisverzeichnis des DR Hub-Repositorys mit dieser Option an. Verwenden Sie anschließend die Option fbbranch, um die Filialen-ID des zu sichernden Servers anzugeben. Wenn Sie die Option fbreposlocation für den FastBack-Server angeben, müssen Sie das Format `\\<fbserver>\REP` verwenden. Verwenden Sie in diesem Fall nicht die Option fbbranch.

Linux-BetriebssystemeBei Verwendung des Formats `-fbr=\\<fbserver>\REP` müssen Sie zwei umgekehrte Schrägstriche vor der Zeichenfolge `<fbserver>` und einen umgekehrten Schrägstrich vor der Zeichenfolge 'REP' angeben, wenn Sie den Client für Sichern/Archivieren im interaktiven Modus ausführen. Wenn Sie dieses Format als Linux-Befehl `dsmc backup fastback -fbr=\\\\<fbserver>\\REP` verwenden, müssen Sie vier umgekehrte Schrägstriche vor der Zeichenfolge `<fbserver>` und zwei umgekehrte Schrägstriche vor der Zeichenfolge 'REP' angeben. Die Ursache dafür ist, dass die Linux-Shell einen umgekehrten Schrägstrich als Escapezeichen interpretiert; der erste umgekehrte Schrägstrich wird als Escapezeichen für den darauffolgenden umgekehrten Schrägstrich behandelt.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

Keine. Sie können diese Option nur in der Befehlszeile angeben. Diese Option kann auch auf dem Server definiert oder vom Server überschrieben werden.

Syntax

```
>>-FBReposlocation--Repository-Position------------------------><
```

Parameter

Repository-Position
Gibt die Tivoli Storage Manager FastBack-Repository-Position an.

Beispiele

Linux-BetriebssystemeBefehlszeile:
Linux-Betriebssysteme

```
dsmc backup fastback -fbpolicyname=Policy1
  -fbclientname=fbclient1,fbclient2  -fbserver=myFbDrHub
  -fbreposlocation=\\myFbDrHub\rep_myFbServer
```

Anmerkung: Da Linux nur als dedizierte Proxy-Konfiguration unterstützt wird, ist unter Linux immer eine Repository-Position erforderlich.

Linux-BetriebssystemeBefehlszeile:
Linux-Betriebssysteme

```
dsmc backup fastback -fbpolicyname=Policy1
  -fbclientname=fbclient1,fbclient2  -fbserver=myFbDrHub
  -fbreposlocation=myFbDrHub  -fbbranch=rep_myFbServer
```

Anmerkung: Da Linux nur als dedizierte Proxy-Konfiguration unterstützt wird, ist unter Linux immer eine Repository-Position erforderlich.

Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme

Die Option fbreposlocation ist nur auf einer dedizierten Proxy-Maschine erforderlich. Wenn die Option fbreposlocation auf einer Maschine angegeben wird, auf der der FastBack-Server oder FastBack Disaster Recovery Hub installiert ist, wird sie ignoriert.

Verwenden Sie den folgenden Befehl, wenn der dedizierte IBM Spectrum Protect-Proxy-Client eine Verbindung zu einem fernen Tivoli Storage Manager FastBack-Server-Repository herstellt:

```
dsmc backup fastback -fbpolicyname="Policy 1" -fbserver=myFbServer
  -fbreposlocation=\\myFbServer.company.com\REP
```

Eine Repository-Position ist erforderlich.

myFbServer ist der kurze Hostname der Maschine, auf der der FastBack-Server installiert ist.

Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme

Verwenden Sie den folgenden Befehl, wenn der dedizierte IBM Spectrum Protect-Proxy-Client eine Verbindung zu einem fernen Repository auf dem FastBack Disaster Recovery Hub herstellt:

```
dsmc backup fastback -fbpolicyname="Policy 1" -fbserver=myFbServer
  -fbreposlocation=\\myfbdrhub.company.com\REP
  -fbbranch=aFbServerBranch
```

Eine Repository-Position ist erforderlich.

Der Parameter myFbServer gibt den kurzen Hostnamen des FastBack-Servers an, dessen FastBack-Filiale über die Option FBBranch angegeben wird.

Die Option fbbranch gibt die Filialen-ID des FastBack-Servers auf dem Disaster Recovery Hub an.

Linux-BetriebssystemeWindows-Betriebssysteme

Fbserver

Verwenden Sie die Option fbserver mit dem Befehl backup fastback oder archive fastback.

Mit der Option fbserver können Sie den kurzen Hostnamen der Tivoli Storage Manager FastBack-Server-Workstation angeben, die der Eigner des durch die Option fbreposlocation angegebenen Repositorys ist. Für einen DR Hub gibt die Option fbserver den Kurznamen der FastBack-Server-Workstation an, zu deren Repository einer Filiale der Client für Sichern/Archivieren eine Verbindung herstellt.

Die Option fbserver stellt einen Schlüssel zum Abrufen der Benutzerberechtigungsnachweise dar, die erforderlich sind, um für die Mountverarbeitung eine Verbindung zum FastBack-Server-Repository oder DR Hub-Server-Repository herzustellen.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

Linux-BetriebssystemeKeine. Sie können diese Option nur in der Befehlszeile angeben.

Windows-BetriebssystemeKeine. Sie können diese Option nur in der Befehlszeile angeben. Diese Option kann auch auf dem Server definiert oder vom Server überschrieben werden.

Syntax

```
>>- -FBServer-- --Servername-----------------------------------><
```

Parameter

Servername
: Gibt den kurzen Hostnamen der Maschine an, auf der der FastBack-Server installiert ist.

Beispiele

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeDer Client für Sichern/Archivieren ist auf einer Linux-Proxy-Client-Maschine installiert. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle Linux FastBack-Clients zu archivieren, die für die FastBack-Maßnahme Policy1 definiert sind:

```
dsmc archive fastback -fbpolicyname=Policy1
  -fbserver=myfbserver
  -fbreposlocation=myfbserver@WORKGROUP
```

Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

Der FastBack-Servername -myfbserver ist der kurze Hostname des FastBack-Servers, auf dem sich das Repository befindet.

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeDas Repository rep_server1 befindet sich auf dem FastBack Disaster Recovery Hub myFbDrHub.

```
dsmc archive fastback -fbpolicyname="Policy 1"
  -fbserver=myFbDrHub
  -fbreposlocation=\\myFbDrHub\rep_server1
```

Der FastBack-Servername -myFbDrHub ist der kurze Hostname des FastBack Disaster Recovery Hub-Servers, auf dem sich das Repository befindet.

Die Option -fbreposlocation gibt die Position des Repositorys an. Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

In diesem Fall sollte -fbserver auf den kurzen Hostnamen des FastBack DR Hub verweisen.

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeAlle Datenträger, die durch die FastBack-Maßnahme mit dem Namen policy1 geschützt sind, für den FastBack-Server mit dem Namen basil archivieren:

```
dsmc archive fastback -Fbpolicyname=policy1
  -FBServer=basil -ARCHMC="my_tsm_mgmt_class"
  -fbreposlocation=basil@WORKGROUP
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeDer IBM Spectrum Protect-Client für Sichern/Archivieren wird auf einer FastBack-Servermaschine mit dem Kurznamen myFbServer ausgeführt:

```
dsmc archive fastback -fbpolicyname=Policy1 -fbserver=myFbServer
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeDer IBM Spectrum Protect-Client für Sichern/Archivieren wird auf der FastBack Disaster Recovery Hub-Maschine ausgeführt und stellt eine Verbindung zu dem Repository branch1 einer Filiale des FastBack-Servers her. Der kurze Hostname des FastBack-Servers lautet myFbServer:

```
dsmc archive fastback -fbpolicyname=Policy1 -fbserver=myFbServer
  -fbbranch=branch1
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeDer Client für Sichern/Archivieren wird auf einer dedizierten Proxy-Maschine ausgeführt und stellt eine Verbindung zu einem fernen FastBack-Server-Repository her. Der FastBack-Server ist auf einer Maschine mit dem Kurznamen myFbServerMachine installiert:

```
dsmc archive fastback -fbpolicyname=Policy1 -fbserver=myFbServerMachine
  -fbreposlocation=\\myFbServerMachine.company.com\Rep
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeDer Client für Sichern/Archivieren wird auf einer dedizierten Proxy-Maschine ausgeführt und stellt eine Verbindung zu einem fernen FastBack-Rository auf dem FastBack DR Hub her. Der FastBack-Server mit der Filialen-ID branch1 ist auf einer Maschine mit dem Kurznamen myFbServer installiert.

```
dsmc backup fastback -fbpolicyname=Policy1 -fbserver=myFbServer
  -fbreposlocation=\\myDrHubMachine.company.com\Rep
  -fbbranch=branch1
```

Linux-Betriebssysteme Windows-Betriebssysteme

Fbvolumename

Verwenden Sie die Option fbvolumename mit dem Befehl backup fastback oder archive fastback.

Mit der Option fbvolumename können Sie den Namen eines Datenträgers oder mehrere durch Kommas getrennte Namen von Datenträgern in Tivoli Storage Manager FastBack angeben, die vom Sicherungsproxy gesichert oder archiviert werden sollen. Werte für die Option fbvolumename sind nicht gültig, wenn mehrere FastBack-Clients in der Option fbclientname angegeben werden.

Wenn Sie mehrere FastBack-Clients in der Option fbclientname angeben, können Sie keine Werte für die Option fbvolumename angeben.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

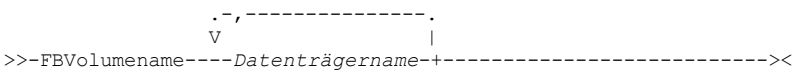
Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

Linux-BetriebssystemeKeine. Sie können diese Option nur in der Befehlszeile angeben.

Windows-BetriebssystemeKeine. Sie können diese Option nur in der Befehlszeile angeben. Diese Option kann auch auf dem Server definiert oder vom Server überschrieben werden.

Syntax



Parameter

Datenträgername
: Gibt die Namen der Tivoli Storage Manager FastBack-Datenträger an. Sie können bis zu 10 FastBack-Datenträgernamen angeben.

Wichtig:

Wenn Sie den Befehl archive fastback oder backup fastback angeben:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.

5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBCLientName angegeben werden. Sie müssen genau einen Wert für FBClientName angeben. Der Wert kann nicht übergangen werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Linux-BetriebssystemeSie müssen die Option FBReposLocation angeben.

Beispiele

Linux-BetriebssystemeBefehlszeile:
Linux-Betriebssysteme

```
dsmc backup fastback -fbpolicyname=Policy1 -fbclientname=client1
  -fbvolumename=data1,data2 -fbserver=myFbDrHub
  -fbreposlocation=\\myFbDrHub\rep_server1
```

Sichert die Datenträger data1 und data2 des FastBack-Clients client1, der sich in der Maßnahme Policy1 befindet.

Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme

```
dsmc backup fastback -fbpolicyname=Policy1 -fbclientname=client1
  -fbvolumename=c:,f: -fbserver=myFbServer
  -fbreposlocation=\\myFbServer.company.com\REP
```

Sichert die Datenträger C:\ und F:\ des FastBack-Clients client1, der sich in der Maßnahme Policy1 befindet.

Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme

```
dsmc archive fastback -fbpolicyname=Policy1 -fbclientname=client1
  -fbvolumename=c:,f: -fbserver=myFbServer
  -fbreposlocation=\\myFbServer.company.com\REP
```

Archiviert die Datenträger C: und F: des FastBack-Clients client1, der sich in der Maßnahme Policy1 befindet.

Filelist

Verwenden Sie die Option filelist, um eine Liste von Dateien zu verarbeiten.

Die Option filelist können Sie in folgenden Befehlen verwenden:

- archive
- Windows-Betriebssystemebackup group
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemebackup group
- delete archive
- delete backup
- expire
- incremental
- query archive
- query backup
- restore
- retrieve
- selective

Der Client für Sichern/Archivieren öffnet die Datei, die Sie mit dieser Option angeben, und verarbeitet die darin enthaltene Liste der Dateien dem jeweiligen Befehl entsprechend. Außer für die Befehle restore und retrieve ignoriert der Client alle anderen Dateispezifikationen in der Befehlszeile, wenn Sie die Option filelist verwenden.

Für die in der Dateiliste aufgeführten Dateien (Einträge) gelten folgende Regeln:

- Jeder Eintrag muss ein vollständig qualifizierter oder relativer Pfad zu einer Datei oder einem Verzeichnis sein. Wenn Sie ein Verzeichnis in einen Dateilisteneintrag einschließen, wird das Verzeichnis gesichert, aber der Inhalt des Verzeichnisses wird nicht gesichert.
- Jeder Pfad muss in einer einzelnen Zeile angegeben werden. Eine Zeile kann nur einen Pfad enthalten.
- Pfade dürfen keine Steuerzeichen enthalten, wie beispielsweise 0x18 (STRG-X), 0x19 (STRG-Y) und 0x0A (neue Zeile).
- Standardmäßig dürfen die Pfade keine Platzhalterzeichen enthalten. Geben Sie keinen Stern (*) und kein Fragezeichen (?) in einem Pfad an. Diese Einschränkung kann durch Aktivierung der Option wildcardsareliteral außer Kraft gesetzt werden. Weitere Informationen zu dieser Option finden Sie in Wildcardsareliteral.
- Mac OS X-BetriebssystemeWindows-BetriebssystemeDie Dateiliste kann eine MBCS-Datei oder eine Unicode-Datei mit allen Unicode-Einträgen sein. Für Mac OS X kann die Dateiliste in der aktuellen Betriebssystemsprache oder in UTF-16 codiert sein.
- Wenn die Clientoption quotessareliteral definiert ist, können Hochkommas und Anführungszeichen in einer Dateispezifikation in der eigentlichen Bedeutung als Hochkommas und Anführungszeichen und nicht als Begrenzungszeichen interpretiert werden. Weitere Informationen zu dieser Option finden Sie in Quotesareliteral. Wennn quotesareliteral und wildcardsareliteral nicht definiert sind, findet die Verarbeitung von Anführungszeichen und Platzhalterzeichen wie folgt statt:

- Wenn ein Pfad oder ein Dateiname ein Leerzeichen enthält, schließen Sie den vollständigen Pfad in Anführungszeichen (") oder Hochkommas (') ein. Beispiel: "C:\My Documents\spreadsheet.xls" oder 'C:\My documents\spreadsheet.xls'.
- Enthält ein Pfad ein oder mehrere Hochkommas ('), schließen Sie den vollständigen Eintrag in Anführungszeichen (") ein. Enthält ein Pfad ein oder mehrere Anführungszeichen, schließen Sie den vollständigen Pfad in Hochkommas ein. Die Dateilistenverarbeitung unterstützt keine Pfade, die eine Mischung aus Anführungszeichen und Hochkommas einschließen.

  Die folgenden Beispiele zeigen die korrekte und die falsche Verwendung von Anführungszeichen und Hochkommas in Pfaden.

  Dieses Beispiel für einen Pfad enthält ein Hochkomma. Der Pfad muss daher in Anführungszeichen eingeschlossen werden:

  ```
  "/home/gatzby/mydir/gatzby's_report.out"
  ```

  Dieses Beispiel für einen Pfad enthält Anführungszeichen. Der Pfad muss daher in Hochkommas eingeschlossen werden:

  ```
  '/home/gatzby/mydir/"top10".out'
  ```

  Dieses Beispiel für einen Pfad enthält ein Leerzeichen. Daher muss der Pfad entweder in Anführungszeichen oder in Hochkommas eingeschlossen werden:

  ```
  "/home/gatzby/mydir/top 10.out"
  ```

  oder

  ```
  '/home/gatzby/mydir/top 10.out'
  ```

  Dieses Beispiel für einen Pfad wird für die Dateilistenverarbeitung nicht unterstützt, da der Pfad Begrenzer ohne Entsprechung (" und ') enthält:

  ```
  /home/gatzby/mydir/andy's_"top 10" report.out
  ```

  Diese Pfade werden für die Dateilistenverarbeitung nicht unterstützt, da sie Platzhalterzeichen enthalten:

  ```
  /home/gatzby*
  /home/*/20??.txt
  ```

- Alle IBM Spectrum Protect-Dateilisteneinträge, die diesen Regeln nicht entsprechen, werden ignoriert.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme
Die folgenden Beispiele sind gültige Pfade in einer Dateiliste:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

```
/home/dir/file1
/usr/tivoli/file2
/usr/avi/dir1
/fs1/dir2/file3
"/fs2/Ha Ha Ha/file.txt"
"/fs3/file.txt"
```

Windows-Betriebssysteme

```
c:\myfiles\directory\file1
c:\tivoli\mydir\yourfile.doc
..\notes\avi\dir1
..\fs1\dir2\file3
"d:\fs2\Ha Ha Ha\file.txt"
"d:\fs3\file.txt"
```

Informationen darüber, wie die Standardverarbeitung von Anführungszeichen und Platzhalterzeichen außer Kraft gesetzt wird, finden Sie in Quotesareliteral und in Wildcardsareliteral.

Sie können die Option filelist während einer OFS-Operation (OFS = Open File Support = Unterstützung offener Dateien) verwenden. In diesem Fall verarbeitet der Client die Einträge in der Dateiliste vom virtuellen und nicht vom realen Datenträger.

Wenn ein Eintrag in der Dateiliste ein Verzeichnis angibt, wird nur dieses Verzeichnis und nicht die darin enthaltenen Dateien verarbeitet.

Ist der für die Option filelist angegebene Dateiname (`Dateilistenspezifikation`) nicht vorhanden, schlägt der Befehl fehl. Der Client überspringt alle Einträge in der Dateiliste, die keine gültigen Dateien oder Verzeichnisse sind. Der Client protokolliert Fehler und die Verarbeitung wird mit dem nächsten Eintrag fortgesetzt.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeVerwenden Sie Dateispezifikationen im Befehl restore und retrieve, um das Ziel für die zurückgeschriebenen Dateilisteneinträge anzugeben. Beispiel: In dem folgenden restore-Befehl stellt die Dateispezifikation `/user/record/` das Zurückschreibungsziel für alle Einträge in der Dateiliste dar.

```
restore -filelist=/home/dir/file3 /usr/record/
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeIn dem folgenden selective-Befehl wird die Dateispezifikation `/usr/record/` jedoch ignoriert.

```
selective -filelist=/home/dir/file3 /usr/record/
```

Windows-BetriebssystemeVerwenden Sie Dateispezifikationen im Befehl restore und retrieve, um das Ziel für die zurückgeschriebenen Dateilisteneinträge anzugeben. Beispiel: In dem folgenden restore-Befehl stellt `d:\dir\` das Zurückschreibungsziel für alle Einträge in der Dateiliste dar.

```
restore -filelist=c:\filelist.txt d:\dir\
```

Windows-BetriebssystemeIn dem folgenden selective-Befehl wird die Dateispezifikation `d:\dir\` jedoch ignoriert.

```
selective -filelist=c:\filelist.txt d:\dir\
```

Wenn Sie für den Befehl delete archive oder delete backup ein Verzeichnis in einer Dateiliste angeben, wird das Verzeichnis nicht gelöscht. Dateilisten, die Sie im Befehl delete archive oder delete backup verwenden, dürfen keine Verzeichnisse enthalten.

Die Einträge in der Liste werden in der Reihenfolge der Dateiliste verarbeitet. Um eine optimale Verarbeitungsleistung zu erzielen, sollten Sie die Dateiliste nach Dateibereichsnamen und -pfad vorsortieren.

Anmerkung: Der Client sichert ein Verzeichnis möglicherweise zweimal, wenn folgende Bedingungen auftreten:

- Die Dateiliste enthält einen Eintrag für das Verzeichnis
- Die Dateiliste enthält mindestens einen Eintrag für Dateien in diesem Verzeichnis
- Es ist keine Sicherung des Verzeichnisses vorhanden

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAngenommen, Ihre Dateiliste enthält die Einträge `/home/dir/file1` und `/home/dir`. Wenn das Verzeichnis `/dir` auf dem Server nicht vorhanden ist, wird das Verzeichnis `/home/dir` ein zweites Mal an den Server gesendet.

Windows-BetriebssystemeAngenommen, Ihre Dateiliste enthält die Einträge `c:\dir0\myfile` und `c:\dir0`. Wenn das Verzeichnis `\dir0` auf dem Server nicht vorhanden ist, wird das Verzeichnis `c:\dir0` ein zweites Mal an den Server gesendet.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-FILEList = - --Dateilistenspezifikation---------------------><
```

Parameter

Dateilistenspezifikation
: Gibt die Position und den Namen der Datei an, die die Liste der Dateien enthält, die für den Befehl verarbeitet werden sollen.
Anmerkung: Wenn Sie die Option filelist in der Befehlszeile angeben, wird die Option subdir ignoriert.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme`sel -filelist=/home/avi/filelist.txt`

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`sel -filelist=c:\avi\filelist.txt`

Filename

Verwenden Sie die Option filename im Befehl query systeminfo, um den Namen einer Datei anzugeben, in der Informationen gespeichert werden sollen.

Sie können Informationen speichern, die von einen oder mehreren der folgenden Elemente zusammengestellt wurden:

- DSMOPTFILE - Der Inhalt der Datei dsm.opt
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDSMSYSFILE - Inhalt der Datei dsm.sys
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeENV - Umgebungsvariablen
- ERRORLOG - IBM Spectrum Protect-Fehlerprotokolldatei
- FILE - Attribute für den angegebenen Dateinamen.
- Windows-BetriebssystemeFILESNOTTOBACKUP - Aufzählung des Windows-Registerschlüssels:

```
HKEY_LOCAL_MACHINE\
   SYSTEM\
      CurrentControlSet\
         BackupRestore\
            FilesNotToBackup
```

Dieser Schlüssel gibt diejenigen Dateien an, die von Sicherungsprodukten nicht gesichert werden sollen. Der Befehl query inclexcl zeigt an, dass diese Dateien vom Betriebssystem ausgeschlossen sind.

- INCLEXCL - Stellt eine Liste der Einschluss/Ausschlussanweisungen in der Reihenfolge zusammen, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden.
- Windows-BetriebssystemeKEYSNOTTORESTORE - Aufzählung des Windows-Registerschlüssels:

```
HKEY_LOCAL_MACHINE\
   SYSTEM\
      ControlSet001\
         BackupRestore\
            KeysNotToRestore
```

Dieser Schlüssel gibt diejenigen Windows-Registerschlüssel an, die von Sicherungsprodukten nicht zurückgeschrieben werden sollen.

- Windows-BetriebssystemeMSINFO - Windows-Systeminformationen (Ausgabe von MSINFO32.EXE).
- OPTIONS - Optionen
- Windows-BetriebssystemeOSINFO - Name und Version des Clientbetriebssystems.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeOSINFO - Name und Version des Clientbetriebssystems (umfasst ULIMIT-Informationen für UNIX und Linux).
- POLICY - Speicherauszug der Maßnahmengruppe
- Windows-BetriebssystemeREGISTRY - IBM Spectrum Protect-bezogene Windows-Registry-Einträge.
- SCHEDLOG - Inhalt des Planungsprotokolls (normalerweise dsmsched.log.
- Windows-BetriebssystemeSFP - Liste der Dateien, die durch Windows-Systemdateischutz geschützt sind, und für jede Datei die Anzeige, ob diese Datei vorhanden ist. Diese Dateien werden als Teil des Systemobjekts SYSFILES gesichert.
- Windows-BetriebssystemeSFP=*Dateiname* - Zeigt an, ob die angegebene Datei (*Dateiname*) durch den Windows-Systemdateischutz geschützt ist. Zum Beispiel:

```
SFP=C:\WINNT\SYSTEM32\MSVCRT.DLL
```

- Windows-BetriebssystemeSYSTEMSTATE - Informationen zum Windows-Systemstatus
- AIX-BetriebssystemeCLUSTER - AIX-Clusterinformationen
- Windows-BetriebssystemeCLUSTER - Windows-Clusterinformationen

Anmerkung: Der Befehl query systeminfo ist in erster Linie als Hilfe für die IBM® Unterstützungsfunktion bei der Diagnose von Problemen gedacht. Aber Benutzer, die mit den in diesen Informationen angesprochenen Konzepten vertraut sind, finden ihn möglicherweise auch nützlich. Wenn Sie die Option console verwenden, wird keine besondere Formatierung der Ausgabe ausgeführt, um die Anzeigenhöhe oder -breite anzupassen. Aus diesem Grund ist die Konsolausgabe wegen der Länge und des Zeilenumbruchs unter Umständen schwierig zu lesen. In diesem Fall verwenden Sie die Option filename mit dem Befehl query systeminfo, damit die Ausgabe in eine Datei geschrieben wird, die anschließend an die IBM Unterstützungsfunktion übergeben werden kann.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Syntax

```
>>-FILEName = - --Ausgabedateiname-----------------------------><
```

Parameter

Ausgabedateiname
: Gibt den Namen der Datei an, in der die Informationen gespeichert werden sollen. Wird kein Dateiname angegeben, werden die Informationen standardmäßig in der Datei dsminfo.txt gespeichert.

Beispiele

Befehlszeile:

```
query systeminfo dsmoptfile errorlog -filename=tsminfo.txt
```

Filesonly

Mit der Option filesonly wird die Verarbeitung beim Sichern, Zurückschreiben, Abrufen oder Abfragen *nur* auf Dateien beschränkt.

Sie können keine Verzeichnisse vom IBM Spectrum Protect-Server zurückschreiben oder abrufen, wenn Sie die Option filesonly in den Befehlen restore oder retrieve verwenden. Falls erforderlich, werden jedoch Verzeichnisse mit Standardattributen als Platzhalter für Dateien erstellt, die zurückgeschrieben oder abgerufen werden.

Die Option filesonly können Sie auch in folgenden Befehlen verwenden:

- archive
- incremental
- query archive
- query backup
- restore
- restore backupset
- restore group
- retrieve
- selective

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-FILESOnly-------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme
Befehlszeile:
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
Windows-Betriebssysteme`dsmc incremental -filesonly`

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

Followsymbolic

Bei einer Sicherungsoperation gibt die Option followsymbolic an, ob Sie eine symbolische Verbindung als virtuellen Mountpunkt verwenden wollen. Bei einer Zurückschreibungs- oder Abrufoperation gibt die Option followsymbolic an, wie der Client für Sichern/Archivieren ein Verzeichnis zurückschreibt, dessen Name mit einer symbolischen Verbindung auf dem Zieldateisystem für die Zurückschreibung übereinstimmt.

Bei Sicherungsoperationen kann die Option followsymbolic sich auf die Einstellung der Option virtualmountpoint auswirken. Wenn Sie die Option virtualmountpoint verwenden, um eine symbolische Verbindung als virtuellen Mountpunkt anzugeben, müssen Sie auch die Option followsymbolic definieren.

Bei Zurückschreibungs- und Abrufoperationen kann followsymbolic beeinflussen, wie der Client eine symbolische Verbindung im Dateisystem verarbeitet. Definieren Sie followsymbolic nur, wenn der Client versucht, ein Verzeichnis zurückzuschreiben, dessen Name mit einer symbolischen Verbindung auf dem Zieldateisystem für die Zurückschreibung übereinstimmt.

Wenn Sie `followsymbolic=no` (den Standardwert) angeben, schreibt der Client den Inhalt des Verzeichnisses nicht zurück, sondern gibt die folgende Fehlernachricht zurück:

```
ANS4029E Fehler bei der Verarbeitung von 'Dateibereichsname Pfadname Dateiname':
Verzeichnispfad kann nicht erstellt werden; eine Datei hat denselben Namen
wie ein Verzeichnis.
```

Wenn Sie `followsymbolic=yes` angeben, schreibt der Client den Inhalt des Verzeichnisses in das Ziel der symbolischen Verbindung zurück.

Beispiel: Angenommen, der Client hat eine Datei mit dem folgenden Pfad gesichert: /fs1/dir1/subdir1/file1. Weiterhin wird angenommen, dass die symbolische Verbindung /fs1/dir1, die im Zieldateisystem für die Zurückschreibung vorhanden ist, mit dem Verzeichnis /fs88/dir88/subdir88 verbunden ist. Die Datei wird mit dem folgenden Befehl zurückgeschrieben:

```
restore /fs1/dir1/subdir1/file1
```

Wenn Sie `followsymbolic=no` angeben, schreibt der Client die Datei nicht zurück, sondern gibt die obige Fehlernachricht zurück. Wenn Sie `followsymbolic=yes` angeben, schreibt der Client file1 in das Verzeichnis /fs88/dir88/subdir88/subdir1/file1 zurück.

Wenn Sie eine symbolische Verbindung (kein Verzeichnis) zurückschreiben, deren Name mit einer symbolischen Verbindung auf dem Zieldateisystem für die Zurückschreibung übereinstimmt, schreibt der Client die symbolische Verbindung zurück.

Wird eine symbolische Verbindung als virtueller Mountpunkt verwendet, muss der Pfad zum Ziel der Verbindung in Form eines absoluten Dateipfads angegeben werden.

Verwenden Sie diese Option mit den Befehlen restore und retrieve oder in der Clientbenutzeroptionsdatei (dsm.opt).

Unterstützte Clients

Diese Option ist für alle UNIX-Clients außer Mac OS X gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                    .-No--.
>>-FOLlowsymbolic--+-----+-------------------------------------><
                    '-Yes-'
```

Parameter

No
: Einen virtuellen Mountpunkt, der eine symbolische Verbindung ist, nicht sichern. Ein Verzeichnis nicht zurückschreiben, wenn das Zieldateisystem für die Zurückschreibung eine symbolische Verbindung mit übereinstimmendem Namen enthält. Dies ist der Standardwert.

Yes
: Den Inhalt eines Verzeichnisses in das Ziel einer symbolischen Verbindung zurückschreiben.

Beispiele

Optionsdatei:
```
followsymbolic Yes
```
Befehlszeile:
```
-fol=Yes
```

Forcefailover

Mit der Option forcefailover kann eine sofortige Übernahme des Clients auf dem Sekundärserver stattfinden.

Sie können mit der Option forcefailover eine sofortige Verbindung zum Sekundärserver herstellen, auch wenn der Primärserver noch online ist. Sie können mit dieser Option beispielsweise prüfen, ob eine Übernahme des Clients für Sichern/Archivieren auf dem erwarteten Sekundärserver stattfindet.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) ein.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                    .-No--.
>>-FORCEFAILOVER--+-----+-------------------------------------><
                    '-Yes-'
```

Parameter

Yes
: Gibt an, dass der Client sofort eine Verbindung zum Sekundärserver herstellt.

No
: Gibt an, dass eine Übernahme des Clients auf dem Sekundärserver während der nächsten Anmeldung stattfindet, wenn der Primärserver nicht verfügbar ist. Dies ist der Standardwert.

Beispiele

Optionsdatei:
```
FORCEFAILOVER yes
```
Befehlszeile:
```
-FORCEFAILOVER=yes
```

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Client für automatisierte Übernahme konfigurieren

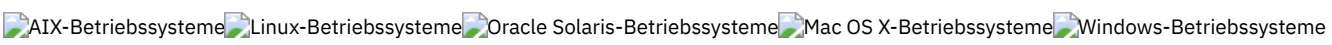
Fromdate

Mit der Option fromdate können Sie in Verbindung mit der Option fromtime ein Datum mit Uhrzeit angeben, ab dem Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.

Vor diesem Datum und dieser Zeit gesicherte oder archivierte Dateien werden nicht berücksichtigt; falls erforderlich, werden jedoch ältere Verzeichnisse berücksichtigt, um die Dateien zurückzuschreiben oder abzurufen.

Die Option fromdate ist in den folgenden Befehlen zu verwenden:

- delete backup
- query archive
- query backup
- restore
- restore group
- retrieve



Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-FROMDate = - --Datum-----------------------------------------><
```

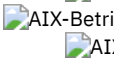
Parameter

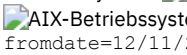
Datum
: Das Datum, ab dem nach Sicherungsversionen oder Archivierungskopien gesucht werden soll. Das Datum muss in dem mit der Option dateformat ausgewählten Format eingegeben werden.

  Wenn dateformat in einem Befehl angegeben wird, muss diese Option vor den Optionen fromdate, pitdate und todate stehen.

Beispiele

Befehlszeile:


```
dsmc query backup -fromdate=12/11/2003 "/Users/van/Documents/*"
```


Befehlszeile:


```
dsmc query backup -fromdate=12/11/2003 /home/dilbert/*
```


Befehlszeile:


```
dsmc query backup -fromdate=12/11/2003 c:\Windows\Program Files\*.exe
```

Fromnode

Mit der Option fromnode kann ein Knoten Befehle für einen anderen Knoten ausführen. Ein Benutzer auf einem anderen Knoten muss mit dem Befehl set access die Berechtigung zum Abfragen, Zurückschreiben oder Abrufen von Dateien für diesen anderen Knoten erteilen.

Die Option fromnode ist in den folgenden Befehlen zu verwenden:

- query archive
- query backup
- query filespace
- Windows-Betriebssystemequery group
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssystemequery image
- query mgmtclass
- restore
- restore group
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemerestore image
- retrieve

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Syntax

```
>>-FROMNode = - --Knoten----------------------------------------><
```

Parameter

Knoten
: Gibt den Namen des Knotens auf einer Workstation oder auf einem Dateiserver an, auf dessen Sicherungskopien oder archivierte Dateien zugegriffen werden soll.

Beispiele

Mac OS X-BetriebssystemeBefehlszeile:
: Mac OS X-Betriebssystemedsmc query archive -fromnode=bob -subdir=yes "/Users/van/Documents/*"

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBefehlszeile:
: AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedsmc query archive -fromnode=bob -subdir=yes "/home/jones/*"

Windows-BetriebssystemeBefehlszeile:
: Windows-Betriebssystemedsmc query archive -fromnode=bob -subdir=yes d:\

Windows-BetriebssystemeAnmerkung: Der Client für Sichern/Archivieren kann beim Zurückschreiben von Dateien Dateibereichsinformationen verwenden. Die Dateibereichsinformationen können den Namen des Computers enthalten, von dem die Dateien gesichert wurden. Wenn Sie Dateien von einem anderen Knoten des Clients für Sichern/Archivieren zurückschreiben und kein Ziel für die zurückgeschriebenen Dateien angeben, verwendet der Client die Dateibereichsinformationen zum Zurückschreiben der Dateien. In einem derartigen Fall versucht der Client, die Dateien in das Dateisystem auf dem ursprünglichen Computer zurückzuschreiben. Hat der zurückschreibende Computer Zugriff auf das Dateisystem des ursprünglichen Computers, können Dateien in das ursprüngliche Dateisystem zurückgeschrieben werden. Hat der zurückschreibende Computer keinen Zugriff auf das Dateisystem des ursprünglichen Computers, kann der Client eine Netzfehlernachricht zurückgeben. Wenn die ursprüngliche Verzeichnisstruktur zurückgeschrieben werden soll, dies jedoch auf einen anderen Computer erfolgen soll, geben Sie bei der Zurückschreibung nur das Zieldateisystem an. Dies gilt sowohl für das Zurückschreiben von Dateien von einem anderen Knoten als auch für das Abrufen von Dateien von einem anderen Knoten.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

Fromowner

Die Option fromowner gibt einen alternativen Eigner an, von dem Sicherungsversionen oder archivierte Dateien oder Images zurückgeschrieben werden sollen. Der Eigner muss einem anderen Benutzer eine Zugriffsberechtigung für die Dateien oder Images erteilen.

Sollen beispielsweise Dateien aus dem Verzeichnis `/home/devel/proja` zurückgeschrieben werden, das *usermike* auf dem System ***puma*** gehört, und sollen die zurückgeschriebenen Dateien in Ihr eigenes Verzeichnis mit dem Namen `/home/id/proja` gestellt werden, geben Sie den folgenden Befehl ein:

```
dsmc restore -fromowner=usermike -fromnode=puma /home/devel/proja/
/home/id/proja/
```

Mac OS X-BetriebssystemeAnmerkung: Die Archivierung von Imagezurückschreibungen ist nicht für Mac OS X-Betriebssysteme anwendbar.

Benutzer ohne Rootberechtigung können fromowner=*root* angeben, um auf Dateien des Rootbenutzers zuzugreifen, wenn der Rootbenutzer ihnen eine Zugriffsberechtigung erteilt hat.

Anmerkung: Wenn Sie die Option fromowner ohne die Option fromnode angeben, muss der aktive Benutzer sich auf demselben Knoten befinden wie der in fromowner angegebene Benutzer.

Die Option fromowner ist in den folgenden Befehlen zu verwenden:

- query archive
- query backup
- query group
- query image
- restore
- restore image
- restore group
- retrieve

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Syntax

```
>>-FROMOwner = - --Eigner---------------------------------------><
```

Parameter

Eigner
: Name eines alternativen Eigners.

Beispiele

Befehlszeile:

```
dsmc query archive "/home/id/proja/*" -fromowner=mark
```

Fromtime

Mit der Option fromtime können Sie in Verbindung mit der Option fromdate eine Anfangszeit angeben, ab der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.

Der Client für Sichern/Archivieren ignoriert diese Option, wenn Sie nicht die Option fromdate angeben.

Die Option fromtime ist in den folgenden Befehlen zu verwenden:

- delete backup
- query archive
- query backup
- restore
- restore group
- retrieve

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-FROMTime = - --Zeit-------------------------------------><
```

Parameter

Zeit
: Gibt eine Anfangszeit an einem bestimmten Datum an, ab der gesicherte oder archivierte Dateien gesucht werden sollen. Wenn keine Zeit angegeben wird, lautet der Standardwert 00:00:00. Die Zeit muss in dem mit der Option timeformat ausgewählten Format angegeben werden.

  Wenn die Option timeformat in einem Befehl angegeben wird, muss sie vor den Optionen fromtime, pittime und totime stehen.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemedsmc q b -timeformat=4 -fromt=11:59AM -fromd=06/30/2003 -tot=11:59PM -tod=06/30/2003 /home/*

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssystemedsmc q b -timeformat=4 -fromt=11:59AM -fromd=06/30/2003 -tot=11:59PM -tod=06/30/2003 c:*

Groupname

Verwenden Sie die Option groupname im Befehl backup group, um den Namen für eine Gruppe anzugeben. Operationen können nur mit neuen Gruppen oder der zurzeit aktiven Version einer Gruppe ausgeführt werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist für alle UNIX- und Linux-Clients außer Mac OS X gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Syntax

```
>>-GROUPName = - --Name----------------------------------------><
```

Parameter

Name

Gibt den Namen der Gruppe an, die die Dateien enthält, die mit der Option filelist gesichert wurden. Verzeichnisbegrenzer sind im Gruppennamen nicht zulässig, da der Gruppenname keine Dateispezifikation, sondern ein Namensfeld ist.

Beispiele

Befehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1
-virtualfsname=/virtfs -mode=full
```

Windows-Betriebssysteme

```
backup group -filelist=c:\dir1\filelist1 -groupname=group1
-virtualfsname=\virtfs -mode=full
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

Groups (veraltet)

Diese Option ist veraltet.

Linux-BetriebssystemeWindows-Betriebssysteme

Host

Die Option 'host' gibt die Position des ESX-Zielservers an, auf dem die neue virtuelle Maschine während einer VMware-Zurückschreibungsoperation erstellt wird.

Verwenden Sie diese Option in restore vm-Befehlen, um den ESX-Host-Server anzugeben, auf den die Daten zurückgeschrieben werden sollen.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Beispiel

Die virtuelle Maschine auf den ESX-Server mit dem Namen vmesxbld1 zurückschreiben.

```
restore vm -host=vmesxbld1.us.acme.com
```

Httpport

Mit der Option httpport wird eine TCP/IP-Anschlussadresse für den Web-Client angegeben.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Web-Client im Feld HTTP-Anschluss des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Web-Client im Feld HTTP-Anschluss des Profileditors definieren.

Syntax

```
>>-HTTPport-- --Anschlussadresse------------------------------><
```

Parameter

Anschlussadresse
: Gibt die TCP/IP-Anschlussadresse für die Datenübertragung mit dem Web-Client an. Der Wertebereich ist 1000 bis 32767; der Standardwert ist 1581.

Beispiele

Optionsdatei:

```
httpport 1502
```

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme

```
-httpport=1502
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeNicht zutreffend.

Hsmreparsetag

Die Option hsmreparsetag gibt eine eindeutige Analysekennung an, die von einem auf Ihrem System installierten HSM-Produkt erstellt wird.

Viele HSM-Produkte verwenden Analysepunkte, um umgelagerte Dateien abzurufen oder zurückzurufen. Nach der Umlagerung einer Datei verbleibt eine kleine Stubdatei mit demselben Namen wie die ursprüngliche Datei in dem Dateisystem. Die Stubdatei ist ein Analysepunkt, der einen Rückruf der ursprünglichen Datei auslöst, wenn ein Benutzer oder eine Anwendung auf die Stubdatei zugreift. Der Analysepunkt schließt eine eindeutige Kennung mit der Bezeichnung *Analysekennung* ein, um anzugeben, welches HSM-Produkt die Datei umgelagert hat.

Wenn der IBM Spectrum Protect-Client für Sichern/Archivieren die Analysekennung in einer Stubdatei nicht erkennt, weist der Client für Sichern/Archivieren das HSM-Produkt an, die ursprüngliche Datei zurückzurufen. Sie können verhindern, dass Dateien zurückgerufen werden, wenn Sie die Analysekennung mit der Option hsmreparsetag angeben.

Der Client für Sichern/Archivieren erkennt die Analysekennung von HSM-Produkten der folgenden Unternehmen:

- International Business Machines Corp.
- Wisdata System Co. Ltd.
- BridgeHead Software Ltd.
- CommVault Systems, Inc.
- Data Storage Group, Inc.
- Enigma Data Solutions, Ltd.
- Enterprise Data Solutions, Inc.
- Global 360
- GRAU DATA AG
- Hermes Software GmbH

- Hewlett Packard Company
- International Communication Products Engineering GmbH
- KOM Networks
- Memory-Tech Corporation
- Moonwalk Universal
- Pointsoft Australia Pty. Ltd.
- Symantec Corporation

Ist das von Ihnen verwendete HSM-Produkt nicht in der vorherigen Liste enthalten, verwenden Sie die Option hsmreparsetag, um die Analysekennung anzugeben. Fragen Sie den Lieferanten des HSM-Produkts nach der Analysekennung, die von dem Produkt verwendet wird.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>---HSMREPARSETAG----Wert_für_Analysekennung------------------><
```

Parameter

Wert_für_Analysekennung
: Ein Dezimalwert (Basis 10) oder Hexadezimalwert (Basis 16), der die Analysekennung angibt.

Beispiele

Optionsdatei:
: Eine HSM-Analysekennung im Dezimalformat angeben:

```
hsmreparsetag 22
```

Eine HSM-Analysekennung im Hexadezimalformat angeben:

```
hsmreparsetag 0x16
```

Befehlszeile:
: Nicht zutreffend.

Ieobjtype

Verwenden Sie die Option ieobjtype, um einen Objekttyp für eine clientseitige Operation für die Datendeduplizierung innerhalb von Einschluss-/Ausschlussanweisungen anzugeben.

Die Option ieobjtype ist ein zusätzlicher Parameter für die Option include.dedup oder exclude.dedup.

Unterstützte Clients

Diese Option ist für alle Client gültig. Auch die IBM Spectrum Protect-API unterstützt diese Option.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Systemoptionsdatei (dsm.sys) ein. Sie können diese Option auf der Registerkarte Einschluss/Ausschluss im Profileditor definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Einschluss/Ausschluss im Profileditor definieren. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax

```
              .-File--------.
>>-IEObjtype--+-Image-------+---------------------------------><
```

```
+-SYSTEMState-+
'-Asr---------'
```

Parameter

File
: Gibt an, dass Dateien in die clientseitige Datendeduplizierungsverarbeitung eingeschlossen oder von ihr ausgeschlossen werden sollen. File ist der Standardwert.

Image
: Gibt an, dass Images in die clientseitige Datendeduplizierungsverarbeitung eingeschlossen oder von ihr ausgeschlossen werden sollen.

Windows-BetriebssystemeSystem State
: Windows-BetriebssystemeGibt an, dass der Systemstatus in die clientseitige Datendeduplizierungsverarbeitung eingeschlossen oder von ihr ausgeschlossen werden soll.

Windows-BetriebssystemeAsr
: Windows-BetriebssystemeGibt an, dass ASR-Objekte in die clientseitige Datendeduplizierungsverarbeitung eingeschlossen oder von ihr ausgeschlossen werden sollen.

Beispiele

Optionsdatei:
: Windows-Betriebssysteme`exclude.dedup e:\*\* ieobjtype=image`
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme`exclude.dedup /home/*/* ieobjtype=image`

Befehlszeile:
: Nicht zutreffend.

Zugehörige Verweise:
Ausschlussoptionen
Einschlussoptionen

Ifnewer

Mit der Option ifnewer wird eine vorhandene Datei nur dann durch die letzte Sicherungsversion ersetzt, wenn die Sicherungsversion neuer ist als die vorhandene Datei.

Wenn die Option inactive oder latest nicht verwendet wird, werden nur aktive Sicherungsversionen berücksichtigt.

Anmerkung: Verzeichniseinträge werden durch die neueste Sicherungsversion ersetzt, unabhängig davon, ob diese älter oder neuer als die vorhandene Version ist.

Verwenden Sie die Option ifnewer in den folgenden Befehlen:

- restore
- restore backupset
- restore group
- retrieve

Anmerkung: Diese Option wird ignoriert, wenn für die Option replace der Wert No definiert wird.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-IFNewer---------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeBefehlszeile:
: AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme
Mac OS X-Betriebssystemedsmc restore "/Users/grover/Documents/*" -sub=y -rep=y -ifnewer

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssystemedsmc restore "/home/grover/*" -sub=y -rep=y -ifnewer

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssystemedsmc restore -ifnewer d:\logs*.log

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Imagegapsize

Verwenden Sie die Option imagegapsize im Befehl backup image, in der Optionsdatei oder mit der Option include.image, um die Mindestgröße der leeren Bereiche auf einem Datenträger anzugeben, die Sie während der Imagesicherung überspringen wollen.

Verwenden Sie diese Option für die LAN-gestützte und die LAN-unabhängige Imagesicherung.

Wenn Sie beispielsweise eine Abstandsgröße von 10 angeben, bedeutet dies, dass ein leerer Plattenbereich mit einer Größe von mehr als 10 KB nicht gesichert wird. Abstände, die genau 10 KB groß sind, werden gesichert. Leere Bereiche, die genau 10 KB und kleiner als 10 KB sind, werden jedoch gesichert, auch wenn sie keine Daten enthalten. Ein leerer Bereich, der kleiner als 10 KB ist, wird jedoch gesichert, auch wenn er keine Daten enthält. Eine kleinere Imageabstandsgröße bedeutet, dass weniger Daten übertragen werden müssen, aber möglicherweise auch einen verminderten Durchsatz. Eine größere Imageabstandsgröße führt dazu, dass mehr Daten übertragen werden müssen, aber möglicherweise auch zu einem besseren Durchsatz.

Windows-BetriebssystemeFügen Sie die Anweisung include.image mit dem imagegapsize-Wert in Ihre Datei `dsm.opt` ein.

Unterstützte Clients

AIX-Betriebssysteme Linux-Betriebssysteme Diese Option ist nur für AIX-, Linux- und JFS2-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeFügen Sie diese Option in die Serverzeilengruppe der Clientsystemoptionsdatei (dsm.sys) oder in die Anweisung include.image in der Datei dsm.sys ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-IMAGEGapsize-- --Größe-------------------------------------><
```

Parameter

AIX-BetriebssystemeGröße

AIX-BetriebssystemeGibt die Mindestgröße leerer Bereiche in einem AIX JFS2-Dateisystem an, die während einer Imagesicherung übersprungen werden sollen. Sie können das Qualifikationsmerkmal `k` (Kilobyte), `m` (Megabyte) oder `g` (Gigabyte) zusammen mit dem Wert angeben. Ohne Angabe eines Qualifikationsmerkmals wird Kilobyte angenommen. Gültige Werte sind 0 bis 4294967295 KB. Wenn Sie den Wert 0 angeben, werden alle Blöcke einschließlich der unbenutzten Blöcke am Ende des Datenträgers gesichert. Wenn Sie einen anderen Wert als 0 angeben, werden unbenutzte Blöcke am Ende des Datenträgers nicht gesichert. Für LAN-gestützte und LAN-unabhängige Imagesicherung beträgt der Standardwert 32 KB. Diese Option ist sowohl für statische Imagesicherungen als auch für Imagesicherungen auf Momentaufnahmebasis gültig.
Anmerkung: Diese Option ist für AIX JFS2-Dateisysteme gültig. Wenn Sie für imagegapsize einen Wert größer 0 für ein anderes Dateisystem als AIX JFS2 angeben, empfangen Sie eine Warnung.

Windows-BetriebssystemeGröße

Windows-BetriebssystemeGibt die Mindestgröße leerer Bereiche auf einem formatierten logischen Datenträger an, die während einer Imagesicherung übersprungen werden soll. Sie können das Qualifikationsmerkmal `k` (Kilobyte), `m` (Megabyte) oder `g` (Gigabyte) zusammen mit dem Wert angeben. Ohne Angabe eines Qualifikationsmerkmals wird KB angenommen. Gültige Werte sind 0 bis 4294967295 KB. Wenn Sie den Wert 0 angeben, werden alle Blöcke einschließlich der unbenutzten Blöcke am Ende des Datenträgers gesichert. Wenn Sie einen anderen Wert als 0 angeben, werden unbenutzte Blöcke am Ende des Datenträgers nicht gesichert. Für LAN-gestützte und LAN-unabhängige Imagesicherung beträgt der Standardwert 32 KB.
Anmerkung: Wegen Einschränkungen des Betriebssystems können Sie diese Option nur für NTFS-Dateisysteme verwenden. Wenn Sie für imagegapsize einen Wert größer 0 für ein anderes Dateisystem als NTFS angeben, empfangen Sie eine Warnung.

Beispiele

AIX-BetriebssystemeOptionsdatei:

AIX-BetriebssystemeFügen Sie Folgendes der Serverzeilengruppe in der Datei dsm.sys hinzu: `imagegapsize 1m`

Beispiel einer Einschluss-/Ausschlussliste: `include.image /kalafs1 imagegapsize=-128k`

Windows-BetriebssystemeOptionsdatei:
Windows-Betriebssysteme`imagegapsize 1m`

Beispiel einer Einschluss-/Ausschlussliste: `include.image h: MYMC imagegapsize=1m`

Befehlszeile:
`-imagegapsize=64k`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme

Imagetofile

Verwenden Sie die Option imagetofile im Befehl restore image, um anzugeben, dass Sie das Quellenimage in eine Datei zurückschreiben wollen.

Es kann erforderlich sein, das Image in eine Datei zurückzuschreiben, wenn der Zieldatenträger defekte Sektoren enthält oder die Imagedaten bearbeitet werden sollen. Später können Sie ein Datenkopierprogramm Ihrer Wahl verwenden, um das Image von der Datei auf einen Plattendatenträger zu übertragen.

Linux-BetriebssystemeLinux unterstützt das Anhängen einer Imagedatei als logischen Datenträger, sodass Sie innerhalb des Image auf Dateidaten zugreifen können. Nachfolgend einige Beispiele:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

- Das Dateisystem `/usr` wurde vom Client für Sichern/Archivieren gesichert. Mit dem folgenden Befehl wird das Dateisystemimage in die Datei `/home/usr.img` zurückgeschrieben:

  ```
  # dsmc restore image /usr /home/usr.img -imagetofile
  ```

- Um die Imagedatei unter dem Verzeichnis `/mnt/usr` anzuhängen, kann der folgende Mountbefehl ausgeführt werden:

  ```
  # mount /home/usr.img /mnt/usr -o loop=/dev/loop0
  ```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeJetzt ist der Inhalt des Image unter `/mnt/usr` so verfügbar, als wäre ein reguläres Dateisystem an dieses Verzeichnis angehängt.

Unterstützte Clients

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDiese Option ist nur für AIX-, Oracle Solaris- und alle Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-IMAGETOfile-----------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeBefehlszeile:
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme`dsmc restore image /usr /home/usr.img -imagetofile`
Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme`dsmc restore image d: e:\diskD.img -imagetofile`

Inactive

Verwenden Sie die Option inactive, um sowohl aktive als auch inaktive Objekte anzuzeigen.

Die Option inactive können Sie in folgenden Befehlen verwenden:

- delete group
- Windows-Betriebssystemequery asr

- query backup
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemequery group
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemequery image
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemequery nas
- Windows-Betriebssystemequery systemstate
- Windows-Betriebssystemequery vm (vmbackuptype=fullvm und vmbackuptype=hypervfull)
- restore
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemerestore group
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemerestore image
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemerestore nas
- Windows-Betriebssystemerestore vm (vmbackuptype=fullvm und vmbackuptype=hypervfull)

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Wichtig: Wenn Sie die Option inactive bei einer Zurückschreibungsoperation verwenden, sollten Sie auch die Option pick oder eine andere Filteroption verwenden, da im Gegensatz zur Option latest alle Versionen in einer unbestimmten Reihenfolge zurückgeschrieben werden. Diese Option wird implizit unterstellt, wenn pitdate verwendet wird.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-INActive---------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssystemedsmc restore "/Users/zoe/Documents/*" -inactive -pick

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemedsmc restore "/home/zoe/*" -inactive -pick

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssystemedsmc restore -inactive c:\id\projecta\ -pick

Inclexcl

Die Option inclexcl gibt den Pfad und Dateinamen der Einschluss-/Ausschlussoptionsdatei an.

Mehrere Anweisungen inclexcl sind zulässig. Sie müssen diese Option jedoch für jede Einschluss-/Ausschlussdatei angeben.

Windows-BetriebssystemeStellen Sie sicher, dass Sie Ihre Einschluss-/Ausschlussoptionsdatei in einem Verzeichnis speichern, für das alle Benutzer Lesezugriff haben.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeStellen Sie sicher, dass Sie Ihre Einschluss-/Ausschlussoptionsdatei in einem Verzeichnis speichern, für das alle Benutzer Lesezugriff haben, z. B. `/etc`.

Bei der Verarbeitung werden die Einschluss-/Ausschlussanweisungen innerhalb der Einschluss-/Ausschlussdatei in derselben Reihenfolge in die Listenpositionen gestellt, die durch die Option inclexcl belegt sind, und entsprechend verarbeitet.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeIst der Client für die hierarchische Speicherverwaltung auf der Workstation installiert, können Dateien mithilfe einer Einschluss-/Ausschlussoptionsdatei von der Sicherung und von der Speicherverwaltung, nur von der Sicherung oder nur von der Speicherverwaltung ausgeschlossen werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys *innerhalb* einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Einschluss/Ausschluss im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Einschluss/Ausschluss im Profileditor definieren.

Syntax

```
>>-INCLExcl-- --Dateispezifikation----------------------------><
```

Parameter

Dateispezifikation
: Gibt den Pfad und den Dateinamen *einer* Einschluss-/Ausschlussoptionsdatei an.

Beispiele

Optionsdatei:

Mac OS X-Betriebssysteme

```
INCLExcl /Users/user1/Documents/backup.excl
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
inclexcl /usr/dsm/backup.excl
inclexcl /etc/inclexcl.def
```

Windows-Betriebssysteme

```
inclexcl c:\dsm\backup.excl
```

Befehlszeile:
: Nicht zutreffend.

- Hinweise für Clients, die für Unicode aktiviert wurden
  Eine Einschluss-/Ausschlussdatei kann Unicode-Format oder Nicht-Unicode-Format haben.

Einschlussoptionen

Die Einschlussoptionen geben Objekte an, die Sie für Sicherungs- und Archivierungsservices eingeschlossen werden sollen.

Die Einschlussoptionen geben Folgendes an:

- Mac OS X-BetriebssystemeObjekte in einer großen Gruppe ausgeschlossener Objekte, die Sie für Sicherungs- und Archivierungsservices einschließen wollen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeObjekte in einer großen Gruppe ausgeschlossener Objekte, die Sie für Sicherungs-, Archivierungs-, Image- und Speicherverwaltungsservices einschließen wollen.
- Windows-BetriebssystemeObjekte in einer großen Gruppe ausgeschlossener Objekte, die Sie für Sicherungs-, Archivierungs- und Imageservices einschließen wollen.
- Dateien, die für die Sicherungs- oder Archivierungsverarbeitung eingeschlossen sind und die Sie für die Verschlüsselungsverarbeitung einschließen wollen.
- Dateien, die für die Sicherungs- oder Archivierungsverarbeitung eingeschlossen sind und die Sie auch für die Komprimierungsverarbeitung einschließen wollen.
- Objekte, denen Sie eine bestimmte Verwaltungsklasse zuordnen wollen.
- Eine Verwaltungsklasse, die allen Objekten zugeordnet werden soll, denen nicht explizit eine Verwaltungsklasse zugeordnet wird.
- Dateibereiche, denen Sie speichereffiziente Sicherungsverarbeitung zuordnen wollen.
- Dateibereiche, für die Sie die Option diskcachelocation verwenden wollen, damit bestimmte Dateisysteme verschiedene, bestimmte Positionen für ihren Plattencache verwenden.

Wenn Sie Objekten keine bestimmte Verwaltungsklasse zuordnen, wird die Standardverwaltungsklasse in der aktiven Maßnahmengruppe Ihrer Maßnahmendomäne verwendet. Verwenden Sie den Befehl query mgmtclass, um Informationen zu den Verwaltungsklassen anzuzeigen, die in der aktiven Maßnahmengruppe verfügbar sind.

Windows-BetriebssystemeSie können Dateien mit Fernzugriff einschließen, indem Sie UNC-Namen (d. h. Namen, die der allgemeinen Namenskonvention entsprechen) in Ihrer Einschlussanweisung angeben.

Hinweis: Der Client für Sichern/Archivieren vergleicht die Dateien, die verarbeitet werden, mit den in den Einschluss-/Ausschlussanweisungen angegebenen Mustern, wobei die Optionsdatei von unten nach oben gelesen wird.
Anmerkung:

1. Windows-BetriebssystemeDie Anweisung exclude.dir überschreibt alle Einschlussanweisungen, die mit dem Muster übereinstimmen.
2. AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie Anweisungen exclude.fs und exclude.dir überschreiben alle Einschlussanweisungen, die mit dem Muster übereinstimmen.
3. Windows-BetriebssystemeBei den include-Anweisungen muss die Groß-/Kleinschreibung nicht beachtet werden.
4. Auf dem Server können diese Optionen auch mit der Option inclexcl definiert werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die Option include.fs.nas kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Optionen auf der Registerkarte Einschluss/Ausschluss im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Optionen in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Optionen auf der Registerkarte Einschluss/Ausschluss im Profileditor definieren.

Syntax

```
>>-Optionen-- --Muster-- --+-------------------------+--------><
                           '- --optionaler Parameter-'
```

include, include.backup, include.file
: Mit diesen Optionen können Sie Dateien einschließen oder Verwaltungsklassen für die Sicherungsverarbeitung zuordnen.
Die Option include hat Auswirkungen auf die Archivierungs- und Sicherungsverarbeitung. Wenn Sie unterschiedliche Verwaltungsklassen für die Archivierungs- und Sicherungsverarbeitung zuordnen wollen, müssen Sie include.archive und include.backup immer mit ihren eigenen Verwaltungsklassen angeben. In diesem Beispiel wird die Verwaltungsklasse `archmc` zugeordnet, wenn eine Archivierungsoperation ausgeführt wird. Die Verwaltungsklasse wird zugeordnet, wenn eine Archivierungsoperation ausgeführt wird, da include.backup nur für die Sicherungsverarbeitung und nicht für die Archivierungsverarbeitung verwendet wird. AIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
include.archive /home/test/* archmc
include.backup /home/test/*
```

Windows-Betriebssysteme

```
include.archive c:\test\*\ archmc
include.backup c:\test\*
```

include.archive
: Schließt Dateien für die Archivierungsverarbeitung ein oder ordnet Verwaltungsklassen zu.
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

include.attribute.symlink
: Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme
Mac OS X-Betriebssysteme

Schließt eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt, innerhalb einer größeren Gruppe von ausgeschlossenen Dateien nur bei der Sicherungsverarbeitung ein.

Mac OS X-BetriebssystemeAnmerkung: Für Mac OS X werden Aliasnamen eingeschlossen.

include.compression
: Schließt Dateien für die Komprimierungsverarbeitung ein, wenn Sie die Option compression auf yes setzen. Diese Option gilt für Sicherungen und Archivierungen.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

include.dedup
: AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Windows-BetriebssystemeSchließt Dateien bei der clientseitigen Datendeduplizierung ein. Zum Steuern einer clientseitigen Operation für die Datendeduplizierung können Sie ieobjtype als Wert der Option include.dedup angeben. Standardmäßig werden alle Objekte, die für die clientseitige Datendeduplizierung in Frage kommen, bei der clientseitigen Datendeduplizierung eingeschlossen.
Gültige Parameter für ieobjtype sind:

- File
- Image
- Windows-BetriebssystemeSYSTEMState

- Windows-BetriebssystemeAsr

Der Standardwert ist File.

include.encrypt
Schließt die angegebenen Dateien in die Verschlüsselungsverarbeitung ein. Standardmäßig führt der Client keine Verschlüsselungsverarbeitung durch.
Anmerkungen:

1. Die Option include.encrypt ist die einzige Möglichkeit, die Verschlüsselung auf dem Client für Sichern/Archivieren zu aktivieren. Werden keine Anweisungen include.encrypt verwendet, findet keine Verschlüsselung statt.
2. Die Verschlüsselung ist nicht mit der clientseitigen Deduplizierung kompatibel. Bei der Verschlüsselung eingeschlossene Dateien werden bei der clientseitigen Deduplizierung nicht dedupliziert.
3. Die Verschlüsselung ist nicht mit Sicherungen virtueller VMware-Maschinen kompatibel, bei denen die immer inkrementellen Sicherungsmodi (MODE=IFIncremental und MODE=IFFull) verwendet werden. Ist der Client für die Verschlüsselung konfiguriert, können Sie nicht die immer inkrementelle Sicherung verwenden.
4. Die Verschlüsselung ist nicht mit IBM Spectrum Protect for Virtual Environments Data Protection for VMware Recovery Agent kompatibel. Ist der Client für die Verschlüsselung konfiguriert, können Sie mit dem Client Sicherungen zurückschreiben, die mit dem Gesamt- oder Teilsicherungsmodus (MODE=Full oder MODE=Incremental) erstellt wurden. Sie können jedoch nicht den Recovery Agent für die Zurückschreibung der verschlüsselten Sicherungen verwenden. Sicherungen, die im vollständigen oder inkrementellen Modus erstellt wurden, wurden mit dem Client der Version 7.1 oder früher erstellt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemeinclude.fs
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

AIX-BetriebssystemeFür AIX JFS2-Dateisysteme: Verwenden Sie die Option snapshotcachesize in der Datei dsm.sys oder mit der Option include.fs, um eine geeignete Momentaufnahmengröße anzugeben, sodass während der Dateisicherung oder -archivierung auf Momentaufnahmebasis alle alten Datenblöcke gespeichert werden können.

Für die Steuerung der Verarbeitung Ihres Dateibereichs durch den Client für die Teilsicherung können Sie die folgenden zusätzlichen Optionen in Ihrer Datei dsm.sys als Werte der Option include.fs angeben: diskcachelocation und memoryefficientbackup.

Jede der Optionen include.fs, memoryefficientbackup und diskcachelocation muss in der Optionsdatei in derselben Zeile stehen.

```
include.fs /home
     memoryefficientbackup=diskcachemethod
     diskcachelocation=/usr
include.fs /usr
     memoryefficientbackup=diskcachemethod
     diskcachelocation=/home
include.fs /Volumes/hfs3
     memoryefficientbackup=diskcachemethod
     diskcachelocation=/Volumes/hfs2
 Nur für AIX JFS2-Dateisysteme: include.fs
     /kalafs1 snapshotproviderfs=JFS2
```

Werden diese Optionen sowohl in der Optionsdatei als auch in der Option include.fs angegeben, werden die Werte von include.fs statt der Werte in einer Optionsdatei oder in der Befehlszeile für den angegebenen Dateibereich verwendet.

Windows-Betriebssystemeinclude.fs
Windows-BetriebssystemeWurde die Unterstützung offener Dateien konfiguriert, führt der Client eine Momentaufnahmesicherung oder Archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder im Gebrauch) sind. Über die Momentaufnahme wird die Sicherung von einer Kopie des Dateisystems erstellt, die dem Dateisystemstatus zum Zeitpunkt der Erstellung der Momentaufnahme entspricht. Nachfolgende Änderungen am Dateisystem werden bei der Sicherung nicht berücksichtigt. Sie können den Parameter snapshotproviderfs der Option include.fs auf none setzen, um anzugeben, welche Laufwerke keine Unterstützung für offene Dateien verwenden.
Für die Steuerung der Verarbeitung Ihres Dateibereichs durch den Client für die Teilsicherung können Sie die folgenden zusätzlichen Optionen in Ihrer Datei dsm.opt als Werte der Option include.fs angeben: diskcachelocation und memoryefficientbackup.

```
include.fs d: memoryefficientbackup=diskcachem
  diskcachelocation=e:\temp
include.fs e: memoryefficientbackup=diskcachem
  diskcachelocation=c:\temp
```

Werden diese Optionen sowohl in der Optionsdatei als auch in der Option include.fs angegeben, werden die Werte von include.fs statt der Werte in einer Optionsdatei oder in der Befehlszeile für den angegebenen Dateibereich verwendet.
AIX-BetriebssystemeOracle Solaris-Betriebssystemeinclude.fs.nas
AIX-BetriebssystemeOracle Solaris-BetriebssystemeVerwenden Sie die Option include.fs.nas, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Sie können auch angeben, ob der Client während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Verwenden Sie dazu die Option toc mit der Option include.fs.nas in Ihrer Datei dsm.sys. Diese Option ist nur für AIX- und Solaris-Clients gültig.
Windows-Betriebssystemeinclude.fs.nas
Windows-BetriebssystemeVerwenden Sie die Option include.fs.nas, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden. Sie können auch angeben, ob der Client während einer Imagesicherung des NAS-Dateisystems Inhaltsverzeichnisinformationen (TOC-

Informationen) speichert. Verwenden Sie dazu die Option toc mit der Option include.fs.nas in Ihrer Clientoptionsdatei (dsm.opt).

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemeinclude.image

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSchließt einen Dateibereich oder einen logischen Datenträger ein oder ordnet eine Verwaltungsklasse zu (bei Verwendung im Befehl backup image). Der Befehl backup image ignoriert alle anderen Einschlussoptionen.

Linux-BetriebssystemeFür Linux x86_64-Clients: Verwenden Sie die Option snapshotcachesize in den folgenden Situationen:

- Mit dem Befehl backup image
- In der Datei dsm.sys
- Mit der Option include.image

Wenn Sie die Option snapshotcachesize in diesen Situationen verwenden, können Sie eine geeignete Momentaufnahmengröße angeben, sodass während der Imagesicherung alle alten Datenblöcke gespeichert werden können.

Eine Momentaufnahmengröße von 100 Prozent gewährleistet eine gültige Momentaufnahme.

AIX-BetriebssystemeFür AIX JFS2-Dateisysteme: Verwenden Sie die Option snapshotcachesize in den folgenden Situationen:

- Mit dem Befehl backup image
- In der Datei dsm.sys
- Mit der Option include.image

Wenn Sie die Option snapshotcachesize in diesen Situationen verwenden, können Sie eine geeignete Momentaufnahmengröße angeben, sodass während der Imagesicherung alle alten Datenblöcke gespeichert werden können.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Windows-Betriebssystemeinclude.image

Windows-BetriebssystemeSchließt einen Dateibereich oder einen logischen Datenträger ein oder ordnet eine Verwaltungsklasse zu (bei Verwendung im Befehl backup image). Der Befehl backup image ignoriert alle anderen Einschlussoptionen.

Standardmäßig führt der Client eine Offline-Imagesicherung aus. Zum Aktivieren und Steuern einer Online-Imageoperation können Sie die folgenden Optionen in Ihrer Datei dsm.opt als Werte der Option include.image angeben: snapshotproviderimage, presnapshotcmd, postsnapshotcmd.

Windows-Betriebssystemeinclude.systemstate

Windows-BetriebssystemeDiese Option bindet Systemstatussicherungen an die angegebene Verwaltungsklasse. Bei der Angabe dieser Option müssen Sie 'all' als Muster angeben. Wenn Sie diese Option nicht angeben, werden Systemstatussicherungen an die Standardverwaltungsklasse gebunden.

Parameter

Muster

Gibt die Objekte an, die für die Sicherungs- oder Archivierungsverarbeitung berücksichtigt werden sollen oder denen eine bestimmte Verwaltungsklasse zugeordnet werden soll.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAnmerkung: Für NAS-Dateisysteme: Sie müssen den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Einschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, bezieht sich das identifizierte Dateisystem auf den NAS-Knotennamen, der in der Clientsystemoptionsdatei (dsm.sys) oder in der Befehlszeile angegeben ist.

Windows-BetriebssystemeAnmerkung: Für NAS-Dateisysteme: Sie müssen den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Einschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, bezieht sich das identifizierte Dateisystem auf den NAS-Knotennamen, der in der Clientoptionsdatei (dsm.opt) oder in der Befehlszeile angegeben ist.

Wenn das Muster mit einem einfachen oder doppelten Anführungszeichen beginnt oder eingebettete Leerzeichen oder Gleichheitszeichen enthält, muss der Wert in einfache (') oder doppelte (") Anführungszeichen eingeschlossen werden. Die Anführungszeichen am Anfang und am Ende müssen identisch sein.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeFür die Option include.image ist das Muster der Name eines angehängten Dateisystems oder eines unformatierten logischen Datenträgers.

Windows-BetriebssystemeFür die Option include.image ist das Muster der Name eines Dateisystems oder eines unformatierten logischen Datenträgers.

Windows-Betriebssysteme
Anmerkung: Wenn Sie include.systemstate angeben, ist all das einzige gültige Muster.

Optionaler Parameter

Name der Verwaltungsklasse

Gibt den Namen der Verwaltungsklasse an, die den Objekten zugeordnet werden soll. Wenn keine Verwaltungsklasse angegeben wird, wird die Standardverwaltungsklasse verwendet. Verwenden Sie folgende Syntax, um eine Verwaltungsklasse einer Sicherungsgruppe in einer Einschlussanweisung zuzuordnen:
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
include Name_des_virtuellen_Dateibereichs\Gruppenname Verwaltungsklassenname
```

Windows-Betriebssysteme

```
include Name_des_virtuellen_Dateibereichs/Gruppenname Verwaltungsklassenname
```

Hierbei gilt Folgendes:

Name_des_virtuellen_Dateibereichs
Gibt den Namen des virtuellen Dateibereichs des IBM Spectrum Protect-Servers, den Sie im Befehl Backup Group der Gruppe zugeordnet haben.
Gruppenname
Der Name der Gruppe, die Sie bei Ausführung des Befehls Backup Group erstellt haben.
Verwaltungsklassenname
Der Name der Verwaltungsklasse, die den Dateien in der Gruppe zugeordnet werden soll.
Beispiel: Eine Gruppe mit dem Namen 'MyGroup' ist in einem virtuellen Dateibereich mit dem Namen 'MyVirtualFileSpace' gespeichert. Verwenden Sie folgende Syntax, um der Gruppe eine Verwaltungsklasse mit dem Namen TEST zuzuordnen:
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
include MyVirtualFileSpace/MyGroup TEST
```

Windows-Betriebssysteme

```
include MyVirtualFileSpace\MyGroup TEST
```

Tabelle 1. Weitere optionale Parameter

Optionaler Parameter	**Verwendung mit der Option**
ieobjtype	include.dedup
memoryefficientbackup	include.fs
diskcachelocation	include.fs
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemedynamicimage	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemeinclude.image
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssystemepostsnapshotcmd	AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssystemeinclude.image
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssystemepresnapshotcmd	AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssystemeinclude.image
AIX-BetriebssystemeLinux-Betriebssystemesnapshotcachesize	AIX-BetriebssystemeLinux-Betriebssystemeinclude.image
AIX-BetriebssystemeWindows-Betriebssysteme snapshotproviderfs	AIX-BetriebssystemeWindows-Betriebssystemeinclude.image
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssystemesnapshotproviderimage	AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssystemeinclude.image

Beispiele

Optionsdatei:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
include /home/proj/text/devel.*
include /home/proj/text/* textfiles
include * managall
include /WAS_ND_NDNODE mgmtclass
include /WAS_APPNODE mgmtclass
include.image /home
include.archive /home/proj/text/
  * myarchiveclass
include.backup /home/proj/text/
  * mybackupclass
```

```
include.compression /home/proj/text/
  devel.*
include.encrypt /home/proj/gordon/*
include.fs.nas netappsj/vol/vol0
  homemgmtclass
```

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
include.dedup /Users/Administrator/Documents/Important/.../*
```

AIX-Betriebssysteme

```
Nur für AIX:

include.image /home
  MGMTCLASSNAME
  snapshotproviderimage=JFS2
  snapshotcachesize=40
include.image /home
  snapshotproviderimage=NONE
include.fs /kalafs1
  snapshotproviderfs=JFS2
```

Linux-Betriebssysteme

```
Nur für LINUX:

include.image /home
  snapshotproviderimage=LINUX_LVM
include.image /myfs1 dynamicimage=yes
include.image /home MGMTCLASSNAME
  snapshotproviderimage=NONE
include.image /myfs1 dynamicimage=yes
include.attribute.symlink /home/spike/.../*
include.fs /usr
  memoryefficientbackup=diskcachemethod
```

Windows-Betriebssysteme

```
Nur für Windows:

include c:\proj\text\devel.*
include c:\proj\text\* textfiles
include ?:\* managall
include WAS_ND_NDNODE mgmtclass
include WAS_APPNODE mgmtclass
include.backup c:\win98\system\* mybackupclass
include.archive c:\win98\system\* myarchiveclass
include.encrypt c:\win98\proj\gordon\*
include.compress c:\test\file.txt

include.image h: MGMTCLASSNAME
  snapshotproviderimage=vss

include.image x:
  snapshotproviderimage=none
include.image y:
  snapshotproviderimage=vss
include.image z: MGMTCLASSNAME
  snapshotproviderimage=none
include.fs c:
  snapshotproviderfs=vss

include.systemstate ALL mgmtc3
include.dedup c:\Users\Administrator\Documents\Important\...\*
include.dedup e:\*\* ieobjtype=image
include.dedup ALL ieobjtype=systemstate
include.dedup ALL ieobjtype=ASR
```

Windows-BetriebssystemeAlle Dateien in allen Laufwerken verschlüsseln:

```
include.encrypt ?:\...\*
```

Befehlszeile:
Nicht zutreffend.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie Verarbeitung symbolischer Verbindungen und Aliasnamen steuern
  IBM Spectrum Protect behandelt symbolische Verbindungen und Aliasnamen (Aliasnamen gelten nur für Mac OS X) als tatsächliche Dateien und sichert sie. Die Datei, auf die durch die symbolische Verbindung verwiesen wird, wird jedoch nicht gesichert.

- Windows-BetriebssystemeKomprimierungs- und Verschlüsselungsverarbeitung
  Beachten Sie die folgenden Informationen, wenn bestimmte Dateien oder Dateigruppen während einer Sicherungs- oder Archivierungsoperation für die Komprimierung und Verschlüsselung eingeschlossen werden sollen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeKomprimierungs- und Verschlüsselungsverarbeitung bei der Sicherung
  In diesem Abschnitt sind einige Hinweise aufgeführt, die Sie beachten sollten, wenn Sie bestimmte Dateien oder Dateigruppen während einer Sicherungs- oder Archivierungsoperation bei der Komprimierungs- und Verschlüsselungsverarbeitung einschließen wollen.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeVerarbeitung von NAS-Dateisystemen
  Verwenden Sie die Option include.fs.nas, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden und zu steuern, ob für die Dateisystemsicherung Inhaltsverzeichnisinformationen gespeichert werden.
- Linux-Betriebssysteme Windows-BetriebssystemeEinschlussoptionen für virtuelle Maschinen
  Einschluss- und Ausschlussoptionen für virtuelle Maschinen wirken sich auf das Verhalten von Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen aus. Diese Optionen werden vor allen Befehlszeilenoptionen verarbeitet. Daher können Optionen in der Befehlszeile Optionen überschreiben, die in den Einschluss- oder Ausschlussoptionen für virtuelle Maschinen angegebenen sind. Informationen zu den Optionen finden Sie in der jeweiligen Optionsbeschreibung.

Zugehörige Konzepte:
Windows-BetriebssystemeDateien ausschließen, deren Namen der allgemeinen Namenskonvention entsprechen
Zugehörige Tasks:
Windows-BetriebssystemeUnterstützung offener Dateien konfigurieren
Zugehörige Verweise:
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeSnapshotcachesize
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeToc
Zugehörige Informationen:
AIX-Betriebssysteme Linux-Betriebssysteme Befehl 'mmbackup': IBM Spectrum Protect-Voraussetzungen
AIX-Betriebssysteme Linux-Betriebssysteme Anleitung für die Integration von IBM Spectrum Scale AFM mit IBM Spectrum Protect
AIX-Betriebssysteme Linux-Betriebssysteme Verwendung der Einschluss- und Ausschlussoptionen von IBM Spectrum Protect in Verbindung mit dem IBM Spectrum Scale-Befehl 'mmbackup'
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

Die Verarbeitung symbolischer Verbindungen und Aliasnamen steuern

IBM Spectrum Protect behandelt symbolische Verbindungen und Aliasnamen (Aliasnamen gelten nur für Mac OS X) als tatsächliche Dateien und sichert sie. Die Datei, auf die durch die symbolische Verbindung verwiesen wird, wird jedoch nicht gesichert.

In einigen Fällen können symbolische Verbindungen und Aliasnamen problemlos erneut erstellt werden und müssen nicht gesichert werden. Darüber hinaus kann durch das Sichern dieser symbolischen Verbindungen oder Aliasnamen die Sicherungsverarbeitungszeit zunehmen und ein wesentlicher Bereich des Speichers auf dem IBM Spectrum Protect-Server eingenommen werden.

Sie können die Option exclude.attribute.symlink verwenden, um eine Datei oder Dateigruppe, bei denen es sich um symbolische Verbindungen oder Aliasnamen handelt, von der Sicherungsverarbeitung ausschließen. Falls notwendig, können Sie mithilfe der Option include.attribute.symlink symbolische Verbindungen oder Aliasnamen innerhalb einer breiten Gruppe ausgeschlossener Dateien für die Sicherungsverarbeitung einschließen. Sollen beispielsweise alle symbolischen Verbindungen oder Aliasnamen von der Sicherungsverarbeitung ausgeschlossen werden, mit Ausnahme derjenigen, die sich unter dem Verzeichnis `/home/spike` befinden, geben Sie die folgenden Anweisungen in Ihre Datei dsm.sys ein:

```
exclude.attribute.symlink  /.../*
include.attribute.symlink /home/spike/.../*
```

Zugehörige Verweise:
Ausschlussoptionen
Windows-Betriebssysteme

Komprimierungs- und Verschlüsselungsverarbeitung

Beachten Sie die folgenden Informationen, wenn bestimmte Dateien oder Dateigruppen während einer Sicherungs- oder Archivierungsoperation für die Komprimierung und Verschlüsselung eingeschlossen werden sollen.

- Sie müssen die Option compression auf *yes* setzen, um die Komprimierungsverarbeitung zu aktivieren. Wenn Sie die Option compression nicht angeben oder die Option compression auf *no* setzen, führt der Client für Sichern/Archivieren keine Komprimierungsverarbeitung aus.
- Der Client verarbeitet exclude.dir und andere Einschluss-/Ausschlussanweisungen zuerst. Danach berücksichtigt der Client alle Anweisungen include.compression und include.encrypt. Wenn beispielsweise folgende Einschluss-/Ausschlussliste eingegeben wird:

  ```
  exclude c:\test\file.txt
  include.compression c:\test\file.txt
  include.encrypt c:\test\file.txt
  ```

  Der Client prüft zuerst die Anweisung `exclude c:\test\file.txt` und stellt fest, dass `c:\test\file.txt` von der Sicherungsverarbeitung ausgeschlossen ist und daher kein Kandidat für die Komprimierungs- oder Verschlüsselungsverarbeitung ist.

- Die Komprimierungs- und Verschlüsselungsverarbeitung von Einschluss-/Ausschlussdateien ist *nur* für die Sicherungs- und Archivierungsverarbeitung gültig.
- Wie bei anderen Einschluss-/Ausschlussanweisungen können Sie mithilfe der Option inclexcl eine Datei im Unicode-Format angeben, die Anweisungen include.compression und include.encrypt für Unicode-Dateien enthält. Weitere Informationen finden Sie in Inclexcl.

Zugehörige Verweise:
Compression
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme

Komprimierungs- und Verschlüsselungsverarbeitung bei der Sicherung

In diesem Abschnitt sind einige Hinweise aufgeführt, die Sie beachten sollten, wenn Sie bestimmte Dateien oder Dateigruppen während einer Sicherungs- oder Archivierungsoperation bei der Komprimierungs- und Verschlüsselungsverarbeitung einschließen wollen.

- Sie müssen die Option compression auf *yes* setzen, um die Komprimierungsverarbeitung zu aktivieren. Wenn Sie die Option compression nicht angeben oder die Option compression auf *no* setzen, führt der Client für Sichern/Archivieren keine Komprimierungsverarbeitung aus.
- Der Client verarbeitet exclude.fs, exclude.dir und andere Einschluss-/Ausschlussanweisungen zuerst. Danach berücksichtigt der Client alle Anweisungen include.compression und include.encrypt. Wenn beispielsweise folgende Einschluss-/Ausschlussliste eingegeben wird:

  ```
  exclude /home/jones/proj1/file.txt
  include.compression /home/jones/proj1/file.txt
  include.encrypt /home/jones/proj1/file.txt
  ```

  Der Client prüft die Anweisung `exclude /home/jones/proj1/file.txt` zuerst und stellt fest, dass `/home/jones/proj1/file.txt` von der Sicherungsverarbeitung ausgeschlossen und daher kein Kandidat für die Komprimierungs- und Verschlüsselungsverarbeitung ist.

- Die Komprimierungs- und Verschlüsselungsverarbeitung von Einschluss-/Ausschlussdateien ist *nur* für die Sicherungs- und Archivierungsverarbeitung gültig.

Zugehörige Verweise:
Compression
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Verarbeitung von NAS-Dateisystemen

Verwenden Sie die Option include.fs.nas, um eine Verwaltungsklasse an NAS-Dateisysteme zu binden und zu steuern, ob für die Dateisystemsicherung Inhaltsverzeichnisinformationen gespeichert werden.

Linux-Betriebssysteme Windows-BetriebssystemeAnmerkung: Die Option include.fs.nas gilt nicht für eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz.

Für eine NAS-Dateisystemspezifikation werden folgende Konventionen verwendet:

- NAS-Knoten stellen eine neue Knotenart dar. Der Name des NAS-Knotens identifiziert einen NAS-Dateiserver und seine Daten eindeutig für den Client für Sichern/Archivieren. Sie können den NAS-Knotennamen als Präfix vor die Dateispezifikation setzen, um den Dateiserver anzugeben, für den die Einschlussanweisung gilt. Wenn Sie keinen NAS-Knotennamen angeben, gilt das angegebene Dateisystem für alle NAS-Dateiserver.
- Unabhängig vom Clientbetriebssystem wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet, wie in diesem Beispiel: `/vol/vol0`.
- Windows-BetriebssystemeFür NAS-Dateisystembezeichnungen, die in der Befehlszeile angegeben werden, müssen geschweifte Klammern ({ and }) als Begrenzer um Dateisystemnamen verwendet werden, z. B.: `{/vol/vol0}`. Verwenden Sie keine geschweiften Klammern, wenn Sie diese Option in der Optionsdatei angeben.

Verwenden Sie die folgende Syntax:

```
>>-Muster-- Verwaltungsklassenname- toc=Wert------------------><
```

Dabei gilt:

Muster
: Gibt die Objekte an, die für die Sicherungsservices berücksichtigt werden sollen, denen eine bestimmte Verwaltungsklasse zugeordnet werden soll oder für die die TOC-Erstellung gesteuert werden soll. Sie können Platzhalterzeichen im Muster verwenden.

Verwaltungsklassenname
: Gibt den Namen der Verwaltungsklasse an, die den Objekten zugeordnet werden soll. Wird keine Verwaltungsklasse angegeben, wird die Standardverwaltungsklasse verwendet.

toc=Wert
: Weitere Informationen finden Sie in Toc.

Beispiel 1: Soll dem Dateisystem /vol/vol1 eines NAS-Knotens mit dem Namen `netappsj` eine Verwaltungsklasse zugeordnet werden, geben Sie die folgende Einschlussanweisung an:

```
include.fs.nas netappsj/vol/vol1 nasMgmtClass toc=yes
```

Beispiel 2: Soll dieselbe Verwaltungsklasse allen Pfaden zugeordnet werden, die dem Dateisystem /vol/ auf einem NAS-Knoten mit dem Namen `netappsj` untergeordnet sind (beispielsweise /vol/vol1, /vol/vol2 und /vol/vol3), geben Sie die folgende Einschlussanweisung an:

```
include.fs.nas netappsj/vol/* nasMgmtClass toc=yes
```

Linux-BetriebssystemeWindows-Betriebssysteme

Einschlussoptionen für virtuelle Maschinen

Einschluss- und Ausschlussoptionen für virtuelle Maschinen wirken sich auf das Verhalten von Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen aus. Diese Optionen werden vor allen Befehlszeilenoptionen verarbeitet. Daher können Optionen in der Befehlszeile Optionen überschreiben, die in den Einschluss- oder Ausschlussoptionen für virtuelle Maschinen angegebenen sind. Informationen zu den Optionen finden Sie in der jeweiligen Optionsbeschreibung.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

- Linux-BetriebssystemeWindows-BetriebssystemeInclude.vm
  Bei VM-Operationen überschreibt diese Option die Verwaltungsklasse, die in der Option vmmc angegeben ist.
- Linux-BetriebssystemeWindows-BetriebssystemeInclude.vmdisk
  Mit der Option INCLUDE.VMDISK wird eine Platte einer virtuellen Maschine (VM) in Sicherungsoperationen eingeschlossen. Wenn Sie nicht mindestens einen Plattenkennsatz angeben, werden alle Platten in der VM gesichert.
- Linux-BetriebssystemeWindows-BetriebssystemeINCLUDE.VMSNAPSHOTATTEMPTS
  Bestimmen Sie mithilfe der Option INCLUDE.VMSNAPSHOTATTEMPTS die Gesamtzahl Versuche, eine Momentaufnahme für eine Sicherungsoperation für eine virtuelle Maschine (VM) zu erstellen, die aufgrund eines Momentaufnahmefehlers fehlschlägt.
- Linux-BetriebssystemeWindows-BetriebssystemeINCLUDE.VMTSMVSS
  Mit der Option INCLUDE.VMTSMVSS werden Anwendungen einer virtuellen Maschine benachrichtigt, dass eine Sicherung bevorsteht. Durch diese Option ist es möglich, dass die Anwendung Transaktionsprotokolle abschneidet und Transaktionen festschreibt, so dass sie nach Beendigung der Sicherung in einem konsistenten Zustand fortfahren kann. Ein optionaler Parameter kann angegeben werden, der das Abschneiden der Transaktionsprotokolle unterdrückt. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Zugehörige Verweise:
Include.vmdisk
INCLUDE.VMTSMVSS
INCLUDE.VMSNAPSHOTATTEMPTS
Linux-BetriebssystemeWindows-Betriebssysteme

Include.vm

Bei VM-Operationen überschreibt diese Option die Verwaltungsklasse, die in der Option vmmc angegeben ist.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Die in der Option vmmc angegebene Verwaltungsklasse gilt für alle VMware-Sicherungen.

Die in der Option vmmc angegebene Verwaltungsklasse gilt für alle Hyper-V-Sicherungen.

Sie können die Option include.vm verwenden, um diese Verwaltungsklasse für eine oder mehrere virtuelle Maschinen zu überschreiben. Die durch die Option vmctlmc angegebene Verwaltungsklasse wird durch die Option include.vm weder überschrieben noch beeinflusst. Die Option vmctlmc bindet Steuerdateien für gesicherte virtuelle Maschinen an eine bestimmte Verwaltungsklasse.

Unterstützte Clients

LinuxDiese Option kann für unterstützte Linux-Clients verwendet werden, die für die Sicherung virtueller VMware-Maschinen konfiguriert sind.

WindowsDiese Option kann für unterstützte Windows-Clients verwendet werden, die für die Sicherung virtueller VMware-Maschinen konfiguriert sind.

WindowsDiese Option kann für unterstützte Windows-Clients verwendet werden, die für die Sicherung virtueller Hyper-V-Maschinen konfiguriert sind.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei.

Syntax

```
>>-INCLUDE.VM-- --VM-Name-- --+-----------------------------+--><
                              '-Name_der_Verwaltungsklasse-'
```

Parameter

VM-Name
: Erforderlicher Parameter. Gibt den Namen einer virtuellen Maschine an, die Sie an die angegebene Verwaltungsklasse binden wollen. Der Name ist der Anzeigename der virtuellen Maschine. In jeder Anweisung include.vm kann nur eine einzige virtuelle Maschine angegeben werden. Sie können jedoch so viele include.vm-Anweisungen angeben wie für das Binden jeder virtuellen Maschine an eine bestimmte Verwaltungsklasse benötigt werden.

  Sie können Platzhalterzeichen im Namen der virtuellen Maschine verwenden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem einzelnen Zeichen. Wenn der Name der virtuellen Maschine ein Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen (") ein.

  Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, ersetzen Sie die Sonderzeichen durch das Platzhalterzeichen ? (Fragezeichen), wenn Sie den Namen der virtuellen Maschine angeben.

Verwaltungsklassenname
: Optionaler Parameter. Gibt die Verwaltungsklasse an, die bei der Sicherung der angegebenen virtuellen Maschine verwendet werden soll. Wird dieser Parameter nicht angegeben, wird standardmäßig die globale Verwaltungsklasse für virtuelle Maschinen verwendet, die durch die Option vmmc angegeben ist.

Beispiele

Für diese Beispiele wird vorausgesetzt, dass die folgenden Verwaltungsklassen vorhanden und auf dem IBM Spectrum Protect-Server aktiv sind:

- MCFORTESTVMS
- MCFORPRODVMS
- MCUNIQUEVM

Beispiel 1
: Mit der folgenden Anweisung include.vm in der Clientoptionsdatei werden alle virtuellen Maschinen, deren Namen mit VMTEST beginnen, an die Verwaltungsklasse MCFORTESTVMS gebunden:

  ```
  include.vm vmtest* MCFORTESTVMS
  ```

Beispiel 2
: Mit der folgenden Anweisung include.vm in der Clientoptionsdatei wird die virtuelle Maschine mit dem Namen WHOPPER VM1 [PRODUCTION] an die Verwaltungsklasse MCFORPRODVMS gebunden:

  ```
  include.vm "WHOPPER VM1 ?PRODUCTION?" MCFORPRODVMS
  ```

  Der Name der virtuellen Maschine muss in Anführungszeichen eingeschlossen werden, weil er Leerzeichen enthält. Außerdem wird das Fragezeichen als Platzhalterzeichen für die Sonderzeichen im Namen der virtuellen Maschine verwendet.

Beispiel 3
: Mit der folgenden Anweisung include.vm in der Clientoptionsdatei wird die virtuelle Maschine VM1 an die Verwaltungsklasse MCUNIQUEVM gebunden:

  ```
  include.vm VM1 MCUNIQUEVM
  ```

Linux-Betriebssysteme Windows-Betriebssysteme

Include.vmdisk

Mit der Option INCLUDE.VMDISK wird eine Platte einer virtuellen Maschine (VM) in Sicherungsoperationen eingeschlossen. Wenn Sie nicht mindestens einen Plattenkennsatz angeben, werden alle Platten in der VM gesichert.

Diese Option ist nur verfügbar, wenn Sie das lizenzierte Produkt 'IBM Spectrum Protect for Virtual Environments' verwenden. Weitere Informationen zu dieser Option finden Sie in der Produktdokumentation zu IBM Spectrum Protect for Virtual Environments im IBM® Knowledge Center unter http://www.ibm.com/support/knowledgecenter/SSERB6/welcome.

Die Option INCLUDE.VMDISK gibt den Kennsatz einer VM-Platte an, die in eine Operation backup vm eingeschlossen werden soll. Wenn Sie im Befehl backup vm eine Platte einschließen, überschreiben die Befehlszeilenparameter alle Anweisungen INCLUDE.VMDISK in der Optionsdatei.

Diese Option gilt sowohl für Platten virtueller VMware-Maschinen als auch für Platten virtueller Microsoft Hyper-V-Maschinen.

Linux-Betriebssysteme Windows-Betriebssysteme

INCLUDE.VMDISK für virtuelle VMware-Maschinen

Verwenden Sie die Option INCLUDE.VMDISK, um eine virtuelle VMware-Maschine in Sicherungsoperationen einzuschließen.

Unterstützte Clients

 Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

 Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Befehlszeilenparameter überschreiben Anweisungen in der Optionsdatei.

Syntax für virtuelle VMware-Maschinen

```
>>-INCLUDE.VMDISK--VM-Name-- -VM-Plattenkennsatz--------------><
```

Parameter

VM-Name
Gibt den Namen der virtuellen Maschine an, die eine Platte enthält, die in eine Operation Backup VM eingeschlossen werden soll. Der Name ist der Anzeigename der virtuellen Maschine. In jeder Anweisung INCLUDE.VMDISK können Sie nur den Namen einer einzigen virtuellen Maschine angeben. Geben Sie zusätzliche INCLUDE.VMDISK-Anweisungen für jede Platte einer virtuellen Maschine, die Sie einschließen wollen, an.
Der Name der virtuellen Maschine kann einen Stern (*) enthalten, der einer beliebigen Zeichenfolge entspricht, und ein Fragezeichen (?), das einem beliebigen einzelnen Zeichen entspricht. Schließen Sie den VM-Namen in Anführungszeichen (" ") ein, wenn der VM-Name Leerzeichen enthält.
Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, wie z. B. eckige Klammern ([oder]), wird der Name der virtuellen Maschine möglicherweise nicht korrekt abgeglichen. Enthält der Name der virtuellen Maschine Sonderzeichen, müssen Sie möglicherweise ein Fragezeichen (?) verwenden, um die Sonderzeichen im VM-Namen abzugleichen.

Um beispielsweise `Festplatte 1` in die Sicherung einer virtuellen Maschine mit dem Namen `"Windows VM3 [2012R2]"` einzuschließen, verwenden Sie diese Syntax in der Optionsdatei: `INCLUDE.VMDISK "Windows VM3 ?2012R2?" "Festplatte 1"`.

VM-Plattenkennsatz
Gibt den Plattenkennsatz der Platte an, die eingeschlossen werden soll. Platzhalterzeichen sind nicht zulässig. Verwenden Sie den Befehl Backup VM mit der Option -preview, um die Plattenkennsätze der Platten in einer bestimmten virtuellen Maschine zu bestimmen. Informationen zur Syntax finden Sie in der Beschreibung des Befehls "Backup VM".

Beispiele

Optionsdatei
Beispiel: Eine virtuelle Maschine mit dem Namen vm1 enthält vier Platten mit den Kennsätzen "Festplatte 1", "Festplatte 2", "Festplatte 3" und "Festplatte 4". Um nur Festplatte 2 in Operationen Backup VM einzuschließen, geben Sie in der Optionsdatei Folgendes an:

```
INCLUDE.VMDISK "vm1" "Festplatte 2"
```

Festplatte 2 und Festplatte 3 in Operationen Backup VM einschließen:

```
INCLUDE.VMDISK "vm1" "Festplatte 2"
INCLUDE.VMDISK "vm1" "Festplatte 3"
```

Befehlszeile:
Eine einzelne Platte bei der Sicherung von vm1 einschließen:

```
dsmc backup vm "vm1:vmdk=Festplatte 1"
```

Festplatte 2 und Festplatte 3 bei der Sicherung von vm1 einschließen:

```
dsmc backup vm "vm1:vmdk=Festplatte 2:vmdk=Festplatte 3"
```

 Windows-Betriebssysteme

INCLUDE.VMDISK für virtuelle Microsoft Hyper-V-Maschinen

Verwenden Sie die Option INCLUDE.VMDISK, um eine VM-Platte in Hyper-V-RCT-Sicherungsoperationen unter dem Betriebssystem Windows Server 2016 oder Betriebssystemen einer höheren Version einzuschließen.

Unterstützte Clients

Diese Option kann mit Clients unter Windows Server 2016 oder Betriebssystemen einer höheren Version verwendet werden.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Befehlszeilenparameter überschreiben Anweisungen in der Optionsdatei.

Syntax für virtuelle Microsoft Hyper-V-Maschinen

```
>>-INCLUDE.VMDISK--VM-Name-- -Plattenposition------------------><
```

Parameter

VM-Name
Gibt den Namen der VM an, die eine Platte enthält, die in eine Operation backup vm eingeschlossen werden soll. Der Name ist der Anzeigename der virtuellen Maschine. In jeder Anweisung INCLUDE.VMDISK können Sie nur einen einzigen VM-Namen angeben. Geben Sie weitere Anweisungen INCLUDE.VMDISK für jede VM-Platte an, die eingeschlossen werden soll.
Der VM-Name kann einen Stern (*) enthalten, der einer beliebigen Zeichenfolge entspricht, und ein Fragezeichen (?), das einem beliebigen einzelnen Zeichen entspricht. Wenn der VM-Name Leerzeichen enthält, schließen Sie ihn in Anführungszeichen (" ") ein.
Tipp: Wenn der VM-Name Sonderzeichen enthält, wie beispielsweise eckige Klammern ([oder]), wird der VM-Name möglicherweise nicht korrekt abgeglichen. Wenn ein VM-Name Sonderzeichen enthält, stellen Sie die Sonderzeichen mithilfe von Fragezeichen (?) dar.
Um beispielsweise eine SCSI-VM-Platte in die Sicherung einer virtuellen Maschine mit dem Namen `"Windows VM3 [2012R2]"` einzuschließen, verwenden Sie in der Optionsdatei die folgende Syntax:

```
INCLUDE.VMDISK "Windows VM3 ?2012R2?" "SCSI 0 1"
```

Plattenposition
Geben Sie die Position der VM-Platte an, die in eine Hyper-V-RCT-Sicherungsoperation eingeschlossen werden soll. Die Plattenpositionsbezeichnung muss mit "SCSI" oder "IDE" beginnen, gefolgt von der Controllernummer und der Einheitenpositionsnummer. Platzhalterzeichen sind nicht zulässig.
Tipp: Verwenden Sie den Befehl backup vm mit der Option -preview, um die Position der Platten in einer bestimmten VM zu bestimmen. Informationen zur Syntax finden Sie in der Beschreibung des Befehls "Backup VM".

Beispiele

Optionsdatei
Die virtuelle Maschine `vm1` enthält eine IDE-VM-Platte (VHDX) mit der Controllernummer 1 und der Einheitenposition 0. Um diese VHDX in Operationen backup vm einzuschließen, geben Sie in der Optionsdatei die folgende Anweisung an:

```
INCLUDE.VMDISK vm1 "IDE 1 0"
```

Die virtuelle Maschine `vm2` enthält eine SCSI-VM-Platte mit Controllernummer 0 und Einheitenposition 1. Schließen Sie diese VHDX in Sicherungsoperationen ein, indem Sie in der Optionsdatei die folgende Anweisung angeben:

```
INCLUDE.VMDISK vm2 "SCSI 0 1"
```

Befehlszeile:
Schließen Sie eine einzelne IDE-Platte (mit der Controllernummer 1 und der Einheitenposition 0) in die Sicherungsoperation für die virtuelle Maschine `vm1` ein:

```
dsmc backup vm "vm1:vhdx=IDE 1 0"
```

Schließen Sie eine SCSI-Platte (mit der Controllernummer 0 und der Einheitenposition 1) in die Sicherungsoperation für die virtuelle Maschine `vm2` ein:

```
dsmc backup vm "vm2:vhdx=SCSI 0 1"
```

Zugehörige Verweise:
Backup VM
Restore VM
Domain.vmfull
Exclude.vmdisk
 Linux-Betriebssysteme  Windows-Betriebssysteme

INCLUDE.VMSNAPSHOTATTEMPTS

Bestimmen Sie mithilfe der Option INCLUDE.VMSNAPSHOTATTEMPTS die Gesamtzahl Versuche, eine Momentaufnahme für eine Sicherungsoperation für eine virtuelle Maschine (VM) zu erstellen, die aufgrund eines Momentaufnahmefehlers fehlschlägt.

Unterstützte Clients

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

 Diese Option kann für unterstützte Linux-Clients verwendet werden, die für die Sicherung virtueller VMware-Maschinen konfiguriert sind.

 Diese Option kann für unterstützte Windows-Clients verwendet werden, die für die Sicherung virtueller VMware-Maschinen konfiguriert sind.

 Diese Option kann für unterstützte Windows-Clients verwendet werden, die für die Sicherung von VMs auf Hyper-V-Hosts konfiguriert sind, die unter Windows Server 2016-Betriebssystemen ausgeführt werden.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie ist nicht in der Befehlszeile gültig.

Syntax

```
>>-INCLUDE.VMSNAPSHOTATTEMPTS--VM-Name--------------------------->

>--Anzahl_mit_Stilllegung--Anzahl_ohne_Stilllegung------------><
```

Parameter

VM-Name

Ein erforderlicher positionsgebundener Parameter, der den Namen der virtuellen Maschine angibt, für die die Gesamtzahl Versuche zur Erstellung einer Momentaufnahme ausgeführt werden soll, wenn ein Sicherungsversuch aufgrund eines Momentaufnahmefehlers fehlschlägt. Der Name ist der Anzeigename der virtuellen Maschine.
In einer Anweisung INCLUDE.VMSNAPSHOTATTEMPTS kann nur jeweils eine virtuelle Maschine angegeben werden. Sie können jedoch mit den folgenden Methoden die Gesamtzahl Versuche zur Erstellung einer Momentaufnahme für andere virtuelle Maschinen konfigurieren:

- Geben Sie für jede virtuelle Maschine, für die diese Option gelten soll, so viele Anweisungen INCLUDE.VMSNAPSHOTATTEMPTS an. wie Wiederholungsversuche zur Erstellung von Momentaufnahmen, die fehlgeschlagen sind, erforderlich sind.
- Verwenden Sie Platzhalterzeichen für den Parameterwert *VM-Name*, um Namen virtueller Maschinen anzugeben, die mit dem Platzhalterzeichenmuster übereinstimmen. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem einzelnen Zeichen. Wenn der Name der virtuellen Maschine ein Leerzeichen enthält, schließen Sie den Namen in Anführungszeichen (") ein.

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, ersetzen Sie die Sonderzeichen durch das Platzhalterzeichen ? (Fragezeichen), wenn Sie den Namen der virtuellen Maschine angeben.

Anzahl_mit_Stilllegung

Ein positionsgebundener Parameter, der die folgende Aktion angibt:

Für VMware-Sicherungsoperation:

- Für virtuelle Windows-Maschinen mit aktiviertem IBM Spectrum Protect-Anwendungsschutz gibt *Anzahl_mit_Stilllegung* die Anzahl auszuführender Versuche zur Erstellung der Momentaufnahme mit IBM Spectrum Protect-VSS-Stilllegung und Microsoft Windows-System-Provider-VSS-Stilllegung an. VSS-Stilllegung ist nur für virtuelle Windows-Maschinen gültig.

  Abhängig von der von Ihnen angegebenen Anzahl, erfolgt der erste Versuch zur Erstellung einer Momentaufnahme immer mit IBM Spectrum Protect-VSS-Stilllegung. Nachfolgende Versuche zur Erstellung einer Momentaufnahme erfolgen mit Windows-System-Provider-VSS-Stilllegung.

- Für virtuelle Windows-Maschinen ohne aktivierten IBM Spectrum Protect-Anwendungsschutz und für virtuelle Linux-Maschinen gibt *Anzahl_mit_Stilllegung* die Anzahl Versuche zur Erstellung einer Momentaufnahme mit VMware Tools-Dateisystemstilllegung an.

Der Maximalwert, den Sie angeben können, ist zehn (10). Der Standardwert ist zwei (2). Der Mindestwert, den Sie angeben können, ist null (0).

Für Hyper-V-RCT-Sicherungsoperationen:
Der Parameter *Anzahl_mit_Stilllegung* gibt an, wie oft versucht werden soll, Momentaufnahmen mit Stilllegung zu erstellen, um anwendungskonsistente Sicherungen zu erstellen.

Sie können einen Wert im Bereich von 0 bis 10 angeben. Der Standardwert ist 2.

Anzahl_ohne_Stilllegung

Für VMware-Sicherungsoperation:
Ein positionsgebundener Parameter, der die Anzahl Versuche zur Erstellung einer Momentaufnahme mit inaktivierter VMware Tools-Dateisystemstilllegung und Anwendungsstilllegung (VSS-Stilllegung) angibt, nachdem die angegebene Anzahl Versuche mit VSS-Stilllegung (*Anzahl_mit_Stilllegung*) ausgeführt wurde. Sie können diesen Parameter beispielsweise für eine virtuelle Maschine angeben, die bereits durch einen in einer virtuellen Gastmaschine installierten IBM® Data Protection-Agenten geschützt wird.

Der Maximalwert, den Sie angeben können, ist zehn (10). Der Mindestwert, den Sie angeben können und der gleichzeitig der Standardwert ist, ist null (0).

Wichtig: Wenn dieser Parameter auf die Sicherung einer virtuellen Maschine angewendet wird, wird die Sicherung als absturzkonsistent betrachtet. Demzufolge sind Betriebssystem-, Dateisystem- und Anwendungskonsistenz nicht garantiert. Ein Eintrag `include.vmsnapshotattempts 0 0` ist nicht gültig. Für Sicherungsoperationen ist mindestens eine Momentaufnahme erforderlich.

Für Hyper-V-RCT-Sicherungsoperationen:
Die Option *Anzahl_ohne_Stilllegung* gibt die Anzahl Versuche zur Erstellung von Momentaufnahmen ohne Stilllegung an, nachdem die angegebene Anzahl Versuche, die in der Option *Anzahl_mit_Stilllegung* angegeben ist, ausgeführt wurde.

Sie können einen Wert im Bereich von 0 bis 10 angeben. Der Standardwert ist 0.

Wichtig: Wenn dieser Parameter auf eine VM-Sicherung angewendet wird, wird die Sicherung als absturzkonsistent betrachtet. Demzufolge sind Betriebssystem-, Dateisystem- und Anwendungskonsistenz nicht garantiert. Ein Eintrag `include.vmsnapshotattempts 0 0` ist nicht gültig. Für Sicherungsoperationen ist mindestens eine Momentaufnahme erforderlich.

Beispiele

Beispiele für VMware:

Beispiel 1
Mit der folgenden Anweisung INCLUDE.VMSNAPSHOTATTEMPTS in der Clientoptionsdatei werden insgesamt zwei Versuche zur Erstellung einer Momentaufnahme (mit VSS-Stilllegung) für die virtuelle Maschine 'VM_a' ausgeführt:

```
INCLUDE.VMSNAPSHOTATTEMPTS VM_a 2 0
```

Beispiel 2
Mit der folgenden Anweisung INCLUDE.VMSNAPSHOTATTEMPTS in der Clientoptionsdatei werden insgesamt drei Versuche zur Erstellung einer Momentaufnahme für virtuelle Windows-Maschinen ausgeführt, deren Namen mit der Zeichenfolge 'vmServer_Dept*' übereinstimmen:

- Der erste Versuch erfolgt mit IBM Spectrum Protect-VSS-Stilllegung.
- Der zweite Versuch erfolgt mit Windows-System-Provider-VSS-Stilllegung.
- Der dritte Versuch zur Erstellung einer Momentaufnahme erfolgt ohne VSS-Stilllegung.

```
INCLUDE.VMSNAPSHOTATTEMPTS vmServer_Dept* 2 1
```

Beispiel 3
Mit der folgenden Anweisung INCLUDE.VMSNAPSHOTATTEMPTS in der Clientoptionsdatei wird insgesamt ein Versuch zur Erstellung einer Momentaufnahme (mit VSS-Stilllegung) für virtuelle Maschinen ausgeführt, deren Namen mit der Zeichenfolge 'vmDB_Dept*' übereinstimmen:

```
INCLUDE.VMSNAPSHOTATTEMPTS vmDB_Dept* 1 0
```

Beispiel 4
Mit der folgenden Anweisung INCLUDE.VMSNAPSHOTATTEMPTS in der Clientoptionsdatei werden insgesamt zwei Versuche zur Erstellung einer Momentaufnahme (mit VSS-Stilllegung) für alle virtuellen Maschinen ausgeführt:

- Der erste Versuch erfolgt mit IBM Spectrum Protect-VSS-Stilllegung.
- Der zweite Versuch erfolgt mit Windows-System-Provider-VSS-Stilllegung.

```
INCLUDE.VMSNAPSHOTATTEMPTS * 2 0
```

Beispiel 5
In diesem Beispiel verfügt die virtuelle Maschine DB15 über einen in einer virtuellen Gastmaschine installierten IBM Data Protection-Agenten und benötigt keine anwendungskonsistente Momentaufnahme. Mit der folgenden Anweisung INCLUDE.VMSNAPSHOTATTEMPTS in der Clientoptionsdatei wird insgesamt ein Versuch zur Erstellung einer Momentaufnahme (ohne VSS-Stilllegung) für die virtuelle Maschine DB15 ausgeführt:

```
INCLUDE.VMSNAPSHOTATTEMPTS DB15 0 1
```

Beispiele für Hyper-V:

Beispiel 1

Geben Sie die folgende Anweisung in der Clientoptionsdatei an, um insgesamt zwei Versuche zur Erstellung einer Momentaufnahme mit absturzkonsistenten Sicherungen für alle virtuellen Hyper-V-Maschinen auszuführen, deren Namen mit `LinuxVM` beginnen:

```
INCLUDE.VMSNAPSHOTATTEMPTS LinuxVM* 0 2
```

Beispiel 2

Geben Sie die folgende Anweisung in der Clientoptionsdatei an, um drei Versuche zur Erstellung einer Momentaufnahme für die virtuelle Maschine VM1 auszuführen: zwei Versuche zur Erstellung einer anwendungskonsistenten Momentaufnahme und - wenn diese fehlschlagen - ein Versuch zur Erstellung einer absturzkonsistenten Momentaufnahme:

```
INCLUDE.VMSNAPSHOTATTEMPTS VM1 2 1
```

Windows-BetriebssystemeInformationen zur Zurückschreibung von Sicherungen mit Anwendungsschutz finden Sie in Hinweise zu Schattenkopien für das Zurückschreiben einer Sicherung mit Anwendungsschutz von der Einheit zum Versetzen von Daten.

Zugehörige Verweise:
INCLUDE.VMTSMVSS
Linux-BetriebssystemeWindows-Betriebssysteme

INCLUDE.VMTSMVSS

Mit der Option INCLUDE.VMTSMVSS werden Anwendungen einer virtuellen Maschine benachrichtigt, dass eine Sicherung bevorsteht. Durch diese Option ist es möglich, dass die Anwendung Transaktionsprotokolle abschneidet und Transaktionen festschreibt, so dass sie nach Beendigung der Sicherung in einem konsistenten Zustand fortfahren kann. Ein optionaler Parameter kann angegeben werden, der das Abschneiden der Transaktionsprotokolle unterdrückt. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Wenn eine virtuelle Maschine durch diese Option eingeschlossen wird, stellt IBM Spectrum Protect Anwendungsschutz bereit. Das heißt, der Client blockiert (freeze) die VSS-Ausgabeprogramme, gibt sie frei (thaw) und schneidet optional die Anwendungsprotokolle ab. Wird eine virtuelle Maschine nicht durch diese Option geschützt, wird der Anwendungsschutz durch VMware bereitgestellt. VMware blockiert (freeze) die VSS-Ausgabeprogramme und gibt sie frei (thaw), aber Anwendungsprotokolle werden nicht abgeschnitten.

Wichtig: Bevor Sie anfangen, Sicherungen mit Anwendungsschutz auszuführen, müssen Sie sicherstellen, dass sich die Anwendungsdatenbank, z. B. Microsoft SQL Server oder Microsoft Exchange Server, auf einem beliebigen Laufwerk befindet, das kein Bootlaufwerk ist, falls eine Operation diskshadow revert während der Zurückschreibung erforderlich ist.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Diese Option kann nicht vom Profileditor und nicht in der Befehlszeile angegeben werden.

Syntax

```
>>-INCLUDE.VMTSMVSS----VM-Name---- --OPTions=KEEPSqllog-------><
```

Parameter

VM-Name

Gibt den Namen der virtuellen Maschine an, die die Anwendungen enthält, die in den Wartemodus versetzt werden sollen. Der Name ist der Anzeigename der virtuellen Maschine. Geben Sie eine einzige virtuelle Maschine pro Anweisung INCLUDE.VMTSMVSS an. Um beispielsweise eine virtuelle Maschine mit dem Namen 'Windows VM3 [2012R2]' einzuschließen, verwenden Sie diese Syntax in der Optionsdatei: `INCLUDE.VMTSMVSS "Windows VM3 [2012R2]"`.

Verwenden Sie einen Stern als Platzhalterzeichen, um alle virtuellen Maschinen mit dieser Option zu schützen (INCLUDE.VMTSMVSS *). Sie können auch Fragezeichen als Platzhalterzeichen für beliebige einzelne Zeichen verwenden. Mit der Angabe INCLUDE.VMTSMVSS vm?? werden z. B. alle virtuellen Maschinen geschützt, deren Namen mit 'vm' und zwei beliebigen weiteren Zeichen beginnen (vm10, vm11, vm17 usw.).

Tipp: Wenn der Name der virtuellen Maschine Sonderzeichen enthält, wie z. B. eckige Klammern ([oder]), wird der Name der virtuellen Maschine möglicherweise nicht korrekt abgeglichen. Enthält der Name einer virtuellen Maschine Sonderzeichen, können Sie mit dem Fragezeichen (?) die Sonderzeichen im VM-Namen abgleichen.

Für diesen Parameter gibt es keinen Standardwert. Sie müssen virtuelle Maschinen, die geschützt werden sollen, in mindestens einer Anweisung INCLUDE.VMTSMVSS angeben, um den Anwendungsschutz zu aktivieren. Stellen Sie sicher, dass keine Platte in einer virtuellen

Maschine ausgeschlossen wird (mit der Option EXCLUDE.VMDISK), wenn die Platte Anwendungsdaten enthält, die geschützt werden sollen.

OPTions=KEEPSqllog
Wenn der Parameter `OPTions KEEPSqllog` in einer Anweisung INCLUDE.VMTSMVSS angegeben wird, verhindert er, dass SQL Server-Protokolle abgeschnitten werden, wenn ein Client für Sichern/Archivieren, der auf einem Knoten der Einheit zum Versetzen von Daten installiert ist, eine virtuelle Maschine sichert, auf der ein SQL Server ausgeführt wird. Die Angabe dieses Parameters ermöglicht es dem SQL Server-Administrator, die SQL Server-Protokolle manuell zu verwalten (sichern und ggf. abschneiden), sodass sie beibehalten und für die Zurückschreibung von SQL-Transaktionen an einen bestimmten Prüfpunkt verwendet werden können, nachdem die virtuelle Maschine zurückgeschrieben wurde.
Wenn diese Option angegeben wird, wird das SQL-Protokoll nicht abgeschnitten und die folgende Nachricht wird angezeigt und auf dem Server protokolliert:

```
ANS4179I Der IBM Spectrum Protect-Anwendungsschutzhat die Microsoft SQL
Server-Protokolle auf der virtuellen Maschine 'VM' nicht abgeschnitten.
```

Sie können die Option `OPTIONS=KEEPSQLLOG` entfernen, um das Abschneiden der SQL-Protokolle bei Beendigung einer Sicherung zu ermöglichen.
Anmerkung: Der Client sichert nicht die SQL-Protokolldateien. Der SQL-Administrator muss die Protokolldateien sichern, damit sie nach dem Zurückschreiben der Datenbank angewendet werden können.

Beispiele

Optionsdatei
Anwendungsschutz für eine virtuelle Maschine mit dem Namen 'vm_example' konfigurieren:

```
INCLUDE.VMTSMVSS vm_example
```

Anwendungsschutz für vm11, vm12 und vm15 konfigurieren:

```
INCLUDE.VMTSMVSS vm11
INCLUDE.VMTSMVSS vm12
INCLUDE.VMTSMVSS vm15 options=keepsqllog
```

Befehlszeile:
Nicht gültig. Diese Option kann nicht in der Befehlszeile angegeben werden.

Zugehörige Konzepte:
Windows-BetriebssystemeHinweise zu Schattenkopien für das Zurückschreiben einer Sicherung mit Anwendungsschutz von der Einheit zum Versetzen von Daten
Zugehörige Verweise:
Vmtimeout
Exclude.vmdisk
Include.vmdisk
INCLUDE.VMSNAPSHOTATTEMPTS

Incrbydate

Verwenden Sie die Option incrbydate im Befehl incremental, um neue und geänderte Dateien zu sichern, deren Änderungsdatum nach dem Datum der letzten auf dem Server gespeicherten Teilsicherung liegt (sofern die Dateien nicht von der Sicherung ausgeschlossen sind).

Wichtig: Dateien, die nach der Verarbeitung des jeweiligen Verzeichnisses durch den Client für Sichern/Archivieren, aber vor Vollendung der Teilsicherung nach Datum geändert oder erstellt werden, werden nicht gesichert und werden auch in zukünftigen Teilsicherungen nach Datum nicht gesichert; es sei denn, die Dateien werden erneut geändert. Führen Sie aus diesem Grund eine regelmäßige reguläre Teilsicherung ohne Angabe der Option incrbydate aus.

Eine Teilsicherung nach Datum aktualisiert das Datum und die Uhrzeit der letzten Teilsicherung auf dem Server. Wenn Sie eine Teilsicherung nach Datum nur für einen Teil eines Dateisystems ausführen, wird das Datum der letzten vollständigen Teilsicherung nicht aktualisiert und bei der nächsten Teilsicherung nach Datum werden die Dateien erneut gesichert.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWichtig:

Mac OS X-BetriebssystemeDer Zeitpunkt der letzten Teilsicherung bezieht sich auf die Serverzeit und der Zeitpunkt der letzten Dateiänderung auf die Clientzeit. Sind die Clientzeit und die Serverzeit nicht synchronisiert oder befinden der Client und der Server sich in verschiedenen Zeitzonen, wirkt sich dies auf die Teilsicherung nach Datum mit `mode=incremental` aus.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDer Zeitpunkt der letzten Teilsicherung bezieht sich auf die Serverzeit und der Zeitpunkt der letzten Dateiänderung auf die Clientzeit. Sind die Clientzeit und die Serverzeit nicht synchronisiert oder befinden der Client und der Server sich in verschiedenen Zeitzonen, wirkt sich dies auf die Teilsicherung nach Datum und die Imagesicherung mit `mode=incremental` aus.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Sowohl bei vollständigen Teilsicherungen als auch bei Teilsicherungen nach Datum werden neue und geänderte Dateien gesichert. Eine Teilsicherung nach Datum hat eine kürzere Verarbeitungszeit als eine vollständige Teilsicherung und benötigt weniger Speicherbereich. Anders als eine vollständige Teilsicherung hält eine Teilsicherung nach Datum den Serverspeicher jedoch nicht auf dem aktuellen Stand aller Workstationdateien, weil:

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeSicherungsversionen von Dateien, die aus der Workstation gelöscht wurden, hierbei nicht verfallen.
- Sicherungsversionen nicht erneut an eine neue Verwaltungsklasse gebunden werden, wenn sich die Verwaltungsklasse geändert hat.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDateien mit geänderten Attributen, wie z. B. ACL-Daten (ACL = Access Control List, Zugriffssteuerungsliste) nur dann gesichert werden, wenn sich auch das Änderungsdatum und die Änderungszeit geändert haben.
- Windows-BetriebssystemeDateien mit geänderten Attributen, wie z. B. NTFS-Sicherheitsinformationen, nur dann gesichert werden, wenn sich auch das Änderungsdatum und die Änderungszeit geändert haben.
- Das Attribut 'Häufigkeit' der Kopiengruppe in den Verwaltungsklassen ignoriert wird.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme Tipp: Wenn während der Woche zu wenig Zeit für Sicherungen zur Verfügung steht, aber freie Zeit am Wochenende vorhanden ist, können Sie den Serverspeicher Ihrer Workstationdateien durch eine Teilsicherung mit der Option incrbydate an den Wochentagen und eine vollständige Teilsicherung am Wochenende auf dem aktuellen Stand halten.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-INCRbydate-------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc incremental -incrbydate
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Incremental

Verwenden Sie die Option incremental im Befehl restore image, um sicherzustellen, dass am Basisimage vorgenommene Änderungen auch auf das zurückgeschriebene Image angewendet werden.

Wird außerdem die Option deletefiles verwendet, beinhalten die Änderungen das Löschen von Dateien und Verzeichnissen, die in dem ursprünglichen Image waren, später aber aus der Workstation gelöscht wurden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAnmerkung: Die Verwendung der Option incremental im Befehl restore image zur Ausführung einer dynamischen Imagesicherung wird nicht unterstützt.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist nur für AIX, Linux x86_64, Linux on POWER und Solaris gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-INCREmental-----------------------------------------------><
```

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme`res i "/home/devel/projecta/*" -incremental`

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`res i d: -incremental`

Windows-Betriebssysteme

Incrthreshold

Die Option incrthreshold gibt den Schwellenwert für die Anzahl Verzeichnisse in einem Journaldateibereich an, für die aktive Objekte auf dem Server, aber keine äquivalenten Objekte auf der Workstation vorhanden sein können.

Wenn ein Windows-Client eine Datei oder ein Verzeichnis mit einem langen Namen löscht, wird dies gelegentlich unter Verwendung eines komprimierten Namens gemeldet. Nach dem Löschen des Objekts könnte der komprimierte Name erneut verwendet werden, und der Löschhinweis gibt möglicherweise kein eindeutiges Objekt mehr an. Während einer Journalteilsicherung eines Dateibereichs kann dies eine Antwort *keine aktive Version* vom Server auslösen und einen nicht erfolgreichen Verfall eines Objekts verursachen.

Mit der Option incrthreshold können Sie angeben, was passieren soll, wenn diese Situation eintritt:

- Wenn Sie die Option incrthreshold auf 0 (den Standardwert) setzen, wird keine Aktion ausgeführt. Die wichtigste Konsequenz dieser Einstellung besteht darin, dass diese Objekte während einer Zurückschreibung eines solchen Verzeichnisses versehentlich zurückgeschrieben werden könnten. Bei der nächsten Nicht-Journalteilsicherung für dieses Verzeichnis lässt der IBM Spectrum Protect-Server alle Objekte in dem Verzeichnis verfallen, die auf dem Server, aber nicht auf der Workstation vorhanden sind.
- Wenn Sie einen Wert größer 0 angeben, speichert der Client bei Journalsicherungen den Verzeichnisnamen eines Objekts im Journal. Wenn während einer vollständigen Journalteilsicherung eines Dateibereichs die Anzahl der Verzeichnisse in dem Dateibereich mindestens so groß wie dieser Wert ist, erfolgt eine vollständige Teilsicherung jedes Verzeichnisses. Dies findet automatisch nach Beendigung der Journalsicherung statt und erfordert keine weitere Befehlseingabe.
- Wenn Sie die Option incrthreshold auf 1 setzen, führt der Client eine vollständige Teilsicherung dieser Verzeichnisse aus, sobald während einer vollständigen Journalteilsicherung eines Dateibereichs die Antwort *keine aktive Version* empfangen wird.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option im Feld Sichern > Schwellenwert für Teilsicherung ohne Journal im Profileditor definieren.

Syntax

```
>>-INCRTHreshold--Verzeichnisanzahl----------------------------><
```

Parameter

Verzeichnisanzahl
Gibt den Schwellenwert für die Anzahl Verzeichnisse in einem Journaldateibereich an, der aktive Dateien enthalten könnte, die verfallen sollten. Wenn dieser Schwellenwert während einer vollständigen Journalteilsicherung eines Dateibereichs erreicht wird, leitet der Client nach Beendigung der Journalsicherung eine Teilsicherung für jedes dieser Verzeichnisse ein. Gültige Werte sind 0 bis 2.000.000.000. Der Standardwert ist 0.

Beispiele

Optionsdatei:

```
incrthreshold 1
```

Befehlszeile:

```
-increthreshold=1
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Instrlogmax

Die Option instrlogmax gibt die maximale Größe des Instrumentierungsprotokolls (dsminstr.log) in MB an. Während der Sicherungs- oder Zurückschreibungsverarbeitung werden Leistungsdaten für den Client in der Datei dsminstr.log erfasst, wenn die Option enableinstrumentation auf *yes* gesetzt ist.

Wenn Sie den Wert der Option instrlogmax ändern, wird das vorhandene Protokoll erweitert oder gekürzt, um der neuen Größe zu entsprechen. Wird der Wert verkleinert, werden die ältesten Einträge gelöscht, um die Datei auf die neue Größe zu verkleinern.

Unterstützte Clients

Diese Option ist für alle Clients und die IBM Spectrum Protect-API gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Syntax

```
>>-INSTRLOGMAX-- --Größe----------------------------------------><
```

Parameter

Größe
: Gibt die maximale Größe für die Instrumentierungsprotokolldatei in MB an. Der Wertebereich ist 0 bis 2047. Der Standardwert ist 25.

  Wenn die Größe der Datei dsminstr.log die maximale Größe überschreitet, wird die Protokolldatei in dsminstr.log.bak umbenannt. Nachfolgende Instrumentierungsdaten werden weiterhin in der Datei dsminstr.log gesichert.

  Wenn Sie 0 angeben, wächst die Protokolldatei unbegrenzt an.

Beispiele

Optionsdatei:

```
instrlogmax 100
```

Befehlszeile:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-Betriebssysteme`dsmc sel /home/mydir/* -subdir=yes -enableinstrumentation=yes -instrlogmax=100`

 Windows-Betriebssysteme`dsmc sel c:\mydir\* -subdir=yes -enableinstrumentation=yes -instrlogmax=100`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Verweise:
Enableinstrumentation
Instrlogname

Instrlogname

Die Option instrlogname gibt den Pfad und den Namen der Datei an, in der Leistungsdaten gespeichert werden sollen, die der Client für Sichern/Archivieren erfasst.

Wenn Sie die Option enableinstrumentation yes verwenden, um Leistungsdaten während der Ausführung von Sicherungs- und Zurückschreibungsoperationen zu erfassen, speichert der Client die Informationen automatisch in einer Protokolldatei.

Standardmäßig werden die Leistungsdaten in der Instrumentierungsprotokolldatei (dsminstr.log) in dem Verzeichnis gespeichert, das mit der Umgebungsvariablen DSM_LOG (oder der Umgebungsvariablen DSMI_LOG für die API-abhängigen Produkte IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server und IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server) angegeben wird. Wenn Sie die Umgebungsvariable DSM_LOG nicht definiert haben, wird die Instrumentierungsprotokolldatei im aktuellen Verzeichnis gespeichert (das Verzeichnis, in dem der Befehl dsmc ausgegeben wurde).

Verwenden Sie diese Option nur, wenn der Dateiname und die Position des Instrumentierungsprotokolls geändert werden sollen.

Soll die Größe der Protokolldatei gesteuert werden, verwenden Sie die Option instrlogmax.

Unterstützte Clients

Diese Option ist für alle Clients und die IBM Spectrum Protect-API gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Wichtig: Geben Sie für die Umgebungsvariable `DSM_LOG` ein Verzeichnis an, in das das Protokoll gestellt werden soll. Das angegebene Verzeichnis muss Berechtigungen aufweisen, die einen Schreibzugriff von dem Konto zulassen, unter dem der Client ausgeführt wird. Das Stammverzeichnis ist kein gültiger Wert für `DSM_LOG`.
Windows-Betriebssysteme
Wichtig: Geben Sie für die Umgebungsvariable `DSM_LOG` ein Verzeichnis an, in das das Protokoll gestellt werden soll. Das angegebene Verzeichnis muss Berechtigungen aufweisen, die einen Schreibzugriff von dem Konto zulassen, unter dem der Client ausgeführt wird.

Syntax

```
>>-INSTRLOGNAME-- --Dateispezifikation-------------------------><
```

Parameter

Dateispezifikation
Gibt den Pfad und den Namen der Datei an, in der Leistungsdaten während der Sicherungs- und Zurückschreibungsverarbeitung gespeichert werden sollen. Wenn ein Teil des von Ihnen angegebenen Pfads nicht vorhanden ist, versucht der Client, ihn zu erstellen.

Windows-BetriebssystemeWird nur ein Dateiname angegeben, wird die Datei in dem Verzeichnis gespeichert, das mit der Umgebungsvariablen DSM_LOG angegeben wird. Wenn Sie die Umgebungsvariable DSM_LOG nicht definiert haben, wird die Instrumentierungsprotokolldatei im aktuellen Verzeichnis gespeichert (das Verzeichnis, in dem der Befehl dsmc ausgegeben wurde).

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWird nur ein Dateiname angegeben, wird die Datei in dem Verzeichnis gespeichert, das mit der Umgebungsvariablen DSM_LOG angegeben wird. Wenn Sie die Umgebungsvariable DSM_LOG nicht definiert haben, wird die Instrumentierungsprotokolldatei im aktuellen Verzeichnis gespeichert (das Verzeichnis, in dem der Befehl dsmc ausgegeben wurde). Die Instrumentierungsprotokolldatei kann keine symbolische Verbindung sein.

Mac OS X-BetriebssystemeFür Mac OS X: Wenn Sie nur einen Dateinamen angeben, wird die Datei in Ihrem Standardordner gespeichert. Die Standardverzeichnisse sind:

```
~/Library/Logs/tivoli/tsm
/Library/Logs/tivoli/tsm
```

Dieser Instrumentierungsprotokolldateiname ersetzt den vorherigen Instrumentierungsprotokolldateinamen dsminstr.report.pXXX, der von der Option TESTFLAG=instrument:detail oder instrument:API erstellt wurde.

Beispiele

Optionsdatei:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeFür AIX-, Linux- und Oracle Solaris-Clients:

```
instrlogname /home/user1/mydir/mydsminstr.log
```

Mac OS X-BetriebssystemeFür Mac OS X-Clients:

```
instrlogname /Users/user1/Library/Logs/mydsminstr.log
```

Windows-BetriebssystemeFür Windows-Clients:

```
instrlogname c:\mydir\mydsminstr.log
```

Befehlszeile:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeFür AIX-, Linux- und Oracle Solaris-Clients:

```
dsmc sel /home/user1/mydir/* -subdir=yes -instrlogname=/usr/log/mydsminstr.log
```

Mac OS X-BetriebssystemeFür Mac OS X-Clients:

```
dsmc sel /Users/user1/mydir/* -subdir=yes -instrlogname=/Users/user1/Library/Logs/mydsminstr.log
```

Windows-BetriebssystemeFür Windows-Clients:

```
dsmc sel c:\mydir\* -subdir=yes -instrlogname=c:\temp\mydsminstr.log
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Verweise:
Enableinstrumentation
Instrlogmax
 Windows-Betriebssysteme

Journalpipe

Die Option journalpipe gibt den Namen der Pipe eines Journaldämonsitzungsmanagers an, zu dem die Sicherungsclients eine Verbindung herstellen.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

```
JournalPipe \\.\pipe\jnlSessionMgr1
```

Syntax

```
>>-JOURNALPipe--Pipename----------------------------------------><
```

Parameter

Pipename
Geben Sie den Namen der Pipe an, der der Client während einer journalbasierten Sicherung zugeordnet wird. Der Standardpipename ist \\.\pipe\jnlSessionMgr.

Beispiele

Optionsdatei:

```
JOURNALPipe \\.\pipe\jnlSessionMgr
```

Befehlszeile:
Diese Option kann nicht in der Befehlszeile angegeben werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Lanfreecommmethod

Die Option lanfreecommmethod gibt das Übertragungsprotokoll zwischen dem IBM Spectrum Protect-Client und dem Speicheragenten an. Dadurch wird die Verarbeitung zwischen dem Client und der an SAN angeschlossenen Speichereinheit aktiviert.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeBei Verwendung der LAN-Übernahme müssen Sie lanfreecommmethod in der Datei dsm.sys innerhalb einer Serverzeilengruppe angegeben haben.

 Windows-BetriebssystemeBei Verwendung der LAN-Übernahme müssen Sie lanfreecommmethod TCPip in der Clientoptionsdatei (dsm.opt) angegeben haben.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeFür AIX, Linux und Solaris: Verwenden Sie die Option lanfreeshmport, um die Shared-Memory-Anschlussnummer anzugeben, an der der Speicheragent empfangsbereit ist.

 Windows-BetriebssystemeFür Windows: Verwenden Sie die Option lanfreeshmport, um den Speicheragenten eindeutig anzugeben, zu dem der Client eine Verbindung herzustellen versucht.

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

 Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-LANFREECommmethod-- --Übertragungsmethode------------------><
```

Parameter

Übertragungsmethode
Gibt das unterstützte Protokoll für den Client für Sichern/Archivieren an:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTCPip
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDie Übertragungsmethode Transmission Control Protocol/Internet Protocol (TCP/IP).

Verwenden Sie die Option lanfreetcpport, um die Nummer des TCP/IP-Anschlusses anzugeben, an dem der Speicheragent empfangsbereit ist. Die Übertragungsmethode TCP/IP ist die Standardeinstellung für Benutzer ohne Rootberechtigung auf allen unterstützten Plattformen.

Windows-BetriebssystemeTCPip
Windows-BetriebssystemeDie Übertragungsmethode Transmission Control Protocol/Internet Protocol (TCP/IP).

Verwenden Sie die Option lanfreetcpport, um die Nummer des TCP/IP-Anschlusses anzugeben, an dem der Speicheragent empfangsbereit ist.

V6Tcpip
Gibt an, dass abhängig von der Systemkonfiguration und den Ergebnissen einer DNS-Suche (Domain Name Service - Domänennamensservice) entweder TCP/IP v4 oder v6 verwendet werden soll. Das einzige Mal, wenn dies nicht zutrifft, ist bei Verwendung von dsmc schedule und schedmode=prompt. Es muss eine gültige DNS-Umgebung verfügbar sein.

Windows-BetriebssystemeNAMedpipes
Windows-BetriebssystemeDie Interprozesskommunikationsmethode, bei der Nachrichtendatenströme zwischen einem Client und einem Server fließen können. Dies ist der Standardwert. Geben Sie die Option lanfreetcpport nicht an, wenn Sie die Übertragungsmethode NAMedpipes für LAN-unabhängige Übertragung verwenden wollen.

Windows-BetriebssystemeSHAREdmem
Windows-BetriebssystemeVerwenden Sie die Shared-Memory-Übertragungsmethode, wenn der Client und der Speicheragent auf demselben System ausgeführt werden. Shared Memory ermöglicht eine bessere Leistung als das TCP/IP-Protokoll. Der Client für Sichern/Archivieren muss über lokale Administratorberechtigungen verfügen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSHAREdmem
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeVerwenden Sie die Shared-Memory-Übertragungsmethode, wenn der Client und der Speicheragent auf demselben System ausgeführt werden. Shared Memory ermöglicht eine bessere Leistung als das TCP/IP-Protokoll. Dies ist die Standardübertragungsmethode für AIX-, Linux- und Solaris-Rootbenutzer.Wenn Sie diese Übertragungsmethode unter `AIX` angeben, kann der Benutzer des Clients für Sichern/Archivieren als Root oder Nicht-Root angemeldet sein, solange der Speicheragent als Root ausgeführt wird. Wird der Speicheragent nicht als Root ausgeführt, muss die Benutzer-ID, die den Client für Sichern/Archivieren ausführt, mit der Benutzer-ID, die den Speicheragenten ausführt, übereinstimmen.

Beispiele

Optionsdatei:

lanfreecommmethod tcp

Nur TCP/IP v4 verwenden

lanfreecommmethod V6Tcpip

Sowohl TCP/IP v4 als auch v6 verwenden, abhängig von der Systemkonfiguration und den Ergebnissen einer DNS-Suche.

Befehlszeile:

```
-lanfreec=tcp
```

```
-lanfreec=V6Tcpip
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Lanfreeshmport

Verwenden Sie die Option lanfreeshmport, wenn `lanfreecommmethod=SHAREdmem` für die Übertragung zwischen dem Client für Sichern/Archivieren und dem Speicheragenten angegeben wird. Dadurch wird die Verarbeitung zwischen dem Client und der an SAN angeschlossenen Speichereinheit aktiviert.

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

 Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-LANFREEShmport-- --Anschlussadresse------------------------><
```

Parameter

Anschlussadresse
: Gibt die Nummer an, mit der die Verbindung zum Speicheragenten hergestellt wird. Der Wertebereich ist 1 bis 32767.

  Für Windows-Clients lautet der Standardwert 1.

  Mit Ausnahme von Windows-Clients lautet der Standardwert für alle Clients 1510.

Beispiele

Optionsdatei:
```
lanfrees 1520
```
Befehlszeile:
```
-lanfrees=1520
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Lanfreetcpport

Die Option lanfreetcpport gibt die Nummer des TCP/IP-Anschlusses an, an dem der IBM Spectrum Protect-Speicheragent empfangsbereit ist.

Verwenden Sie diese Option, wenn Sie lanfreecommmethod=TCPip für die Übertragung zwischen dem Client für Sichern/Archivieren und dem Speicheragenten angeben. Geben Sie die Option lanfreetcpport nicht an, wenn Sie die Übertragungsmethode NAMedpipes für LAN-unabhängige Übertragung verwenden wollen.

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist nur für AIX-, Linux x86_64-, Linux on POWER- und Oracle Solaris-Clients gültig.

 Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-LANFREETCPPort-- --Anschlussadresse------------------------><
```

Parameter

Anschlussadresse
: Gibt die Nummer des TCP/IP-Anschlusses an, an dem der Speicheragent empfangsbereit ist. Der Wertebereich ist 1 bis 32767; der Standardwert ist 1500.

  Anmerkung: Für die Kommunikation mit dem Speicheragenten (virtuellen Server) muss der lanfreetcpport-Wert des Clients mit dem tcpport-Wert des Speicheragenten übereinstimmen. Für die Kommunikation mit dem tatsächlichen Server muss der tcpport-Wert des Clients dem tcpport-Wert des Servers entsprechen.

Beispiele

Optionsdatei:
```
lanfreetcpp 1520
```
Befehlszeile:
```
-lanfreetcpp=1520
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Lanfreessl

Verwenden Sie die Option lanfreessl, um Secure Sockets Layer (SSL) für eine sichere Client- und Speicheragentenkommunikation zu aktivieren. Diese Option wird nicht mehr unterstützt, wenn Sie die Verbindung zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen.

Unterstützte Clients

Mit Ausnahme von Mac OS X-Clients wird diese Option auf allen Clients unterstützt.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei ein. Sie können diese Option nicht in der grafischen Benutzerschnittstelle oder in der Befehlszeile definieren.

Syntax

```
              .-No--.
>>-LANFREESSL-+-----+-----------------------------------------><
              '-Yes-'
```

Parameter

No
: Gibt an, dass der Client für Sichern/Archivieren bei der Kommunikation mit dem Speicheragenten nicht SSL verwendet. No ist der Standardwert.

Yes
: Gibt an, dass der Client für Sichern/Archivieren bei der Kommunikation mit dem Speicheragenten SSL aktiviert. Zum Aktiveren von SSL geben Sie lanfreessl=yes an und ändern Sie den Wert der Option lanfreetcpport. Die Änderung des Werts der Option lanfreetcpport ist erforderlich, da der IBM Spectrum Protect-Speicheragent in der Regel so konfiguriert ist, dass er an einem anderen Anschluss für SSL-Verbindungen empfangsbereit ist.

Beispiele

Optionsdatei:

```
lanfreessl yes
lanfreessl no
```

Befehlszeile:
: Nicht gültig. Sie können diese Option nicht in der Befehlszeile definieren.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Lanfreetcpserveraddress

Die Option lanfreetcpserveraddress gibt die TCP/IP-Adresse für den IBM Spectrum Protect-Speicheragenten an.

Verwenden Sie diese Option, wenn Sie lanfreecommmethod=TCPip oder V6Tcpip für die Übertragung zwischen dem Client für Sichern/Archivieren und dem Speicheragenten angeben.

Das Überschreiben des Standardwerts für diese Option ist nützlich, wenn Sie LAN-unabhängig in einer Umgebung konfigurieren, in der der Client und der Speicheragent auf unterschiedlichen Systemen ausgeführt werden. Sie können diese Speicheragentenadresse von Ihrem Administrator erfahren.

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist nur für AIX-, Linux x86_64-, Linux on POWER- und Oracle Solaris-Clients gültig.

Windows-BetriebssystemeDiese Option ist für alle unterstützten Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei ein.

Syntax

```
>>-LANFREETCPServeraddress-- --Speicheragentenadresse---------><
```

Parameter

Speicheragentenadresse
: Gibt eine 1- bis 64-stellige TCP/IP-Adresse für einen Server an. Geben Sie einen TCP/IP-Domänennamen oder eine numerische IP-Adresse an. Die numerische IP-Adresse kann entweder eine TCP/IP-V4- oder eine TCP/IP-V6-Adresse sein. Der Standardwert ist 127.0.0.1 (localhost).

Beispiele

Optionsdatei:

```
LANFREETCPServeraddress stagent.example.com

LANFREETCPServeraddress 192.0.2.1
```

Befehlszeile:
: Nicht zutreffend.

Windows-Betriebssysteme

Language

Mit der Option language wird die Landessprache für die angezeigten Clientnachrichten angegeben.

Amerikanisches Englisch (ENU) kann für alle Clients verwendet werden.

Die Sprache, die von der Java™-GUI des Clients für Sichern/Archivieren angezeigt wird, wird über die Windows-Anzeigeländereinstellung und nicht über die Windows-Systemländereinstellung definiert. Wenn beispielsweise für die System- und Eingabeländereinstellung unter Windows Französisch festgelegt ist, für die Anzeigeländereinstellung jedoch Russisch definiert ist, wird von der Java-GUI als Sprache standardmäßig Russisch angezeigt, sofern die Option language nicht verwendet wird. Wenn die Java-GUI in amerikanischem Englisch oder einer anderen Sprache angezeigt werden soll, können Sie die Standardanzeigesprache überschreiben, indem Sie die Option language angeben.

Tipp: Die Option language wirkt sich nicht auf den Web-Client aus. Der Web-Client wird in der Sprache angezeigt, die der Ländereinstellung des Browsers zugeordnet ist. Ist im Browser eine Ländereinstellung aktiv, die der Client nicht unterstützt, wird der Web-Client in amerikanischem Englisch angezeigt.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Regionale Einstellungen in der Dropdown-Liste Sprache im Profileditor definieren.

Syntax

```
>>-LANGuage-- --Sprache----------------------------------------><
```

Parameter

Sprache
: Gibt die Sprache an, die verwendet werden soll. Folgende Sprachen sind verfügbar:

  - ENU (Englisch, Vereinigte Staaten)
  - PTB (Brasilianisches Portugiesisch)
  - CHS (Vereinfachtes Chinesisch)
  - CHT (Traditionelles Chinesisch)
  - FRA (Standardfranzösisch)
  - DEU (Standarddeutsch)
  - ITA (Standarditalienisch)
  - JPN (Japanisch)
  - KOR (Koreanisch)
  - ESP (Standardspanisch)
  - CSY (Tschechisch)
  - HUN (Ungarisch)
  - PLK (Polnisch)
  - RUS (Russisch)

Beispiele

Optionsdatei:
```
language deu
```
Befehlszeile:
: Nicht zutreffend.

Latest

Verwenden Sie die Option latest, um die neueste Sicherungsversion einer Datei zurückzuschreiben, auch wenn die Sicherung inaktiv ist.

Die Option latest können Sie in folgenden Befehlen verwenden:

- restore
- restore group

Wenn Sie eine zeitpunktgesteuerte Zurückschreibung (mit der Option pitdate) ausführen, ist es nicht notwendig, latest anzugeben, da diese Option bei Verwendung von pitdate implizit verwendet wird.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-LATest----------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

 Mac OS X-BetriebssystemeBefehlszeile:
:  Mac OS X-Betriebssystemedsmc restore "/Users/devel/projecta/*" -latest

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeBefehlszeile:
:  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssystemedsmc restore "/home/devel/projecta/*" -latest

 Windows-BetriebssystemeBefehlszeile:
:  Windows-Betriebssystemedsmc restore c:\devel\projecta\ -latest

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Localbackupset

Die Option localbackupset gibt an, ob die GUI des Clients für Sichern/Archivieren die anfängliche Anmeldung beim IBM Spectrum Protect-Server umgeht, um einen lokalen Sicherungssatz auf einer eigenständigen Workstation zurückzuschreiben.

Wenn Sie die Option localbackupset auf yes setzen, versucht die GUI keine anfängliche Anmeldung beim Server. In diesem Fall aktiviert die GUI nur die Funktionalität für Zurückschreiben.

Wenn Sie die Option localbackupset auf no (Standardwert) setzen, versucht die GUI die anfängliche Anmeldung beim Server und aktiviert alle GUI-Funktionen.

Anmerkung: Der Befehl restore backupset unterstützt die Zurückschreibung lokaler Sicherungssätze auf einer eigenständigen Workstation ohne Verwendung der Option localbackupset.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Windows-BetriebssystemeFügen Sie diese Option in die Datei dsm.opt ein.

Syntax

```
                    .-No--.
>>-LOCALbackupset--+-----+-------------------------------------><
                    '-Yes-'
```

Parameter

No
: Gibt an, dass die GUI eine anfängliche Anmeldung am Server versucht, und aktiviert alle Funktionen. Dies ist der Standardwert.

Yes
: Gibt an, dass die GUI keine anfängliche Anmeldung am Server versucht, und aktiviert nur die Funktionalität für Zurückschreiben.

Beispiele

Optionsdatei:

```
localbackupset yes
```

Diese Option ist mit dem Befehlszeilenclient dsmc nicht gültig.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Makesparsefile

Verwenden Sie die Option makesparsefile im Befehl restore oder retrieve, um anzugeben, wie Dateien mit freien Bereichen erneut erstellt werden.

Dateien mit freien Bereichen haben keinen Plattenspeicherplatz für jeden Block im gesamten Adressraum zugeordnet, was zu freien Datenbereichen innerhalb der Datei führt. Der Client für Sichern/Archivieren erkennt Dateien mit freien Bereichen während einer Sicherungsoperation und markiert sie als solche auf dem IBM Spectrum Protect-Server. Freie Datenbereiche werden durch ihren Inhalt erkannt, der immer null ist.

Wenn Sie die Option makesparsefile auf yes (Standardwert) setzen, werden die freien Datenbereiche innerhalb der Datei nicht auf Platte geschrieben, sodass während einer Zurückschreibung kein zusätzlicher Plattenspeicherplatz zugeordnet wird.

Wenn Sie die Option makesparsefile auf no setzen, werden die freien Datenbereiche nicht erneut erstellt, was dazu führt, dass für den gesamten Adressraum Plattenblöcke zugeordnet werden. Dies kann unter Umständen einen größeren belegten Plattenspeicherplatz zum Ergebnis haben. Stellen Sie sicher, dass Sie über ausreichend Plattenspeicherplatz verfügen, um alle Daten zurückzuschreiben.

Auf einigen UNIX- und Linux-Systemen ist es möglicherweise erforderlich, systemspezifische Dateien nicht als Dateien mit freien Bereichen zu sichern. Verwenden Sie die Option makesparsefile für Dateien, bei denen die Existenz physischer Plattenblöcke erforderlich ist, wie z. B. bei der

Datei ufsboot in Solaris, die beim Booten ausgeführt wird. Das Bootdateiladeprogramm des Betriebssystems greift direkt auf die physischen Plattenblöcke zu und unterstützt keine Dateien mit freien Bereichen.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients außer Mac OS X gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

```
                    .-Yes-.
>>-MAKESParsefile--+-----+-------------------------------------><
                    '-No--'
```

Parameter

Yes
: Gibt an, dass freie Datenbereiche innerhalb der Datei nicht geschrieben werden, sodass während einer Zurückschreibung kein zusätzlicher Plattenspeicherplatz zugeordnet wird. Dies ist der Standardwert.

No
: Gibt an, dass freie Datenbereiche nicht erneut erstellt werden, was dazu führt, dass für den gesamten Adressraum Plattenblöcke zugeordnet werden.

Beispiele

Optionsdatei:
```
makesparsefile no
```
Befehlszeile:
```
-makesparsefile=no
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Managedservices

Die Option managedservices gibt an, ob der IBM Spectrum Protect-Clientakzeptorservice den Scheduler und/oder den Web-Client verwaltet.

Einschränkung: Sie können den dsmcad nicht für die Planung verwenden, wenn Sie die Option sessioninitiation auf serveronly setzen.
Der Clientakzeptordämon dient als externer Zeitgeber für den Scheduler. Wenn der Scheduler gestartet wird, fragt er den Server nach dem nächsten geplanten Ereignis. Das Ereignis wird entweder sofort ausgeführt oder der Scheduler wird beendet. Der Clientakzeptordämon startet den Scheduler erneut, wenn der Zeitpunkt für die Ausführung des geplanten Ereignisses gekommen ist.
Anmerkung:

1. Wenn Sie die Option schedmode auf prompt setzen, fordert der Server über Systemanfrage den Clientakzeptordämon zur Aktion auf, wenn es Zeit ist, den Zeitplan auszuführen. Der Scheduler stellt die Verbindung zum Server her und unterbricht diese, wenn der Clientakzeptordämon zum ersten Mal gestartet wird.

   Der Befehl 'dsmc schedule' kann nicht verwendet werden, wenn sowohl schedmode prompt als auch commmethod V6Tcpip angegeben werden.

2. Mac OS X-BetriebssystemeWenn Sie unter Mac OS X die Option managedservices nicht angeben, verwaltet der Clientakzeptordämon standardmäßig sowohl das Schedulerprogramm als auch den Web-Client.
3. Windows-BetriebssystemeSetzen Sie die Option passwordaccess in Ihrer Clientoptionsdatei (dsm.opt) auf generate und generieren Sie ein Kennwort, damit IBM Spectrum Protect Ihr Kennwort automatisch verwalten kann.
4. AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeSetzen Sie die Option passwordaccess in Ihrer Datei dsm.sys auf generate und generieren Sie ein Kennwort, damit IBM Spectrum Protect Ihr Kennwort automatisch verwalten kann.

Die Verwendung des Clientakzeptordämons zum Verwalten des Scheduler-Service kann folgende Vorteile bieten:

- Probleme mit der Speicheraufbewahrungsdauer, die bei den traditionellen Ausführungsmethoden des Schedulers auftreten können, werden beseitigt. Die Verwendung des Clientakzeptordämons zum Verwalten des Schedulers erfordert zwischen den geplanten Operationen sehr wenig Speicher.
- Der Clientakzeptordämon kann sowohl das Schedulerprogramm als auch den Web-Client verwalten, wodurch die Anzahl der Hintergrundprozesse auf Ihrer Workstation reduziert wird.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDamit der Web-Client verwendet werden kann, müssen Sie diese Option in der Clientsystemoptionsdatei angeben.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Web-Client im Profileditor definieren.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Web-Client im Profileditor definieren.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Syntax

```
>>-MANAGEDServices--Modus--------------------------------------><
```

Parameter

Modus
Gibt an, ob der Clientakzeptordämon den Scheduler und/oder den Web-Client verwaltet.

Windows-Betriebssystemewebclient
Windows-BetriebssystemeGibt an, dass der Clientakzeptordämon den Web-Client verwaltet.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemewebclient
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt an, dass der Clientakzeptordämon den Web-Client verwaltet. Dies ist der Standardwert für UNIX und Linux. Beide Werte, webclient und schedule, sind der Standardwert für Mac OS X.

Mac OS X-BetriebssystemeWindows-Betriebssystemeschedule
Mac OS X-BetriebssystemeWindows-BetriebssystemeGibt an, dass der Clientakzeptordämon den Scheduler verwaltet. Beide Werte, webclient und schedule, sind der Standardwert für Mac OS X.

Mac OS X-Betriebssystemenone
Mac OS X-BetriebssystemeFür Mac OS X: Gibt an, dass der Clientakzeptordämon weder den Web-Client noch Zeitpläne verwaltet. Setzen Sie managedservices auf none, um den Befehl dsmc schedule zu aktivieren.

Beispiele

Windows-BetriebssystemeOptionsdatei:
Windows-BetriebssystemeEs folgen Beispiele für die Angabe der Option managedservices in Ihrer Clientoptionsdatei (dsm.opt).

Task
Angeben, dass der Clientakzeptordämon nur den Web-Client verwaltet.

```
managedservices webclient
```

Task
Angeben, dass der Clientakzeptordämon nur den Scheduler verwaltet.

```
managedservices schedule
```

Task
Angeben, dass der Clientakzeptordämon sowohl den Web-Client als auch den Scheduler verwaltet.

```
managedservices schedule webclient
```

Anmerkung: Die Reihenfolge, in der diese Werte angegeben werden, ist unwichtig.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Optionsdatei:
Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme
Mac OS X-BetriebssystemeEs folgen Beispiele für die Angabe der Option managedservices in Ihrer Clientsystemoptionsdatei (dsm.sys).

Task
Angeben, dass der Clientakzeptordämon nur den Web-Client verwaltet.

```
managedservices webclient
```

Task
: Angeben, dass der Clientakzeptordämon nur den Scheduler verwaltet.

```
managedservices schedule
```

Task
: Angeben, dass der Clientakzeptordämon sowohl den Web-Client als auch den Scheduler verwaltet.

```
managedservices schedule webclient
```

Anmerkung: Die Reihenfolge, in der diese Werte angegeben werden, ist unwichtig.


Task
: Zur Verwendung des Befehls dsmc schedule unter Mac OS X Folgendes angeben:

```
managedservices none
```

Befehlszeile:
: Nicht zutreffend.

Maxcmdretries

Mit der Option maxcmdretries kann angegeben werden, wie oft der Client-Scheduler auf Ihrer Workstation einen geplanten Befehl, der bei der Ausführung fehlgeschlagen ist, maximal wiederholt.

Die Befehlswiederholung startet nur, wenn der Client-Scheduler noch keine Datei gesichert hat, noch nie eine Verbindung zum Server hergestellt hat oder vor dem Sichern einer Datei fehlgeschlagen ist. Diese Option wird nur verwendet, wenn der Scheduler aktiv ist.

Diese Option kann auch der IBM Spectrum Protect-Administrator definieren. Gibt Ihr Administrator einen Wert für diese Option an, überschreibt dieser Ihre Angabe in der Clientoptionsdatei, nachdem Ihr Clientknoten erfolgreich den Kontakt zum Server hergestellt hat.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei




 Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Scheduler im Feld Max. Anz. Befehlswiederholungen im Profileditor definieren.

 Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Scheduler im Feld Max. Anz. Befehlswiederholungen im Profileditor definieren.

Syntax

```
>>-MAXCMDRetries-- --Maximale Anzahl Befehlswiederholungen-----><
```

Parameter

Maximale Anzahl Befehlswiederholungen
: Gibt an, wie oft der Client-Scheduler einen geplanten Befehl, der bei der Ausführung fehlgeschlagen ist, maximal wiederholen kann. Der Wertebereich ist Null bis 9999; Standardwert ist 2.

Beispiele

Optionsdatei:
: `maxcmdr 4`

Befehlszeile:
: `-maxcmdretries=4`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.


Mbobjrefreshthresh

Die Option mbobjrefreshthresh (Aktualisierungsschwellenwert für Megablockobjekte) gibt eine Zahl an, die einen Schwellenwert definiert. Wenn die Anzahl der IBM Spectrum Protect-Objekte, die zum Beschreiben eines 128-MB-Megablocks benötigt werden, diesen Wert überschreitet, wird der gesamte Megablock aktualisiert und die Objekte, mit denen dieser Bereich in vorherigen Sicherungen dargestellt wurde, verfallen.

Beim Sichern einer virtuellen Maschine werden die Daten in 128-MB-Einheiten, den sogenannten *Megablöcken*, auf dem IBM Spectrum Protect-Server gespeichert. Wenn sich ein Bereich auf der Produktionsplatte ändert und eine neue Teilsicherung ausgeführt wird, wird ein neuer Megablock erstellt, um die Änderungen an den zuvor gesicherten Daten darzustellen. Da bei jeder Teilsicherung ein neuer Megablock erstellt werden kann, können die Megablöcke schließlich die Leistung der IBM Spectrum Protect-Datenbank und folglich die Leistung der meisten IBM Spectrum Protect-Operationen beeinträchtigen.

Verwenden Sie diese Option bei der Schätzung von IBM Spectrum Protect-Objekten, die Produktionsdaten darstellen, für jede Sicherung virtueller Maschinen. Wenn beispielsweise die Anzahl der IBM Spectrum Protect-Objekte diesen Wert überschreitet, wird der Megablock aktualisiert. Bei dieser Aktion wird der gesamte 128-MB-Block auf den Server kopiert und als ein einziges IBM Spectrum Protect-Objekt dargestellt. Der Mindestwert ist 2 und der Maximalwert 8192. Der Standardwert ist 50.

Unterstützte Clients

Linux-BetriebssysteWindows-BetriebssystemeDiese Option ist für Einheiten zum Versetzen von Daten gültig, die virtuelle VMware-Maschinen schützen. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Windows-BetriebssystemeDiese Option ist für Einheiten zum Versetzen von Daten gültig, die virtuelle Microsoft Hyper-V-Maschinen schützen. Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware oder IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie ist nicht in der Befehlszeile gültig.

Syntax

```
                      .-50---------.
>>-MBOBJREFRESHTHRESH -+------------+--------------------------><
                      '-ganze_Zahl-'
```

Parameter

Der zulässige Mindestwert ist 2 Megablöcke, der größte Wert ist 8192 Megablöcke. Der Standardwert ist 50 Megablöcke.

Beispiele

Definieren Sie die folgende Option, um eine Megablockaktualisierung auszulösen, wenn die Anzahl der Objekte, die zur Darstellung eines aktualisierten Megablocks benötigt werden, 20 Objekte überschreitet:

```
MBOBJREFRESHTHRESH 20
```

Linux-BetriebssysteWindows-Betriebssysteme

Mbpctrefreshthresh

Die Option mbpctrefreshthresh (Aktualisierungsschwellenwert für Megablockprozentsatz) gibt eine Zahl an, die einen Schwellenwert definiert. Wenn der Prozentsatz der IBM Spectrum Protect-Objekte, die zum Beschreiben eines 128-MB-Megablocks benötigt werden, diesen Wert überschreitet, wird der gesamte Megablock aktualisiert und die Objekte, mit denen dieser Bereich in vorherigen Sicherungen dargestellt wurde, verfallen.

Beim Sichern einer virtuellen Maschine werden die Daten in 128-MB-Einheiten, den sogenannten *Megablöcken*, auf dem IBM Spectrum Protect-Server gespeichert. Wenn sich ein Bereich auf der Produktionsplatte ändert und eine neue Teilsicherung ausgeführt wird, wird ein neuer Megablock erstellt, um die Änderungen an den zuvor gesicherten Daten darzustellen. Da bei jeder Teilsicherung ein neuer Megablock erstellt werden kann, können die Megablöcke schließlich die Leistung der IBM Spectrum Protect-Datenbank und folglich die Leistung der meisten IBM Spectrum Protect-Operationen beeinträchtigen.

Verwenden Sie diese Option für die Schätzung des zusätzlichen Datenvolumens, das für jede virtuelle Maschine gesichert wird. Wenn sich beispielsweise ein 128-MB-Block einer Produktionsplatte um mehr als den angegebenen Prozentsatz ändert, wird der gesamte 128-MB-Block auf den Server kopiert. Der Block wird als ein einziges IBM Spectrum Protect-Objekt dargestellt.

Unterstützte Clients

Linux-BetriebssystemeWindows-BetriebssystemeDiese Option ist für Clients gültig, die als Knoten der Einheit zum Versetzen von Daten agieren und virtuelle VMware-Maschinen schützen. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Windows-BetriebssystemeDiese Option ist für Clients gültig, die als Knoten der Einheit zum Versetzen von Daten agieren und virtuelle Microsoft Hyper-V-Maschinen schützen. Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware oder IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie ist nicht in der Befehlszeile gültig.

Syntax

```
                      .-50---------.
>>-MBPCTREFRESHTHRESH -+------------+-------------------------><
                      '-ganze_Zahl-'
```

Parameter

Der zulässige Mindestwert ist 1 Prozent, der größte Wert ist 99 Prozent. Der Standardwert ist 50 Prozent.

Beispiele

Definieren Sie die folgende Option, um eine Megablockaktualisierung auszulösen, wenn sich mindestens 50 Prozent der Objekte in einem Megablock auf einer Produktionsplatte geändert haben:

```
MBPCTREFRESHTHRESHOLD 50
```

Memoryefficientbackup

Mit der Option memoryefficientbackup wird der Speichersparalgorithmus für die Verwendung bei der Verarbeitung von Gesamtsicherungen für Dateibereiche angegeben.

Eine Methode sichert jeweils nur ein einziges Verzeichnis, wodurch weniger Speicher benötigt wird. Die andere Methode verwendet viel weniger Speicher, erfordert aber mehr Plattenspeicherplatz.

Verwenden Sie die Option memoryefficientbackup im Befehl incremental, wenn Ihre Workstation über wenig Speicher verfügt. Sie können diese Option auch als Parameter für die Option include.fs verwenden, um den vom Client für Sichern/Archivieren verwendeten Algorithmus auf Dateibereichsbasis auszuwählen.

Windows-BetriebssystemeVerwenden Sie memoryefficientbackup=diskcachemethod für Dateibereiche, die so viele Dateien enthalten, dass der Client die Teilsicherung weder mit der Standardeinstellung, memoryefficientbackup=no, noch mit der Einstellung memoryefficientbackup=yes ausführen kann. Die Plattencachedatei, die bei der ersten Teilsicherung des Plattencaches erstellt wird, kann bis zu 5 GB Plattenspeicherplatz pro Million Dateien oder Verzeichnisse erfordern, die gesichert wird.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeVerwenden Sie memoryefficientbackup=diskcachemethod für Dateibereiche, die so viele Dateien enthalten, dass der Client die Teilsicherung weder mit der Standardeinstellung, memoryefficientbackup=no, noch mit der Einstellung memoryefficientbackup=yes ausführen kann.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Der tatsächlich erforderliche Plattenspeicherplatz für die Plattencachedatei, die bei Teilsicherungen des Plattencaches erstellt wird, ist von der Anzahl der Dateien und Verzeichnisse abhängig, die in die Sicherung eingeschlossen werden, sowie von der durchschnittlichen Pfadlänge der zu sichernden Dateien und Verzeichnisse. Für UNIX und Linux beträgt der Schätzwert 1 Byte pro Zeichen im Pfadnamen. Für Mac OS X beträgt der Schätzwert 4 Byte pro Zeichen im Pfadnamen. Beispiel: Es müssen 1 000 000 Dateien und Verzeichnisse gesichert werden und die durchschnittliche Pfadlänge beträgt 200 Zeichen. In diesem Fall belegt die Datenbank etwa 200 MB für UNIX- und Linux-Clients und 800 MB für Mac OS X-Clients. Ein anderes Schätzverfahren für Planungszwecke besteht darin, die Anzahl der Dateien und Verzeichnisse mit der Länge des längsten Pfads zu multiplizieren, um eine maximale Datenbankgröße zu ermitteln.

Windows-BetriebssystemeDer tatsächlich erforderliche Plattenspeicherplatz für die Plattencachedatei, die bei Teilsicherungen des Plattencaches erstellt wird, ist von der Anzahl der Dateien und Verzeichnisse abhängig, die in die Sicherung eingeschlossen werden, sowie von der durchschnittlichen Pfadlänge der zu sichernden Dateien und Verzeichnisse. Der Schätzwert beträgt 2 Byte pro Zeichen im Pfadnamen. Beispiel: Es müssen 1 000 000 Dateien und Verzeichnisse gesichert werden und die durchschnittliche Pfadlänge beträgt 200 Zeichen. In diesem Fall belegt die Datenbank etwa 400 MB. Ein anderes Schätzverfahren für Planungszwecke besteht darin, die Anzahl der Dateien und Verzeichnisse mit der Länge des längsten Pfads zu multiplizieren, um eine maximale Datenbankgröße zu ermitteln.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBeim Sichern eines über HSM verwalteten Dateisystems wird eine zweite Plattencachedatei für die Liste der umgelagerten Dateien erstellt. Für beide Plattencachedateien

zusammen - die bei Teilsicherungen des Plattencaches erstellte Plattencachedatei und die bei Sicherungen von über HSM verwalteten Dateisystemen erstellte Plattencachedatei - können mehr als 400 MB Plattenspeicherplatz pro Million zu sichernder Dateien erforderlich sein. Die Plattencachedatei kann sehr groß werden. Auf dem Dateisystem, das für die Plattencachedatei verwendet wird, muss Unterstützung für große Dateien aktiviert sein.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDiese Option ist sowohl in dsm.opt als auch innerhalb einer Serverzeilengruppe in dsm.sys zulässig; der Wert in dsm.opt wird jedoch ignoriert, wenn die Option auch in dsm.sys vorhanden ist. Sie können diese Option auch in die Anfangsbefehlszeile einfügen. Im interaktiven Modus kann diese Option mit dem Befehl incremental verwendet werden. Sie können diese Option auch auf der Registerkarte Leistungsoptimierung im Profileditor und durch Auswahl des Kontrollkästchens Speichersparalgorithmus verwenden definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) oder in die Anfangsbefehlszeile ein. Sie können diese Option auch auf der Registerkarte Leistungsoptimierung im Profileditor und durch Auswahl des Kontrollkästchens Speichersparalgorithmus verwenden definieren.

Syntax

```
                          .-No--------------.
>>-MEMORYEFficientbackup--+-----------------+------------------><
                          +-Yes-------------+
                          '-DISKCACHEMethod-'
```

Parameter

No
: Der Clientknoten verwendet die schnellere, speicherintensivere Methode für die Verarbeitung von Teilsicherungen. Dies ist der Standardwert.

Yes
: Der Clientknoten verwendet die Methode, bei der weniger Speicher für die Verarbeitung von Teilsicherungen benötigt wird.

Diskcachemethod
: Der Clientknoten verwendet die Methode, bei der viel weniger Speicher, aber mehr Plattenspeicherplatz für die Verarbeitung von Teilsicherungen für komplette Dateisysteme benötigt wird.

Beispiele

Optionsdatei:

```
memoryefficientbackup yes
memoryefficientbackup diskcachem
```

Befehlszeile:

```
-memoryef=no
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Mode

Mit der Option 'mode' können Sie den Sicherungsmodus angeben, der bei bestimmten Sicherungsoperationen verwendet werden soll.

Die Option mode bleibt bei Sicherungen unformatierter logischer Einheiten ohne Wirkung.

Die Option mode können Sie in folgenden Sicherungsbefehlen verwenden:

backup image
: Angeben, ob eine selektive Imagesicherung oder eine Imageteilsicherung von Clientdateisystemen ausgeführt werden soll.

AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemebackup nas
: Angeben, ob eine vollständige oder eine differenzielle Imagesicherung von NAS-Dateisystemen ausgeführt werden soll.

backup group
: Angeben, ob eine vollständige oder differenzielle Gruppensicherung einer Liste von Dateien ausgeführt werden soll, die sich in einem oder mehreren Dateibereichen befinden.

backup vm

Linux-BetriebssystemeWindows-BetriebssystemeFür virtuelle VMware-Maschinen gibt dieser Parameter an, ob eine immer inkrementelle Gesamtsicherung oder eine immer inkrementelle Teilsicherung virtueller VMware-Maschinen ausgeführt werden soll.
Windows-BetriebssystemeFür virtuelle Microsoft Hyper-V-Maschinen gibt dieser Parameter an, ob eine immer inkrementelle Gesamtsicherung oder eine immer inkrementelle Teilsicherung virtueller Hyper-V-Maschinen ausgeführt werden soll.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Unterstützte Clients

Mit Ausnahme von Mac OS ist diese Option auf allen unterstützten Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Linux-BetriebssystemeWindows-BetriebssystemeDiese Option ist für Einheiten zum Versetzen von Daten gültig, die virtuelle VMware-Maschinen schützen. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Windows-BetriebssystemeDiese Option ist für Einheiten zum Versetzen von Daten gültig, die virtuelle Microsoft Hyper-V-Maschinen schützen. Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware oder IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Syntax

Für Imagesicherungen von Clientdateisystemen

```
              .-Selective---.
>>-MODE = -+-------------+-------------------------------------><
           '-Incremental-'
```

AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Für Imagesicherungen von NAS-Dateisystemen

```
              .-differential-.
>>-MODE = -+---------------+-------------------------------------><
           '-full----------'
```

Für Gruppensicherungen

```
              .-full----------.
>>-MODE = -+---------------+-------------------------------------><
           '-differential-'
```

Linux-BetriebssystemeWindows-Betriebssysteme

Für die Sicherung virtueller VMware-Maschinen

```
             .-IFIncremental-.
>>-MODE= -+----------------+-------------------------------------><
          '-IFFull---------'
```

Windows-Betriebssysteme

Für die Sicherung virtueller Microsoft Hyper-V-Maschinen

```
              .-IFIncremental-.
>>-MODE = -+----------------+-------------------------------------><
           '-IFFull---------'
```

Parameter

Imagesicherungsparameter

selective
: Gibt an, dass Sie eine vollständige (selektive) Imagesicherung ausführen wollen. Dies ist der Standardmodus für Imagesicherungen von Clientdateisystemen.

incremental

Gibt an, dass Sie nur die Daten sichern wollen, die sich seit der letzten Imagesicherung geändert haben. Wenn noch keine Imagesicherung erstellt wurde, ist die erste Sicherung eine vollständige Imagesicherung (mode=selective); die Angabe für die Option 'mode' hat dabei keinen Einfluss.

 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

NAS-Sicherungsparameter

differential
: Dies ist der Standardwert für NAS-Objekte. Gibt an, dass Sie eine NAS-Sicherung von Dateien ausführen wollen, die sich seit der letzten vollständigen Sicherung geändert haben. Ist keine Kopie eines Gesamtimage auf dem IBM Spectrum Protect-Server vorhanden, wird eine vollständige Sicherung ausgeführt. Ist ein Gesamtimage vorhanden, wird bei Angabe von MODE=differential eine differenzielle Imagesicherung gesendet, unabhängig davon, ob das Image zurückgeschrieben werden kann oder verfallen ist und nur wegen abhängiger differenzieller Images aufbewahrt wird. Wird ein Gesamtimage während einer differenziellen Sicherung gesendet, wird dieses bei Ausführung des Serverbefehls QUERY NASBACKUP als Gesamtimage angezeigt.

  Ein Gesamtimage kann auf Basis der Versionsverarbeitung oder der Aufbewahrung (verexists retextra) für den Verfall ausgewählt sein, aber dennoch weiter auf dem Server verwaltet werden, damit abhängige differenzielle Images zurückgeschrieben werden können. Ein Gesamtimage, das für den Verfall ausgewählt ist, kann nicht zum Zurückschreiben ausgewählt werden. Daher wird es nicht angezeigt, wenn der Serverbefehl QUERY NASBACKUP verwendet wird. Die differenziellen Imagesicherungen, die von einem "verfallenen" Gesamtimage abhängig sind, können zurückgeschrieben werden.

full
: Gibt an, dass Sie eine vollständige Sicherung von NAS-Dateisystemen ausführen wollen.

Gruppensicherungsparameter

full
: Gibt an, dass Sie eine vollständige Sicherung von Gruppenobjekten ausführen wollen. Dies ist der Standardwert für Gruppensicherungen.

differential
: Gibt an, dass Sie eine Gruppensicherung von Dateien ausführen wollen, die sich seit der letzten vollständigen Sicherung geändert haben. Ist keine Kopie eines Gesamtimage auf dem IBM Spectrum Protect-Server vorhanden, wird eine vollständige Sicherung ausgeführt. Ist ein Gesamtimage vorhanden, wird bei Angabe von MODE=differential eine differenzielle Imagesicherung gesendet, unabhängig davon, ob das Image zurückgeschrieben werden kann oder verfallen ist und nur wegen abhängiger differenzieller Images aufbewahrt wird. Wird ein Gesamtimage während einer differenziellen Sicherung gesendet, wird dieses bei Ausführung des Serverbefehls QUERY GROUP als Gesamtimage angezeigt.

  Ein Gesamtimage kann auf Basis der Versionsverarbeitung oder der Aufbewahrung (verexists retextra) für den Verfall ausgewählt sein, aber dennoch weiter auf dem Server verwaltet werden, damit abhängige differenzielle Images zurückgeschrieben werden können. Ein Gesamtimage, das für den Verfall ausgewählt ist, kann nicht zum Zurückschreiben ausgewählt werden. Daher wird es nicht angezeigt, wenn der Serverbefehl QUERY GROUP verwendet wird. Die differenziellen Imagesicherungen, die von einem "verfallenen" Gesamtimage abhängig sind, können zurückgeschrieben werden.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Parameter für virtuelle VMware-Maschinen

IFFull
: Gibt an, dass eine immer inkrementelle Gesamtsicherung einer virtuellen Maschine ausgeführt werden soll. Bei einer immer inkrementellen Gesamtsicherung werden alle verwendeten Blöcke auf den Platten einer virtuellen VMware-Maschine gesichert.

  Standardmäßig ist die erste Sicherung einer virtuellen VMware-Maschine selbst dann eine immer inkrementelle Gesamtsicherung (`mode=iffull`), wenn Sie `mode=ifincremental` angeben (oder den Standardwert der Option mode verwenden). Bei nachfolgenden Sicherungen wird standardmäßig `mode=ifincremental` verwendet.

  Diesen Sicherungsmodus können Sie nicht für die Sicherung einer virtuellen Maschine verwenden, wenn der Client für die Verschlüsselung der Sicherungsdaten konfiguriert ist.

  Eine Beschreibung der Sicherungsstrategie "Immer inkrementell" finden Sie in Sicherungs- und Wiederherstellungstypen.

IFIncremental
: Gibt an, dass Sie eine immer inkrementelle Teilsicherung einer virtuellen Maschine ausführen möchten. Bei einer immer inkrementellen Teilsicherung werden nur die Plattenblöcke gesichert, die sich seit der letzten Sicherung geändert haben.

  Dieser Modus ist der Standardsicherungsmodus für Sicherungen virtueller VMware-Maschinen.

  Diesen Sicherungsmodus können Sie nicht für die Sicherung einer virtuellen Maschine verwenden, wenn der Client für die Verschlüsselung der Sicherungsdaten konfiguriert ist.

Windows-Betriebssysteme

Parameter für virtuelle Microsoft Hyper-V-Maschinen

IFIncremental
: Gibt an, dass Sie eine immer inkrementelle Teilsicherung einer virtuellen Hyper-V-Maschine ausführen möchten. Bei einer immer inkrementellen Teilsicherung werden nur die Plattenblöcke gesichert, die sich seit der letzten Sicherung geändert haben.

  Dieser Modus ist der Standardsicherungsmodus für Hyper-V-Sicherungen.

  Diesen Sicherungsmodus können Sie nicht für die Sicherung einer virtuellen Maschine verwenden, wenn der Client für die Verschlüsselung der Sicherungsdaten konfiguriert ist.

  Eine Beschreibung der Sicherungsstrategie "Immer inkrementell" für virtuelle Hyper-V-Maschinen finden Sie in Sicherungsstrategie "Immer inkrementell".

IFFull
: Gibt an, dass eine immer inkrementelle Gesamtsicherung einer virtuellen Hyper-V-Maschine ausgeführt werden soll. Bei einer immer inkrementellen Gesamtsicherung werden alle verwendeten Blöcke auf den Platten einer virtuellen Maschine gesichert.

  Standardmäßig ist die erste Sicherung einer virtuellen Hyper-V-Maschine selbst dann eine immer inkrementelle Gesamtsicherung (`mode=iffull`), wenn Sie `mode=ifincremental` angeben (oder den Standardwert der Option mode verwenden). Bei nachfolgenden Sicherungen wird standardmäßig `mode=ifincremental` verwendet.

  Diesen Sicherungsmodus können Sie nicht für die Sicherung einer virtuellen Maschine verwenden, wenn der Client für die Verschlüsselung der Sicherungsdaten konfiguriert ist.

Beispiele

Task
: Linux-Betriebssysteme Windows-BetriebssystemeEine Sicherung der virtuellen VMware-Maschine vm1 mit dem Modus ifincremental (immer inkrementell, inkrementell) ausführen, damit nur die Daten gesichert werden, die sich seit der letzten Sicherung geändert haben.

```
dsmc backup vm vm1 -mode=ifincremental
 -vmbackuptype=full
```

Windows-BetriebssystemeTask
: Windows-BetriebssystemeEine immer inkrementelle VM-Gesamtsicherung der virtuellen Hyper-V-Maschine mit dem Namen msvm1 ausführen.

```
dsmc backup vm msvm1 -mode=iffull
```

Windows-BetriebssystemeTask
: Windows-BetriebssystemeEine immer inkrementelle Teilsicherung der virtuellen Hyper-V-Maschine mit dem Namen msvm1 ausführen.

```
dsmc backup vm msvm1 -mode=ifincremental
```

AIX-Betriebssysteme Oracle Solaris-BetriebssystemeTask
: AIX-Betriebssysteme Oracle Solaris-BetriebssystemeDie NAS-Imagesicherung des gesamten Dateisystems ausführen.

```
dsmc backup nas -mode=full -nasnodename=nas1
 /vol/vol0 /vol/vol1
```

Windows-BetriebssystemeTask
: Windows-BetriebssystemeDie NAS-Imagesicherung des gesamten Dateisystems ausführen.

```
dsmc backup nas -mode=differential -nasnodename=nas1
 {/vol/vol0} {/vol/vol1}
```

AIX-Betriebssysteme Linux-BetriebssystemeTask
: AIX-Betriebssysteme Linux-BetriebssystemeDen Dateibereich `/home/test` mithilfe einer Imageteilsicherung sichern, bei der nur Dateien gesichert werden, die seit der letzten vollständigen Imagesicherung neu sind oder sich geändert haben.

```
dsmc backup image /home/test -mode=incremental -snapshotproviderimage=none
```

Windows-BetriebssystemeTask
: Windows-BetriebssystemeDas Laufwerk `c:` mithilfe einer Imageteilsicherung sichern, bei der nur Dateien gesichert werden, die seit der letzten vollständigen Imagesicherung neu sind oder sich geändert haben.

```
dsmc backup image c: -mode=full
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeTask
: AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeEine vollständige Sicherung aller in der Dateiliste `/home/dir1/filelist1` angegebenen Dateien auf den virtuellen Dateibereich mit dem Namen `/virtfs` und mit der Hauptmemberdatei `/home/group1` ausführen.

```
dscm backup group -filelist=/home/dir1/filelist1
 -groupname=group1 -virtualfsname=/virtfs -mode=full
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine vollständige Sicherung aller in der Dateiliste `c:\dir1\filelist1` angegebenen Dateien auf den virtuellen Dateibereich mit dem Namen `\virtfs` und mit der Hauptmemberdatei `c:\group1` ausführen.

```
dsmc backup group -filelist=c:\dir1\filelist1 -groupname=group1
 -virtualfsname=\virtfs -mode=incremental -vmbackuptype=fullvm
```

Zugehörige Verweise:
Backup VM
Backup Group
Backup Image
Backup NAS
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Monitor

Die Option monitor gibt an, ob eine Imagesicherung oder -zurückschreibung von Dateisystemen, die zu einem NAS-Dateiserver gehören, überwacht werden soll.

Wenn Sie monitor=*yes* angeben, überwacht der Client für Sichern/Archivieren die aktuelle NAS-Imagesicherungs- oder -zurückschreibungsoperation und zeigt Verarbeitungsinformationen am Bildschirm an. Dies ist der Standardwert.

Wenn Sie monitor=*no* angeben, überwacht der Client die aktuelle NAS-Imagesicherungs- oder -zurückschreibungsoperation nicht und ist für die Verarbeitung des nächsten Befehls verfügbar.

Verwenden Sie diese Option im Befehl backup nas oder restore nas.

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist *nur* für AIX-, Linux- und Solaris-Clients gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Syntax

```
                .-Yes-.
>>-MONitor = -+-----+-------------------------------------------><
              '-No--'
```

Parameter

Yes
Gibt an, dass Sie die aktuelle NAS-Imagesicherungs- oder -zurückschreibungsoperation überwachen und Verarbeitungsinformationen am Bildschirm anzeigen wollen. Dies ist der Standardwert.

No
Gibt an, dass Sie die aktuelle NAS-Imagesicherungs- oder -zurückschreibungsoperation nicht überwachen wollen.

Beispiele

Befehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
backup nas -mode=full -nasnodename=nas1 -monitor=yes
/vol/vol0 /vol/vol1
```

Windows-Betriebssysteme

```
backup nas -mode=full -nasnodename=nas1 -monitor=yes
{/vol/vol0} {/vol/vol1}
```

Windows-Betriebssysteme

Myprimaryserver

Die Option myprimaryserver gibt den Namen des Primärservers an, mit dem sich der Client im Übernahmemodus beim Sekundärserver anmeldet.

Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option myprimaryserver an den Client gesendet und in der Datei dsm.opt gespeichert. Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Wichtig: Wenn Sie den Wert der Option myprimaryserver ändern, funktionieren Authentifizierungsdaten wie das IBM Spectrum Protect-Kennwort und der Verschlüsselungsschlüssel auf dem neuen Primärserver nicht mehr. Sie müssen das Kennwort und den Verschlüsselungsschlüssel für Operationen eingeben, die eine Authentifizierung erfordern. Ändern Sie diesen Wert daher nicht, auch wenn Sie die Verbindungsinformationen des Sekundärservers ändern.

Unterstützte Clients

Diese Option ist nur für Windows-Clients gültig.

Optionsdatei

Diese Option wird in die Clientoptionsdatei (dsm.opt) eingefügt.

Syntax

```
>>-MYPRIMARYServer----Name_des_primären_Servers----------------><
```

Parameter

Name_des_primären_Servers
: Gibt den Namen des Primärservers an, der im Fall einer Übernahme für die Authentifizierung verwendet werden soll. Der Primärserver ist der IBM Spectrum Protect-Server, den ein Client für die normale Produktion verwendet.

Beispiele

Optionsdatei:

```
*** Diese Optionen sollten nicht manuell geändert werden
REPLSERVERNAME          TARGET
   REPLTCPSERVERADDRESS 192.0.2.9
   REPLTCPPORT          1501
   REPLSERVERGUID       60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

MYREPLICATIONServer TARGET
MYPRIMARYSERVERNAME SERVER1
*** Ende der automatisch aktualisierten Optionen
```

Befehlszeile:
: Nicht zutreffend.

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Client für automatisierte Übernahme konfigurieren

Myreplicationserver

Die Option myreplicationserver gibt an, welche Zeilengruppe des Sekundärservers der Client im Fall einer Übernahme verwendet.

Die Zeilengruppe des Sekundärservers wird durch die Option replservername angegeben und enthält Verbindungsinformationen zum Sekundärserver.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDiese Option wird in eine Serverzeilengruppe in der Datei dsm.sys eingefügt.

Windows-BetriebssystemeDiese Option wird in die Clientoptionsdatei (dsm.opt) eingefügt.

Syntax

```
>>-MYREPLICATIONServer----Replikationsservername---------------><
```

Parameter

Replikationsservername
: Gibt den Namen der Zeilengruppe für den Sekundärserver an, die im Fall einer Übernahme verwendet werden soll. Dieser Wert ist in der Regel der Name des Sekundärservers, nicht der Hostname des Servers. Außerdem muss bei dem Wert des Parameters Replikationsservername nicht die Groß-/Kleinschreibung beachtet werden, aber der Wert muss dem für die Option REPLSERVERName angegebenen Wert entsprechen.

Beispiele

Optionsdatei:

```
MYREPLICATIONServer TargetReplicationServer1
```

Befehlszeile:

Nicht zutreffend.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeOptionsdatei:

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei dsm.sys angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Verbindungsinformationen für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option replservername und den Namen des Sekundärservers angegeben. Die Zeilengruppe servername muss die Option myreplicationserver enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe replservername angegeben wird. Nur ein Sekundärserver kann für jeweils eine Zeilengruppe servername angegeben werden.

```
REPLSERVERNAME    TargetReplicationServer1
  REPLTCPSERVERADDRESS TargetReplicationServer1
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

REPLSERVERNAME   TargetReplicationServer2
  REPLTCPSERVERADDRESS TargetReplicationServer2
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02

SErvername     server_a
     COMMMethod               TCPip
  TCPPort                  1500
     TCPServeraddress         server_hostname1.example.com
  PASSWORDAccess           prompt
  MYREPLICATIONServer      TargetReplicationServer1

SErvername     server_b
  COMMMethod               TCPip
  TCPPort                  1500
     TCPServeraddress         server_hostname2.example.com
  PASSWORDAccess           generate
     INCLExcl                 /adm/tsm/archive.excl
     MYREPLICATIONServer      TargetReplicationServer2

SErvername     server_c
  COMMMethod               TCPip
  TCPPort                  1500
     TCPServeraddress         server_hostname3.example.com
  PASSWORDAccess           generate
  MYREPLICATIONServer      TargetReplicationServer1
```

Windows-BetriebssystemeOptionsdatei:

Windows-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für den Sekundärserver in der Datei dsm.opt angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Die Verbindungsinformationen für den Sekundärserver befinden sich in der Zeilengruppe REPLSERVERName. Die Option MYREPLICATIONServer verweist auf den Namen des Sekundärservers, der durch die Zeilengruppe REPLSERVERName angegeben wird.

```
REPLSERVERNAME    TargetReplicationServer1
    REPLTCPSERVERADDRESS TargetReplicationServer1
    REPLTCPPORT          1505
```

```
        REPLSSLPORT          1506
        REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

    COMMMethod               TCPip
    TCPPort                  1500
    TCPServeraddress         server_hostname1.example.com
    PASSWORDAccess           prompt
    MYREPLICATIONServer      TargetReplicationServer1
    MYPRIMARYSERVER          Server1
```

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Client für automatisierte Übernahme konfigurieren
Windows-Betriebssysteme

Namedpipename

Die Option namedpipename gibt den Namen der benannten Pipe an, die für die Übertragung zwischen einem Client und einem Server in derselben Windows-Serverdomäne verwendet werden soll.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung des Profileditors definieren.

Syntax

```
>>-NAMedpipename-- --Name---------------------------------------><
```

Parameter

Name
Der Name einer benannten Pipe. Standardwert ist **\\.\pipe\Server1**.

Beispiele

Optionsdatei:
```
namedpipename \\.\pipe\dsmser1
```
Befehlszeile:
```
-namedpipename=\\.\pipe\dsmser1
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Nasnodename

Die Option nasnodename gibt den Knotennamen des NAS-Dateiservers bei der Verarbeitung von NAS-Dateisystemen an. Der Client fordert Sie zur Eingabe einer Administrator-ID auf.

Der Knotenname identifiziert den NAS-Dateiserver für den IBM Spectrum Protect-Server. Der Server muss den NAS-Dateiserver registrieren.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeSie können diese Option in der Befehlszeile oder in der Clientsystemoptionsdatei (dsm.sys) angeben.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeSie können den Standardwert in der Datei dsm.sys überschreiben, indem Sie einen anderen Wert in die Befehlszeile eingeben. Wenn Sie die Option nasnodename nicht in der Datei dsm.sys angeben, müssen Sie diese Option bei der Verarbeitung von NAS-Dateisystemen in der Befehlszeile angeben.

 Windows-BetriebssystemeSie können diese Option in der Befehlszeile oder in der Clientoptionsdatei (dsm.opt) angeben.

 Windows-BetriebssystemeSie können den Standardwert in der Datei dsm.opt überschreiben, indem Sie einen anderen Wert in die Befehlszeile eingeben. Wenn Sie die Option nasnodename nicht in der Datei dsm.opt angeben, müssen Sie diese Option bei der Verarbeitung von NAS-Dateisystemen in der Befehlszeile angeben.

Die Option nasnodename können Sie in folgenden Befehlen verwenden:

- backup nas
- delete filespace
- query backup
- query filespace
- restore nas

Mit dem Befehl delete filespace können Sie NAS-Dateibereiche interaktiv aus dem Serverspeicher löschen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeVerwenden Sie die Option nasnodename, um den NAS-Dateiserver zu identifizieren. Fügen Sie die Option nasnodename in Ihre Clientsystemoptionsdatei (dsm.sys) ein. Der Wert in der Clientsystemoptionsdatei ist der Standardwert, dieser Wert kann jedoch in der Befehlszeile überschrieben werden. Ist die Option nasnodename nicht in der Clientsystemoptionsdatei angegeben, müssen Sie diese Option bei der Verarbeitung von NAS-Dateisystemen in der Befehlszeile angeben.

 Windows-BetriebssystemeVerwenden Sie die Option nasnodename, um den NAS-Dateiserver zu identifizieren. Fügen Sie die Option nasnodename in Ihre Clientoptionsdatei (dsm.opt) ein. Der Wert in der Clientoptionsdatei ist der Standardwert, dieser Wert kann jedoch in der Befehlszeile überschrieben werden. Ist die Option nasnodename nicht in der Clientoptionsdatei angegeben, müssen Sie diese Option bei der Verarbeitung von NAS-Dateisystemen in der Befehlszeile angeben.

Mit der Option class können Sie die Klasse des zu löschenden Dateibereichs angeben. Verwenden Sie die Option -class=nas, um eine Liste der zu einem NAS-Knoten gehörenden Dateibereiche anzuzeigen, in der Sie einen Dateibereich zum Löschen auswählen können.

Informationen zum Löschen von NAS-Dateibereichen mit dem Web-Client finden Sie im Abschnitt zum Sichern Ihrer Daten.

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist nur für die AIX-, Linux- und Solaris-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

 Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-Client-API unterstützt diese Option nicht.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Allgemein des Profileditors definieren.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Allgemein des Profileditors definieren.

Syntax

```
>>-NASNodename-- --Knotenname---------------------------------><
```

Parameter

Knotenname
: Gibt den Knotennamen für den NAS-Dateiserver an.

Beispiele

Optionsdatei:
```
nasnodename nas2
```
Befehlszeile:
```
-nasnodename=nas2
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

Nfstimeout

Die Option nfstimeout gibt die Wartezeit des Clients auf einen Statussystemaufruf für ein NFS-Dateisystem in Sekunden an, bevor eine Zeitlimitüberschreitung auftritt.

Mit dieser Option können Sie das Standardverhalten von Statusaufrufen für Dateisysteme abmildern. Wenn ein NFS-Dateisystem beispielsweise nicht aktuell ist, wird ein Statussystemaufruf durch NFS wegen Zeitlimitüberschreitung beendet (bedingter Mount) oder er blockiert den Prozess (absoluter Mount).

Wird der Wert dieser Option in einen anderen Wert außer Null geändert, wird vom aufrufenden Modul ein neuer Thread erstellt, um den Statussystemaufruf auszugeben. Der neue Prozess wird vom aufrufenden Thread wegen Zeitlimitüberschreitung beendet, und die Operation kann fortgesetzt werden.

Oracle Solaris-BetriebssystemeAnmerkung: Unter Solaris kann die Option nfstimeout fehlschlagen, wenn der NFS-Mount ein absoluter Mount ist. Bleibt das System hängen, müssen Sie die Option nfstimeout inaktivieren und das NFS-Dateisystem wie folgt mit einem bedingten Mount anhängen:

```
mount -o soft,timeo=5,retry=5 machine:/filesystem /mountpoint
```

Die Parameter sind wie folgt definiert:

soft
: Generiert einen bedingten Mount des NFS-Dateisystems. Tritt ein Fehler auf, gibt die Funktion stat() einen Fehler zurück. Wird die Option hard verwendet, gibt stat() erst dann einen Rückkehrcode aus, wenn das Dateisystem verfügbar ist.

timeo=n
: Setzt das Zeitlimit für den Fehler eines bedingten Mounts auf *n* Zehntel einer Sekunde.

retry=n
: Setzt die internen Wiederholungen und die Mountwiederholungen auf *n*, Standardwert ist 10000.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe *oder* in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-NFSTIMEout-- --Zahl-----------------------------------------><
```

Parameter

Zahl
: Gibt die Wartezeit des Clients auf einen Statussystemaufruf für ein Dateisystem in Sekunden an, bevor eine Zeitlimitüberschreitung auftritt. Der Wertebereich ist 0 bis 120; Standardwert ist 0 Sekunden.

Beispiele

Optionsdatei:
```
nfstimeout 10
```
Befehlszeile:
```
-nfstimeout=10
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Nodename

Verwenden Sie die Option nodename in Ihrer Clientoptionsdatei, um Ihre Workstation beim Server zu identifizieren. Für mehrere Betriebssysteme auf der Workstation können verschiedene Knotennamen verwendet werden.

Wenn Sie die Option nodename verwenden, werden Sie zur Eingabe des Kennworts aufgefordert, das dem angegebenen Knoten zugeordnet ist, falls ein Kennwort erforderlich ist.

Wenn Sie Dateien vom Server zurückschreiben oder abrufen wollen, während Sie an einer anderen Workstation arbeiten, müssen Sie die Option virtualnodename verwenden. Sie können auch die Option asnodename verwenden, wenn sie vom Administrator definiert wurde.

Windows-BetriebssystemeWenn Sie an einer anderen Workstation arbeiten, können Sie die Option nodename selbst dann verwenden, wenn die Option passwordaccess auf generate gesetzt ist. Um dies zu verhindern, verwenden Sie die Option virtualnodename anstelle von nodename.

Windows-BetriebssystemeDer Knotenname ist nicht notwendigerweise der TCP/IP-Hostname.

Wenn eine Verbindung zu einem Server hergestellt wird, muss sich der Client beim Server identifizieren. Diese Anmeldeidentifikation wird wie folgt bestimmt:

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeIst weder ein Eintrag nodename in der Datei dsm.sys noch ein Eintrag virtualnodename in der Clientbenutzeroptionsdatei (dsm.opt) vorhanden und wird kein virtueller Knotenname in einer Befehlszeile angegeben, ist die Standardanmelde-ID der Name, den der Befehl hostname zurückgibt.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeIst ein Eintrag nodename in der Datei dsm.sys vorhanden, überschreibt der Eintrag nodename den Namen, den der Befehl hostname zurückgibt.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeIst ein Eintrag virtualnodename in der Clientsystemoptionsdatei (dsm.sys) vorhanden oder wird ein virtueller Knotenname in einer Befehlszeile angegeben, darf dieser Name nicht dem Namen entsprechen, den der Befehl hostname zurückgibt. Wenn der Server den virtuellen Knotennamen akzeptiert, ist ein Kennwort erforderlich (wenn die Authentifizierung aktiv ist), auch wenn für die Option passwordaccess der Wert generate gilt. Sobald eine Verbindung zum Server besteht, ist der Zugriff auf alle Dateien zulässig, die unter Verwendung dieser Anmelde-ID gesichert werden.
- Windows-BetriebssystemeIst weder ein Eintrag nodename in der Datei dsm.opt noch ein Eintrag virtualnodename in der Clientoptionsdatei (dsm.opt) vorhanden und wird kein virtueller Knotenname in einer Befehlszeile angegeben, gibt der Befehl hostname den Namen der Standardanmelde-ID zurück.
- Windows-BetriebssystemeIst ein Eintrag nodename in der Datei dsm.opt vorhanden, überschreibt der Eintrag nodename den Namen, den der Befehl hostname zurückgibt.
- Windows-BetriebssystemeIst ein Eintrag virtualnodename in der Clientoptionsdatei (dsm.opt) vorhanden oder wird ein virtueller Knotenname in einer Befehlszeile angegeben, darf dieser Name nicht dem Namen entsprechen, den der Befehl hostname zurückgibt. Wenn der Server den virtuellen Knotennamen akzeptiert, ist ein Kennwort erforderlich (wenn die Authentifizierung aktiv ist), auch wenn für die Option passwordaccess der Wert generate gilt. Sobald eine Verbindung zum Server besteht, ist der Zugriff auf alle Dateien zulässig, die unter Verwendung dieser Anmelde-ID gesichert werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Allgemein im Feld Knotenname im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Allgemein im Feld Knotenname im Profileditor definieren.

Syntax

```
>>-NODename-- --Knotenname-------------------------------------><
```

Parameter

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeKnotenname
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt einen aus 1 bis 64 Zeichen bestehenden Knotennamen an, für den IBM Spectrum Protect-Services angefordert werden sollen. Der Standardwert ist der Wert, der mit dem Befehl hostname zurückgegeben wird.

Wird kein Knotenname angegeben, kann der Knotenname standardmäßig den Hostnamen der Workstation annehmen.

Windows-BetriebssystemeKnotenname
Windows-BetriebssystemeGibt einen aus 1 bis 64 Zeichen bestehenden Knotennamen an, für den IBM Spectrum Protect-Services angefordert werden sollen. Der Standardwert ist der Wert, der mit dem Befehl hostname zurückgegeben wird.

Wird kein Knotenname angegeben, kann der Knotenname standardmäßig den Hostnamen der Workstation annehmen.

Beispiele

Optionsdatei:
```
nodename cougar
```
Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme`-nodename=cougar`

Windows-BetriebssystemeDiese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Windows-Betriebssysteme

Nojournal

Verwenden Sie die Option nojournal im Befehl incremental, um anzugeben, dass statt der standardmäßigen journalbasierten Sicherung eine traditionelle vollständige Teilsicherung ausgeführt werden soll.

Die journalbasierte Teilsicherung unterscheidet sich von der traditionellen vollständigen Teilsicherung wie folgt:

- Nicht standardmäßige Kopienhäufigkeiten (außer 0) werden auf dem IBM Spectrum Protect-Server nicht erzwungen.
- Attributänderungen an einem Objekt erfordern eine Sicherung des gesamten Objekts.

Aus diesen Gründen empfiehlt es sich möglicherweise, regelmäßig die Option nojournal zu verwenden, um eine traditionelle vollständige Teilsicherung auszuführen.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-NOJournal-------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc incr c: -nojournal
```

 AIX-Betriebssysteme  Linux-Betriebssysteme

Nojournal

Verwenden Sie die Option nojournal im Befehl incremental, um anzugeben, dass statt der standardmäßigen journalbasierten Sicherung eine traditionelle vollständige Teilsicherung ausgeführt werden soll.

Die journalbasierte Teilsicherung unterscheidet sich von der traditionellen vollständigen Teilsicherung wie folgt:

- Nicht standardmäßige Kopienhäufigkeiten (außer 0) werden auf dem IBM Spectrum Protect-Server nicht erzwungen.
- Änderungen an speziellen UNIX-Dateien werden vom Journaldämon nicht festgestellt und folglich auch nicht gesichert.

Aus diesen Gründen empfiehlt es sich möglicherweise, regelmäßig die Option nojournal zu verwenden, um eine traditionelle vollständige Teilsicherung auszuführen.

Unterstützte Clients

Diese Option ist für den AIX- und Linux-Client für Sichern/Archivieren gültig.

Syntax

```
>>-NOJournal-------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
dsmc incr /home -nojournal
```

Noprompt

Die Option noprompt unterdrückt die Bestätigungsaufforderung, die von den Befehlen delete group, delete archive, expire, restore image und set event angezeigt wird.

- delete archive
- delete backup

- delete group
- expire
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemerestore image

Mac OS X-BetriebssystemeAnmerkung: Der Befehl restore image ist nicht für Mac OS X-Betriebssysteme anwendbar.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-NOPrompt---------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssystemedsmc delete archive -noprompt "/Users/van/Documents/*"

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemedsmc delete archive -noprompt "/home/project/*"

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssystemedsmc delete archive -noprompt c:\home\project*

Nrtablepath

Die Option nrtablepath gibt die Position der Knotenreplikationstabelle auf dem Client an. Der Client für Sichern/Archivieren verwendet diese Tabelle für die Speicherung von Informationen zu jeder Sicherungs- oder Archivierungsoperation auf dem IBM Spectrum Protect-Server.

Der Server, auf dem Sie Ihre Daten sichern, muss mindestens die Version 7.1 aufweisen und muss Clientknotendaten auf dem Sekundärserver replizieren.

Wenn eine Übernahme stattfindet, könnten die Informationen auf dem Sekundärserver nicht die neueste Version aufweisen, falls vor der Übernahme keine Replikation stattfand. Der Client kann die Informationen in der Knotenreplikationstabelle mit den Informationen vergleichen, die sich auf dem Sekundärserver befinden, um festzustellen, ob die Sicherung auf dem Server die neueste Sicherungsversion ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Diese Option kann auch in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server konfiguriert werden.

Syntax

```
>>-NRTABLEPath----Pfad----------------------------------------><
```

Parameter

Pfad

Gibt die Position an, an der die Datenbank der Knotenreplikationstabelle erstellt wird. Die Standardposition ist das Installationsverzeichnis des Clients für Sichern/Archivieren.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeFür Benutzer ohne Rootberechtigung müssen Sie einen Pfad angeben, für den Ihre Benutzer-ID Schreibzugriff hat, z. B. ein temporäres Verzeichnis. Die

meisten Benutzer ohne Rootberechtigung haben keinen Zugriff auf das Clientinstallationsverzeichnis.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeEinschränkung: Die Knotenreplikationstabelle kann nicht im Stammverzeichnis (/) erstellt werden. Wenn Sie eine Position für die Knotenreplikationstabelle angeben wollen, verwenden Sie nicht das Stammverzeichnis.
Windows-BetriebssystemeEinschränkung: Die Knotenreplikationstabelle kann nicht im Verzeichnis C:\ erstellt werden. Wenn Sie eine Position für die Knotenreplikationstabelle angeben wollen, verwenden Sie nicht das Verzeichnis C:\.

Beispiel

Optionsdatei:

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme`nrtablepath /Volumes/nrtbl`

Windows-Betriebssysteme`nrtablepath C:\nrtbl`

Befehlszeile:

Nicht zutreffend.

Zugehörige Tasks:
Status replizierter Clientdaten bestimmen
Client für automatisierte Übernahme konfigurieren

Numberformat

Mit der Option numberformat wird das Format angegeben, das zum Anzeigen von Zahlen verwendet werden soll.

Windows-BetriebssystemeVerwenden Sie diese Option, wenn Sie das standardmäßige Zahlenformat für die Sprache des von Ihnen verwendeten Nachrichtenrepositorys ändern wollen.

AIX-Betriebssysteme Oracle Solaris-BetriebssystemeDie AIX- und Solaris-Clients unterstützen andere Ländereinstellungen als Englisch, die jede Benutzerschnittstelle beschreiben, deren Position oder Sprache abweicht.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme Der Client für Sichern/Archivieren und der Verwaltungsclient erhalten standardmäßig Formatinformationen aus der Ländereinstellungsdefinition, die beim Aufruf des Clients aktiv ist. Ausführliche Informationen zur Definition der länderspezifischen Angaben können der Dokumentation auf dem lokalen System entnommen werden.

Anmerkung: Die Option numberformat wirkt sich nicht auf den Web-Client aus. Der Web-Client verwendet das Zahlenformat der Ländereinstellung, die im Browser aktiv ist. Ist im Browser eine nicht unterstützte Ländereinstellung aktiv, verwendet der Web-Client das Zahlenformat für amerikanisches Englisch.

Die Option numberformat können Sie in folgenden Befehlen verwenden:

- delete archive
- delete backup
- expire
- query archive
- Windows-Betriebssystemequery asr
- query backup
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemequery image
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme AIX-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssystemequery nas
- Windows-Betriebssystemequery systemstate
- restore
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemerestore image
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssystemerestore nas
- Windows-Betriebssystemerestore registry
- retrieve
- set event

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Regionale Einstellungen im

Feld Zahlenformat im Profileditor definieren.

Syntax

```
>>-NUMberformat-- --Nummer-------------------------------------><
```

Parameter

Zahl
: Zeigt Zahlen in einem der folgenden Formate an. Die Nummer (0–6) für das Zahlenformat angeben, das verwendet werden soll.

  0
  : Das in den länderspezifischen Angaben definierte Datumsformat verwenden. Dies ist der Standardwert (gilt nicht für Mac OS X).

  1
  : 1,000.00

     AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
     Windows-BetriebssystemeDies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

     AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
     Windows-Betriebssysteme

    - Amerikanisches Englisch
    - Japanisch
    - Traditionelles Chinesisch
    - Vereinfachtes Chinesisch
    - Koreanisch

  2
  : 1,000,00

  3
  : 1 000,00

     AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
     Windows-BetriebssystemeDies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

     AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
    Windows-Betriebssysteme

    - Französisch
    - Tschechisch
    - Ungarisch
    - Polnisch
    - Russisch

  4
  : 1 000.00

  5
  : 1.000,00

     AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
    Windows-BetriebssystemeDies ist der Standardwert für die folgenden verfügbaren Übersetzungen:

     AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
    Windows-Betriebssysteme

    - Brasilianisches Portugiesisch
    - Deutsch
    - Italienisch
    - Spanisch

  6
  : 1'000,00

 AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeFür AIX und Solaris: Um Zahlenformate zu definieren, ändern Sie die folgenden Zeilen in der Quellendatei für Ihre Ländereinstellung. Das ausgewählte Format gilt sowohl für die Ausgabe als auch für die Eingabe.

 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme

decimal_point
: Dezimalzeichen. Das Zeichen, das die ganze Zahl von ihrem Bruchteil trennt.

thousands_sep
: Tausendertrennzeichen. Das Zeichen, das die Hunderter, Tausender und Millionen trennt.

grouping
: Gruppierung. Die Anzahl Stellen in jeder Gruppe, die durch das Tausendertrennzeichen getrennt werden.

Beispiele

Optionsdatei:
```
num 4
```
Befehlszeile:
```
-numberformat=4
```

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Optfile

Die Option optfile gibt die Clientoptionsdatei an, die verwendet werden soll, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Syntax

```
>>-OPTFILE = - --Dateiname-------------------------------------><
```

Parameter

Dateiname
: Gibt eine alternative Clientoptionsdatei an, wenn Sie den vollständig qualifizierten Pfadnamen verwenden. Wenn Sie nur den Dateinamen angeben, nimmt der Client an, dass die angegebene Datei sich im aktuellen Arbeitsverzeichnis befindet. Der Standardwert ist dsm.opt.

  AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme**Einschränkung:** Geben Sie den vollständigen Pfad an, wenn Sie diese Option mit dem Clientakzeptordämon (dsmcad) verwenden, da der Clientakzeptordämon sein Arbeitsverzeichnis nach der Initialisierung in das Stammverzeichnis ("/") ändert.

Beispiele

Befehlszeile:
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

```
dsmc query session -optfile=myopts.opt
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

Clientakzeptordämon:
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

```
dsmcad -optfile=/usr/tivoli/tsm/client/ba/bin/myopts.opt
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Password

Die Option password gibt ein Kennwort für IBM Spectrum Protect an.

Wenn Sie diese Option nicht angeben und Ihr Administrator die Authentifizierung auf On gesetzt hat, werden Sie zur Eingabe eines Kennworts aufgefordert, wenn Sie eine Sitzung des Clients für Sichern/Archivieren starten.

Anmerkung:

1. Wenn der Server die Kennworteingabe anfordert, wird das Kennwort während der Eingabe nicht angezeigt. Wenn Sie die Option password in der Befehlszeile verwenden, wird Ihr Kennwort jedoch bei der Eingabe angezeigt.
2. Wenn sich der Name des IBM Spectrum Protect-Servers ändert oder die Clients für Sichern/Archivieren zu einem anderen Server geleitet werden, müssen alle Clients sich erneut beim Server authentifizieren, da das gespeicherte verschlüsselte Kennwort neu generiert werden muss.

Die Option password wird ignoriert, wenn für die Option passwordaccess der Wert generate definiert wird.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

```
>>-PASsword-- --Kennwort---------------------------------------><
```

Parameter

Kennwort
Gibt das Kennwort an, mit dem Sie sich beim IBM Spectrum Protect-Server anmelden.

Die maximale Kennwortlänge beträgt 63 Zeichen. Die Vorgaben für Kennwörter sind davon abhängig, wo die Kennwörter gespeichert und verwaltet werden und von der Version des Servers, zu dem Ihr Client eine Verbindung herstellt.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden
Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Bei den Kennwörtern muss die Groß-/Kleinschreibung beachtet werden. Außerdem können die Kennwörter weiteren Einschränkungen aufgrund von LDAP-Richtlinien unterliegen.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie keinen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden
Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Kennwörter werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

Wenn Ihr IBM Spectrum Protect-Server eine Version vor Version 6.3.3 aufweist
Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
_ - & + .
```

Kennwörter werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-Betriebssysteme
 Windows-BetriebssystemeHinweis:

Schließen Sie in der Befehlszeile alle Parameter, die mindestens ein Sonderzeichen enthalten, in Anführungszeichen ein. Ohne Anführungszeichen können die Sonderzeichen als Shell-Escapezeichen, als Dateiumleitungszeichen oder als andere Zeichen, die eine Bedeutung für das Betriebssystem haben, interpretiert werden.

Windows-Betriebssysteme

Auf Windows-Systemen:
Schließen Sie die Befehlsparameter in Anführungszeichen (") ein.

Beispiel für die Befehlszeile:
```
dsmc set password "t67@#$%^&" "pass2><w0rd"
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Auf AIX-, Linux- und Solaris-Systemen:
Schließen Sie die Befehlsparameter in Hochkommas (') ein.

Beispiel für die Befehlszeile:
```
dsmc set password -type=vmguest 'Win 2012 SQL' 'tsml2dag\administrator' '7@#$%^&7'
```

Anführungszeichen sind nicht erforderlich, wenn Sie ein Kennwort mit Sonderzeichen in einer Optionsdatei eingeben.

Beispiele

Optionsdatei:
```
password secretword
```
Befehlszeile:
```
-password=secretword
```
Windows-Betriebssysteme-password="secret>shhh"
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme-password='my>pas$word'

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Passwordaccess

Mit der Option passwordaccess kann angegeben werden, ob Ihr Kennwort automatisch generiert oder als Benutzereingabeaufforderung definiert werden soll.

Ihr Administrator kann ein Kennwort für Ihren Clientknoten erforderlich machen, indem die Authentifizierungsfunktion aktiviert wird. Fragen Sie Ihren Administrator, ob für Ihren Clientknoten ein Kennwort erforderlich ist.

Wenn ein Kennwort erforderlich ist, können Sie eine der folgenden Methoden auswählen:

- Das Kennwort für den Clientknoten selbst definieren und den Client bei jeder Serviceanforderung zur Eingabe des Kennworts auffordern lassen.
- Den Client automatisch ein neues Kennwort für den Clientknoten generieren lassen, sobald ein Kennwort abläuft, das Kennwort verschlüsseln und in einer Datei speichern und bei einer Serviceanforderung aus dieser Datei abrufen. Sie werden nicht zur Eingabe des Kennworts aufgefordert.
- Ist in der Serverkonfiguration nicht festgelegt, dass ein Kennwort für die Anmeldung erforderlich ist, können Sie dennoch zur Eingabe Ihres Knotenkennworts aufgefordert werden, wenn der Client für Sichern/Archivieren eine Verbindung zu dem Server herstellt. Dieses Verhalten tritt auf, wenn für diese Option, passwordaccess, der Standardwert verwendet wird oder wenn Sie sie auf passwordaccess prompt setzen. Das Kennwort, das Sie bei der Eingabeaufforderung angeben, wird nur zur Verschlüsselung Ihrer Anmeldeinformationen verwendet und nicht für die Anmeldung beim Server. In dieser Konfiguration können Sie die Kennworteingabe vermeiden, indem Sie diese Option auf passwordaccess generate setzen. Die Festlegung von passwordaccess generate bewirkt, dass der Client das Kennwort für Sie erstellt, speichert und übergibt. Ist passwordaccess generate festgelegt, wird die Option password ignoriert.

Das Setzen der Option passwordaccess auf generate ist in folgenden Situationen erforderlich:

- AIX-BetriebssystemeLinux-BetriebssystemeBei Verwendung des HSM-Clients.
- Bei Verwendung des Web-Clients.
- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeBei der Ausführung von NAS-Operationen.
- Bei Verwendung von IBM Spectrum Protect for Workstations.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Berechtigung im Abschnitt Kennwortzugriff des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Berechtigung im Abschnitt Kennwortzugriff des Profileditors definieren.

Syntax

```
                    .-prompt---.
>>-PASSWORDAccess--+----------+--------------------------------><
                    '-generate-'
```

Parameter

prompt
: Sie werden jedes Mal, wenn ein Client eine Verbindung zum Server herstellt, zur Eingabe des Kennworts für Ihren Clientknoten aufgefordert. Dies ist der Standardwert.

  Zur Geheimhaltung des Kennworts des Clientknotens sollten Befehle ohne das Kennwort eingegeben und stattdessen auf die Kennworteingabeaufforderung durch den Client gewartet werden.

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeJeder Benutzer muss das IBM Spectrum Protect-Kennwort für Ihren Clientknoten kennen. Alle Benutzer, die das Kennwort für Ihren Clientknoten kennen, können auf alle Sicherungen und Archivierungen zugreifen, die auf Ihrem Clientknoten vorgenommen wurden. Wenn der Benutzer beispielsweise den Knotennamen und das Kennwort für Ihren Clientknoten von einem anderen Clientknoten aus eingibt, wird der Benutzer zu einem virtuellen Root.

  API-Anwendungen müssen das Kennwort zur Verfügung stellen, wenn eine Sitzung eingeleitet wird. Die Anwendung ist verantwortlich für das Abrufen des Kennworts.

generate
: Das Kennwort des Benutzers wird verschlüsselt und lokal gespeichert; wenn das alte Kennwort verfällt, wird ein neues Kennwort generiert. Das neue Kennwort wird vom Client zufällig generiert. Die Vorgaben für Kennwörter sind davon abhängig, wo die Kennwörter gespeichert und verwaltet werden und von der Version des Servers, zu dem Ihr Client eine Verbindung herstellt. Generierte Kennwörter haben eine Länge von 63 Zeichen und enthalten mindestens zwei der folgenden Zeichen:

  - Großbuchstaben
  - Kleinbuchstaben
  - Numerische Zeichen
  - Sonderzeichen

  Außerdem ist das erste und das letzte Zeichen eines generierten Kennworts ein alphabetisches Zeichen in Groß- oder Kleinschreibung. Generierte Kennwörter enthalten keine wiederholten Zeichen.

Eine Aufforderung zur Kennworteingabe erfolgt bei der offenen Registrierung einer Workstation in einem Server oder wenn Ihr Administrator Ihr Kennwort manuell ändert.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBei einer lokalen Anmeldung müssen die Benutzer das Kennwort für den Clientknoten nicht kennen. Mithilfe der Option nodename auf einem fernen Knoten können Benutzer jedoch auf eigene Dateien zugreifen und auf Dateien, für die ihnen ein anderer Benutzer Zugriffsberechtigung erteilt hat.

Beispiele

Optionsdatei:

```
passwordaccess generate
```

Befehlszeile:

Nicht zutreffend.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

Passworddir

Die Option passworddir gibt die Verzeichnisposition an, in der eine verschlüsselte Kennwortdatei gespeichert werden soll.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDas Standardverzeichnis für AIX ist /etc/security/adsm. Für andere UNIX- und Linux-Plattformen ist das Standardverzeichnis /etc/adsm. Das Standardverzeichnis für Mac ist /Library/Preferences/Tivoli Storage Manager. Unabhängig von ihrem Speicherort wird der vom Client erstellten Kennwortdatei immer der Name TSM.sth zugeordnet. Eine Kennwortdatei wird aus drei Dateien gebildet. In TSM.KDB werden die verschlüsselten Kennwörters gespeichert. In

TSM.sth wird der Verschlüsselungszufallsschlüssel gespeichert, mit dem Kennwörter in der Datei TSM.KDB verschlüsselt werden. Diese Datei wird durch das Dateisystem geschützt. TSM.IDX ist eine indexierte Datei zur Protokollierung der Kennwörter in der Datei TSM.KDB.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle UNIX-Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

```
>>-PASSWORDDIR-- --Verzeichnisname----------------------------><
```

Parameter

Verzeichnisname
: Gibt den Pfad an, in dem die verschlüsselte Kennwortdatei gespeichert werden soll. Die Kennwortdatei hat den Namen TSM.sth. Ist ein Bestandteil des angegebenen Pfads nicht vorhanden, versucht IBM Spectrum Protect, ihn zu erstellen.

Beispiele

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
Optionsdatei:

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme
 Mac OS X-Betriebssysteme  Mac OS X-Betriebssysteme

```
passworddir "/Users/user1/Library/Preferences/Tivoli Storage Manager/"
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

```
passworddir /etc/security/tsm
```

Befehlszeile:
: Nicht zutreffend.

Pick

Die Option pick erstellt eine Liste der Sicherungsversionen oder Archivierungskopien, die mit der von Ihnen eingegebenen Dateispezifikation übereinstimmen.

Aus der Liste können die zu verarbeitenden Versionen ausgewählt werden. Fügen Sie die Option inactive ein, um sowohl aktive als auch inaktive Objekte anzuzeigen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-BetriebssystemeWerden bei Images kein Quellendateibereich und kein Zieldateibereich angegeben, enthält die Auswahlliste alle gesicherten Images. In diesem Fall werden die aus der Liste ausgewählten Images an ihre ursprüngliche Position zurückgeschrieben. Werden der Quellendateibereich und der Zieldateibereich angegeben, darf nur ein einziger Eintrag aus der Liste ausgewählt werden.

Die Option pick ist in den folgenden Befehlen zu verwenden:

- delete archive
- delete backup
- delete group
- expire
- restore
-  Windows-Betriebssystemerestore asr
- restore group
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssystemerestore image
-  AIX-Betriebssysteme  Linux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
   Windows-Betriebssystemerestore nas
-  Windows-Betriebssystemerestore vm
- retrieve

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-PIck-----------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssysteme `dsmc restore "/Users/van/Documents/*" -pick -inactive`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme`dsmc restore "/home/project/*" -pick -inactive`

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`dsmc restore c:\project\* -pick -inactive`

Pitdate

Verwenden Sie die Option pitdate mit der Option pittime, um einen Zeitpunkt zu definieren, für den die letzte Version Ihrer Sicherungen angezeigt oder zurückgeschrieben werden soll.

Dateien, deren Sicherung *zu oder vor* dem von Ihnen angegebenen Zeitpunkt (Datum und Uhrzeit) erfolgte und die nicht *vor* diesem Zeitpunkt gelöscht wurden, werden verarbeitet. Nach diesem Datum und dieser Uhrzeit erstellte Sicherungsversionen werden ignoriert.

Die Option pitdate ist in den folgenden Befehlen zu verwenden:

- delete backup
- Windows-Betriebssystemequery asr
- query backup
- query group
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemequery image
- Windows-Betriebssystemequery nas
- Windows-Betriebssystemequery systemstate
- Windows-Betriebssystemequery vm (vmbackuptype=fullvm und vmbackuptype=hypervfull)
- restore
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemerestore group
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemerestore image
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemerestore nas
- Windows-Betriebssystemerestore vm (vmbackuptype=fullvm und vmbackuptype=hypervfull)

Wird pitdate verwendet, werden die Optionen inactive und latest implizit verwendet.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-PITDate = - --Datum-------------------------------------><
```

Parameter

Datum

Gibt das entsprechende Datum an. Das Datum muss in dem mit der Option dateformat ausgewählten Format eingegeben werden.

Wenn dateformat in einem Befehl angegeben wird, muss diese Option vor den Optionen fromdate, pitdate und todate stehen.

Beispiele

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssystemedsmc restore "/Volumes/proj4/myproj/*" -sub=y -pitdate=08/01/2003 -pittime=06:00:00

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedsmc restore "/fs1/*" -sub=y -pitdate=08/01/2003 -pittime=06:00:00

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssystemedsmc restore -pitdate=08/01/2003 c:\myfiles\

Pittime

Verwenden Sie die Option pittime mit der Option pitdate, um einen Zeitpunkt zu definieren, für den die letzte Version Ihrer Sicherungen angezeigt oder zurückgeschrieben werden soll.

Dateien, deren Sicherung *zu oder vor* dem von Ihnen angegebenen Zeitpunkt (Datum und Uhrzeit) erfolgte und die nicht *vor* diesem Zeitpunkt gelöscht wurden, werden verarbeitet. Nach diesem Datum und dieser Uhrzeit erstellte Sicherungsversionen werden ignoriert. Diese Option wird ignoriert, wenn Sie die Option pitdate nicht angeben.

Die Option pittime ist in den folgenden Befehlen zu verwenden:

- delete backup
- Windows-Betriebssystemequery asr
- query backup
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemequery image
- Windows-Betriebssystemequery nas
- Windows-Betriebssystemequery systemstate
- Windows-Betriebssystemequery vm(vmbackuptype=fullvm und vmbackuptype=hypervfull)
- restore
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemerestore image
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssystemerestore nas
- Windows-Betriebssystemerestore vm (vmbackuptype=fullvm und vmbackuptype=hypervfull)

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-PITTime = - --Zeit-----------------------------------------><
```

Parameter

Zeit

Gibt eine Uhrzeit an einem bestimmten Datum an. Wenn keine Zeit angegeben wird, lautet der Standardwert 23:59:59. Die Zeit muss in dem mit der Option timeformat ausgewählten Format angegeben werden.

Wenn die Option timeformat in einem Befehl angegeben wird, muss sie vor den Optionen fromtime, pittime und tottime stehen.

Beispiele

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssystemedsmc query backup -pitt=06:00:00 -pitd=08/01/2003 "/Volumes/proj5/myproj/*"

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedsmc q b "/fs1/*" -pitt=06:00:00 -pitd=08/01/2003

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssystemedsmc query backup -pitt=06:00:00 -pitd=08/01/2003 c:\myfiles\

Postschedulecmd/Postnschedulecmd

Die Option postschedulecmd/postnschedulecmd gibt einen Befehl an, den das Clientprogramm verarbeitet, nachdem ein Zeitplan ausgeführt wurde.

Wenn das Clientprogramm auf die Beendigung des Befehls warten soll, bevor es andere Verarbeitungsschritte fortsetzt, verwenden Sie die Option postschedulecmd. Wenn nicht auf die Beendigung des Befehls gewartet werden soll, bevor der Client andere Verarbeitungsschritte fortsetzt, geben Sie die Option postnschedulecmd an.

Die Handhabung von Rückkehrcodes und das Verhalten bei geplanten Aktionen ist einerseits von der angegebenen Option und andererseits vom Typ der geplanten Operation abhängig:

- Geplante Operationen, bei denen die geplante Aktion nicht COMMAND ist:

  Wenn der Befehl postschedulecmd nicht mit dem Rückkehrcode 0 (null) beendet wird, ist der Rückkehrcode für das geplante Ereignis entweder 8 oder der Rückkehrcode der geplanten Operation (der höhere der beiden Codes). Wenn Sie nicht wollen, dass diese Regel auf den Befehl postschedulecmd angewendet wird, können Sie eine Script- oder Stapeldatei erstellen, die den Befehl aufruft und mit dem Rückkehrcode 0 beendet wird. Dann müssen Sie postschedulecmd so konfigurieren, dass die Script- oder Stapeldatei gestartet wird.

- Geplante Operationen, bei denen die geplante Aktion COMMAND ist:

  Der Rückkehrcode des mit der Option postschedulecmd angegebenen Befehls hat keinen Einfluss auf den Rückkehrcode, der dem Server nach Beendigung des geplanten Ereignisses gemeldet wird. Wenn die Ergebnisse der postschedulecmd-Operationen Einfluss auf den Rückkehrcode des geplanten Ereignisses nehmen sollen, fügen Sie die postschedulecmd-Operationen in das Befehlsscript der geplanten Aktion ein und verwenden Sie nicht die Option postschedulecmd.

- Wenn die Scheduleraktion nicht gestartet werden kann und der mit der Option preschedulecmd angegebene Befehl mit dem Rückkehrcode 0 (null) beendet wird, wird der mit der Option postschedulecmd angegebene Befehl ausgeführt.
- Der Rückkehrcode von einer mit der Option postnschedulecmd angegebenen Operation wird nicht protokolliert und hat keinen Einfluss auf den Rückkehrcode des geplanten Ereignisses.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Scheduler im Textfeld Befehl für Zeitplan im Profileditor definieren. Diese Optionen können auch auf dem Server definiert werden.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Scheduler im Textfeld Befehl für Zeitplan im Profileditor definieren. Diese Optionen können auch auf dem Server definiert werden.

Syntax

```
>>-+-POSTSChedulecmd--+-- --Befehlszeichenfolge----------------><
   '-POSTNSChedulecmd-'
```

Parameter

Befehlszeichenfolge
: Gibt den zu verarbeitenden Befehl an. Mit dieser Option kann ein Befehl eingegeben werden, der nach einem Zeitplan ausgeführt werden soll. Es darf nur eine Option postschedulecmd verwendet werden.

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Haben Sie innerhalb der Befehlszeichenfolge Anführungszeichen verwendet, müssen Sie die gesamte Befehlszeichenfolge in Hochkommas einschließen.

  Windows-BetriebssystemeGeben Sie die Befehlszeichenfolge genau so an, wie Sie sie an der Eingabeaufforderung des Betriebssystems eingeben würden. Wenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Hochkommas eingeschlossen werden. Zum Beispiel:

  ```
  'net stop someservice'
  ```

  Eine Leer- oder Nullzeichenfolge für *Befehlszeichenfolge* angeben, wenn die Ausführung aller Befehle verhindert werden soll, die der IBM Spectrum Protect-Serveradministrator für postschedulecmd oder preschedulecmd verwendet. Wird eine Leer- oder Nullzeichenfolge in einer der beiden Optionen angegeben, kann der Administrator in beiden Optionen keinen Befehl verwenden.

  Gibt der Administrator eine Leer- oder Nullzeichenfolge in der Option postschedulecmd an, kann der Benutzer keinen Befehl nach einem Zeitplan ausführen.

  Mac OS X-BetriebssystemeFür Mac OS X: Wenn der Zeitplanbefehl postschedulecmd ein AppleScript ist, müssen Sie den Befehl osascript zum Ausführen des Scripts verwenden. Beispiel: Ist "Database Script" ein AppleScript, geben Sie den folgenden Befehl ein:

```
postschedulecmd osascript "/Volumes/La Pomme/Scripting/
  Database Script"
```

Beispiele

Mac OS X-BetriebssystemeOptionsdatei:

Mac OS X-BetriebssystemeFür Mac OS X: `postschedulecmd "/Volumes/La Pomme/Scripting/postsched.sh"`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeOptionsdatei:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme`postschedulecmd "restart database"`

Die Befehlszeichenfolge ist ein gültiger Befehl zum Neustart der Datenbank.

Windows-BetriebssystemeOptionsdatei:

Windows-Betriebssysteme

```
posts startdb.cmd
posts 'rename c:\myapp\logfile.log logfile.new'
posts 'net start "simple service"'
posts 'rename "c:\myapp\log file.log" "log file.new"'
posts '"C:\Programme\MyTools\runreport.bat"
  log1.in log2.in'
```

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssysteme`-postschedulecmd="/Volumes/La Pomme/Scripting/postsched.sh"`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme Befehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme`-postschedulecmd="'restart database'"`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Konzepte:
Clientrückkehrcodes
Zugehörige Verweise:
Befehl DEFINE SCHEDULE
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Postsnapshotcmd

Mit der Option postsnapshotcmd können Sie Shellbefehle oder Scripts des Betriebssystems ausführen, nachdem der Client für Sichern/Archivieren während einer Sicherungsoperation auf Momentaufnahmebasis eine Momentaufnahme gestartet hat.

Windows-BetriebssystemeDiese Option kann in Verbindung mit der Option presnapshotcmd verwendet werden, um Ihnen die Möglichkeit zu geben, eine Anwendung in den Wartemodus zu versetzen, während eine Momentaufnahme erstellt wird, und anschließend diese Anwendung erneut zu starten, nachdem die Momentaufnahme gestartet worden ist. Diese Option ist nur gültig, wenn die OFS- oder Online-Imagesicherung konfiguriert wurde.

AIX-BetriebssystemeNur für AIX: Diese Option ist nur für JFS2-Dateisicherung oder -archivierung auf Momentaufnahmebasis und für Imagesicherung auf Momentaufnahmebasis gültig. Verwenden Sie diese Option bei Dateisicherungen oder -archivierungen auf Momentaufnahmebasis im Befehl backup, mit der Option include.fs oder in der Datei dsm.sys.

Linux-BetriebssystemeNur für Linux: Diese Option ist nur gültig, wenn der LVM auf Ihrem System installiert und so konfiguriert ist, dass Sie eine Imagesicherungsoperation auf Momentaufnahmebasis ausführen können.

AIX-Betriebssysteme Linux-BetriebssystemeNur für AIX und Linux: Verwenden Sie diese Option für eine Imagesicherung auf Momentaufnahmebasis im Befehl backup image, mit der Option include.image oder in der Datei dsm.sys.

Windows-BetriebssystemeVerwenden Sie diese Option für eine Online-Imagesicherung im Befehl backup image, mit der Option include.image oder in der Datei dsm.opt.

Windows-BetriebssystemeFür OFS-Operationen verwenden Sie die Option postsnapshotcmd in einer Anweisung include.fs oder in Ihrer Clientoptionsdatei (dsm.opt).

Wenn postsnapshotcmd fehlschlägt, wird die Operation fortgesetzt. Es werden jedoch entsprechende Warnungen protokolliert.

Windows-BetriebssystemeAchtung: Wenn der Befehl, den Sie in der Anweisung presnapshotcmd oder postsnapshotcmd angeben, während Imagesicherungs- oder Momentaufnahmedifferenzsicherungsoperationen einen asynchronen Prozess startet, ist es möglich, dass der Befehl bei Beendigung der Sicherungsoperation noch nicht beendet ist. Wenn der Befehl vor Beendigung der Sicherung nicht beendet wird, könnten temporäre Dateien gesperrt werden, was ihre Löschung verhindert. Ein Datenbankereignis tritt auf und die folgende Nachricht wird in der Datei dsmerror.log aufgezeichnet:

```
ANS0361I DIAG: ..\..\common\db\cacheobj.cpp( 777): dbDelete():
 remove('C:\adsm.sys\SystemExcludeCache__24400820.TsmCacheDB'):
  errno 13: "Permission denied".
```

Die in der Nachricht angegebene Datei (cacheobj.cpp) kann nach Beendigung des Befehls, der durch die Option presnapshotcmd oder postsnapshotcmd gestartet wurde, manuell gelöscht werden.

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeDiese Option ist nur für AIX-Clients und Linux x86_64-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch auf der Registerkarte Momentaufnahmeimage des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auch auf der Registerkarte Momentaufnahmeimage des Profileditors definieren.

Syntax

```
>>---POSTSNAPshotcmd---- --"Befehlszeichenfolge"--------------><
```

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme"Befehlszeichenfolge"
AIX-BetriebssystemeLinux-BetriebssystemeGibt einen Befehl an, der verarbeitet werden soll.

Verwenden Sie die Option srvprepostsnapdisabled, um zu verhindern, dass der IBM Spectrum Protect-Serveradministrator Betriebssystembefehle auf dem Clientsystem ausführt.

Wenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden:

```
"resume database myDb"
```

Haben Sie innerhalb der Befehlszeichenfolge Anführungszeichen verwendet, müssen Sie die gesamte Befehlszeichenfolge in Hochkommas einschließen:

```
'resume database "myDb"'
```

Windows-Betriebssysteme"Befehlszeichenfolge"
Windows-BetriebssystemeGibt den zu verarbeitenden Befehl für die Versetzung in den Wartemodus an.

Geben Sie eine Leer- oder Nullzeichenfolge für Befehlszeichenfolge an, wenn die Ausführung aller Befehle verhindert werden soll, die der Administrator für postsnapshotcmd verwendet. Wird eine Leer- oder Nullzeichenfolge angegeben, wird verhindert, dass der Administrator einen Befehl für diese Option verwendet. Gibt Ihr Administrator eine Leer- oder Nullzeichenfolge in der Option postsnapshotcmd an, können Sie keinen Befehl nach der Momentaufnahme ausführen.

Verwenden Sie die Option srvprepostsnapdisabled, um zu verhindern, dass der IBM Spectrum Protect-Serveradministrator Betriebssystembefehle auf dem Clientsystem ausführt.

Wenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden:

```
"resume database myDb"
```

Haben Sie innerhalb der Befehlszeichenfolge Anführungszeichen verwendet, müssen Sie die gesamte Befehlszeichenfolge in Hochkommas einschließen:

```
'resume database "myDb"'
```

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOptionsdatei:
AIX-BetriebssystemeLinux-Betriebssystemepostsnapshotcmd "beliebiger Befehl"

Die Befehlszeichenfolge ist ein gültiger Befehl zum Neustart der Anwendung.

Windows-BetriebssystemeOptionsdatei:

Windows-Betriebssysteme`postsnapshotcmd "restart application"`

Die Befehlszeichenfolge ist ein gültiger Befehl zum Neustart der Anwendung.

AIX-Betriebssysteme Linux-BetriebssystemeBefehlszeile:
AIX-Betriebssysteme Linux-Betriebssysteme`backup image -postsnapshotcmd="beliebiger Befehl"`
Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme`backup image -postsnapshotcmd="restart application"`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Preschedulecmd/Prenschedulecmd

Mit der Option preschedulecmd wird ein Befehl angegeben, den das Clientprogramm vor der Ausführung eines Zeitplans verarbeitet.

Das Clientprogramm wartet auf die Beendigung des Befehls, bevor der Zeitplan gestartet wird. Soll nicht gewartet werden, muss prenschedulecmd angegeben werden.

Anmerkung:

1. Die erfolgreiche Beendigung des Befehls preschedulecmd wird als Voraussetzung für das Ausführen der geplanten Operation angesehen. Wenn der Befehl preschedulecmd nicht mit dem Rückkehrcode 0 beendet wird, werden die geplante Operation und die Befehle postschedulecmd und postnschedulecmd nicht ausgeführt. Der Client meldet, dass das geplante Ereignis fehlgeschlagen ist und der Rückkehrcode 12 lautet. Wenn Sie nicht wollen, dass der Befehl preschedulecmd von dieser Regel gesteuert wird, können Sie eine Script- oder Stapeldatei erstellen, die den Befehl aufruft und mit dem Rückkehrcode 0 beendet wird. Dann müssen Sie preschedulecmd so konfigurieren, dass die Script- oder Stapeldatei aufgerufen wird. Der Rückkehrcode für den Befehl prenschedulecmd wird nicht protokolliert und hat keinen Einfluss auf den Rückkehrcode des geplanten Ereignisses.
2. Die Option preschedulecmd kann (wie die Option prenschedulecmd) auch auf dem Server definiert werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Scheduler im Dialogfeld Befehl für Zeitplan im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Scheduler im Dialogfeld Befehl für Zeitplan im Profileditor definieren.

Syntax

```
>>-+-PRESChedulecmd--+-- --Befehlszeichenfolge----------------><
   '-PRENSChedulecmd-'
```

Parameter

Befehlszeichenfolge
Gibt den zu verarbeitenden Befehl an. Nur eine Option preschedulecmd verwenden. Mit dieser Option kann ein Befehl eingegeben werden, der vor einem Zeitplan ausgeführt werden soll.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Haben Sie innerhalb der Befehlszeichenfolge Anführungszeichen verwendet, müssen Sie die gesamte Befehlszeichenfolge in Hochkommas einschließen.

Windows-BetriebssystemeGeben Sie die Befehlszeichenfolge genau so an, wie Sie sie an der Eingabeaufforderung des Betriebssystems eingeben würden. Wenn für die angegebene Zeichenfolge Anführungszeichen erforderlich wären, damit sie an einer Windows-Eingabeaufforderung ausgeführt werden kann, fügen Sie die Anführungszeichen nach Bedarf ein. Wenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Hochkommas eingeschlossen werden.

Windows-BetriebssystemeIn dem folgenden Beispiel sind Hochkommas erforderlich, weil der Befehl Leerzeichen enthält:

```
'net stop someservice'
```

Windows-BetriebssystemeIn dem folgenden Beispiel sind Anführungszeichen erforderlich, weil sowohl der Name der umzubenennenden Datei als auch der neue Dateiname Leerzeichen enthält. Da auch die Befehlszeichenfolge Leerzeichen enthält, muss

die gesamte Zeichenfolge in Hochkommas eingeschlossen werden.

```
presc 'rename "c:\myapp\log file.log" "log file.old"'
```

Geben Sie eine Leer- oder Nullzeichenfolge für Befehlszeichenfolge an, wenn die Ausführung aller Befehle verhindert werden soll, die der IBM Spectrum Protect-Serveradministrator für postschedulecmd und preschedulecmd verwendet. Wird eine Leer- oder Nullzeichenfolge in einer der beiden Optionen angegeben, kann der Administrator in beiden Optionen keinen Befehl verwenden.

Gibt der Administrator eine Leer- oder Nullzeichenfolge in der Option preschedulecmd an, kann der Benutzer keinen Befehl vor einem Zeitplan ausführen.

 Für Mac OS X: Wenn der Zeitplanbefehl preschedulecmd ein AppleScript ist, müssen Sie den Befehl osascript zum Ausführen des Scripts verwenden. Beispiel: Ist "Database Script" ein AppleScript, geben Sie den folgenden Befehl ein:

```
preschedulecmd osascript "/Volumes/La Pomme/Scripting/
  Database Script"
```

Beispiele

Optionsdatei:




```
preschedulecmd "<Befehl zum Versetzen Ihres Datenbankprodukts in den Wartemodus>
Datenbank"
```




 Die Befehlszeichenfolge ist ein gültiger Befehl zum Versetzen der Datenbank in den Wartemodus.

```
presc stopdb.cmd
presc 'rename c:\myapp\logfile.log logfile.old'
presc 'net stop "simple service"'
presc 'rename "c:\myapp\log file.log" "log file.old"'
presc '"C:\Program Files\MyTools\runreport.bat"
   log1.in log2.in'
```




 Befehlszeile:




 -preschedulecmd="'quiesce database'"

 Befehlszeile:

 -preschedulecmd='"quiesce database"'

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Konzepte:
Clientrückkehrcodes

Preservelastaccessdate

Mit der Option preservelastaccessdate können Sie angeben, ob eine Sicherungs- oder Archivierungsoperation die letzte Zugriffszeit ändert.

Eine Sicherungs- oder Archivierungsoperation kann die letzte Zugriffszeit einer Datei ändern. Nach einer Operation kann der Client für Sichern/Archivieren die letzte Zugriffszeit auf den Wert vor der Operation zurücksetzen. Die letzte Zugriffszeit wird vom Client für Sichern/Archivieren nicht geändert, sondern kann beibehalten werden. Das Zurücksetzen der letzten Zugriffszeit erfordert zusätzliche Verarbeitung für jede gesicherte oder archivierte Datei.

Wenn Sie die Unterstützung offener Dateien aktivieren, wird das Datum des letzten Zugriffs auf Dateien immer beibehalten, unabhängig von der Einstellung für preservelastaccessdate. Wenn die Unterstützung offener Dateien aktiviert ist, verwenden Sie die Option preservelastaccessdate nicht.

Verwenden Sie diese Option in den Befehlen incremental, selective oder archive.

Anmerkung:

1. Diese Option gilt nur für Dateien, nicht für Verzeichnisse.
2. 


 Das Zurücksetzen des Datums des letzten Zugriffs wirkt sich auf die Sicherungs- und Archivierungsleistung aus.
3. Das Zurücksetzen des Datums des letzten Zugriffs kann sich auf Anwendungen auswirken, die sich auf ein präzises Datum des letzten Zugriffs stützen, z. B. eine SRM-Anwendung (SRM = Storage Resource Management).
4. 
 Auf Dateisystemen, die nicht vom IBM Spectrum Protect for Space Management-Client verwaltet werden, oder wenn Benutzer ohne Rootberechtigung sichern oder archivieren, wird das Attribut ctime zurückgesetzt. Das Attribut für die Uhrzeit und das Datum der letzten Änderung (ctime) wird auf das Datum und die Uhrzeit der Sicherungs- oder Archivierungsoperation zurückgesetzt.

5. AIX-BetriebssystemeLinux-BetriebssystemeDie Option updatectime hat Vorrang vor der Option preservelastaccessdate. Wenn beide Optionen auf yes gesetzt sind, wird die Option preservelastaccessdate ignoriert.
6. AIX-BetriebssystemeLinux-BetriebssystemeVerwenden Sie auf Dateisystemen, die nicht vom IBM Spectrum Protect for Space Management-Client verwaltet werden, nicht `preservelastaccessdate yes` und den GPFS-Befehl mmbackup. Mit dem Befehl mmbackup und mit `preservelastaccessdate yes` werden alle Dateien für jede Sicherungsoperation ausgewählt.
7. Windows-BetriebssystemeDas Datum des letzten Zugriffs kann bei Dateien, die durch das Attribut 'schreibgeschützt' oder durch eine restriktive NTFS-Sicherheitsberechtigung schreibgeschützt sind, nicht beibehalten werden.
8. Sie können das Datum des letzten Zugriffs von schreibgeschützten Dateien nicht zurücksetzen. Die Option preservelastaccessdate ignoriert schreibgeschützte Dateien und ändert deren Datum nicht.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

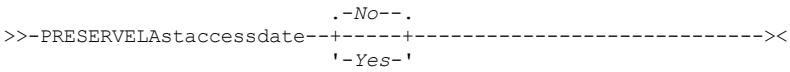
Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte 'Sichern' des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Sichern des Profileditors definieren.

Syntax



Parameter

No
: Eine Sicherungs- oder Archivierungsoperation kann das Datum des letzten Zugriffs ändern. Dies ist der Standardwert.

Yes
: Eine Sicherungs- oder Archivierungsoperation ändert das Datum des letzten Zugriffs nicht.

Beispiele

Optionsdatei:

```
preservelastaccessdate yes
```

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme`Incremental /proj/test/test_file -preservelastaccessdate=yes`

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`dsmc incr c: e: f: -preservelastaccessdate=yes`

Zugehörige Informationen:

AIX-BetriebssystemeLinux-Betriebssysteme Befehl 'mmbackup': IBM Spectrum Protect-Voraussetzungen

AIX-BetriebssystemeLinux-Betriebssysteme Anleitung für die Integration von IBM Spectrum Scale AFM mit IBM Spectrum Protect

AIX-BetriebssystemeLinux-Betriebssysteme Verwendung der Einschluss- und Ausschlussoptionen von IBM Spectrum Protect in Verbindung mit dem IBM Spectrum Scale-Befehl 'mmbackup'

Preservepath

Mit der Option preservepath wird angegeben, wie viel vom Quellenpfad als Teil des Zielverzeichnispfades wiederherzustellen ist, wenn Dateien an eine neue Position zurückgeschrieben oder abgerufen werden.

Verwenden Sie die Option -subdir=yes, um die vollständige Unterverzeichnisstruktur des Quellenverzeichnisses (Verzeichnisse und Dateien unter dem Quellenverzeichnis der untersten Ebene) als zurückzuschreibende Quelle festzulegen. Ist ein erforderliches Zielverzeichnis nicht vorhanden, wird es erstellt. Hat eine Zieldatei denselben Namen wie eine Quellendatei, wird sie überschrieben. Verwenden Sie die Option -replace=prompt, damit der Client eine Bestätigung anfordert, bevor Dateien überschrieben werden.

Verwenden Sie die Option preservepath in den folgenden Befehlen:

- restore
- restore backupset
- restore group

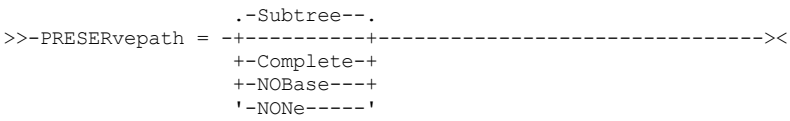
- retrieve

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Syntax



Parameter

Subtree
: Das Quellenverzeichnis der untersten Ebene wird als ein Unterverzeichnis des Zielverzeichnisses erstellt. Dateien aus dem Quellenverzeichnis werden in dem neuen Unterverzeichnis gespeichert. Dies ist der Standardwert.

Complete
: Der gesamte Pfad wird ab dem Stammverzeichnis in das angegebene Verzeichnis zurückgeschrieben. Der vollständige Pfad umfasst alle Verzeichnisse mit Ausnahme des Dateibereichsnamens.

NOBase
: Der Inhalt des Quellenverzeichnisses wird ohne das Verzeichnis der untersten Ebene (Basisverzeichnis) in das angegebene Zielverzeichnis zurückgeschrieben.

NONe
: Alle ausgewählten Quellendateien werden in das Zielverzeichnis zurückgeschrieben. Im Ziel werden keine Teile des Quellenpfades im oder oberhalb des Quellenverzeichnisses wiederhergestellt.

  Wenn Sie SUBDIR=yes angeben, schreibt der Client alle Dateien in den Quellenverzeichnissen in das einzelne Zielverzeichnis zurück.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBefehlszeile:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeVoraussetzung ist, dass der Serverdateibereich folgende Sicherungskopien enthält:

```
/fs/h1/m1/file.a
/fs/h1/m1/file.b
/fs/h1/m1/l1/file.x
/fs/h1/m1/l1/file.y
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser Befehl:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=complete
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/h1/m1/file.a
/u/ann/h1/m1/file.b
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser Befehl:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=nobase
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a
/u/ann/file.b
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser Befehl:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc res backupset /fs/h1/m1/ /u/ann/ -su=yes
-preser=nobase -loc=file
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a
/u/ann/file.b
/u/ann/file.x
/u/ann/file.y
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser Befehl:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=subtree
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/m1/file.a
/u/ann/m1/file.b
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser Befehl:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=none
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a
/u/ann/file.b
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser Befehl:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=complete
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/h1/m1/file.a
/u/ann/h1/m1/file.b
/u/ann/h1/m1/l1/file.x
/u/ann/h1/m1/l1/file.y
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser Befehl:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=nobase
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a
/u/ann/file.b
/u/ann/l1/file.x
/u/ann/l1/file.y
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser Befehl:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=subtree
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/m1/file.a
/u/ann/m1/file.b
/u/ann/m1/l1/file.x
/u/ann/m1/l1/file.y
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser Befehl:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=none
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
/u/ann/file.a
/u/ann/file.b
/u/ann/file.x
/u/ann/file.y
```

Windows-BetriebssystemeBefehlszeile:
Windows-BetriebssystemeVoraussetzung ist, dass der Serverdateibereich folgende Sicherungskopien enthält:

```
c:\h1\m1\file.a
c:\h1\m1\file.b
c:\h1\m1\l1\file.x
c:\h1\m1\l1\file.y
```

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssystemedsmc res backupset my.backupset.file /fs/h1/m1/ /u/ann/ -su=yes erstellt eine Datei eines lokalen Sicherungssatzes mit dem Namen "my.backupset.file".

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
c:\ann\h1\m1\file.a
c:\ann\h1\m1\file.b
```

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssystemedsmc res c:\h1\m1\ c:\ann\ -preser=nobase.

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
c:\ann\file.a
c:\ann\file.b
```

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssystemedsmc res c:\h1\m1\ c:\ann\ -preser=subtree.

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
c:\ann\m1\file.a
c:\ann\m1\file.b
```

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssystemedsmc res c:\h1\m1\ c:\ann\ -preser=none.

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
c:\ann\file.a
c:\ann\file.b
```

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssysteme

```
dsmc res c:\h1\m1\ c:\ann\ -su=yes -preser=
complete
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
c:\ann\h1\m1\file.a
c:\ann\h1\m1\file.b
c:\ann\h1\m1\l1\file.x
c:\ann\h1\m1\l1\file.y
```

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssystemedsmc res c:\h1\m1\ c:\ann\ -su=yes -preser=nobase.

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
c:\ann\file.a
c:\ann\file.b
c:\ann\l1\file.x
c:\ann\l1\file.y
```

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssystemedsmc res c:\h1\m1\ c:\ann\ -su=yes -preser=subtree.

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
c:\ann\m1\file.a
c:\ann\m1\file.b
c:\ann\m1\l1\file.x
c:\ann\m1\l1\file.y
```

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssystemedsmc res c:\h1\m1\ c:\ann\ -su=yes -preser=none.

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
c:\ann\file.a
c:\ann\file.b
c:\ann\file.x
c:\ann\file.y
```

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssysteme

```
dsmc res backupset c:\h1\m1\ c:\ann\ -su=yes
-preser=nobase -loc=file
```

Schreibt die folgenden Verzeichnisse und Dateien zurück:

```
c:\ann\file.a
c:\ann\file.b
```

```
c:\ann\file.x
c:\ann\file.y
```

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Presnapshotcmd

Mit der Option presnapshotcmd können Sie Betriebssystembefehle ausführen, bevor der Client für Sichern/Archivieren eine Momentaufnahme startet.

Dadurch sind Sie in der Lage, eine Anwendung in den Wartemodus zu versetzen, bevor der Client während einer Sicherung oder Archivierung auf Momentaufnahmebasis die Momentaufnahme startet.

Windows-BetriebssystemeDiese Option kann in Verbindung mit der Option postsnapshotcmd verwendet werden, um Ihnen die Möglichkeit zu geben, eine Anwendung in den Wartemodus zu versetzen, während eine Momentaufnahme erstellt wird, und anschließend diese Anwendung erneut zu starten, nachdem die Momentaufnahme gestartet worden ist. Diese Option ist nur gültig, wenn die OFS- oder Online-Imagesicherung konfiguriert wurde.

AIX-BetriebssystemeNur für AIX: Diese Option ist nur für JFS2-Dateisicherung oder -archivierung auf Momentaufnahmebasis und für Imagesicherung auf Momentaufnahmebasis gültig. Verwenden Sie diese Option bei Dateisicherungen oder -archivierungen auf Momentaufnahmebasis im Befehl backup, mit der Option include.fs oder in der Datei dsm.sys.

Linux-BetriebssystemeNur für Linux: Diese Option ist nur gültig, wenn der LVM auf Ihrem System installiert und so konfiguriert ist, dass Sie eine Imagesicherung auf Momentaufnahmebasis ausführen können.

AIX-BetriebssystemeLinux-BetriebssystemeNur für AIX und Linux: Verwenden Sie diese Option für eine Imagesicherung auf Momentaufnahmebasis im Befehl backup image, mit der Option include.image oder in der Datei dsm.sys.

Windows-BetriebssystemeVerwenden Sie diese Option für eine Online-Imagesicherung im Befehl backup image, mit der Option include.image oder in der Datei dsm.opt.

Windows-BetriebssystemeFür OFS-Operationen verwenden Sie die Option presnapshotcmd in einer Anweisung include.fs oder in Ihrer Clientoptionsdatei (dsm.opt).

Wenn presnapshotcmd fehlschlägt, wird angenommen, dass die Anwendung nicht in einem konsistenten Status ist, und der Client stoppt die Verarbeitung und zeigt die entsprechende Fehlernachricht an.

Windows-BetriebssystemeAchtung: Wenn der Befehl, den Sie in der Anweisung presnapshotcmd oder postsnapshotcmd angeben, während Imagesicherungs- oder Momentaufnahmedifferenzsicherungsoperationen einen asynchronen Prozess startet, ist es möglich, dass der Befehl bei Beendigung der Sicherungsoperation noch nicht beendet ist. Wenn der Befehl vor Beendigung der Sicherung nicht beendet wird, könnten temporäre Dateien gesperrt werden, was ihre Löschung verhindert. Ein Datenbankereignis tritt auf und die folgende Nachricht wird in der Datei dsmerror.log aufgezeichnet:

```
ANS0361I DIAG: ..\..\common\db\cacheobj.cpp( 777): dbDelete():
 remove('C:\adsm.sys\SystemExcludeCache__24400820.TsmCacheDB'):
  errno 13: "Permission denied".
```

Die in der Nachricht angegebene Datei (cacheobj.cpp) kann nach Beendigung des Befehls, der durch die Option presnapshotcmd oder postsnapshotcmd gestartet wurde, manuell gelöscht werden.

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeDiese Option ist nur für AIX JFS2- und Linux x86_64-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch auf der Registerkarte **Momentaufnahmeimage** des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auch auf der Registerkarte Momentaufnahmeimage des Profileditors definieren.

Syntax

```
>>---PRESNAPshotcmd---- --"Befehlszeichenfolge"---------------><
```

Parameter

AIX-Betriebssysteme Linux-Betriebssysteme"Befehlszeichenfolge"
AIX-Betriebssysteme Linux-BetriebssystemeGibt einen Befehl an, der verarbeitet werden soll.

Verwenden Sie die Option srvprepostsnapdisabled, um zu verhindern, dass der IBM Spectrum Protect-Serveradministrator Betriebssystembefehle auf dem Clientsystem ausführt.

Wenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden:

```
"quiesce database myDb"
```

Haben Sie innerhalb der Befehlszeichenfolge Anführungszeichen verwendet, müssen Sie die gesamte Befehlszeichenfolge in Hochkommas einschließen:

```
'resume database "myDb"'
```

Windows-Betriebssysteme"Befehlszeichenfolge"
Windows-BetriebssystemeGibt den zu verarbeitenden Befehl für die Versetzung in den Wartemodus an.

Geben Sie eine Leer- oder Nullzeichenfolge für Befehlszeichenfolge an, wenn die Ausführung aller Befehle verhindert werden soll, die der Administrator für presnapshotcmd verwendet. Wird eine Leer- oder Nullzeichenfolge angegeben, wird verhindert, dass der Administrator einen Befehl für diese Option verwendet. Gibt Ihr Administrator eine Leer- oder Nullzeichenfolge in der Option presnapshotcmd an, können Sie keinen Befehl vor der Momentaufnahme ausführen.

Verwenden Sie die Option srvprepostsnapdisabled, um zu verhindern, dass der IBM Spectrum Protect-Serveradministrator Betriebssystembefehle auf dem Clientsystem ausführt.

Wenn die Befehlszeichenfolge Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden:

```
"quiesce database myDb"
```

Haben Sie innerhalb der Befehlszeichenfolge Anführungszeichen verwendet, müssen Sie die gesamte Befehlszeichenfolge in Hochkommas einschließen:

```
'resume database "myDb"'
```

Beispiele

AIX-Betriebssysteme Linux-BetriebssystemeOptionsdatei:
AIX-Betriebssysteme Linux-Betriebssysteme

```
presnapshotcmd "beliebiger Shellbefehl oder beliebiges Script"
```

Windows-BetriebssystemeOptionsdatei:
Windows-Betriebssysteme

```
presnapshotcmd "<hier den Inaktivierungsbefehl für Ihre Anwendung einfügen>
  Anwendung"
```

Die Befehlszeichenfolge ist ein gültiger Befehl zum Inaktivieren der Anwendung.

AIX-Betriebssysteme Linux-BetriebssystemeBefehlszeile:
AIX-Betriebssysteme Linux-Betriebssysteme

```
backup image -presnapshotcmd="beliebiger Shellbefehl oder beliebiges Script"
```

Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme

```
backup image -presnapshotcmd="<hier den Inaktivierungsbefehl für Ihre Anwendung
  einfügen> Anwendung"
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Queryschedperiod

Mit der Option queryschedperiod kann die Anzahl Stunden festgelegt werden, die der Client-Scheduler zwischen den Versuchen, den Server nach geplanter Arbeit abzufragen, warten soll.

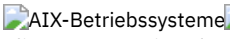
Diese Option ist nur gültig, wenn Sie die Option schedmode auf polling setzen. Diese Option wird nur verwendet, wenn der Scheduler aktiv ist.

Ihr Administrator kann diese Option auch definieren. Gibt Ihr Administrator einen Wert für diese Option an, überschreibt dieser den in Ihrer Clientoptionsdatei definierten Wert, nachdem Ihr Clientknoten erfolgreich den Kontakt zum Server hergestellt hat.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

 Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

 Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-QUERYSCHedperiod-- --Stunden--------------------------------><
```

Parameter

Stunden
: Gibt die Anzahl Stunden an, die der Client-Scheduler zwischen den Versuchen, geplante Arbeit auf dem Server abzufragen, wartet. Der Wertebereich ist 1 bis 9999; der Standardwert ist 4.

Beispiel

Optionsdatei:

```
querysch 6
```

Querysummary

Die Option querysummary stellt Statistikdaten zu Dateien, Verzeichnissen und Objekten bereit, die von den Befehlen query backup oder query archive zurückgegeben werden.

Die Option querysummary stellt die folgenden Statistikdaten bereit:

- Die Gesamtanzahl der Dateien und Verzeichnisse, die vom Befehl query backup oder query archive zurückgegeben werden.
- Das gesamte Datenvolumen der Objekte, die vom Befehl query backup oder query archive zurückgegeben werden.
- Den Schätzwert für den erforderlichen Speicher, wenn die vom Befehl query backup oder query archive zurückgegebenen Objekte mit einer klassischen Zurückschreibung zurückgeschrieben werden.
- Die Gesamtanzahl der eindeutigen Serverdatenträger, auf denen die Objekte gespeichert sind, die vom Befehl query zurückgegeben werden.

 Für einzelne Objekte, die mehrere Datenträger umspannen, wird nur ein Datenträger in die Statistikdaten für die Gesamtanzahl der Datenträger aufgenommen. Beispiel: Wenn `c:\bigfile` zwei Datenträger umspannt, wird nur einer der Datenträger bei der geschätzten Anzahl der Datenträger berücksichtigt.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

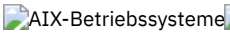
Syntax

```
>>-QUERYSUMMARY-------------------------------------------------><
```

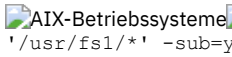
Parameter

Für diese Option gibt es keine Parameter.

Beispiele



Befehlszeile:

 `dsmc q ba '/usr/fs1/*' -sub=yes -querysummary`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
[root@kaveri:/home/cpark] $ dsmc q ba '/kalafs1/*' -sub=yes -querysummary
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
  Clientversion 8, Release 1, Stufe 0.0
  Clientdatum/-zeit: 09.12.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016. Alle Rechte vorbehalten.

Knotenname: KAVERI
Sitzung hergestellt mit Server TEMPLAR: AIX-RS/6000
  Serverversion 8, Release 1, Stufe 0.0
  Serverdatum/-zeit: 09.12.2016 12:05:35  Letzter Zugriff: 07.12.2016 07:48:59

      Größe       Sicher.-Datum             Verw.-Kl.            A/I Datei
      ----      -----------           ----------      --- ----
     4,096  B  08/07/08   12:07:30       BASVT2       A  /kalafs1/
       256  B  08/07/08   12:07:30       BASVT2       A  /kalafs1/dir1
10,485,760  B  08/07/08   12:07:30      DEFAULT       A  /kalafs1/info1
 5,242,880  B  08/07/08   12:07:30      DEFAULT       A  /kalafs1/info2
     1,044  B  08/07/08   12:07:30      DEFAULT       A  /kalafs1/dir1/subfile1
     1,044  B  08/07/08   12:07:30      DEFAULT       A  /kalafs1/dir1/subfile2


Übersichtsstatistik

Anz. Dat.     Anz. Verz.   Dsn. Dat.-Größe      Gesamtdaten     Gesch. Sp.
---------- ----------  -------------- ----------  ----------
         4           2     3.75 MB      15.00 MB     1.07 KB


Geschätzte Anzahl Datenträger: 2

[root@kaveri:/home/cpark] $
```

Windows-Betriebssysteme

Befehlszeile:

Windows-Betriebssystemedsmc query backup k:\.* -subdir=yes -QUERYSUMMARY

Windows-Betriebssysteme

```
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
  Clientversion 8, Release 1, Stufe 0.0
  Clientdatum/-zeit: 09.12.2016 12:05:35
(c) Copyright IBM Corporation und andere 1990, 2016. Alle Rechte vorbehalten.

Knotenname: BARKENSTEIN
Sitzung hergestellt mit Server BARKENSTEIN_SERVER1: Windows
  Serverversion 8, Release 1, Stufe 0.0
  Serverdatum/-zeit: 09.12.2016 12:05:35  Letzter Zugriff: 08.12.2016 05:46:09

Größe       Sicher.-Datum             Verw.-Kl.            A/I Datei
----        -----------               ----------            --- ----
0  B        04/02/2008 20:21:51       STANDARD             A  \\barkenstein\k$\
0  B        04/02/2008 20:21:51       STANDARD             A  \\barkenstein\k$\jack_test
0  B        04/01/2008 12:37:07       STANDARD             A  \\barkenstein\k$\
                                                              System Volume Information
0  B        04/01/2008 12:37:07       STANDARD             A  \\barkenstein\k$\Test1
0  B        04/02/2008 20:21:51       STANDARD             A  \\barkenstein\k$\TestTree
0  B        04/01/2008 12:37:07       STANDARD             A  \\barkenstein\k$\Tree150
0  B        04/02/2008 19:49:20       STANDARD             A  \\barkenstein\k$\Tree150.1
0  B        04/01/2008 12:37:07       STANDARD             A  \\barkenstein\k$\Tree150.2
0  B        04/02/2008 19:50:51       STANDARD             A  \\barkenstein\k$\Tree150.3
0  B        04/01/2008 12:37:07       STANDARD             A  \\barkenstein\k$\Tree1500
0  B        04/02/2008 10:41:40       STANDARD             A  \\barkenstein\k$\Tree150_2
0  B        04/02/2008 20:02:31       STANDARD             A  \\barkenstein\k$\tree18
0  B        04/02/2008 20:15:04       STANDARD             A  \\barkenstein\k$\Tree18.test
0  B        04/01/2008 12:37:07       STANDARD             A  \\barkenstein\k$\Tree30
0  B        04/01/2008 12:37:07       STANDARD             A  \\barkenstein\k$\Tree30.2
0  B        04/02/2008 19:52:30       STANDARD             A  \\barkenstein\k$\tree30.test
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file1
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file10
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file11
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file12
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file13
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file14
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file15
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file16
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file17
11,788  B   04/02/2008 19:55:32       DEFAULT              A  \\barkenstein\k$\file18
```

```
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file19
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file2
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file20
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file21
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file3
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file4
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file5
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file6
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file7
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file8
11,788  B   04/02/2008 19:55:32        DEFAULT             A  \\barkenstein\k$\file9
11,788  B   04/02/2008 13:31:06        DEFAULT             A  \\barkenstein\k$\file910
10,964  B   04/01/2008 12:37:07        DEFAULT             A  \\barkenstein\k$\filea
10,964  B   04/01/2008 12:37:07        DEFAULT             A  \\barkenstein\k$\fileb
10,964  B   04/01/2008 12:37:07        DEFAULT             A  \\barkenstein\k$\x


Übersichtsstatistik

 Anz. Dat.     Anz. Verz.   Dsn. Dat.-Größe      Gesamtdaten     Gesch. Sp.
 -----------   ----------   --------------      ----------      -----------
 25            16           11.41 KB            285.37 KB       10.58 KB

Geschätzte Anzahl Datenträger: 2
```

Quiet

Mit der Option quiet wird die Anzahl der Nachrichten, die während der Verarbeitung auf dem Bildschirm angezeigt werden, begrenzt.

Bei der Ausführung der Befehle incremental, selective oder archive können beispielsweise Informationen zu allen Dateien, die gesichert werden, angezeigt werden. Verwenden Sie die Option quiet, wenn diese Informationen nicht angezeigt werden sollen.

Wenn die Option quiet verwendet wird, werden Fehler- und Verarbeitungsdaten weiterhin angezeigt, und die Nachrichten werden in Protokolldateien geschrieben. Wird quiet nicht angegeben, wird die Standardoption verbose verwendet.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die Option quiet kann auch auf dem Server definiert werden; sie überschreibt dann die Clienteinstellung. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Befehlszeile über das Kontrollkästchen Keine Verarbeitungsdaten auf dem Bildschirm anzeigen im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Befehlszeile über das Kontrollkästchen Keine Verarbeitungsdaten auf dem Bildschirm anzeigen im Profileditor definieren.

Syntax

```
>>-QUIET-----------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Optionsdatei:

```
quiet
```

Befehlszeile:

```
-quiet
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Quotesareliteral

Die Option quotesareliteral gibt an, ob Hochkommas (') oder Anführungszeichen (") in der eigentlichen Bedeutung interpretiert werden, wenn sie in einer Dateilistenspezifikation in einer Option filelist angegeben werden.

Normalerweise müssen Sie im Client Dateispezifikationen, die Leerzeichen enthalten, mit Hochkommas oder Anführungszeichen begrenzen. In einigen Dateisystemen sind Hochkommas oder Anführungszeichen in Datei- und Verzeichnisnamen zulässig.

Um Fehler zu verhindern, die auftreten, wenn in einer Option filelist Dateispezifikationen angegeben werden, die Hochkommas (') oder Anführungszeichen (") enthalten, definieren Sie `quotesareliteral yes`. Wenn quotesareliteral auf yes gesetzt ist, werden Hochkommas und Anführungszeichen, die in einer Dateilistenspezifikation in einer Option filelist enthalten sind, in der eigentlichen Bedeutung als Hochkommas und Anführungszeichen und nicht als Begrenzungszeichen interpretiert.

Diese Option ist für jeden Befehl gültig, der eine Option filelist als Befehlsparameter akzeptiert.

Unterstützte Clients

Diese Option ist für alle unterstützten Plattformen gültig. Die Option wird auf jeden Befehl angewendet, der eine Dateilistenspezifikation als Parameter akzeptiert.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

```
                      .-no------.
>>-QUOTEsareliteral--+-+-----+-+------------------------------><
                      '-yes-'
```

Parameter

no
: Gibt an, dass Hochkommas (') und Anführungszeichen (") als Begrenzungszeichen für Dateilistenspezifikationen in einer Option filelist interpretiert werden. No ist die Standardeinstellung.

yes
: Gibt an, dass Hochkommas (') und Anführungszeichen (") in der eigentlichen Bedeutung und nicht als Begrenzungszeichen für Dateilistenspezifikationen in einer Option filelist interpretiert werden. Geben Sie diesen Wert an, wenn Sie Dateien aus einem Dateisystem sichern, in dem Anführungszeichen in Datei- oder Verzeichnisnamen zulässig sind.

Beispiele

Optionsdatei:

```
QUOTESARELITERAL YES
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeBei den folgenden Beispielen wird vorausgesetzt, dass das Dateisystem Hochkommas und Anführungszeichen in Pfadangaben zulässt. Die Beispiele zeigen Dateien in einer Dateilistenspezifikation, die erfolgreich verarbeitet werden können, wenn QUOTESARELITERAL auf YES gesetzt wird.

Windows-BetriebssystemeDer ausgegebene Befehl ist `dsmc sel -filelist=c:\important_files.txt`, wobei important_files.txt die Liste der zu verarbeitenden Dateien enthält.

Windows-Betriebssystemeimportant_files.txt enthält die folgende Dateiliste:

```
c:\home\myfiles\"file"1000
c:\home\myfiles\'file'
c:\home\myfiles\file'ABC
c:\home\myfiles\ABC"file"
```

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeBei den folgenden Beispielen wird vorausgesetzt, dass das Dateisystem Hochkommas und Anführungszeichen in Pfadangaben zulässt. Die Beispiele zeigen Dateien in einer Dateilistenspezifikation, die erfolgreich verarbeitet werden können, wenn QUOTESARELITERAL auf YES gesetzt wird.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeDer ausgegebene Befehl ist `dsmc sel -filelist=/home/user1/important_files`, wobei important_files die Liste der zu verarbeitenden Dateien enthält.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme

```
/home/user1/myfiles/"file"1000
/home/user1/myfiles/'file'
/home/user1/myfiles/file'ABC
/home/user1/myfiles/ABC"file"
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

Removeoperandlimit

Die Option removeoperandlimit gibt an, dass der Client die Beschränkung auf 20 Operanden entfernt.

Geben Sie die Option removeoperandlimit mit dem Befehl incremental, selective oder archive an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt.

Die Option removeoperandlimit kann nützlich sein, wenn Sie Scripts generieren, die den Befehlszeilenclient unter Umständen mit einer großen Anzahl Operanden aufrufen. So können Sie beispielsweise auf der Suche nach zu sichernden Dateien eine Verzeichnisbaumstruktur durchsuchen. Jede *in Frage kommende* Datei, die erkannt wird, wird zur Operandenliste des Befehls selective hinzugefügt. Später wird dieser Befehl selective von einem Steuerungsscript übergeben. In diesem Fall wird durch Angabe der Option removeoperandlimit die Beschränkung auf 20 Operanden entfernt.
Anmerkung:

1. Die Option removeoperandlimit *muss* unmittelbar nach den Befehlen incremental, selective oder archive vor allen Dateispezifikationen angegeben werden.
2. Diese Option akzeptiert keinen Wert. Wird diese Option in einem Befehl angegeben, wird die Beschränkung auf 20 Operanden entfernt.
3. Da die Erlaubnis der Shell zum Erweitern von Platzhalterzeichen die Leistung nachteilig beeinflusst, sollten Sie die Option removeoperandlimit in Sicherungs- oder Archivierungsoperationen einsetzen, in denen keine Platzhalterzeichen verwendet werden.
4. Die Option removeoperandlimit ist nur in den Befehlen incremental, selective oder archive im Stapelmodus gültig. In der Clientoptionsdatei (dsm.opt) oder Datei dsm.sys ist sie nicht gültig.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Syntax

```
>>-REMOVEOPerandlimit-----------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

```
-removeoperandlimit
```

Replace

Die Option replace gibt an, ob vorhandene Dateien auf Ihrer Workstation überschrieben werden sollen oder ob Sie zur Eingabe Ihrer Auswahl aufgefordert werden sollen, wenn Sie Dateien zurückschreiben oder abrufen.

Wichtig: Die Option replace hat keinen Einfluss auf die Wiederherstellung von Verzeichnisobjekten. Verzeichnisobjekte werden immer wiederhergestellt, auch bei Angabe von replace=no. Sollen vorhandene Verzeichnisse nicht überschrieben werden, müssen Sie die Option filesonly verwenden.

Diese Option können Sie in folgenden Befehlen verwenden:

- restore
- restore backupset
- restore group
- retrieve

Anmerkung: Bei geplanten Operationen erfolgt keine Eingabeaufforderung für das Überschreiben. Wenn Sie die Option replace auf prompt setzen, überspringt der Client für Sichern/Archivieren bei einer geplanten Operation Dateien ohne Eingabeaufforderung.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Restore im Abschnitt Aktion für bereits vorhandene Dateien im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Restore im Abschnitt Aktion für bereits vorhandene Dateien im Profileditor definieren.

Syntax

```
            .-Prompt-.
>>-REPlace--+--------+-----------------------------------------><
            +-All----+
            +-Yes----+
            '-No-----'
```

Parameter

Prompt
: Bei nicht geplanten Operationen geben Sie an, ob vorhandene Dateien überschrieben werden sollen. Bei geplanten Operationen werden vorhandene Dateien nicht überschrieben und keine Bedienerführungen angezeigt. Dies ist der Standardwert.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAll
: AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle vorhandenen Dateien werden überschrieben, auch schreibgeschützte Dateien. Wird der Zugriff auf eine Datei verweigert, hat der Benutzer die Auswahl, die Datei zu überspringen oder zu überschreiben. Die Datei wird erst bearbeitet, wenn die Bedienerführung beantwortet wurde.

Windows-BetriebssystemeAll
: Windows-BetriebssystemeAlle vorhandenen Dateien werden überschrieben, auch schreibgeschützte Dateien. Alle gesperrten Dateien werden ersetzt, wenn das System erneut gestartet wird. Wird der Zugriff auf eine Datei verweigert, hat der Benutzer die Auswahl, die Datei zu überspringen oder zu überschreiben. Die Datei wird erst bearbeitet, wenn die Bedienerführung beantwortet wurde.

Yes
: *Mit Ausnahme* von schreibgeschützten Dateien werden alle vorhandenen Dateien überschrieben. Bei nicht geplanten Operationen geben Sie an, ob vorhandene schreibgeschützte Dateien überschrieben werden sollen. Bei geplanten Operationen werden vorhandene schreibgeschützte Dateien nicht überschrieben und keine Bedienerführungen angezeigt. Wird der Zugriff auf eine Datei verweigert, wird sie übersprungen.

Windows-BetriebssystemeNo
: Windows-BetriebssystemeVorhandene Dateien werden nicht überschrieben. Eingabeaufforderungen werden nicht angezeigt.

  Mac OS X-Betriebssysteme**Anmerkung:** Ist beim Zurückschreiben oder Abrufen von Dateien die Option replace auf no gesetzt, werden vorhandene Dateien nicht überschrieben, aber vorhandene Verzeichnisse werden überschrieben. Sollen vorhandene Verzeichnisse während einer Zurückschreibungs- oder Abrufoperation intakt bleiben, wählen Sie Optionen > Alle ausgewählten Dateien und Verzeichnisse > Nur Dateien in der GUI des Clients für Sichern/Archivieren aus.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeNo
: AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeVorhandene Dateien werden nicht überschrieben. Eingabeaufforderungen werden nicht angezeigt.

Windows-BetriebssystemeAnmerkung: Sie können auswählen, dass gesperrte Dateien ersetzt werden sollen, wenn das System erneut gestartet wird. Der Client kann keine Zurückschreibung aktiver Dateien am Platz ausführen. Zurückgeschriebene Versionen aktiver Dateien werden jedoch für die Ersetzung beim nächsten Warmstart zwischengespeichert. Ausgenommen sind hierbei Dateien mit benannten Datenströmen, Dateien mit freien Bereichen und Verzeichnisse. Diese Dateien können Sie nur zurückschreiben, wenn sie entsperrt sind.

Beispiele

Optionsdatei:
```
replace all
```
Befehlszeile:
```
-replace=no
```

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Replserverguid

Die Option replserverguid gibt die global eindeutige ID (GUID) an, die verwendet wird, wenn der Client während der Übernahme eine Verbindung zum Sekundärserver herstellt. Mit der GUID wird der Sekundärserver validiert, um sicherzustellen, dass es sich um den erwarteten Server handelt.

Die Replikations-GUID weicht von der Maschinen-GUID des Servers ab. Sie wird einmal für einen Server generiert, der die Replikation ausführt, und ändert sich nie.

Diese Option muss in einer Zeilengruppe replservername in der Clientoptionsdatei angegeben werden. Die Zeilengruppe replservername enthält Verbindungsinformationen des Sekundärservers.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDiese Option wird in der Datei dsm.sys in die Zeilengruppe replservername eingefügt.

Windows-BetriebssystemeDiese Option wird in die Clientoptionsdatei (dsm.opt) eingefügt.

Syntax

```
>>-replserverguid----Server-GUID------------------------------><
```

Parameter

Server-GUID
: Gibt die GUID des Sekundärservers an, der im Fall einer Übernahme verwendet wird.

Beispiele

Optionsdatei:

```
REPLSERVERGUID 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

Befehlszeile:

Nicht zutreffend.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeOptionsdatei:

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei dsm.sys angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Verbindungsinformationen für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option replservername und den Namen des Sekundärservers angegeben. Die Zeilengruppe servername muss die Option myreplicationserver enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe replservername angegeben wird. Nur ein Sekundärserver kann für jeweils eine Zeilengruppe servername angegeben werden.

```
REPLSERVERNAME    TargetReplicationServer1
  REPLTCPSERVERADDRESS TargetReplicationServer1
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

REPLSERVERNAME   TargetReplicationServer2
  REPLTCPSERVERADDRESS TargetReplicationServer2
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02

SErvername     server_a
      COMMMethod              TCPip
  TCPPort                  1500
      TCPServeraddress         server_hostname1.example.com
  PASSWORDAccess           prompt
  MYREPLICATIONServer      TargetReplicationServer1

SErvername     server_b
  COMMMethod               TCPip
  TCPPort                  1500
      TCPServeraddress         server_hostname2.example.com
```

```
    PASSWORDAccess            generate
        INCLExcl                  /adm/tsm/archive.excl
        MYREPLICATIONServer       TargetReplicationServer2

  SErvername     server_c
    COMMMethod                TCPip
    TCPPort                   1500
        TCPServeraddress          server_hostname3.example.com
    PASSWORDAccess            generate
    MYREPLICATIONServer       TargetReplicationServer1
```

 Windows-BetriebssystemeOptionsdatei:

 Windows-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für den Sekundärserver in der Datei dsm.opt angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Die Verbindungsinformationen für den Sekundärserver befinden sich in der Zeilengruppe REPLSERVERName. Die Option MYREPLICATIONServer verweist auf den Namen des Sekundärservers, der durch die Zeilengruppe REPLSERVERName angegeben wird.

```
REPLSERVERNAME    TargetReplicationServer1
    REPLTCPSERVERADDRESS TargetReplicationServer1
    REPLTCPPORT          1505
    REPLSSLPORT          1506
    REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

COMMMethod               TCPip
TCPPort                  1500
TCPServeraddress         server_hostname1.example.com
PASSWORDAccess           prompt
MYREPLICATIONServer      TargetReplicationServer1
MYPRIMARYSERVER          Server1
```

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Client für automatisierte Übernahme konfigurieren

Replservername

Die Option replservername gibt den Namen des Sekundärservers an, zu dem der Client während einer Übernahme eine Verbindung herstellt.

Die Option replservername beginnt eine Zeilengruppe in der Clientoptionsdatei, die Verbindungsinformationen zu dem Sekundärserver enthält.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDiese Option wird in die Clientsystemoptionsdatei (dsm.sys) eingefügt.

 Windows-BetriebssystemeDiese Option wird in die Clientoptionsdatei (dsm.opt) eingefügt.

Syntax

```
>>-replservername----Replikationsservername--------------------><
```

Parameter

Replikationsservername

Gibt den Namen des Sekundärservers an, der im Fall einer Übernahme verwendet werden soll. Dieser Wert ist in der Regel der Name des Sekundärservers, nicht der Hostname des Servers.

Beispiele

Optionsdatei:

```
REPLSERVERName TargetReplicationServer1
```

Befehlszeile:

Nicht zutreffend.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeOptionsdatei:

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei dsm.sys angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Verbindungsinformationen für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option replservername und den Namen des Sekundärservers angegeben. Die Zeilengruppe servername muss die Option myreplicationserver enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe replservername angegeben wird. Nur ein Sekundärserver kann für jeweils eine Zeilengruppe servername angegeben werden.

```
REPLSERVERNAME    TargetReplicationServer1
  REPLTCPSERVERADDRESS TargetReplicationServer1
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

REPLSERVERNAME   TargetReplicationServer2
  REPLTCPSERVERADDRESS TargetReplicationServer2
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02

SErvername     server_a
     COMMMethod              TCPip
  TCPPort                 1500
     TCPServeraddress        server_hostname1.example.com
  PASSWORDAccess          prompt
  MYREPLICATIONServer     TargetReplicationServer1

SErvername     server_b
  COMMMethod              TCPip
  TCPPort                 1500
     TCPServeraddress        server_hostname2.example.com
  PASSWORDAccess          generate
     INCLExcl                /adm/tsm/archive.excl
     MYREPLICATIONServer     TargetReplicationServer2

SErvername     server_c
  COMMMethod              TCPip
  TCPPort                 1500
     TCPServeraddress        server_hostname3.example.com
  PASSWORDAccess          generate
  MYREPLICATIONServer     TargetReplicationServer1
```

 Windows-BetriebssystemeOptionsdatei:

 Windows-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für den Sekundärserver in der Datei dsm.opt angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Die Verbindungsinformationen für den Sekundärserver befinden sich in der Zeilengruppe REPLSERVERName. Die Option MYREPLICATIONServer verweist auf den Namen des Sekundärservers, der durch die Zeilengruppe REPLSERVERName angegeben wird.

```
REPLSERVERNAME    TargetReplicationServer1
    REPLTCPSERVERADDRESS TargetReplicationServer1
    REPLTCPPORT          1505
    REPLSSLPORT          1506
    REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

COMMMethod               TCPip
TCPPort                  1500
TCPServeraddress         server_hostname1.example.com
PASSWORDAccess           prompt
MYREPLICATIONServer      TargetReplicationServer1
MYPRIMARYSERVER          Server1
```

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Client für automatisierte Übernahme konfigurieren

Replsslport

Die Option replsslport gibt den SSL-fähigen TCP/IP-Anschluss des Sekundärservers an. Die Option replsslport wird verwendet, wenn der Client während einer Übernahme eine Verbindung zum Sekundärserver herstellt. Diese Option wird nicht mehr unterstützt, wenn Sie die Verbindung zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen.

Der Primärserver sendet die Option replsslport nur dann an den Client, wenn der Sekundärserver für SSL konfiguriert ist.

Diese Option ist nur anwendbar, wenn der Client für die Verwendung von SSL für die sichere Kommunikation zwischen dem IBM Spectrum Protect-Server und -Client konfiguriert ist. Wenn der Client nicht für die Verwendung von SSL konfiguriert ist, wird der durch die Option repltcpport angegebene Anschluss verwendet. Wenn Sie feststellen wollen, ob der Client SSL verwendet, prüfen Sie die Clientoption SSL.

Diese Option muss in einer Zeilengruppe replservername in der Clientoptionsdatei angegeben werden. Die Zeilengruppe replservername enthält Verbindungsinformationen des Sekundärservers.

Während des normalen Anmeldeprozesses (ohne Übernahme) wird diese Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDiese Option wird in der Datei dsm.sys in die Zeilengruppe replservername eingefügt.

Windows-BetriebssystemeDiese Option wird in die Clientoptionsdatei (dsm.opt) eingefügt.

Syntax

```
>>-replsslport----Anschlussadresse----------------------------><
```

Parameter

Anschlussadresse
: Gibt die SSL-fähige TCP/IP-Anschlussadresse für die Datenübertragung mit dem Sekundärserver an.

Beispiele

Optionsdatei:

```
REPLSSLPORT 1506
```

Befehlszeile:

Nicht zutreffend.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeOptionsdatei:

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei dsm.sys angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Verbindungsinformationen für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option replservername und den Namen des Sekundärservers angegeben. Die Zeilengruppe servername muss die Option myreplicationserver enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe replservername angegeben wird. Nur ein Sekundärserver kann für jeweils eine Zeilengruppe servername angegeben werden.

```
REPLSERVERNAME    TargetReplicationServer1
  REPLTCPSERVERADDRESS TargetReplicationServer1
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

REPLSERVERNAME   TargetReplicationServer2
  REPLTCPSERVERADDRESS TargetReplicationServer2
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SErvername     server_a
      COMMMethod              TCPip
   TCPPort                 1500
      TCPServeraddress        server_hostname1.example.com
   PASSWORDAccess          prompt
   MYREPLICATIONServer     TargetReplicationServer1

SErvername     server_b
   COMMMethod              TCPip
   TCPPort                 1500
      TCPServeraddress        server_hostname2.example.com
   PASSWORDAccess          generate
      INCLExcl                /adm/tsm/archive.excl
      MYREPLICATIONServer     TargetReplicationServer2

SErvername     server_c
   COMMMethod              TCPip
   TCPPort                 1500
      TCPServeraddress        server_hostname3.example.com
   PASSWORDAccess          generate
   MYREPLICATIONServer     TargetReplicationServer1
```

Windows-BetriebssystemeOptionsdatei:

Windows-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für den Sekundärserver in der Datei dsm.opt angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Die Verbindungsinformationen für den Sekundärserver befinden sich in der Zeilengruppe REPLSERVERName. Die Option MYREPLICATIONServer verweist auf den Namen des Sekundärservers, der durch die Zeilengruppe REPLSERVERName angegeben wird.

```
REPLSERVERNAME    TargetReplicationServer1
    REPLTCPSERVERADDRESS TargetReplicationServer1
    REPLTCPPORT          1505
    REPLSSLPORT          1506
    REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

COMMMethod               TCPip
TCPPort                  1500
TCPServeraddress         server_hostname1.example.com
PASSWORDAccess           prompt
MYREPLICATIONServer      TargetReplicationServer1
MYPRIMARYSERVER          Server1
```

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Client für automatisierte Übernahme konfigurieren

Repltcpport

Die Option repltcpport gibt den TCP/IP-Anschluss des Sekundärservers an, der verwendet werden soll, wenn der Client während einer Übernahme eine Verbindung zum Sekundärserver herstellt.

Diese Option muss in einer Zeilengruppe replservername in der Clientoptionsdatei angegeben werden. Die Zeilengruppe replservername enthält Verbindungsinformationen des Sekundärservers.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDiese Option wird in der Datei dsm.sys in die Zeilengruppe replservername eingefügt.

Windows-BetriebssystemeDiese Option wird in die Clientoptionsdatei (dsm.opt) eingefügt.

Syntax

```
>>-repltcpport----Anschlussadresse-----------------------------><
```

Parameter

Anschlussadresse
Gibt die TCP/IP-Anschlussadresse für die Datenübertragung mit dem Sekundärserver an.

Beispiele

Optionsdatei:

```
REPLTCPPort 1500
```

Befehlszeile:
Nicht zutreffend.
AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeOptionsdatei:
AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei dsm.sys angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Verbindungsinformationen für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option replservername und den Namen des Sekundärservers angegeben. Die Zeilengruppe servername muss die Option myreplicationserver enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe replservername angegeben wird. Nur ein Sekundärserver kann für jeweils eine Zeilengruppe servername angegeben werden.

```
REPLSERVERNAME    TargetReplicationServer1
  REPLTCPSERVERADDRESS TargetReplicationServer1
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

REPLSERVERNAME   TargetReplicationServer2
  REPLTCPSERVERADDRESS TargetReplicationServer2
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02

SErvername     server_a
     COMMMethod              TCPip
  TCPPort                 1500
     TCPServeraddress        server_hostname1.example.com
  PASSWORDAccess          prompt
  MYREPLICATIONServer     TargetReplicationServer1

SErvername     server_b
  COMMMethod              TCPip
  TCPPort                 1500
     TCPServeraddress        server_hostname2.example.com
  PASSWORDAccess          generate
     INCLExcl                /adm/tsm/archive.excl
     MYREPLICATIONServer     TargetReplicationServer2

SErvername     server_c
  COMMMethod              TCPip
  TCPPort                 1500
     TCPServeraddress        server_hostname3.example.com
  PASSWORDAccess          generate
  MYREPLICATIONServer     TargetReplicationServer1
```

Windows-BetriebssystemeOptionsdatei:
Windows-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für den Sekundärserver in der Datei dsm.opt angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Die Verbindungsinformationen für den Sekundärserver befinden sich in der Zeilengruppe REPLSERVERName. Die Option MYREPLICATIONServer verweist auf den Namen des Sekundärservers, der durch die Zeilengruppe REPLSERVERName angegeben wird.

```
REPLSERVERNAME    TargetReplicationServer1
    REPLTCPSERVERADDRESS TargetReplicationServer1
    REPLTCPPORT          1505
    REPLSSLPORT          1506
    REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

COMMMethod               TCPip
TCPPort                  1500
TCPServeraddress         server_hostname1.example.com
PASSWORDAccess           prompt
MYREPLICATIONServer      TargetReplicationServer1
MYPRIMARYSERVER          Server1
```

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Client für automatisierte Übernahme konfigurieren

Repltcpserveraddress

Die Option repltcpserveraddress gibt die TCP/IP-Adresse des Sekundärservers an, die verwendet werden soll, wenn der Client während einer Übernahme eine Verbindung zum Sekundärserver herstellt.

Diese Option muss in einer Zeilengruppe replservername in der Clientoptionsdatei angegeben werden. Die Zeilengruppe replservername enthält Verbindungsinformationen des Sekundärservers.

Diese Option wird vom Administrator des IBM Spectrum Protect-Servers für den Clientknoten definiert. Während des normalen Anmeldeprozesses (ohne Übernahme) wird die Option an den Client gesendet und in der Clientoptionsdatei gespeichert.

Bearbeiten Sie diese Option nicht während des Normalbetriebs.

Bearbeiten Sie diese Option nur in Situationen wie den folgenden:

- Der Primärserver ist offline und die Informationen für den Sekundärserver befinden sich nicht in der Optionsdatei.
- Die Informationen des Sekundärservers sind nicht auf dem neuesten Stand oder falsch.

Alle von Ihnen bearbeiteten Werte werden bei Ihrer nächsten Anmeldung am Primärserver entfernt oder aktualisiert.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDiese Option wird in der Datei dsm.sys in die Zeilengruppe replservername eingefügt.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-REPLTCPServeraddress----Serveradresse----------------------><
```

Parameter

Serveradresse
: Gibt eine TCP/IP-Adresse für einen Server mit einer Länge von 1 - 64 Zeichen an. Geben Sie einen TCP/IP-Domänennamen oder eine numerische IP-Adresse an. Die numerische IP-Adresse kann entweder eine TCP/IP-V4- oder eine TCP/IP-V6-Adresse sein. Sie können IPv6-Adressen nur verwenden, wenn Sie die Option `commmethod V6Tcpip` angegeben haben.

Beispiele

Optionsdatei:
```
REPLTCPServeraddress dsmchost.example.com
```
Befehlszeile:
Nicht zutreffend.
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeOptionsdatei:
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für drei unterschiedliche Server in der Datei dsm.sys angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Verbindungsinformationen für mehrere Sekundärserver liegen in Zeilengruppen vor. Jede Zeilengruppe wird durch die Option replservername und den Namen des Sekundärservers angegeben. Die Zeilengruppe servername muss die Option myreplicationserver enthalten, die auf den Sekundärserver verweist, der durch die Zeilengruppe replservername angegeben wird. Nur ein Sekundärserver kann für jeweils eine Zeilengruppe servername angegeben werden.

```
REPLSERVERNAME    TargetReplicationServer1
  REPLTCPSERVERADDRESS TargetReplicationServer1
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

REPLSERVERNAME   TargetReplicationServer2
  REPLTCPSERVERADDRESS TargetReplicationServer2
```

```
  REPLTCPPORT          1505
  REPLSSLPORT          1506
  REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02

SErvername     server_a
     COMMMethod              TCPip
  TCPPort                 1500
     TCPServeraddress        server_hostname1.example.com
  PASSWORDAccess          prompt
  MYREPLICATIONServer     TargetReplicationServer1

SErvername     server_b
  COMMMethod              TCPip
  TCPPort                 1500
     TCPServeraddress        server_hostname2.example.com
  PASSWORDAccess          generate
     INCLExcl                /adm/tsm/archive.excl
     MYREPLICATIONServer     TargetReplicationServer2

SErvername     server_c
  COMMMethod              TCPip
  TCPPort                 1500
     TCPServeraddress        server_hostname3.example.com
  PASSWORDAccess          generate
  MYREPLICATIONServer     TargetReplicationServer1
```

Windows-BetriebssystemeOptionsdatei:

Windows-BetriebssystemeDas folgende Beispiel zeigt, wie Optionen für den Sekundärserver in der Datei dsm.opt angegeben werden und wie ein Verweis auf den Sekundärserver aussieht. Die Verbindungsinformationen für den Sekundärserver befinden sich in der Zeilengruppe REPLSERVERName. Die Option MYREPLICATIONServer verweist auf den Namen des Sekundärservers, der durch die Zeilengruppe REPLSERVERName angegeben wird.

```
REPLSERVERNAME    TargetReplicationServer1
    REPLTCPSERVERADDRESS TargetReplicationServer1
    REPLTCPPORT          1505
    REPLSSLPORT          1506
    REPLSERVERGUID       91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

COMMMethod               TCPip
TCPPort                  1500
TCPServeraddress         server_hostname1.example.com
PASSWORDAccess           prompt
MYREPLICATIONServer      TargetReplicationServer1
MYPRIMARYSERVER          Server1
```

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Client für automatisierte Übernahme konfigurieren
Windows-Betriebssysteme

Resetarchiveattribute

Verwenden Sie die Option resetarchiveattribute, um anzugeben, ob der Client für Sichern/Archivieren das Windows-Archivierungsattribut für Dateien zurücksetzt, die erfolgreich auf dem IBM Spectrum Protect-Server gesichert wurden.

Der Client setzt das Archivierungsattribut auch bei Teilsicherungen zurück, wenn festgestellt wird, dass bereits ein aktives Objekt auf dem Server vorhanden ist. Die Option resetarchiveattribute ist in Verbindung mit Anwendungen wie IBM Spectrum Control nützlich, um auf einfache Weise den Sicherungsstatus von Dateien zurückzumelden.

Das Windows-Archivierungsattribut gibt an, dass sich eine Datei seit der letzten Sicherung geändert hat. Nachdem der Client das Archivierungsattribut zurückgesetzt hat, setzt das Windows-Betriebssystem das Attribut wieder auf ON, nachdem die Datei geändert wurde. Der Client verwendet nicht das Windows-Archivierungsattribut, um festzustellen, ob eine Datei ein Kandidat für die Teilsicherung ist. Dieses Attribut wird nur zu Meldezwecken bearbeitet. Der Client verwendet eine wesentlich ausgereiftere Methode, um zu bestimmen, ob eine Datei ein Kandidat für die Teilsicherung ist.

Es gibt verschiedene Anwendungen, die das Windows-Archivierungsattribut bearbeiten oder untersuchen. Beachten Sie die Konsequenzen bei der Verwendung der Option resetarchiveattribute in Verbindung mit diesen Produkten.

Wenn Sie die Option resetarchiveattribute auf yes setzen, setzt der Client das Windows-Archivierungsattribut auf dem lokalen Dateisystem zurück, wenn eine Datei erfolgreich auf dem IBM Spectrum Protect-Server gesichert wurde:

- Das Windows-Archivierungsattribut wird nach Teilsicherungen und selektiven Sicherungen zurückgesetzt, nachdem die Datei erfolgreich auf der IBM Spectrum Protect-Serverdatenbank festgeschrieben wurde. Dieses Attribut wird nicht für Archivierungs- oder Imageoperationen zurückgesetzt.
- Das Windows-Archivierungsattribut wird nicht bei der Verarbeitung von Systemobjekten oder Systemstatusobjekten zurückgesetzt.

- Das Windows-Archivierungsattribut wird nicht für Verzeichniseinträge zurückgesetzt.

Damit das lokale Dateisystem den aktuellen aktiven Objektbestand auf dem IBM Spectrum Protect-Server widerspiegelt, weist die Option resetarchiveattribute den Client ferner an, das Windows-Archivierungsattribut im lokalen Dateisystem zurückzusetzen, wenn bei der Teilsicherung festgestellt wird, dass bereits eine gültige, aktive Sicherungskopie der Datei auf dem Server vorhanden ist. Dieses Verhalten wird in den folgenden Fällen nicht gezeigt:

- Bei Teilsicherungsoperationen, bei denen die gespeicherten Clientattribute auf dem Server nicht untersucht werden, wie beispielsweise journalbasierte Sicherungsverarbeitung oder Teilsicherung nach Datum.
- Bei Dateien, die während einer Teilsicherungsoperation nicht untersucht werden, da sie von der Sicherungsverarbeitung ausgeschlossen sind.

Der Client garantiert nicht die Richtigkeit der aktuellen Einstellung des Windows-Archivierungsattributs. Beispiel: Ist die Option resetarchiveattribute auf yes gesetzt und gibt eine von einem Berichtsprodukt untersuchte Datei an, dass das Windows-Archivierungsattribut für eine bestimmte Datei auf OFF gesetzt ist, bedeutet dies nicht notwendigerweise, dass eine gültige aktive Sicherungskopie der Datei auf dem IBM Spectrum Protect-Server vorhanden ist. Zu den Faktoren, die zu dieser Situation beitragen können, gehören:

- Ein Produkt eines unabhängigen Softwareanbieters bearbeitet das Windows-Archivierungsattribut.
- Ein Dateibereich wurde auf dem Server gelöscht.
- Ein Sicherungsband ist verloren gegangen oder wurde zerstört.

Es sollte zu keiner wesentlichen Leistungsverschlechterung kommen, wenn die Option resetarchiveattribute verwendet wird. Die Option resetarchiveattribute hat keine Auswirkungen auf die Zurückschreibungsverarbeitung.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) oder der Clientoptionsgruppe des Servers gültig. Sie können diese Option auf der Registerkarte Sichern des Profileditors definieren.

Syntax

```
                          .-No--.
>>-RESETARCHIVEATTRibute = -+-----+----------------------------><
                          '-Yes-'
```

Parameter

Yes
: Gibt an, dass das Windows-Archivierungsattribut für Dateien während einer Sicherungsoperation zurückgesetzt werden soll.

No
: Gibt an, dass das Windows-Archivierungsattribut für Dateien während einer Sicherungsoperation nicht zurückgesetzt werden soll. Dies ist der Standardwert.

Beispiele

Optionsdatei:

```
resetarchiveattribute yes
```

Resourceutilization

Mit der Option resourceutilization in Ihrer Optionsdatei können Sie den Umfang der Ressourcen steuern, die der IBM Spectrum Protect-Server und -Client während der Verarbeitung verwenden können.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Allgemein im Feld Ressourcenauslastung des Profileditors definieren.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Allgemein im Feld Ressourcenauslastung des Profileditors definieren.

Syntax

```
>>-RESOURceutilization-- --Nummer------------------------------><
```

Parameter

Zahl
: Gibt den Umfang der Ressourcen an, die der IBM Spectrum Protect-Server und -Client während der Verarbeitung verwenden können. Der Wertebereich, der angegeben werden kann, ist 1 bis 100. Der Standardwert ist 2.

Beispiele

Optionsdatei:
```
resourceutilization 7
```

Befehlszeile:
```
-resourceutilization=7
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

- Sicherungs- und Archivierungssitzungen steuern
  Wenn Sie eine Sicherung oder Archivierung anfordern, kann der Client mehrere Sitzungen mit dem Server verwenden.
- Zurückschreibungssitzungen steuern
  Wenn Sie eine Zurückschreibung anfordern, wird standardmäßig maximal eine Sitzung verwendet.
- Hinweise für mehrere Clientsitzungen
  In diesem Abschnitt sind einige Hinweise aufgeführt, die Sie beachten sollten, wenn Sie mit mehreren Clientsitzungen arbeiten.

Sicherungs- und Archivierungssitzungen steuern

Wenn Sie eine Sicherung oder Archivierung anfordern, kann der Client mehrere Sitzungen mit dem Server verwenden.

Standardmäßig werden maximal zwei Sitzungen verwendet, eine für die Abfrage des Servers und eine zum Senden von Dateidaten. Der Client kann nur eine Serversitzung verwenden, wenn Sie die Option resourceutilization auf 1 setzen.

Ein Client kann mehr als die standardmäßige Anzahl Sitzungen verwenden, wenn er eine Verbindung zum IBM Spectrum Protect-Server herstellt. Bei der Angabe `resourceutilization 10` sind beispielsweise bis zu acht Sitzungen mit dem Server möglich. Mehrere Sitzungen können zur Abfrage des Servers und zum Senden von Dateidaten verwendet werden.

Mehrere Abfragesitzungen werden verwendet, wenn in einem Sicherungs- oder Archivierungsbefehl mehrere Dateispezifikationen angegeben sind. Wenn Sie beispielsweise die folgenden Befehle eingeben und `resourceutilization 5` angeben, könnte der Client eine zweite Sitzung starten, um Dateien im Dateibereich `B` abzufragen.

```
inc /Volumes/filespaceA /Volumes/filespaceB
```

Ob die zweite Sitzung tatsächlich gestartet wird, hängt davon ab, wie lange es dauert, den Server nach Dateien abzufragen, die in Dateibereich `A` gesichert sind. Außerdem könnte der Client versuchen, Daten aus dem Dateisystem zu lesen und in mehreren Sitzungen an den Server zu senden.

Anmerkung: Wenn Sie während einer Sicherungsoperation mehrere Dateispezifikationen eingeben, kann dies unter Umständen dazu führen, dass Dateien von einer Dateispezifikation auf mehreren Bändern gespeichert und mit Dateien von anderen Dateispezifikationen durchsetzt werden. Dies kann die Zurückschreibungsleistung verringern. Durch das Setzen der Option collocatebyfilespec auf yes wird das Durchsetzen von Dateien von unterschiedlichen Dateispezifikationen eliminiert, indem der Client auf eine Serversitzung pro Dateispezifikation begrenzt wird. Wenn Sie Daten auf Band speichern, werden Dateien für jede Dateispezifikation deshalb zusammen auf einem Band gespeichert (sofern auf Grund erhöhter Kapazität kein weiteres Band erforderlich ist).

Zurückschreibungssitzungen steuern

Wenn Sie eine Zurückschreibung anfordern, wird standardmäßig maximal eine Sitzung verwendet.

Weitere Zurückschreibungssitzungen basieren auf den folgenden Faktoren:

- Wert der Option resourceutilization
- Auf wie vielen Bändern die angeforderten Daten gespeichert sind
- Wie viele Bandlaufwerke verfügbar sind
- Die für den Knoten zulässige maximale Anzahl der Mountpunkte

Anmerkung:

1. Wenn alle Dateien auf Platte sind, wird nur eine Sitzung verwendet. Für eine reine Plattenspeicherpoolzurückschreibung gibt es keine Mehrfachsitzung. Wenn Sie jedoch eine Zurückschreibung ausführen, bei der sich die Dateien auf 4 Bändern und andere auf der Platte befinden, könnten Sie während der Zurückschreibung bis zu 5 Sitzungen verwenden.
2. Der IBM Spectrum Protect-Server kann die maximale Anzahl Mountpunkte, die ein Knoten auf dem Server verwenden kann, mithilfe des Parameters MAXNUMMP definieren. Wenn der Wert der Option resourceutilization den Wert für MAXNUMMP auf dem Server für einen Knoten überschreitet, kann die Sicherung mit der Nachricht `Unbekannter Systemfehler` fehlschlagen.
3. Sie können eine Zurückschreibung in Mehrfachsitzung aus Ihrem einzelnen Zurückschreibungsbefehl (restore) und von einem einzelnen Datenträger auf dem Server abrufen, wenn dieser Datenträger die Einheitenklasse FILE aufweist.

Befinden sich die Daten, die Sie zurückschreiben wollen, beispielsweise auf 5 verschiedenen Banddatenträgern, beträgt die maximale Anzahl Mountpunkte für Ihren Knoten 5 und ist für resourceutilization 3 definiert, werden 3 Sitzungen zum Zurückschreiben verwendet. Wenn Sie die Einstellung für resourceutilization auf 5 erhöhen, werden 5 Sitzungen zum Zurückschreiben verwendet. Es gibt eine Eins-zu-Eins-Beziehung zwischen der zulässigen Anzahl Zurückschreibungssitzungen und der Einstellung für resourceutilization. Mehrere Zurückschreibungssitzungen sind nur für Zurückschreibungsoperationen ohne Abfrage zulässig.

Hinweise für mehrere Clientsitzungen

In diesem Abschnitt sind einige Hinweise aufgeführt, die Sie beachten sollten, wenn Sie mit mehreren Clientsitzungen arbeiten.

Folgende Faktoren können den Durchsatz von Mehrfachsitzungen beeinflussen:

- Die Fähigkeit des Servers, mehrere Clientsitzungen auszuführen. Sind ausreichender Speicher, mehrere Speicherdatenträger und Prozessorzyklen zur Steigerung des Sicherungsdurchsatzes vorhanden?
- Die Fähigkeit des Clients, mehrere Sitzungen auszuführen (genügend Prozessorzyklen, Speicher etc.).
- Die Konfiguration des Clientspeichersubsystems. Dateisysteme, die über mehrere Datenträger einheitenübergreifend gespeichert sind, entweder durch einheitenübergreifendes Lesen und Schreiben von Daten (Software Striping) oder RAID-5, können eine Zunahme wahlfreier Leseanforderungen besser bearbeiten als ein Dateisystem mit einem einzigen Laufwerk. Außerdem ist in einem Dateisystem mit einem einzigen Laufwerk möglicherweise keine Leistungsverbesserung zu verzeichnen, wenn es versucht, viele wahlfreie, gleichzeitige Leseanforderungen zu bearbeiten.
- Ausreichende Bandbreite im Netz zur Unterstützung des erhöhten Datenaustauschs.

Zu den möglichen unerwünschten Aspekten der Ausführung von Mehrfachsitzungen gehören:

- Der Client könnte mehrere Abrechnungssätze generieren.
- Der Server könnte nicht genügend gleichzeitige Sitzungen starten. Um dies zu vermeiden, muss der Parameter *maxsessions* überprüft und eventuell geändert werden.
- Ein Befehl query node könnte die Clientaktivität nicht zusammenfassen.
- Es ist möglich, dass Dateien anstelle von festen Verbindungen zurückgeschrieben werden.
  Dateien können anstelle von festen Verbindungen zurückgeschrieben werden, wenn alle der folgenden Bedingungen zutreffen:
  - Sie schreiben ein gesamtes Dateisystem zurück.
  - Während der Zurückschreibungsoperation ist der Wert der Option *resourceutilization* größer als 1.
  - Das Dateisystem enthielt bei seiner Sicherung feste Verbindungen.

  Die Wahrscheinlichkeit, dass verbundene Dateien anstelle von festen Verbindungen zurückgeschrieben werden, erhöht sich mit der Anzahl der Sitzungen. Wenn Sie ein Dateisystem zurückschreiben, das bei seiner Sicherung feste Verbindungen enthielt, geben Sie `resourceutilization=1` an, um sicherzustellen, dass feste Verbindungen zurückgeschrieben werden.

Retryperiod

Mit der Option retryperiod wird die Wartezeit (in Minuten) des Client-Schedulers zwischen den Versuchen, einen geplanten Befehl, der fehlgeschlagen ist, auszuführen oder zwischen fehlgeschlagenen Versuchen, Ergebnisse an den Server zu melden, angegeben. Verwenden Sie diese Option nur, wenn der Scheduler aktiv ist.

Windows-BetriebssystemeIhr Administrator kann diese Option auch definieren. Gibt Ihr Administrator einen Wert für diese Option an, überschreibt dieser den Wert in Ihrer Clientoptionsdatei, nachdem Ihr Clientknoten erfolgreich den Kontakt zum Server hergestellt hat.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeIhr Administrator kann diese Option auch definieren. Gibt Ihr Administrator einen Wert für diese Option an, überschreibt dieser den Wert in Ihrer Clientsystemoptionsdatei, nachdem Ihr Clientknoten erfolgreich den Kontakt zum Server hergestellt hat.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Scheduler im Feld

Wiederholungszeitlimit im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Scheduler im Feld Wiederholungszeitlimit im Profileditor definieren.

Syntax

```
>>-RETRYPeriod-- --Minuten-------------------------------------><
```

Parameter

Minuten
: Gibt die Anzahl Minuten an, die der Client-Scheduler zwischen den Versuchen wartet, eine Verbindung zum Server herzustellen oder einen geplanten Befehl, der fehlschlägt, zu verarbeiten. Der Wertebereich ist 1 bis 9999; Standardwert ist 20.

Beispiele

Optionsdatei:
```
retryp 10
```
Befehlszeile:
```
-retryperiod=10
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Revokeremoteaccess

Die Option revokeremoteaccess schränkt den Zugriff eines Administrators mit Clientzugriffsberechtigung auf eine Client-Workstation, auf der der Web-Client aktiv ist, ein.

Diese Option schränkt den Zugriff von Administratoren mit Clienteigner-, System- oder Maßnahmenberechtigung auf die Workstation des Benutzers mithilfe des Web-Clients nicht ein.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Web-Client im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Web-Client im Profileditor definieren.

Syntax

```
                        .-None---.
>>-REVOKEremoteaccess--+--------+------------------------------><
                        '-Access-'
```

Parameter

None
: Der Zugriff von Administratoren mit Clientzugriffsberechtigung für den Client wird nicht widerrufen. Dies ist der Standardwert.

Access
: Der Zugriff von Administratoren mit Clientzugriffsberechtigung für den Client wird widerrufen.

Beispiele

Optionsdatei:
```
revokeremoteaccess none
```
Befehlszeile:
: Nicht zutreffend.

Windows-Betriebssysteme

Runasservice

Mit der Option runasservice wird die Fortsetzung der Clientbefehlsverarbeitung erzwungen, auch wenn sich das Konto, das den Client gestartet hat, abmeldet.

Diese Option ist mit den Befehlen AT und dsmc sched zu verwenden, wenn Stapeljobs für Clientbefehle geplant werden. Die Option runasservice ist in *keiner* Optionsdatei (dsm.opt oder tsmasr.opt) gültig.

Wichtig: Verwenden Sie den Scheduler-Service, wenn Sie IBM Spectrum Protect-Services unbeaufsichtigt ausführen. Definieren Sie runasservice=yes nur, um Clientbefehle mit dem Windows-Befehl AT zu planen. Die Einstellung runasservice=yes beeinträchtigt möglicherweise andere interaktive Verwendungen des Clients für Sichern/Archivieren.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
                .-No--.
>>-RUNASSERVice--+-----+----------------------------------------><
                '-Yes-'
```

Parameter

No
: Erzwingt nicht die Fortsetzung der Clientbefehlsverarbeitung, auch wenn sich das Konto, das den Client gestartet hat, abmeldet. Dies ist der Standardwert.

Yes
: Erzwingt die Fortsetzung der Clientbefehlsverarbeitung, auch wenn sich das Konto, das den Client gestartet hat, abmeldet.

  Einschränkungen:

  1. Bei runasservice=yes wird die Einstellung für REPLACE immer zugunsten des Verhaltens replace=no überschrieben.
  2. Die Option runasservice=yes kann nicht in Kombination mit passwordaccess=prompt verwendet werden.
  3. Mit runasservice=yes ausgeführte Sicherungs-, Archivierungs-, Zurückschreibungs- und Abrufoperationen, bei denen Eingabeaufforderungen auftreten, schlagen immer fehl. Zur Vermeidung dieses Problems müssen Sie entweder das Kennwort für den Verschlüsselungsschlüssel mit encryptkey=save speichern oder die Option runasservice inaktivieren.

Beispiele

Befehlszeile:

```
-runasservice=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Schedcmddisabled

Die Option schedcmddisabled gibt an, ob die Zeitplanung von Befehlen durch die Serveroption action=command im Serverbefehl define schedule inaktiviert werden soll.

Durch diese Option werden die Befehle preschedulecmd und postschedulecmd nicht inaktiviert. Sie können jedoch preschedulecmd oder postschedulecmd mit einem Leerzeichen oder einer Nullzeichenfolge angeben, um die Zeitplanung dieser Befehle zu inaktivieren.

Sie können die Zeitplanung von Befehlen, die von Ihrem IBM Spectrum Protect-Administrator definiert wurden, inaktivieren, indem Sie die Option schedcmddisabled auf yes setzen.

Verwenden Sie den Befehl query schedule, um die von Ihrem Administrator definierten Zeitpläne abzufragen.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein.

Syntax

```
                     .-No--.
>>-SCHEDCMDDisabled--+-----+-----------------------------------><
                     '-Yes-'
```

Parameter

Yes
: Gibt an, dass der Server die Planung von Befehlen mit der Option action=command des Serverbefehls DEFINE SCHEDULE inaktiviert.

No
: Gibt an, dass der Server die Planung von Befehlen mit der Option action=command des Serverbefehls DEFINE SCHEDULE nicht inaktiviert. Dies ist der Standardwert.

Beispiele

Optionsdatei:
```
schedcmddisabled no
```
Befehlszeile:
: Nicht zutreffend.

Schedcmdexception

Die Option schedcmdexception wird in Kombination mit der Option schedcmddisabled verwendet, um die Planung von Befehlen durch die Serveroption action=command im Serverbefehl DEFINE SCHEDULE zu inaktivieren, mit Ausnahme bestimmter Befehlszeichenfolgen.

Sie müssen die genaue Zeichenfolge angeben, die mit der Definition des "Objekts" im Zeitplan übereinstimmt, damit der geplante Serverbefehl akzeptiert wird. Stimmt die Zeichenfolge nicht genau überein (sie enthält beispielsweise ein zusätzliches Leerzeichen oder die Groß-/Kleinschreibung unterscheidet sich), wird die geplante Befehlsaktion blockiert.

Sie können mehrere Optionen schedcmdexception in der Optionsdatei angeben. Diese Option wird nur berücksichtigt, wenn die Option schedcmddisabled aktiviert ist. Die Position dieser Option in der Optionsdatei ist unabhängig von der Position der Option schedcmddisabled.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option ist nicht in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server gültig.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein.

Syntax

```
>>-SCHEDCMDException--string----------------------------------><
```

Parameter

Zeichenfolge
: Für Befehle, die mit der Option action=command im Serverbefehl DEFINE SCHEDULE geplant werden, gibt dieser Parameter das Objektmuster an, das zu aktivieren ist, wenn die Option schedcmddisabled=yes angegeben wird. Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden und der Parameter muss genau mit der Befehlszeichenfolge in der Zeitplandefinition auf dem IBM Spectrum Protect-Server übereinstimmen.

Beispiel

Optionsdatei:
```
schedcmddisabled yes
```
Windows-Betriebssysteme`schedcmdexception "start dir c: /s"`

```
schedcmdexception "start echo hello, world!"
```

Schedgroup

Mit der Option schedgroup wird ein Zeitplan einer Gruppe zugeordnet.

Ein Beispiel für die Verwendung dieser Option ist die Gruppierung mehrerer Zeitpläne zur täglichen lokalen Sicherung in einem einzigen Zeitplan zur Sicherung des Servers.

Unterstützte Clients

Diese Option ist für alle Clients als Befehlszeilenoption für den Serverbefehl DEFINE SCHEDULE gültig. Diese Option kann nicht einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server hinzugefügt werden.

Syntax

```
>>-SCHEDGROUP-- --Name_der_Zeitplangruppe---------------------><
```

Parameter

Name_der_Zeitplangruppe
: Gibt den Namen der Zeitplangruppe an. Sie können bis zu 30 Zeichen für den Namen angeben.
Eine Liste der gültigen Zeichen, die im Namen der Zeitplangruppe verwendet werden können, finden Sie in IBM Spectrum Protect-Objekte benennen.

Beispiele

Mit den folgenden Beispielbefehlen werden die Zeitpläne SCHED_A_1, SCHED_A_2, SCHED_A_3 und SCHED_A_4 in der Zeitplangruppe GROUP_A gruppiert.

Befehlszeile:

Dieses Beispiel zeigt eine lokale Sicherung um 6 Uhr:

```
define schedule standard SCHED_A_1 Type=Client ACTion=Backup SUBACTion=VM OPTions='-vmfulltype=vstor -
vmbackuptype=fullvm -vmbackuplocation=local -domain.vmfull="SCHEDULE-TAG" -asnodename=DC_SARTRE_WB -
SCHEDGROUP=GROUP_A' STARTDate=02/06/2017 STARTTime=06:00:00 SCHEDStyle=Enhanced DAYofweek=ANY
```

Dieses Beispiel zeigt eine lokale Sicherung um 12 Uhr:

```
define schedule standard SCHED_A_2 Type=Client ACTion=Backup SUBACTion=VM OPTions='-vmfulltype=vstor -
vmbackuptype=fullvm -vmbackuplocation=local -domain.vmfull="SCHEDULE-TAG" -asnodename=DC_SARTRE_WB -
SCHEDGROUP=GROUP_A' STARTDate=02/06/2017 STARTTime=12:00:00 SCHEDStyle=Enhanced DAYofweek=ANY
```

Dieses Beispiel zeigt eine lokale Sicherung um 18 Uhr:

```
define schedule standard SCHED_A_3 Type=Client ACTion=Backup SUBACTion=VM OPTions='-vmfulltype=vstor -
vmbackuptype=fullvm -vmbackuplocation=local -domain.vmfull="SCHEDULE-TAG" -asnodename=DC_SARTRE_WB -
SCHEDGROUP=GROUP_A' STARTDate=02/06/2017 STARTTime=18:00:00 SCHEDStyle=Enhanced DAYofweek=ANY
```

Dieses Beispiel zeigt eine lokale Sicherung und eine Serversicherung um 0 Uhr (Mitternacht):

```
define schedule standard SCHED_A_4 Type=Client ACTion=Backup SUBACTion=VM OPTions='-vmfulltype=vstor -
vmbackuptype=fullvm -vmbackuplocation=both -domain.vmfull="SCHEDULE-TAG" -asnodename=DC_SARTRE_WB -
SCHEDGROUP=GROUP_A' STARTDate=02/06/2017 STARTTime=00:00:00 SCHEDStyle=Enhanced DAYofweek=ANY
```

Tipp: Stellen Sie sicher, dass jeder Zeitplan in der Gruppe vor dem festgelegten Start des nächsten Zeitplans abgeschlossen werden kann. Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Schedlogmax

Die Option schedlogmax gibt die maximale Größe des Planungsprotokolls (dsmsched.log) und des Web-Client-Protokolls (dsmwebcl.log) in Megabyte an.

Diese Option bewirkt, dass bei den Protokolldateien, die für Schedulerereignisse (dsmsched.log) und für Web-Client-Ereignisse (dsmwebcl.log) erstellt werden, ein Umlauf stattfindet, wenn sie ihre maximale Größe erreichen. Bei der Protokollierung von Scheduler- und Web-Client-Ereignissen werden Protokollsätze bis zum Erreichen der angegebenen maximalen Größe an das Ende der Protokolldateien angefügt. Wenn die maximale Größe erreicht ist, wird ein Protokollsatz mit dem Inhalt `Wird am Dateianfang fortgesetzt` als letzter Satz in die Datei gestellt. Die nachfolgende Protokollierung wird am Anfang der Datei wieder aufgenommen. Das Ende des Umlaufprotokolls wird durch einen Satz mit dem Inhalt `DATENENDE` angezeigt.

Wenn Sie die Option schedlogmax angeben, werden Scheduler- und Web-Client-Protokollnachrichten nicht in einer bereinigten Datei gespeichert. Wenn Sie Protokolle bereinigen und die bereinigten Protokolleinträge in einer anderen Datei speichern wollen, lesen Sie die Informationen zur Option schedlogretention.

Wenn Sie vom Protokollumlauf (Option schedlogmax) zur Protokollbereinigung (Option schedlogretention) wechseln, werden alle vorhandenen Protokolleinträge aufbewahrt, und das Protokoll wird mit den neuen Kriterien von schedlogretention bereinigt.

Wenn Sie von der Protokollbereinigung (Option schedlogretention) zum Protokollumlauf (Option schedlogmax) wechseln, werden alle Sätze in den vorhandenen Protokollen in eine Datei kopiert, die die bereinigten Einträge enthält. Aus der Datei dsmsched.log bereinigte Protokollsätze werden beispielsweise in die Datei dsmsched.pru kopiert. Aus der Datei dsmwebcl.log bereinigte Protokollsätze werden in die Datei dsmweblog.pru kopiert. Die vorhandenen Protokolle (dsmsched.log und dsmwebcl.log) werden geleert und die Protokollierung beginnt mit den neuen Protokollumlaufbedingungen.

Wenn Sie lediglich den Wert der Option schedlogmax ändern, wird das vorhandene Protokoll erweitert oder gekürzt, um der neuen Größe zu entsprechen. Wird der Wert verkleinert, werden die ältesten Einträge gelöscht, um die Datei auf die neue Größe zu verkleinern.

Wird weder schedlogmax noch schedlogretention angegeben, kann das Fehlerprotokoll uneingeschränkt wachsen. Sie müssen den Protokollinhalt manuell verwalten, um zu verhindern, dass das Protokoll die Plattenressourcen verbraucht. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option schedlogretention ausgeben, wird das Protokoll mit dem angegebenen Wert für die Aufbewahrungsdauer bereinigt. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option schedlogmax ausgeben, wird das vorhandene Protokoll als bereinigtes Protokoll behandelt. Das heißt, der Inhalt der Datei dsmsched.log wird in eine Datei mit dem Namen dsmsched.pru kopiert, der Inhalt der Datei dsmwebcl.log wird in eine Datei mit dem Namen dsmwebcl.pru kopiert und sowohl in dsmsched.log als auch in dsmwebcl.log werden neue Protokolleinträge erstellt. In beiden Dateien findet ein Umlauf statt, wenn sie ihre maximale Größe erreichen.

Anmerkung: Wenn Sie für schedlogmax einen Wert ungleich null angeben (wodurch der Protokollumlauf aktiviert wird), können Sie nicht die Option schedlogretention verwenden, um bereinigte Protokolle zu erstellen. Für Protokolle kann entweder eine Bereinigung oder ein Umlauf durchgeführt werden, aber nicht beides.
Mit der Option schedlogmax erstellte Protokolle enthalten einen Protokollkopfsatz, der Informationen wie in dem folgenden Beispieldatensatz enthält:

```
LOGHEADERREC 661  104857600 IBM Spectrum Protect 8.1.0.0 Fri Dec 9 06:46:53 2014
```

Beachten Sie, dass die Datums- und Zeitmarkenangaben im Text von LOGHEADERREC nicht mithilfe der Einstellungen übersetzt oder formatiert werden, die in den Optionen dateformat und timeformat angegeben sind.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme
Sie können diese Option auch auf der Registerkarte Clientvorgaben > Scheduler in der GUI definieren. Wählen Sie hierfür Umlauf für Schedulerprotokolldatei aktivieren aus und geben Sie einen Wert ungleich null für Maximale Größe der Protokolldatei an. Geben Sie für die maximale Größe null an, um den Umlauf der Protokolldatei zu verhindern. Wenn die maximale Größe auf null gesetzt ist, bleibt die Option Umlauf für Schedulerprotokolldatei aktivieren wirkungslos. Es findet kein Protokollumlauf statt, wenn die maximale Größe auf null gesetzt ist.

Syntax

```
>>-SCHEDLOGMAX-- --Größe-----------------------------------------><
```

Parameter

Größe
: Gibt die maximale Größe für die Protokolldatei in Megabyte an. Der Wertebereich ist 0 bis 2047. Der Standardwert ist 0, wodurch der Protokolldateiumlauf inaktiviert und die Größe der Protokolldatei unbeschränkt wird.

Beispiele

Optionsdatei:

```
schedlogmax 100
```

Befehlszeile:

```
-schedlogmax=100
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Schedlogname

Die Option schedlogname gibt den Pfad und den Namen der Datei an, in der Planungsprotokollinformationen gespeichert werden sollen.

Verwenden Sie diese Option nur, wenn Sie Planungsprotokollinformationen speichern wollen. Diese Option wird nur angewendet, wenn der Scheduler aktiv ist.

Wird diese Option nicht verwendet, wird die Datei `dsmsched.log` in demselben Verzeichnis erstellt wie die Datei `dsmerror.log`.

Wenn Sie den Befehl schedule ausführen, wird die Ausgabe geplanter Befehle auf Ihrem Bildschirm angezeigt. Außerdem wird die Ausgabe in die mit dieser Option angegebene Datei gesendet. Wenn ein Teil des von Ihnen angegebenen Pfads nicht vorhanden ist, versucht der Client, ihn zu erstellen.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Scheduler im Textfeld Planungsprotokoll im Profileditor definieren.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Scheduler im Textfeld Planungsprotokoll im Profileditor definieren.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
Anmerkung: Geben Sie für die Umgebungsvariable `DSM_LOG` ein Verzeichnis an, in das das Protokoll gestellt werden soll. Das angegebene Verzeichnis muss Berechtigungen aufweisen, die einen Schreibzugriff von dem Konto zulassen, unter dem der Client ausgeführt wird. Das Stammverzeichnis ist kein gültiger Wert für `DSM_LOG`.
 Windows-Betriebssysteme
Anmerkung: Geben Sie für die Umgebungsvariable `DSM_LOG` ein Verzeichnis an, in das das Protokoll gestellt werden soll. Das angegebene Verzeichnis muss Berechtigungen aufweisen, die einen Schreibzugriff von dem Konto zulassen, unter dem der Client ausgeführt wird.

Syntax

```
>>-SCHEDLOGName-- --Dateispezifikation-------------------------><
```

Parameter

Dateispezifikation
Gibt den Pfad und den Namen der Datei an, in der Planungsprotokolldaten bei der Verarbeitung geplanter Arbeit gespeichert werden sollen. Wenn ein Teil des von Ihnen angegebenen Pfads nicht vorhanden ist, versucht der Client, ihn zu erstellen.

 Windows-BetriebssystemeWird nur ein Dateiname angegeben, wird die Datei im aktuellen Verzeichnis gespeichert. Standardwert ist das aktuelle Arbeitsverzeichnis und der Dateiname `dsmsched.log`.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeWird nur ein Dateiname angegeben, wird die Datei im aktuellen Verzeichnis gespeichert. Standardwert ist das aktuelle Arbeitsverzeichnis und der Dateiname `dsmsched.log`. Die Datei `dsmsched.log` darf *keine* symbolische Verbindung sein.

 Mac OS X-BetriebssystemeFür Mac OS X: Wenn Sie nur einen Dateinamen angeben, wird die Datei in Ihrem Standardordner gespeichert. Die Standardverzeichnisse sind:

```
~/Library/Logs/tivoli/tsm
/Library/Logs/tivoli/tsm
```

Beispiele

Optionsdatei:
 Mac OS X-Betriebssysteme

```
SCHEDLOGN /Users/user1/Library/Logs/schedlog.jan
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
schedlogname /home/mydir/schedlog.jan
```

Windows-Betriebssysteme

```
schedlogname c:\mydir\schedlog.jan
```

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssysteme`-schedlogname=/Users/user1/Library/Logs/schedlog.jan`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme`-schedlogname=/home/mydir/schedlog.jan`

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`-schedlogn=c:\mydir\schedlog.jan`

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Schedlogretention

Mit der Option schedlogretention kann die Aufbewahrungsdauer in Tagen für Einträge im Planungsprotokoll (dsmsched.log) und im Web-Client-Protokoll (dsmwebcl.log) festgelegt werden und ob bereinigte Einträge in einer anderen Datei gespeichert werden sollen.

Das Planungsprotokoll (dsmsched.log) wird beim Start des Schedulers und nach Beendigung eines geplanten Ereignisses bereinigt. Bereinigte Einträge werden in eine Datei mit dem Namen dsmsched.pru geschrieben.

Das Web-Client-Protokoll (dsmwebcl.log) wird beim anfänglichen Start des Clientakzeptordämons bereinigt. Bereinigte Einträge werden in eine Datei mit dem Namen dsmwebcl.pru geschrieben.

Wenn Sie von der Protokollbereinigung (Option schedlogretention) zum Protokollumlauf (Option schedlogmax) wechseln, werden alle Sätze im vorhandenen Protokoll in das bereinigte Protokoll (dsmsched.pru und dsmwebcl.pru) kopiert und die vorhandenen Protokolle (dsmsched.log und dsmwebcl.log) werden geleert. Die Protokollierung beginnt dann mit den neuen Protokollumlaufbedingungen.

Wenn Sie vom Protokollumlauf (Option schedlogmax) zur Protokollbereinigung (Option schedlogretention) wechseln, werden alle vorhandenen Protokolleinträge aufbewahrt, und das Protokoll wird mit den neuen Kriterien von schedlogretention bereinigt. Die bereinigten Einträge werden in den entsprechenden *.pru-Dateien gespeichert.

Wird weder schedlogmax noch schedlogretention angegeben, können die Protokolle uneingeschränkt wachsen. Sie müssen den Protokollinhalt manuell verwalten, um zu verhindern, dass das Protokoll die Plattenressourcen verbraucht. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option schedlogretention ausgeben, wird das Protokoll mit dem angegebenen Wert für die Aufbewahrungsdauer bereinigt. Wenn das Protokoll ohne eine der beiden Optionen erstellt wurde und wenn Sie später einen Befehl mit der Option schedlogmax ausgeben, wird das vorhandene Protokoll als bereinigtes Protokoll behandelt. Das heißt, der Inhalt der Datei dsmsched.log wird in eine Datei mit dem Namen dsmsched.pru kopiert, der Inhalt der Datei dsmwebcl.log wird in dsmwebcl.pru kopiert und sowohl in dsmsched.log als auch in dsmwebcl.log werden neue Protokolleinträge erstellt. In beiden Dateien findet ein Umlauf statt, wenn sie ihre maximale Größe erreichen.

Anmerkung: Wenn Sie die Option schedlogretention angeben, um bereinigte Protokolle zu erstellen, können Sie die Option schedlogmax nicht angeben. Für Protokolle kann entweder eine Bereinigung oder ein Umlauf durchgeführt werden, aber nicht beides.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme Sie können diese Option auch auf der Registerkarte Clientvorgaben > Scheduler in der grafischen Benutzerschnittstelle definieren. Wählen Sie hierfür Alte Einträge bereinigen aus und geben Sie einen Wert für Einträge bereinigen, die älter sind als an. Durch Auswahl der Option Bereinigte Einträge sichern werden die bereinigten Schedulerprotokolleinträge in der Protokolldatei dsmsched.pru gespeichert. Durch die Auswahl von Bereinigte Einträge sichern werden außerdem die Protokolleinträge des Web-Clients in der Protokolldatei dsmwebcl.pru gespeichert.

Syntax

```
                    .-N----.  .-D-.
>>-SCHEDLOGRetention--+------+--+---+-------------------------><
```

```
'-Tage-'  '-S-'
```

Parameter

N oder Tage
: Gibt die Wartezeit vor dem Bereinigen des Protokolls an.

  N
  : Das Protokoll nicht bereinigen. Das Protokoll kann unendlich groß werden. Dies ist der Standardwert.

  Tage
  : Gibt die Anzahl Tage an, die Protokolldateieinträge vor dem Bereinigen aufbewahrt werden sollen. Der Wertebereich ist 0 bis 9999.

D oder S
: Gibt an, ob bereinigte Einträge gesichert werden sollen. Ein Leerzeichen oder ein Komma verwenden, um diesen Parameter vom vorherigen zu trennen.

  D
  : Löscht die Protokolleinträge, wenn das Protokoll bereinigt wird. Dies ist der Standardwert.

  S
  : Sichert die Protokolleinträge, wenn das Protokoll bereinigt wird.

    Bereinigte Einträge werden in die Datei der bereinigten Einträge (dsmsched.pru oder dsmsched.pru) kopiert, die in demselben Verzeichnis gespeichert ist wie das Protokoll.

Beispiele

Optionsdatei:
```
schedlogretention 30 S
```
Befehlszeile:
```
-schedlogretention=30,S
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Schedmode

Mit der Option schedmode kann angegeben werden, ob der Modus Polling (Clientsendeaufruf: der Clientknoten fragt den Server regelmäßig nach geplanter Arbeit) oder der Modus Prompted (Servergesteuerte Ausführung: der Server stellt eine Verbindung zum Clientknoten her, wenn eine geplante Operation gestartet werden muss) verwendet werden soll.

'Polling' (Clientsendeaufruf) kann für alle Übertragungsmethoden verwendet werden, 'Prompted' (Servergesteuerte Ausführung) jedoch nur für TCP/IP.

Diese Option ist nur gültig, wenn Sie die TCP/IP-Übertragungsmethode verwenden und der Befehl schedule aktiv ist.

 Der Administrator kann angeben, dass der Server beide Modi oder nur einen Modus unterstützt. Gibt der Administrator an, dass beide Modi unterstützt werden, können Sie einen der beiden Planungsmodi auswählen. Gibt der Administrator nur einen Modus an, müssen Sie diesen Modus in Ihrer Datei dsm.opt angeben, damit geplante Arbeit verarbeitet wird.

 Der Administrator kann angeben, dass der Server beide Modi oder nur einen Modus unterstützt. Gibt der Administrator an, dass beide Modi unterstützt werden, können Sie einen der beiden Planungsmodi auswählen. Gibt der Administrator nur einen Modus an, müssen Sie diesen Modus in Ihrer Datei dsm.sys angeben, damit geplante Arbeit verarbeitet wird.

 Wenn Sie den Modus prompted angeben, empfiehlt es sich, Werte für die Optionen tcpclientaddress und tcpclientport in Ihrer Datei dsm.opt oder im Befehl schedule anzugeben; der Client kann dann entweder an einer Adresse oder an einem Anschluss Ihrer Wahl kontaktiert werden (nützlich für Clientsysteme mit mehreren Netzschnittstellenkarten).

 Wenn Sie den Modus prompted angeben, empfiehlt es sich, Werte für die Optionen tcpclientaddress und tcpclientport in Ihrer Datei dsm.sys oder im Befehl schedule anzugeben; der Client kann dann entweder an einer Adresse oder an einem Anschluss Ihrer Wahl kontaktiert werden (nützlich für Clientsysteme mit mehreren Netzschnittstellenkarten).

Anmerkung:

1.  Wenn Sie die Einstellung dieser Option in der Clientoptionsdatei (dsm.opt) ändern, müssen Sie den Scheduler-Service stoppen und erneut starten, damit die Einstellung wirksam wird.
2.  Wenn Sie die Einstellung dieser Option in der Datei dsm.sys ändern, müssen Sie den Scheduler-Service stoppen und erneut starten, damit die Einstellung wirksam wird.
3. Diese Option kann auch auf dem Server definiert werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Scheduler im Abschnitt Planungsmodus im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Scheduler im Abschnitt Planungsmodus im Profileditor definieren.

Syntax

```
              .-POlling--.
>>-SCHEDMODe--+----------+-------------------------------------><
              '-PRompted-'
```

Parameter

POlling
: Der Client-Scheduler fragt den Server in festgelegten Zeitintervallen nach geplanter Arbeit ab. Dies ist der Standardwert. Die Zeitintervalle werden mit der Option queryschedperiod festgelegt.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

PRompted
: AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Windows-BetriebssystemeDer Client-Scheduler wartet, bis der Server eine Verbindung zum Clientknoten herstellt, wenn geplante Arbeit ausgeführt werden muss.
Anmerkung:

1. Windows-BetriebssystemeVerwenden Sie schedmode prompted gemeinsam mit der Option autodeploy, um die sofortige Verarbeitung des Clientimplementierungszeitplans durch den Scheduler zu aktivieren.
2. Wenn Sie den Befehl dsmc schedule verwenden und sowohl schedmode prompted als auch commmethod V6Tcpip angegeben sind, müssen der Client und der IBM Spectrum Protect-Server für IPv6 konfiguriert sein. Darüber hinaus muss der Client-Hostname für die IPv6-Adresse definiert sein.

Beispiele

Optionsdatei:
```
schedmode prompted
```
Befehlszeile:
```
-schedmod=po
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Zugehörige Verweise:
Windows-BetriebssystemeAutodeploy
Cadlistenonport
Tcpclientaddress
Tcpclientport

Schedrestretrdisabled

Die Option schedrestretrdisabled gibt an, ob die Ausführung von Zurückschreibungs- oder Abrufplanungsoperationen inaktiviert werden soll.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann nicht auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe für den Scheduler ein. Sie können diese Option auf der Registerkarte Scheduler im Abschnitt

Befehl für Zeitplan im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) für den Scheduler ein. Sie können diese Option auf der Registerkarte Scheduler im Abschnitt Befehl für Zeitplan im Profileditor definieren.

Syntax

```
                          .-No--.
>>-SCHEDRESTRETRDisabled--+-----+------------------------------><
                          '-Yes-'
```

Parameter

No
: Gibt an, dass der Client die Ausführung von Zurückschreibungs- und Abrufplanungsoperationen nicht inaktiviert. Dieser Parameter ist der Standardwert.

Yes
: Gibt an, dass der Client die Ausführung von Zurückschreibungs- und Abrufplanungsoperationen inaktiviert.

Beispiele

Optionsdatei:
```
schedrestretrdisabled yes
```
Befehlszeile:
: Nicht zutreffend.

Scrolllines

Mit der Option scrolllines wird die Anzahl Datenzeilen angegeben, die gleichzeitig auf dem Bildschirm angezeigt werden.

Verwenden Sie diese Option, wenn Sie die Option scrollprompt auf Yes setzen.

Die Option scrolllines können Sie nur mit den folgenden Befehlen verwenden:

- delete filespace
- query archive
- query backup
- query backupset
- query filespace
- query group
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemequery image
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemequery nas
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemequery node
- query options

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option im Feld Befehlszeile > Anzahl Zeilen, die angezeigt werden sollen im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option im Feld Befehlszeile > Anzahl Zeilen, die angezeigt werden sollen im Profileditor definieren.

Syntax

```
>>-SCROLLLines-- --Nummer---------------------------------------><
```

Parameter

Zahl
: Gibt die Anzahl Datenzeilen an, die gleichzeitig auf dem Bildschirm angezeigt werden. Der Wertebereich ist 1 bis 80; Standardwert ist 20.

Beispiele

Optionsdatei:
```
scrolllines 25
```
Befehlszeile:
```
-scrolll=25
```

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Scrollprompt

Die Option scrollprompt gibt an, ob der Client für Sichern/Archivieren nach dem Anzeigen der Anzahl Datenzeilen, die Sie in der Option scrolllines angegeben haben, stoppen und warten soll oder ob er alle Zeilen durchblättern und am Ende der Datenliste stoppen soll.

Die Option scrollprompt können Sie nur mit den folgenden Befehlen verwenden:

- delete filespace
- query archive
- query backup
- query backupset
- query filespace
- query group
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemequery image
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemequery nas
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemequery node
- query options

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Befehlszeile im Feld Nach dem Anzeigen der folgenden Anzahl Zeilen anhalten definieren.

Syntax

```
                .-No--.
>>-SCROLLPrompt--+-----+----------------------------------------><
                '-Yes-'
```

Parameter

No
: Bis zum Ende der Liste blättern und stoppen. Dies ist der Standardwert.

Yes
: Nach dem Anzeigen der Anzahl Zeilen, die in der Option scrolllines angegeben wird, stoppen und warten. Die folgende Bedienerführung wird angezeigt:

  ```
  Zum Verlassen 'Q', für fortlaufendes Blättern 'C' oder zum Fortfahren 'Eingabe'
  drücken.
  ```

Beispiele

Optionsdatei:
```
scrollprompt yes
```
Befehlszeile:
```
-scrollp=yes
```

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

Servername

In Ihrer Datei dsm.sys gibt die Option servername den Namen an, den Sie für die Identifikation eines Servers und am Anfang einer Zeilengruppe mit Optionen für diesen Server verwenden wollen. Es können mehrere Server benannt und Optionen für sie angegeben werden.

Das folgende Beispiel zeigt, wie Optionen für zwei unterschiedliche Server angegeben werden:

In Ihrer Clientbenutzeroptionsdatei (dsm.opt) gibt die Option servername an, zu welchem der in Ihrer Datei dsm.sys genannten Server zwecks Sicherungs-/Archivierungsservices der Kontakt hergestellt werden soll. Wird die Option servername in einer Clientbenutzeroptionsdatei (dsm.opt) oder in der Befehlszeile angegeben, überschreibt sie den Standardserver, der in Ihrer Clientsystemoptionsdatei angegeben ist.

Anmerkung:

1. Der Server, der in der Clientsystemoptionsdatei für die Umlagerung angegeben ist, kann mit der Option servername nicht überschrieben werden.
2. Wenn sich der Name des IBM Spectrum Protect-Servers ändert oder Clients für Sichern/Archivieren zu einem anderen IBM Spectrum Protect-Server geleitet werden, muss für alle Clients ein neues Kennwort für den neuen Servernamen initialisiert werden.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) und in die Clientsystemoptionsdatei (dsm.sys) ein. In der Datei dsm.sys bildet die Option servername den Anfang einer Serverzeilengruppe.

Ändern Sie diese Option nicht in dsm.opt, wenn Sie den Client für Sichern/Archivieren in einer Befehlszeilensitzung ausführen oder wenn Sie die grafische Benutzerschnittstelle des Clients für Sichern/Archivieren ausführen.

Syntax

```
>>-SErvername-- --Servername-----------------------------------><
```

Parameter

Servername
: Geben Sie in Ihrer Datei dsm.sys den Namen an, der einem bestimmten Server zugeordnet werden soll. Geben Sie in Ihrer Clientbenutzeroptionsdatei (dsm.opt) oder in der Befehlszeile den Namen des Servers an, zu dem zwecks Sicherungs-/Archivierungsservices der Kontakt hergestellt werden soll. Der Wert von *Servername* in dsm.opt muss einem *Servername*-Wert in dsm.sys entsprechen. Andernfalls kann der Client keinen Kontakt zum Server herstellen.

  Ein Servername ist nicht von der Groß-/Kleinschreibung abhängig; er kann bis zu 64 Zeichen haben.

Beispiele

Optionsdatei:
```
servername server_a
```
Befehlszeile:
```
-se=server_b
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Sessioninitiation

Verwenden Sie die Option sessioninitiation, um zu steuern, ob der Server oder der Client Sitzungen durch eine Firewall einleiten soll. Standardwert ist, dass der Client Sitzungen einleitet. Sie können diese Option im Befehl schedule verwenden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFür den Client-Scheduler ist es nicht erforderlich, Anschlüsse in der Firewall zu öffnen. Wenn Sie die Option sessioninitiation auf serveronly setzen, versucht der Client nicht, Kontakt zum Server aufzunehmen. Alle Sitzungen müssen durch die Zeitplanung über Serversystemanfrage an dem mit der Option tcpclientport

auf dem Client definierten Anschluss eingeleitet werden. Die Option sessioninitiation beeinflusst nur das Verhalten des Client-Schedulers, der im Modus mit Bedienerführung ausgeführt wird. Wenn Sie die Option sessioninitiation auf serveronly setzen, versuchen der Befehlszeilenclient, die GUI des Clients für Sichern/Archivieren und die Web-Client-GUI - mit Ausnahme der Scheduler, die vom Clientakzeptordämon verwaltet werden - dennoch, Sitzungen einzuleiten.

Windows-BetriebssystemeFür den Client-Scheduler ist es nicht erforderlich, Anschlüsse in der Firewall zu öffnen. Wenn Sie die Option sessioninitiation auf serveronly setzen, versucht der Client nicht, Kontakt zum Server aufzunehmen. Alle Sitzungen müssen durch die Zeitplanung über Serversystemanfrage an dem mit der Option tcpclientport auf dem Client definierten Anschluss eingeleitet werden. Die Option sessioninitiation beeinflusst nur das Verhalten des Client-Schedulers, der im Modus mit Bedienerführung ausgeführt wird. Wenn Sie die Option sessioninitiation auf serveronly setzen, versuchen der Befehlszeilenclient, die GUI des Clients für Sichern/Archivieren und die Web-Client-GUI - mit Ausnahme der Scheduler, die vom Clientakzeptordämon verwaltet werden - dennoch, Sitzungen einzuleiten.

Achtung: Sie können den dsmcad nicht für die Planung verwenden, wenn Sie die Option sessioninitiation auf serveronly setzen.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAnmerkung: Wenn Sie die Option sessioninitiation auf serveronly setzen, sind der Client-Setup-Assistent und der Scheduler-Service nicht in der Lage, sich beim IBM Spectrum Protect-Server zu authentifizieren. In diesem Fall können Sie den Scheduler von der Befehlszeile aus ausführen (`dsmc schedule`) und bei der entsprechenden Aufforderung das Kennwort für Ihren Knoten eingeben.
Windows-BetriebssystemeAnmerkung: Wenn Sie die Option sessioninitiation auf serveronly setzen, sind der Client-Setup-Assistent und der Scheduler-Service nicht in der Lage, sich beim IBM Spectrum Protect-Server zu authentifizieren. In diesem Fall können Sie den Scheduler von der Befehlszeile aus ausführen (dsmc schedule) und bei der entsprechenden Aufforderung das Kennwort für Ihren Knoten eingeben oder den folgenden Befehl dsmcutil verwenden, um das Kennwort zu aktualisieren.

```
dsmcutil updatepw /node:nnn /commServer:server1.example.com /password:ppp
/validate:no
```

Ein ähnliches Problem kann auftreten, wenn ein Verschlüsselungsschlüssel für Sicherungsoperationen erforderlich ist. In diesem Fall können Sie den Scheduler über die Befehlszeile ausführen (`dsmc schedule`) und den Verschlüsselungsschlüssel eingeben, wenn Sie dazu aufgefordert werden. Nachdem das Kennwort und der Verschlüsselungsschlüssel aktualisiert wurden, müssen Sie den Scheduler erneut starten.

Wenn Sie die Option sessioninitiation auf client setzen, leitet der Client Sitzungen mit dem Server ein, indem er über den TCP/IP-Anschluss kommuniziert, der durch die Serveroption tcpport definiert ist. Dies ist der Standardwert. Mit der Zeitplanung über Serversystemanfrage kann der Client dazu aufgefordert werden, eine Verbindung zum Server herzustellen.

Anmerkung:

1. Der IBM Spectrum Protect-Server kann SESSIONINITiation=clientorserver oder SESSIONINITiation=serveronly in den Befehlen register node und update node angeben. Wenn der Server SESSIONINITiation=clientorserver angibt, kann der Client entscheiden, welche Methode verwendet werden soll. Wenn der Server SESSIONINITiation=serveronly angibt, werden alle Sitzungen vom Server eingeleitet.
2. Wird sessioninitiation auf serveronly gesetzt, muss der Wert für die Clientoption tcpclientaddress mit dem Wert für die Option HLAddress im Serverbefehl update node oder register node übereinstimmen. Der Wert für die Clientoption tcpclientport muss mit dem Wert für die Option LLAddress im Serverbefehl update node oder register node übereinstimmen.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Scheduler im Feld Sitzungsstart im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Scheduler im Feld Sitzungsstart im Profileditor definieren.

Syntax

```
                      .-Client-----.
>>-SESSIONINITiation--+------------+--------------------------><
                      '-SERVEROnly-'
```

Parameter

Client
: Gibt an, dass der Client Sitzungen mit dem Server einleitet, indem er über den TCP/IP-Anschluss kommuniziert, der durch die Serveroption TCPPORT definiert ist. Dies ist der Standardwert. Mit der Zeitplanung über Serversystemanfrage kann der Client dazu aufgefordert werden, eine Verbindung zum Server herzustellen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSERVEROnly

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt an, dass der Server keine Clientanforderungen für Sitzungen akzeptiert. Alle Sitzungen müssen durch die Zeitplanung über Serversystemanfrage an dem mit der Option tcpclientport auf dem Client definierten Anschluss eingeleitet werden. Mit Ausnahme der Scheduler, die vom Clientakzeptordämon verwaltet werden, versuchen der Befehlszeilenclient, die GUI des Clients für Sichern/Archivieren und die Web-Client-GUI dennoch, Sitzungen einzuleiten.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWenn die Serveroption AUTHENTICATION auf LDAP gesetzt ist, geben Sie für die Clientoption sessioninitiation nicht serveronly an; andernfalls können keine Zeitpläne ausgeführt werden.

Windows-BetriebssystemeSERVEROnly
Windows-BetriebssystemeGibt an, dass der Server keine Clientanforderungen für Sitzungen akzeptiert. Alle Sitzungen müssen durch die Zeitplanung über Serversystemanfrage an dem mit der Option tcpclientport auf dem Client definierten Anschluss eingeleitet werden. Mit Ausnahme der Scheduler, die vom Clientakzeptordämon verwaltet werden, versuchen der Befehlszeilenclient, die GUI des Clients für Sichern/Archivieren und die Web-Client-GUI dennoch, Sitzungen einzuleiten.
Windows-BetriebssystemeWenn die Serveroption AUTHENTICATION auf LDAP gesetzt ist, geben Sie für die Clientoption sessioninitiation nicht serveronly an; andernfalls können keine Zeitpläne ausgeführt werden.

Beispiele

Optionsdatei:
```
sessioninitiation serveronly
```
Befehlszeile:
```
schedule -sessioninitiation=serveronly
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Setwindowtitle

Verwenden Sie die Option setwindowtitle, um den Titel des Befehlsfensters für den Verwaltungsclient während der Verarbeitung zu ändern.

Wenn Sie beispielsweise den Befehl des Verwaltungsclients (dsmadmc) auf dem Clientknoten ausführen und der Verwaltungsclient die Verbindung zum IBM Spectrum Protect-Server herstellt, wird im Titel des Befehlsfensters der folgende Text angezeigt:

```
VERBUNDEN MIT SERVER: Servername(Server-Hostname)
```

Dabei ist *Servername* der Name des IBM Spectrum Protect-Servers und *Server-Hostname* der Hostname des IBM Spectrum Protect-Servers.

Wenn Sie die Option setwindowtitle verwenden, wird jeder benutzerdefinierte Titel des Befehlsfensters überschrieben. Nachdem die Verbindung zwischen dem Verwaltungsclient und dem IBM Spectrum Protect-Server getrennt wurde, wird der Fenstertitel auf den benutzerdefinierten Fenstertitel zurückgesetzt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeUnter AIX-, Linux- und Oracle Solaris-Betriebssystemen wird der Titel des Terminalfensters auf den Titel "Terminal" zurückgesetzt, nachdem die Verbindung zum Server getrennt wurde.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) oder die Clientsystemoptionsdatei (dsm.sys) ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                    .-No--.
>>-SETWINDOWTITLE--+-----+-----------------------------------><
                    '-Yes-'
```

Parameter

No
: Der Titel des Befehlsfensters für den Verwaltungsclient wird während der Verarbeitung nicht geändert. Dieser Parameter ist der Standardwert.

Yes
: Der IBM Spectrum Protect-Servername und der Host-Server-Name werden im Titel des Befehlsfensters für den Verwaltungsclient angezeigt.

Beispiele

Optionsdatei:

```
SETWINDOWTITLE YES
```

Befehlszeile:

```
-setwindowtitle=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Shmport

Die Option shmport gibt die TCP/IP-Anschlussadresse eines Servers an, wenn gemeinsam genutzter Speicher verwendet wird. Alle Übertragungen mit gemeinsam genutztem Speicher starten mit einer TCP/IP-Verbindung.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeAnmerkung: Der für die Option shmport in der Datei dsm.sys angegebene Wert muss mit dem Wert übereinstimmen, der für shmport in der Serveroptionsdatei angegeben ist.
 Windows-BetriebssystemeAnmerkung: Der für die Option shmport in der Clientoptionsdatei (dsm.opt) angegebene Wert muss mit dem Wert übereinstimmen, der für shmport in der Serveroptionsdatei angegeben ist.

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

 Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-SHMPort-- --Anschlussnummer--------------------------------><
```

Parameter

Anschlussnummer
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeGibt die Anschlussnummer an. Sie können einen Wert zwischen 1000 und 32767 angeben. Der Standardwert ist 1510.
 Windows-BetriebssystemeGibt die Anschlussnummer an. Sie können einen Wert zwischen 1 und 32767 angeben. Der Standardwert ist 1510.

Beispiele

Optionsdatei:

```
shmport 1580
```

Befehlszeile:

Nicht zutreffend.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Showmembers

Verwenden Sie die Option showmembers, um alle Member einer Gruppe anzuzeigen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeSie können die Option showmembers in den Befehlen query group und restore group verwenden.

 Windows-BetriebssystemeSie können die Option showmembers in den Befehlen query group, query systemstate und restore group verwenden.

Die Option showmembers ist mit der Option inactive nicht gültig. Um Member in einer Gruppe anzuzeigen, die zurzeit nicht aktiv sind, die Optionen pitdate und pittime verwenden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist für alle UNIX- und Linux-Clients außer Mac OS X gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Syntax

```
>>-SHOWMembers-------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Befehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
restore group /virtfs/* -pick -showmembers
```

Windows-Betriebssysteme

```
restore group {virtfs}\* -pick -showmembers
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

Skipacl

Mit der Option skipacl können Sie ACL-Daten während einer Sicherungs- oder Archivierungsoperation einschließen oder ausschließen (ACL = Access Control List, Zugriffssteuerungsliste). ACL-Daten werden standardmäßig eingeschlossen.

Wenn diese Option auf yes gesetzt ist, schließt der Client für Sichern/Archivieren bei der Sicherung oder Archivierung von Dateien und Verzeichnissen keine ACL-Daten ein. Der Standardwert ist no. Dadurch ist es möglich, die ACL-Daten beim Kopieren von Objekten auf den Server einzuschließen. Sie sollten die Option skipacl nur dann auf yes setzen, wenn im Dateisystem keine Zugriffssteuerungslisten definiert sind oder wenn Sie sicher sind, dass Sie die ACL-Daten nicht benötigen, wenn die Dateien abgerufen oder zurückgeschrieben werden.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig. Wenn skipacl auf Linux- und AIX-Systemen auf yes gesetzt wird, werden auch die erweiterten Attribute übergangen.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

```
            .-No--.
>>-SKIPACL--+-----+-------------------------------------------><
            '-Yes-'
```

Parameter

No
: Bei der Angabe No werden die ACL-Daten gesichert. Dies ist der Standardwert.

Yes
: Bei der Angabe Yes werden die ACL-Daten nicht gesichert und können folglich nicht zurückgeschrieben werden. skipacl=yes überschreibt die Einstellungen für skipaclupdatecheck.

Beispiele

Optionsdatei:

```
skipacl yes
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme

Skipaclupdatecheck

Die Option skipaclupdatecheck inaktiviert Kontrollsummen- und Größenvergleiche von ACL-Daten.

Wird diese Option auf yes gesetzt (der Standardwert ist no), führt der Client für Sichern/Archivieren vor oder nach einer Sicherung und während der Teilsicherungsverarbeitung (ACL-Kontrollsumme von vorheriger Sicherung und aktueller ACL) keine Kontrollsummen- und Größenvergleiche durch, um ACL-Aktualisierungen zu ermitteln. Aktuelle ACL-Daten werden jedoch gesichert, wenn die Datei aus anderen Gründen zum Sichern ausgewählt wird. Werden nur die ACLs für eine Datei aktualisiert, wird bei der nächsten Teilsicherung diese ACL-Aktualisierung nicht erkannt und die Datei wird nicht gesichert.

Unterstützte Clients

Diese Option ist für alle UNIX- und Linux-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

```
                        .-No--.
>>-SKIPACLUPdatecheck--+-----+---------------------------------><
                        '-Yes-'
```

Parameter

No
: Wenn Sie No angeben, führt der Client vor und nach einer Sicherung und während der Teilsicherungsverarbeitung Kontrollsummen- und Größenvergleiche der ACL-Daten durch. Dies ist der Standardwert.

Yes
: Wenn Sie Yes angeben, führt der Client keine Kontrollsummen- und Größenvergleiche der ACL-Daten durch.

Beispiele

Optionsdatei:
```
skipaclup yes
```

Windows-Betriebssysteme

Skipmissingsyswfiles

Verwenden Sie die Option skipmissingsyswfiles, um anzugeben, ob der Client für Sichern/Archivieren bestimmte fehlende VSS Writer-Dateien überspringt und die Systemstatussicherung fortsetzt.

Wenn die Option skipmissingsyswfile auf 'yes' gesetzt wird, werden bestimmte VSS Writer-Dateien übersprungen, die bei einer Systemstatussicherung nicht gefunden werden. Diese Option ist nur für fehlende Dateien der folgenden VSS Writer wirksam:

- System Writer
- Windows Deployment Service Writer
- Event Log Writer

Beachten Sie die folgenden Hinweise, bevor Sie die Option skipmissingsyswfile verwenden:

- Wird die Option skipmissingsyswfile auf *yes* gesetzt, können Sicherungen, die mit vorherigen Versionen des Clients für Sichern/Archivieren fehlgeschlagen sind, möglicherweise ausgeführt werden.
- Es besteht ein geringes Risiko einer inkonsistenten Sicherung, da eine Datei übersprungen wird.
- Dieses Risiko wird durch die folgenden Faktoren minimiert:
  - Die Sicherung kann nur ausgeführt werden, wenn das System aktiv ist.
  - Kritische Systemdateien sind durch Microsoft Windows gegen Löschen geschützt.

Unterstützte Clients

Diese Option ist für Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                          .-Yes-.
>>-SKIPMISSingsyswfiles--+-----+-------------------------------><
                          '-No--'
```

Parameter

Yes
: Gibt an, dass der Client für Sichern/Archivieren bestimmte Dateien überspringen soll, die bei der Systemstatussicherung nicht gefunden werden. Die nicht gefundenen Dateien werden sowohl im Fehlerprotokoll als auch im Serveraktivitätenprotokoll protokolliert. Der endgültige Rückkehrcode wird auf 8 gesetzt. Dies ist der Standardwert.

No
: Gibt an, dass der Client für Sichern/Archivieren die Sicherung stoppen soll, wenn Dateien bei der Systemstatussicherung nicht gefunden werden. Die nicht gefundenen Dateien werden im Fehlerprotokoll und im Serveraktivitätenprotokoll protokolliert. Der endgültige Rückkehrcode ist 12.

Beispiele

Optionsdatei:

```
SKIPMISSingsyswfiles yes
```

Befehlszeile:

```
 -SKIPMISSingsyswfiles=yes
```

Zugehörige Verweise:
Backup Systemstate
Windows-Betriebssysteme

Skipntpermissions

Die Option skipntpermissions übergeht die Verarbeitung der Sicherheitsinformationen für Windows-Dateisysteme.

Sie können diese Option für Teilsicherungen, selektive Sicherungen sowie Zurückschreibungs-, Archivierungs- und Abrufoperationen verwenden.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie ist für folgende Befehle gültig: incremental, selective, restore, archive und retrieve. Sie können diese Option auch auf der Registerkarte Allgemein des Profileditors definieren.

Syntax

```
                          .-No--.
>>-SKIPNTPermissions--+-----+-----------------------------------><
                      '-Yes-'
```

Parameter

No
: Bei der Angabe No werden die Sicherheitsinformationen für das Windows-Dateisystem gesichert, zurückgeschrieben, archiviert oder abgerufen. Dies ist die Standardeinstellung.

Yes
: Bei der Angabe Yes werden die Sicherheitsinformationen für das Windows-Dateisystem nicht gesichert, zurückgeschrieben, archiviert oder abgerufen.

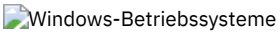
Beispiele

Optionsdatei:

```
skipntp yes
```

Befehlszeile:

```
-skipntp=yes
```



Skipntsecuritycrc

Die Option skipntsecuritycrc steuert die Berechnung der zyklischen Blockprüfung (CRC = Cyclic Redundancy Check) für einen Vergleich der Windows NTFS- oder ReFS-Sicherheitsinformationen während der folgenden Operationen: Teilsicherung, selektive Sicherung, Archivierung, Zurückschreibung oder Abruf.

Wenn Sie die Option skipntsecuritycrc auf no (den Standardwert) setzen, kann die Leistung langsamer sein, weil das Programm alle Sicherheitsdeskriptoren abrufen muss.

Diese Option ist in den folgenden Befehlen zu verwenden:

- archive
- incremental
- restore
- retrieve
- selective

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                      .-No--.
>>-SKIPNTSecuritycrc--+-----+-----------------------------------><
                      '-Yes-'
```

Parameter

No
: Bei der Angabe No wird die CRC während einer Sicherung generiert. Dies ist die Standardeinstellung.

Yes
: Bei der Angabe Yes wird die CRC während einer Sicherung nicht generiert. Alle Berechtigungen werden gesichert; das Programm kann jedoch während der nächsten Teilsicherung nicht feststellen, ob sich die Berechtigungen geändert haben. Wenn die Option skipntpermissions auf yes gesetzt ist, wird die Option skipntsecuritycrc nicht angewendet.

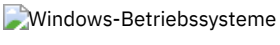
Beispiele

Optionsdatei:

```
skipnts no
```

Befehlszeile:

```
-skipnts=no
```



Skipsystemexclude

Verwenden Sie die Option skipsystemexclude, um anzugeben, wie Ausschlussanweisungen für bestimmte Betriebssystemdateien, die der IBM Spectrum Protect for Virtual Environments-Client standardmäßig überspringt, verarbeitet werden sollen.

Bestimmte Windows-Betriebssystemdateien, die für die Systemwiederherstellung normalerweise nicht erforderlich sind, werden von IBM Spectrum Protect for Virtual Environments-Clients während Sicherungsoperationen für die virtuelle Maschine (VM) standardmäßig übersprungen. Zu diesen Dateien können Windows-Systemdateien, temporäre Internetdateien und Dateien im Papierkorb gehören.

Mit dieser Option können Sie die Verarbeitung von Ausschlussanweisungen für diese Betriebssystemdateien überspringen. Die Nichtverarbeitung dieser Ausschlussanweisungen kann dazu beitragen, die erforderliche Sicherungszeit für virtuelle Maschinen zu verringern.

Unterstützte Clients

Diese Option ist nur für IBM Spectrum Protect for Virtual Environments-Clients in Windows-Betriebssystemen gültig.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile gültig. Diese Option kann in der Clientoptionsgruppe auf dem IBM Spectrum Protect-Server definiert werden. Die Option wird bei allen anderen Clients ignoriert.

Syntax

```
                        .-Yes-.
>>-SKIPSYSTemexclude--+-----+-----------------------------------><
                      '-No--'
```

Parameter

Yes
: Geben Sie diesen Parameter an, um die Verarbeitung von Ausschlussanweisungen für bestimmte Windows-Betriebssystemdateien während VM-Sicherungsoperationen zu überspringen. Dieser Parameter ist der Standardwert.

No
: Geben Sie diesen Parameter an, um Ausschlussanweisungen für Windows-Betriebssystemdateien zu verarbeiten. Wenn Sie diesen Parameter auswählen und eine Dateisicherung des Hyper-V-Hosts ausführen, werden die Betriebssystemdateien ausgeschlossen.

Beispiele

Optionsdatei

```
SKIPSYSTemexclude yes
```

Befehlszeile

```
dsmc backup vm -SKIPSYST=yes
dsmc incr -skipsyst=no
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Snapdiff

Die Verwendung der Option snapdiff mit dem Befehl incremental optimiert den Teilsicherungsprozess. Der Befehl führt eine Teilsicherung der Dateien aus, die von NetApp als geändert zurückgemeldet wurden, und durchsucht nicht den gesamten Datenträger nach geänderten Dateien.

 Windows-BetriebssystemeDie Option snapdiff (Momentaufnahmedifferenz) wird für das Sichern der Datenträger von NAS-/N-Series-Dateiservern verwendet, die über NFS oder CIFS angeschlossen sind.

 Windows-BetriebssystemeEinschränkung: Keine der vordefinierten NetApp-Freigaben, auch nicht `C$`, funktioniert mit der IBM Spectrum Protect-Option für die Momentaufnahmedifferenz, da der Client für Sichern/Archivieren ihre Mountpunkte nicht über das Programm bestimmen kann.

Sie müssen eine Benutzer-ID und ein Kennwort auf dem Client für Sichern/Archivieren konfigurieren, um die Momentaufnahmedifferenzverarbeitung zu aktivieren.

Verwenden Sie diese Option bei einer Teilsicherung eines Datenträgers eines NAS-Dateiservers anstelle einer einfachen Teilsicherung oder einer Teilsicherung mit der Option snapshotroot, wenn auf dem NAS-Dateiserver ONTAP 7.3.0 oder höher ausgeführt wird. Verwenden Sie die Optionen snapdiff und snapshotroot nicht zusammen.

 Linux-BetriebssystemeEinschränkung: Teilsicherungen mit Momentaufnahmedifferenzverarbeitung sind nur für den Linux x86_64-Client für Sichern/Archivieren verfügbar.

Bei der ersten Ausführung einer Teilsicherung mit der Option für die Momentaufnahmedifferenz wird eine Momentaufnahme (die Basismomentaufnahme) erstellt und eine traditionelle Teilsicherung ausgeführt, wobei diese Momentaufnahme als Quelle verwendet wird. Der Name der erstellten Momentaufnahme wird in der IBM Spectrum Protect-Serverdatenbank aufgezeichnet. Die erste Teilsicherung muss fehlerfrei ausgeführt werden, damit bei der nächsten Sicherungsoperation die Momentaufnahmedifferenzverarbeitung verwendet werden kann.

Bei der zweiten Ausführung einer Teilsicherung mit dieser Option wird entweder eine neue Momentaufnahme erstellt oder eine vorhandene Momentaufnahme verwendet (abhängig vom Wert für die Option diffsnapshot), um die Unterschiede zwischen diesen beiden Momentaufnahmen zu ermitteln. Die zweite Momentaufnahme wird als *diffsnapshot* (Differenzmomentaufnahme) bezeichnet. Anschließend sichert der Client die Dateien, die von NetApp als geändert aufgelistet werden, über eine Teilsicherung auf dem IBM Spectrum Protect-Server. Das Dateisystem, das für die Momentaufnahmedifferenzverarbeitung ausgewählt wird, muss an das Stammverzeichnis des Datenträgers angehängt sein. Sie können die Option snapdiff nicht für Dateisysteme verwenden, die nicht an das Stammverzeichnis des Datenträgers angehängt sind. Nach der Sicherung

der Daten mit der Option snapdiff wird die Momentaufnahme, die als Basismomentaufnahme verwendet wurde, aus dem Momentaufnahmeverzeichnis gelöscht.

 Auf Windows-Systemen befindet sich das Momentaufnahmeverzeichnis in ~snapshot.

 Auf Linux-Systemen befindet sich das Momentaufnahmeverzeichnis in .snapshot.

Der Client löscht nur Momentaufnahmen, die er selbst erstellt hat.

Wenn eine Teilsicherungsoperation unter Verwendung der Momentaufnahmedifferenz beendet wird, stellt der Client sicher, dass nur die zuletzt registrierte Basismomentaufnahme auf dem Dateiserverdatenträger verbleibt. Alle Momentaufnahmen, die durch eine Momentaufnahmedifferenzteilsicherung auf dem Client für Sichern/Archivieren erstellt werden, beginnen mit den Zeichen "TSM_". Wenn Sie Momentaufnahmen mit einem anderen Momentaufnahmetool als dem Client für Sichern/Archivieren erstellen, müssen Sie sicherstellen, dass nicht die Zeichenfolge "TSM_" am Anfang des Momentaufnahmenamens verwendet wird. Wenn die Momentaufnahmenamen mit "TSM_" beginnen, werden die Dateien gelöscht, wenn der Client die nächste Teilsicherungsoperation unter Verwendung der Momentaufnahmedifferenz einleitet.

Um eine Momentaufnahmedifferenzteilsicherung von schreibgeschützten NetApp-Dateiserverdatenträgern auszuführen, muss die Option useexistingbase angegeben werden, um zu verhindern, dass eine Momentaufnahme auf dem schreibgeschützten Datenträger erstellt wird. Geben Sie außerdem den Namen der zu verwendenden Basismomentaufnahme (Option basesnapshotname) und den Namen der zu verwendenden Differenzmomentaufnahme (Option diffsnapshotname) an.

Bei NAS- und N-Series-Dateiservern, auf denen ONTAP 7.3.0 oder höher ausgeführt wird, können Sie die Option createnewbase verwenden, um alle Dateien zu sichern, die aufgrund einer der folgenden Ursachen übersprungen wurden:

- Eine Datei wird ausgeschlossen, da die Einschluss-/Ausschlussdatei über eine Ausschlussregel verfügt, die wirksam ist. Eine Datei wird ausgeschlossen, wenn Sie die Einschluss-/Ausschlussdatei nicht geändert, aber die Regel entfernt haben, die die Datei ausgeschlossen hat. Die NetApp-API erkennt nur Dateiänderungen zwischen zwei Momentaufnahmen, aber keine Änderungen an der Einschluss-/Ausschlussdatei.
- Wenn Sie der Optionsdatei eine Einschlussanweisung hinzugefügt haben, tritt diese Einschlussoption erst in Kraft, wenn NetApp feststellt, dass die Datei sich geändert hat. Der Client überprüft während einer Sicherung nicht jede Datei auf dem Datenträger.
- Sie haben mit dem Befehl dsmc delete backup explizit eine Datei aus dem IBM Spectrum Protect-Serverbestand gelöscht. NetApp erkennt nicht, dass eine Datei manuell auf dem Server gelöscht wurde. Daher verbleibt die Datei ungeschützt im IBM Spectrum Protect-Speicher, bis sie auf dem Datenträger geändert wird, diese Änderung von NetApp festgestellt wird und der Client angewiesen wird, die Datei erneut zu sichern.
- Maßnahmenänderungen wie die Änderung der Maßnahme von mode=modified in mode=absolute werden nicht festgestellt.
- Der gesamte Dateibereich wird aus dem IBM Spectrum Protect-Datenbestand gelöscht. Diese Aktion bewirkt, dass die Option für die Momentaufnahmedifferenz eine Momentaufnahme erstellt, die als Quelle verwendet wird, und dass eine vollständige Teilsicherung ausgeführt wird.
- Eine Datei wird von der Sicherung ausgeschlossen, da der Dateiname ein Zeichen enthält, das im 7-Bit-ASCII-Zeichensatz nicht enthalten ist. Die Option createnewbase erstellt eine Basismomentaufnahme und verwendet sie als Quelle für die Ausführung einer vollständigen Teilsicherung.NetApp steuert, was als geändertes Objekt angesehen wird.

Tipp: Sie können mit der Option snapdiffhttps Momentaufnahmedifferenzteilsicherungen von NetApp-Dateiservern mit einer sicheren HTTPS-Verbindung ausführen. Damit Momentaufnahmedifferenzteilsicherungen erfolgreich ausgeführt werden konnten, musste in früheren Releases des Clients für Sichern/Archivieren HTTP-Verwaltungszugriff auf dem NetApp-Dateiserver aktiviert sein. Mit der Option snapdiffhttps können Sie eine sichere Verwaltungssitzung mit dem NetApp-Dateiserver aufbauen, ohne dass hierfür der HTTP-Verwaltungszugriff auf dem Dateiserver aktiviert sein muss.
In der Liste der vom traditionellen Befehl incremental verwendeten Optionen zeigt die letzte Spalte die Interaktion jeder Option mit der Option snapdiff an. Die Definitionen der Begriffe *gültig*, *nicht gültig* und *keine Auswirkung* lauten wie folgt:

Gültig
: Die Verarbeitung verläuft normal, wenn die Option verwendet wird.

Nicht gültig
: Wird die Option mit der Option snapdiff verwendet, wird eine Fehlernachricht generiert.

Keine Auswirkung
: Die Option kann verwendet werden; sie wird jedoch ignoriert.

Tabelle 1. Befehl Incremental: Zugehörige Optionen

Option	Verwendung	Mit snapdiff
AIX-BetriebssystemeLinux-Betriebssystemeasnodename	 AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
 Windows-Betriebssystemeasnodename	 Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig

Option	Verwendung	Mit snapdiff
AIX-BetriebssystemeLinux-Betriebssystemeautomount	AIX-Betriebssysteme Linux-BetriebssystemeClientoptionsdatei (dsm.opt).	AIX-Betriebssysteme Linux-Betriebssysteme Keine Auswirkung
Windows-Betriebssystemeautofsrename	Windows-BetriebssystemeNur Clientoptionsdatei (dsm.opt).	Windows-Betriebssysteme Keine Auswirkung
AIX-BetriebssystemeLinux-Betriebssystemebasesnapshotname	AIX-Betriebssysteme Linux-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemebasesnapshotname	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemechangingretries	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Keine Auswirkung
Windows-Betriebssystemechangingretries	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Keine Auswirkung
Windows-Betriebssystemecompressalways	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemecompressalways	AIX-Betriebssysteme Linux-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemecompression	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemecompression	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssysteme Windows-Betriebssystemecreatenewbase	AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeNur in der Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme Gültig
diffsnapshot	Nur in der Befehlszeile.	Gültig
AIX-BetriebssystemeLinux-Betriebssystemediffsnapshotname	AIX-Betriebssysteme Linux-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemediffsnapshotname	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
dirsonly	Nur in der Befehlszeile.	Gültig

Option	Verwendung	Mit snapdiff
Windows-Betriebssystemedomain	Windows-BetriebssystemeNur Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemedomain	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys), Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemeefsdecrypt	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys), Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Keine Auswirkung
AIX-BetriebssystemeLinux-Betriebssystemeenablelanfree	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemeenablelanfree	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemeencryptiontype	AIX-Betriebssysteme Linux-BetriebssystemeSystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemeencryptiontype	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt).	Windows-Betriebssysteme Gültig
Windows-Betriebssystemeencryptkey	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt).	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemeencryptkey	AIX-Betriebssysteme Linux-BetriebssystemeSystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemeexclude.fs.nas	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys).	AIX-Betriebssysteme Linux-Betriebssysteme Keine Auswirkung
Windows-Betriebssystemeexclude.fs.nas	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt).	Windows-Betriebssysteme Keine Auswirkung
filelist	Nur in der Befehlszeile.	Nicht gültig
filesonly	Nur in der Befehlszeile.	Gültig
AIX-BetriebssystemeLinux-Betriebssystemefollowsymboliclink	AIX-Betriebssysteme Linux-BetriebssystemeClientoptionsdatei (dsm.opt).	AIX-Betriebssysteme Linux-Betriebssysteme Keine Auswirkung
AIX-BetriebssystemeLinux-Betriebssystemeinclude.fs.nas	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Keine Auswirkung

Option	Verwendung	Mit snapdiff
Windows-Betriebssystemeinclude.fs.nas	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Keine Auswirkung
AIX-BetriebssystemeLinux-Betriebssystemeinclexcl	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys).	AIX-Betriebssysteme Linux-Betriebssysteme Gültig, jedoch nur, wenn NetApp eine Dateiänderung feststellt.
Windows-Betriebssystemeinclexcl	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt).	Windows-Betriebssysteme Gültig, jedoch nur, wenn NetApp eine Dateiänderung feststellt.
incrbydate	Nur in der Befehlszeile.	Nicht gültig
Windows-Betriebssystememememoryefficientbackup	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt), Server oder Befehlszeile.	Windows-Betriebssysteme Keine Auswirkung
AIX-BetriebssystemeLinux-Betriebssysteme memoryefficientbackup	AIX-Betriebssysteme Linux-BetriebssystemeDiese Option ist sowohl in dsm.sys als auch in dsm.opt zulässig; der Wert in dsm.opt wird jedoch ignoriert, wenn die Option auch in dsm.sys vorhanden ist. Sie können diese Option auch innerhalb einer Serverzeilengruppe oder in der Anfangsbefehlszeile verwenden.	AIX-Betriebssysteme Linux-Betriebssysteme Keine Auswirkung
monitor	Nur in der Befehlszeile.	Nicht gültig
AIX-BetriebssystemeLinux-Betriebssystemenojournal	AIX-Betriebssysteme Linux-BetriebssystemeNur in der Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Nicht gültig
Windows-Betriebssystemenojournal	Windows-BetriebssystemeNur in der Befehlszeile.	Windows-Betriebssysteme Nicht gültig
AIX-BetriebssystemeLinux-Betriebssystemepostsnapshotcmd	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder mit der Option include.fs.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemepostsnapshotcmd	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder mit der Option include.fs.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssysteme preservelastaccessdate	AIX-Betriebssysteme Linux-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemepreservelastaccessdate	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemepresnapshotcmd	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder mit der Option include.fs.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig

Option	Verwendung	Mit snapdiff
Windows-Betriebssystemepresnapshotcmd	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder mit der Option include.fs.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemeremoveoperandlimit	AIX-Betriebssysteme Linux-BetriebssystemeNur in der Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemeresetarchiveattribute	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt).	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemeskipaclupdatecheck	AIX-Betriebssysteme Linux-BetriebssystemeClientoptionsdatei (dsm.opt).	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemeskipntpermissions	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
Windows-Betriebssystemeskipntsecuritycrc	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssysteme Windows-Betriebssystemesnapdiffhttps	AIX-Betriebssysteme Linux-Betriebssysteme Windows-BetriebssystemeNur in der Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemesnapshotcachesize	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder mit der Option include.fs.	AIX-Betriebssysteme Linux-Betriebssysteme Keine Auswirkung
AIX-BetriebssystemeLinux-Betriebssystemesnapshotproviderfs	AIX-Betriebssysteme Linux-BetriebssystemeSystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder mit der Option include.fs.	AIX-Betriebssysteme Linux-Betriebssysteme Nicht gültig
Windows-Betriebssystemesnapshotproviderfs	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder mit der Option include.fs.	Windows-Betriebssysteme Nicht gültig
AIX-BetriebssystemeLinux-Betriebssysteme snapshotproviderimage	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder mit der Option include.image.	AIX-Betriebssysteme Linux-Betriebssysteme Nicht gültig
Windows-Betriebssystemesnapshotproviderimage	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder mit der Option include.image.	Windows-Betriebssysteme Nicht gültig
snapshotroot	Nur in der Befehlszeile.	Nicht gültig
subdir	Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Nicht gültig
AIX-BetriebssystemeLinux-Betriebssystemetapeprompt	AIX-Betriebssysteme Linux-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig

Option	Verwendung	Mit snapdiff
Windows-Betriebssystemetapeprompt	Windows-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.	Windows-Betriebssysteme Gültig
AIX-BetriebssystemeLinux-Betriebssystemetoc	AIX-Betriebssysteme Linux-BetriebssystemeNur in der Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Nicht gültig
Windows-Betriebssystemetoc	Windows-BetriebssystemeNur in der Befehlszeile.	Windows-Betriebssysteme Nicht gültig
AIX-BetriebssystemeLinux-Betriebssystemeuseexistingbase	AIX-Betriebssysteme Linux-BetriebssystemeNur in der Befehlszeile.	AIX-Betriebssysteme Linux-Betriebssysteme Gültig
Windows-Betriebssystemeuseexistingbase	Windows-BetriebssystemeNur in der Befehlszeile.	Windows-Betriebssysteme Gültig
virtualfsname	Nur in der Befehlszeile.	Nicht gültig
AIX-BetriebssystemeLinux-Betriebssystemevirtualmountpoint	AIX-Betriebssysteme Linux-Betriebssysteme Clientsystemoptionsdatei (dsm.sys).	AIX-Betriebssysteme Linux-Betriebssysteme Nicht gültig

Unterstützte Clients

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

Syntax

```
>>-SNAPDiff---------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeEine Teilsicherung unter Verwendung der Momentaufnahmedifferenz für das über NFS-Mount angehängte Dateisystem `/vol/vol1` ausführen, das sich auf dem Dateiserver `homestore.example.com` befindet. Dabei ist `/net/home1` der Mountpunkt von `/vol/vol1`.

Linux-Betriebssysteme
```
incremental -snapdiff -diffsnapshot=latest /net/home1
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeEine Teilsicherung unter Verwendung der Momentaufnahmedifferenz auf der Basis einer Momentaufnahme ausführen, die von dem gemeinsam genutzten Netzbereich (Netzwerkfreigabe) `//homestore.example.com/vol/vol1` erstellt wurde, der als Laufwerk `H:` angehängt ist. Dabei ist `homestore.example.com` ein Dateiserver.

Windows-Betriebssysteme
```
incremental -snapdiff H:
```

Windows-BetriebssystemeEine Teilsicherung unter Verwendung der Momentaufnahmedifferenz auf der Basis einer Momentaufnahme ausführen, die von dem gemeinsam genutzten Netzbereich (Netzwerkfreigabe) `//homestore.example.com/vol/vol1` erstellt wurde, der als Laufwerk `H:` angehängt ist. Dabei ist `homestore.example.com` ein Dateiserver. Der Wert `LATEST` der Option -diffsnapshot bedeutet, dass bei der Operation die letzte Momentaufnahme (die aktive Momentaufnahme) für Datenträger `H:` verwendet wird.

Windows-Betriebssysteme
```
incremental -snapdiff H: -diffsnapshot=latest
```

Befehlszeile:

Eine einmalige vollständige Teilsicherung ausführen, nachdem festgestellt wurde, dass der NetApp-Dateiserver von einer Version, die keine Unicode-Dateinamen unterstützt hat, auf einen Unicode-fähigen Dateiserver migriert wurde. AIX-Betriebssysteme Linux-Betriebssysteme

```
dsmc incremental -snapdiff -createnewbase=migrate /net/home1
```

Windows-Betriebssysteme

```
dsmc incremental -snapdiff -createnewbase=migrate h:
```

Eine Teilsicherung unter Verwendung der Momentaufnahmedifferenz ausführen, nachdem festgestellt wurde, dass der NetApp-Dateiserver von einer Version, die keine Unicode-Dateinamen unterstützt hat, auf einen Unicode-fähigen Dateiserver migriert wurde. Dieser Befehl unterdrückt die Warnung. AIX-BetriebssystemeLinux-Betriebssysteme

```
dsmc incremental -snapdiff -createnewbase=ign /net/home1
```

Windows-Betriebssysteme

```
dsmc incremental -snapdiff -createnewbase=ign h:
```

Eine vollständige Teilsicherung ausführen, da einige Einschluss- oder Ausschlussänderungen vorgenommen wurden:
AIX-BetriebssystemeLinux-Betriebssysteme

```
dsmc incremental -snapdiff -createnewbase=yes /net/home1
```

Windows-Betriebssysteme

```
dsmc incremental -snapdiff -createnewbase=yes h:
```

Zugehörige Konzepte:
Linux-BetriebssystemeMomentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung
SnapMirror-Unterstützung für momentaufnahmegestützte progressive Teilsicherung von NetApp (snapdiff)
Zugehörige Tasks:
NetApp und IBM Spectrum Protect für Teilsicherungen unter Verwendung der Momentaufnahmedifferenz konfigurieren
Zugehörige Verweise:
Snapdiffhttps
Basesnapshotname
Diffsnapshotname
Useexistingbase
Diffsnapshot
Set Password
Linux-BetriebssystemeWindows-Betriebssysteme

Snapdiffchangelogdir

Die Option snapdiffchangelogdir definiert die Position, an der der Client persistente Änderungsprotokolle speichert, die für Momentaufnahmedifferenzsicherungsoperationen verwendet werden.

Wichtig: Wenn Sie zuvor Momentaufnahmedifferenzsicherungen mit einem Client für Sichern/Archivieren einer älteren Version als Version 8.1.2 verwendet haben, ist die erste Momentaufnahmedifferenzsicherung, die Sie mit dem Client der Version 8.1.2 oder höher ausführen, eine progressive vollständige Teilsicherung. Um diese progressive vollständige Teilsicherung zu verhindern, versetzen Sie die vorhandenen Änderungsprotokolldateien von der alten Position, die durch die Option stagingdirectory angegeben wird, an die neue Position, die durch die Option snapdiffchangelogdir angegeben wird, bevor Sie die erste Momentaufnahmedifferenzsicherung ausführen.
Führen Sie beispielsweise den folgenden Kopierbefehl aus: Linux-Betriebssysteme

```
cp -R /tmp/TSM/TsmSnapDiff /opt/tivoli/tsm/client/ba/TsmSnapDiff
```

Windows-Betriebssysteme

```
xcopy C:\Users\Bob\AppData\Local\Temp\TSM\TsmSnapDiff
"C:\Programme\Tivoli\TSM\baclient\TsmSnapDiff" /s /y
```

Die Änderungsprotokolldateien haben die folgenden Benennungsmuster: Linux-Betriebssysteme

```
.../TSM/TsmSnapDiff/.TsmSnapdiffChangeLogs/NetApp-Dateiserver/
SnapdiffChangeLog__Datenträgername__.tsmDB
.../TSM/TsmSnapDiff/.TsmSnapdiffChangeLogs/NetApp-Dateiserver/
SnapdiffChangeLog__Datenträgername__.tsmDB.Lock
```

Windows-Betriebssysteme

```
...\TSM\TsmSnapDiff\.TsmSnapdiffChangeLogs\NetApp-Dateiserver\
SnapdiffChangeLog__Datenträgername__.tsmDB
...\TSM\TsmSnapDiff\.TsmSnapdiffChangeLogs\NetApp-Dateiserver\
SnapdiffChangeLog__Datenträgername__.tsmDB.Lock
```

Hierbei gilt Folgendes:

- *NetApp-Dateiserver* ist der Hostname oder die IP-Adresse der Storage Virtual Machine (SVM) des Cluster-Management-Servers oder des 7-Mode-Dateiservers an.

- *Datenträgername* ist der Datenträger, der geschützt werden soll.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Wird snapdiffchangelogdir in der Befehlszeile angegeben, überschreibt diese Angabe die Werte, die in der Optionsdatei angegeben sind. Sie können diese Option auf der Registerkarte Allgemein des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Wird snapdiffchangelogdir in der Befehlszeile angegeben, überschreibt diese Angabe die Werte, die in der Optionsdatei angegeben sind. Sie können diese Option auf der Registerkarte Allgemein des Profileditors definieren.

Syntax

```
>>-SNAPDIFFCHANGELOGDir--Pfad----------------------------------><
```

Parameter

Pfad

Gibt den Verzeichnispfad an, in dem der Client persistente Änderungsprotokolle für Momentaufnahmedifferenzsicherungsoperationen speichert. Wenn Sie die Option snapdiffchangelogdir nicht angeben, verwendet der Client das Verzeichnis, in dem der Client installiert ist. Das Standardinstallationsverzeichnis ist: Linux-Betriebssysteme

```
/opt/tivoli/tsm/client/ba
```

Windows-Betriebssysteme

```
C:\Programme\Tivoli\TSM\baclient
```

Der exakte Name der Änderungsprotokolldatei hat das folgende Format: Linux-Betriebssysteme

```
Verzeichnis_des_Momentaufnahmedifferenzänderungsprotokolls/TsmSnapDiff/
.TsmSnapdiffChangeLogs/NetApp-Dateiserver/
SnapdiffChangeLog__Datenträgername__.tsmDB
```

Windows-Betriebssysteme

```
Verzeichnis_des_Momentaufnahmedifferenzänderungsprotokolls\TsmSnapDiff\
.TsmSnapdiffChangeLogs\NetApp-Dateiserver\
SnapdiffChangeLog__Datenträgername__.tsmDB
```

Hierbei gilt Folgendes:

- *Verzeichnis_des_Momentaufnahmedifferenzänderungsprotokolls* ist der Name des Verzeichnisses zum Speichern der Änderungsprotokolle für Momentaufnahmedifferenzsicherungen, das durch die Option snapdiffchangelogdir angegeben wird.
- *NetApp-Dateiserver* ist der Hostname oder die IP-Adresse der Storage Virtual Machine (SVM) des Cluster-Management-Servers oder des 7-Mode-Dateiservers an.
- *Datenträgername* ist der Datenträger, der geschützt werden soll.

Außerdem wird eine Sperrdatei erstellt, um zu verhindern, dass die Änderungsprotokolldatei durch unterschiedliche Momentaufnahmedifferenzsicherungen, die gleichzeitig ausgeführt werden, aktualisiert wird.
Windows-BetriebssystemeIm UNC-Format (Universal Naming Convention) muss der Pfad einen Laufwerkbuchstaben enthalten. In dem folgenden Beispiel für das UNC-Format enthält der Pfad den Laufwerkbuchstaben:

```
\\computer7\C$\tsmdata
```

Beispiele

Optionsdatei:

Linux-Betriebssystemesnapdiffchangelogdir /tmp/tsmdata
Windows-Betriebssystemesnapdiffchangelogdir c:\tsmdata

Befehlszeile:

Linux-Betriebssysteme-snapdiffchangelogd=/tmp/tsmdata
Windows-Betriebssysteme-snapdiffchangelogd="c:\tsmdata"

Zugehörige Verweise:

Diffsnapshot
Snapdiff
Linux-Betriebssysteme Windows-Betriebssysteme

Snapdiffhttps

Geben Sie die Option snapdiffhttps an, um eine sichere HTTPS-Verbindung für die Kommunikation mit einem NetApp-Dateiserver während einer Momentaufnahmedifferenzsicherung zu verwenden.

Wenn Sie diese Option angeben, kann der Client für Sichern/Archivieren eine sichere Verwaltungssitzung mit dem NetApp-Dateiserver aufbauen, ohne dass hierfür der HTTP-Verwaltungszugriff auf dem NetApp-Dateiserver aktiviert sein muss.

Wichtig: Das Standardübertragungsprotokoll, mit dem der Client für Sichern/Archivieren eine Verwaltungssitzung mit dem NetApp-Dateiserver aufbaut, ist HTTP. Damit eine sichere HTTPS-Verbindung verwendet werden kann, müssen Sie die Option snapdiffhttps bei jeder Ausführung einer Momentaufnahmedifferenzsicherung angeben.
Einschränkungen:

Für Momentaufnahmedifferenzsicherungen mit HTTPS gelten die folgenden Einschränkungen:

- Die HTTPS-Verbindung wird nur für die sichere Übertragung von Daten über die Verwaltungssitzung zwischen dem Client für Sichern/Archivieren und dem NetApp-Dateiserver verwendet. Zu den Daten der Verwaltungssitzung gehören z. B. Berechtigungsnachweise des Dateiservers, Momentaufnahmeinformationen sowie Dateinamen und Attribute, die durch den Momentaufnahmedifferenzierungsprozess generiert werden. Über die HTTPS-Verbindung werden keine normalen Dateidaten übertragen, auf die der Client über die Dateifreigabe auf dem Dateiserver zugreift. Die HTTPS-Verbindung ist auch nicht für normale Dateidaten gültig, die der Client über das normale IBM Spectrum Protect-Client/Server-Protokoll an den IBM Spectrum Protect-Server überträgt.
- Die Option snapdiffhttps gilt nicht für vFilers, da das HTTPS-Protokoll auf dem NetApp vFiler nicht unterstützt wird.
- Die Option snapdiffhttps ist nur bei Verwendung der Befehlszeilenschnittstelle verfügbar. In der grafischen Benutzerschnittstelle (GUI) des Clients für Sichern/Archivieren kann sie nicht verwendet werden.

Unterstützte Clients

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

Optionsdatei

Diese Option ist nur in der Befehlszeilenschnittstelle gültig. Sie können sie nicht in einer Clientoptionsdatei angeben.

Syntax

```
>>-SNAPDIFFHTTPS-----------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Linux-BetriebssystemeBefehlszeile:
Linux-BetriebssystemeGeben Sie den folgenden Befehl auf einem Linux-System mit einem über NFS-Mount angehängten Dateisystem `/vol/vol1` aus, das sich auf dem Dateiserver `homestore.example.com` befindet; dabei ist `/net/home1` der Mountpunkt von `/vol/vol1`.

```
dsmc incr /net/home1 -snapdiff -snapdiffhttps
```

Windows-BetriebssystemeBefehlszeile:
Windows-BetriebssystemeGeben Sie den folgenden Befehl auf einem Windows-System mit der Netzwerkfreigabe `\\netapp1\vol1` aus, wobei `netapp1` ein Dateiserver ist.

```
dsmc incr \\netapp1\vol1 -snapdiff -snapdiffhttps
```

Windows-BetriebssystemeBefehlszeile:
Windows-BetriebssystemeGeben Sie den folgenden Befehl auf einem Windows-System mit der an Laufwerk `v:` bereitgestellten Netzwerkfreigabe `\\netapp1.example.com\petevol` aus, wobei `netapp1.example.com` ein Dateiserver ist.

```
dsmc incr v: -snapdiff -snapdiffhttps
```

```
IBM Spectrum Protect
Befehlszeilenschnittstelle des Clients für Sichern/Archivieren
  Clientversion 8, Release 1, Stufe 0.0
  Clientdatum/-zeit: 09.12.2016 15:36:53
(c) Copyright IBM Corporation und andere 1990, 2016. Alle Rechte vorbehalten.

Knotenname: THINKCENTRE
Sitzung hergestellt mit Server BARKENSTEIN_SERVER1: Windows
  Serverversion 8, Release 1, Stufe 0.0
  Serverdatum/-zeit: 09.12.2016 15:36:53  Letzter Zugriff: 09.12.2016 11:21:14


Teilsicherung nach Momentaufnahmedifferenz des Datenträgers 'v:'
Verbunden mit NetApp-Dateiserver netapp1.example.com als Benutzer pete über HTTPS
NetApp Release 8.1.1RC1 7-Mode: Thu May 31 21:30:59 PDT 2012
Momentaufnahmedifferenzsicherung wird ausgeführt für Datenträger
'\\netapp1.example.com\petevol'
Differenzmomentaufnahme wird erstellt.
Basismomentaufnahme 'TSM_THIN5086B9441A1F8_PETEVOL' mit Zeitmarke 09.12.2016
15:36:53 wird verwendet
Differenzmomentaufnahme 'TSM_THIN5086B9772AF8_PETEVOL' mit Zeitmarke 09.12.2016
15:37:44 wird verwendet
Erfolgreiche Teilsicherung von '\\netapp1.example.com\petevol'
```

Zugehörige Konzepte:
Linux-BetriebssystemeMomentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung
Windows-BetriebssystemeMomentaufnahmedifferenzsicherung mit einer HTTPS-Verbindung
Zugehörige Verweise:
Snapdiff

Snapshotcachesize

Verwenden Sie die Option snapshotcachesize, um eine angemessene Cachegröße zum Erstellen der Momentaufnahme anzugeben.

AIX-BetriebssystemeLinux-BetriebssystemeDie geschätzte Größe muss ausreichen, um die Originaldatenblöcke für geänderte und gelöschte Daten für den Zeitpunkt zu speichern, zu dem die Momentaufnahme erstellt wurde.

AIX-BetriebssystemeLinux-BetriebssystemeFür eine Dateisicherung oder -archivierung auf Momentaufnahmebasis verwenden Sie die Option snapshotcachesize zusammen mit der Option include.fs oder in der Serverzeilengruppe der Datei dsm.sys.

AIX-BetriebssystemeLinux-BetriebssystemeFür Imagesicherungen auf Momentaufnahmebasis verwenden Sie die Option snapshotcachesize im Befehl backup image, mit der Option include.image oder in Ihrer Datei dsm.sys.

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeDiese Option ist *nur* für AIX- und Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeFügen Sie diese Option in die Serverzeilengruppe in der Datei dsm.sys ein. Sie können diese Option auf der Registerkarte Momentaufnahmeimage im Profileditor definieren.

Syntax

```
>>-SNAPSHOTCACHESize-- --Größe---------------------------------><
```

Parameter

AIX-BetriebssystemeLinux-Betriebssysteme

Größe
: Gibt eine entsprechende Momentaufnahmengröße zum Erstellen der Momentaufnahme an, damit die Originaldatenblöcke für geänderte und gelöschte Daten für den Zeitpunkt gespeichert werden können, als die Momentaufnahme erstellt wurde. Der Wert ist der Prozentsatz der Dateisystemgröße, die sich auf Grund der Dateisystemaktivität ändert. Der Wertebereich ist 1 bis 100 Prozent. Für AIX JFS2 und Linux beträgt der Standardwert 100 Prozent der Dateisystemgröße. Falls nicht genügend freier Speicherbereich verfügbar ist, um die Momentaufnahme zu erstellen, schlägt der Befehl mit einer Fehlernachricht fehl. Sie können dann entweder die Größe der Datenträgergruppe erhöhen oder die Operation wiederholen. Wenn Sie auf der Grundlage Ihrer Erfahrung mit der Aktivität des AIX JFS2-Dateisystems glauben, dass eine Momentaufnahmengröße von 100 Prozent nicht notwendig ist, können Sie den Wert optimieren.

AIX-BetriebssystemeLinux-Betriebssysteme

Beispiele

Optionsdatei:

```
snapshotcachesize 95
AIX-BetriebssystemeNur für AIX: include.fs /kalafs1
  snapshotproviderfs=JFS2 snapshotcachesize=95
AIX-BetriebssystemeNur für AIX: include.image /kalafs2
  snapshotcachesize=95
Linux-BetriebssystemeNur für Linux: include.image /linuxfs1
  snapshotcachesize=100
```

Befehlszeile:

```
-snapshotcachesize=95
```

AIX-Betriebssysteme Windows-Betriebssysteme

Snapshotproviderfs

Verwenden Sie die Option snapshotproviderfs, um Dateisicherungs- und Dateiarchivierungsoperationen auf Momentaufnahmebasis zu aktivieren und einen Momentaufnahmeprovider anzugeben.

AIX-BetriebssystemeSie müssen Root sein, um eine Dateisicherungs- oder Dateiarchivierungsoperation auf Momentaufnahmebasis auszuführen. Wenn Sie kein Rootbenutzer sind, schlägt die Operation mit einer Fehlernachricht fehl.

AIX-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssystemeDiese Option ist nur für AIX-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeGeben Sie diese Option in der Serverzeilengruppe der Systemoptionsdatei dsm.sys an, um Momentaufnahmen für alle JFS2-Dateisysteme auf dem Client zu aktivieren. Sie können die clientweite Option für eine bestimmte Operation überschreiben, indem Sie diese Option in der Befehlszeile für die Sicherungs- und Archivierungsbefehle angeben. Sie können die clientweite Option auch für ein bestimmtes Dateisystem überschreiben, indem Sie die Anweisung include.fs in der Datei dsm.sys verwenden. Sie können diese Option auch mithilfe des Profileditors setzen.

Windows-BetriebssystemeGeben Sie diese Option in der Clientoptionsdatei dsm.opt an. Sie können die clientweite Option für eine bestimmte Operation überschreiben, indem Sie diese Option in der Befehlszeile für die Sicherungs- und Archivierungsbefehle angeben. Sie können die clientweite Option auch für ein bestimmtes Dateisystem überschreiben, indem Sie die Anweisung include.fs in der Datei dsm.opt verwenden. Sie können diese Option auch mithilfe des Profileditors setzen.

Syntax

```
>>-SNAPSHOTPROVIDERFs-- --Wert---------------------------------><
```

Parameter

Wert

Gibt einen der folgenden Werte an:

AIX-BetriebssystemeJFS2

AIX-BetriebssystemeGibt an, dass Sie eine Dateisicherung oder -archivierung auf Momentaufnahmebasis ausführen wollen, während das Dateisystem für andere Systemanwendungen verfügbar ist. *Nur* für JFS2-Dateisysteme auf AIX-Clients gültig.

Windows-BetriebssystemeVSS

Windows-BetriebssystemeGibt an, dass VSS zur Bereitstellung der OFS-Unterstützung verwendet werden soll.

AIX-BetriebssystemeNONE

AIX-BetriebssystemeGibt an, dass keine Momentaufnahmen verwendet werden sollen. Für das angegebene Dateisystem wird eine Dateisicherungs- oder -archivierungsoperation ausgeführt. Dies ist der Standardwert.

Windows-BetriebssystemeNONE

Windows-BetriebssystemeGibt an, dass kein Momentaufnahmeprovider verwendet werden soll; OFS-Unterstützung ist inaktiviert. Dies ist der Standardwert.

Beispiele

AIX-BetriebssystemeOptionsdatei:
AIX-Betriebssysteme

```
snapshotproviderfs JFS2
include.fs   /kalafs1   snapshotproviderfs=JFS
```

Windows-BetriebssystemeOptionsdatei:
Windows-Betriebssysteme

```
snapshotproviderfs VSS
include.fs d: snapshotproviderfs=vss
```

AIX-BetriebssystemeBefehlszeile:
AIX-Betriebssysteme`-SNAPSHOTPROVIDERFs=JFS2`
Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme`-SNAPSHOTPROVIDERFs=VSS`

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Snapshotproviderimage

Verwenden Sie die Option snapshotproviderimage, um Imagesicherung auf Momentaufnahmebasis zu aktivieren und einen Momentaufnahmeprovider anzugeben.

AIX-BetriebssystemeLinux-BetriebssystemeSie müssen Root sein, um eine Imagesicherungsoperation auf Momentaufnahmebasis auszuführen. Wenn Sie kein Rootbenutzer sind, schlägt die Operation mit einer Fehlernachricht fehl.

AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeDiese Option ist nur für AIX- und Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeGeben Sie diese Option in der Serverzeilengruppe der Systemoptionsdatei dsm.sys an, um Momentaufnahmen für alle Dateisysteme auf dem Client zu aktivieren. Sie können die clientweite Option für eine bestimmte Operation überschreiben, indem Sie diese Option in der Befehlszeile für den Befehl backup image angeben. Sie können die clientweite Option auch für ein bestimmtes Dateisystem überschreiben, indem Sie die Anweisung include.image in der Datei dsm.sys verwenden. Sie können diese Option auch mithilfe des Profileditors setzen.

Windows-BetriebssystemeGeben Sie diese Option in der Clientoptionsdatei dsm.opt an, um Momentaufnahmen für alle Dateisysteme auf dem Client zu aktivieren. Sie können die clientweite Option für eine bestimmte Operation überschreiben, indem Sie diese Option in der Befehlszeile für den Befehl backup image angeben. Sie können die clientweite Option auch für ein bestimmtes Dateisystem überschreiben, indem Sie die Anweisung include.image in der Datei dsm.opt verwenden. Sie können diese Option auch mithilfe des Profileditors setzen.

Syntax

```
>>-SNAPSHOTPROVIDERImage-- --Wert------------------------------><
```

Parameter

Wert
Gibt einen der folgenden Werte an:
AIX-BetriebssystemeJFS2
AIX-BetriebssystemeGibt an, dass Sie eine Imagesicherung auf Momentaufnahmebasis ausführen wollen, während das Dateisystem für andere Systemanwendungen verfügbar ist. Dies ist der Standardwert für JFS2-Dateisysteme. *Nur* für AIX-Clients gültig.
Linux-BetriebssystemeLINUX_LVM
Linux-BetriebssystemeGibt an, dass Sie eine Imagesicherung auf Momentaufnahmebasis ausführen wollen, während das Dateisystem für andere Systemanwendungen verfügbar ist. Dies ist der Standardwert für Dateisysteme, die sich auf logischen Datenträgern befinden, die durch den Linux Logical Volume Manager erstellt wurden. *Nur* für Linux-Clients gültig.
Windows-BetriebssystemeVSS
Windows-BetriebssystemeGibt an, dass VSS zur Bereitstellung der Online-Imageunterstützung verwendet werden soll.

AIX-BetriebssystemeLinux-BetriebssystemeNONE
AIX-BetriebssystemeLinux-BetriebssystemeGibt an, dass Sie keine Imagesicherungsoperation auf Momentaufnahmebasis ausführen wollen. Damit wird für das angegebene Dateisystem eine statische Imagesicherungsoperation ausgeführt. Dies ist der Standardwert für andere Dateisysteme als AIX JFS2 und Linux LVM.
Windows-BetriebssystemeNONE
Windows-BetriebssystemeGibt an, dass kein Momentaufnahmeprovider verwendet werden soll. Damit wird die Online-Imageunterstützung inaktiviert. Dies ist der Standardwert.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOptionsdatei:
AIX-BetriebssystemeLinux-Betriebssysteme

```
snapshotprovideri JFS2
include.image   /kalafs1   snapshotprovideri=JFS2
```

Windows-BetriebssystemeOptionsdatei:
Windows-Betriebssysteme

```
snapshotprovideri VSS
include.image d: snapshotprovideri=vss
```

Befehlszeile:

```
-SNAPSHOTPROVIDERImage=NONE
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Snapshotroot

Verwenden Sie die Option snapshotroot im Befehl incremental, selective oder archive mit einer Anwendung eines unabhängigen Softwareanbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDie Option snapshotroot kann zum Sichern von über NFS-Mount zugeordneten Dateisystemen verwendet werden. Sowohl die Sicherungsspezifikation (Quelle) als auch der Wert für snapshotroot kann über NFS-Mount zugeordnete Dateien angeben. Die Option snapshotroot kann beispielsweise zum Sichern eines NFS-Dateisystems verwendet werden, das sich auf einem NAS (Network-Attached Storage) befindet, der Momentaufnahmen unterstützt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeAus Leistungsgründen sollte diese Option bei einer Teilsicherung eines Datenträgers eines NAS-Dateiservers anstelle einer einfachen Teilsicherung oder einer Teilsicherung mit der Option snapshotroot verwendet werden, wenn auf dem NAS-Dateiserver ONTAP V7.3 ausgeführt wird. Die Optionen snapdiff und snapshotroot sollten nicht gemeinsam verwendet werden.

Windows-BetriebssystemeDie Option snapshotroot kann zum Sichern angehängter Dateisysteme in gemeinsam genutzten Netzbereichen verwendet werden. Sowohl die Sicherungsspezifikation (Quelle) als auch der Wert für snapshotroot kann angehängte Dateien in gemeinsam genutzten Netzbereichen angeben. Die Option snapshotroot kann beispielsweise zum Sichern eines Dateisystems in einem gemeinsam genutzten Netzbereich verwendet werden, das sich auf einem NAS (Network-Attached Storage) befindet, der Momentaufnahmen unterstützt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeIm folgenden Beispiel ist das Dateisystem `test495` ein vom NAS-Dateiserver `philo` über NFS-Mount zugeordnetes Dateisystem und `/philo/test945/.snapshot/backupsnap` stellt die auf dem NAS-Dateiserver erstellte Momentaufnahme dar.

Windows-BetriebssystemeIm folgenden Beispiel ist `c:\snapshots\snapshot.0` ein auf einem NAS-Dateiserver angehängter gemeinsam genutzter Netzbereich und `\\florance\c$` stellt die auf dem NAS-Dateiserver erstellte Momentaufnahme dar.

Windows-Betriebssysteme

```
dsmc incr \\florance\C$ -snapshotroot=c:\shapshots
   \snapshot.0
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeSie können ein Verzeichnis auch mit der Option snapshotroot angeben, wenn Sie jede Dateigruppe als separaten Dateibereich sichern.

Die Option snapshotroot bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeBeispiel: Eine Anwendung erstellt eine Momentaufnahme des Dateisystems `/usr` und hängt sie als `/snapshot/day1` an. Wenn Sie diese Daten mit dem folgenden Befehl sichern, wird ein eindeutiger Dateibereich mit dem Namen `/snapshot/day1` auf dem Server erstellt.

```
dsmc incremental /snapshot/day1
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMöglicherweise möchten Sie die Momentaufnahmedaten den Daten zuordnen, die für das Dateisystem `/usr` bereits verarbeitet wurden. Mit der Option snapshotroot können Sie die Daten dem Dateibereich zuordnen, der der Dateisystem `/usr` auf dem IBM Spectrum Protect-Server entspricht:

```
dsmc incremental /usr -snapshotroot=/snapshot/day1
```

Windows-BetriebssystemeBeispiel: Eine Anwendung erstellt eine Momentaufnahme des Laufwerks `c:` und hängt sie als NTFS-Zusammenführungspunkt `\\florence\c$\snapshots\snapshot.0` an. Wenn Sie diese Daten mit dem folgenden Befehl sichern, wird ein eindeutiger Dateibereich mit dem Namen `\\florence\c$\snapshots\snapshot.0` auf dem Server erstellt.

```
dsmc incremental \\florence\c$\snapshots\snapshot.0
```

Windows-BetriebssystemeMöglicherweise möchten Sie die Momentaufnahmedaten den Daten zuordnen, die für das Laufwerk `c: (\\florence\c$)` bereits verarbeitet wurden. Mit der Option snapshotroot können Sie die Daten dem Dateibereich zuordnen, der der Laufwerk `c: (\\florence\c$)` auf dem IBM Spectrum Protect-Server entspricht:

```
dsmc incr c: -snapshotroot=\\florence\c$\snapshots\snapshot.0
-oder-
dsmc incr \\florence\c$ -snapshotroot=\\florence\c$\snapshots\
  snapshot.0
```

An einem späteren Tag können Sie eine Momentaufnahme sichern, die an einer anderen Position gespeichert wurde, jedoch unter demselben Dateibereich auf dem Server verwaltet wird: AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
dsmc incremental /usr -snapshotroot=/snapshot/day2
```

Windows-Betriebssysteme

```
dsmc incr c: -snapshotroot=\\florence\c$\snapshots\snapshot.1
```

Mithilfe der Option snapshotroot können Sie Teilsicherungen, selektive Sicherungen oder Archivierungen von einzelnen Verzeichnissen, Verzeichnisstrukturen oder einzelnen Dateien ausführen. In allen Fällen muss die Option snapshotroot den logischen Datenträger angeben, der durch die Momentaufnahme erstellt wurde. Zum Beispiel: AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
dsmc incremental /usr/dir1/* -subdir=yes
  -snapshotroot=/snapshot/day1
dsmc selective /usr/dir1/sub1/file.txt
  -snapshotroot=/snapshot/day1
dsmc archive /usr/dir1/sub1/*.txt
  -snapshotroot=/snapshot/day1
```

Windows-Betriebssysteme

```
dsmc incr c:\dir1\* -subdir=yes  -snapshotroot=\\florence\c$\
  snapshots\snapshot.1
dsmc sel c:\dir1\sub1\file.txt -snapshotroot=\\florence\c$\
  snapshots\snapshot.1
dsmc archive c:\mydocs\*.doc -snapshotroot=\\florence\c$\
  snapshots\snapshot.1
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSollen bestimmte Dateispezifikationen ein- oder ausgeschlossen werden, müssen die entsprechenden Einschluss- und Ausschlussanweisungen den Namen des Dateisystems enthalten, das die Quelle der Momentaufnahme (Dateisystem `/usr`) darstellt, und nicht den Namen des Ziels der Momentaufnahme `(/snapshot/day1)`. Auf diese Weise ist die Beibehaltung einer Gruppe von Einschluss- und Ausschlussanweisungen möglich, auch wenn der Name des logischen Datenträgers, auf den die Momentaufnahme geschrieben wird, sich ändert. Die folgenden Beispiele zeigen Einschluss- und Ausschlussanweisungen.

```
include /usr/dir1/*.txt 1yrmgmtclass
exclude /usr/mydocs/*.txt
```

Windows-BetriebssystemeSollen bestimmte Dateispezifikationen ein- oder ausgeschlossen werden, müssen die entsprechenden Einschluss- und Ausschlussanweisungen den Namen des Dateisystems enthalten, das die Quelle der Momentaufnahme (Laufwerk `c:`) darstellt, und nicht den Namen des Ziels der Momentaufnahme `(\\florence\c$\snapshots\snapshot.1)`. Auf diese Weise ist die Beibehaltung einer Gruppe von Einschluss- und Ausschlussanweisungen möglich, auch wenn der Name des logischen Datenträgers, auf den die Momentaufnahme geschrieben wird, sich ändert. Die folgenden Beispiele zeigen Einschluss- und Ausschlussanweisungen.

```
include c:\dir1\.../*.txt lyrmgmtclass
exclude \\florence\c$\mydocs\*.doc
```

Die folgenden Einschluss-/Ausschlussanweisungen sind nicht gültig, da sie den Namen der Momentaufnahme enthalten: AIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme

```
include /snapshot/day1/dir1/*.txt 1yrmgmtclass
exclude /snapshot/day1/mydocs/*.txt
```

Windows-Betriebssysteme

```
include \\florence\c$\snapshots\snapshot.1\dir1\...\
  *.txt 1yrmgmtclass
exclude \\florence\c$\mydocs\*.doc
```

Bei Teilsicherungen, selektiven Sicherungen oder Archivierungen müssen Sie die Option snapshotroot mit einer einzelnen Dateispezifikation verwenden. Es ist nicht möglich, mehrere Dateispezifikationen oder keine Dateispezifikation anzugeben. Die folgenden Befehle sind beispielsweise gültig: AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
dsmc incremental /usr -snapshotroot=/snapshot/day1
dsmc incremental /usr/dir1/* -snapshotroot=/snapshot/day1
```

Windows-Betriebssysteme

```
dsmc incr c: -snapshotroot=\\florence\c$\snapshots\snapshot.0
dsmc incr c:\dir1\* -snapshotroot=\\florence\c$\snapshots\
  snapshot.0
```

Der folgende Befehl ist ungültig, da er zwei Dateispezifikationen enthält: AIX-BetriebssystemeLinux-Betriebssysteme
Oracle Solaris-Betriebssysteme

```
dsmc incremental /usr/dir1/* /home/dir2/*
  -snapshotroot=/snapshot/day1
```

Windows-Betriebssysteme

```
dsmc incr c:\dir1\* e:\dir1\* -snapshotroot=\\florence\c$\
  snapshots\snapshot.0
```

Der folgende Befehl ist ungültig, da er keine Dateispezifikation enthält: AIX-BetriebssystemeLinux-Betriebssysteme
Oracle Solaris-Betriebssysteme

```
dsmc incremental -snapshotroot=/snapshot/day1
```

Windows-Betriebssysteme

```
dsmc incr -snapshotroot=\\florence\c$\snapshots\snapshot.0
```

Anmerkungen:

1. Stellen Sie sicher, dass die Option snapshotroot auf eine Momentaufnahme des richtigen Datenträgers verweist. Stellen Sie sicher, dass die snapshotroot-Position auf das Stammverzeichnis der Momentaufnahme verweist. Werden diese Regeln nicht befolgt, kann es zu unbeabsichtigten Ergebnissen kommen, sodass Dateien z. B. fälschlicherweise als verfallen markiert werden.
2. Wenn Sie die Option filelist und die Option snapshotroot angeben, wird angenommen, dass sich alle in der Option filelist angegebenen Dateien in demselben Dateisystem befinden. Befinden sich Einträge in der Option filelist in einem anderen Dateisystem, werden sie übersprungen und ein Fehler wird protokolliert. Enthält die Option filelist Dateien, die nach der Erstellung der Momentaufnahme in dem Dateisystem erstellt wurden, werden diese Einträge ebenfalls übersprungen und ein Fehler wird protokolliert.
3. Windows-BetriebssystemeSie können die Option snapshotroot nicht in einem Sicherungsbefehl wie z. B. backup image oder backup systemstate verwenden.
4. Linux-BetriebssystemeWindows-BetriebssystemeSie können die Option snapshotroot nicht mit der Option snapdiff verwenden.
5. Windows-BetriebssystemeVerwenden Sie die Option snapshotroot mit Vorsicht, wenn Sie die journalbasierte IBM Spectrum Protect-Sicherungsfunktion verwenden. Da keine Koordination zwischen dem IBM Spectrum Protect-Journal und dem Momentaufnahmeprovider (VSS) eines anderen Anbieters existiert, können bei Journalbenachrichtigungen, die nach Erstellung der Momentaufnahme empfangen werden, Unregelmäßigkeiten auftreten. So werden Dateien möglicherweise gar nicht oder mehrfach auf dem IBM Spectrum Protect-Server gesichert.
6. Sie können die Option snapshotroot mit den Optionen preschedulecmd und postschedulecmd oder in automatisierten Scripts verwenden, die Sie mit dem Client-Scheduler ausführen.

Unterstützte Clients

Diese Option ist für die folgenden Clients gültig:

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeUNIX- und Linux-Clients mit Ausnahme von Mac OS X.
- Windows-BetriebssystemeAlle Windows-Clients.

Syntax

```
>>-SNAPSHOTRoot = - --Momentaufnahmedatenträgername------------><
```

Parameter

Momentaufnahmedatenträgername
: Gibt das Stammverzeichnis des logischen Datenträgers an, der durch die Anwendung eines unabhängigen Softwareanbieters zur Momentaufnahmenerstellung generiert wurde.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssystemedsmc incremental /usr -SNAPSHOTRoot=/snapshot/day1

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssystemedsmc incr c: -SNAPSHOTRoot=\\florence\c$\snapshots\snapshot.0

Srvoptsetencryptiondisabled

Die Option srvoptsetencryptiondisabled ermöglicht es dem Client, die Verschlüsselungsoptionen in einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server zu ignorieren.

Ist die Option in der Clientoptionsdatei auf yes gesetzt, ignoriert der Client die folgenden Optionen in einer Clientoptionsgruppe auf dem Server:

- encryptkey generate
- exclude.encrypt
- include.encrypt

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax

```
                              .-no--.
>>-SRVOPTSETENCryptiondisabled--+-----+------------------------><
                              '-yes-'
```

Parameter

yes
: Der Client für Sichern/Archivieren ignoriert die Werte der aufgelisteten Verschlüsselungsoptionen in einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server.

no
: Der Client für Sichern/Archivieren verarbeitet die Einstellung der aufgelisteten Verschlüsselungsoptionen in einer Clientoptionsgruppe auf dem IBM Spectrum Protect-Server. Dies ist der Standardwert.

Beispiele

Optionsdatei:

```
srvoptsetencryptiondisabled no
```

Befehlszeile:

Nicht zutreffend.

Srvprepostscheddisabled

Die Option srvprepostscheddisabled gibt an, ob verhindert werden soll, dass die vom IBM Spectrum Protect-Administrator angegebenen Befehle vor und nach dem Zeitplan bei der Ausführung geplanter Operationen auf dem Clientsystem ausgeführt werden.

Die Option srvprepostscheddisabled kann zusammen mit den Optionen schedcmddisabled und srvprepostscheddisabled verwendet werden, um die Ausführung unerwünschter Betriebssystembefehle durch den IBM Spectrum Protect-Administrator auf einem Clientknoten zu inaktivieren.

Unterstützte Clients

Diese Option ist für alle Clients für Sichern/Archivieren gültig, die den IBM Spectrum Protect-Client-Scheduler verwenden. Diese Option kann nicht auf dem Server definiert werden.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe für den Scheduler ein. Sie können diese Option auf der Registerkarte Scheduler des Profileditors im Abschnitt Befehl für Zeitplan definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) für den Scheduler ein. Sie können diese Option auf der Registerkarte Scheduler des Profileditors im Abschnitt Befehl für Zeitplan definieren.

Syntax

```
                              .-No--.
>>-SRVPREPOSTSCHeddisabled--+-----+----------------------------><
                            '-Yes-'
```

Parameter

No
: Gibt an, dass der Client die Ausführung von Befehlen vor und nach dem Zeitplan, die vom IBM Spectrum Protect-Administrator definiert wurden, bei der Ausführung geplanter Operationen auf dem Clientsystem zulässt. Wird ein Befehl vor oder nach dem Zeitplan sowohl vom Client als auch vom IBM Spectrum Protect-Administrator definiert, überschreibt der vom Administrator definierte Befehl den entsprechenden in der Clientoptionsdatei definierten Befehl. Dies ist der Standardwert.

Yes
: Gibt an, dass der Client die Ausführung von Befehlen vor und nach dem Zeitplan, die vom IBM Spectrum Protect-Administrator definiert wurden, bei der Ausführung geplanter Operationen auf dem Clientsystem verhindert. Wird ein Befehl vor oder nach dem Zeitplan sowohl vom Client als auch vom IBM Spectrum Protect-Administrator definiert, überschreibt der vom Administrator definierte Befehl *nicht* den entsprechenden in der Clientoptionsdatei definierten Befehl. Diese Option kann zusammen mit den Optionen schedcmddisabled und srvprepostscheddisabled verwendet werden.

Beispiele

Optionsdatei:

```
srvprepostscheddisabled yes
```

Befehlszeile:
: Nicht zutreffend.

Linux-BetriebssystemeWindows-Betriebssysteme

Srvprepostsnapdisabled

Die Option srvprepostsnapdisabled gibt an, ob verhindert werden soll, dass die vom IBM Spectrum Protect-Administrator angegebenen Befehle vor und nach der Momentaufnahme bei der Ausführung geplanter Sicherungsoperationen für Image-Momentaufnahmen ausgeführt werden.

Die Option srvprepostsnapdisabled kann zusammen mit den Optionen schedcmddisabled und srvprepostsnapdisabled verwendet werden, um die Ausführung unerwünschter Betriebssystembefehle durch den IBM Spectrum Protect-Administrator auf einem Clientknoten zu inaktivieren.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux-Clients gültig, die den Befehl zum Sichern von Image-Momentaufnahmen unterstützen. Diese Option kann nicht auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Windows-BetriebssystemeDiese Option ist für Windows-Clients gültig, die den Befehl zum Sichern von Image-Momentaufnahmen unterstützen. Diese Option kann nicht auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe für den Scheduler ein. Sie können diese Option auf der Registerkarte Momentaufnahme des Profileditors im Abschnitt Momentaufnahmeoptionen definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) für den Scheduler ein. Sie können diese Option auf der Registerkarte Momentaufnahme des Profileditors im Abschnitt Momentaufnahmeoptionen definieren.

Syntax

```
                              .-No--.
>>-SRVPREPOSTSNApdisabled--+-----+----------------------------><
                           '-Yes-'
```

Parameter

No
: Gibt an, dass der Client die Ausführung von Befehlen vor und nach der Momentaufnahme, die vom IBM Spectrum Protect-Administrator definiert wurden, bei der Ausführung geplanter Operationen für Image-Momentaufnahmesicherungen auf dem Clientsystem zulässt. Wird ein Befehl vor oder nach der Momentaufnahme sowohl vom Client als auch vom IBM Spectrum Protect-Administrator definiert, überschreibt der vom Administrator definierte Befehl den entsprechenden in der Clientoptionsdatei definierten Befehl. Dies ist der Standardwert.

Yes
: Gibt an, dass der Client die Ausführung von Befehlen vor und nach der Momentaufnahme, die vom IBM Spectrum Protect-Administrator definiert wurden, bei der Ausführung geplanter Operationen für Image-Momentaufnahmesicherungen auf dem Clientsystem nicht zulässt. Wird ein Befehl vor oder nach der Momentaufnahme sowohl vom Client als auch vom IBM Spectrum Protect-Administrator definiert, überschreibt der vom Administrator definierte Befehl *nicht* den entsprechenden in der Clientoptionsdatei definierten Befehl. Diese Option kann zusammen mit den Optionen schedcmddisabled und srvprepostsnapdisabled verwendet werden.

Beispiele

Optionsdatei:
```
srvprepostsnapdisabled yes
```
Befehlszeile:
: Nicht zutreffend.

Ssl

Verwenden Sie die Option ssl, um Secure Sockets Layer (SSL) für eine sichere Client- und Serverkommunikation zu aktivieren. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Versionen kommuniziert, legt der Client fest, ob SSL aktiviert wird. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.2 und höher kommuniziert, wird SSL immer verwendet und mithilfe dieser Option gesteuert, ob Objektdaten verschlüsselt werden oder nicht. Aufgrund von Leistungsaspekten ist es möglicherweise sinnvoll, die Objektdaten nicht zu verschlüsseln.

Unterstützte Clients

Diese Option ist für alle unterstützten Clients gültig.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auch auf der Registerkarte Übertragung des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auch auf der Registerkarte Übertragung des Profileditors definieren.

Syntax

```
        .-No--.
>>-SSL--+-----+-------------------------------------------------><
        '-Yes-'
```

Parameter für die Kommunikation mit einem IBM Spectrum Protect-Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Versionen

No
: Gibt an, dass der Client für Sichern/Archivieren SSL nicht verwendet, um Informationen zu verschlüsseln. No ist der Standardwert.

Yes
: Gibt an, dass der Client für Sichern/Archivieren SSL verwendet, um Informationen zu verschlüsseln.

  Um SSL zu aktivieren, geben Sie SSL Yes an und ändern Sie den Wert der Option TCPPORT. Die Änderung des Werts der Option TCPPORT ist im Allgemeinen erforderlich, da der IBM Spectrum Protect-Server in der Regel so konfiguriert ist, dass er an einem anderen Anschluss für SSL-Verbindungen empfangsbereit ist.

Parameter für die Kommunikation mit einem IBM Spectrum Protect-Server der Version 8.1.2 und höher

No
: Gibt an, dass der Client für Sichern/Archivieren bei der Kommunikation mit dem Server SSL nicht verwendet, um Objektdaten zu verschlüsseln. Alle anderen Informationen werden verschlüsselt. No ist der Standardwert.

Yes
: Gibt an, dass der Client für Sichern/Archivieren bei der Kommunikation mit dem Server SSL für die Verschlüsselung aller Informationen, einschließlich Objektdaten, verwendet.

  Um SSL für alle Daten zu verwenden, geben Sie SSL Yes an.

Beispiele

Optionsdatei:
```
ssl yes
```
Befehlszeile:
: Nicht zutreffend.

Sslacceptcertfromserv

Mithilfe der Option sslacceptcertfromserv können Sie steuern, ob der Client für Sichern/Archivieren oder die API-Anwendung das öffentliche SSL-Zertifikat des IBM Spectrum Protect-Servers akzeptiert und als vertrauenswürdig anerkennt, wenn das erste Mal eine Verbindung zwischen ihnen hergestellt wird. Diese Option gilt nur für das erste Herstellen der Verbindung zwischen dem Client für Sichern/Archivieren oder der API-Anwendung und dem IBM Spectrum Protect-Server. Wenn das öffentliche SSL-Zertifikat akzeptiert wird, werden zukünftige Änderungen an dem Zertifikat nicht automatisch akzeptiert; sie müssen manuell in den Client für Sichern/Archivieren importiert werden. Mit dieser Option können Sie die Verbindung nur zu einem IBM Spectrum Protect-Server der Version 8.1.2 und höher herstellen.

Unterstützte Clients

Diese Option ist für alle unterstützten Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                          .-Yes-.
>>-SSLACCEPTCERTFROMSERV--+-----+------------------------------><
                          '-No--'
```

Parameter

Yes
: Gibt an, dass der Client für Sichern/Archivieren das öffentliche Zertifikat des IBM Spectrum Protect-Servers automatisch akzeptiert. Yes ist der Standardwert.

No
: Gibt an, dass der Client für Sichern/Archivieren das öffentliche Zertifikat des IBM Spectrum Protect-Servers nicht automatisch akzeptiert.

  Um SSLACCEPTCERTFROMSERV zu inaktivieren, geben Sie sslacceptcertfromserv no an.

Beispiele

Optionsdatei:
```
sslacceptcertfromserv no
```
Befehlszeile:
: Nicht zutreffend.

Ssldisablelegacytls

Verwenden Sie die Option ssldisablelegacytls, um die Verwendung von SSL-Protokollen mit einer niedrigeren Stufe als TLS 1.2 nicht zuzulassen.

Unterstützte Clients

Diese Option ist für alle unterstützten Clients gültig.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys ein. Sie können diese Option auch in der GUI definieren, indem Sie das Kontrollkästchen TLS 1.2 oder höher erforderlich auf der Registerkarte Übertragung des Profileditors auswählen. Sie können diese Option nicht in der Befehlszeile definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auch in der GUI definieren, indem Sie das Kontrollkästchen TLS 1.2 oder höher erforderlich auf der Registerkarte Übertragung des Profileditors auswählen. Sie können diese Option nicht in der Befehlszeile definieren.

Syntax

```
                          .-No--.
>>-SSLDISABLELEGACYtls--+-----+---------------------------------><
                          '-Yes-'
```

Parameter

No
: Gibt an, dass beim Client für Sichern/Archivieren für SSL-Sitzungen nicht TLS 1.2 erforderlich ist. Der Client lässt Verbindungen mit TLS 1.1 und niedrigeren SSL-Protokollen zu. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.1 und früheren Stufen der Version 8 bzw. Version 7.1.7 und früheren Versionen kommuniziert, ist No der Standardwert.

Yes
: Gibt an, dass beim Client für Sichern/Archivieren für alle SSL-Sitzungen das Protokoll TLS 1.2 (oder höher) erforderlich ist. Wenn der Client für Sichern/Archivieren mit einem IBM Spectrum Protect-Server der Version 8.1.2 und höher kommuniziert, ist Yes der Standardwert.

Beispiele

Optionsdatei:
```
ssldisablelegacytls yes
```
Befehlszeile:
: Nicht zutreffend.

Sslfipsmode

Die Option sslfipsmode gibt an, ob der Client den FIPS-Modus (FIPS = Federal Information Processing Standards) für die SSL-Übertragung (SSL = Secure Sockets Layer) mit dem Server verwendet. Der Standardwert ist No.

Unterstützte Clients

Diese Option wird auf allen Clients unterstützt.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei. Sie können die Option weder als Befehlszeilenparameter angeben noch in einer Clientoptionsgruppe definieren.

Syntax

```
                   .-No--.
>>-SSLFIPSMODE = -+-----+---------------------------------------><
                   '-Yes-'
```

Parameter

No
: Gibt an, dass der Client den SSL FIPS-Modus nicht für die sichere Kommunikation mit dem Server verwendet. SSL im FIPS-Modus wird nur von Version 6.3 und neueren Versionen des Servers unterstützt. Setzen Sie diese Clientoption auf no, wenn der Client SSL verwendet, um eine Verbindung zu einem Server herzustellen, der nicht Version 6.3 oder eine neuere Version aufweist.

Yes
: Gibt an, dass der Client den SSL FIPS-Modus für die sichere Kommunikation mit dem Server verwendet. Die Angabe von yes für diese Option beschränkt die SSL-Sitzungsvereinbarung auf die Verwendung von FIPS-konformen Cipher-Suites. SSL im FIPS-Modus wird nur vom Server der Version 6.3 (oder neueren Versionen) unterstützt.

Beispiel

Um SLL im FIPS-Modus auf Client zu aktivieren, geben Sie Folgendes ein:

```
SSLFIPSMODE yes
```

Sslrequired

Die Option sslrequired gibt die Bedingungen an, unter denen SSL erforderlich ist, wenn sich der Client beim IBM Spectrum Protect-Server oder bei den Speicheragenten anmeldet. Um SSL zu aktivieren, damit die Kommunikation zwischen Client und Server sowie Client und Speicheragent sicher ist, müssen Sie die Clientoption ssl auf yes setzen. Bei der Kommunikation mit dem IBM Spectrum Protect-Server der Version 8.1.2 und höher ist diese Option nicht mehr gültig, da SSL immer verwendet wird.

Unterstützte Clients

Diese Option wird auf allen Clients unterstützt.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei oder, in der grafischen Benutzerschnittstelle, auf der Registerkarte 'Übertragung' ein. Sie können diese Option nicht in der Befehlszeile definieren.

Syntax

```
                .-Default----.
>>-SSLREQuired-+------------+-----------------------------------><
                +-Yes--------+
                +-No---------+
                '-SERVERonly-'
```

Parameter

Default
: Diese Einstellung gibt an, dass SSL zum Schützen der Kommunikation zwischen dem Client und dem Server sowie dem Client und den Speicheragenten erforderlich ist, wenn `AUTHENTICATION=LDAP` auf dem Server definiert ist. Um die Kommunikation mit SSL zu sichern, müssen Sie außerdem `ssl=yes` auf dem Client definieren.
Ist `AUTHENTICATION=LOCAL` auf dem Server definiert, gibt diese Einstellung an, dass SSL nicht erforderlich ist. Auch wenn SSL nicht erforderlich ist, wenn `AUTHENTICATION=LOCAL` und `sslrequired=default` definiert sind, können Sie SSL dennoch verwenden, indem Sie die Clientoption ssl auf yes setzen.

Yes
: Gibt an, dass SSL immer erforderlich ist, um die Kommunikation zwischen dem Client und dem Server sowie dem Client und den Speicheragenten zu schützen. `sslrequired=yes` ist nicht von der Serveroption AUTHENTICATION abhängig. Wenn Sie `sslrequired=yes` auf dem Client definieren, müssen Sie auch `ssl=yes` auf dem Client angeben.

No
: Gibt an, dass SSL nicht erforderlich ist, um die Kommunikation zwischen dem Client und dem Server oder dem Client und den Speicheragenten zu schützen. Wählen Sie diese Option nur aus, wenn Sie ein virtuelles privates Netz oder eine andere Methode zum Schützen Ihrer Sitzungskommunikation verwenden. Sie können SSL dennoch aktivieren, indem Sie `ssl=yes` auf dem Client definieren; `sslrequired=no` gibt jedoch an, dass SSL keine Voraussetzung ist.

SERVERonly
: Gibt an, dass SSL für die Kommunikation zwischen dem Client und dem Server erforderlich ist und für die Kommunikation zwischen dem Server und dem Speicheragenten nicht erforderlich ist. Soll SSL für die Kommunikation zwischen dem Client und dem Server verwendet werden, definieren Sie `sslrequired=serveronly` und `ssl=yes`. Die Servereinstellung für die Option AUTHENTICATION kann LOCAL oder LDAP lauten.
Verwenden Sie für die Kommunikation zwischen dem Client und dem Speicheragenten die Clientoption lanfreessl, um SSL zu aktivieren.

Die folgende Tabelle enthält Beschreibungen der Situationen, in denen die Authentifizierung erfolgreich ist oder fehlschlägt, je nach Einstellung der Option SSLREQUIRED auf dem Server und dem Client und der Einstellung der Option ssl auf dem Client. Voraussetzung ist, dass gültige Berechtigungsnachweise angegeben werden.

Tabelle 1. Auswirkungen der SSL-Einstellungen des Servers und des Clients auf den Erfolg bzw. Misserfolg von Anmeldeversuchen

Option SSLREQUIRED (Servereinstellung)	Option sslrequired (Clienteinstellung)	Option ssl (Clienteinstellung)	Erfolg oder Misserfolg der Authentifizierung
Yes	Yes	Yes	Authentifizierung erfolgreich
Yes	Yes	No	Authentifizierung schlägt fehl; der Client weist die Sitzung zurück
Yes	No	Yes	Authentifizierung erfolgreich

Option SSLREQUIRED (Servereinstellung)	Option sslrequired (Clienteinstellung)	Option ssl (Clienteinstellung)	Erfolg oder Misserfolg der Authentifizierung
Yes	No	No	Authentifizierung schlägt fehl; der Server weist die Sitzung zurück
No	Yes	Yes	Authentifizierung erfolgreich
No	Yes	No	Authentifizierung schlägt fehl; der Client weist die Sitzung zurück
No	No	Yes	Authentifizierung erfolgreich
No	No	No	Authentifizierung erfolgreich

Im folgenden Text wird beschrieben, wie sich die Einstellungen `SSLREQUIRED=DEFAULT` und `SSLREQUIRED=SERVERONLY` auf dem Server auf die Option ssl auf dem Client auswirken.

Wenn auf dem Server `SSLREQUIRED=DEFAULT` und `AUTHENTICATION=LDAP` definiert sind, muss auf dem Client `ssl=yes` definiert werden. Andernfalls schlägt die Authentifizierung fehl.

Wenn auf dem Server `SSLREQUIRED=DEFAULT` und `AUTHENTICATION=LOCAL` definiert sind, kann auf dem Client `ssl=yes` oder `ssl=no` definiert werden.

Wenn auf dem Server `SSLREQUIRED=SERVERONLY` definiert ist, muss auf dem Client `ssl=yes` definiert werden. Die Clientoption lanfreessl kann auf yes gesetzt werden, um die Kommunikation mit einem Speicheragenten zu schützen, oder kann auf no gesetzt werden, wenn die sichere Kommunikation mit Speicheragenten nicht erforderlich ist.

Beispiele

Optionsdatei:

```
sslrequired yes
sslrequired no
sslrequired default
sslrequired serveronly
```

Befehlszeile:
Nicht gültig; Sie können diese Option nicht in der Befehlszeile definieren.

Linux-Betriebssysteme Windows-Betriebssysteme

Stagingdirectory

Die Option stagingdirectory definiert die Position, an der der Client alle Daten speichert, die er zum Ausführen seiner Operationen generiert. Die Daten werden gelöscht, wenn die Verarbeitung abgeschlossen ist.

Windows-BetriebssystemeDer Client verwendet die durch stagingdirectory angegebene Position für Active Directory-Objektabfrage- und -zurückschreibungsoperationen. Der Client verwendet die durch stagingdirectory angegebene Position auch für temporäre Dateien, wenn der Client Dateien verarbeitet, die mit IBM Spectrum Protect HSM for Windows umgelagert wurden.

Wichtig: Ab Version 8.1.2 wird die Option snapdiffchangelogdir verwendet, um die Position zum Speichern von Änderungsprotokollen für Momentaufnahmedifferenzsicherungsoperationen anzugeben. Die Option stagingdirectory wird nicht mehr zu diesem Zweck verwendet. Weitere Informationen finden Sie in Snapdiffchangelogdir.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Wird stagingdirectory in der Befehlszeile angegeben, überschreibt diese Angabe die Werte, die in der Optionsdatei angegeben sind.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Wird stagingdirectory in der Befehlszeile angegeben, überschreibt diese Angabe die Werte, die in der Optionsdatei angegeben sind.

Syntax

```
>>-STAGINGDIRectory--Pfad-------------------------------------><
```

Parameter

Pfad

 Linux-BetriebssystemeGibt den Verzeichnispfad an, in den der Client zwischenzuspeichernde Daten schreibt. Wenn Sie kein Zwischenspeicherungsverzeichnis angeben, speichert der Client temporäre Daten im temporären Dateisystem (normalerweise /tmp).
 Windows-BetriebssystemeGibt den Verzeichnispfad an, in den der Client zwischenzuspeichernde Daten schreibt. Wenn Sie kein Zwischenspeicherungsverzeichnis angeben, prüft der Client in der folgenden Reihenfolge, ob die Umgebungsvariablen für den Benutzer vorhanden sind, und verwendet den Pfad, der zuerst gefunden wird:

1. Der Pfad, der durch die Benutzervariable TMP angegeben wird
2. Der Pfad, der durch die Systemvariable TMP angegeben wird
3. Der Pfad, der durch die Benutzervariable TEMP angegeben wird
4. Der Pfad, der durch die Systemvariable TEMP angegeben wird
5. Das Windows-Systemverzeichnis

 Windows-BetriebssystemeIm UNC-Format (Universal Naming Convention) muss der Pfad einen Laufwerkbuchstaben enthalten. In dem folgenden Beispiel für das UNC-Format enthält der Pfad den Laufwerkbuchstaben D$:

```
\\computer7\D$\temp\tsmstaging
```

Beispiele

Optionsdatei:

 Linux-Betriebssysteme`stagingdirectory /usr/tsmdata`
 Linux-Betriebssysteme`stagingdirectory /private/tmp`
 Windows-Betriebssysteme`stagingdirectory c:\tsmdata`

Befehlszeile:

 Linux-Betriebssysteme`-stagingdir="/tmp/tsmtempdata"`
 Windows-Betriebssysteme`-stagingdir="e:\tsmdata"`

Zugehörige Verweise:

 Windows-BetriebssystemeQuery Adobjects
 Windows-BetriebssystemeRestore Adobjects
Diffsnapshot
Snapdiff

Zugehörige Informationen:

http://www.ibm.com/support/knowledgecenter/SSERBH

Subdir

Die Option subdir gibt an, ob Unterverzeichnisse benannter Verzeichnisse bei der Verarbeitung berücksichtigt werden sollen.

Die Option subdir können Sie in folgenden Befehlen verwenden:

- archive
- delete archive
- delete backup
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssystemeincremental
- query archive
- query backup
- restore
- restore backupset
- restore group
- retrieve
- selective

Wenn Sie beim Sichern eines bestimmten Pfads und einer bestimmten Datei die Option subdir auf `yes` setzen, durchsucht der Client für Sichern/Archivieren rekursiv alle Unterverzeichnisse unter diesem Pfad und sucht nach allen Instanzen der angegebenen Datei, die sich unter einem dieser Unterverzeichnisse befinden. Beispiel: Angenommen, eine Datei mit dem Namen myfile.txt ist auf einem Client in den folgenden Verzeichnissen vorhanden:

```
//myfile.txt
/dir1/myfile.txt
/dir1/dir_a/myfile.txt
/dir1/dir_b/myfile.txt
```

Wenn eine selektive Sicherung dieser Datei durchgeführt wird, werden alle vier Instanzen von myfile.txt gesichert:

```
dsmc sel /myfile.txt -subdir=yes
```

Dementsprechend werden mit dem folgenden Befehl alle Instanzen von myfile.txt angezeigt, wenn Sie subdir=yes in der Clientoptionsdatei oder einer Clientoptionsgruppe angeben.

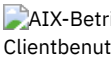
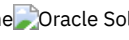
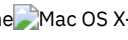
```
dsmc restore /myfile.txt -pick
```

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

 Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

    Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

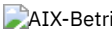
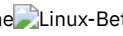
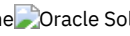
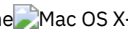
```
           .-No--.
>>-SUbdir--+-----+-----------------------------------------------><
           '-Yes-'
```

Parameter

No
: Unterverzeichnisse werden nicht verarbeitet. Dies ist der Standardwert.

Yes
: Unterverzeichnisse werden verarbeitet. Da das Clientprogramm alle Unterverzeichnisse eines Verzeichnisses, das verarbeitet wird, durchsucht, kann die Verarbeitung länger dauern. Yes sollte nur im Bedarfsfall angegeben werden.

  Wenn Sie die Option preservepath zusätzlich zu subdir=`yes` verwenden, kann dies einen Einfluss darauf haben, welche Unterverzeichnisse verarbeitet werden.

      Handelt es sich bei einem Unterverzeichnis um ein angehängtes Dateisystem, wird es nicht verarbeitet, auch wenn Sie subdir=`yes` angeben.

Anmerkung:

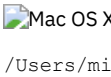
1. Wenn Sie den Client im interaktiven Modus ausführen und die Option -subdir=yes verwenden, bleibt die Einstellung für alle Befehle bestehen, die im interaktiven Modus eingegeben werden, bis Sie den interaktiven Modus durch Eingabe von `Quit` beenden.
2. Ist subdir=yes wirksam, wenn Sie mehrere Dateien zurückschreiben, fügen Sie am Ende der Zieldateispezifikation einen Verzeichnisbegrenzer ein. Wird der Begrenzer nicht angegeben, zeigt der Client eine Nachricht an, die angibt, dass die Zieldateispezifikation nicht gültig ist.
3. Es wird empfohlen, nur den Standardwert für subdir (No) in eine Clientoptionsdatei oder eine Clientoptionsgruppe einzuschließen.

Beispiele

Optionsdatei:

```
subdir no
```

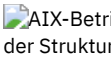
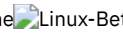
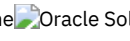
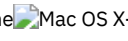
Befehlszeile:

 Zum Zurückschreiben der Struktur:

```
/Users/mike/dir1
/Users/mike/dir1/file1
/Users/mike/dir1/dir2
/Users/mike/dir1/dir2/file1
```

einen der folgenden Befehle eingeben:

```
dsmc rest "/Users/van/dir1/*" /Users/mike/ -su=yes
dsmc rest "/Users/van/dir1/file*" /Users/mike/ -su=yes
dsmc rest "/Users/van/dir1/file1*" /Users/mike/ -su=yes
```

    Zum Zurückschreiben der Struktur:

```
/path2/dir1
/path2/dir1/file1
/path2/dir1/dir2
/path2/dir1/dir2/file1
```

einen der folgenden Befehle eingeben:

```
dsmc rest "/path/dir1/*" /path2/ -su=yes
dsmc rest "/path/dir1/file*" /path2/ -su=yes
dsmc rest "/path/dir1/file1*" /path2/ -su=yes
```

 Windows-Betriebssysteme Zum Zurückschreiben der Struktur:

```
\path2\dir1
\path2\dir1\file1
\path2\dir1\dir2
\path2\dir1\dir2\file1
```

einen der folgenden Befehle eingeben:

```
rest \path\dir1\* \path2\ -su=yes
rest \path\dir1\file* \path2\ -su=yes
rest \path\dir1\file1* \path2\ -su=yes
```

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

 Windows-Betriebssysteme

Systemstatebackupmethod

Mit der Option systemstatebackupmethod können Sie angeben, welche Sicherungsmethode für die Sicherung des System Writer-Abschnitts der Systemstatusdaten verwendet werden soll. Die von Ihnen ausgewählte Methode wird bei der Sicherung der Systemstatusdaten verwendet.

Unterstützte Clients

Diese Option ist für Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Bei Angabe in der Datei dsm.opt wirkt sich die Option auf Systemstatussicherungen aus, die durch BACKUP SYSTEMSTATE-Befehle erstellt werden, und auf Systemstatusdaten, die durch INCREMENTAL-Befehle gesichert werden. Der einzige Befehl, in dem Sie diese Option angeben können, ist BACKUP SYSTEMSTATE.

Zeitplandefinitionen

Sie können diese Option auch im Parameter options einer Zeitplandefinition für Zeitpläne angeben, in denen sowohl action=backup als auch subaction=systemstate definiert ist. Wenn Sie einen selten ausgeführten Zeitplan mit der Angabe FULL für diese Option definieren, ist sichergestellt, dass regelmäßig eine Gesamtsicherung von Windows-Systemstatusdaten ausgeführt wird.

Syntax

```
                            .-PROGressive---.
>>-SYSTEMSTATEBACKUPMethod--+---------------+------------------><
                            +-OPPortunistic-+
                            '-FULL----------'
```

Parameter

PROGressive

Bei der Methode 'PROGressive' wird der System Writer-Abschnitt der Systemstatusdaten mithilfe der progressiven Teilsicherung gesichert. Das heißt, wenn sich System Writer-Dateien seit der letzten Systemstatussicherung nicht geändert haben, werden sie bei dieser Sicherung nicht berücksichtigt. Nur die geänderten System Writer-Dateien werden gesichert. Dies ist die Standardmethode der Systemstatussicherung.

Diese Art der Systemstatussicherung erfordert die geringste Netzbandbreite und den geringsten IBM Spectrum Protect-Serverspeicher, erhöht jedoch den Umfang der Serverdatenbankverarbeitung, die zur Überwachung der Änderungen erforderlich ist.

OPPortunistic

Wenn sich bei der Methode 'OPPortunistic' System Writer-Dateien seit der letzten Systemstatussicherung geändert haben, werden alle System Writer-Dateien gesichert.

Wie die Methode 'PROGressive' erfordert diese Art der Systemstatussicherung auch die geringste Netzbandbreite und den geringsten IBM Spectrum Protect-Serverspeicher, wenn sich System Writer-Dateien seit der letzten Systemstatussicherung nicht geändert haben. Wenn sich System Writer-Dateien seit der letzten Systemstatussicherung geändert haben, wird der System Writer vollständig gesichert, was mehr Netzbandbreite und Serverspeicher erfordert. Bei der Methode 'OPPortunistic' ist der Umfang der durchgeführten Serverdatenbankverarbeitung geringer als bei der Methode 'PROGressive'.

FULL

Wenn FULL angegeben wird, werden alle System Writer-Dateien gesichert, selbst wenn sie sich seit der letzten Systemstatussicherung nicht geändert haben.

Diese Art der Systemstatussicherung erfordert die meiste Netzbandbreite und den meisten IBM Spectrum Protect-Serverspeicher, weil bei jeder Systemstatussicherungsoperation alle System Writer-Dateien gesichert werden. Diese Systemstatussicherungsmethode verursacht jedoch wenig Serverdatenbankverarbeitung.

Beispiele

Optionsdatei:

```
SYSTEMSTATEBACKUPMETHOD FULL
SYSTEMSTATEBACKUPMETHOD OPPORTUNISTIC
```

Befehlszeile:

```
backup systemstate -SYSTEMSTATEBACKUPMETHOD=FULL
```

Tapeprompt

Die Option tapeprompt gibt an, ob der Client für Sichern/Archivieren auf auf einen Bandladevorgang warten soll, der für eine Sicherung, Archivierung, Zurückschreibung oder einen Abruf erforderlich ist, oder ob eine Bedienerführung für die Auswahl angezeigt werden soll.

In der GUI des Clients für Sichern/Archivieren kann im Dialog 'Datenträgermount' der Wert `Informationen nicht verfügbar` in den Feldern für Einheit und Datenträgerkennsatz angezeigt werden, wenn Sie eine standardmäßige (auch als klassisch bezeichnete) Zurückschreibungs- oder Abrufoperation ausführen. Dieser Wert bedeutet, dass diese Informationen nur für Zurückschreibungs- oder Abrufoperationen ohne Abfrage verfügbar sind, nicht für eine Standardzurückschreibungs- oder -abrufoperation. Im Feld Einheit wird der Name der Einheit angezeigt, auf der der für die Verarbeitung eines Objekts benötigte Datenträger geladen werden soll. Im Feld Datenträgerkennsatz wird der Name des für die Verarbeitung benötigten Datenträgers angezeigt.

Unabhängig von der Einstellung der Option tapeprompt erfolgt während einer geplanten Operation keine Aufforderung zum Bandladevorgang.

Die Option tapeprompt kann in den folgenden Befehlen verwendet werden:

- archive
- delete archive
- delete backup
- incremental
- restore
- retrieve
- selective

Anmerkung: Diese Option kann auch auf dem Server definiert werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Allgemein über das Kontrollkästchen Bedienerführung vor dem Bandladevorgang im Profileditor definieren.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Allgemein über das Kontrollkästchen Bedienerführung vor dem Bandladevorgang im Profileditor definieren.

Syntax

```
.-No--.
```

```
>>-TAPEPrompt--+-----+-----------------------------------------><
              '-Yes-'
```

Parameter

No
: Es wird keine Bedienerführung für die Auswahl angezeigt. Der Server wartet auf das Laden des entsprechenden Bandes. Dies ist der Standardwert.
Anmerkung: Für API-Anwendungen ermöglicht dies die direkte Sicherung auf Band.

Yes
: Wenn zum Sichern, Archivieren, Zurückschreiben oder Abrufen von Daten ein Band erforderlich ist, wird eine Bedienerführung angezeigt. Auswahlmöglichkeiten der Bedienerführung: Auf das Laden des entsprechenden Bandes warten, immer auf das Laden eines Bandes warten, ein bestimmtes Objekt überspringen, alle Objekte auf einem Band überspringen, alle Objekte auf allen Bändern überspringen oder die gesamte Operation abbrechen.

Beispiele

Optionsdatei:
```
tapeprompt yes
```
Befehlszeile:
```
-tapep=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Tcpadminport

Verwenden Sie die Option tcpadminport, um eine separate TCP/IP-Anschlussnummer anzugeben, an der der Server Anforderungen für Verwaltungsclientsitzungen erwartet. Dies ermöglicht sichere Verwaltungssitzungen innerhalb eines privaten Netzwerks.

Die Einstellung für die Clientoption tcpadminport ist davon abhängig, wie die IBM Spectrum Protect-Serveroptionen tcpadminport und adminonclientport konfiguriert sind. Der Server verfügt über eine Einstellung tcpadminport, die anzeigt, an welchem Anschluss der Server für Verwaltungssitzungen empfangsbereit ist, und über die Einstellung adminonclientport, die entweder yes oder no sein kann.

Ist tcpadminport auf dem Server nicht definiert, sind Verwaltungssitzungen an demselben Anschluss zulässig wie Clientsitzungen.

Ist tcpadminport auf dem Server definiert, sind Verwaltungssitzungen an dem durch diese Einstellung angegebenen Anschluss zulässig. In diesem Fall können die Verwaltungssitzungen, falls adminonclientport yes aktiv ist, entweder am regulären Clientanschluss eine Verbindung herstellen oder an dem Anschluss, der durch tcpadminport angegeben ist. Wenn adminonclientport no aktiv ist, können die Verwaltungssitzungen nur an dem Anschluss, der durch tcpadminport angegeben ist, eine Verbindung herstellen.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Verwaltungsanschluss des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Verwaltungsanschluss des Profileditors definieren.

Syntax

```
>>-TCPADMINPort--+- ---------------------------+--------------><
                 '-Verwaltungsanschlussadresse-'
```

Parameter

Verwaltungsanschlussadresse
: Gibt die Anschlussnummer des Servers an. Der Standardwert ist der Wert der Option tcpport.

Beispiele

Optionsdatei:

```
tcpadminport 1502
```

Tcpbuffsize

Die Option tcpbuffsize gibt die Größe des internen TCP/IP-Kommunikationspuffers an, der verwendet wird, um Daten zwischen dem Clientknoten und dem Server zu übertragen. Ein größerer Puffer kann die Übertragungsleistung verbessern, benötigt jedoch mehr Speicher.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Puffergröße des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Puffergröße des Profileditors definieren.

Syntax

```
>>-TCPBuffsize-- --Größe----------------------------------------><
```

Parameter

Größe
: Gibt die gewünschte Größe (in Kilobyte) für den internen TCP/IP-Kommunikationspuffer an. Der Wertebereich ist 1 bis 512; Standardwert ist 32.

  Je nach den Betriebssystemeinstellungen für die Übertragung akzeptiert das System unter Umständen nicht alle Werte in dem Bereich von 1 bis 512.

Beispiele

Optionsdatei:

```
tcpb 32
```

Befehlszeile:

```
-tcpbuffsize=32
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Tcpcadaddress

Die Option tcpcadaddress gibt eine TCP/IP-Adresse für dsmcad an. Normalerweise wird diese Option nicht benötigt. Verwenden Sie diese Option nur, wenn Ihr Clientknoten mehrere TCP/IP-Adressen hat oder wenn TCP/IP nicht die Standardübertragungsmethode ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein.

Syntax

```
>>-TCPCADAddress-- --CAD-Adresse------------------------------><
```

Parameter

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme
CAD-Adresse
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Windows-BetriebssystemeGibt einen TCP/IP-Internetdomänennamen oder eine numerische IP-Adresse an. Wenn Sie eine IPv6-Adresse angeben, müssen Sie die Option commmethod V6Tcpip angeben.

Beispiele

Optionsdatei:

```
tcpcada dsmclnt.example.com
```

Befehlszeile:

```
-tcpcadaddress=192.0.2.0
```

```
-tcpcadaddress=mycompany.example.com
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Windows-Betriebssysteme

```
-tcpcadaddress=2001:0DB8:0:0:0:0:0:0
```

Diese Option ist nur in der Anfangsbefehlszeile des Programms dsmcad gültig. Sie ist nicht mit anderen dsm-Modulen gültig.

Tcpclientaddress

Mit der Option tcpclientaddress kann eine TCP/IP-Adresse angegeben werden, wenn der Clientknoten des Benutzers über mehrere Adressen verfügt und der Server eine Verbindung zu einer anderen Adresse herstellen soll, als die, mit der die erste Verbindung zum Server hergestellt wurde.

Der Server verwendet diese Adresse, wenn er die Operation mit Zeitplanung über Serversystemanfrage beginnt.

Diese Option darf nur verwendet werden, wenn Sie für die Option schedmode den Parameter prompted angeben.

Wird sessioninitiation auf serveronly gesetzt, sollte der Wert für die Clientoption tcpclientaddress mit dem Wert der Servereinstellung HLAddress übereinstimmen.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys *innerhalb* einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Scheduler im Feld Ihre TCP/IP-Adresse im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Scheduler im Feld Ihre TCP/IP-Adresse im Profileditor definieren.

Syntax

```
>>-TCPCLIENTAddress-- --Clientadresse--------------------------><
```

Parameter

Clientadresse
Gibt die TCP/IP-Adresse an, die der Server für die Kommunikation mit Ihrem Clientknoten verwenden soll. Geben Sie einen TCP/IP-Internetdomänennamen oder eine numerische IP-Adresse an. Die numerische IP-Adresse kann entweder eine TCP/IPv4- oder eine TCP/IPv6-Adresse sein. Sie können IPv6-Adressen nur verwenden, wenn Sie die Option commmethod *V6Tcpip* angegeben haben.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeOptionsdatei:
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
tcpclienta dsmclnt.example.comoder
tcpclienta 192.0.2.21
```

Windows-BetriebssystemeBefehlszeile:
Windows-Betriebssysteme

```
-tcpclientaddress=192.0.2.0
-tcpclientaddress=example.mycompany.mydomain.com
-tcpclientaddress=2001:0DB8:0:0:0:0:0:0
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Tcpclientport

Mit der Option tcpclientport wird eine TCP/IP-Anschlussnummer für den Server angegeben, mit der eine Verbindung zum Client hergestellt wird, wenn der Server die Operation mit Zeitplanung über Serversystemanfrage beginnt.

Diese Option darf nur verwendet werden, wenn Sie für die Option schedmode den Parameter prompted angeben.

Wird sessioninitiation auf serveronly gesetzt, sollte der Wert für die Clientoption tcpclientport mit dem Wert für die Serveroption LLAddress übereinstimmen.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Scheduler im Feld Ihr TCP/IP-Anschluss im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Scheduler im Feld Ihr TCP/IP-Anschluss im Profileditor definieren.

Syntax

```
>>-TCPCLIENTPort-- --Clientanschlussadresse--------------------><
```

Parameter

Clientanschlussadresse
: Gibt die TCP/IP-Anschlussadresse an, die der Server für die Kommunikation mit Ihrem Clientknoten verwenden soll. Der Wertebereich ist 1 bis 32767; der Standardwert ist 1501.

Beispiele

Optionsdatei:

```
tcpclientp 1502
```

Befehlszeile:

```
-tcpclientport=1492
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Tcpnodelay

Die Option tcpnodelay gibt an, ob der Client die Verzögerung beim Senden aufeinanderfolgender kleiner Pakete im Netz pro Transaktion inaktiviert.

Ändern Sie den Wert nur unter den folgenden Bedingungen vom Standardwert in yes:

- Sie werden von der technischen Unterstützung von IBM® aufgefordert, die Option zu ändern.
- Sie kennen die Auswirkung des TCP-Nagle-Algorithmus auf die Netzübertragung. Wird für die Option der Wert no angegeben, wird der Nagle-Algorithmus aktiviert, wodurch das Senden kleiner, aufeinanderfolgender Pakete verzögert wird.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeDiese Option ist für alle UNIX- und Linux-Clients gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Optionsdatei

AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Übertragung des Profileditors definieren. Wählen Sie Transaktion sofort an den Server senden aus.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung des Profileditors definieren. Wählen Sie Transaktion sofort an den Server senden aus.

Syntax

```
                .-Yes-.
>>-TCPNodelay--+-----+-----------------------------------------><
                '-No--'
```

Parameter

No
: Gibt an, dass der Server das Senden kleiner, aufeinanderfolgender Pakete über das Netz verzögert. Die Einstellung dieser Option auf no kann die Leistung herabsetzen.

Yes
: Gibt an, dass der Server das sofortige Senden kleiner, aufeinanderfolgender Pakete über das Netz gestattet. Der Standardwert ist yes.

Beispiele

Optionsdatei:

```
tcpnodelay yes
```

Befehlszeile:

Nicht zutreffend.

Tcpport

Die Option tcpport gibt eine TCP/IP-Anschlussadresse für den IBM Spectrum Protect-Server an. Diese Adresse kann beim Administrator erfragt werden.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Serveranschluss des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Serveranschluss des Profileditors definieren.

Syntax

```
>>-TCPPort-- --Anschlussadresse------------------------------><
```

Parameter

Anschlussadresse
: Gibt die TCP/IP-Anschlussadresse für die Datenübertragung mit einem Server an. Der Wertebereich ist 1 bis 32767; der Standardwert ist 1500.

Beispiele

Optionsdatei:

```
tcpp 1501
```

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`-tcpport=1501`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeNicht zutreffend.

Windows-BetriebssystemeDiese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Tcpserveraddress

Die Option tcpserveraddress gibt die TCP/IP-Adresse für den IBM Spectrum Protect-Server an. Sie können diese Serveradresse beim Administrator erfragen.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Serveradresse des Profileditors definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Serveradresse des Profileditors definieren.

Wird diese Option nicht angegeben, versucht der Client, einen Server zu kontaktieren, der auf demselben Computer wie der Client für Sichern/Archivieren ausgeführt wird.

Syntax

```
>>-TCPServeraddress-- --Serveradresse-------------------------><
```

Parameter

Serveradresse

Gibt eine 1- bis 64-stellige TCP/IP-Adresse für einen Server an. Geben Sie einen TCP/IP-Domänennamen oder eine numerische IP-Adresse an. Die numerische IP-Adresse kann entweder eine TCP/IP-V4- oder eine TCP/IP-V6-Adresse sein. Sie können IPv6-Adressen nur verwenden, wenn Sie die Option commmethod V6Tcpip angegeben haben.

Beispiele

Optionsdatei:

```
tcps dsmchost.example.com
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeNicht zutreffend.

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`-tcpserveraddress=129.33.24.99`

```
-tcpserveraddress=2002:92b:111:221:128:33:10:249
```

Windows-BetriebssystemeDiese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Tcpwindowsize

Mit der Option tcpwindowsize können Sie die Größe in Kilobyte angeben, die Sie für das TCP/IP-Schiebefenster für Ihren Clientknoten verwenden wollen.

Der sendende Host kann keine mehr Daten senden, bis er eine Empfangsbestätigung und eine Aktualisierung des TCP-Empfangsfensters empfängt. Jedes TCP-Paket enthält das in der Verbindung angegebene TCP-Empfangsfenster. Ein größeres Fenster ermöglicht dem Sender, weiterhin Daten zu senden, und verbessert möglicherweise die Leistung.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Fenstergröße im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung im Feld Fenstergröße im Profileditor definieren.

Syntax

```
>>-TCPWindowsize-- --Fenstergröße------------------------------><
```

Parameter

AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeFenstergröße
AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeGibt die gewünschte Größe (in Kilobyte) für das TCP/IP-Schiebefenster des Clientknotens an. Der Wertebereich ist 0 bis 2048. Der Wert 0 ermöglicht dem Client die Verwendung der standardmäßigen TCP-Fenstergröße des Betriebssystems. Werte von 1 bis 2048 zeigen an, dass die Fenstergröße im Bereich von 1 KB bis 2 MB liegt. Wenn Sie einen Wert kleiner als 1 angeben, nimmt die TCP-Fenstergröße standardmäßig den Wert 1 an. Wenn Sie einen Wert größer als 2048 angeben, nimmt die TCP-Fenstergröße standardmäßig den Wert 2048 an.
AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeFür Clients für Sichern/Archivieren ist der Standardwert für diesen Parameter 63 KB.
AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-BetriebssystemeFür IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ist der Standardwert für diesen Parameter 512 KB.
AIX-BetriebssysteLinux-BetriebssysteOracle Solaris-BetriebssysteMac OS X-Betriebssysteme
Anmerkungen:

- Das TCP-Fenster fungiert als Puffer im Netzwerk. Es bezieht sich nicht auf die Option tcpbuffsize oder auf die im Client- oder Serverspeicher zugeordneten Sende- und Empfangspuffer.
- Eine Fenstergröße, die größer als der Pufferspeicherbereich auf dem Netzadapter ist, kann unter Umständen den Durchsatz verschlechtern, da Pakete, die auf dem Adapter verloren gingen, erneut gesendet werden müssen.
- Je nach den Betriebssystemeinstellungen für die Übertragung akzeptiert das System unter Umständen nicht alle Werte des Wertebereichs.
- Die Option tcpwindowsize überschreibt die Standardgröße der Sende- und Empfangsfenster für TCP/IP-Sitzungen des Betriebssystems.

Windows-BetriebssystemeFenstergröße
Windows-BetriebssystemeGibt die gewünschte Größe (in Kilobyte) für das TCP/IP-Schiebefenster des Clientknotens an. Der Wertebereich ist 0 bis 2048. Der Wert 0 ermöglicht dem Client die Verwendung der standardmäßigen TCP-Fenstergröße des Betriebssystems. Werte von 1 bis 2048 zeigen an, dass die Fenstergröße im Bereich von 1 KB bis 2 MB liegt. Wenn Sie einen Wert kleiner als 1 angeben, nimmt die TCP-Fenstergröße standardmäßig den Wert 1 an. Wenn Sie einen Wert größer als 2048 angeben, nimmt die TCP-Fenstergröße standardmäßig den Wert 2048 an.
Windows-BetriebssystemeFür Clients für Sichern/Archivieren ist der Standardwert für diesen Parameter 63 KB.
Windows-BetriebssystemeFür IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ist der Standardwert für diesen Parameter 512 KB.
Windows-Betriebssysteme
Anmerkungen:

- Das TCP-Fenster fungiert als Puffer im Netzwerk. Es bezieht sich nicht auf die Option tcpbuffsize oder auf die im Client- oder Serverspeicher zugeordneten Sende- und Empfangspuffer.
- Eine Fenstergröße, die größer als der Pufferspeicherbereich auf dem Netzadapter ist, kann unter Umständen den Durchsatz verschlechtern, da Pakete, die auf dem Adapter verloren gingen, erneut gesendet werden müssen.
- Je nach den Betriebssystemeinstellungen für die Übertragung akzeptiert das System unter Umständen nicht alle Werte des Wertebereichs.
- Die Option tcpwindowsize überschreibt die Standardgröße der Sende- und Empfangsfenster für TCP/IP-Sitzungen des Betriebssystems.
- Windows stellt eine größere TCP-Empfangsfenstergröße zur Verfügung, wenn mit Hosts kommuniziert wird, die ebenfalls diese Unterstützung (bekannt als RFC1323) bieten. In diesen Umgebungen kann ein Wert größer als 63 nützlich sein.

Beispiele

Optionsdatei:

```
tcpwindowsize 63
```

Befehlszeile:

```
-tcpw=63
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Timeformat

Mit der Option timeformat wird das Format angegeben, in dem die Systemzeit angezeigt oder eingegeben werden soll.

Windows-BetriebssystemeVerwenden Sie diese Option, wenn Sie das standardmäßige Zeitformat für die Sprache des von Ihnen verwendeten Nachrichtenrepositorys ändern wollen.

Der Client für Sichern/Archivieren und der Verwaltungsclient erhalten standardmäßig Formatinformationen aus der Ländereinstellungsdefinition, die beim Aufruf des Clients aktiv ist. Ausführliche Informationen zur Definition der länderspezifischen Angaben können der Dokumentation auf dem lokalen System entnommen werden.

Anmerkung: Die Option timeformat betrifft nicht den Web-Client. Der Web-Client verwendet das Zeitformat der Ländereinstellung, die im Browser aktiv ist. Ist im Browser eine Ländereinstellung aktiv, die der Client nicht unterstützt, verwendet der Web-Client das Zeitformat für amerikanisches Englisch.

Die Option timeformat können Sie in folgenden Befehlen verwenden:

- delete archive
- delete backup
- expire
- query archive
- Windows-Betriebssystemequery asr
- query backup
- query filespace
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemequery image
- query nas
- Windows-Betriebssystemequery systemstate
- restore
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemerestore image
- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssystemerestore nas
- Windows-Betriebssystemerestore registry
- retrieve
- set event

Wenn Sie die Option timeformat mit einem Befehl eingeben, muss diese Option vor den Optionen fromtime, pittime und totime stehen.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Regionale Einstellungen im Feld Zeitformat im Profileditor definieren.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Regionale Einstellungen im Feld Zeitformat im Profileditor definieren.

Syntax

```
>>-TIMEformat-- --Formatnummer-------------------------------><
```

Parameter

Formatnummer
: Zeigt die Zeit in einem der hier aufgeführten Formate an. Wählen Sie die Formatnummer aus, die dem zu verwendenden Format entspricht. Wenn Sie die Option timeformat in einem Befehl eingeben, muss sie vor den Optionen fromtime, pittime und totime stehen.

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme0
  : AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDas durch die Ländereinstellung definierte Zeitformat verwenden (gilt nicht für Mac OS X). Dieser Wert ist der Standardwert, wenn das durch die Ländereinstellung angegebene Format aus Ziffern, Trennzeichen und, falls anwendbar, der Zeichenfolge AM oder PM besteht.

  1
  : 23:00:00

    AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeDies ist der Standardwert, wenn das durch die Ländereinstellung angegebene Format nicht aus Ziffern, Trennzeichen und, falls anwendbar, der

Zeichenfolge AM oder PM besteht.

2
: 23,00,00

3
: 23.00.00

4
: 12:00:00 A/P

5
: A/P 12:00:00

Beispiele

Optionsdatei:
```
timeformat 4
```
Befehlszeile:
```
-time=3
```

Diese Option ist in der Anfangsbefehlszeile und im interaktiven Modus gültig. Wird die Option im interaktiven Modus eingegeben, ist nur der Befehl betroffen, mit dem sie eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf den Wert zu Beginn der interaktiven Sitzung zurückgesetzt. Dies ist der Wert aus der Datei dsm.opt, sofern er nicht durch die Anfangsbefehlszeile oder eine vom Server erzwungene Option überschrieben wurde.

Weitere Hinweise zur Angabe von Datums- und Zeitformaten

Das Datums- oder Zeitformat, das Sie mit dieser Option angeben, muss verwendet werden, wenn Optionen verwendet werden, deren Eingabe aus Datums- und Zeitangaben besteht. Beispiele sind: totime, fromtime, todate, fromdate und pittime.

Wenn Sie beispielsweise die Option timeformat als `TIMEFORMAT 4` angeben, muss der Wert, den Sie für die Option fromtime oder totime angeben, als Zeit angegeben werden, wie z. B. `12:24:00pm`. Die Angabe `13:24:00` wäre nicht gültig, da `TIMEFORMAT 4` als Angabe für die Stunde eine ganze Zahl, die kleiner-gleich 12 ist, erfordert. Wenn in einer Option für die Stunde Werte bis zu 24 angegeben und Kommas als Trennzeichen verwendet werden sollen, müssen Sie `TIMEFORMAT 2` angeben.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-Betriebssysteme

Datums- und Zeitformate in der Konfigurationsdatei für die Systemländereinstellung konfigurieren

Sie können Datums- und Zeitformate angeben, indem Sie diese in der Ländereinstellungsdatei des Systems konfigurieren. Wenn Sie Datums- und Zeitformate in der Ländereinstellungsdatei angeben, müssen diese mithilfe einer Untermenge von Formatkennungen definiert werden, die Zahlen erstellen und von der Funktion `strftime()` der Programmiersprache C unterstützt werden. Sie können Datums- und Zeitformate in den Konfigurationseinstellungen für Ihre Ländereinstellung mithilfe der folgenden Kennungen definieren.

Datumskennungen

- `%Y` - das Jahr, angegeben mit 4 Ziffern, z. B. 2011
- `%y` - das Jahr, Angabe nur der letzten beiden Ziffern, z. B. 11 (nicht 2011)
- `%m` - der Monat, angegeben als Dezimalzahl (1-12)
- `%d` - der Tag des Monats (1-31)

In den Datumskennungen können Sie nur eine einzige Jahreskennung angeben. Sie dürfen `%Y` und `%y` nicht gleichzeitig angeben. Der Modifikator E (Großbuchstabe E) kann vor Datumskennungen stehen, um das Alternativformat der Ländereinstellung für das Jahr, den Monat oder den Tag zu erstellen. Wenn kein Alternativformat vorhanden ist, wird der Modifikator E ignoriert. Trennen Sie die Kennungen durch ein einzelnes 7-Bit-ASCII-Zeichen voneinander. Häufig verwendete Trennzeichen umfassen Doppelpunkte (:), Kommas (,), Punkte (.), Bindestriche (-) und Schrägstriche (/). Sie dürfen keine Mehrbytezeichen als Trennzeichen verwenden.

Zeitkennungen

- `%H` - die Stunde, angegeben im 24-Stunden-Format (00-23)
- `%I` - die Stunde, angegeben im 12-Stunden-Format (00-12)
- `%M` - die Minuten nach der Stunde (00-59)
- `%S` - die Sekunden nach der Minute (00-59)
- `%p` - fügt den Anzeiger AM (vor 12 Uhr mittags) oder PM (nach 12 Uhr mittags) ein.

In den Zeitkennungen können Sie nur eine einzige Stundenkennung angeben. Sie dürfen `%I` und `%H` nicht gleichzeitig angeben.

Der Modifikator O (Großbuchstabe O) kann vor Zeitkennungen stehen, um das Alternativformat der Ländereinstellung für die Stunde, die Minuten oder die Sekunden zu erstellen. Der Modifikator O darf nicht vor der Kennung `%p` stehen. Trennen Sie die Kennungen durch ein einzelnes 7-Bit-ASCII-Zeichen voneinander. Häufig verwendete Trennzeichen umfassen Doppelpunkte (:), Kommas (,) oder Punkte (.). Sie dürfen keine Mehrbytezeichen als Trennzeichen verwenden. Zwischen der Kennung `%p` und dem Trennzeichen, das vor oder hinter der Kennung steht, dürfen Sie kein Trennzeichen angeben.

Beispiele für in den Ländereinstellungen konfigurierte Zeitformate

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeUm ein bestimmtes Zeitformat zu definieren, editieren Sie die Konfigurationsdatei für die Ländereinstellung und ändern Sie die Zeile `t_fmt` gemäß den Anforderungen. Das ausgewählte Zeitformat gilt sowohl für die Ausgabe als auch für die Eingabe. Nachdem die Konfigurationsdatei für die Ländereinstellung editiert wurde, muss der Befehl localedef ausgeführt werden, um die endgültige Ländereinstellungsdatei zu erstellen.

Tabelle 1. Mustereinstellungen für das Zeitformat in der Konfigurationsdatei für die Ländereinstellung (Zeile t_fmt)

Beispiel	Ergebnis
"%H:%M:%S"	Zeigt die Zeit im Format *hh:mm:ss* an; *hh* liegt im Bereich von 0 bis 23.
"%H,%M,%S"	Zeigt die Zeit im Format *hh,mm,ss* an; *hh* liegt im Bereich von 0 bis 23.
"%I,%M,13p"	Zeigt die Zeit im Format *hh,mm,ssA/P* an, wobei *hh* (Stunde) den Bereich 1 bis 12 aufweist und *A/P* die Abkürzung für ante-meridian (vormittags, AM in Englisch) oder post-meridian (nachmittags, PM in Englisch) ist.

Beispiele für in den Ländereinstellungen konfigurierte Datumsformate

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeUm ein bestimmtes Datumsformat zu definieren, editieren Sie die Konfigurationsdatei und ändern Sie die Zeile `d_fmt` gemäß Ihren Anforderungen. Das ausgewählte Datumsformat gilt sowohl für die Ausgabe als auch für die Eingabe.

Tabelle 2. Mustereinstellungen für das Datumsformat in der Konfigurationsdatei für die Ländereinstellung (Zeile d_fmt)

Beispiel	Ergebnis
"%m/%d/%y"	Zeigt das Datum im Format MM/TT/JJ an.
"%d.%m.%Y"	Zeigt das Datum im Format TT.MM.JJJJ an.

AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Toc

Verwenden Sie die Option toc mit dem Befehl backup nas oder der Option include.fs.nas, um anzugeben, ob der Client für Sichern/Archivieren für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) speichern soll.

Bei der Entscheidung, ob die Inhaltsverzeichnisinformationen (TOC-Informationen) gespeichert werden sollen, müssen Sie Folgendes berücksichtigen:

- Wenn Sie TOC-Informationen speichern, können Sie den Serverbefehl QUERY TOC verwenden, um den Inhalt einer Dateisystemsicherung zu bestimmen, sowie den Serverbefehl RESTORE NODE, um einzelne Dateien oder Verzeichnisstrukturen zurückzuschreiben.
- Sie können auch den Web-Client verwenden, um die gesamte Baumstruktur des Dateisystems zu untersuchen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen.
- Die Erstellung eines Inhaltsverzeichnisses erfordert, dass Sie das Attribut TOCDESTINATION in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsimage gebunden wird. Beachten Sie, dass die TOC-Erstellung während der Sicherungsoperation eine zusätzliche Verarbeitung, zusätzliche Netzressourcen, zusätzlichen Speicherpoolspeicher und möglicherweise einen zusätzlichen Mountpunkt erfordert.
- Wenn Sie keine TOC-Informationen speichern, können Sie über den Serverbefehl RESTORE NODE dennoch einzelne Dateien und Verzeichnisstrukturen zurückschreiben, wenn Sie den vollständig qualifizierten Namen jeder Datei bzw. jedes Verzeichnisses und das Image kennen, in dem das Objekt gesichert wurde.

Unterstützte Clients

AIX-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist nur für AIX- und Solaris-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssystemeOracle Solaris-BetriebssystemeFügen Sie die Anweisung include.fs.nas, die den Wert toc enthält, in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein.

Windows-BetriebssystemeFügen Sie die Anweisung include.fs.nas, die den Wert toc enthält, in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
        .-Preferred-.
>>-TOC--+-----------+-----------------------------------------><
```

```
+-Yes-------+
'-No--------'
```

Parameter

Yes
: Gibt an, dass der Client während einer Imagesicherung des NAS-Dateisystems TOC-Informationen speichert. Die Sicherung schlägt jedoch fehl, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt.

No
: Gibt an, dass der Client während einer Imagesicherung des NAS-Dateisystems keine TOC-Informationen speichert.

Preferred
: Gibt an, dass der Client während einer Imagesicherung des NAS-Dateisystems TOC-Informationen speichert. Die Sicherung schlägt nicht fehl, wenn während der Erstellung des Inhaltsverzeichnisses ein Fehler auftritt. Dies ist der Standardwert.

Anmerkung: Ist die Option mode auf differential gesetzt und setzen Sie die Option toc auf preferred oder yes, ohne dass das letzte vollständige Image über ein Inhaltsverzeichnis (TOC) verfügt, führt der Client eine vollständige Imagesicherung aus und erstellt ein TOC.

Beispiele

Optionsdatei:

```
include.fs.nas netappsj/vol/vol0 homemgmtclass toc=yes
```

AIX-Betriebssysteme Oracle Solaris-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Oracle Solaris-Betriebssysteme`backup nas -nasnodename=netappsj /vol/vol0 -toc=yes`

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`backup nas -nasnodename=netappsj {/vol/vol0} -toc=yes`

Todate

Mit der Option todate können Sie in Verbindung mit der Option totime ein Enddatum und eine Endzeit angeben, bis zu der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen.

Mit den Optionen todate und totime kann in Verbindung mit den Optionen fromtime und fromdate eine Liste der in einem bestimmten Zeitraum gesicherten oder archivierten Dateien angefordert werden. Es kann beispielsweise eine Liste mit Dateien angefordert werden, die zwischen 6:00 Uhr am 1. Juli 2002 und 23:59 Uhr am 30. Juli 2002 gesichert wurden.

Die Option todate ist in den folgenden Befehlen zu verwenden:

- delete backup
- query archive
- query backup
- restore
- restore group
- retrieve

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-TODate = - --Datum-----------------------------------------><
```

Parameter

Datum
: Gibt ein Enddatum an. Das Datum muss in dem mit der Option dateformat ausgewählten Format eingegeben werden.

  Wenn dateformat in einem Befehl angegeben wird, muss diese Option vor den Optionen fromdate, pitdate und todate stehen.

Beispiele

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssysteme `dsmc restore "/Users/agordon/Documents/*" -todate=12/11/2003`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme`dsmc restore "/home/user1/*" -todate=12/11/2003`

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme
```
dsmc restore -todate=12/11/2003 c:\myfiles\
```

Totime

Mit der Option totime können Sie in Verbindung mit der Option todate ein Enddatum und eine Endzeit angeben, bis zu der Sie während einer Zurückschreibungs-, Abruf- oder Abfrageoperation nach Sicherungen oder Archivierungen suchen wollen. Der Client für Sichern/Archivieren ignoriert diese Option, wenn Sie die Option todate nicht angeben.

Mit den Optionen totime und todate kann in Verbindung mit den Optionen fromtime und fromdate eine Liste der in einem bestimmten Zeitraum gesicherten Dateien angefordert werden. Beispielsweise können Sie eine Liste mit Dateien anfordern, die zwischen 6:00 Uhr am 1. Juli 2003 und 23:59 Uhr am 30. Juli 2003 gesichert wurden.

Die Option totime ist in den folgenden Befehlen zu verwenden:

- delete backup
- query archive
- query backup
- restore
- restore group
- retrieve

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-TOTime = - --Zeit-----------------------------------------><
```

Parameter

Zeit

Gibt eine Endzeit an. Wenn keine Zeit angegeben wird, lautet der Standardwert 23:59:59. Die Zeit muss in dem mit der Option timeformat ausgewählten Format angegeben werden.

Wenn die Option timeformat in einem Befehl angegeben wird, muss sie vor den Optionen fromtime, pittime und totime stehen.

Beispiele

Mac OS X-BetriebssystemeBefehlszeile:

Mac OS X-Betriebssysteme
```
dsmc restore "/Users/van/Documents/myfiles/*" -todate=09/17/2003 -totime=23:00:00
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme
```
dsmc restore "/home/user1/*" -todate=09/17/2003 -totime=23:00:00
```

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme
```
dsmc query backup -totime=23:59:00 -todate=06/30/2003 c:\mybackups\
```

Txnbytelimit

Mit der Option txnbytelimit wird die Anzahl Kilobyte angegeben, die das Clientprogramm puffert, bevor eine Transaktion an den Server gesendet wird.

Eine *Transaktion* ist die Arbeitseinheit, die zwischen dem Client und dem Server ausgetauscht wird. Eine Transaktion kann mehrere Dateien oder Verzeichnisse enthalten. Diese werden als *Transaktionsgruppe* bezeichnet.

Mit der Option txnbytelimit können Sie steuern, wie viele Daten zwischen Client und Server gesendet werden, bevor der Server die Daten und Änderungen in der Serverdatenbank festschreibt. Die Steuerung des gesendeten Datenvolumens wirkt sich auf die Geschwindigkeit aus, mit der der Client die Transaktionen ausführt. Die gesendete Datenmenge gilt, wenn Dateien während der Sicherung zusammengefasst werden oder wenn Dateien während einer Zurückschreibung vom Server empfangen werden.

Wenn die in txngroupmax angegebene Anzahl erreicht ist, sendet der Client die Dateien an den Server, auch wenn der Bytegrenzwert für die Transaktion nicht erreicht ist.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein. Sie können diese Option auf der Registerkarte Allgemein im Feld Transaktionspuffergröße des Profileditors definieren.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Allgemein im Feld Transaktionspuffergröße des Profileditors definieren.

Syntax

```
>>-TXNBytelimit-- --Nummer-------------------------------------><
```

Parameter

Zahl
: Gibt die Anzahl Kilobyte an, die das Clientprogramm an den Server sendet, bevor die Transaktion festgeschrieben wird. Der Wertebereich ist 300 bis 34359738368 (32 GB). Der Standardwert ist 25600 KB. Die Anzahl kann als Ganzzahl oder als Ganzzahl mit einem der folgenden Qualifikationsmerkmale für die Einheit angegeben werden:

  - K oder k (Kilobyte)
  - M oder m (Megabyte)
  - G oder g (Gigabyte)

  Wird kein Qualifikationsmerkmal für die Einheit angegeben, wird Kilobyte für die Ganzzahl verwendet.

  Einschränkung: Die Option txnbytelimit unterstützt keine Dezimalzahlen und nur ein Buchstabe für die Einheit ist zulässig. Beispiele: K, M oder G.

Beispiele

Optionsdatei:

```
txnb 25600
txnb 2097152
txnb 2097152k
txnb 2048m
txnb 2g
txnb 32G
```

Befehlszeile:

```
-txnb=25600
-txnb=16G
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Type

Verwenden Sie die Option type im Befehl query node, um den Typ des abzufragenden Knotens anzugeben. Verwenden Sie diese Option im Befehl set event, um eine Löschsperre zu aktivieren oder freizugeben bzw. um den Aufbewahrungszeitraum zu starten.

Unterstützte Clients

 AIX-BetriebssystemeDiese Option ist auch für den Befehl set password mit dem Typ TSM auf AIX-Clients gültig.

 Windows-BetriebssystemeDiese Option ist auch für den Befehl set password mit dem Typ TSM oder FILER gültig.

 AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist nur für AIX- und Solaris-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

 Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Syntax

```
.-any----.
```

```
>>-TYpe = -+--------+-------------------------------------------><
          +-nas----+
          +-server-+
          '-client-'
```

Parameter

nas
: Gibt alle auf dem Server registrierten NAS-Knoten an.

server
: Gibt Clientknoten an, die andere IBM Spectrum Protect-Server sind.

client
: Gibt Clientknoten an, die Clients für Sichern/Archivieren sind.

Beispiele

Befehlszeile:
:  AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme`query node -type=nas`

AIX-BetriebssystemeLinux-Betriebssysteme

Updatectime

Überprüfen Sie mithilfe der Option updatectime das Attribut für die Änderungszeit (ctime) während einer Teilsicherungsoperation.

Unterstützte Clients

Diese Option ist nur für AIX- und Linux-Clients in GPFS-Dateisystemen gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

```
                .-no--.
>>-UPDATECTime--+-----+-----------------------------------------><
                '-yes-'
```

Parameter

no
: Der Client für Sichern/Archivieren überprüft während einer Sicherungsoperation nicht das Attribut für die Änderungszeit (ctime). Dies ist der Standardwert.

yes
: Der Client für Sichern/Archivieren überprüft während einer Sicherungsoperation das Attribut für die Änderungszeit (ctime). Wenn sich das Attribut ctime seit der letzten Sicherungsoperation geändert hat, wird das Attribut ctime auf dem IBM Spectrum Protect-Server aktualisiert. Das Objekt wird nur gesichert, wenn es über ACLs oder erweiterte Attribute verfügt. Der Client überprüft Dateien und Verzeichnisse.

Beispiele

Optionsdatei:
```
updatect yes
```
Befehlszeile:
```
dsmc incr /proj/gpfs/test/ -updatectime=yes
```

 Windows-Betriebssysteme

Usedirectory

Die Option usedirectory fragt im Active Directory die Übertragungsmethode und den Server ab, zu dem eine Verbindung hergestellt werden soll.

Diese Option überschreibt die Parameter commmethod, die in der Clientoptionsdatei (dsm.opt) angegeben sind. Im Optimalfall aktiviert der Administrator nur einen einzigen Server und nur ein bestimmtes Übertragungsprotokoll für einen bestimmten Clientknoten. Die Angabe dieser Informationen in Active Directory erfolgt mithilfe des IBM Spectrum Protect-Servers unter Windows, der über einen Assistenten verfügt, der Sie

bei dieser Konfiguration unterstützt. Ist ein Knoten bei mehreren Servern registriert, die im Active Directory veröffentlicht sind, wird der erste Server verwendet, der bei der Active Directory-Abfrage zurückgegeben wird. Kann der Client keinen Kontakt zum Server herstellen, schlägt die Clientsitzung fehl.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Übertragung des Profileditors definieren.

Syntax

```
                .-No--.
>>-USEDIRectory--+-----+----------------------------------------><
                '-Yes-'
```

Parameter

Yes
: Gibt an, dass der Client die in der Clientoptionsdatei definierten commmethod-Parameter ignoriert und die Übertragungsmethode und den Server, zu dem eine Verbindung hergestellt werden soll, im Active Directory abfragt.

No
: Gibt an, dass der Client die in der Optionsdatei angegebene Übertragungsmethode verwendet. Ist keine Übertragungsmethode in der Optionsdatei angegeben, werden die Standardeinstellungen für Übertragungsmethode und Server verwendet.

Beispiele

Optionsdatei:

```
usedirectory no
```

Befehlszeile:

```
-usedir=yes
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme

Useexistingbase

Die Option useexistingbase wird verwendet, wenn Sie Momentaufnahmen sichern, die sich auf NetApp-Dateiserverdatenträgern befinden. Die Option useexistingbase gibt an, dass die jüngste Momentaufnahme, die sich auf dem zu sichernden Datenträger befindet, als Basismomentaufnahme während einer Momentaufnahmedifferenzsicherung verwendet werden soll.

Wenn diese Option nicht angegeben wird, wird eine neue Momentaufnahme auf dem Datenträger erstellt, der gesichert wird. Da Datenträger des Ziel-Dateiservers schreibgeschützt sind, muss useexistingbase bei der Ausführung von Momentaufnahmedifferenzsicherungen von Datenträgern des Ziel-Dateiservers angegeben werden. Wenn useexistingbase nicht angegeben wird, schlagen Momentaufnahmedifferenzsicherungen eines Datenträgers des Ziel-Dateiservers fehl, weil die neue Momentaufnahme auf dem schreibgeschützten Datenträger nicht erstellt werden kann.

Verwenden Sie bei der Sicherung von Datenträgern des Ziel-Dateiservers sowohl die Option useexistingbase als auch die Option diffsnapshot=latest, um sicherzustellen, dass während der Datenträgersicherung die neuesten Basis- und Differenzmomentaufnahmen verwendet werden.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Diese Option ist nur in der Befehlszeile gültig.

Syntax

```
>>-USEEXISTINGBase-------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Optionsdatei:

Nicht zutreffend.

Befehlszeile:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff
  -useexistingbase -basenameshotname="nightly.?"
```

Zugehörige Verweise:
Basesnapshotname

Usereplicationfailover

Die Option usereplicationfailover gibt an, ob die automatisierte Clientübernahme auf einem Clientknoten stattfindet.

Mit dieser Option können Sie die Übernahme eines Clientknotens aktivieren oder verhindern, dass eine Übernahme eines Clientknotens auf dem Sekundärserver stattfindet. Diese Option setzt die Konfiguration außer Kraft, die durch die Einstellungen des IBM Spectrum Protect-Serveradministrators auf dem Primärserver angegeben ist.

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in eine Serverzeilengruppe in der Datei dsm.sys ein.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                          .-Yes-.
>>-USEREPLICATIONFailover--+-----+-----------------------------><
                          '-No--'
```

Parameter

Yes
: Gibt an, dass eine automatische Übernahme des Clients auf dem Sekundärserver stattfinden soll, falls der Primärserver nicht verfügbar ist. Der Client verwendet die durch den Primärserver bereitgestellte Konfiguration, um eine Verbindung zum Sekundärserver herzustellen. Dies ist der Standardwert.

No
: Gibt an, dass keine automatische Übernahme des Clients auf dem Sekundärserver stattfindet.

Beispiele

Optionsdatei:

```
USEREPLICATIONFailover no
```

Befehlszeile:

Nicht zutreffend.

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme
Zugehörige Tasks:
Client für automatisierte Übernahme konfigurieren
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

Users (veraltet)

Diese Option ist veraltet.

V2archive

Verwenden Sie die Option v2archive im Befehl archive, um anzugeben, dass nur Dateien auf dem Server archiviert werden sollen.

Der Client für Sichern/Archivieren verarbeitet keine Verzeichnisse, die in dem Pfad der Quellendateispezifikation vorhanden sind.

Diese Option unterscheidet sich von der Option filesonly dadurch, dass bei der Option filesonly die Verzeichnisse, die im Pfad der Quellendateispezifikation bestehen, archiviert werden.

Die Optionen v2archive und dirsonly schließen sich gegenseitig aus und es wird eine Fehlernachricht angezeigt, wenn Sie beide Optionen zusammen im Befehl archive verwenden.

Wenn Sie diese Option verwenden, sollten Sie Folgendes berücksichtigen:

- Es kommt unter Umständen zu Leistungsproblemen, wenn große Datenmengen abgerufen werden, die mit dieser Option archiviert wurden.
- Sie sollten diese Option nur verwenden, wenn Sie über die Verfallsleistung auf einem Server besorgt sind, der bereits extrem große Mengen an archivierten Daten enthält.
- Gibt es mehrere Dateien mit demselben Namen für die Option v2archive, werden die Dateien mehrfach mit ihrer Verzeichnisstruktur archiviert. Die Option v2archive archiviert nur die Dateien.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-V2archive-------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Mac OS X-BetriebssystemeDieser Befehl:

Mac OS X-Betriebssysteme`dsmc archive "/Users/user2/Documents/*" -v2archive -su=y`.

Archiviert diese Dateien:

```
/Users/user2/Documents/file1
/Users/user2/Documents/file2
/Users/user2/Documents/file3
/Users/user2/Documents/dir2/file4
/Users/user2/Documents/dir2/file5
```

Anmerkung: Der Client archiviert `/Users/user2/Documents` und `/Users/user2/Documents/dir2` nicht.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDieser Befehl:

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme`dsmc archive "/home/relx/dir1/*" -v2archive -su=y`.

Archiviert diese Dateien:

```
/home/relx/dir1/file1
/home/relx/dir1/file2
/home/relx/dir1/file3
/home/relx/dir1/dir2/file4
/home/relx/dir1/dir2/file5
```

Anmerkung: Der Client archiviert `/home/relx/dir1` und `/home/relx/dir1/dir2` nicht.

Windows-BetriebssystemeDieser Befehl:

Windows-Betriebssysteme`dsmc archive c:\relx\dir1\ -v2archive -su=y`

Archiviert diese Dateien:

```
c:\relx\dir1\file1
c:\relx\dir1\file2
c:\relx\dir1\file3
c:\relx\dir1\dir2\file4
c:\relx\dir1\dir2\file5
```

Anmerkung: Der Client archiviert `c:\relx\dir1` und `c:\relx\dir1\dir2` nicht.

Verbose

Mit der Option verbose können Sie angeben, dass Sie detaillierte Verarbeitungsinformationen auf Ihrem Bildschirm anzeigen wollen. Dies ist der Standardwert.

Bei der Ausführung des Befehls incremental, selective oder archive werden Informationen zu allen Dateien angezeigt, die gesichert werden. Verwenden Sie die Option quiet, wenn diese Informationen nicht angezeigt werden sollen.

Das folgende Verhalten gilt, wenn die Optionen verbose und quiet verwendet werden:

- Wenn der Server entweder die Option quiet oder verbose in der Clientoptionsgruppe des Servers angibt, überschreiben die Servereinstellungen die Clientwerte, auch wenn auf dem Server für force der Wert no definiert ist.
- Wenn Sie quiet in Ihrer Datei dsm.opt und -verbose in der Befehlszeile angeben, hat -verbose Vorrang.
- Wenn Sie sowohl -quiet als auch -verbose in demselben Befehl angeben, hat die letzte Option, die bei der Optionsverarbeitung festgestellt wird, Vorrang. Wenn Sie -quiet -verbose angeben, hat -verbose Vorrang. Wenn Sie -verbose -quiet angeben, hat -quiet Vorrang.

 Mac OS X-BetriebssystemeDie Informationen werden im Fenster 'Schedulerstatus' auf Ihrem Bildschirm angezeigt. Diese Option ist nur gültig, wenn der Scheduler aktiv ist und der Client geplante Arbeit ausführt.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Befehlszeile über das Kontrollkästchen Keine Verarbeitungsdaten auf dem Bildschirm anzeigen im Profileditor definieren.

 Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Sie können diese Option auf der Registerkarte Befehlszeile über das Kontrollkästchen Keine Verarbeitungsdaten auf dem Bildschirm anzeigen im Profileditor definieren.

Syntax

```
>>-VErbose-----------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

Optionsdatei:

```
verbose
```

Befehlszeile:

```
-verbose
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Verifyimage

Verwenden Sie die Option verifyimage im Befehl restore image, um anzugeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll.

Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client für Sichern/Archivieren eine Warnung auf der Konsole und im Fehlerprotokoll aus.

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist nur für AIX-, Oracle Solaris- und alle Linux-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

 Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Syntax

```
>>-VERIFYImage-------------------------------------------------><
```

Parameter

Für diese Option gibt es keine Parameter.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeBefehlszeile:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme`dsmc restore image /usr -verifyimage`

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`dsmc restore image d: -verifyimage`

Virtualfsname

Verwenden Sie die Option virtualfsname im Befehl backup group, um den Namen des virtuellen Dateibereichs für die Gruppe anzugeben, mit dem die Operation ausgeführt werden soll. Die Angabe für virtualfsname darf nicht mit einem vorhandenen Dateibereichsnamen übereinstimmen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist für alle UNIX- und Linux-Clients außer Mac OS X gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig.

Syntax

```
>>-VIRTUALFsname = - --Dateibereichsname-----------------------><
```

Parameter

Dateibereichsname
: Gibt den Namen des Containers für die Gruppe an, mit dem die Operation ausgeführt werden soll.

Beispiele

Befehlszeile:

Mac OS X-Betriebssysteme

```
backup group -filelist=/Users/van/Documents/filelist1 -groupname=group1
-virtualfsname=/virtfs -mode=full
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1
-virtualfsname=/virtfs -mode=full
```

Windows-Betriebssysteme

```
backup group -filelist=c:\dir1\filelist1 -groupname=group1
-virtualfsname=\virtfs -mode=full
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Virtualmountpoint

Die Option virtualmountpoint definiert einen virtuellen Mountpunkt für ein Dateisystem, wenn Dateien für die Sicherung berücksichtigt werden sollen, die mit einem bestimmten Verzeichnis innerhalb dieses Dateisystems beginnen.

Die Verwendung der Option virtualmountpoint zum Angeben eines Verzeichnisses innerhalb eines Dateisystems ermöglicht einen direkten Pfad zu den Dateien, die gesichert werden sollen, wodurch sich die Verarbeitungszeit verkürzt. Das Definieren eines virtuellen Mountpunktes innerhalb

eines Dateisystems ist effizienter als das Definieren dieses Dateisystems mithilfe der Option domain und das anschließende Ausschließen der Dateien, die nicht gesichert werden sollen, mit der Option exclude in der Einschluss-/Ausschlussoptionsliste.

Mit der Option virtualmountpoint können virtuelle Mountpunkte für mehrere Dateisysteme, für lokale und ferne Dateisysteme und mehrere virtuelle Mountpunkte innerhalb desselben Dateisystems definiert werden. Virtuelle Mountpunkte können in einem Dateisystem, das durch ein automatisches Mountprogramm bearbeitet wird, nicht verwendet werden.

Sie können die Option virtualmountpoint verwenden, um nicht unterstützte Dateisysteme mit bestimmten Einschränkungen zu sichern. Informationen zur Verwendung von virtualmountpoint mit nicht unterstützten Dateisystemen befinden sich in Dateisystem- und ACL-Unterstützung.

Anmerkung: Wenn es sich bei dem Verzeichnis, das als virtueller Mountpunkt angegeben werden soll, um eine symbolische Verbindung handelt, muss für die Option followsymbolic der Wert Yes definiert werden. Wenn für diese Option no (der Standardwert) definiert wird, ist die Verwendung einer symbolischen Verbindung als virtueller Mountpunkt nicht zulässig. Zudem gilt: Wenn Sie ein Dateisystem sichern, dann einen virtuellen Mountpunkt hinzufügen und anschließend eine weitere Teilsicherung für das Dateisystem ausführen, verfallen die Dateien und Verzeichnisse in dem als virtueller Mountpunkt definierten Verzeichnis, da sie logisch in dem als virtueller Mountpunkt definierten Verzeichnis und nicht im Dateisystem enthalten sind.

Nach der Definition eines virtuellen Mountpunkts können Sie den Pfad und Verzeichnisnamen mit der Option domain entweder in der Clientoptionsdatei oder im Befehl incremental angeben, damit er bei Teilsicherungen berücksichtigt wird. Wenn Sie mit der Option virtualmountpoint eine Sicherung oder Archivierung ausführen, listet der Befehl query filespace in seiner Antwort den virtuellen Mountpunkt zusammen mit den anderen Dateisystemen auf. Im Allgemeinen werden Verzeichnisse, die Sie als virtuelle Mountpunkte definieren, als tatsächliche Dateisysteme behandelt, und sie erfordern, dass die Option virtualmountpoint in der Datei dsm.sys angegeben ist, damit die Dateien zurückgeschrieben oder abgerufen werden können.

Anmerkung: Wenn Sie eine Option virtualmountpoint angeben, wird der von dieser angegebene Pfad der Standardsicherungsdomäne (domain all-local) hinzugefügt. Der virtualmountpoint-Pfad wird immer als lokaler "Mountpunkt" angesehen, unabhängig vom Typ des realen Dateisystems, auf das er verweist.

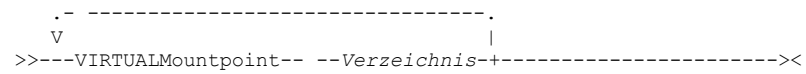
Unterstützte Clients

Diese Option ist für alle UNIX-Clients außer Mac OS X gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Syntax



Parameter

Verzeichnis
: Gibt den Pfad und den Verzeichnisnamen für das Verzeichnis an, das als virtueller Mountpunkt für ein Dateisystem verwendet werden soll. Im Pfad und im Verzeichnisnamen dürfen keine Platzhalterzeichen verwendet werden.

  Definieren Sie nur einen virtuellen Mountpunkt für jede Option virtualmountpoint, die Sie in Ihre Clientsystemoptionsdatei einfügen. Die Option virtualmountpoint können Sie nach Bedarf so oft angeben, dass alle gewünschten virtuellen Mountpunkte definiert werden.

Beispiele

Optionsdatei:

```
virtualmountpoint /afs/xyzcorp.com/home/ellen
virtualmountpoint /afs/xyzcorp.com/home/ellen/test/data
```

Befehlszeile:
: Nicht zutreffend.

Virtualnodename

Die Option virtualnodename gibt den Knotennamen Ihrer Workstation an, wenn Sie Dateien auf einer anderen Workstation zurückschreiben oder abrufen wollen.

Wenn Sie die Option virtualnodename in Ihrer Clientoptionsdatei oder in einem Befehl verwenden, gilt Folgendes:

- Windows-BetriebssystemeSie müssen den Namen angeben, den Sie mit der Option nodename in Ihrer Clientoptionsdatei (dsm.opt) angegeben haben. Dieser Name sollte sich von dem Namen unterscheiden, den der Befehl hostname auf Ihrer Workstation zurückgibt.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSie müssen den Namen angeben, den Sie mit der Option nodename in Ihrer Clientsystemoptionsdatei (dsm.sys) angegeben haben. Dieser Name sollte sich von dem Namen unterscheiden, den der Befehl hostname auf Ihrer Workstation zurückgibt.
- Der Client fordert Sie zur Eingabe des Kennworts auf, das dem angegebenen Knoten zugeordnet ist, falls ein Kennwort erforderlich ist (auch wenn die Option passwordaccess auf generate gesetzt ist). Wenn Sie das korrekte Kennwort eingeben, haben Sie Zugriff auf alle Sicherungen und Archivierungen, die von dem angegebenen Knoten ausgingen.

Wenn eine Verbindung zu einem Server hergestellt wird, muss sich der Client beim Server identifizieren. Diese Anmeldeidentifikation wird wie folgt bestimmt:

- Sind die Optionen nodename und virtualnodename nicht angegeben und wird kein virtueller Knotenname in der Befehlszeile angegeben, gibt der Befehl hostname den Namen der Standardanmelde-ID zurück.
- Ist die Option nodename angegeben, überschreibt der mit der Option nodename angegebene Name den Namen, der vom Befehl hostname zurückgegeben wird.
- Ist die Option virtualnodename angegeben oder wird ein virtueller Knotenname in der Befehlszeile angegeben, darf dieser Name nicht dem Namen entsprechen, den der Befehl hostname zurückgibt.

Windows-BetriebssystemeAnmerkung: Der Client kann beim Zurückschreiben von Dateien Dateibereichsinformationen verwenden. Die Dateibereichsinformationen können den Namen des Computers enthalten, von dem die Dateien gesichert wurden. Wenn Sie Dateien von einem anderen Clientknoten zurückschreiben und kein Ziel für die zurückgeschriebenen Dateien angeben, verwendet der Client die Dateibereichsinformationen zum Zurückschreiben der Dateien. In einem derartigen Fall versucht der Client, die Dateien in das Dateisystem auf dem ursprünglichen Computer zurückzuschreiben. Hat der zurückschreibende Computer Zugriff auf das Dateisystem des ursprünglichen Computers, können Dateien in das ursprüngliche Dateisystem zurückgeschrieben werden. Hat der zurückschreibende Computer keinen Zugriff auf das Dateisystem des ursprünglichen Computers, kann der Client eine Netzfehlernachricht zurückgeben. Wenn die ursprüngliche Verzeichnisstruktur zurückgeschrieben werden soll, dies jedoch auf einen anderen Computer erfolgen soll, geben Sie bei der Zurückschreibung nur das Zieldateisystem an. Dies gilt sowohl für das Zurückschreiben von Dateien von einem anderen Knoten als auch für das Abrufen von Dateien von einem anderen Knoten.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Diese Option ist für alle Clients gültig.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeFügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

```
>>-VIRTUALNodename-- --Knotenname------------------------------><
```

Parameter

Knotenname
: Gibt einen aus 1 bis 64 Zeichen bestehenden Namen an, der den Knoten identifiziert, für den IBM Spectrum Protect-Services angefordert werden sollen. Es gibt keinen Standardwert.

Beispiele

Optionsdatei:
```
virtualnodename cougar
```
Befehlszeile:
```
-virtualn=banshee
```

Diese Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

Windows-Betriebssysteme

Vmautostartvm

Mit der Option vmautostartvm in Verbindung mit dem Befehl restore VM vmrestoretype=instantaccess können Sie angeben, ob die virtuelle Maschine, die während der Sofortzugriffsverarbeitung erstellt wird, automatisch eingeschaltet wird.

Diese Option ist nur für virtuelle VMware-Maschinen gültig. Die virtuellen Maschinen müssen auf Servern mit VMware ESXi 5.1 oder höher gehostet werden. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Unterstützte Clients

 Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein. Diese Option ist nur bei Verwendung für eine Operation mit der Angabe `vmrestoretype=instantaccess` gültig.

Syntax

```
                  .-NO--.
>>-VMAUTOSTARTvm--+-----+---------------------------------------><
                  '-YES-'
```

Parameter

NO
: Die für den Sofortzugriff erstellte virtuelle Maschine wird nicht automatisch gestartet. Die virtuelle Maschine muss manuell gestartet werden. Dies ist die Standardeinstellung. Bei der Standardeinstellung besteht die Möglichkeit, die virtuelle Maschine neu zu konfigurieren, bevor Sie sie einschalten, um mögliche Konflikte mit vorhandenen virtuellen Maschine zu vermeiden.

YES
: Die für den Sofortzugriff erstellte virtuelle Maschine wird automatisch gestartet.

Beispiele

Optionsdatei:

```
VMAUTOSTARTvm NO
```

Befehlszeile:

```
dsmc restore vm Oslo -VMRESToretype=INSTANTAccess -vmname=Oslo_verify
-VMAUTOSTARTvm=YES
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmbackdir

Die Option vmbackdir gibt die temporäre Plattenposition an, an der der Client Steuerdateien speichert, die während VM-Gesamtsicherungs- und -Zurückschreibungsoperationen für virtuelle Maschinen erstellt werden.

Unterstützte Einheiten zum Versetzen von Daten

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Wenn ein Client auf einem Knoten der Einheit zum Versetzen von Daten eine VM-Gesamtsicherung einer virtuellen Maschine startet, erstellt der Client Metadaten in Dateien, die der gesicherten virtuellen Maschine und ihren Daten zugeordnet werden. Die Dateien, die die Metadaten enthalten, werden als *Steuerdateien* bezeichnet.

Bei VM-Gesamtsicherungsoperationen werden Metadaten auf einer Platte des Knotens der Einheit zum Versetzen von Daten gespeichert, bis die Sicherung beendet ist und sowohl die Daten der virtuellen Maschine als auch die Steuerdateien im Serverspeicher gespeichert werden. Bei einer vollständigen VM-Zurückschreibungsoperation werden die Steuerdateien vom Server kopiert und temporär auf der Platte der Einheit zum Versetzen von Daten gespeichert. Dort werden sie zur Zurückschreibung der virtuellen Maschine und ihrer Daten verwendet. Nach der Beendigung einer Sicherungs- oder Zurückschreibungsoperation werden die Steuerdateien nicht mehr benötigt und der Client löscht sie aus der temporären Plattenposition.

Das durch diese Option angegebene Verzeichnis muss sich auf einem Laufwerk befinden, das so viel freien Speicherbereich enthält, dass die Steuerinformationen aus einer vollständigen VM-Sicherung gespeichert werden können.

 Linux-Betriebssysteme  Windows-BetriebssystemeDiese Option ist für Linux- und Windows-Einheiten zum Versetzen von Daten gültig, die auf einem vStorage-Sicherungsserver installiert sind.

 Windows-BetriebssystemeDiese Option ist für Windows-Einheiten zum Versetzen von Daten gültig, die auf einem Hyper-V-Server installiert sind.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei oder geben Sie sie in die Befehlszeile als Option für den Befehl backup vm oder restore vm ein.

Syntax

```
>>-VMBACKDir--Verzeichnis----------------------------------------><
```

Parameter

Verzeichnis
Gibt den Pfad an, in dem die Steuerdateien auf dem Sicherungsserver gespeichert werden.
 Windows-BetriebssystemeDer Standardwert ist c:\mnt\tsmvmbackup\fullvm\.
 Linux-BetriebssystemeDer Standardwert ist /tmp/tsmvmbackup/fullvm/

Beispiele

Optionsdatei:
 Windows-Betriebssysteme`VMBACKD c:\mnt\tsmvmbackup\`
Linux-Betriebssysteme`VMBACKD /tmp/tmsvmbackup/`
Befehlszeile:
 Windows-Betriebssysteme`dsmc backup vm -VMBACKUPT=fullvm -VMBACKD=G:\virtual_machine\control_files\`
 Windows-Betriebssysteme`dsmc restore vm -VMBACKUPT=fullvm -VMBACKD=G:\san_temp\`
Linux-Betriebssysteme`dsmc backup vm -VMBACKUPT=fullvm -VMBACKD=/home/vmware/control_files`
 Linux-Betriebssysteme`dsmc restore vm -VMBACKUPT=fullvm -VMBACKD=/home/mine/bkup_ctrl`

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmbackuplocation

Verwenden Sie die Option vmbackuplocation mit dem Befehl backup vm oder restore vm, um die Sicherungsposition für Sicherungs- und Zurückschreibungsoperationen für virtuelle Maschinen anzugeben.

Diese Option ist nur für virtuelle VMware-Maschinen gültig. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Für Zurückschreibungsoperationen wird diese Option ignoriert, wenn die Option vmrestoretype auf mountcleanup oder mountcleanupall gesetzt ist.

Unterstützte Clients

 LinuxBetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

 WindowsBetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Diese Option muss in der Befehlszeile eines Befehls backup vm oder restore vm angegeben werden. Sie können diese Option nicht in der Clientoptionsdatei angeben.

Syntax

```
                          .-SERVER-.
>>- -VMBACKUPLOCation-- --+-LOCAL--+--------------------------><
                          '-BOTH---'
```

Parameter

SERVER
Gibt für Sicherungsoperationen an, dass virtuelle Maschinen auf dem IBM Spectrum Protect-Server gesichert werden.
Gibt für Zurückschreibungsoperationen an, dass virtuelle Maschinen vom IBM Spectrum Protect-Server zurückgeschrieben werden.
Dies ist der Standardwert.
LOCAL

Gibt für Sicherungsoperationen an, dass virtuelle Maschinen im Hardwarespeicher gesichert werden. Bei der Sicherung handelt es sich selbst dann um eine vollständige Imagemomentaufnahmen virtueller Maschinen, wenn eine Teilsicherung angegeben ist.
Um eine lokale Sicherung erstellen zu können, muss die virtuelle Maschine in einem VMware-Datenspeicher für virtuelle Datenträger (VVOL) gespeichert sein. Wenn sich eine virtuelle Platte der virtuellen Maschine nicht in einem VVOL-Datenspeicher befindet, ist die lokale Sicherung nicht zulässig.
Gibt für Zurückschreibungsoperationen an, dass virtuelle Maschinen aus Momentaufnahmen zurückgeschrieben werden, die im Hardwarespeicher gespeichert sind.
Bei der Zurückschreibung aus einer lokalen Momentaufnahme kann nur eine vorhandene virtuelle Maschine zurückgesetzt werden. Es ist nicht möglich, eine gelöschte virtuelle Maschine zurückzuschreiben oder eine virtuelle Maschine mit einem anderen Namen oder an eine andere Position zurückzuschreiben.
Eine lokale Zurückschreibung ist nicht gültig, wenn die folgenden Parameter im Befehl restore vm verwendet werden:

- VMNAME
- DATACENTER
- HOST
- DATASTORE
- :vmdk

Dieser Wert ist ebenfalls nicht gültig, wenn die Option vmrestoretype auf einen der folgenden Werte gesetzt ist. Wenn diese Werte definiert sind, wird eine Fehlernachricht angezeigt.

- instantaccess
- instantrestore
- mount

Da für lokale Momentaufnahmen keine Netzdatenversetzung erforderlich ist, können Sicherungs- und -zurückschreibungsoperationen schneller als Serversicherungs- und Zurückschreibungsoperationen ausgeführt werden.

BOTH
Gibt für Sicherungsoperationen an, dass virtuelle Maschinen sowohl auf dem IBM Spectrum Protect-Server als auch lokal gesichert werden. Bei der lokalen Sicherung handelt es sich immer um eine vollständige Imagemomentaufnahme der VMs, selbst wenn Teilsicherungen für den Server konfiguriert sind.
Gibt für Zurückschreibungsoperationen an, dass virtuelle Maschinen aus der neuesten aktiven Version zurückgeschrieben werden; dies ist unabhängig davon, ob es sich um eine lokale Sicherung oder eine Sicherung auf dem Server handelt. Wenn die Zeitmarke für beide aktive Sicherungen identisch ist, wird die lokale Sicherung für die Zurückschreibung verwendet.
Dieser Wert ist mit den oben für den Wert LOCAL aufgelisteten Parametern und Werten für die Option vmrestoretype nicht gültig.

Beispiele

Befehlszeile:
Servergesamtsicherung und lokale Sicherung für die virtuelle Maschine vm1 ausführen:

```
dsmc backup vm vm1 -vmbackuplocation=BOTH -vmbackuptype=FUllvm
```

Lokale Zurückschreibung für die virtuelle Maschine vm1 ausführen:

```
dsmc restore vm vm1 -vmbackuplocation=LOCAL
```

Vmbackupmailboxhistory

Die Option vmbackupmailboxhistory gibt an, ob die Mailbox-History automatisch mit der VM-Sicherung hochgeladen wird, wenn IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server auf einer virtuellen Maschine erkannt wird.

Unterstützte Clients

Linux-BetriebssystemeWindows-BetriebssystemeDiese Option ist auf Clients gültig, die als Einheit zum Versetzen von Daten für VMware-Gastmaschinensicherungen agieren.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
.-Yes-.
```

```
>>-VMBACKUPMAILBoxhistory--+-----+----------------------------><
                           '-No--'
```

Parameter

Yes
: Die Mailbox-History wird automatisch mit der VM-Sicherung hochgeladen, wenn IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server auf einer virtuellen Maschine erkannt wird.

No
: Die Mailbox-History wird nicht automatisch mit der VM-Sicherung hochgeladen.

Beispiele

Optionsdatei:
: vmbackupmailboxhistory yes

Linux-BetriebssystemeWindows-Betriebssysteme

Vmbackuptype

Verwenden Sie die Option vmbackuptype mit dem Befehl backup VM oder restore VM, um den Typ der Sicherung oder Zurückschreibung der virtuellen Maschine anzugeben, der ausgeführt werden soll. Sie können diese Option auch in query VM-Befehlen verwenden, um die Abfrageergebnisse zu filtern, sodass nur virtuelle Maschinen angezeigt werden, die mit einem bestimmten Sicherungstyp gesichert wurden. Beispiele finden Sie in der Beschreibung des Befehls query VM.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

 Linux-Betriebssysteme

Sie können eine vollständige VM-Sicherung für VMware angeben.

 Windows-Betriebssysteme

Sie können eine VM-Gesamtsicherung für VMware oder eine VM-Gesamtsicherung für Hyper-V angeben.

Unterstützte Clients

 LinuxBetriebssystemeDiese Option ist für Linux-Einheiten zum Versetzen von Daten gültig, die auf einem vStorage-Sicherungsserver installiert sind. Diese Option kann auch auf dem Server definiert werden.

 WindowsBetriebssystemeDiese Option ist für Windows-Einheiten zum Versetzen von Daten gültig, die auf einem vStorage-Sicherungsserver installiert sind. Diese Option kann auch auf dem Server definiert werden.

 WindowsBetriebssystemeDiese Option ist für Windows-Einheiten zum Versetzen von Daten gültig, die auf einem Microsoft-Hyper-V-System installiert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

 LinuxBetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

 WindowsBetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

 Linux-Betriebssysteme

Syntax

```
                .-FUllvm-.
>>-VMBACKUPType--+--------+-------------------------------------><
```

 Linux-Betriebssysteme

Parameter

FUllvm
: Geben Sie diesen Wert an, um eine traditionelle VM-Gesamtsicherung einer virtuellen VMware-Maschine auszuführen. Dies ist der Standardsicherungstyp für Linux-Clients.

Windows-Betriebssysteme

Syntax

```
                .-FUllvm-----.
>>-VMBACKUPType--+-HYPERVFULL-+-------------------------------><
```

Windows-Betriebssysteme

Parameter

FUllvm
: Geben Sie diesen Wert an, um eine traditionelle VM-Gesamtsicherung einer virtuellen VMware-Maschine auszuführen. Dies ist der Standardsicherungstyp für Windows-Clients, die auf Windows-Serversystemen ausgeführt werden, auf denen die Hyper-V-Serverrolle nicht aktiviert ist. Gegensatz zu `vmbackuptype=hypervfull`.

HYPERVFULL
: Gibt an, dass Sie mindestens eine virtuelle Hyper-V-Maschine sichern. Wenn Sie die Hyper-V-Serverrolle aktivieren, ist dieser Wert der Standardsicherungstyp. Wenn Sie die Option vmbackuptype=hypervfull angeben, werden alle Optionen für die Sicherung von VMware-Dateien auf einem vStorage-Sicherungsserver ignoriert (z. B. VMCHOST, VMCUSER, VMCPW, VMFULLNODELETE).

Beispiele

Optionsdatei:

```
VMBACKUPT full
```

Befehlszeile:

Linux-BetriebssystemeWindows-Betriebssysteme`dsmc backup vm vm1 -VMBACKUPT=full -vmchost=virtctr -vmcuser=virctr_admin -vmcpw=xxxxx`

Führt eine vollständige VM-Sicherung der virtuellen Maschine `vm1.example.com`, die die VMware VirtualCenter-Maschine `virtctr.example.com` verwendet, auf dem IBM Spectrum Protect-Server unter Verwendung des Maschinennamens `vm1` aus.

Windows-Betriebssysteme`dsmc backup vm -VMBACKUPT=hypervfull -vmlist="VM 1,VM 2"`

Führt eine vollständige VM-Sicherung der virtuellen Hyper-V-Maschinen mit den Namen "VM 1" und "VM 2" auf dem IBM Spectrum Protect-Server aus.

Linux-BetriebssystemeWindows-Betriebssysteme

Vmchost

Verwenden Sie die Option vmchost im Befehl backup VM, restore VM oder query VM, um den Hostnamen des VMware VirtualCenter- oder ESX-Servers anzugeben, der gesichert, zurückgeschrieben oder abgefragt werden soll.

Verwenden Sie das VirtualCenter, falls es verfügbar ist. Wenn Sie keinen VirtualCenter-Server verwenden können und Sicherungen mehrerer Systeme auf mehreren ESX-Servern ausführen müssen, geben Sie diese Option nicht an, sondern geben Sie stattdessen die Option mit dem Befehl an, damit sie für jeden ESX-Server variiert werden kann.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Dieser Befehl ist für Clients gültig, die zur Ausführung einer Off-Host-Sicherung einer virtuellen VMware-Maschine konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

WindowsBetriebssystemeDiese Option wird für Hyper-V-Sicherungen nicht unterstützt.

Optionsdatei

WindowsBetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

LinuxBetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt), in die Clientsystemoptionsdatei (dsm.sys) oder in die Befehlszeile ein.

Syntax

```
>>-VMCHost-- --Hostname-----------------------------------------><
```

Parameter

Hostname
Gibt den Hostnamen des VMware VirtualCenter- oder ESX-Servers an, der gesichert, zurückgeschrieben oder abgefragt werden soll.

Beispiele

Optionsdatei:
```
VMCH vcenter.storage.usca.example.com
```
Befehlszeile:

```
-VMCH=esx1.storage.usca.example.com
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmcpw

Verwenden Sie die Option vmcpw im Befehl backup VM, restore VM oder query VM, um das Kennwort für die VMware VirtualCenter- oder ESX-Benutzer-ID anzugeben, die mit der Option vmcuser angegeben wird.

Verwenden Sie das VirtualCenter, falls es verfügbar ist. Wenn Sie keinen VirtualCenter-Server verwenden können und Sicherungen mehrerer Systeme auf mehreren ESX-Servern ausführen müssen, geben Sie diese Option nicht an, sondern geben Sie stattdessen die Option mit dem Befehl an, damit sie für jeden ESX-Server variiert werden kann.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

 LinuxBetriebssystemeDiese Option ist nur auf unterstützten Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind, der zum Sichern einer virtuellen VMware-Maschine verwendet wird.

 WindowsBetriebssystemeDiese Option ist nur auf unterstützten Windows-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind, der zum Sichern einer virtuellen VMware-Maschine verwendet wird. Diese Option ist nicht für Hyper-V-Sicherungen gültig.

Optionsdatei

 WindowsBetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

 LinuxBetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) oder in die Befehlszeile ein.

1. Klicken Sie auf Editieren > Clientvorgaben > VM-Sicherung. Geben Sie in das Feld Kennwort das Kennwort ein, das gespeichert werden soll.
2. Klicken Sie auf OK.

Als Alternative zum Profileditor können Sie das Kennwort mit dem Befehl set password auch lokal speichern. Zum Beispiel:

```
dsmc SET PASSWORD -type=vm
vcenter.us.ibm.com Administrator secret
```

Syntax

```
>>-VMCPw-- --Kennwortname-------------------------------------><
```

Parameter

Kennwortname
Gibt das Kennwort für den VMware VirtualCenter- oder ESX-Server an, der gesichert, zurückgeschrieben oder abgefragt werden soll.

Beispiele

Optionsdatei:
```
VMCPw SECRET
```
Befehlszeile:
```
-VMCPw=SECRET
```

Zugehörige Verweise:
Set Password
 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmctlmc

Diese Option gibt die Verwaltungsklasse an, die beim Sichern von Steuerdateien für virtuelle Maschinen verwendet werden soll.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Standardmäßig sind die Steuerdateien für virtuelle Maschinen an die Standardverwaltungsklasse gebunden. Mit der Option vmmc kann eine andere Verwaltungsklasse angegeben werden, an die die Daten und Steuerdateien für virtuelle Maschinen gebunden werden. Die Option vmctlmc überschreibt die Standardverwaltungsklasse und die Option vmmc für die Steuerdateien virtueller Maschinen.

Unter bestimmten Bedingungen könnte es wünschenswert oder erforderlich sein, die Steuerdateien an eine andere Verwaltungsklasse als die Datendateien zu binden.

Die Option vmctlmc ist erforderlich, wenn Datendateien virtueller Maschinen auf Band gesichert werden. Steuerdateien für virtuelle Maschinen müssen in einem plattenbasierten Speicherpool gesichert werden, der nicht auf Band umgelagert wird. Der Speicherpool kann aus Datenträgern mit wahlfreiem Zugriff und sequenziellen FILE-Datenträgern bestehen. Der Speicherpool kann außerdem ein dedupliziertes Pool sein. Geben Sie mit der Option vmctlmc eine Verwaltungsklasse an, durch die Daten in einem solchen Speicherpool gespeichert werden.

Einschränkung: Die durch die Option vmctlmc angegebene Verwaltungsklasse gibt nur den Zielspeicherpool für die Steuerdateien virtueller Maschinen an. Die Aufbewahrung der Steuerdateien wird durch die Option vmmc festgelegt, falls angegeben, oder durch die Standardverwaltungsklasse. Die Aufbewahrungsdauer der Steuerdateien von virtuellen Maschinen stimmt immer mit der Aufbewahrungsdauer der Datendateien von virtuellen Maschinen überein.

Unterstützte Clients

Linux-BetriebssystemeWindows-BetriebssystemeDiese Option ist für Clients gültig, die als Knoten der Einheit zum Versetzen von Daten agieren und virtuelle VMware-Maschinen schützen.

Windows-BetriebssystemeDiese Option ist für Clients gültig, die als Knoten der Einheit zum Versetzen von Daten agieren und virtuelle Microsoft Hyper-V-Maschinen schützen.

Die Option kann nur für Sicherungen virtueller Maschinen mit einem immer inkrementellen Sicherungsmodus verwendet werden.

Diese Option ist nur verfügbar, wenn Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware oder IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V besitzen.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Systemoptionsdatei (dsm.sys) ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-VMCTLmc--Klassenname----------------------------------------><
```

Parameter

Klassenname
: Gibt eine Verwaltungsklasse an, die für die Sicherung der Steuerdateien für virtuelle Maschinen gilt. Wird diese Option nicht definiert, wird die in der Option vmmc angegebene Verwaltungsklasse verwendet. Wird diese Option nicht definiert und ist die Option vmmc nicht definiert, wird die Standardverwaltungsklasse des Knotens verwendet.

Beispiele

Optionsdatei:

```
vmctlmc diskonlymc
```

Befehlszeile:
: Nicht zutreffend.

Linux-BetriebssystemeWindows-Betriebssysteme

Vmcuser

Verwenden Sie die Option vmcuser im Befehl backup VM, restore VM oder query VM, um den Benutzernamen des VMware VirtualCenter- oder ESX-Servers anzugeben, der gesichert, zurückgeschrieben oder abgefragt werden soll.

Verwenden Sie das VirtualCenter, falls es verfügbar ist. Wenn Sie keinen VirtualCenter-Server verwenden können und Sicherungen mehrerer Systeme auf mehreren ESX-Servern ausführen müssen, geben Sie diese Option nicht an, sondern geben Sie stattdessen die Option mit dem Befehl an, damit sie für jeden ESX-Server variiert werden kann.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Diese Option ist für Clients gültig, die zur Ausführung einer Off-Host-Sicherung virtueller VMware-Maschinen konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist nicht für Hyper-V-Sicherungen gültig.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt), in die Clientsystemoptionsdatei (dsm.sys) oder in die Befehlszeile ein.

Syntax

```
>>-VMCUser-- --Benutzername-------------------------------------><
```

Parameter

Benutzername
: Gibt den Benutzernamen des VMware VirtualCenter- oder ESX-Servers an, der gesichert, zurückgeschrieben oder abgefragt werden soll.

  Wird mit einem Virtual Center gearbeitet, ist eine Benutzer-ID mit Zugriff auf das Windows-System, auf dem sich das Virtual Center befindet, erforderlich. Diese Benutzer-ID muss entweder über Administratorberechtigungen oder über die Mindestberechtigungen verfügen, die in der Technote 1659544 angegeben sind.

Beispiele

Optionsdatei:

```
VMCUser administrator
```

Befehlszeile:

```
backup vm -VMCUser=domainname\administrator
```

Befehlszeile:

Beispiel für die Herstellung einer Verbindung zu einem ESX-Server:

```
backup vm -VMCUser=root
```

Linux-BetriebssystemeWindows-Betriebssysteme

Vmdatastorethreshold

Verwenden Sie die Option vmdatastorethreshold, um den Prozentsatz für den Schwellenwert der Speicherbelegung für jeden VMware-Datenspeicher einer virtuellen Maschine zu definieren.

Wenn Sie diese Option angeben, wird die Speicherbelegung überprüft, bevor eine VM-Momentaufnahme erstellt wird. Ist der Schwellenwert überschritten, wird die virtuelle Maschine nicht gesichert. Wenn diese Option festgelegt wird, können Fehler aufgrund fehlenden Speicherbereichs bei der Sicherung virtueller Maschinen verhindert werden.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Linux-BetriebssystemeSie können diese Option für unterstützte Linux x86_64-Clients verwenden.

Windows-BetriebssystemeSie können diese Option für unterstützte Windows 64-Bit-Clients verwenden.

Optionsdatei

Linux-BetriebssystemeSie können diese Option in der Clientsystemoptionsdatei (dsm.sys) oder mit dem Befehl backup vm in der Befehlszeile angeben. Sie können diese Option auf einem IBM Spectrum Protect-Server mit Version 7.1.5 oder höher auch in einer Clientoptionsgruppe angeben. Sie können diese Option nicht im Profileditor definieren.

Windows-BetriebssystemeSie können diese Option in der Clientoptionsdatei (dsm.opt) oder mit dem Befehl backup vm in der Befehlszeile angeben. Sie können diese Option auf einem IBM Spectrum Protect-Server mit Version 7.1.5 oder höher auch in einer Clientoptionsgruppe angeben. Sie können diese Option nicht im Profileditor definieren.

Syntax

```
>>-VMDATASTORETHreshold----Prozent-----------------------------><
```

Parameter

Prozent
Gibt den Schwellenwertprozentsatz für jeden VMware-Datenspeicher der virtuellen Maschine an, die gesichert werden soll. Sie können eine ganze Zahl von 0 bis 100 angeben. Der Standardwert ist 100. Wenn Sie diese Option nicht definieren, startet der Client eine Sicherung der virtuellen Maschine, ohne zuvor die vorhandene Speicherbelegung zu überprüfen.
Voraussetzungen:

- Stellen Sie sicher, dass der Schwellenwert nicht zu hoch ist, damit die Momentaufnahme nicht den gesamten verfügbaren Speicherbereich in den VMware-Datenspeichern belegt. Andernfalls ist in den VMware-Datenspeichern kein Speicherbereich mehr verfügbar und die Momentaufnahme wird nicht erstellt.
- Wenn Sie mehrere Clients verwenden, die als Einheiten zum Versetzen von Daten agieren, müssen Sie diese Option der Optionsdatei für jede Einheit zum Versetzen von Daten hinzufügen.
- Der Client überprüft die Datennutzung des VMware-Datenspeichers, der die VM-Plattenmomentaufnahmen enthält. Standardmäßig werden die Momentaufnahmen in dem Verzeichnis erstellt, in dem sich auch die übergeordnete Datei der virtuellen Platte (.vmdk) befindet.

  Wenn Sie die Momentaufnahmeposition in ein neues Verzeichnis in demselben Datenspeicher oder in einem anderen Datenspeicher mit der Option workingDir in der VM-Konfigurationsdatei ändern, müssen Sie sicherstellen, dass der Pfad des Arbeitsverzeichnisses korrekt ist. Ist der Pfad nicht korrekt, kann der Client möglicherweise die Datennutzung des falschen Datenspeichers überprüfen.

Wenn Sie die Option EXCLUDE.VMDISK verwenden, um eine oder mehrere Platten von einer Sicherung auszuschließen, wird dennoch die Schwellenwertüberprüfung auf diesen Platten ausgeführt. Diese Platten werden zwar nicht gesichert; jedoch erstellt VMware dennoch eine Momentaufnahme dieser Platten.

Unabhängige Platten werden während der Verarbeitung der Speicherbereichsüberprüfung nicht überprüft, da eine Momentaufnahme dieser Platten keinen Speicherbereich in einem VMware-Datenspeicher belegt.

Beispiel 1

Die virtuelle Maschine `vm1` erstreckt sich über `datastore1` und `datastore2`. Setzen Sie die Option vmdatastorethreshold auf 90, um sicherzustellen, dass beide VMware-Datenspeicher maximal zu 90 % belegt sind, wenn die virtuelle Maschine gesichert wird.

Optionsdatei:
```
vmdatastorethreshold 90
```
Befehlszeile:
```
dsmc backup vm vm1 -vmdatastorethreshold=90
```

Beispiel 2

Der Schwellenwert des Datenspeichers `datastore2` wird auf 85 gesetzt. Der Schwellenwert des Datenspeichers wird während der Sicherung der virtuellen Maschine `vm5` überschritten. Die folgende Fehlernachricht wird angezeigt:

```
ANS14200E Die virtuelle Maschine 'vm5' konnte nicht gesichert werden, da die
Datennutzung des Datenspeichers 'datastore2' den Schwellenwert von
85 Prozent für den Datenspeicher überschritten hat.
```

Erhöhen Sie den Wert der Option vmdatastorethreshold auf 95 und starten Sie die Sicherung erneut.

Optionsdatei:
```
vmdatastorethreshold 95
```
Befehlszeile:
```
dsmc backup vm vm5 -vmdatastorethreshold=95
```

Zugehörige Verweise:
Backup VM

Linux-BetriebssystemeWindows-Betriebssysteme

Vmdefaultdvportgroup

Mit dieser Option können Sie die Portgruppe angeben, die NICs (Netzschnittstellenkarten) während restore vm-Operationen für eine virtuelle Maschine verwenden sollen, die bei ihrer Sicherung mit einer verteilten virtuellen Portgruppe verbunden war, ohne dass der Zielhost der Zurückschreibungsoperation eine ähnliche verteilte virtuelle Portgruppe enthält.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist nicht für Sicherungs- oder Zurückschreibungsoperationen für virtuelle Microsoft-Hyper-V-Maschinen gültig.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Windows-BetriebssystemeDiese Option ist für Windows-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Clientsystemoptionsdatei (dsm.sys) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Syntax

```
>>-VMDEFAULTDVPORTGROUP--Portgruppenname----------------------><
```

Parameter

Portgruppenname
Gibt den Namen der Portgruppe an, der verwendet werden soll. Beim Portgruppennamen muss die Groß-/Kleinschreibung beachtet werden.

Beispiele

Optionsdatei:

```
VMDEFAULTDVPORTGROUP dvPortGroup
```

Befehlszeile:

```
dsmc restore vm vm123 -VMDEFAULTDVPORTGROUP=dvPortGroup
```

Zugehörige Verweise:
Vmdefaultnetwork
Vmdefaultdvswitch
Linux-BetriebssystemeWindows-Betriebssysteme

Vmdefaultdvswitch

Mit dieser Option können Sie den verteilten virtuellen Switch (dvSwitch) angeben, der die Portgruppe enthält, die Sie mit der Option vmdefaultdvportgroup definieren. Die Option bleibt ohne Wirkung, wenn nicht auch die Option vmdefaultdvportgroup angegeben wird.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist nicht für Sicherungs- oder Zurückschreibungsoperationen für virtuelle Microsoft-Hyper-V-Maschinen gültig.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Windows-BetriebssystemeDiese Option ist für Windows-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Clientsystemoptionsdatei (dsm.sys) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Syntax

```
>>-VMDEFAULTDVSWITCH--dvSwitch---------------------------------><
```

Parameter

dvSwitch
Gibt den Namen des virtuellen Switch an, der verwendet werden soll. Beim Namen des virtuellen Switch muss die Groß-/Kleinschreibung beachtet werden.

Beispiele

Optionsdatei:

```
VMDEFAULTDVSWITCH dvSwitch
```

Befehlszeile:

```
dsmc restore vm vm123 -VMDEFAULTDVSWITCH=dvSwitch -VMDEFAULTDVPORTGROUP=dvPortGroup
```

Zugehörige Verweise:
Vmdefaultdvportgroup
Linux-BetriebssystemeWindows-Betriebssysteme

Vmdefaultnetwork

Mit dieser Option können Sie ein Netz angeben, das NICs (Netzschnittstellenkarten) während einer restore vm-Operation für eine virtuelle Maschine verwenden sollen, die bei ihrer Sicherung mit einer verteilten virtuellen Portgruppe verbunden war, ohne dass für den Zielhost der Zurückschreibungsoperation verteilte Switch-Portgruppen konfiguriert sind.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist nicht für Zurückschreibungsoperationen für virtuelle Microsoft-Hyper-V-Maschinen gültig.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Windows-BetriebssystemeDiese Option ist für Windows-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Clientsystemoptionsdatei (dsm.sys) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Syntax

```
>>-VMDEFAULTNETWORK--VM-Netzname------------------------------><
```

Parameter

VM-Netzname
Gibt den Namen des Netzes der virtuellen Maschine an, der verwendet werden soll. Beim Netznamen muss die Groß-/Kleinschreibung beachtet werden. Wenn der Name Leerzeichen enthält, muss er in Anführungszeichen eingeschlossen werden.

Beispiele

Optionsdatei:

```
VMDEFAULTNETWORK "VM Network"
```

Befehlszeile:

```
dsmc restore vm vm123 -VMDEFAULTNETWORK="VM Network"
```

Zugehörige Verweise:
Vmdefaultdvportgroup
Vmdefaultdvswitch
 Windows-Betriebssysteme

Vmdiskprovision

Mit der Option vmdiskprovision können Sie eine Bereitstellungsmaßnahme für die virtuelle Plattendatei angeben, die für die Zurückschreibung von Daten virtueller VMware-Maschinen verwendet wird. Diese Option ist nur für restore vm-Operationen mit der Angabe `vmrestoretype=instantrestore` gültig.

Diese Option ist nur für virtuelle VMware-Maschinen gültig. Die virtuellen Maschinen müssen auf Servern mit VMware ESXi 5.1 oder höher gehostet werden. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Unterstützte Clients

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

Syntax

```
                    .-THICK-.
>>-VMDISKPROvision--+-------+---------------------------------><
                    '-THIN--'
```

Parameter

THICK
: Erstellt eine virtuelle Platte in einem Standardformat 'thick'. Hierbei wird der für die virtuelle Platte erforderliche Speicherplatz bei der Erstellung der virtuellen Platte zugeordnet. Dies ist die Standardeinstellung.

THIN
: Erstellt eine virtuelle Platte in einem Format 'thin'.
Anmerkung: Wenn Sie beim Zurückschreiben einer virtuellen Maschine Thin Provisioning angeben, muss der Datenspeicher, in den Sie die VM zurückschreiben, über genügend freien Speicherbereich für die Gesamtkapazität der VM-Platte verfügen und nicht nur für die verwendete Kapazität. Beispiel: Wenn die gesamte Plattenkapazität einer mit Thin Provisioning bereitgestellten VM 300 GB beträgt, können Sie diese VM nicht in einen Datenspeicher mit einer Kapazität kleiner als 300 GB zurückschreiben, selbst wenn nur ein Teil der Gesamtkapazität verwendet wird.

Beispiele

Optionsdatei:

```
VMDISKPROvision THIN
```

Befehlszeile:

```
dsmc restore vm Mainz -VMRESToretype=INSTANTRestore
 -VMTEMPDAtastore=Temporary_Datastore -VMDISKPROvision=THIN
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmenabletemplatebackups

Die Option vmenabletemplatebackups gibt an, ob der Client virtuelle VMware-Schablonenmaschinen sichert, wenn er virtuelle Maschinen auf einem vCenter-Server schützt. Virtuelle VMware-Schablonenmaschinen können nicht gesichert werden, wenn sie sich auf einem ESXi-Host befinden, weil ESXi Schablonen nicht unterstützt.

Wenn diese Option aktiviert ist, können Sie VMware-Schablonenmaschinen in vollständige VM-Sicherungsoperationen einschließen. Sie verwenden den vorhandenen Befehl Backup VM und die Option DOMAIN.VMFULL, um die virtuellen Maschinen anzugeben, die bei der Sicherungsoperation berücksichtigt werden sollen.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Teilsicherungen werden nicht unterstützt und Momentaufnahmen nicht erstellt; daher müssen Sie MODE=IFFULL verwenden. Mit MODE=IFFULL können Sie selbst dann eine neue Sicherung virtueller VMware-Schablonenmaschinen erzwingen, wenn diese sich seit der letzten Sicherung nicht geändert haben.

Wenn vmenabletemplatebackups aktiviert ist, wird jeder Sicherungsprozess, der mit MODE=IFINCREMENTAL eingeleitet wird, unter Verwendung von MODE=IFFULL verarbeitet. Virtuelle VMware-Schablonenmaschinen werden bei einer Sicherung nur berücksichtigt, wenn sie seit der letzten Sicherung geändert wurden.

Wenn diese Option aktiviert ist, müssen Sie sicherstellen, dass vmvstortransport-Optionen den Wert NBDSSL oder NBD enthalten. Wird nur der Transportmodus SAN oder HOTADD in Verbindung mit dieser aktivierten Option verwendet, schlagen Sicherungen der Schablonenmaschinen fehl.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Linux-BetriebssystemeSie können diese Option in der Befehlszeile, in der Clientsystemoptionsdatei (dsm.sys), in der Clientoptionsdatei (dsm.opt) oder auf dem Server in einer Clientoptionsgruppe definieren.

Windows-BetriebssystemeSie können diese Option in der Befehlszeile, in der Clientoptionsdatei (dsm.opt) oder auf dem Server in einer Clientoptionsgruppe definieren.

Linux-BetriebssystemeWindows-BetriebssystemeSie können die Option auch im Profileditor auf der Registerkarte 'VM-Sicherung' definieren (wählen Sie die Option für die Sicherung von Schablonen virtueller Maschinen aus).

Syntax

```
                              .-No------.
>>-VMENABLETEMPlatebackups--+-+-----+-+------------------------><
                              '-Yes-'
```

Parameter

No
Gibt an, dass virtuelle Schablonenmaschinen in vollständigen VM-Sicherungsoperationen nicht eingeschlossen werden. Dies ist die Standardeinstellung.

Yes
Gibt an, dass virtuelle Schablonenmaschinen in vollständigen VM-Sicherungsoperationen eingeschlossen werden.

Beispiele

Optionsdatei
vmenabletemplatebackups yes

Befehlszeile:
Eine virtuelle VMware-Schablonenmaschine sichern:

```
dsmc backup vm VM-Name -VMENABLETEMPLATEBACKUPS=YES
```

VM-Name ist der Name der Schablonenmaschine.

Befehlszeile:
Eine virtuelle VMware-Schablonenmaschine an dieselbe Position und mit demselben Namen zurückschreiben:

```
dsmc restore vm VM-Name -VMENABLETEMPLATEBACKUPS=YES
```

VM-Name ist der Name der Schablonenmaschine.

Befehlszeile:
Eine virtuelle Schablonenmaschine an eine neue Position zurückschreiben:

```
dsmc restore vm VM-Name -vmname=win7x64
  -datastore=datastore22 -host=supersht.labx.com
   -datacenter="Lab Center" -VMENABLETEMPLATEBACKUPS=YES
```

VM-Name ist der Name der Schablonenmaschine. "win7x64" ist der neue Name der virtuellen Schablonenmaschine. Das neue Datencenter, der neue Host und der neue Datenspeicher sind ebenfalls enthalten.

Zugehörige Verweise:
Backup VM
Restore VM
Domain.vmfull
 Windows-Betriebssysteme

Vmexpireprotect

Verwenden Sie diese Option, um Momentaufnahmen virtueller Maschinen zu schützen, sodass sie nicht verfallen können, während eine Sofortzurückschreibungs- oder Sofortzugriffsoperation für virtuelle VMware-Maschinen oder eine Zurückschreibung auf Dateiebene für eine virtuelle VMware-Maschine aktiv ist. Verwenden Sie diese Option, um Momentaufnahmen virtueller Maschinen zu schützen, sodass sie nicht verfallen können, während eine Sofortzurückschreibungs- oder Sofortzugriffsoperation für virtuelle Hyper-V-Maschinen oder eine Zurückschreibung auf Dateiebene für eine virtuelle Hyper-V-Maschine aktiv ist.

Bei einer Mount- oder Zurückschreibungsoperation wird die Momentaufnahme auf dem IBM Spectrum Protect-Server gesperrt, damit sie nicht während der Operation verfallen kann. Der Verfall ist möglich, weil eine weitere Momentaufnahme der Momentaufnahmefolge hinzugefügt wird. Diese Option gibt an, ob der Verfall von Momentaufnahmen während einer Mount- oder Zurückschreibungsoperation verhindert werden soll.

Unterstützte Clients

 Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden, die für die Zurückschreibung virtueller Maschinen konfiguriert sind.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Optionsdatei

Bei der Zurückschreibung virtueller VMware-Maschinen definieren Sie diese Option in der Clientoptionsdatei (dsm.opt) oder in einem restore vm-Befehl, bei dem die Option vmrestoretype auf instantaccess oder instantrestore gesetzt ist.

Bei der Zurückschreibung von Sicherungen auf Dateiebene für virtuelle Maschinen geben Sie diese Option in der Clientoptionsdatei oder im restore vm-Befehl an.

Anmerkung: Sicherungen auf Dateiebene wurden mit Clients für Sichern/Archivieren der Version 7.1 oder früher erstellt.

Syntax

```
                    .-No--.
>>-VMEXPIREPROTECT--+-Yes-+-------------------------------------><
```

Parameter

Yes
: Geben Sie Yes an, um die Momentaufnahme vor dem Verfall zu schützen. Die Momentaufnahme auf dem IBM Spectrum Protect-Server wird gesperrt und ist vor dem Verfall während einer Mount- oder Zurückschreibungsoperation geschützt.

No
: Geben Sie No an, um den Verfallsschutz zu inaktivieren. Dies ist der Standardwert. Die Momentaufnahme auf dem IBM Spectrum Protect-Server wird nicht gesperrt und ist nicht vor dem Verfall geschützt. Wenn eine Momentaufnahme während der Bereitstellung oder Zurückschreibung verfällt, ist das Ergebnis der Mount- oder Zurückschreibungsoperation unvorhersehbar. Der Mountpunkt kann beispielsweise nicht mehr verwendbar sein oder Fehler enthalten. Der Verfall wirkt sich jedoch nicht auf die zurzeit aktive Kopie der virtuellen Maschine aus. Die aktive Kopie kann während einer Operation nicht verfallen.

  Wenn die Momentaufnahme auf einem Zielreplikationsserver gespeichert ist, kann die Momentaufnahme gesperrt werden, da sie sich im Lesezugriffsmodus befindet. Ein Sperrversuch des Servers bewirkt, dass die Mount- oder Zurückschreibungsoperation fehlschlägt.

  Inaktivieren Sie den Verfallsschutz, indem Sie No angeben oder den Standardwert für diese Option verwenden, um den Sperrversuch zu verhindern und dieses Fehlschlagen zu vermeiden.

Beispiele

Clientoptionsdatei:

VMEXPIREPROTECT YES

Befehlszeile:

Eine Sofortzugriffsoperation für eine virtuelle VMware-Maschine ausführen:

```
dsmc restore vm vm1 -vmname=new_vm1 -vmrestoretype=instantaccess
  -vmexpireprotect=no
```

Verwenden Sie die IBM Spectrum Protect Recovery Agent-GUI, um Dateien aus einer Sicherung einer virtuellen Maschine zurückzuschreiben.

Informationen zu IBM Spectrum Protect Recovery Agent finden Sie in der Dokumentation zu IBM Spectrum Protect for Virtual Environments.

 Windows-Betriebssysteme

Vmiscsiadapter

Diese Option gibt an, welcher iSCSI-Adapter auf dem ESX-Host für Sofortzurückschreibungsoperationen und Sofortzugriffsoperationen für virtuelle VMware-Maschinen verwendet werden soll.

Unterstützte Clients

Diese Option ist für 64-Bit-Windows-Clients gültig, die als Einheiten zum Versetzen von Daten konfiguriert sind, die virtuelle VMware-Maschinen sichern.

Optionsdatei

Definieren Sie diese Option in der Clientoptionsdatei (dsm.opt). Sie können diese Option auch als Befehlszeilenparameter im Befehl restore vm angeben, mit dem eine Sofortzurückschreibungs- oder Sofortzugriffsoperation eingeleitet wird. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Syntax

```
>>-VMISCSIAdapter=--iSCSI-Adaptername--------------------------><
```

iSCSI-Adaptername

Gibt den Namen des iSCSI-Adapters an, zu dem die Verbindung auf dem ESX-Host hergestellt werden soll. Wenn Sie diese Option nicht angeben, wird der erste iSCSI-Adapter verwendet, der auf dem Host gefunden wird.

Beispiele

Optionsdatei:

```
vmiscsiadapter "vmhba36"
```

Befehlszeile:

```
dsmc restore vm “Haifa” -VMRESToretype=INSTANTAccess -vmname=”Haifa_verify" -VMISCSIAdapter="vmhba36"
```

Windows-Betriebssysteme

Vmiscsiserveraddress

Verwenden Sie die Option vmiscsiserveraddress mit dem Befehl restore VM, um den Hostnamen oder die IP-Adresse des iSCSI-Servers anzugeben, der die iSCSI-Ziele für Sofortzurückschreibungs- und Sofortzugriffsoperationen bereitstellt.

Die Option vmiscsiserveraddress ist für alle Sofortoperationen (`vmrestoretype=instantaccess` und `vmrestoretype=instantrestore`) für virtuelle VMware-Maschinen gültig.

Die virtuellen Maschinen müssen auf Servern mit VMware ESXi 5.1 oder höher gehostet werden. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Unterstützte Clients

 WindowsBetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

Syntax

```
>>-VMISCSIServeraddress-- --Hostname oder IP-Adresse des iSCSI-Servers-><
```

Parameter

Hostname oder IP-Adresse des iSCSI-Servers

Geben Sie den Hostnamen oder die IP-Adresse des iSCSI-Servers an, der die iSCSI-Zielplatten bereitstellt. Dieser iSCSI-Server muss die Maschine der Einheit zum Versetzen von Daten mit allen ESX-Hosts verbinden, die für Sofortzurückschreibungsoperationen verwendet werden. Wenn vmiscsiserveraddress nicht angegeben wird, wird der Hostname oder die IP-Adresse der Einheit zum Versetzen von Daten verwendet.

Bei Sofortzurückschreibungsoperationen muss sich die IP-Adresse der Netzkarte auf der Maschine der Einheit zum Versetzen von Daten, die für die iSCSI-Übertragung verwendet wird, in demselben Teilnetz wie der iSCSI-Adapter auf dem ESX-Host befinden.

Bei Dateizurückschreibungsmountoperationen müssen die Windows- und Linux-Mount-Proxy-Systeme sich in demselben Netzbereich befinden.

Beispiele

Optionsdatei:

```
VMISCSIServeraddress 192.168.42.50
```

Befehlszeile:

```
dsmc restore vm Oslo -VMRESToretype=INSTANTAccess -vmname=Oslo_verify
-VMISCSIServeraddress=odin.oslo.no.xyzco.com
```

Linux-Betriebssysteme Windows-Betriebssysteme

Vmlimitperdatastore

Die Option vmlimitperdatastore gibt die Anzahl virtueller Maschinen (VMs) und virtueller Platten in einem Datenspeicher an, die während einer optimierten Sicherungsoperation parallel verarbeitet werden können.

Bei einer optimierten Sicherungsoperation sind parallele Sicherungen auf der VM-Ebene, auf der Ebene der virtuellen Platte oder auf der Unterplattenebene aktiviert.

Die Option vmlimitperdatastore wird zusammen mit den Optionen vmmaxparallel, vmmaxbackupsessions und vmlimitperhost verwendet, um Sicherungsoperationen zu optimieren und das Ressourcenvolumen zu steuern, das durch die Sicherung auf einem Host in der vSphere-Infrastruktur erstellt werden kann. Passen Sie die Werte dieser Optionen an, um die Werte zu ermitteln, mit denen eine optimale Leistung für die Sicherungen in Ihrer Umgebung erzielt wird.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden. Diese Option ist nicht für Data Protection for Microsoft Hyper-V-Sicherungen gültig.

Optionsdatei

Linux-BetriebssystemeDiese Option ist in der Clientsystemoptionsdatei (dsm.sys), in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Windows-BetriebssystemeDiese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

```
                          .-0--------------.
>>-VMLIMITPERDatastore-- --+-+------------+-+------------------><
                            '-ganze_Zahl-'
```

Parameter

ganze_Zahl
Gibt die maximale Anzahl VMs in einem beliebigen Datenspeicher an, die in eine optimierte Sicherungsoperation eingeschlossen werden. Sie können maximal 50 virtuelle Maschinen angeben. Der Standardwert ist 0 (null).
Die Angabe 0 bedeutet, dass die Anzahl der virtuellen Maschinen, die parallel aus einem Datenspeicher gesichert werden können, keine Rolle spielt. Stattdessen soll die maximale Anzahl virtueller Maschinen, die in eine Sicherung eingeschlossen werden sollen, mit dem für die Option vmmaxparallel angegebenen Wert begrenzt werden. Die Option vmlimitperdatastore wird auch dann umgesetzt, wenn VM-Daten in zwei oder mehr Datenspeichern vorhanden sind.

Beispiele

Optionsdatei
VMLIMITPERD 5
Befehlszeile:
```
dsmc backup vm -VMLIMITPERD=5
```

Zugehörige Verweise:
Backup VM
Domain.vmfull
Vmmaxbackupsessions
Vmmaxparallel
Vmlimitperhost
Zugehörige Informationen:
Mehrere virtuelle Maschinen parallel sichern
Linux-Betriebssysteme Windows-Betriebssysteme

Vmlimitperhost

Die Option vmlimitperhost gibt die Anzahl virtueller Maschinen (VMs) und virtueller Platten in einem Host an, die während einer optimierten Sicherungsoperation parallel verarbeitet werden können.

Bei einer optimierten Sicherungsoperation sind parallele Sicherungen auf der VM-Ebene, auf der Ebene der virtuellen Platte oder auf der Unterplattenebene aktiviert.

Die Option vmlimitperhost wird zusammen mit den Optionen vmmaxparallel, vmmaxbackupsessions und vmlimitperdatastore verwendet, um Sicherungsoperationen zu optimieren und das Ressourcenvolumen zu steuern, das durch die Sicherung auf einem Host in der vSphere-Infrastruktur erstellt werden kann. Passen Sie die Werte dieser Optionen an, um die Werte zu ermitteln, mit denen eine optimale Leistung für die Sicherungen in Ihrer Umgebung erzielt wird.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden. Diese Option ist nicht für Data Protection for Microsoft Hyper-V-Sicherungen gültig.

Optionsdatei

Linux-BetriebssystemeDiese Option ist in der Clientsystemoptionsdatei (dsm.sys), in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Windows-BetriebssystemeDiese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

```
                      .-0--------------.
>>-VMLIMITPERHost-- --+-+-------------+-+-----------------------><
                      '-ganze_Zahl-'
```

Parameter

ganze_Zahl
Gibt die maximale Anzahl VMs auf einem beliebigen ESX-Server an, die in eine optimierte Sicherungsoperation eingeschlossen werden können. Sie können maximal 50 virtuelle Maschinen angeben. Der Standardwert ist 0 (null).

Die Angabe 0 bedeutet, dass die Anzahl der virtuellen Maschinen, die parallel auf einem ESX-Server gesichert werden können, keine Rolle spielt. Stattdessen soll die maximale Anzahl virtueller Maschinen, die in eine Sicherung eingeschlossen werden sollen, mit dem für die Option vmmaxparallel angegebenen Wert begrenzt werden.

Beispiele

Optionsdatei
VMLIMITPERH 5
Befehlszeile:
```
dsmc backup vm -VMLIMITPERH=5
```

Zugehörige Verweise:
Backup VM
Domain.vmfull
Vmmaxparallel
Vmlimitperhost
Zugehörige Informationen:
Mehrere virtuelle Maschinen parallel sichern
Windows-Betriebssysteme

Vmlist

Die Option vmlist ist für Hyper-V-Sicherungsoperationen veraltet. Um eine oder mehrere virtuelle Hyper-V-Maschinen (VMs) in Data Protection for Microsoft Hyper-V-Sicherungsoperation einzuschließen, verwenden Sie die Option domain.vmfull oder geben Sie die VMs bei der Ausführung des Befehls backup vm an.

Informationen zur Verwendung der Option vmlist enthält die Dokumentation in früheren Releases von IBM Spectrum Protect.

Zugehörige Verweise:
Domain.vmfull
Backup VM
Linux-Betriebssysteme Windows-Betriebssysteme

Vmmaxbackupsessions

Die Option vmmaxbackupsessions gibt die maximale Anzahl IBM Spectrum Protect-Serversitzungen zum Versetzen von VM-Daten auf den Server an, die in eine optimierte Sicherungsoperation eingeschlossen werden können.

Bei einer optimierten Sicherungsoperation sind parallele Sicherungen auf der VM-Ebene, auf der Ebene der virtuellen Platte oder auf der Unterplattenebene aktiviert.

Die Option vmmaxbackupsessions wird zusammen mit den Optionen vmmaxparallel, vmlimitperdatastore und vmlimitperhost verwendet, um Sicherungsoperationen zu optimieren und das Ressourcenvolumen zu steuern, das durch die Sicherung auf einem Host in der vSphere-Infrastruktur erstellt werden kann. Passen Sie die Werte dieser Optionen an, um die Werte zu ermitteln, mit denen eine optimale Leistung für die Sicherungen in Ihrer Umgebung erzielt wird.

Unterstützte Clients

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden. Diese Option ist nicht für Data Protection for Microsoft Hyper-V-Sicherungen gültig.

Optionsdatei

Linux-BetriebssystemeDiese Option ist in der Clientsystemoptionsdatei (dsm.sys), in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Windows-BetriebssystemeDiese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

```
.-vmmaxparallelvalue-.
```

```
>>-VMMAXBACKUPSEssions-- --+-+------------+-----+--------------><
                          '-ganze_Zahl-'
```

Parameter

ganze_Zahl

Gibt die maximale Anzahl IBM Spectrum Protect-Serversitzungen an, die während der Sicherungsoperation erstellt werden können.

Lesen Sie die folgenden Informationen zur Verwendung der Option vmmaxbackupsessions in Verbindung mit der Option vmmaxparallel oder dem Serverparameter maxnummp:

vmmaxparallel
: Die Option vmmaxparallel gibt die maximale Anzahl virtueller Maschinen an, die gleichzeitig auf dem IBM Spectrum Protect-Server gesichert werden können. Der Wert für die Option vmmaxbackupsessions muss größer-gleich dem Wert für die Option vmmaxparallel sein.
Wenn der Wert kleiner als der Wert für die Option vmmaxparallel ist, wird die folgende Nachricht zurückgegeben und der Wert in denselben Wert wie für die Option vmmaxparallel geändert:
ANS9995W `Der Wert der Option VMMAXBACKUPSESSIONS ist 'Zahlenwert'. Dieser Wert muss größer-gleich dem Wert der Option VMMAXPARALLEL sein, der 'Zahlenwert' lautet. Der Wert wird auf den Wert der Option VMMAXPARALLEL gesetzt.`

maxnummp
: Der Serverparameter maxnummp gibt die maximale Anzahl Mountpunkte an, die ein Knoten auf dem Server verwenden darf, wenn das Kopienziel des Speicherpools FILE oder TAPE lautet. Der Parameter maxnummp muss größer-gleich der Einstellung für die Optionen vmmaxparallel und vmmaxbackupsessions sein. Wenn mehrere Instanzen des Clients Dateien sichern oder wenn ein einziger Client parallele Sicherungen ausführt, sind unter Umständen mehr Mountpunkte erforderlich.
Wenn der Wert für vmmaxparallel oder vmmaxbackupsessions den Wert für maxnummp überschreitet, werden Nachricht ANS0266I und andere Nachrichten angezeigt. Abhängig von der Nachricht verringert der Client den Wert für die Option vmmaxparallel auf die Anzahl, die durch den Parameter maxnummp angegeben ist, oder verhindert das Öffnen weiterer Sitzungen für die angegebene VM. In jeder dieser Situationen wird die Sicherungsoperation fortgesetzt.
Werden weitere Fehler ANS0266I gefunden, verringert der Client den Wert für vmmaxparallel um 1 und versucht, die Sicherung fortzusetzen. Wenn der Wert für vmmaxparallel auf 1 verringert wird und der Client weitere Fehler ANS0266I empfängt, beendet der Client die Sicherung und gibt den folgenden Fehler aus:
ANS5228E `Eine VM-Sicherungsoperation ist fehlgeschlagen, weil VMMAXPARALLEL auf 1 reduziert wurde und der Client noch immer keinen Servermountpunkt abrufen kann.`
Wenden Sie sich an Ihren Serveradministrator, wenn der aktuelle Wert für maxnummp erhöht werden soll, damit Ihr Knoten weitere parallele Sicherungssitzungen unterstützen kann.
Unter Windows Server 2012 und 2012 R2 erstellt IBM Spectrum Protect während der Sicherungen virtueller Hyper-V-Maschinen VSS-Momentaufnahmen aller Datenträger, die Daten virtueller Maschinen enthalten. Sicherungsdaten werden aus den VSS-Momentaufnahmen und nicht aus Daten auf dem Livedateisystem gelesen. Wenn IBM Spectrum Protect versucht, mehrere Momentaufnahmen gleichzeitig zu erstellen, kann es in vielen Fällen vorkommen, dass der VSS-Software-Provider eine Momentaufnahmeanforderung für mehrere virtuelle Maschinen nicht ausführen kann. Ursache für das Auftreten der Fehler ist, dass der VSS-Softwaremomentaufnahmeprovider die Last nicht handhaben kann, die durch den Versuch, mehrere Sicherungen gleichzeitig auszuführen, erstellt wird. Um dieses Problem zu verhindern, verwenden Sie statt eines VSS-Software-Providers einen VSS-Hardwaremomentaufnahmeprovider.

Sie können maximal 100 Sitzungen angeben. Der Standardwert ist der für die Option vmmaxparallel festgelegte Wert.

Beispiele

Optionsdatei
: VMMAXBACKUPS 10

Befehlszeile:
```
dsmc backup vm -VMMAXBACKUPS=10
```

Zugehörige Verweise:
Backup VM
Domain.vmfull
Vmmaxparallel
Vmlimitperdatastore
Vmlimitperhost

Zugehörige Informationen:
Mehrere virtuelle Maschinen parallel sichern
Linux-Betriebssysteme Windows-Betriebssysteme

Vmmaxparallel

Die Option vmmaxparallel dient zum Konfigurieren optimierter Sicherungen mehrerer virtueller Maschinen mithilfe einer einzigen Instanz des Clients für Sichern/Archivieren. Diese Option gibt die maximale Anzahl virtueller Maschinen an, die gleichzeitig auf dem IBM Spectrum Protect-

Server gesichert werden können.

Bei einer optimierten Sicherungsoperation sind parallele Sicherungen auf der VM-Ebene, auf der Ebene der virtuellen Platte oder auf der Unterplattenebene aktiviert.

Die Option vmmaxparallel wird zusammen mit den Optionen vmmaxbackupsessions, vmlimitperhost und vmlimitperdatastore verwendet, um Sicherungsoperationen zu optimieren und das Ressourcenvolumen zu steuern, das durch die Sicherung auf einem Host in der vSphere-Infrastruktur erstellt werden kann. Passen Sie die Werte dieser Optionen an, um die Werte zu ermitteln, mit denen eine optimale Leistung für die Sicherungen in Ihrer Umgebung erzielt wird.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Für Data Protection for Microsoft Hyper-V ist diese Option nur bei Hyper-V-Sicherungsoperationen unter den Betriebssystemen Windows Server 2012 und 2012 R2 gültig.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Linux-BetriebssystemeDiese Option ist in der Clientsystemoptionsdatei (dsm.sys) und in der Befehlszeile für den Befehl Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Windows-BetriebssystemeDiese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für den Befehl Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

```
                  .-4--------------.
>>-VMMAXParallel--+-+------------+-+--------------------------><
                    '-ganze_Zahl-'
```

Parameter

ganze_Zahl
Gibt die maximale Anzahl virtueller Maschinen an, die während einer optimierten Sicherungsoperation gleichzeitig gesichert werden können. Der Standardwert ist 4. Der Maximalwert ist 50.
Tipp: Wenn Sie die clientseitige Datendeduplizierung verwenden, wird eine Datendeduplizierungssitzung für jede VM gestartet. Diese Datendeduplizierungssitzungen werden bei vmmaxparallel nicht mitgezählt.
Lesen Sie die folgenden Informationen zur Verwendung der Option vmmaxparallel zusammen mit der Option vmmaxbackupsessions oder dem Serverparameter maxnummp:

vmmaxbackupsessions
Die Option vmmaxbackupsessions gibt die maximale Anzahl Sitzungen zum Versetzen von Daten virtueller Maschinen auf den Server an, die in eine optimierte Sicherungsoperation eingeschlossen werden können. Der Wert für die Option vmmaxbackupsessions muss größer-gleich dem Wert für die Option vmmaxparallel sein.

maxnummp
Der Serverparameter maxnummp gibt die maximale Anzahl Mountpunkte an, die ein Knoten auf dem Server verwenden darf, wenn das Kopienziel des Speicherpools FILE oder TAPE lautet. Der Parameter maxnummp muss größer-gleich der Einstellung für die Optionen vmmaxparallel und vmmaxbackupsessions sein. Wenn mehrere Instanzen des Clients Dateien sichern oder wenn ein einziger Client parallele Sicherungen ausführt, sind unter Umständen mehr Mountpunkte erforderlich.
Wenn der Wert für vmmaxparallel oder vmmaxbackupsessions den Wert für maxnummp überschreitet, werden Nachricht ANS0266I und andere Nachrichten angezeigt. Abhängig von der Nachricht verringert der Client den Wert für die Option vmmaxparallel auf die Anzahl, die durch den Parameter maxnummp angegeben ist, oder verhindert das Öffnen weiterer Sitzungen für die angegebene VM. In jeder dieser Situationen wird die Sicherungsoperation fortgesetzt.
Werden weitere Fehler ANS0266I gefunden, verringert der Client den Wert für vmmaxparallel um 1 und versucht, die Sicherung fortzusetzen. Wenn der Wert für vmmaxparallel auf 1 verringert wird und der Client weitere Fehler ANS0266I empfängt, beendet der Client die Sicherung und gibt den folgenden Fehler aus:
ANS5228E `Eine VM-Sicherungsoperation ist fehlgeschlagen, weil VMMAXPARALLEL auf 1 reduziert wurde und der Client noch immer keinen Servermountpunkt abrufen kann.`
Wenden Sie sich an Ihren Serveradministrator, wenn der aktuelle Wert für maxnummp erhöht werden soll, damit Ihr Knoten weitere parallele Sicherungssitzungen unterstützen kann.
Unter Windows Server 2012 und 2012 R2 erstellt IBM Spectrum Protect während der Sicherungen virtueller Hyper-V-Maschinen VSS-Momentaufnahmen aller Datenträger, die Daten virtueller Maschinen enthalten. Sicherungsdaten werden aus den VSS-Momentaufnahmen und nicht aus Daten auf dem Livedateisystem gelesen. Wenn IBM Spectrum Protect versucht, mehrere

Momentaufnahmen gleichzeitig zu erstellen, kann es in vielen Fällen vorkommen, dass der VSS-Software-Provider eine Momentaufnahmeanforderung für mehrere virtuelle Maschinen nicht ausführen kann. Ursache für das Auftreten der Fehler ist, dass der VSS-Softwaremomentaufnahmeprovider die Last nicht handhaben kann, die durch den Versuch, mehrere Sicherungen gleichzeitig auszuführen, erstellt wird. Um dieses Problem zu verhindern, verwenden Sie statt eines VSS-Software-Providers einen VSS-Hardwaremomentaufnahmeprovider.

Beispiele

Optionsdatei

VMMAXP 10


Befehlszeile:


```
dsmc backup vm -VMMAXP=10
```

Zugehörige Verweise:
Backup VM
Domain.vmfull
Vmlimitperhost
Vmlimitperdatastore

Zugehörige Informationen:
Mehrere virtuelle Maschinen parallel sichern


Vmmaxpersnapshot

Mithilfe der Option vmmaxpersnapshot können Sie die maximale Anzahl virtueller Maschinen (VMs) angeben, die in eine Hyper-V-Momentaufnahme eingeschlossen werden sollen. Die VMs in der Momentaufnahme werden auf dem IBM Spectrum Protect-Server gesichert.

Indem die Anzahl virtueller Maschinen in einer Momentaufnahme erhöht wird, können Sie die Anzahl Momentaufnahmen, die für eine Sicherungsoperation erstellt werden, reduzieren. Dadurch werden Konkurrenzsituationen bei der Planung, die während Clustersicherungsoperationen für virtuelle Maschinen auf freigegebenen Clusterdatenträgern (CSVs = Clustered Shared Volumes) auftreten, reduziert.

Die Erstellung einer Momentaufnahme mit vielen virtuellen Maschinen dauert länger und erhöht die Systembelastung. Eine größere Anzahl virtueller Maschinen bedeutet, dass die Momentaufnahme länger bestehen bleibt, was Auswirkungen auf die Leistung haben kann.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ausgeführt wird.

Diese Option ist nur für Hyper-V-Sicherungsoperationen unter Betriebssystemen Windows Server 2012 und 2012 R2 gültig.

Unterstützte Clients

Diese Option ist für alle unterstützten Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für den Befehl Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

```
                    .-20---------.
>>-VMMAXPERSnapshot--+-ganze_Zahl-+----------------------------><
```

Parameter

ganze_Zahl

Gibt die maximale Anzahl VMs an, die in eine Hyper-V-Momentaufnahme eingeschlossen werden können. Der Standardwert ist 20. Der Maximalwert ist 100. Der Mindestwert ist 1.

Wenn einige VMs auf lokalen Datenträgern und einige VMs auf freigegebenen Clusterdatenträgern (CSVs) gespeichert sind, ist die Anzahl VMs in einer Momentaufnahme unter Umständen kleiner als die Einstellung für vmmaxpersnapshot. Eine Momentaufnahme kann nicht gleichzeitig VMs auf lokalen Datenträgern und VMs auf CSV-Datenträgern enthalten.

Um zu verhindern, dass eine Momentaufnahme erstellt wird, die sich über mehrere Datenträger erstreckt, kann die Anzahl VMs in einer Momentaufnahme kleiner als die maximale Anzahl sein, wenn sich die VMs auf unterschiedlichen Datenträgern befinden. Beispiel: Vier

VMs befinden sich auf Datenträger A und eine VM befindet sich auf Datenträger B. Es wird eine Momentaufnahme mit nur vier VMs (von Datenträger A) erstellt, obwohl die maximale Einstellung fünf ist. Für Datenträger B wird eine zweite Momentaufnahme erstellt.

Beispiele

Optionsdatei

```
vmmaxpersnapshot 10
```

Befehlszeile

```
dsmc backup vm -vmmaxpers=10
```

Zugehörige Verweise:
Vmmaxsnapshotretry
Zugehörige Informationen:
Geplante VM-Sicherungen für Windows Server 2012- und 2012 R2-Cluster optimieren
Linux-BetriebssystemeWindows-Betriebssysteme

Vmmaxrestoresessions

Die Option vmmaxrestoresessions gibt die maximale Anzahl IBM Spectrum Protect-Serversitzungen an, die in eine optimierte Zurückschreibungsoperation für eine virtuelle Maschine (VM) eingeschlossen werden können.

Bei einer optimierten Zurückschreibungsoperation sind parallele Zurückschreibungen auf der Unterplattenebene einer virtuellen Platte aktiviert.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden. Diese Option ist nicht für Data Protection for Microsoft Hyper-V-Sicherungen gültig.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Linux-BetriebssystemeDiese Option ist in der Clientsystemoptionsdatei (dsm.sys), in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für Restore VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Windows-BetriebssystemeDiese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für Restore VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

```
                          .-1--------------.
>>-VMMAXRESTORESessions-- --+-+------------+-+-----------------><
                            '-ganze_Zahl-'
```

Parameter

ganze_Zahl

Gibt die Anzahl IBM Spectrum Protect-Serversitzungen an, die während der Zurückschreibungsoperation erstellt werden. Der Standardwert ist 1.

Beispiele

Optionsdatei

```
VMMAXRESTORES 10
```

Windows-BetriebssystemeBefehlszeile:

Windows-Betriebssysteme`dsmc restore vm -VMMAXRESTORES=10`

Zugehörige Verweise:
Restore VM
Linux-BetriebssystemeWindows-Betriebssysteme

Vmmaxrestoreparalleldisks

Die Option vmmaxrestoreparalleldisks ermöglicht einem IBM Spectrum Protect-Client die gleichzeitige Zurückschreibung mehrerer virtueller Platten.

Sie können die Anzahl zu öffnender Plattensitzungen bis zu einem Maximalwert von 50 Sitzungen angeben. Die Anzahl verfügbarer Plattenzurückschreibungssitzungen wird mit der Option vmmaxrestoresessions angegeben. Die Zuordnung verfügbarer Sitzungen erfolgt gemäß der mit vmmaxrestoreparalleldisks angegebenen Anzahl Plattensitzungen; dabei wird die Anzahl Sitzungen pro Platte auf die nächste ganze Zahl abgerundet.

Unterstützte Clients

 Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

 Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden. Diese Option ist nicht für Data Protection for Microsoft Hyper-V-Sicherungen gültig.

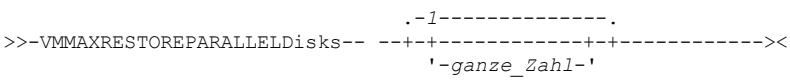
 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

 Linux-BetriebssystemeDiese Option ist in der Clientsystemoptionsdatei (dsm.sys) und in der Befehlszeile für Restore VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

 Windows-BetriebssystemeDiese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für Restore VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax



Parameter

ganze_Zahl

Gibt die Anzahl virtueller Festplatten an, die gleichzeitig zurückgeschrieben werden können. Der Standardwert ist 1. Der Maximalwert ist 50.

Beispiele

Task

Maximal 10 simultane Zurückschreibungsoperationen für virtuelle Platten in der VM vm1 festlegen:

```
dsmc restore vm vm1 -vmmaxrestoreparalleldisks=10 -vmmaxrestoresessions=20
```

Damit werden pro virtueller Platte zwei simultane Zurückschreibungssitzungen zugeordnet.

Zugehörige Verweise:
Restore VM
Windows-Betriebssysteme

Vmmaxsnapshotretry

Verwenden Sie die Option vmmaxsnapshotretry, um die maximale Anzahl Wiederholungen einer Momentaufnahmeoperation für eine virtuelle Maschine (VM) anzugeben, wenn die erste Momentaufnahmeoperation mit einer wiederherstellbaren Bedingung fehlschlägt.

Wenn während einer VM-Sicherung eine Momentaufnahmeoperation für eine VM aufgrund einer temporären Bedingung fehlschlägt, versucht Data Protection for Microsoft Hyper-V automatisch, die Momentaufnahmeoperation zu wiederholen, bis die durch die Option vmmaxsnapshotretry angegebene Anzahl Wiederholungen erreicht ist. Wenn die Momentaufnahmeoperation immer noch fehlschlägt, nachdem die maximale Anzahl Wiederholungen erreicht ist, wird nicht erneut versucht, die Momentaufnahmeoperation für die VM auszuführen, und der Sicherungsversuch schlägt fehl.

Eine wiederherstellbare Bedingung kann beispielsweise durch zwei Sicherungsanforderungen verursacht werden, die etwa zu derselben Zeit gestartet werden, um VMs zu sichern, die sich auf demselben Datenträger befinden. Eine der Sicherungsoperationen meldet, dass die Momentaufnahmeoperation fehlgeschlagen ist, da die Sicherung nicht gestartet werden kann, während eine andere Sicherung für dieselbe VM aktiv ist. In diesem Fall versucht Data Protection for Microsoft Hyper-V, die Momentaufnahmeoperation zu wiederholen, nachdem die erste VM-Sicherung abgeschlossen ist.

Wenn der ursprüngliche Fehler nicht behebbar ist, wird nicht versucht, eine Momentaufnahmeoperation auszuführen. Wenn beispielsweise während des ersten Momentaufnahmeprozesses ein Fehler beim VSS-Writer auftritt, wird die Sicherungsverarbeitung gestoppt und Data Protection for Microsoft Hyper-V versucht nicht, die Momentaufnahmeoperation zu wiederholen.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ausgeführt wird.

Diese Option ist nur für Hyper-V-Sicherungsoperationen unter Betriebssystemen Windows Server 2012 und 2012 R2 gültig.

Unterstützte Clients

Diese Option ist für alle unterstützten Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Diese Option ist in der Clientoptionsdatei (dsm.opt) und in der Befehlszeile für den Befehl Backup VM gültig. Sie kann auch auf dem Server in einer Clientoptionsgruppe angegeben werden. Sie kann nicht im Profileditor definiert werden.

Syntax

```
                        .-20---------.
>>-VMMAXSNApshotretry--+-ganze_Zahl-+--------------------------><
```

Parameter

ganze_Zahl
Gibt die maximale Anzahl Wiederholungen der Momentaufnahmeoperation für eine VM an, wenn der erste Versuch zur Erstellung einer Momentaufnahme mit einer wiederherstellbaren Bedingung fehlschlägt. Der Standardwert ist 20. Der Maximalwert ist 30. Der Mindestwert ist 1.

Wenn beispielsweise die Option vmmaxsnapshotretry auf 12 gesetzt ist, versucht Data Protection for Microsoft Hyper-V bis zu 12 Mal, die Momentaufnahmeoperation zu wiederholen, nachdem die erste Momentaufnahmeoperation während einer VM-Sicherungsoperation fehlgeschlagen ist. Wenn die Momentaufnahmeoperation immer noch fehlschlägt, nachdem die 12 Wiederholungen ausgeführt wurden, wird nicht versucht, weitere Wiederholungen auszuführen, und der Sicherungsversuch schlägt fehl.

Vor dem nächsten Wiederholungsversuch für eine Momentaufnahmeoperation müssen mindestens 10 Minuten verstreichen. Die Zeit zwischen Versuchen verlängert sich, wenn die fehlgeschlagene VM Teil einer Momentaufnahme für VMs ist, die gerade gesichert werden. Die Sicherungsoperation für die anderen VMs muss abgeschlossen sein und die Momentaufnahme von der Sicherungsoperation entfernt werden, bevor ein Wiederholungsversuch erfolgen kann.

Beispiele

Optionsdatei
```
vmmaxsna 12
```
Befehlszeile
```
dsmc backup vm -vmmaxsna=12
```

Zugehörige Verweise:
Vmmaxpersnapshot
Zugehörige Informationen:
Geplante VM-Sicherungen für Windows Server 2012- und 2012 R2-Cluster optimieren
Linux-Betriebssysteme Windows-Betriebssysteme

Vmmaxvirtualdisks

Die Option vmmaxvirtualdisks gibt die maximale Größe von Platten virtueller VMware-Maschinen (VMDKs) an, die in eine Sicherungsoperation eingeschlossen werden sollen.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Verwenden Sie die Option vmmaxvirtualdisks mit der Option vmskipmaxvirtualdisks, um anzugeben, wie der Client große VMDKs während einer Sicherungsoperation verarbeitet:

- Definieren Sie die Option vmmaxvirtualdisks, um die maximale Größe von VMDKs anzugeben, die eingeschlossen werden sollen.
- Die Option vmskipmaxvirtualdisks können Sie so definieren, dass entweder VMDKs, die die maximale Größe nicht überschreiten, gesichert (und die VMDKs, die die Größe überschreiten, ausgeschlossen) werden oder dass die Operation fehlschlägt.

Unterstützte Clients

 Linux-BetriebssystemeDiese Option ist für 64-Bit-Linux-Clients gültig, die als Einheiten zum Versetzen von Daten für das Sichern virtueller VMware-Maschinen konfiguriert sind.

 Windows-BetriebssystemeDiese Option ist für 64-Bit-Windows-Clients gültig, die als Einheiten zum Versetzen von Daten für das Sichern virtueller VMware-Maschinen konfiguriert sind.

Optionsdatei

 Linux-BetriebssystemeDefinieren Sie die Option vmmaxvirtualdisks in der Clientsystemoptionsdatei (dsm.sys). Sie können diese Option auch als Befehlszeilenparameter im Befehl backup vm angeben.

 Windows-BetriebssystemeDefinieren Sie die Option vmmaxvirtualdisks in der Clientoptionsdatei (dsm.opt). Sie können diese Option auch als Befehlszeilenparameter im Befehl backup vm angeben.

Syntax

```
                      .-2----------.
>>-VMMAXVIRTUALDisks--+-Größe -----+---------------------------><
                      '-2...8, 999-'
```

Parameter

Größe

Gibt die maximale Größe der VMDKs in Terabyte an, die in eine Sicherungsoperation eingeschlossen werden sollen. Der Bereich ist eine ganze Zahl von 2 bis 8; der Standardwert ist 2. Der Maximalwert ist 8.
Geben Sie 999 an, um sicherzustellen, dass die Größe der VMware-VMDKs, die in Sicherungsoperationen eingeschlossen sind, immer die maximale Größe ist. Dieser Wert ist die einfachste Methode, um sicherzustellen, dass immer der Maximalwert definiert ist. Mit diesem Wert entfällt die kontinuierliche Änderung der Optionsdatei.
Wenn Sie außerdem die Option vmskipmaxvirtualdisks yes angeben, werden die VMDKs gesichert, die die angegebene maximale Größe nicht überschreiten, und die VMDKs ausgeschlossen, die die angegebenen maximale Größe überschreiten.
Wenn Sie außerdem die Option vmskipmaxvirtualdisks no angeben, schlagen Sicherungsoperationen fehl, wenn die Größe einer VMDK die angegebene maximale Größe überschreitet.

Beispiele

Optionsdatei:

```
vmmaxvirtualdisks 3
```

Befehlszeile:

VMDKs sichern, die maximal 5 TB groß sind, und VMDKs ausschließen, die größer als 5 TB sind:

```
backup vm VM1 -vmmaxvirtualdisks=5 -vmskipmaxvirtualdisks=yes
```

VMDKs sichern, die maximal 3 TB groß sind, und die Sicherung fehlschlagen lassen, wenn eine VMDK größer als 3 TB ist:

```
backup vm VM1 -vmmaxvirtualdisks=3 -vmskipmaxvirtualdisks=no
```

VMDKs sichern, die maximal 8 TB groß sind, und VMDKs ausschließen, die größer als 8 TB sind:

```
backup vm VM1 -vmmaxvirtualdisks=8 -vmskipmaxvirtualdisks=yes
```

oder

```
backup vm VM1 -vmmaxvirtualdisks=999 -vmskipmaxvirtualdisks=yes
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmmc

Verwenden Sie die Option vmmc, um die Sicherungen virtueller Maschinen mit einer anderen Verwaltungsklasse als der Standardverwaltungsklasse zu speichern. Für Sicherungen virtueller VMware-Maschinen ist die Option vmmc nur gültig, wenn die Option vmbackuptype=fullvm festgelegt ist.

Unterstützte Clients

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Linux-Betriebssysteme Windows-BetriebssystemeDiese Option ist für Clients gültig, die für die Sicherung virtueller VMware-Maschinen konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Windows-BetriebssystemeDiese Option ist für Clients gültig, die für die Sicherung virtueller Hyper-V-Maschinen konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei dsm.opt, in die Clientsystemoptionsdatei dsm.sys oder in die Befehlszeile ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

Syntax

```
>>-VMMC--Name der Verwaltungsklasse----------------------------><
```

Parameter

Name der Verwaltungsklasse
: Gibt eine Verwaltungsklasse an, die für die Sicherung von Daten virtueller Maschinen angewendet wird. Wird diese Option nicht definiert, wird die Standardverwaltungsklasse des Knotens verwendet.

Beispiele

Task:
: Eine Sicherung der virtuellen Maschine mit dem Namen `myVirtualMachine` ausführen und die Sicherung gemäß der Verwaltungsklasse mit dem Namen `myManagmentClass` speichern.
```
dsmc backup vm "myVirtualMachine" -vmmc=myManagmentClass
```

Windows-Betriebssysteme

Vmmountage

Verwenden Sie die Option vmmountage mit dem Befehl restore VM "*" -vmrestoretype=mountcleanupall, um die Dauer in Stunden anzugeben, während der eine VM-Zurückschreibung auf Dateiebene aktiv sein muss, damit sie bereinigt wird.

Unterstützte Clients

Windows-BetriebssystemeDiese Option ist nur für Windows-Clients gültig.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Windows-BetriebssystemeKeine. Sie können diese Option nur in der Befehlszeile angeben.

Syntax

```
>>-VMMOUNTAge = - --Stunden-------------------------------------><
```

Parameter

Stunden
: Gibt die Dauer in Stunden an, während der eine VM-Zurückschreibung auf Dateiebene aktiv sein muss, damit sie bereinigt wird. Alle aktiven Mountoperationen, die diesen Zeitraum überschreiten, werden bereinigt.
Der angegebene Wert muss eine ganze Zahl zwischen 0 und 10000 sein. Der Standardwert ist 0.

Beispiele

Befehlszeile:
: Alle Mountoperationen bereinigen, die länger als 24 Stunden aktiv sind:

```
dsmc restore vm "*" -VMRESToretype=MOUNTCLEANUPALL -VMMOUNTAge=24
```

Alle aktiven Mountoperationen bereinigen:

```
dsmc restore vm "*" -VMRESToretype=MOUNTCLEANUPALL -VMMOUNTAge=0
```

oder

```
dsmc restore vm "*" -VMRESToretype=MOUNTCLEANUPALL
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmnoprdmdisks

Diese Option ermöglicht dem Client die Zurückschreibung von Konfigurationsinformationen für die pRDM-Datenträger, die einer virtuellen VMware-Maschine zugeordnet sind, auch wenn die LUNs, die den Datenträgern zugeordnet wurden, nicht gefunden werden. Da pRDM-Datenträger in einer VM-Momentaufnahme nicht enthalten sind, können nur die Konfigurationsinformationen und nicht die Daten zurückgeschrieben werden, die sich auf den Datenträgern befanden.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist für Sicherungen von virtuellen Microsoft-Hyper-V-Maschinen nicht gültig.

Unterstützte Clients

Diese Option ist für Windows- und Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

 WindowsBetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

 Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Clientsystemoptionsdatei (dsm.sys) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Syntax

```
                .-NO--.
>>-VMNOPRDmdisks--+-----+----------------------------------------><
                '-YES-'
```

Parameter

YES
: Geben Sie diesen Wert an, wenn Sie eine virtuelle Maschine zurückschreiben müssen, die mit der Angabe `-vmprocesswithprdm=yes` gesichert wurde, und die ursprünglichen LUNs, die durch die RDM-Datei zugeordnet wurden, nicht lokalisiert werden können. Diese Einstellung hat zur Folge, dass der Client Versuche, die fehlenden, von den pRDM-Datenträgern verwendeten LUNs zu finden, überspringt und die ihnen zugeordneten Konfigurationsinformationen (Plattenkennsätze) zurückschreibt. Die pRDM-Datenträger werden als mit Thin-Provisioning definierte VMFS VMDKs zurückgeschrieben. Anschließend können Sie mit dem vSphere-Client die erforderlichen pRDM-Zuordnungen erstellen.

NO
: Bei Angabe von `-vmnoprdmdisk=no` schlagen Zurückschreibungsoperationen für virtuelle Maschinen, die mit `-processvmwithprdm=yes` gesichert wurden, fehl, wenn die ursprünglichen LUNs, die durch die RDM-Datei zugeordnet wurden, nicht lokalisiert werden können. Dies ist der Standardwert.

Beispiele

Optionsdatei:

```
VMNOPRDMDISKS YES
```

Befehlszeile:

```
dsmc restore vm vm123 -vmnoprdmdisks=yes
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmnovrdmdisks

Diese Option ermöglicht dem Client die Zurückschreibung von Konfigurationsinformationen und Daten für die vRDM-Datenträger, die einer virtuellen VMware-Maschine zugeordnet sind, auch wenn die LUNs, die den Datenträgern zugeordnet wurden, nicht gefunden werden.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist für Sicherungen von virtuellen Microsoft-Hyper-V-Maschinen nicht gültig.

Unterstützte Clients

Diese Option ist für Windows- und Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Clientsystemoptionsdatei (dsm.sys) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Syntax

```
                  .-NO--.
>>-VMNOVRDmdisks--+-----+---------------------------------------><
                  '-YES-'
```

Parameter

YES
: Geben Sie diesen Wert an, wenn Sie eine virtuelle Maschine zurückschreiben müssen, die gesichert wurde, und die ursprünglichen LUNs, die durch die RDM-Datei zugeordnet wurden, nicht lokalisiert werden können. Diese Einstellung hat zur Folge, dass der Client Versuche, die fehlenden, von den vRDM-Datenträgern verwendeten LUNs zu finden, überspringt und die Konfigurationsinformationen (Plattenkennsätze) sowie die gesicherten Daten zurückschreibt. Die vRDM-Datenträger werden als mit Thin-Provisioning definierte VMFS VMDKs zurückgeschrieben.

NO
: Bei Angabe von `-vmnovrdmdisk=no` schlagen Zurückschreibungsoperationen für virtuelle Maschinen mit vRDM-Datenträgern fehl, wenn die ursprünglichen LUNs, die durch die RDM-Datei zugeordnet wurden, nicht lokalisiert werden können. Dies ist der Standardwert.

Beispiele

Optionsdatei:

```
VMNOVRDMDISKS YES
```

Befehlszeile:

```
dsmc restore vm vm123 -vmnovrdmdisks=yes
```

Vmpreferdagpassive

Die Option vmpreferdagpassive gibt an, ob eine aktive Kopie oder eine passive Kopie einer Datenbank gesichert werden soll, die zu einer Microsoft Exchange Server-Datenbankverfügbarkeitsgruppe (DAG) gehört.

Diese Option gilt für Microsoft Exchange Server-Workloads, die in virtuellen VMware-Gastmaschinen ausgeführt werden, die durch IBM Spectrum Protect for Virtual Environments geschützt sind.

Verwenden Sie die Option vmpreferdagpassive mit dem Befehl backup vm.

Unterstützte Clients

Linux-BetriebssystemeWindows-BetriebssystemeDiese Option ist auf Clients gültig, die als Einheit zum Versetzen von Daten für VMware-Gastmaschinensicherungen agieren.

Optionsdatei

Linux-BetriebssystemeFügen Sie diese Option in die Clientsystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe ein.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                          .-No--.
>>-VMPREFERDAGPassive--+-----+---------------------------------><
                       '-Yes-'
```

Parameter

No
: Die Microsoft Exchange Server-Datenbank, unabhängig davon, ob es sich um eine aktive oder passive Kopie handelt, in einer Datenbankverfügbarkeitsgruppe (DAG) sichern. Dies ist der Standardwert.

Yes
: Die Sicherung einer aktiven Datenbankkopie in einer Datenbankverfügbarkeitsgruppe (DAG) überspringen, wenn eine gültige passive Kopie auf einem anderen Server verfügbar ist. Ist keine gültige passive Kopie verfügbar, wird die aktive Datenbankkopie gesichert.

Beispiele

Optionsdatei:
: vmpreferdagpassive yes

Linux-BetriebssystemeWindows-Betriebssysteme

Vmprocessvmwithindependent

Mit dieser Option können Sie steuern, ob vollständige VMware VM-Sicherungen verarbeitet werden, wenn die Maschine mit einer oder mit mehreren unabhängigen Plattendatenträgern bereitgestellt wird.

Unabhängige Plattendatenträger unterstützen keine Momentaufnahmen. Alle unabhängigen Plattendatenträger, die auf einer virtuellen Maschine gefunden werden, werden nicht als Teil der Sicherungsoperation verarbeitet. Bei der Zurückschreibung der virtuellen Maschine stellt der Client für Sichern/Archivieren die virtuelle Maschine wieder her und es werden nur die Datenträger zurückgeschrieben, die an Momentaufnahmeoperationen teilgenommen haben. Die Konfigurationsinformationen und der Inhalt der unabhängigen Plattendatenträger werden in den Informationen, die auf dem IBM Spectrum Protect-Server gespeichert werden, nicht beibehalten. Benutzer müssen die unabhängigen Plattendatenträger auf der zurückgeschriebenen Maschine erneut erstellen.

Enthält die virtuelle Maschine außerdem einen oder mehrere RDM-Datenträger (RDM = Raw Device Mapping), die im Modus für physische Kompatibilität (pRDM) konfiguriert sind, verwenden Sie die Option vmprocessvmwithprdm, um zu steuern, ob der Client Dateien auf der virtuellen Maschine sichert, wenn eine unabhängige Platte vorhanden ist.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist nur für VMware-Sicherungen gültig und gilt nicht für Microsoft Hyper-V-Sicherungen.

Unterstützte Clients

Diese Option ist für Windows- und Linux-Clients gültig, die als VMware-Sicherungsserver konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt), in die Clientsystemoptionsdatei (dsm.sys) oder in die Befehlszeile ein.

Syntax

```
                                .-NO--.
>>-VMPROCESSVMWITHINDEPENDENT--+-----+-------------------------><
                                '-YES-'
```

Parameter

No
: Die Sicherung der virtuellen Maschine schlägt fehl, wenn ein oder mehrere unabhängige Plattendatenträger erkannt werden. No ist der Standardwert.

Yes
: Virtuelle Maschinen, die einen oder mehrere unabhängige Plattendatenträger enthalten, werden gesichert. Die unabhängigen Plattendatenträger werden jedoch nicht als Teil der VM-Sicherungsoperation verarbeitet.
Enthält die virtuelle Maschine außerdem eine oder mehrere RDM-Platten, die im Modus für physische Kompatibilität bereitgestellt werden, muss auch die Option VMPROCESSVMWITHPRDM angegeben werden.

Beispiele

Optionsdatei:

```
VMPROCESSVMWITHINDEPENDENT Yes
```

Befehlszeile:

```
dsmc backup vm vmlocal -vmbackuptype=fullvm -vmprocessvmwithindependent=yes
```

 Windows-Betriebssysteme

Vmprocessvmwithphysdisks

Mithilfe der Option vmprocessvmwithphysdisks können Sie steuern, ob Hyper-V-RCT-Sicherungen einer virtuellen Maschine (VM) verarbeitet werden, wenn für die VM eine oder mehrere physische Platten (Durchgriffsplatten) bereitgestellt werden.

Eine virtuelle Maschine (VM) kann auf den Speicher auf einer physischen Platte zugreifen, die direkt mit dem Hyper-V-Server verbunden ist. Diese physische Platte wird als *Durchgriff*splatte bezeichnet.

Wenn Sie diese Option auf `yes` setzen, werden die Daten auf allen physischen Platten von Sicherungsoperationen ausgeschlossen, die Konfigurationsinformationen für die physischen Platten werden jedoch bei der VM-Sicherung gespeichert. Bei einer Zurückschreibungsoperation können Sie die Konfiguration der physischen Platten zurückschreiben, indem Sie die Option vmskipphysdisks no festlegen. Wenn die ursprünglichen physischen Platten verfügbar sind, werden sie wieder mit der zurückgeschriebenen VM verbunden.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ausgeführt wird.

Diese Option ist nur für Microsoft Hyper-V-Sicherungen gültig, aber nicht für VMware-Sicherungen.

Diese Option ist nur für RCT-Sicherungen unter Windows Server 2016 gültig. Diese Option ist nicht für Hyper-V-VSS-Sicherungen unter Windows Server 2012 oder Windows Server 2012 R2 gültig.

Unterstützte Clients

Diese Option ist für Clients unter Windows Server 2016 oder Betriebssystemen einer höheren Version gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein oder geben Sie sie als Befehlszeilenparameter im Befehl backup vm an.

Syntax

```
                              .-NO--.
>>-VMPROCESSVMWITHPHYSDisks--+-----+---------------------------><
                              '-YES-'
```

Parameter

No
: Die Sicherungsoperation der VM schlägt fehl, wenn eine oder mehrere physische Platten erkannt werden. Dies ist der Standardwert.

Yes
: VMs, die eine oder mehrere physische Platten enthalten, werden gesichert. Mit dieser Option wird die Konfiguration der physischen Platten gesichert, ohne die Daten auf den physischen Platten zu sichern.

Beispiele

Optionsdatei:

```
VMPROCESSVMWITHPHYSDISKS Yes
```

Befehlszeile:

```
dsmc backup vm vmlocal -vmprocessvmwithphysd=yes
```

Zugehörige Verweise:

Vmskipphysdisks
Linux-Betriebssysteme Windows-Betriebssysteme

Vmprocessvmwithprdm

Mit dieser Option können Sie steuern, ob vollständige VMware VM-Sicherungen verarbeitet werden, wenn die virtuelle Maschine über mindestens einen RDM-Datenträger (RDM = raw device mapping) verfügt, der im Modus für physische Kompatibilität (pRDM) bereitgestellt wird.

pRDM-Datenträger unterstützen keine Momentaufnahmen. Alle pRDM-Datenträger, die auf einer virtuellen Maschine gefunden werden, werden nicht als Teil der Sicherungsoperation verarbeitet. Bei der Zurückschreibung der virtuellen Maschine stellt der Client für Sichern/Archivieren die virtuelle Maschine wieder her und es werden nur die Datenträger zurückgeschrieben, die an Momentaufnahmeoperationen teilgenommen haben. Konfigurationsinformationen und der Inhalt der pRDM-Datenträger werden in den auf dem IBM Spectrum Protect-Server gespeicherten Informationen nicht beibehalten. Benutzer müssen die pRDM-Datenträger auf der zurückgeschriebenen Maschine erneut erstellen.

Diese Option gilt nicht für virtuelle Maschinen, die über mindestens einen RDM-Datenträger verfügen, der im Modus für virtuelle Kompatibilität (vRDM) bereitgestellt wird. Da vRDM-Datenträger Momentaufnahmeoperationen unterstützen, werden sie in eine vollständige VMware VM-Sicherung eingeschlossen.

Enthält die virtuelle Maschine außerdem eine oder mehrere unabhängige Platten, verwenden Sie die Option vmprocessvmwithindependent, um zu steuern, ob der Client Dateien auf der virtuellen Maschine sichert, wenn eine unabhängige Platte vorhanden ist.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Diese Option ist nur für VMware-Sicherungen gültig und gilt nicht für Microsoft Hyper-V-Sicherungen.

Unterstützte Clients

Diese Option ist für Windows- und Linux-Clients gültig, die als VMware-Sicherungsserver konfiguriert sind. Diese Option kann auch auf dem Server definiert werden.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

Linux-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt), in die Clientsystemoptionsdatei (dsm.sys) oder in die Befehlszeile ein.

Syntax

```
                          .-NO--.
>>-VMPROCESSVMWITHPRDM--+-----+---------------------------------><
                          '-YES-'
```

Parameter

No
: Die Sicherung der virtuellen Maschine schlägt fehl, wenn ein oder mehrere pRDM-Datenträger erkannt werden. No ist der Standardwert.

Yes
: Virtuelle Maschinen, die einen oder mehrere RDM-Datenträger enthalten, die im Modus für physische Kompatibilität (pRDM) bereitgestellt werden, werden gesichert. Die pRDM-Datenträger werden jedoch nicht als Teil der VM-Sicherungsoperation verarbeitet.
Enthält die virtuelle Maschine außerdem eine oder mehrere unabhängige Platten, muss auch die Option vmprocessvmwithindependentdisk angegeben werden.

Beispiele

Optionsdatei:

```
VMPROCESSVMWITHPRDM Yes
```

Befehlszeile:

```
dsmc backup vm vmlocal -vmbackuptype=fullvm -vmprocessvmwithprdm=yes
```

Windows-Betriebssysteme

Vmrestoretype

Verwenden Sie die Option vmrestoretype mit dem Befehl query VM oder restore VM, um den Typ der auszuführenden oder abzufragenden Zurückschreibungsoperation anzugeben.

Diese Option ist nur für virtuelle VMware-Maschinen gültig. Die virtuellen Maschinen müssen auf Servern mit VMware ESXi 5.1 oder höher gehostet werden. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Unterstützte Clients

 Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Diese Option muss in der Befehlszeile eines Befehls restore vm oder query vm angegeben werden. Sie können diese Option nicht in der Clientoptionsdatei angeben.

Syntax

```
                  .-NONinstant------.
>>-VMRESToretype--+-----------------+-------------------------><
                  +-INSTANTRestore--+
                  +-INSTANTAccess---+
                  +-VMCLeanup-------+
                  +-VMFULLCLeanup---+
                  +-ALLtype---------+
                  '-MOUNTCLEANUPAll-'
```

Parameter

noninstant
: Gibt an, dass eine klassische vollständige VM-Zurückschreibung ausgeführt wird. Dies ist der Standardzurückschreibungstyp.

instantrestore
: Gibt an, dass eine Sofortzurückschreibung ausgeführt wird. Während einer Sofortzurückschreibungsoperation wird die virtuelle Maschine während der Zurückschreibungsoperation gestartet. Wenn dieser Zurückschreibungstyp in einem Befehl query VM angegeben wird, gibt der Befehl eine Liste der virtuellen Maschinen zurück, die eine Sofortzurückschreibungsoperation ausführen.
  Wichtig: Stellen Sie bei Sofortzurückschreibungsoperationen sicher, dass sowohl der temporäre Datenspeicher, den Sie mit der Option vmtempdatastore angeben, als auch der VMware-Datenspeicher, der mit der Option datastore im Befehl 'restore VM' angegeben wird, über ausreichenden freien Speicherplatz zum Speichern der zurückzuschreibenden virtuellen Maschine und der Momentaufnahmedatei, die die an den Daten vorgenommenen Änderungen enthält, verfügen.

instantaccess
: Gibt an, dass eine temporäre Zurückschreibung der gesicherten virtuellen Maschine (VM) ausgeführt wird. Verwenden Sie diesen Zurückschreibungstyp, wenn eine virtuelle Maschine vorübergehend zurückgeschrieben werden soll, um die Integrität einer Sicherung zu testen, bevor Sie eine Sofortzurückschreibung ausführen. An der temporären virtuellen Maschine vorgenommene Änderungen werden nicht gespeichert.
  Wenn dieser Zurückschreibungstyp in einem Befehl query VM angegeben wird, gibt der Befehl eine Liste der virtuellen Maschinen zurück, die eine Sofortzugriffsoperation ausführen.

vmcleanup
: Gibt an, dass eine Bereinigung der ausgewählten virtuellen Maschine und ihrer Komponenten ausgeführt wird.
  Bei Sofortzugriffsoperationen werden mit dieser Option die temporäre virtuelle Maschine und alle ihre Komponenten entfernt.
  Bei Sofortzurückschreibungsoperationen werden mit dieser Option nur die Komponenten entfernt, die nicht mehr benötigt werden (z. B. iSCSI-Mounts). Die virtuelle Maschine wird nicht entfernt. Bereinigungsoperationen sind nicht zulässig, wenn die virtuelle Maschine auf den iSCSI-Platten noch ausgeführt wird. Informationen zum Erzwingen dieses Verhaltens finden Sie bei vmfullcleanup.

vmfullcleanup
: Die virtuelle Maschine und alle ihre Komponenten werden entfernt, unabhängig vom aktuellen Status. Wenn vMotion eine virtuelle Maschine noch migriert, dürfen Sie keine vollständige Bereinigungsoperation starten.

alltype
: Alle aktiven Sofortzugriffs- und Sofortzurückschreibungssitzungen werden abgefragt.

mountcleanupall
: Bereinigt alle aktiven Mountoperationen für VM-Zurückschreibungen auf Dateiebene, die älter sind als der Zeitraum, der mit der Option vmmountage angegeben ist. Sie müssen restore vm "*" angeben, um die Option mountcleanupall zu verwenden.

Beispiele

Befehlszeile:
: Einen Sofortzugriff für die virtuelle Maschine mit dem Namen Oslo ausführen. Die ursprüngliche virtuelle Maschine ist noch vorhanden. Folglich wird mit der Option -vmname der neue Name 'Oslo_verify' zugeordnet.

```
dsmc restore vm Oslo -vmrest=instantaccess -vmname=Oslo_verify
```

Eine Sofortzurückschreibung der virtuellen Maschine mit dem Namen 'Cologne' ausführen.

```
dsmc restore vm Cologne -vmrest=instantrestore
  -vmtempdatastore=Verify_datastore
```

Eine reguläre Zurückschreibung (vollständige VM-Zurückschreibung) der virtuellen Maschine mit dem Namen 'San_Jose' ausführen.

```
dsmc restore vm San_Jose
```

Sie können auch den folgenden Befehl verwenden: `dsmc restore vm San_Jose -vmrest=noni`
Eine Sofortzurückschreibung der virtuellen Maschine mit dem Namen Oslo mit der Option -pick ausführen, um eine bestimmte Sicherungsversion auszuwählen.

```
dsmc restore vm Oslo -vmrest=instantrestore -pick
```

Eine Bereinigung der virtuellen Maschine und aller ihrer Komponenten ausführen. Zu diesen Komponenten gehören iSCSI-Mounts, -Einheiten und temporäre Daten, die dem Namen der virtuellen Maschine auf dem ESX-Host zugeordnet sind.

```
dsmc restore vm Oslo -VMRESToretype=VMCLeanup -vmname=Oslo_Verify
```

Mit einer Abfrage alle aktiven Sofortzurückschreibungssitzungen suchen und einen abgekürzten Status für jede anzeigen.

```
dsmc query vm * -VMRESToretype=INSTANTRestore
```

Mit einer Abfrage alle aktiven virtuellen Maschinen im Sofortzurückschreibungsmodus und Sofortzugriffsmodus suchen.

```
dsmc query vm * -VMRESToretype=ALLtype
```

Mit einer Abfrage alle aktiven virtuellen Maschinen im Sofortzurückschreibungsmodus suchen und den detaillierten Status für jede virtuelle Maschine abrufen.

```
dsmc query vm * -VMRESToretype=INSTANTRestore -Detail
```

Mit einer Abfrage alle aktiven Sofortzugriffssitzungen suchen.

```
dsmc query vm * -VMRESToretype=INSTANTAccess
```

Führen Sie eine Mountbereinigung für alle Mountoperationen aus, die länger als 24 Stunden aktiv sind.

```
dsmc restore vm "*" -vmrestoretype=mountcleanupall -vmmountage=24
```

Windows-BetriebssystemeLinux-Betriebssysteme

Vmskipctlcompression

Mit der Option vmskipctlcompression können Sie bei VM-Sicherungen angeben, ob Steuerdateien (*.ctl) während einer VM-Sicherung komprimiert werden. Die Option hat keinen Einfluss auf die Komprimierung von Datendateien (*.dat).

Sie können Steuerdateien und Datendateien virtueller Maschinen nur dann komprimieren, wenn die Dateien in einem Speicherpool gespeichert sind, für den die clientseitige Deduplizierung aktiviert ist. Verwenden Sie die folgende Optionskonfiguration, um Datendateien zu komprimieren und Steuerdateien nicht zu komprimieren:

```
compression yes
vmskipctlcompression yes
```

Sie müssen die Datendateien in einen Speicherpool übertragen, für den die clientseitige Deduplizierung aktiviert ist. Sie können die Steuerdateien in einen Speicherpool übertragen, für den die clientseitige Deduplizierung nicht aktiviert ist.

Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments.

Unterstützte Clients

Windows-BetriebssystemeDiese Option kann für unterstützte Windows- und Linux-Clients verwendet werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

Syntax

```
                        .-Yes-.
>>-VMSKIPCTLCOMPRESSION--+-----+-------------------------------><
                        '-No--'
```

Parameter

Yes
: Steuerdateien (*.ctl) während einer VM-Sicherung nicht komprimieren. Die Option hat keinen Einfluss auf die Komprimierung von Datendateien (*.dat).

No
: Steuerdateien (*.ctl) können während einer VM-Sicherung komprimiert werden. Ob Steuerdateien komprimiert werden, ist vom Wert der Option compression abhängig.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmskipmaxvirtualdisks

Die Option vmskipmaxvirtualdisks gibt an, wie die Sicherungsoperation Platten virtueller VMware-Maschinen (VMDKs) verarbeitet, die die maximale Plattengröße überschreiten.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Verwenden Sie die Option vmskipmaxvirtualdisks mit der Option vmmaxvirtualdisks, um anzugeben, wie der Client während einer Sicherungsoperation große VMDKs verarbeitet:

- Die Option vmskipmaxvirtualdisks können Sie so definieren, dass entweder VMDKs, die die maximale Größe nicht überschreiten, gesichert (und die VMDKs, die die Größe überschreiten, ausgeschlossen) werden oder dass die Operation fehlschlägt.
- Definieren Sie die Option vmmaxvirtualdisks, um die maximale Größe von VMDKs anzugeben, die eingeschlossen werden sollen.

In Version 7.1.3 und früheren Versionen hatte die Option vmskipmaxvirtualdisks den Namen vmskipmaxvmdks. In Version 7.1.4 und höher ist vmskipmaxvirtualdisks der bevorzugte Optionsname. Der Client verarbeitet jedoch noch Sicherungsoperationen mit dem Namen vmskipmaxvmdks.

Unterstützte Clients

 Linux-BetriebssystemeDiese Option ist für 64-Bit-Linux-Clients gültig, die als Einheiten zum Versetzen von Daten für das Sichern virtueller VMware-Maschinen konfiguriert sind.

 Windows-BetriebssystemeDiese Option ist für 64-Bit-Windows-Clients gültig, die als Einheiten zum Versetzen von Daten für das Sichern virtueller VMware-Maschinen konfiguriert sind.

Optionsdatei

 Linux-BetriebssystemeDefinieren Sie die Option vmskipmaxvirtualdisks in der Clientsystemoptionsdatei (dsm.sys). Sie können diese Option auch als Befehlszeilenparameter im Befehl backup vm angeben.

 Windows-BetriebssystemeDefinieren Sie die Option vmskipmaxvirtualdisks in der Clientoptionsdatei (dsm.opt). Sie können diese Option auch als Befehlszeilenparameter im Befehl backup vm angeben.

Syntax

```
                          .-No--.
>>-VMSKIPMAXVIRTUALDISKS--+-----+-------------------------------><
                          '-Yes-'
```

Parameter

No
: Gibt an, dass Sicherungsoperationen fehlschlagen, wenn eine virtuelle VMware-Maschine mindestens eine VMDK enthält, die die maximale Größe überschreitet. Dies ist die Standardeinstellung.

Yes
: Gibt an, dass bei Sicherungsoperationen VMware-VMDKs eingeschlossen werden, die die maximale Größe nicht überschreiten, und VMDKs ausgeschlossen werden, die die maximale Größe überschreiten.

Beispiele

Optionsdatei:
```
vmskipmaxvirtualdisks yes
```
Befehlszeile:
: Angeben, dass eine Sicherungsoperation fehlschlagen soll, wenn eine VMDK größer als 2 TB ist:

```
backup vm VM1 -vmskipmaxvirtualdisks=no
```

Angeben, dass eine Sicherungsoperation fehlschlagen soll, wenn eine VMDK größer als 5 TB ist:

```
backup vm VM1 -vmskipmaxvirtualdisks=no -vmmaxvirtualdisks=5
```

VMDKs sichern, die maximal 8 TB groß sind, und VMDKs ausschließen, die größer als 8 TB sind:

```
backup vm VM1 -vmskipvirtualdisks=yes -vmmaxvirtualdisks=8
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmskipmaxvmdks

Die Option vmskipmaxvmdks gibt an, wie die Sicherungsoperation Platten virtueller VMware-Maschinen (VMDKs) verarbeitet, die die maximale Plattengröße überschreiten.

In Version 7.1.4 und höher wird vmskipmaxvmdks in vmskipmaxvirtualdisks umbenannt. Der bevorzugte Name ist zwar vmskipmaxvirtualdisks; der Client verarbeitet jedoch noch Sicherungsoperationen mit dem Namen vmskipmaxvmdks.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

 Windows-Betriebssysteme

Vmskipphysdisks

Mithilfe der Option vmskipphysdisks können Sie Konfigurationsinformationen für physische Platten (Durchgriffsplatten), die einer virtuellen Hyper-V-Maschine zugeordnet sind, zurückschreiben, wenn die Nummern logischer Einheiten (LUNs), die den Datenträgern auf den physischen Platten zugeordnet sind, verfügbar sind.

Da physische Platten nicht in eine VM-Momentaufnahme eingeschlossen sind, können nur die Konfigurationsinformationen, aber nicht die Daten auf den Datenträgern zurückgeschrieben werden.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V ausgeführt wird.

Diese Option ist nur für Microsoft Hyper-V-Sicherungen gültig, aber nicht für VMware-Sicherungen.

Diese Option ist nur für die Zurückschreibung virtueller Hyper-V-Maschinen unter Windows Server 2016 gültig. Diese Option gilt nicht für Hyper-V-Hosts unter Windows Server 2012 oder Windows Server 2012 R2.

Unterstützte Clients

Diese Option ist für Clients unter Windows Server 2016 oder Betriebssystemen einer höheren Version gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein oder geben Sie sie als Befehlszeilenparameter im Befehl restore vm an.

Syntax

```
                    .-NO--.
>>-VMSKIPPHYSDisks--+-----+-----------------------------------><
                    '-YES-'
```

Parameter

NO
: Wenn die ursprünglichen physischen Platten verfügbar sind, geben Sie diesen Wert an, um die Konfigurationsinformationen für die physischen Platten, die mit der Option vmprocessvmwithphysdisks yes gesichert wurden, zurückzuschreiben. Die ursprünglichen physischen Platten werden wieder mit der zurückgeschriebenen VM verbunden. Wenn die ursprünglichen physischen Platten nicht lokalisiert werden können, schlägt die Zurückschreibungsoperation fehl. Dies ist der Standardwert.

YES
: Geben Sie diesen Wert an, wenn Sie eine VM zurückschreiben müssen, die mit der Option vmprocessvmwithphysdisks yes gesichert wurde, und die ursprünglichen physischen Platten nicht lokalisiert werden können. Diese Einstellung hat zur Folge, dass der Client Versuche, die physischen Platten zu lokalisieren, überspringt und die Konfigurationsinformationen für die physischen Platten nicht zurückschreibt.

Beispiele

Optionsdatei:

```
VMSKIPPHYSDISKS YES
```

Befehlszeile:

```
dsmc restore vm vm123 -vmskipphysd=yes
```

Zugehörige Verweise:
Vmprocessvmwithphysdisks
Windows-Betriebssysteme

Vmstoragetype

Verwenden Sie die Option vmstoragetype mit dem Befehl restore VM, um den Typ der Speichereinheit anzugeben, von der die Momentaufnahme mit IBM Spectrum Protect Recovery Agent bereitgestellt wird.

Windows-Betriebssysteme

Sie können die Option vmstoragetype im Befehl restore VM -VMRESToretype=INSTANTRestore oder im Befehl restore VM -VMRESToretype=INSTANTAccess angeben.

Wird vmstoragetype angegeben, ist es nicht erforderlich, die Option für den Speichertyp in der IBM Spectrum Protect Recovery Agent-GUI anzugeben. Die Option vmstoragetype überschreibt die Einstellung für den Speichertyp in der Recovery Agent-GUI.

Unterstützte Clients

Windows-BetriebssystemeDiese Option ist nur unter Windows gültig.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Optionsdatei

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) auf dem Windows-Mount-Proxy-System oder in die Befehlszeile ein.

Windows-Betriebssysteme

Syntax

```
                  .-DISK-.
>>-VMSTORAGEType--+-VTL--+-------------------------------------><
                  '-TAPE-'
```

Parameter

Windows-BetriebssystemeDISK
Windows-BetriebssystemeDie Momentaufnahmen, die von Recovery Agent bereitgestellt werden sollen, befinden sich in Platten- oder Dateispeicherpools. Dies ist der Standardwert.
Windows-BetriebssystemeVTL
Die Momentaufnahmen, die von Recovery Agent bereitgestellt werden sollen, befinden sich in VTL-Speicherpools.
Windows-BetriebssystemeTAPE
Windows-BetriebssystemeDie Momentaufnahmen, die von Recovery Agent bereitgestellt werden sollen, befinden sich in Bandspeicherpools.

Beispiele

Optionsdatei:

```
VMSTORAGETYPE TAPE
```

Befehlszeile:

Windows-BetriebssystemeZurückschreibung einer virtuellen Maschine mit dem Namen Orion mithilfe des folgenden Befehls:

```
dsmc restore vm Orion -Host=esxi.example.com -datacenter=mydatacenter
  -VMTEMPDAtastore=temp_datastore -VMRESToretype=INSTANTRestore
  -datastore=mydatastore -VMSTORAGEType=VTL
```

In diesem Befehl sind der Name der virtuellen Maschine, die zurückgeschrieben werden soll, der Host und das Datencenter, die das Ziel der Zurückschreibung sind, sowie der Zurückschreibungstyp (`-VMRESToretype=INSTANTRestore`) angegeben. Die Option –

`VMSTORAGEType=VTL` gibt an, dass die Momentaufnahme (`Orion`), die von Recovery Agent bereitgestellt werden soll, sich in VTL-Speicherpools befindet. Die Option VMTEMPDAtastore ist bei Sofortzurückschreibungsoperationen ein obligatorischer Parameter.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmtagdatamover

Verwenden Sie die Option vmtagdatamover, um Tagging-Unterstützung auf dem Client für Sichern/Archivieren (Einheit zum Versetzen von Daten) zu aktivieren. Wenn diese Option aktiviert ist, verwaltet der Client Sicherungen virtueller Maschinen in VMware-Bestandsobjekten gemäß den Datenschutztags, die über das IBM Spectrum Protect vSphere-Client-Plug-in des vSphere-Web-Clients oder mithilfe von Tools wie VMware vSphere PowerCLI Version 5.5 R2 oder höher definiert werden.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Weitere Informationen zu Datenschutztags finden Sie in "Übersicht über das Datenschutztagging".

Die Einheit zum Versetzen von Daten verarbeitet Datenschutztags, wenn die Option vmtagdatamover auf yes gesetzt ist. Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

Voraussetzungen:

- Für die Einheit zum Versetzen von Daten:
  - Der VMware vCenter-Server muss über Version 6.0 Update 1 oder eine höhere Version verfügen.
  - Für das Konto, das für Sicherungs- oder Zurückschreibungsoperationen verwendet wird, sind zusätzliche Berechtigungen erforderlich. Die folgenden neuen vCenter-Berechtigungen sind für die Ausführung von Kategorie- und Tagging-Operationen erforderlich. Stellen Sie sicher, dass diese Benutzerberechtigungen auf dem Root-vCenter-Server definiert sind:

    ```
    Inventory Service > vSphere-Tagging > vSphere-Tag zuweisen oder Zuweisung aufheben
    Inventory Service > vSphere-Tagging > vSphere-Tag erstellen
    Inventory Service > vSphere-Tagging > vSphere-Tag-Kategorie erstellen
    Inventory Service > vSphere Tagging > vSphere-Tag löschen
    Inventory Service > vSphere-Tagging > vSphere-Tag-Kategorie löschen
    Inventory Service > vSphere-Tagging > Feld "Verwendet von" für Tag ändern
    Inventory Service > vSphere-Tagging > Feld "Verwendet von" für Kategorie ändern
    ```

    Weitere Informationen zum Definieren von vCenter-Berechtigungen für Sicherungs- und Zurückschreibungsoperationen finden Sie in der Technote 7047438.

- Damit die Data Protection for VMware vSphere-GUI mit Tagging-Unterstützung ordnungsgemäß funktioniert, müssen Sie sicherstellen, dass die folgenden Voraussetzungen während der Installation der GUI erfüllt sind:
  - Mindestens eine Einheit zum Versetzen von Daten und die Data Protection for VMware vSphere-GUI müssen auf demselben Server installiert werden. Dieser Knoten der Einheit zum Versetzen von Daten muss so konfiguriert werden, dass die Berechtigungsnachweise des vCenter-Servers gespeichert werden. Sie können die Berechtigungsnachweise speichern, indem der Konfigurationsassistent zum Speichern des Kennworts für den Knoten der Einheit zum Versetzen von Daten ausgeführt wird oder der Befehl dsmc set password in der Befehlszeile der Einheit zum Versetzen von Daten verwendet wird.

    Wenn Sie andere Einheiten zum Versetzen von Daten verwenden, die auf virtuellen Maschinen oder physischen Maschinen als zusätzliche Einheiten zum Versetzen von Daten ausgeführt werden, können Sie diese auf anderen Servern installieren. Für die Tagging-Unterstützung müssen alle diese Einheiten zum Versetzen von Daten auch mit der Option vmtagdatamover=yes konfiguriert werden. Diese zusätzlichen Einheiten zum Versetzen von Daten erfordern nicht die Installation der Data Protection for VMware vSphere-GUI auf demselben Server für ihre korrekte Funktionsweise als tag-basierte Einheiten zum Versetzen von Daten.

  -  LinuxFür Linux-Einheiten zum Versetzen von Daten müssen Sie das Installationsverzeichnis der Einheit zum Versetzen von Daten und die gemeinsam genutzte Java™-Bibliothek libjvm.so in der Umgebungsvariablen `LD_LIBRARY_PATH` angeben. Der Pfad zu libjvm.so wird für die Tagging-Unterstützung verwendet, wenn Sie die Option vmtagdatamover auf der Einheit zum Versetzen von Daten aktivieren. Anweisungen finden Sie in "Knoten der Einheit zum Versetzen von Daten in einer vSphere-Umgebung definieren".
  -  LinuxUnter Linux-Betriebssystemen muss die Data Protection for VMware vSphere-GUI mit dem Standardbenutzernamen (`tdpvmware`) installiert werden.
  -  LinuxAuf Knoten der Einheit zum Versetzen von Daten unter Linux muss die Standardkennwortdatei (/etc/adsm/TSM.sth) verwendet werden.

Unterstützte Clients

 LinuxDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

WindowsDiese Option kann für unterstützte Windows 64-Bit-Clients verwendet werden.

Optionsdatei

Linux-BetriebssystemeSie können diese Option in der Clientsystemoptionsdatei (dsm.sys) oder in der Befehlszeile für den Befehl backup vm angeben. Sie können diese Option auch auf dem IBM Spectrum Protect-Server in einer Clientoptionsgruppe angeben. Sie können diese Option nicht im Profileditor definieren.

Windows-BetriebssystemeSie können diese Option in der Clientoptionsdatei (dsm.opt) oder in der Befehlszeile für den Befehl backup vm angeben. Sie können diese Option auch auf dem IBM Spectrum Protect-Server in einer Clientoptionsgruppe angeben. Sie können diese Option nicht im Profileditor definieren.

Syntax

```
                    .-No--.
>>-VMTAGDATamover--+-----+--------------------------------------><
                    '-Yes-'
```

Parameter

No
: Der Client ignoriert alle Datenschutzeinstellungen oder -tags, die dem VMware-Asset zugeordnet sind. Dies ist der Standardwert.

Yes
: Der Client verwaltet Sicherungen auf der Basis der Datenschutzeinstellungen im IBM Spectrum Protect vSphere-Client-Plug-in oder auf der Basis der Tagwerte, die dem VMware-Asset zugeordnet sind.

  Wenn die Tagging-Unterstützung aktiviert ist, können einige Clientoptionen von den Datenschutzeinstellungen betroffen sein. Informationen zu den betroffenen Optionen finden Sie in "Unterstützte Datenschutztags".

  Die folgenden Beispiele zeigen, in welcher Form Clientoptionen von Datenschutztags betroffen sein können:

  - Wenn Sie mithilfe von Datenschutzeinstellungen oder -tags steuern, welche virtuellen VMware-Maschinen gesichert werden, überschneiden sich die Tagwerte möglicherweise mit der Einstellung für die Clientoption domain.vmfull. Während die Option domain.vmfull definiert, welche virtuellen Maschinen der Client schützt, überschreiben die Tags `Excluded` und `Included` den durch die Option domain.vmfull definierten Wert.
    Beispielsweise gibt die folgende Anweisung in der Optionsdatei an, welche virtuellen Maschinen bei Gesamtsicherungsoperationen für virtuelle Maschinen gesichert werden:

    ```
    DOMAIN.VMFULL VMHOSTCLUSTER=cluster01,cluster02;VM=Dept20*
    ```

    Wenn Sie Datenschutzeinstellungen oder -tags verwenden, um die virtuelle Maschine `Dept204` auszuschließen, wird die virtuelle Maschine `Dept204` nicht gesichert.
  - Die Einstellung für die Aufbewahrungsmaßnahme im IBM Spectrum Protect vSphere-Client-Plug-in oder die Tageinstellung für die Kategorie `Management Class (IBM Spectrum Protect)` setzt die Clientoptionen include.vm und vmmc außer Kraft, jedoch nicht die Option vmctlmc.

Tipp: Wenn eine Einheit zum Versetzen von Daten als die Standardeinheit zum Versetzen von Daten konfiguriert werden soll, verwenden Sie die Option Vmtagdefaultdatamover.

Beispiele

Optionsdatei:
```
vmtagdat yes
```
Befehlszeile:
```
-vmtagdat=yes
```

Zugehörige Konzepte:
Übersicht über das Datenschutztagging
Zugehörige Tasks:
Tagging-Unterstützung aktivieren
Zugehörige Verweise:
Unterstützte Datenschutztags
Vmtagdefaultdatamover
Domain.vmfull
Include.vm
Vmmc
Vmctlmc
Set vmtags
Linux-BetriebssystemeWindows-Betriebssysteme

Vmtagdefaultdatamover

Verwenden Sie die Option vmtagdefaultdatamover, um virtuelle Maschinen zu schützen, die in einem Zeitplan definiert sind und denen keine Kategorie und kein Tag `Data Mover` zugeordnet ist bzw. die keine derartige Kategorie und keinen derartigen Tag geerbt haben.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Wenn Sie den Knoten einer Einheit zum Versetzen von Daten mit der Option vmtagdefaultdatamover und der Option vmtagdatamover yes angeben, sichert die Einheit zum Versetzen von Daten alle neuen virtuellen Maschinen, die einem beliebigen Container im Datencenter hinzugefügt werden, wenn sich der Container bereits in einer Schutzgruppe befindet. Eine Schutzgruppe besteht aus den virtuellen Maschinen in einem Container, denen die Kategorie und der Tag `Schedule (IBM Spectrum Protect)` zugeordnet sind. Die Standardeinheit zum Versetzen von Daten sichert auch alle virtuellen Maschinen in der Schutzgruppe, denen nicht der Tag `Data Mover` zugeordnet ist.

Wenn mehr als eine Einheit zum Versetzen von Daten einem Zeitplan zugeordnet wird, definieren Sie eine der Einheiten zum Versetzen von Daten mithilfe der Option vmtagdefaultdatamover als die Standardeinheit zum Versetzen von Daten. Wenn nur eine einzige Einheit zum Versetzen von Daten einem Zeitplan zugeordnet wird, ordnen Sie diese Einheit zum Versetzen von Daten als die Standardeinheit zu.

Tipp: Geben Sie für jeden Zeitplan nur eine einzige Einheit zum Versetzen von Daten in der zugehörigen Liste der Einheiten zum Versetzen von Daten als die Standardeinheit an. Andernfalls werden alle neuen virtuellen Maschinen und alle virtuellen Maschinen, denen nicht der Tag `Data Mover` zugeordnet ist, mehrmals gesichert.

Datenschutztags können dem vSphere-Bestand zugeordnet werden, um den Schutz virtueller Maschinen zu steuern. Die Liste der unterstützten Kategorien und Tags finden Sie in "Unterstützte Datenschutztags".

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Einheiten zum Versetzen von Daten verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows 64-Bit-Einheiten zum Versetzen von Daten verwendet werden.

Optionsdatei

Linux-BetriebssystemeSie können diese Option in der Clientsystemoptionsdatei (dsm.sys) oder in der Befehlszeile für den Befehl backup vm angeben. Sie können diese Option auch auf dem IBM Spectrum Protect-Server in einer Clientoptionsgruppe angeben. Sie können diese Option nicht im Profileditor definieren.

Windows-BetriebssystemeSie können diese Option in der Clientoptionsdatei (dsm.opt) oder in der Befehlszeile für den Befehl backup vm angeben. Sie können diese Option auch auf dem IBM Spectrum Protect-Server in einer Clientoptionsgruppe angeben. Sie können diese Option nicht im Profileditor definieren.

Syntax

```
                          .-No----------------------------------------.
>>-VMTAGDEFAULTdatamover--+------------------------------------------+-><
                          +-Yes-----------------------------------------+
                          '-Name_der_Einheit_zum_Versetzen_von_Daten-'
```

Parameter

No
: Die lokale Einheit zum Versetzen von Daten wird nicht als die Standardeinheit zum Versetzen von Daten verwendet. Virtuelle Maschinen, denen nicht der Tag `Data Mover` zugeordnet ist, werden nicht durch diese Einheit zum Versetzen von Daten geschützt. Dies ist der Standardwert.

Yes
: Gibt an, dass die lokale Einheit zum Versetzen von Daten (die Einheit zum Versetzen von Daten, für die diese Option angegeben wird) als die Standardeinheit zum Versetzen von Daten verwendet wird.

  Sie müssen außerdem die Einheit zum Versetzen von Daten für die Tagging-Unterstützung aktivieren, indem Sie die Option vmtagdatamover yes angeben.

Name_der_Einheit_zum_Versetzen_von_Daten
: Der Name der Einheit zum Versetzen von Daten, die als die Standardeinheit zum Versetzen von Daten verwendet werden soll. Diese Option ist nur erforderlich, wenn diese Option in der Optionsdatei für die Standardeinheit zum Versetzen von Daten festgelegt werden soll. Diese Option wird für alle Einheiten zum Versetzen von Daten außer der Standardeinheit zum Versetzen von Daten ignoriert.

  Diese Option kann an alle Einheiten zum Versetzen von Daten im Zeitplanbefehl für den Server übergeben werden oder in alle Optionsdateien der Einheiten zum Versetzen eingeschlossen werden. Diese Option wird nur von der Standardeinheit zum Versetzen von Daten verwendet. Definieren Sie deshalb nur eine einzige Standardeinheit zum Versetzen von Daten.

  Sie müssen außerdem die Option vmtagdatamover yes in der Optionsdatei auf der Einheit zum Versetzen von Daten angeben, die als die Standardeinheit zum Versetzen von Daten festgelegt werden soll.

Beispiel

Ihre Windows Data Protection for VMware-Konfiguration verwendet zwei Einheiten zum Versetzen von Daten, `VC1_DC1_DM1` und `VC1_DC1_DM2`. Um die Einheit zum Versetzen von Daten mit dem Namen `VC1_DC1_DM1` als die Standardeinheit zum Versetzen von Daten festzulegen, führen Sie die folgenden Schritte aus:

1. Fügen Sie in der Optionsdatei für die Einheit zum Versetzen von Daten mit dem Namen `VC1_DC1_DM1` (dsm.VC1_DC1_DM1.opt) die folgenden Anweisungen hinzu:

   ```
   vmtagdatamover yes
   vmtagdefaultdatamover yes
   ```

   oder

   ```
   vmtagdatamover yes
   vmtagdefaultdatamover VC1_DC1_DM1
   ```

2. Fügen Sie in der Optionsdatei für die Einheit zum Versetzen von Daten mit dem Namen `VC1_DC1_DM2` (dsm.VC1_DC1_DM2.opt) die folgenden Anweisungen hinzu:

   ```
   vmtagdatamover yes
   vmtagdefaultdatamover VC1_DC1_DM1
   ```

Die Option vmtagdefaultdatamover kann auch an eine Zeitplandefinition oder einen Befehl übergeben werden, um die Standardeinheit zum Versetzen von Daten zuzuordnen. Wenn die Standardeinheit zum Versetzen von Daten in der Zeitplandefinition definiert wird, können alle Einheiten zum Versetzen von Daten, die dem Zeitplan zugeordnet sind, die Standardeinheit zum Versetzen von Daten für die Schutzgruppe identifizieren.

Beispiel: `dsmc backup vm -vmtagdefaultdatamover=VC1_DC1_DM1`

Zugehörige Tasks:
Tagging-Unterstützung aktivieren
Zugehörige Verweise:
Domain.vmfull
Vmtagdatamover
Set vmtags
Windows-Betriebssysteme

Vmtempdatastore

Verwenden Sie die Option vmtempdatastore mit dem Befehl restore VM, um einen temporären Datenspeicher auf dem ESX-Host für eine Sofortzurückschreibungsoperation zu definieren.

Der mit der Option vmtempdatastore erstellte Datenspeicher wird zur temporären Speicherung der Konfiguration der virtuellen Maschine (VM) verwendet, die während der Zurückschreibungsverarbeitung erstellt wird. Diese Option ist bei Sofortzurückschreibungsoperationen (-vmrestoretype=instantrestore) erforderlich.

Diese Option ist nur für virtuelle VMware-Maschinen gültig. Die virtuellen Maschinen müssen auf Servern mit VMware ESXi 5.1 oder höher gehostet werden. Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Unterstützte Clients

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) oder in die Befehlszeile ein.

Syntax

```
>>-VMTEMPDAtastore-- --Datenspeichername----------------------><
```

Parameter

Datenspeichername
: Geben Sie den Namen eines vorhandenen Datenspeichers auf dem ESX-Host an. Der temporäre Datenspeicher darf nicht mit dem ursprünglichen Datenspeicher oder dem durch die Option datastore angegebenen Datenspeicher identisch sein. Der von Ihnen angegebene Datenspeicher muss ein VMFS-Datenspeicher sein.

Beispiele

Optionsdatei:

```
VMTEMPDAtastore Verify_Datastore
```

Befehlszeile:

```
dsmc restore vm Oslo -VMRESToretype=INSTANTAccess
-vmname=Oslo_instant_restored -VMTEMPDAtastore=Temporary_Datastore
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmverifyifaction

Mit dieser Option können Sie die Aktion angeben, die ausgeführt werden soll, wenn die Einheit zum Versetzen von Daten Integritätsprobleme mit den jüngsten CTL- und Bitmapdateien für eine virtuelle Maschine erkennt.

Diese Option wirkt sich nur dann auf die Sicherungsverarbeitung für eine VM-Gastmaschine aus, wenn alle der folgenden Bedingungen vorliegen:

- Die vorherige Sicherungsoperation für die VM-Gastmaschine war eine immer inkrementelle Teilsicherung (`mode=ifincremental`).
- Die aktuelle Sicherungsoperation für die VM-Gastmaschine ist eine immer inkrementelle Teilsicherung.
- Die Einheit zum Versetzen von Daten erkennt ein Integritätsproblem mit den CTL- und Bitmapdaten der vorherigen immer inkrementellen Teilsicherungsoperation.
- Für die Option vmverifyiflatest ist `yes` definiert.

Wenn nicht alle diese Bedingungen für eine virtuelle Maschine zutreffen, findet die Sicherung wie gewohnt statt und die durch diese Option angegebene Aktion wird nicht eingeleitet.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

 LinuxBetriebssystemeDiese Option ist für Linux-Clients gültig, die als Einheit zum Versetzen von Daten für Sicherungen von VMware-Gastmaschinen fungieren.

 WindowsBetriebssystemeDiese Option ist für Windows-Clients gültig, die als Einheit zum Versetzen von Daten für Sicherungen von VMware-Gastmaschinen fungieren.

Optionsdatei

 WindowsBetriebssystemeDefinieren Sie diese Option in der Clientoptionsdatei (dsm.opt).

 LinuxBetriebssystemeDefinieren Sie diese Option in der Clientoptionsdatei (dsm.opt) oder in der Clientsystemoptionsdatei (dsm.sys).

Diese Option kann auch in einer Clientoptionsgruppe, als Parameter in einem Befehl backup vm oder im Parameter options in einer Zeitplandefinition angegeben werden.

Syntax

```
                    .-FAILbackup-.
>>-VMVERIFYIFAction--+------------+----------------------------><
                    +-FORCEfull--+
                    '-PREview----'
```

Parameter

FAILbackup

Diese Aktion lässt die Sicherungsoperation fehlschlagen. Die folgenden Nachrichten werden in die Fehlerprotokolldatei der Einheit zum Versetzen von Daten (dsmerror.log) geschrieben:

```
ANS9921E Für die Platte der virtuellen Maschine VM-Name (Plattenkennsatz)
ist die Prüfung fehlgeschlagen (xxx/yyy).
```

xxx/yyy in der Nachricht gibt die Größe der Bitmapdateien (xxx) und der CTL-Dateien (yyy) an.

```
ANS9919E Erwartete Steuerdateien für VM-Name wurden nicht gefunden.
```

Führen Sie eine VM-Gesamtsicherung (`-mode=IFFull`) für die betroffenen virtuellen Maschinen zu einem beliebigen Zeitpunkt aus. Eine Alternative ist die Verwendung von `-vmverifyifaction=forcefull` bei der nächsten geplanten immer inkrementellen

Teilsicherungsoperation, um eine Gesamtsicherung dieser virtuellen Maschinen zu erzwingen, falls Sie feststellen, dass Ihr Fenster für die geplante Sicherung die VM-Gesamtsicherungen für diese virtuellen Maschinen aufnehmen kann. Dieser Wert ist der Standardaktionswert.

FORCEfull
Durch diese Aktion wird der Sicherungsmodus `-mode=ifincremental` durch `-mode=iffull` ersetzt; die aktuelle Sicherung wird zu einer VM-Gesamtsicherung. Die VM-Gesamtsicherung wird für Sie eingeleitet. Die folgenden Nachrichten werden in die Fehlerprotokolldatei der Einheit zum Versetzen von Daten (dsmerror.log) geschrieben:

```
ANS9921E Für die Platte der virtuellen Maschine VM-Name (Plattenkennsatz)
ist die Prüfung fehlgeschlagen (xxx/yyy).
```

xxx/yyy in der Nachricht gibt die Größe der Bitmapdateien (xxx) und der CTL-Dateien (yyy) an.

```
ANS9919E Erwartete Steuerdateien für VM-Name wurden nicht gefunden.
```

```
ANS9922I VMVERIFYIFlatest ist für VM-Name aktiviert (Aktion: FORCEFULL).
```

```
ANS9920W Für VM-Name wird eine VM-Gesamtsicherung erzwungen.
```

Verwenden Sie diese Option, wenn Ihr aktuelles Fenster zum Durchführen von Sicherungen eine VM-Gesamtsicherung der betroffenen virtuellen Maschinen aufnehmen kann.

PREview
Diese Aktion führt keine Sicherungen aus. Stattdessen werden die CTL- und Bitmapdaten jeder VM-Gastmaschine, die der Befehl backup vm verarbeitet, in ein temporäres Verzeichnis zurückgeschrieben, wo sie auf Integrität überprüft werden. Wenn die Integritätsprüfung fehlschlägt, werden die folgenden Nachrichten in die Fehlerprotokolldatei der Einheit zum Versetzen von Daten (dsmerror.log) geschrieben:

```
ANS9921E Für die Platte der virtuellen Maschine VM-Name (Plattenkennsatz)
ist die Prüfung fehlgeschlagen (xxx/yyy).
```

xxx/yyy in der Nachricht gibt die Größe der Bitmapdateien (xxx) und der CTL-Dateien (yyy) an.

```
ANS9919E Erwartete Steuerdateien für VM-Name wurden nicht gefunden.
```

```
ANS9922I VMVERIFYIFlatest ist für VM-Name aktiviert (Aktion: PREVIEW).
```

Mit dieser Option können Sie die Integrität der immer inkrementellen Teilsicherungen (`-mode=ifincremental`) überprüfen, die Sie bereits für mindestens eine virtuelle Maschine erstellt haben.

Wenn die Nachrichten anzeigen, dass einige der virtuellen Maschinen die Integritätsprüfungen nicht bestanden haben, starten Sie eine VM-Gesamtsicherung (`-mode=iffull`) zu einem beliebigen Zeitpunkt. Sie können auch `-vmverifyifaction=forcefull` bei der nächsten geplanten immer inkrementellen Teilsicherungsoperation angeben, um eine Gesamtsicherung dieser virtuellen Maschinen zu erzwingen. Das Fenster zum Durchführen von Sicherungen muss so groß sein, dass es mindestens eine VM-Gesamtsicherung aufnehmen kann.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmverifyiflatest

Diese Option ist nur für Sicherungsoperationen von virtuellen VMware-Maschinen gültig, die im Modus der immer inkrementellen Teilsicherung ausgeführt werden (d. h. ein Befehl backup vm mit der Angabe -mode=IFIncremental). Wenn die Option vmverifyiflatest aktiviert ist, führt die Einheit zum Versetzen von Daten eine Integritätsprüfung der CTL- und Bitmapdateien durch, die während der letzten Sicherung auf dem Server erstellt wurden, falls die letzte Sicherung eine immer inkrementelle Teilsicherung war.

Wenn die Dateien die Integritätsprüfungen bestehen, kann die virtuelle Maschine zurückgeschrieben werden. Die aktuelle Sicherung wird fortgesetzt und fügt der Momentaufnahmekette für die virtuelle Maschine eine weitere Momentaufnahme hinzu.

Wenn die Dateien die Integritätsprüfungen nicht bestehen, kann die virtuelle Maschine nicht zurückgeschrieben werden. Die Einheit zum Versetzen von Daten führt dann eine andere Aktion durch, die Sie mit der Option vmverifyifaction angegeben haben. Sie können mit vmverifyifaction angeben, dass sofort eine VM-Gesamtsicherung erstellt wird, oder Sie können die Sicherung vollständig fehlschlagen lassen und eine VM-Gesamtsicherung zu einem anderen Zeitpunkt ausführen. Mit einem dritten Parameter kann angegeben werden, dass die CTL- und Bitmapdateien für eine virtuelle Maschine lediglich überprüft werden, ohne dass eine neue Sicherungsmomentaufnahme erstellt wird.

Die Überprüfung kann nur ausgeführt werden, wenn bei der vorherigen Sicherungsoperation für die virtuelle Maschine `mode=IFIncr` angegeben wurde und wenn bei der aktuellen Sicherungsoperation auch `mode=IFIncr` verwendet wird. Diese Option hat keinen Einfluss auf die anderen Sicherungsmodi für virtuelle Maschinen.

Wichtig:
Wird für diese Option `no` angegeben, wird die Sicherungsverarbeitung der virtuellen Maschinen ohne Prüftests fortgesetzt. Die Verarbeitungsressourcen, die an der Ausführung der Integritätsprüfungen beteiligt sind, sind unerheblich. Um eine fortlaufende Integrität Ihrer immer inkrementellen Teilsicherungskette zu gewährleisten, verwenden Sie den Standardwert (vmverifyiflatest yes). Geben Sie für diese Option nur dann `no` an, wenn Sie eine entsprechende Anweisung durch IBM® Support erhalten.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Unterstützte Clients

 Diese Option ist für Linux-Clients gültig, die als Einheit zum Versetzen von Daten für Sicherungen von VMware-Gastmaschinen fungieren.

 Diese Option ist für Windows-Clients gültig, die als Einheit zum Versetzen von Daten für Sicherungen von VMware-Gastmaschinen fungieren.

Optionsdatei

 Definieren Sie diese Option in der Clientoptionsdatei (dsm.opt).

 Definieren Sie diese Option in der Clientoptionsdatei (dsm.opt) oder in der Clientsystemoptionsdatei (dsm.sys).

Diese Option kann auch in einer Clientoptionsgruppe, als Parameter in einem Befehl backup vm oder im Parameter options in einer Zeitplandefinition angegeben werden.

Syntax

```
                      .-YES-.
>>-VMVERIFYIFlatest--+-----+-----------------------------------><
                      '-NO--'
```

Parameter

YES
: Diese Einstellung gibt an, dass die Überprüfung der CTL- und Bitmapdaten für jede virtuelle Maschine ausgeführt wird, die bei der aktuellen immer inkrementellen Teilsicherungsoperation (mode=IFIncr) verarbeitet wird, wenn die vorherige Sicherungsoperation dieser virtuellen Maschine auch eine immer inkrementelle Teilsicherung war. Dies ist der Standardwert.

NO
: Diese Einstellung gibt an, dass keine Überprüfung der CTL- und Bitmapdaten während der immer inkrementellen Teilsicherungsverarbeitung stattfindet. Geben Sie diesen Wert nur an, wenn Sie eine entsprechende Anweisung durch IBM Support erhalten.

Beispiele

Optionsdatei:

```
vmverifyiflatest yes
```

Befehlszeile:

```
dsmc backup vm vm1 -mode=ifincremental -vmverifyiflatest=yes
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Vmvstortransport

Die Option vmvstortransport gibt die bevorzugte Transportreihenfolge (Hierarchie) an, die beim Sichern oder Zurückschreiben von virtuellen VMware-Maschinen verwendet werden soll. Wenn Sie einen bestimmten Transport mit dieser Option nicht einschließen, wird dieser Transport ausgeschlossen und nicht für die Übertragung von Daten verwendet.

Die von Ihnen angegebene Transportreihenfolge bestimmt, wie die VMware API for Data Protection (VADP) auf Daten virtueller Platten zugreift, aber sie hat keinen Einfluss auf den Datenpfad, der zwischen dem Client für Sichern/Archivieren und dem IBM Spectrum Protect-Server verwendet wird. Zu den gültigen Transportmethoden gehören die folgenden Optionen in beliebiger Reihenfolge oder Kombination:

nbd
: Netzbasierte Datenübertragung (Network based data transfer). Der Zugriff auf virtuelle Plattendaten erfolgt über das LAN. Dieser Transportpfad ist normalerweise in allen Konfigurationen verfügbar.

nbdssl
: Entspricht nbd, die Daten werden jedoch verschlüsselt, bevor sie über das LAN versendet werden. Die Verschlüsselung kann die Leistung beeinträchtigen.

san
: Storage Area Network-Übertragung: Der Zugriff auf virtuelle Plattendaten erfolgt über das SAN (Speicherbereichsnetz).

hotadd
: Wenn Sie den Client für Sichern/Archivieren in einer virtuellen Maschine verwenden, gestattet der Hot-Add-Transport den Transport gesicherter Daten in dynamisch hinzugefügten Speicher.

Trennen Sie die einzelnen Transportoptionen jeweils durch einen Doppelpunkt voneinander. Zum Beispiel: san:nbd:nbdssl:hotadd.

Wenn Sie keine Transporthierarchie angeben, lautet die Standardauswahlreihenfolge für den Transport san:hotadd:nbdssl:nbd.

Die erste verfügbare Transportmethode wird für die Datenübertragung verwendet. Wenn Sie den Datentransport über einen bestimmten Pfad verhindern wollen, darf er in der Transportliste nicht angegeben werden. Wenn es beispielsweise wichtig ist, den LAN-Verkehr nicht zu unterbrechen, lassen Sie die nbd-Transportmethoden in der Hierarchie weg.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Linux-BetriebssystemeDefinieren Sie diese Option in der Datei dsm.sys.

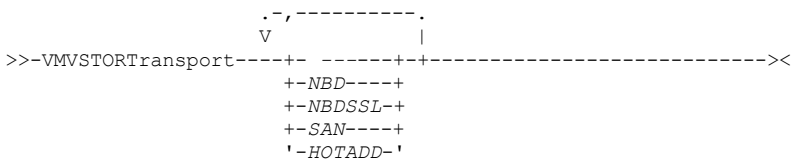
Windows-BetriebssystemeDefinieren Sie diese Option in der Clientoptionsdatei (dsm.opt).

Unterstützte Clients

Windows-BetriebssystemeDiese Option ist für Windows-Clients gültig, die für die Sicherung oder Zurückschreibung von Dateien virtueller Maschinen mithilfe von VADP konfiguriert sind.

Linux-BetriebssystemeDiese Option ist für Linux-Clients gültig, die für die Sicherung oder Zurückschreibung von Dateien virtueller Maschinen mithilfe von VADP konfiguriert sind.

Syntax



Beispiele

Keine Sicherungen oder Zurückschreibungen über das LAN transportieren, wenn das SAN verfügbar ist
VMVSTORTRANSPORT san
Der Client für Sichern/Archivieren wird auf einer virtuellen Maschine ausgeführt, den Hot-Add-Transport jedoch nicht verwenden
VMVSTORTRANSPORT nbdssl:nbd
LAN-Transport verwenden, auch wenn nbdssl verfügbar ist, um eine bessere Leistung zu erzielen
VMVSTORTRANSPORT nbd
Der SAN-Transport wird bevorzugt, aber nbd verwenden, wenn das SAN nicht verfügbar ist, und nicht nbdssl oder hotadd verwenden
VMVSTORTRANSPORT san:nbd

Windows-Betriebssysteme

Vssaltstagingdir

Die Option vssaltstagingdir gibt den vollständig qualifizierten Pfad an, der den Systemausschlusscache und temporäre Daten für VSS-Momentaufnahmeoperationen enthält.

Der Client für Sichern/Archivieren ermittelt den Pfad für temporäre VSS-Dateien anhand der folgenden priorisierten Auswahlmöglichkeiten:

1. Die Option vssaltstagingdir ist in der Datei dsm.opt definiert.
2. Das Verzeichnis c:\adsm.sys ist vorhanden und nicht leer.
3. Wurde die Option vssaltstagingdir nicht definiert und ist das Verzeichnis c:\adsm.sys nicht vorhanden, erhält der Client den Pfad aus einem Registerschlüssel. Der Pfad für temporäre VSS-Dateien ist der Wert von DefaultVssStagingDir und wird mit dem Wert von Path unter dem Schlüssel HKLM\SOFTWARE\IBM\ADSM\CurrentVersion\BackupClient generiert. Nach der Erstellung des Werts für DefaultVssStagingDir wird der Wert nicht geändert, wenn der Client an einer neuen Position erneut installiert wird.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
>>-VSSALTSTAGINGDIR--Dateipfad--------------------------------><
```

Parameter

Dateipfad
: Geben Sie den vollständig qualifizierten Pfad für temporäre Dateien an, die sich auf VSS-Momentaufnahmeoperationen beziehen. Ist ein Bestandteil des Pfads nicht vorhanden, versucht der Client für Sichern/Archivieren, ihn zu erstellen. Der Standardwert ist das Clientinstallationsverzeichnis.

  Im UNC-Format (Universal Naming Convention) muss der Pfad einen Laufwerkbuchstaben enthalten. In dem folgenden Beispiel für das UNC-Format enthält der Pfad den Laufwerkbuchstaben D$: \\computer7\D$\temp\snapshot.

Beispiele

Optionsdatei:

```
vssaltstagingdir "c:\Users\All Users\Tivoli\adsm.sys"
```

Befehlszeile:

```
-vssaltstagingdir ="c:\Users\All Users\Tivoli\adsm.sys"
```

Die Option ist nur in der Anfangsbefehlszeile gültig. Sie ist nicht im interaktiven Modus gültig.

 Windows-Betriebssysteme

Vssusesystemprovider

Die Option vssusesystemprovider gibt an, ob der Windows-Systemprovider verwendet wird oder ob Windows den am besten geeigneten Provider auswählt.

Verwenden Sie die Option vssusesystemprovider für Operationen des Microsoft Windows Volume Shadow Copy Service (VSS), beispielsweise Systemstatussicherung oder IBM Spectrum Protect for Copy Services-Sicherungen.

Unterstützte Clients

Diese Option ist für alle Windows-Clients gültig. Diese Option kann auch auf dem Server definiert werden. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein.

Syntax

```
                          .-No--.
>>-VSSUSESYSTEMProvider--+-----+-------------------------------><
                          '-Yes-'
```

Parameter

Yes
: Gibt an, dass der Microsoft Windows-VSS-Systemprovider verwendet wird.

No
: Gibt an, dass der Standardsystemprovider verwendet wird. Dieser Provider kann mit dem Systemprovider identisch sein, je nachdem, welche anderen Provider auf dem System installiert sind. Verwenden Sie no, wenn Sie den Standardsystemprovider verwenden wollen und der Standardsystemprovider nicht der Microsoft Windows-VSS-Provider ist. No ist der Standardwert.

Beispiele

Optionsdatei:

```
vssusesystemprovider yes
```

Befehlszeile:

Nicht zutreffend.

Linux-Betriebssysteme Windows-Betriebssysteme

Vmtimeout

VMTIMEOut gibt die maximale Wartezeit in Sekunden an, bevor eine VM-Sicherungsoperation (backup vm) abgebrochen wird, wenn die Option INCLUDE.VMTSMVSS für die Bereitstellung von Anwendungsschutz verwendet wird. Um diese Option verwenden zu können, muss die IBM Spectrum Protect for Virtual Environments-Lizenz installiert sein.

Für jede VM-Sicherungsoperation (backup vm), die auf einer virtuellen Maschine ausgeführt wird, die durch eine Option INCLUDE.VMTSMVSS geschützt wird, gibt es einen Zeitgeber. Der Zeitgeberwert legt fest, wie lange der Client warten soll, bis die Anwendung die Aktivität in den Wartemodus versetzt und ihre Protokolle abgeschnitten hat, so dass die Sicherung ausgeführt werden kann. Der Standardzeitlimitüberschreitungswert ist in den meisten Umgebungen ausreichend. Wenn Ihre Anwendungsdaten jedoch nicht gesichert werden können, weil die Anwendung mehr Zeit für die Vorbereitung der Momentaufnahme benötigt, können Sie den Zeitlimitüberschreitungswerts erhöhen. Dieser Zeitgeber ist nur für VM-Sicherungsoperationen (backup vm) gültig, wenn die Option INCLUDE.VMTSMVSS für eine virtuelle Maschine definiert ist.

Unterstützte Clients

Linux-BetriebssystemeDiese Option kann für unterstützte Linux x86_64-Clients verwendet werden.

Windows-BetriebssystemeDiese Option kann für unterstützte Windows-Clients verwendet werden.

Optionsdatei

Fügen Sie diese Option in die Clientoptionsdatei ein. Sie kann nicht in der Befehlszeile oder im Profileditor definiert werden.

Syntax

```
              .-180---------------.
>>-VMTIMEout--+-+---------------+-+---------------------------><
                '-Zeitlimitwert-'
```

Parameter

Zeitlimitwert
: Gibt die für die Ausführung von Sicherungsoperationen zulässige Zeit in Sekunden an, wenn eine virtuelle Maschine durch die Anwendungsschutzoption INCLUDE.VMTSMVSS geschützt ist. Der angegebene Wert muss eine ganze Zahl zwischen 180 und 500 sein. Der Standardwert ist 180 Sekunden.

Beispiele

Optionsdatei
: VMTIMEout 500

Befehlszeile:
: Nicht gültig. Diese Option kann nicht in der Befehlszeile angegeben werden.

Zugehörige Verweise:
INCLUDE.VMTSMVSS

Webports

Die Option webports ermöglicht die Verwendung des Web-Clients außerhalb einer Firewall.

Die Option webports ermöglicht die Verwendung des Web-Clients außerhalb einer Firewall, indem sie die TCP/IP-Anschlussnummer angibt, die der IBM Spectrum Protect-Clientakzeptorservice und der Web-Client-Agentenservice für die Kommunikation mit dem Web-Client verwenden.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeSowohl für den Clientakzeptor als auch für den Web-Client-Agentenservice sind Werte erforderlich.

Windows-BetriebssystemeSowohl für den Clientakzeptorservice als auch für den Web-Client-Agentenservice sind Werte erforderlich.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWenn Sie diese Option nicht angeben, wird der Standardwert 0 für beide Anschlüsse verwendet. Dies bewirkt, dass TCP/IP wahlfrei eine freie Anschlussnummer für den Clientakzeptor und den Web-Client-Agentenservice zuordnet.

Windows-BetriebssystemeWenn Sie diese Option nicht angeben, wird der Standardwert 0 für beide Anschlüsse verwendet. Dies bewirkt, dass TCP/IP wahlfrei eine freie Anschlussnummer für den Clientakzeptorservice und den Web-Client-Agentenservice zuordnet.

Unterstützte Clients

Diese Option ist für alle Clients gültig. Die IBM Spectrum Protect-API unterstützt diese Option nicht.

Optionsdatei

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssystemeFügen Sie diese Option in die Datei dsm.sys innerhalb einer Serverzeilengruppe ein. Um diese Option im Profileditor des Clients zu definieren, klicken Sie auf Editieren > Clientvorgaben > Web-Client und geben Sie die Anschlüsse in den Feldern Webagentenanschluss und Web-Clientakzeptoranschluss an.

Windows-BetriebssystemeFügen Sie diese Option in die Clientoptionsdatei (dsm.opt) ein. Um diese Option im Profileditor des Clients zu definieren, klicken Sie auf Editieren > Clientvorgaben > Web-Client und geben Sie die Anschlüsse in den Feldern Webagentenanschluss und Web-Clientakzeptoranschluss an.

Syntax

```
>>-WEBPorts-- --CAD-Anschluss-- --Agentenanschluss-------------><
```

Parameter

AIX-BetriebssysemeLinux-BetriebssysemeMac OS X-BetriebssysemeOracle Solaris-BetriebssystemeCAD-Anschluss
AIX-BetriebssysemeLinux-BetriebssysemeMac OS X-BetriebssysemeOracle Solaris-BetriebssystemeGibt die erforderliche Anschlussnummer für den Clientakzeptor an. Der Wertebereich ist 1000 bis 32767. Wird kein Wert angegeben, bewirkt der Standardwert Null (0), dass TCP/IP wahlfrei eine freie Anschlussnummer zuordnet.

Windows-BetriebssystemeCAD-Anschluss
Windows-BetriebssystemeGibt die erforderliche Anschlussnummer für den Clientakzeptorservice an. Der Wertebereich ist 1000 bis 32767. Wird kein Wert angegeben, bewirkt der Standardwert Null (0), dass TCP/IP wahlfrei eine freie Anschlussnummer zuordnet.

Agentenanschluss
Gibt die erforderliche Anschlussnummer für den Web-Client-Agentenservice an. Der Wertebereich ist 1000 bis 32767. Wird kein Wert angegeben, bewirkt der Standardwert Null (0), dass TCP/IP wahlfrei eine freie Anschlussnummer zuordnet.

Beispiele

Optionsdatei:

```
webports 2123 2124
```

Befehlszeile:

Windows-Betriebssysteme

```
webports 2123, 2124
```

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssystemeNicht zutreffend.

Wildcardsareliteral

Die Option wildcardsareliteral gibt an, ob Fragezeichen (?) und Sterne (*) in der eigentlichen Bedeutung interpretiert werden, wenn sie in einer Dateilistenspezifikation in einer Option filelist angegeben werden.

Normalerweise akzeptiert der Client keine Platzhalterzeichen (? und *) in einer Dateilistenspezifikation, die in einer Option filelist enthalten ist. In einigen Dateisystemen sind Hochkommas oder Anführungszeichen in Datei- und Verzeichnisnamen zulässig.Um Fehler zu verhindern, die auftreten, wenn in einer Option filelist Dateispezifikationen angegeben werden, die Platzhalterzeichen enthalten, definieren Sie `wildcardsareliteral yes`. Wenn wildcardsareliteral auf yes gesetzt ist, werden Fragezeichen (?) und Sterne (*), die in einer Dateilistenspezifikation in der Option filelist enthalten sind, in der eigentlichen Bedeutung und nicht als Platzhalterzeichen interpretiert.

Diese Option ist für jeden Befehl gültig, der eine Option filelist als Befehlsparameter akzeptiert.

Unterstützte Clients

Diese Option ist für alle unterstützten Plattformen gültig. Die Option wird auf jeden Befehl angewendet, der eine Dateilistenspezifikation als Parameter akzeptiert.

Optionsdatei

Fügen Sie diese Option in die Clientbenutzeroptionsdatei (dsm.opt) ein.

Syntax

```
                          .-no------.
>>-WILDCARDSareliteral--+-+-----+-+---------------------------><
                          '-yes-'
```

Parameter

no
: Gibt an, dass Fragezeichen und Sterne als Platzhalterzeichen interpretiert werden, wenn sie in einer Dateilistenspezifikation verwendet werden, die in einer Option filelist enthalten ist. No ist der Standardwert.Wenn eine Dateilistenspezifikation in einer Option filelist ein Fragezeichen oder einen Stern enthält, tritt ein Fehler auf und die Dateispezifikation kann nicht verarbeitet werden.

yes
: Gibt an, dass Sterne und Fragezeichen in einer Dateilistenspezifikation, die in einer Option filelist enthalten ist, in der eigentlichen Bedeutung und nicht als Platzhalterzeichen interpretiert werden. Geben Sie diesen Wert an, wenn Sie Dateien aus einem Dateisystem sichern, in dem Platzhalterzeichen in Datei- oder Verzeichnisnamen zulässig sind.

Beispiele

Optionsdatei:

```
WILDCARDSARELITERAL YES
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeBei den folgenden Beispielen wird vorausgesetzt, dass das Dateisystem Platzhalterzeichen in Pfadangaben zulässt. Die Beispiele zeigen Dateien in einer Dateilistenspezifikation, die erfolgreich verarbeitet werden können, wenn WILDCARDSARELITERAL auf YES gesetzt wird.

Windows-BetriebssystemeAngenommen, der ausgegebene Befehl lautet `dsmc sel -filelist=c:\important_files.txt`, wobei important_files.txt die Liste der zu verarbeitenden Dateien enthält.

Windows-Betriebssystemeimportant_files.txt enthält die folgende Dateiliste:

```
c:\home\myfiles\file?9000
c:\home\myfiles\?file
c:\home\myfiles\**README**version2
c:\home\myfiles\ABC?file*
```

Windows-BetriebssystemeWenn sowohl WILDCARDSARELITERAL als auch QUOTESARELITERAL auf YES gesetzt ist, können folgende Sicherungen erfolgreich verarbeitet werden:

```
c:\home\myfiles\"file?
c:\home\myfiles\?file'
c:\home\myfiles\**"README Tomorrow"**
c:\home\myfiles\file*
```

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeBefehlszeile:

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeBei den folgenden Beispielen wird vorausgesetzt, dass das Dateisystem Platzhalterzeichen in Pfadangaben zulässt. Die Beispiele zeigen Dateien in einer Dateilistenspezifikation, die erfolgreich verarbeitet werden können, wenn WILDCARDSARELITERAL auf YES gesetzt wird.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeDer ausgegebene Befehl ist `dsmc sel -filelist=/home/user1/important_files`, wobei important_files die Liste der zu verarbeitenden Dateien enthält.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssystemeimportant_files.txt enthält die folgende Dateiliste:

```
/home/user1/myfiles/file?9000
/home/user1/myfiles/?file
/home/user1/myfiles/**README**version2
/home/user1/myfiles/ABC?file*
```

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeWenn sowohl WILDCARDSARELITERAL als auch QUOTESARELITERAL auf YES gesetzt ist, können folgende Sicherungen erfolgreich verarbeitet werden:

```
/home/user1/myfiles/"file?
/home/user1/myfiles/?file'
/home/user1/myfiles/**"README Tomorrow"**
/home/user1/myfiles/file*
```

Befehle verwenden

Der Client für Sichern/Archivieren verfügt über eine Befehlszeilenschnittstelle, die Sie alternativ zur grafischen Benutzerschnittstelle verwenden können. Dieser Abschnitt enthält Informationen zum Starten und Beenden einer Clientbefehlssitzung und Anweisungen zur Eingabe von Befehlen.

- Clientbefehlssitzung starten und beenden
- Clientbefehle, Optionen und Parameter eingeben
- Platzhalterzeichen

Die folgende Tabelle stellt eine alphabetische Liste der Befehle und eine Kurzbeschreibung bereit.

Tabelle 1. Befehle

Befehl	Beschreibung
archive	Archiviert Dateien von einer Workstation in den IBM Spectrum Protect-Speicher.
Windows-Betriebssystemearchive fastback	Windows-BetriebssystemeArchiviert durch die Optionen fbpolicyname, fbclientname und fbvolumename angegebene Datenträger für die langfristige Aufbewahrung.
Linux-Betriebssysteme Windows-Betriebssystemebackup fastback	Linux-BetriebssystemeWindows-BetriebssystemeSichert durch die Optionen fbpolicyname, fbclientname und fbvolumename angegebene Datenträger für die langfristige Aufbewahrung.
backup group	Erstellt eine Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen enthält, und sichert sie in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemebackup image	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeErstellt eine Imagesicherung der von Ihnen angegebenen Dateisysteme oder logischen Datenträger.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemebackup nas	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeErstellt eine Imagesicherung eines oder mehrerer Dateisysteme, die zu einem NAS-Dateiserver gehören.
Windows-Betriebssystemebackup systemstate	Windows-BetriebssystemeSichert alle startfähigen Systemstatus- und Systemservicekomponenten als ein Objekt, um eine konsistente zeitpunktgesteuerte Momentaufnahme des Systemstatus zur Verfügung zu stellen. Dieser Befehl ist für jeden unterstützten Windows-Client gültig.
Linux-Betriebssysteme Windows-Betriebssystemebackup vm	Linux-BetriebssystemeWindows-BetriebssystemeSichert virtuelle Maschinen, die in der Option vmlist angegeben sind.
AIX-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemecancel process	AIX-BetriebssystemeOracle Solaris-Betriebssysteme Windows-Betriebssysteme (Falls NDMP-Unterstützung aktiviert ist:) Zeigt eine Liste der aktuellen Prozesse für NAS-Imagesicherung und -zurückschreibung an, für die der Benutzer mit Verwaltungsaufgaben berechtigt ist.
cancel restore	Zeigt eine Liste der wiederanlauffähigen Zurückschreibungssitzungen an, aus der Sie eine zum Abbrechen auswählen können.
delete access	Löscht Berechtigungsregeln für Dateien, die auf dem Server gespeichert sind. AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeAuf den Clients, die Imagesicherung unterstützen, löscht dieser Befehl die Berechtigungsregeln für Images, die auf dem Server gespeichert sind.
delete archive	Löscht archivierte Dateien aus dem IBM Spectrum Protect-Serverspeicher.
delete backup	Löscht aktive und inaktive Sicherungsdateien aus dem IBM Spectrum Protect-Serverspeicher.
delete filespace	Löscht Dateibereiche aus dem IBM Spectrum Protect-Serverspeicher.
delete group	Löscht eine Gruppensicherung auf dem IBM Spectrum Protect-Server.
expire	Inaktiviert die Sicherungsobjekte, die Sie in der Dateispezifikation oder mit der Option filelist angeben.
help	Zeigt ein Inhaltsverzeichnis der Hilfethemen für den Befehlszeilenclient an.
incremental	Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssysteMac OS X-Betriebssysteme Windows-BetriebssystemeSichert alle neuen oder geänderten Dateien oder Verzeichnisse in der Standardclientdomäne oder in von Ihnen angegebenen Dateisystemen, Verzeichnissen oder Dateien, sofern Sie sie nicht von den Sicherungsservices ausschließen.
loop	Startet eine interaktive Befehlssitzung.
macro	Führt Befehle innerhalb einer Makrodatei aus, die Sie angeben.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystememonitor process	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeZeigt eine Liste der aktuellen NAS-Imagesicherungs- und -zurückschreibungsprozesse an, in der Sie einen Prozess auswählen können, der abgebrochen werden soll.
preview archive	Simuliert einen Archivierungsbefehl, ohne Daten an den Server zu senden.
preview backup	Simuliert einen Sicherungsbefehl, ohne Daten an den Server zu senden.

Befehl	Beschreibung
query access	Zeigt eine Liste der aktuellen Berechtigungsregeln an.
Windows-Betriebssystemequery adobjects	Windows-BetriebssystemeZeigt eine Liste der aktuellen Berechtigungsregeln an.
query archive	Zeigt eine Liste der archivierten Dateien an.
query backup	Zeigt eine Liste der Sicherungsversionen an.
query backupset	Fragt einen Sicherungssatz von einer lokalen Datei oder vom IBM Spectrum Protect-Server ab. Auf den Clients, die Bandeinheiten unterstützen, kann dieser Befehl einen Sicherungssatz von einer Bandeinheit abfragen.
query filespace	Zeigt eine Liste der Dateibereiche im IBM Spectrum Protect-Speicher an. Sie können auch einen einzelnen Dateibereich für die Abfrage angeben.
query group	Zeigt Informationen zu Gruppensicherungen und ihren Members an.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemequery image	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeZeigt Informationen zu Imagesicherungen an.
query inclexcl	Zeigt eine Liste der Einschluss-/Ausschlussanweisungen in der Reihenfolge an, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden.
query mgmtclass	Zeigt Informationen zu verfügbaren Verwaltungsklassen an.
query node	Zeigt alle Knoten an, für die eine Verwaltungsbenutzer-ID die Berechtigung zum Ausführen von Operationen hat.
query options	Zeigt alle oder einen Teil Ihrer Optionen und ihre aktuellen Einstellungen an.
query restore	Zeigt eine Liste der wiederanlauffähigen Zurückschreibungssitzungen in der Serverdatenbank an.
query schedule	Zeigt Informationen zu geplanten Ereignissen für Ihren Knoten an.
query session	Zeigt Informationen zu Ihrer Sitzung an, z. B. den aktuellen Knotennamen, die Angabe, wann die Sitzung aufgebaut wurde, Serverinformationen und Serververbindungsinformationen.
query systeminfo	Stellt IBM Spectrum Protect-Systeminformationen zusammen und gibt diese Informationen in einer Datei oder an der Konsole aus.
Windows-Betriebssystemequery systemstate	Windows-BetriebssystemeZeigt Informationen über die Sicherung des Systemstatus auf dem IBM Spectrum Protect-Server an. Dieser Befehl ist für alle unterstützten Windows-Clients gültig.
Windows-Betriebssysteme Linux-Betriebssystemequery vm	Windows-BetriebssystemeLinux-BetriebssystemeÜberprüft, ob die virtuellen Maschinen erfolgreich von dem vStorage-Sicherungsserver gesichert wurden.
restart restore	Zeigt eine Liste der wiederanlauffähigen Zurückschreibungssitzungen an, aus der Sie eine zum erneuten Starten auswählen können.
restore	Schreibt Kopien von Sicherungsversionen Ihrer Dateien vom IBM Spectrum Protect-Server zurück.
Windows-Betriebssystemerestore adobjects	Windows-BetriebssystemeSchreibt einzelne Active Directory-Objekte aus dem lokalen Container für gelöschte Active Directory-Objekte zurück.
restore backupset	Schreibt einen Sicherungssatz vom IBM Spectrum Protect-Server oder aus einer lokalen Datei zurück. Auf den Clients, die Bandeinheiten unterstützen, kann dieser Befehl einen Sicherungssatz von einer Bandeinheit zurückschreiben.
restore group	Schreibt bestimmte oder alle Member einer Gruppensicherung zurück.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemerestore image	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeSchreibt ein Dateisystemimage oder das Image eines unformatierten Datenträgers zurück.
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssystemerestore nas	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeSchreibt das Image eines Dateisystems zurück, das zu einem NAS-Dateiserver gehört.
Windows-Betriebssystemerestore systemstate	Windows-BetriebssystemeSchreibt eine Sicherung des Systemstatus zurück. Dieser Befehl ist für Onlinezurückschreibungsoperationen für ein System veraltet. Weitere Informationen finden Sie in Restore Systemstate.
Linux-Betriebssysteme Windows-Betriebssystemerestore vm	Linux-BetriebssystemeWindows-BetriebssystemeSchreibt eine VM-Gesamtsicherung zurück und stellt die Dateien der VM-Gesamtsicherung in das Verzeichnis vmbackdir auf dem vStorage-Sicherungsserver.

Befehl	Beschreibung
retrieve	Ruft Kopien archivierter Dateien vom IBM Spectrum Protect-Server ab.
schedule	Startet den Client-Scheduler auf der Workstation.
selective	Sichert ausgewählte Dateien.
set access	Berechtigt einen anderen Benutzer für den Zugriff auf Ihre Sicherungsversionen oder Archivierungskopien. AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeAuf den Clients, die Imagesicherung unterstützen, können Sie mit diesem Befehl die Berechtigungsregeln für Images definieren, die auf dem Server gespeichert sind.
set event	Ermöglicht Ihnen die Angabe der Umstände, wenn archivierte Daten gelöscht werden.
Linux-Betriebssysteme Windows-Betriebssystemeset netappsvm	Linux-BetriebssystemeWindows-BetriebssystemeOrdnet die Berechtigungsnachweise für Anmeldung eines Cluster-Management-Servers einer NetApp Storage Virtual Machine und dem Daten-SVM-Namen (Data Vserver) zu. Dieser Befehl muss eingegeben werden, bevor Sie eine Momentaufnahmedifferenzteilsicherung eines NetApp-Clusterdatenträgers erstellen können.
set password	Ändert das IBM Spectrum Protect-Kennwort für die Workstation.

Für den ordnungsgemäßen Betrieb ist es unbedingt erforderlich, dass der WAS-Knoten an derselben Position und unter demselben Namen zurückgeschrieben wird.

Wichtig: Um Probleme zu vermeiden, sollten Sie Ihre Daten nur auf der Ebene des Network Deployment Manager-Knotens oder des Application Server-Knotens zurückschreiben.

- Clientbefehlssitzung starten und beenden
  Eine Clientbefehlssitzung kann im Stapelmodus oder im interaktiven Modus gestartet oder beendet werden.
- Clientbefehle, Optionen und Parameter eingeben
  Ein Clientbefehl kann eine oder mehrere der folgenden Komponenten beinhalten: *Befehlsname*, *Optionen* und *Parameter*. Diese Komponenten werden in den folgenden Abschnitten beschrieben.
- Platzhalterzeichen
  Platzhalterzeichen werden verwendet, wenn mehrere Dateien mit ähnlichen Namen in *einem* Befehl angegeben werden sollen. Ohne Platzhalterzeichen muss der Befehl für jede Datei wiederholt werden.
- Clientbefehlsreferenz
  Die folgenden Abschnitte enthalten detaillierte Informationen zu den Befehlen des Clients für Sichern/Archivieren.
- Archive
  Mit dem Befehl archive können einzelne Dateien, ausgewählte Dateien oder alle Dateien in einem Verzeichnis und in den zugehörigen Unterverzeichnissen auf einem Server archiviert werden.
- Linux-BetriebssystemeWindows-BetriebssystemeArchive FastBack
  Mit dem Befehl archive fastback können Sie Tivoli Storage Manager FastBack-Datenträger, die durch die Optionen fbpolicyname, fbclientname und fbvolumename angegeben sind, für die langfristige Aufbewahrung archivieren.
- Linux-BetriebssystemeWindows-BetriebssystemeBackup FastBack
  Mit dem Befehl backup fastback können Sie Tivoli Storage Manager FastBack-Datenträger sichern, die durch die Optionen fbpolicyname, fbclientname und fbvolumename für die langfristige Aufbewahrung angegeben sind.
- Backup Group
  Verwenden Sie den Befehl backup group, um eine Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen enthält, zu erstellen und in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server zu sichern.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeBackup Image
  Mit dem Befehl backup image wird eine Imagesicherung eines oder mehrerer Datenträger auf Ihrem System erstellt.
- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeBackup NAS
  Mit dem Befehl backup nas wird eine Imagesicherung eines oder mehrerer Dateisysteme erstellt, die zu einem NAS-Dateiserver (NAS = Network Attached Storage) gehören (wird auch als NDMP-Sicherung bezeichnet). Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.
- Windows-BetriebssystemeBackup Systemstate
  Verwenden Sie den Befehl backup systemstate, um alle bootfähigen Systemstatus- und Systemservicekomponenten als ein einziges Objekt zu sichern, damit eine konsistente zeitpunktgesteuerte Momentaufnahme des Systemstatus zur Verfügung gestellt wird.
- Linux-BetriebssystemeWindows-BetriebssystemeBackup VM
  Mit dem Befehl backup vm können Sie eine Gesamtsicherung einer virtuellen Maschine starten.
- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeCancel Process
  Der Befehl cancel process zeigt (sofern die NDMP-Unterstützung aktiviert ist) eine Liste der aktuellen NAS-Imagesicherungs- und -zurückschreibungsprozesse an, für die der Benutzer mit Verwaltungsaufgaben die Berechtigung hat. Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.
- Cancel Restore
  Mit dem Befehl cancel restore kann eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt werden.

- Delete Access
  Der Befehl delete access löscht Berechtigungsregeln für Dateien, die auf dem Server gespeichert sind.
- Delete Archive
  Mit dem Befehl delete archive können archivierte Dateien aus dem IBM Spectrum Protect-Serverspeicher gelöscht werden. Der Benutzer kann archivierte Dateien nur löschen, wenn ihm der Administrator die entsprechende Berechtigung erteilt hat.
- Delete Backup
  Der Befehl delete backup löscht Dateien, Images und virtuelle Maschinen, die im IBM Spectrum Protect-Serverspeicher gesichert wurden. Ihr Administrator muss Ihnen die Berechtigung zum Löschen von Objekten erteilen.
- Delete Filespace
  Mit dem Befehl delete filespace können Dateibereiche im IBM Spectrum Protect-Serverspeicher gelöscht werden. Ein Dateibereich ist ein logischer Speicherbereich auf dem Server, der die gesicherten oder archivierten Dateien enthält.
- Delete Group
  Verwenden Sie den Befehl delete group, um eine Gruppensicherung auf dem IBM Spectrum Protect-Server zu löschen.
- Expire
  Mit dem Befehl expire werden die Sicherungsobjekte, die Sie in der Dateispezifikation oder mit der Option filelist angeben, inaktiviert. Sie können eine einzelne Datei als verfallen definieren oder eine Datei, die eine Liste mit Dateien enthält, die als verfallen definiert werden sollen. Wird `OBJTYPE=VM` angegeben, inaktiviert dieser Befehl die aktuelle Sicherung für eine virtuelle Maschine.
- Help
  Verwenden Sie den Befehl help, um Informationen zu Befehlen, Optionen und Nachrichten anzuzeigen.
- Incremental
  Der Befehl incremental sichert alle neuen oder geänderten Daten an den Positionen, die Sie angeben, sofern Sie sie nicht von den Sicherungsservices ausschließen.
- Loop
  Der Befehl loop startet eine interaktive Befehlszeilensitzung, die aktiv ist, bis Sie `quit` eingeben.
- Macro
  Der Befehl macro führt eine Serie von Befehlen aus, die Sie in einer Makrodatei angeben.
- AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeMonitor Process
  Der Befehl monitor process zeigt (sofern die NDMP-Unterstützung aktiviert ist) eine Liste der aktuellen NAS-Imagesicherungs- und -zurückschreibungsprozesse an, für die der Benutzer mit Verwaltungsaufgaben die Berechtigung hat. Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.
- Preview Archive
  Der Befehl preview archive simuliert einen Archivierungsbefehl, ohne Daten an den Server zu senden.
- Preview Backup
  Der Befehl preview backup simuliert einen Sicherungsbefehl, ohne Daten an den Server zu senden.
- Query Access
  Der Befehl query access zeigt an, welchen Benutzern Zugriff auf Sicherungsversionen und Archivierungskopien bestimmter Dateien erteilt wurde.
- Windows-BetriebssystemeQuery Adobjects
  Verwenden Sie den Befehl query adobjects, um Informationen zu den gelöschten Objekten anzuzeigen, die sich in der lokalen Active Directory-Domäne befinden.
- Query Archive
  Der Befehl query archive zeigt eine Liste Ihrer archivierten Dateien und folgende Informationen zu jeder Datei an: Dateigröße, Archivierungsdatum, Dateispezifikation, Verfallsdatum und Archivierungsbeschreibung.
- Query Backup
  Der Befehl query backup zeigt eine Liste der Sicherungsversionen Ihrer Dateien an, die auf dem IBM Spectrum Protect-Server gespeichert sind oder sich in einem Sicherungssatz auf dem Server befinden, wenn die Option backupsetname angegeben ist.
- Query Backupset
  Der Befehl query backupset fragt einen Sicherungssatz von einer lokalen Datei, von einer Bandeinheit (falls anwendbar) oder vom IBM Spectrum Protect-Server ab.
- Query Filespace
  Der Befehl query filespace zeigt eine Liste der Dateibereiche für einen Knoten an. Die Dateibereiche sind auf dem IBM Spectrum Protect-Server gespeichert oder befinden sich in einem Sicherungssatz auf dem Server, wenn die Option backupsetname angegeben wird. Sie können auch einen einzelnen Dateibereich für die Abfrage angeben.
- Query Group
  Verwenden Sie den Befehl query group, um Informationen zu einer Gruppensicherung und ihren Membern anzeigen.
- Query Image
  Der Befehl query image zeigt Informationen zu Dateisystemimages an, die auf dem IBM Spectrum Protect-Server gespeichert sind oder sich in einem Sicherungssatz auf dem IBM Spectrum Protect-Server befinden, wenn die Option backupsetname angegeben wurde.
- Query Inclexcl
  Mit dem Befehl query inclexcl wird eine Liste der Einschluss-/Ausschlussanweisungen in der Reihenfolge angezeigt, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden. Die Liste zeigt die Optionsart, den Optionsbereich (archive, all, etc.) und den Namen der Quellendatei.
- Query Mgmtclass
  Mit dem Befehl query mgmtclass können Informationen zu den Verwaltungsklassen angezeigt werden, die in der aktiven Maßnahmengruppe verfügbar sind.
- Query Node
  Der Befehl query node zeigt alle Knoten an, für die eine Verwaltungsbenutzer-ID die Berechtigung zum Ausführen von Operationen hat. Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.

- Query Options
  Verwenden Sie den Befehl query options, um alle Optionen oder einen Teil Ihrer Optionen und ihre aktuelle Einstellung in Bezug auf den Befehlszeilenclient anzuzeigen.
- Query Restore
  Mit dem Befehl query restore kann eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt werden. Die Liste enthält folgende Felder: Eigner, Ersetzen (Ersetz.), Unterverzeichnis (Untver), Pfad beibehalten (Pfad beibeh.), Quelle und Ziel.
- Query Schedule
  Der Befehl query schedule zeigt die Ereignisse an, die für den Knoten geplant sind. Der Administrator kann Zeitpläne für automatische Sicherungen und Archivierungen erstellen. Zur besseren Arbeitsplanung kann mit diesem Befehl festgestellt werden, wann die nächsten geplanten Ereignisse stattfinden.
- Query Session
  Mit dem Befehl query session können Informationen zur Sitzung angezeigt werden, z. B. der aktuelle Knotenname, die Angabe, wann die Sitzung aufgebaut wurde, Serverinformationen und Serververbindungsinformationen.
- Query Systeminfo
  Verwenden Sie den Befehl query systeminfo, um Informationen zusammenzustellen und in eine Datei oder an der Konsole auszugeben.
-  Query Systemstate
  Verwenden Sie den Befehl query systemstate, um Informationen zu einer Sicherung des Systemstatus anzuzeigen, die auf dem IBM Spectrum Protect-Server gespeichert ist oder sich in einem Sicherungssatz auf dem IBM Spectrum Protect-Server befindet, wenn die Option backupsetname angegeben wurde.
-  Query VM
  Verwenden Sie den Befehl query VM, um die erfolgreichen Sicherungen von virtuellen Maschinen (VMs) aufzulisten und zu verifizieren.
- Restart Restore
  Mit dem Befehl restart restore kann eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt werden.
- Restore
  Mit dem Befehl restore werden Kopien der Sicherungsversionen Ihrer Dateien vom IBM Spectrum Protect-Server oder aus einem Sicherungssatz abgerufen.
-  Restore Adobjects
  Verwenden Sie den Befehl restore adobjects, um einzelne Active Directory-Objekte aus dem lokalen Container für gelöschte Objekte zurückzuschreiben.
- Restore Backupset
  Der Befehl restore backupset schreibt einen Sicherungssatz vom IBM Spectrum Protect-Server, von einer lokalen Datei oder von einer lokalen Bandeinheit zurück. Sie können den vollständigen Sicherungssatz oder in einigen Fällen bestimmte Dateien in dem Sicherungssatz zurückschreiben.
- Restore Group
  Verwenden Sie den Befehl restore group, um bestimmte Member oder alle Member einer Gruppensicherung zurückzuschreiben.
-  Restore Image
  Mit dem Befehl restore image wird ein Dateisystemimage oder das Image eines unformatierten Datenträgers zurückgeschrieben, das mithilfe des Befehls backup image gesichert wurde.
-  Restore NAS
  Mit dem Befehl restore nas wird das Image eines Dateisystems zurückgeschrieben, das zu einem NAS-Dateiserver gehört. Wenn Sie eine interaktive Befehlszeilensitzung mit einer ID ohne Verwaltungsberechtigung verwenden, werden Sie zur Eingabe einer Administrator-ID aufgefordert.
- Restore Systemstate
  Der Befehl restore systemstate ist für Onlinezurückschreibungsoperationen des Systemstatus veraltet.
-  Restore VM
  Mit dem Befehl restore vm können Sie eine virtuelle Maschine zurückschreiben, die zuvor gesichert wurde.
- Retrieve
  Mit dem Befehl retrieve können Kopien archivierter Dateien vom IBM Spectrum Protect-Server abgerufen werden. Es können bestimmte Dateien oder vollständige Verzeichnisse abgerufen werden.
- Schedule
  Mit dem Befehl schedule kann der Client-Scheduler auf Ihrer Workstation gestartet werden. Der Client-Scheduler muss aktiv sein, damit geplante Arbeit gestartet werden kann.
- Selective
  Der Befehl selective sichert vom Benutzer angegebene Dateien. Werden diese Dateien beschädigt oder gehen sie verloren, können sie durch Sicherungsversionen vom Server ersetzt werden.
- Set Access
  Der Befehl set access erteilt Benutzern an anderen Knoten Zugriff auf Ihre Sicherungsversionen und Archivierungskopien.
- Set Event
  Mit dem Befehl set event können Sie die Umstände für das Löschen archivierter Daten angeben.
- Set Netappsvm
  Der Befehl set netappsvm ordnet die Berechtigungsnachweise für Anmeldung eines Cluster-Management-Servers, die im Befehl set password angegeben werden, einer NetApp Storage Virtual Machine und dem Daten-SVM-Namen (Data Vserver) zu (SVM = Storage Virtual Machine). Sie müssen diesen Befehl eingeben, bevor Sie eine Momentaufnahmedifferenzteilsicherung eines NetApp-Clusterdatenträgers erstellen können.
- Set Password
  Mit dem Befehl set password können Sie das IBM Spectrum Protect-Kennwort für Ihre Workstation ändern oder die

Berechtigungsnachweise definieren, mit denen auf einen anderen Server zugegriffen wird.

- Linux-BetriebssystemeWindows-BetriebssystemeSet vmtags
  Mit dem Befehl set vmtags werden Datenschutztags und Kategorien erstellt, die VMware-Bestandsobjekten hinzugefügt werden können. Sie können IBM Spectrum Protect-Sicherungen virtueller Maschinen in diesen VMware-Objekten verwalten, indem Sie die Tags mit Tools wie beispielsweise VMware vSphere PowerCLI Version 5.5 R2 oder höher angeben.

Zugehörige Verweise:
Syntaxdiagramme lesen

Clientbefehlssitzung starten und beenden

Eine Clientbefehlssitzung kann im Stapelmodus oder im interaktiven Modus gestartet oder beendet werden.

Verwenden Sie den Stapelmodus, um einen *einzelnen* Clientbefehl einzugeben. Der Client für Sichern/Archivieren verarbeitet den Befehl und kehrt zur Eingabeaufforderung zurück.

Verwenden Sie den interaktiven Modus, um eine *Reihe* von Befehlen einzugeben. Da der Client die Verbindung zum Server nur einmal für den interaktiven Modus aufbaut, können mehrere Befehle schneller verarbeitet werden. Der Client verarbeitet die Befehle und kehrt zur Eingabeaufforderung `Protect>` zurück.

- Befehle im Stapelmodus verarbeiten
  Einige Optionen sind *nur* in Anfangsbefehlszeile und nicht im interaktiven Modus gültig. Diese Optionen haben im Allgemeinen Auswirkungen auf den Betrieb der gesamten Sitzung.
- Befehle im interaktiven Modus verarbeiten
  Der *interaktive Modus* (Dialogmodus oder *Schleifenmodus*) dient zur Eingabe einer Reihe von Befehlen.

Befehle im Stapelmodus verarbeiten

Einige Optionen sind *nur* in Anfangsbefehlszeile und nicht im interaktiven Modus gültig. Diese Optionen haben im Allgemeinen Auswirkungen auf den Betrieb der gesamten Sitzung.

Beispielsweise wird der Befehl **dsmc query session -errorlogname=myerror.log** akzeptiert und gibt den Namen des Fehlerprotokolls an. Er wird jedoch aus dem einfachen Grund akzeptiert, dass er im Anfangsbefehl erscheint, obwohl die Option für den Befehl query nicht gültig ist.

Es gibt auch einige Optionen, die immer in der Anfangsbefehlszeile als auch in einzelnen Befehlen im interaktiven Modus gültig sind. Demzufolge werden bestimmte Optionen in der Anfangsbefehlszeile selbst dann akzeptiert, wenn sie keine Auswirkungen auf den eingegebenen Befehl haben. Beispielsweise ist **dsmc query session -subdir=yes** ein gültiger Befehl; in diesem Fall hat die Option *-subdir* jedoch keine Auswirkungen auf den eingegebenen Befehl.

Wird ein *einzelner* Befehl im Stapelmodus eingegeben, muss ihm der Name des ausführbaren Programms, **dsmc**, vorangestellt werden. Soll beispielsweise der Befehl incremental im Stapelmodus verarbeitet werden, geben Sie Folgendes ein:

```
dsmc incremental
```

Der Client für Sichern/Archivieren fordert Sie bei jeder Befehlseingabe zur Eingabe des Kennworts auf, wenn die Option passwordaccess auf prompt und die Authentifizierung auf dem Server auf *On* gesetzt ist. Das Kennwort eingeben und die Eingabetaste drücken.

Das Kennwort kann auch mit der Option password in einem Befehl eingegeben werden. In diesem Fall wird das Kennwort jedoch auf dem Bildschirm angezeigt. Lautet das Kennwort zum Beispiel ***secret***, Folgendes eingeben:

```
dsmc incremental –password=secret
```

Wird die Option *passwordaccess* in der Datei `dsm.opt` auf generate gesetzt, muss das Kennwort nicht im Befehl angegeben werden. Der Client fordert die Eingabe des Kennworts nur an, wenn Sie die Workstation bei einem Server registrieren oder das Kennwort manuell ändern.

Befehle im interaktiven Modus verarbeiten

Der *interaktive Modus* (Dialogmodus oder *Schleifenmodus*) dient zur Eingabe einer Reihe von Befehlen.

Geben Sie dsmc in die Befehlszeile ein und drücken Sie die Eingabetaste. Wenn die Eingabeaufforderung `Protect>` angezeigt wird, geben Sie den Befehlsnamen ein und drücken Sie die Eingabetaste. Den einzelnen Befehlen muss nicht der Name des ausführbaren Programms, dsmc, vorangestellt werden. Alternativ können Sie dsmc loop in die Befehlszeile eingeben, um eine Clientbefehlssitzung im interaktiven Modus zu starten. Loop ist der Standardbefehl für dsmc.

Falls ein Kennwort erforderlich ist, fordert Sie der Client für Sichern/Archivieren vor der Eingabe des ersten Befehls zur Eingabe des Kennworts auf.

Windows-BetriebssystemeDas Kennwort eingeben und die Eingabetaste drücken.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGeben Sie Ihre Benutzer-ID und Ihr Kennwort ein und drücken Sie die Eingabetaste.

Das Kennwort kann auch mit der Option password im Befehl loop eingegeben werden. In diesem Fall wird das Kennwort jedoch auf dem Bildschirm angezeigt. Lautet das Kennwort zum Beispiel ***secret***, Folgendes eingeben:

```
dsmc loop –password=secret
```

Soll eine interaktive Sitzung beendet werden, `quit` an der Eingabeaufforderung eingeben.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeAnmerkung für UNIX- und Linux-Clients:
Im Schleifenmodus wird der Mountpunkt nach einer Zurückschreibungsoperation direkt vom Band nicht freigegeben, falls weitere Zurückschreibungsanforderungen an den Datenträger gestellt werden. Wenn Sie eine Sicherungsoperation in derselben Sitzung anfordern und dieser Mountpunkt der einzig verfügbare ist, stoppt die Sicherungsoperation mit der folgenden Nachricht:

```
Auf Laden von Offlinedatenträger warten
```

In diesem Fall wird der Mountpunkt erst freigegeben, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Grenzwert der Einheitenklasse MOUNTRETENTION ist erreicht.
- Das Clientinaktivitätszeitlimit ist erreicht.
- Die Sitzung dsmc loop wird geschlossen, nachdem die Zurückschreibungsoperation beendet ist. Dies ermöglicht Ihnen den Start einer nachfolgenden Sitzung im Schleifenmodus, um die Sicherungsoperation auszuführen.

Clientbefehle, Optionen und Parameter eingeben

Ein Clientbefehl kann eine oder mehrere der folgenden Komponenten beinhalten: *Befehlsname*, *Optionen* und *Parameter*. Diese Komponenten werden in den folgenden Abschnitten beschrieben.

- Befehlsname
  Der erste Teil eines Befehls ist der Befehlsname. Der Befehlsname besteht aus einem Wort, wie z. B. **help** (Hilfe) oder **schedule** (Zeitplan), oder aus einem Aktionswort und einem Objekt für die Aktion, wie z. B. **query archive** (Archivierung abfragen).
- Optionen
  Werden Optionen mit einem Befehl eingegeben, muss der Option immer ein Bindestrich (–) vorausgehen. Fügen Sie zwischen dem Bindestrich und dem Optionsnamen kein Leerzeichen ein!
- Parameter
  Befehle können erforderliche Parameter, optionale Parameter oder keine Parameter haben.
- Syntax der Dateispezifikation
  Es gelten einige Syntaxregeln, die Sie kennen sollten, wenn Sie Dateispezifikationsparameter wie Dateispezifikation, Quellendateispezifikation und Zieldateispezifikation angeben.

Befehlsname

Der erste Teil eines Befehls ist der Befehlsname. Der Befehlsname besteht aus einem Wort, wie z. B. **help** (Hilfe) oder **schedule** (Zeitplan), oder aus einem Aktionswort und einem Objekt für die Aktion, wie z. B. **query archive** (Archivierung abfragen).

Der Benutzer kann den vollständigen Befehlsnamen oder seine Mindestabkürzung eingeben.

Für den Befehl query schedule sind beispielsweise folgende Versionen möglich:

```
query schedule
q sc
q sched
query sc
```

Optionen

Werden Optionen mit einem Befehl eingegeben, muss der Option immer ein Bindestrich (–) vorausgehen. Fügen Sie zwischen dem Bindestrich und dem Optionsnamen kein Leerzeichen ein!

In einen Befehl können mehrere Optionen in beliebiger Reihenfolge vor oder hinter der Dateispezifikation eingegeben werden. Mehrere Optionen müssen durch eine Leerstelle voneinander getrennt werden.

Für Befehle können zwei Gruppen von Optionen verwendet werden: Clientoptionen (in der Optionsdatei definiert) oder Clientbefehlsoptionen (in der Befehlszeile verwendet).

- **Clientoptionen**: Die Gruppe von Optionen, die in Ihrer Clientoptionsdatei definiert sind. Sie können eine Option in der Clientoptionsdatei überschreiben, indem Sie die Option zusammen mit einem Befehl in die Befehlszeile eingeben.
- **Clientbefehlsoptionen**: Verwenden Sie eine Clientbefehlsoption *nur*, wenn Sie die Option zusammen mit einem Befehl in die Befehlszeile eingeben. Sie können diese Optionen nicht in einer Optionsdatei definieren.

- Optionen im interaktiven Modus
  Im interaktiven Modus überschreiben die Optionen, die Sie in der Anfangsbefehlszeile eingeben, den Wert, den Sie in Ihrer Optionsdatei

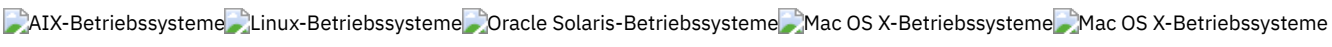
angegeben haben.

Parameter

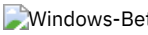
Befehle können erforderliche Parameter, optionale Parameter oder keine Parameter haben.

Erforderliche Parameter liefern Informationen zur Ausführung einer Task. Der am häufigsten verwendete erforderliche Parameter ist eine Dateispezifikation.

Soll beispielsweise die Datei budget.fin aus dem Verzeichnis /project archiviert werden, geben Sie Folgendes ein:



```
dsmc archive /project/budget.fin
```

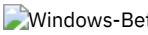


```
dsmc archive c:\project\budget.fin
```

Einige Befehle verfügen über optionale Parameter. Wird für einen optionalen Parameter kein Wert eingegeben, verwendet der Client für Sichern/Archivieren den Standardwert. Der Befehl restore verfügt beispielsweise über einen erforderlichen Parameter, Quellendateispezifikation, der den Pfad und den Namen der Datei im Speicher angibt, die zurückgeschrieben werden soll. Der optionale Parameter, Zieldateispezifikation, gibt den Pfad für die Speicherung der zurückgeschriebenen Dateien an. Wird die Zieldateispezifikation nicht angegeben, schreibt der Client die Dateien standardmäßig in den ursprünglichen Quellenpfad zurück. Sollen die Dateien in ein *anderes* Verzeichnis zurückgeschrieben werden, geben Sie einen Wert für Zieldateispezifikation ein.

Beispiel: Die Datei /project/budget.fin in den neuen Pfad /newproj/newbudg.fin zurückschreiben.

```
dsmc restore /project/budget.fin /newproj/
```



Beispiel: Die Datei c:\project\budget.fin in den neuen Pfad c:\newproj\newbudg.fin zurückschreiben.

```
dsmc restore c:\project\budget.fin c:\newproj\newbudg.fin
```

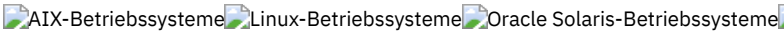
Die Parameter müssen in der im Befehlssyntaxdiagramm angegebenen Reihenfolge eingegeben werden.

Syntax der Dateispezifikation

Es gelten einige Syntaxregeln, die Sie kennen sollten, wenn Sie Dateispezifikationsparameter wie Dateispezifikation, Quellendateispezifikation und Zieldateispezifikation angeben.

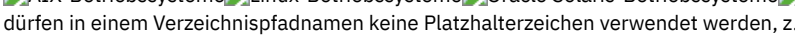
Es folgen die Syntaxregeln:

- Der Dateibereichsname und die Zieldateispezifikation dürfen keine Platzhalterzeichen enthalten. Eine Ausnahme bildet hierbei der Befehl set access, bei dem Platzhalterzeichen in den beiden niedrigsten Ebenen der Dateispezifikation zulässig sind.

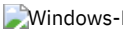
  

  Beispiel: Zugriff auf alle Dateien in allen Verzeichnissen in und unter dem Verzeichnis /home erteilen:

  ```
  set access backup /home/* * *
  set access backup /home/*/* * *
  ```

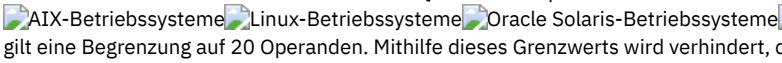
   Bei UNIX-Clients dürfen in einem Verzeichnispfadnamen keine Platzhalterzeichen verwendet werden, z. B.:

  ```
  /home/j*asler/file1.c
  ```

  Beispiel: Zugriff auf alle Dateien in allen Verzeichnissen in und unter dem Verzeichnis d:\test erteilen:

  ```
  set access backup d:\test\* * *
  set access backup d:\test\*\* * *
  ```

- Beachten Sie die maximale Anzahl der Dateispezifikationen pro Befehl:
  - Die Befehle Query können nur eine Dateispezifikation enthalten.
  - Die Befehle restore und retrieve können eine Quellendateispezifikation und eine Zieldateispezifikation enthalten.
  -  Für einige Befehle gilt eine Begrenzung auf 20 Operanden. Mithilfe dieses Grenzwerts wird verhindert, dass sehr viele Sitzungen geöffnet werden, wenn die Platzhalterzeichen vom Befehlsprozessor der UNIX-Shell erweitert werden.

Sie können verhindern, dass aufgrund der Shellerweiterung der Grenzwert von 20 Operanden überschritten wird, indem Sie am Anfang und am Ende der Erweiterungszeichen Ihrer Quellendateispezifikation in Befehlen zum Zurückschreiben Anführungszeichen eingeben.
Anmerkung: Die Verwendung von Anführungszeichen bewirkt als Nebeneffekt die Ausführung einer Zurückschreibung ohne Abfrage.

Sie können mit der Option removeoperandlimit angeben, dass der Client für Sichern/Archivieren die Begrenzung auf 20 Operanden entfernen soll. Geben Sie die Option removeoperandlimit mit dem Befehl incremental, selective oder archive an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt.

- Die Länge einer Dateispezifikation ist begrenzt.
  - AIX-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBei AIX, Solaris und Mac: Die maximale Anzahl Zeichen für einen Dateinamen beträgt 255. Die maximale Länge der Kombination aus Dateiname und Pfadname ist 1024 Zeichen. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthalten könnte, variieren kann.
  - Linux-BetriebssystemeUnter Linux: Die maximale Länge für einen Dateinamen beträgt 255 Byte. Die maximale Länge der Kombination aus Dateiname und Pfadname beträgt 4096 Byte. Diese Länge entspricht dem vom Betriebssystem unterstützten Wert für PATH_MAX. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, aus denen ein Pfad- und Dateiname besteht, variieren kann. Die tatsächliche Begrenzung ist die Anzahl Byte in den Pfad- und Dateikomponenten, die einer gleichen Anzahl Zeichen entsprechen kann.

    Linux-BetriebssystemeUnter Linux: Bei Archivierungs- oder Abrufoperationen bleibt die maximale Länge, die Sie für eine Kombination aus Pfad- und Dateinamen angeben können, bei 1024 Byte.

  - Windows-BetriebssystemeDie maximale Anzahl Byte für die Kombination aus Dateiname und Dateipfad ist 6255. Der Dateiname selbst darf jedoch 255 Byte nicht überschreiten. Darüber hinaus sind Verzeichnisnamen (einschließlich des Verzeichnisbegrenzers) innerhalb eines Pfads auf 255 Byte begrenzt. Die Unicode-Darstellung eines Zeichens kann mehrere Byte in Anspruch nehmen, sodass die maximale Anzahl Zeichen, die ein Dateiname enthalten könnte, variieren kann.

    Wenn Sie die Funktion zur Unterstützung offener Dateien mit VSS verwenden, fügt der Client für Sichern/Archivieren dem Pfad des Objekts, das gerade verarbeitet wird, den Datenträgernamen der Momentaufnahme hinzu. Der sich ergebende Pfad (Datenträgername der Momentaufnahme plus Objektpfad) darf die aufgeführten Grenzwerte nicht überschreiten. Der Datenträgername der Momentaufnahme darf maximal 1024 Byte umfassen.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWenn bei Eingabe der Quellendateispezifikation der Verzeichnisname mit / endet, wird /* impliziert.

  Windows-BetriebssystemeWenn bei Eingabe der Quellendateispezifikation der Verzeichnisname mit \ endet, wird * impliziert.

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWenn bei Eingabe einer Zieldateispezifikation der Name mit / endet, wird er als Verzeichnis betrachtet, andernfalls als Datei.

  Windows-BetriebssystemeWenn bei Eingabe einer Zieldateispezifikation der Name mit \ endet, wird er als Verzeichnis betrachtet, andernfalls als Datei.

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDas folgende Beispiel verdeutlicht diese beiden Regeln. Obwohl es sich bei mydir und yourdir um Verzeichnisse handelt, schlägt der Befehl fehl, weil /* hinter mydir impliziert und yourdir als Datei betrachtet wird.

  ```
  restore /home/mydir/ /away/yourdir
  ```

  Windows-BetriebssystemeDas folgende Beispiel verdeutlicht diese beiden Regeln. Obwohl mydir und yourdir Verzeichnisse sind, schlägt der Befehl fehl, weil * hinter mydir impliziert und yourdir als Datei betrachtet wird.

  ```
  restore c:\home\mydir\ c:\away\yourdir
  ```

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
  Windows-Betriebssysteme

  Wenn eine Dateispezifikation nicht mit einem Verzeichnisbegrenzer beginnt, wird die Dateispezifikation als ein Unterverzeichnis des aktuellen Arbeitsverzeichnisses betrachtet. Der Client hängt die Dateispezifikation an das Arbeitsverzeichnis an, um den vollständigen Pfad zu erstellen.

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBeispiel: Ist das aktuelle Arbeitsverzeichnis /home/me und der Befehl `dsmc res "/fs/dir1/*" mydir/`, lautet der vollständige Zurückschreibungspfad wie folgt: /home/me/mydir.

  Windows-BetriebssystemeBeispiel: Ist das aktuelle Arbeitsverzeichnis c:\home\me und der Befehl `dsmc res c:\fs\dir1\ mydir\`, lautet der vollständige Zurückschreibungspfad wie folgt: c:\home\me\mydir.

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeNur der Befehl incremental akzeptiert einen einfachen Dateibereichsnamen. Das folgende Beispiel ist gültig:
  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc i /Users
```

Das folgende Beispiel ist nicht gültig, da es sich bei dem Befehl um den Befehl selective handelt:
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
dsmc sel /Users
```

- Windows-BetriebssystemeWenn eine Dateispezifikation Leerzeichen enthält, muss sie in Anführungszeichen eingeschlossen werden. Beispiel:

  ```
  dsmc sel "x:\dir one\file1"
  ```

  Wenn eine Dateispezifikation mit einem umgekehrten Schrägstrich endet und in Anführungszeichen eingeschlossen ist, muss am Ende der Dateispezifikation ein zusätzlicher umgekehrter Schrägstrich (\) hinzugefügt werden. Wird kein zusätzlicher umgekehrter Schrägstrich hinzugefügt, wird die Dateispezifikation nicht korrekt verarbeitet und die Operation kann unerwartete Ergebnissen zur Folge haben.

  Das folgende Beispiel ist nicht korrekt:

  ```
  dsmc sel "x:\dir one\"
  ```

  Das folgende Beispiel ist korrekt:

  ```
  dsmc sel "x:\dir one\\"
  ```

  Das folgende Beispiel zeigt, wie der Inhalt eines Verzeichnisses (dir one) in ein anderes Verzeichnis (dir two) zurückgeschrieben wird, wenn beide Verzeichnisnamen Leerzeichen enthalten:

  ```
  dsmc rest "x:\dir one\\" "x:\dir two\\"
  ```

- Windows-BetriebssystemeDer Zugriff auf Microsoft DFS-Datenträger erfolgt mithilfe der Standard-UNC-Namen (UNC = Universal Naming Convention - allgemeine Namenskonvention). Die folgenden Beispiele zeigen die gültige Syntax für den Zugriff auf MS-DFS-Datenträger:

  ```
  \\Server_Name\Dfs_Root_Name\path
  \\Fault_Tolerant_Name\Dfs_Root_Name\path
  ```

Platzhalterzeichen

Platzhalterzeichen werden verwendet, wenn mehrere Dateien mit ähnlichen Namen in *einem* Befehl angegeben werden sollen. Ohne Platzhalterzeichen muss der Befehl für jede Datei wiederholt werden.

In einem Befehl können Sie Platzhalterzeichen *nur* innerhalb des Dateinamens oder innerhalb der Dateierweiterung verwenden. Sie können nicht zur Angabe von Zieldateien, Dateisystemen oder Servernamen verwendet werden. Sie können kein Verzeichnis angeben, dessen Name einen Stern (*) oder ein Fragezeichen (?) enthält.

Folgende Platzhalterzeichen sind gültig:

*
: Stern. Entspricht null oder mehr Zeichen.

?
: Fragezeichen. Entspricht einem beliebigen Einzelzeichen an der aktuellen Position.

Die folgende Tabelle zeigt Beispiele der einzelnen Platzhalterzeichen.

Tabelle 1. Platzhalterzeichen

Muster	Entspricht	Entspricht nicht
Stern (*)		
ab*	ab, abb, abxxx	a, b, aa, bb
ab*rs	abrs, abtrs, abrsrs	ars, aabrs, abrss
ab*ef*rs	abefrs, abefghrs	abefr, abers
abcd.*	abcd.c, abcd.txt	abcd, abcdc, abcdtxt
Fragezeichen (?)		
ab?	abc	ab, abab, abzzz
ab?rs	abfrs	abrs, abllrs
ab?ef?rs	abdefjrs	abefrs, abdefrs, abefjrs
ab??rs	abcdrs, abzzrs	abrs, abjrs, abkkkrs

Wichtig: Verwenden Sie einen Stern (*) statt eines Fragezeichens (?) als Platzhalterzeichen, wenn Sie nach einer Übereinstimmung mit einem Muster in einer Mehrfachbyte-Codepage suchen, um unerwartete Ergebnisse zu verhindern.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAnmerkung: Schließen Sie im Stapelmodus Werte, die Platzhalterzeichen enthalten, in Anführungszeichen ein. Andernfalls erweitern UNIX-Shells Platzhalterzeichen (ohne Anführungszeichen), und es wird schnell die Begrenzung auf 20 Operanden überschritten. Es ist effizienter, dem Client die Verarbeitung von Dateispezifikationen mit Platzhalterzeichen zu überlassen, da hier viel weniger Serverinteraktionen benötigt werden, um die Task zu beenden. Beispiel:

```
dsmc selective "/home/me/*.c"
```

Clientbefehlsreferenz

Die folgenden Abschnitte enthalten detaillierte Informationen zu den Befehlen des Clients für Sichern/Archivieren.

Die Informationen zu jedem Befehl umfassen Folgendes:

- Eine Beschreibung des Befehls.
- Ein Syntaxdiagramm des Befehls.
- Detaillierte Beschreibungen der Befehlsparameter. Ist der Parameter eine Konstante (ein Wert, der sich nicht ändert), wird die Mindestabkürzung in Großbuchstaben angezeigt.
- Beispiele für die Verwendung des Befehls.

Archive

Mit dem Befehl archive können einzelne Dateien, ausgewählte Dateien oder alle Dateien in einem Verzeichnis und in den zugehörigen Unterverzeichnissen auf einem Server archiviert werden.

Es werden die Dateien archiviert, deren aktueller Status aufbewahrt werden soll. Um Speicherbereich auf Ihrer Workstation freizugeben, sollten Sie Dateien mithilfe der Option deletefiles nach ihrer Archivierung löschen. Werden die archivierten Dateien wieder auf der Workstation benötigt, können sie jederzeit abgerufen werden.

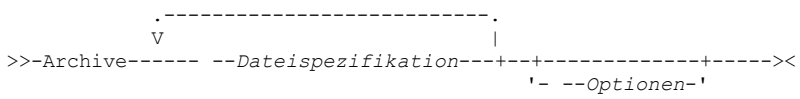
Verwenden Sie die Option snapshotroot im Befehl archive mit einer Anwendung eines unabhängigen Softwareanbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind. Die Option snapshotroot bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

AIX-BetriebssystemeNur für AIX: Mithilfe der Option snapshotproviderfs=*JFS2* können Sie die Dateiarchivierung auf Momentaufnahmebasis aktivieren.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax



Parameter

Dateispezifikation
: Gibt den Pfad und den Namen der Datei an, die archiviert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.
Sollen mehrere Dateispezifikationen angegeben werden, trennen Sie die einzelnen Parameter *Dateispezifikation* durch ein Leerzeichen voneinander. Werden mehrere Dateispezifikationen angegeben und haben mindestens zwei der Spezifikationen gemeinsame übergeordnete Verzeichnisse, kann es vorkommen, dass die gemeinsamen Verzeichnisobjekte mehrmals archiviert werden. Die Bedingungen, unter denen dieses Verhalten auftritt, sind laufzeitabhängig; das Verhalten selbst hat jedoch keine nachteiligen Auswirkungen.

  AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeLautet die Dateispezifikation beispielsweise /home/amr/ice.doc /home/amr/fire.doc, könnten /home und /home/amr zweimal archiviert werden. Die Dateiobjekte ice.doc und fire.doc werden nur einmal archiviert.

  Windows-BetriebssystemeLautet die Dateispezifikation beispielsweise C:\proposals\drafts\ice.doc C:\proposals\drafts\fire.doc, könnten C:\proposals und C:\proposals\drafts zweimal archiviert werden. Die Dateiobjekte, ice.doc und fire.doc, werden nur einmal archiviert.

Wenn Sie verhindern wollen, dass das gemeinsame übergeordnete Verzeichnis mehrmals angegeben wird, verwenden Sie separate, nicht überlappende archive-Befehle, um jede Dateispezifikation zu archivieren.
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWenn Sie ein Dateisystem archivieren, geben Sie einen abschließenden Schrägstrich an (/home/).
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeEs gilt eine Begrenzung auf 20 Operanden. Diese Begrenzung verhindert, dass sehr viele Sitzungen geöffnet werden, wenn die Platzhalterzeichen vom Befehlsprozessor der UNIX-Shell erweitert werden. Sie können verhindern, dass aufgrund der Shellerweiterung der Grenzwert von 20 Operanden überschritten wird, indem Sie am Anfang und am Ende der Dateispezifikationen, die Platzhalterzeichen enthalten ("home/docs/*"), Anführungszeichen eingeben.
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeSie können mit der Option removeoperandlimit angeben, dass die Beschränkung auf 20 Operanden entfernt wird. Wenn Sie die Option removeoperandlimit angeben, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Entfernen Sie beispielsweise die Begrenzung auf 20 Operanden, um 21 Dateispezifikationen zu archivieren:

```
selective -removeoperandlimit filespec1 filespec2 ... filespec21
```

Windows-BetriebssystemeWenn Sie ein Dateisystem archivieren, geben Sie einen abschließenden Schrägstrich an (C:\).
Windows-BetriebssystemeSie können so viele Dateispezifikationen angeben wie die verfügbaren Ressourcen oder andere Betriebssystembeschränkungen erlauben.
Sie können die Option filelist anstelle von Dateispezifikationen verwenden, um anzugeben, welche Dateien bei dieser Operation berücksichtigt werden sollen. Diese beiden Methoden schließen sich jedoch gegenseitig aus. Sie können nicht sowohl Dateispezifikationsparameter angeben als auch die Option filelist verwenden. Wenn die Option filelist angegeben wird, werden alle angegebenen Dateispezifikationen ignoriert.

Tabelle 1. Befehl Archive: Zugehörige Optionen

Option	**Verwendung**
archmc	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemearchsymlinkasfile	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Mac OS X-Betriebssysteme Windows-Betriebssystemeautofsrename	Mac OS X-BetriebssystemeWindows-BetriebssystemeNur Clientoptionsdatei (dsm.opt).
Windows-Betriebssystemechangingretries	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemechangingretries	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei oder Befehlszeile.
Windows-Betriebssystemecompressalways	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemecompressalways	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemecompression	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemecompression	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDatei dsm.sys innerhalb einer Serverzeilengruppe oder Befehlszeile.
deletefiles	Nur in der Befehlszeile.
description	Nur in der Befehlszeile.
dirsonly	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemeencryptiontype	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDatei dsm.sys innerhalb einer Serverzeilengruppe.
Windows-Betriebssystemeencryptiontype	Windows-BetriebssystemeClientoptionsdatei (dsm.opt).
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemeencryptkey	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDatei dsm.sys innerhalb einer Serverzeilengruppe.

Option	Verwendung
Windows-Betriebssystemeencryptkey	Windows-BetriebssystemeClientoptionsdatei (dsm.opt).
filelist	Nur in der Befehlszeile.
filesonly	Nur in der Befehlszeile.
Windows-Betriebssystemepostsnapshotcmd	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.fs.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme preservelastaccessdate	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme preservelastaccessdate	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemepresnapshotcmd	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.fs.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme removeoperandlimit	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssystemeskipntpermissions	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemeskipntsecuritycrc	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssystemesnapshotcachesize	AIX-BetriebssystemeLinux-BetriebssystemeClientoptionsdatei (dsm.opt) oder Option include.fs.
snapshotroot	Nur in der Befehlszeile.
subdir	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
v2archive	Nur in der Befehlszeile.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine einzelne Datei mit dem Namen `budget` im Verzeichnis `/home/proj1` archivieren.

Befehl: archive `/home/proj1/budget`

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine einzelne Datei mit dem Namen `budget.jan` im Verzeichnis `c:\plan\proj1` archivieren.

Befehl: `archive c:\plan\proj1\budget.jan`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien im Verzeichnis `/home/proj1` mit der Dateierweiterung `.txt` archivieren.

Befehl: `archive "/home/proj1/*.txt"`

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Dateien im Verzeichnis `c:\plan\proj1` mit der Dateierweiterung `.txt` archivieren.

Befehl: `archive c:\plan\proj1\*.txt`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien in der Verzeichnisbaumstruktur unter dem Verzeichnis `/home` archivieren.

Befehl: `archive -subdir=yes "/home/*"`

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Dateien im Laufwerk `c:\` archivieren.

Befehl: `archive -subdir=yes c:\*.*`

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Dateien auf dem Microsoft DFS-Datenträger MyDfsVolume archivieren. Sie müssen ***subdir***=*yes* angeben, um *alle* Dateien auf dem Datenträger zu archivieren.

Befehl: `archive \\myserver\mydfsroot\mydfsvolume\*.* -subdir=yes`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAngenommen, Sie haben eine Momentaufnahme des Dateisystems `/usr` gestartet und die Momentaufnahme als `/snapshot/day1` angehängt. Archivieren Sie die Verzeichnisbaumstruktur `/usr/dir1/sub1` aus der lokalen Momentaufnahme und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnames `/usr`.

Befehl: `dsmc archive /usr/dir1/sub1/ -subdir=yes -snapshotroot=/snapshot/day1`

Windows-BetriebssystemeTask
Windows-BetriebssystemeAngenommen, Sie haben eine Momentaufnahme des Laufwerks `C:\` gestartet und die Momentaufnahme als `\\florence\c$\snapshots\snapshot.0` angehängt. Archivieren Sie die Verzeichnisbaumstruktur `c:\dir1\sub1` aus der lokalen Momentaufnahme und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen `C:`.

Befehl: `dsmc archive c:\dir1\sub1\* -subdir=yes -snapshotroot=\\florence\c$\snapshots\snapshot.0`

- Windows-BetriebssystemeUnterstützung offener Dateien
  Wenn die Unterstützung offener Dateien konfiguriert ist, führt der Client für Sichern/Archivieren eine Momentaufnahmesicherung oder -archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder "im Gebrauch") sind.

Linux-Betriebssysteme Windows-Betriebssysteme

Archive FastBack

Mit dem Befehl archive fastback können Sie Tivoli Storage Manager FastBack-Datenträger, die durch die Optionen fbpolicyname, fbclientname und fbvolumename angegeben sind, für die langfristige Aufbewahrung archivieren.

Bevor Sie diesen Befehl verwenden, müssen Sie den Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren. Wenn Sie diesen Befehl ausgeben, sollte zudem mindestens eine Momentaufnahme im FastBack-Repository für die FastBack-Maßnahme vorhanden sein, die archiviert oder gesichert wird.

Windows-BetriebssystemeWenn eine Maßnahmenspezifikation sowohl Windows als auch Linux FastBack-Clients enthält, werden nur die Windows-Datenträger vom Windows-Client für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gesichert oder archiviert.

Linux-BetriebssystemeWenn eine Maßnahmenspezifikation sowohl Windows als auch Linux FastBack-Clients enthält, werden nur die Linux-Datenträger vom Linux-Client für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gesichert oder archiviert.

Sie können Tivoli Storage Manager FastBack-Optionen verwenden, um die neuesten Momentaufnahmen der folgenden Datenträger zu archivieren:

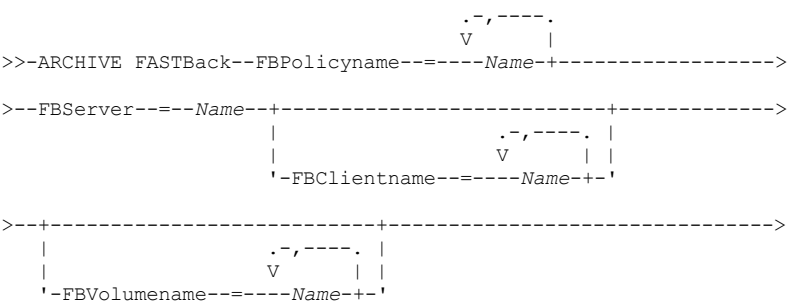
- Alle Clients und Datenträger, die einer bestimmten FastBack-Maßnahme oder einer Liste von FastBack-Maßnahmen zugeordnet sind.
- Alle Datenträger, die einem bestimmten FastBack-Client oder einer Liste von FastBack-Clients für eine angegebene FastBack-Maßnahme zugeordnet sind.
- Ein bestimmter Datenträger oder Datenträger, die einem bestimmten FastBack-Client für eine angegebene FastBack-Maßnahme zugeordnet sind.

Unterstützte Clients

Linux-BetriebssystemeDiese Option ist für Linux x86_64-Clients gültig.

Windows-BetriebssystemeDiese Option ist für alle Windows-Clients gültig, die als dedizierte Proxys konfiguriert sind. Dieser Befehl ist auch für Windows-Clients gültig, die auf der FastBack-Server-Workstation oder dem FastBack Disaster Recovery Hub installiert sind.

Syntax



```
>--+--------------------------+--+------------------+---------->
   '-FBReposlocation--=--Name-'  '-FBBranch--=--Name-'

>--+-----------------+----------------------------------------><
   '-ARCHMc--=--Name-'
```

Wichtig:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBCLientName angegeben werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Sie müssen immer die Option FBReposLocation für Linux angeben.

Parameter

Tabelle 1. Befehl Archive FastBack: Zugehörige Optionen

Option	Verwendung
fbpolicyname	Befehlszeile und Scheduler.
fbserver	Befehlszeile und Scheduler.
fbclientname	Befehlszeile und Scheduler.
fbvolumename	Befehlszeile und Scheduler.
fbreposlocation	Befehlszeile und Scheduler.
fbbranch	Befehlszeile und Scheduler.
archmc	Befehlszeile und Scheduler.

Beispiele

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeDer Client für Sichern/Archivieren ist auf einer Linux-Proxy-Client-Maschine installiert. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle Linux FastBack-Clients zu archivieren, die für die FastBack-Maßnahme Policy1 definiert sind:

```
dsmc archive fastback -fbpolicyname=Policy1
  -fbserver=myfbserver -fbreposlocation=myfbserver@WORKGROUP
```

Der FastBack-Servername -myFbDrHub ist der kurze Hostname des FastBack Disaster Recovery Hub-Servers, auf dem sich das Repository befindet.

Der Parameter -fbreposlocation gibt die Position des Repositorys an. Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

FBServer sollte in diesem Fall auf den kurzen Hostnamen des FastBack DR Hub verweisen.

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeDas Repository rep_server1 befindet sich auf dem FastBack DR Hub myFbDrHub.

```
dsmc archive fastback -fbpolicyname="Policy 1"
  -fbserver=myFbDrHub -fbreposlocation=\\myFbDrHub\rep_server1
```

Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

Der FastBack-Servername -myFbDrHub ist der kurze Hostname des FastBack Disaster Recovery Hub, auf dem sich das Repository befindet.

FBServer sollte in diesem Fall auf den kurzen Hostnamen des FastBack DR Hub verweisen.

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeAlle Datenträger, die durch die FastBack-Maßnahme mit dem Namen policy1 geschützt sind, für den FastBack-Server mit dem Namen basil archivieren:

```
dsmc archive fastback -Fbpolicyname=policy1
  -FBServer=basil -ARCHMC="my_tsm_mgmt_class"
  -fbreposlocation=basil@WORKGROUP
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeDer Client für Sichern/Archivieren ist auf dem FastBack-Server installiert. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle Windows FastBack-Clients zu archivieren, die für die FastBack-Maßnahme Policy1 definiert sind:

```
dsmc archive fastback -fbpolicyname=Policy1
  -fbserver=myfbserver
```

Die Repository-Position ist nicht erforderlich. Wenn Sie die Repository-Position angeben, wird sie ignoriert.

Der FastBack-Servername -myfbserver ist der kurze Hostname des FastBack-Servers, auf dem der Client ausgeführt wird.

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeDer Client für Sichern/Archivieren ist auf dem FastBack Disaster Recovery Hub installiert. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle FastBack-Clients zu archivieren, die in der Maßnahme mit dem Namen Policy 1 enthalten sind:

```
dsmc archive fastback -fbpolicyname="Policy 1"
  -fbserver=myFbServer -fbbranch=branch1
```

Die Repository-Position ist nicht erforderlich. Wenn Sie die Repository-Position angeben, wird sie ignoriert.

Der Parameter myFbServer gibt den kurzen Hostnamen des FastBack-Servers an, dessen FastBack-Filiale mithilfe der Option FBBranch angegeben wird.

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeDer Client für Sichern/Archivieren ist auf einer dedizierten Proxy-Maschine mit Tivoli Storage Manager FastBack-Verwaltungsbefehlszeile und FastBack Mount installiert. Der Client stellt eine Verbindung zu dem FastBack-Server-Repository her. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle FastBack-Clients zu archivieren, die in der Maßnahme mit dem Namen Policy 1 enthalten sind:

```
dsmc archive fastback -fbpolicyname="Policy 1" -fbserver=myFbServer
  -fbreposlocation=\\myFbServer.company.com\REP
```

Die Repository-Position ist erforderlich.

Der kurze Hostname der Maschine, auf der der FastBack-Server installiert ist, lautet myFbServer.

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeDer Client für Sichern/Archivieren ist auf einer dedizierten Proxy-Maschine mit Tivoli Storage Manager FastBack-Verwaltungsbefehlszeile und FastBack Mount installiert. Der Client stellt eine Verbindung zu einem Repository einer fernen Filiale auf dem FastBack Disaster Recovery Hub her. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle FastBack-Clients zu archivieren, die in der Maßnahme mit dem Namen Policy 1 enthalten sind:

```
dsmc archive fastback -fbpolicyname="Policy 1" -fbserver=myFbServer
  -fbreposlocation=\\myfbdrhub.company.com\REP
  -fbbranch=aFbServerBranch
```

Die Repository-Position ist erforderlich.

Der Wert myFbServer, der mit der Option -fbserver angegeben wird, ist der kurze Hostname des FastBack-Servers, dessen FastBack-Filiale mithilfe der Option FBBranch angegeben wird.

Die Option fbbranch gibt die Filialen-ID des FastBack-Servers auf dem Disaster Recovery Hub an.

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeAlle Datenträger, die durch die FastBack-Maßnahme mit dem Namen policy1 geschützt sind, für den FastBack-Server mit dem Namen basil archivieren und die Verwaltungsklasse "my_tsm_mgmt_class" auf die archivierten Datenträger anwenden.

```
dsmc archive fastback -Fbpolicyname=policy1
  -FBServer=basil -ARCHMC=”my_tsm_mgmt_class”
```

Zugehörige Konzepte:
Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren
Zugehörige Tasks:
Clients für Sichern/Archivieren konfigurieren
Linux-BetriebssystemeWindows-Betriebssysteme

Backup FastBack

Mit dem Befehl backup fastback können Sie Tivoli Storage Manager FastBack-Datenträger sichern, die durch die Optionen fbpolicyname, fbclientname und fbvolumename für die langfristige Aufbewahrung angegeben sind.

Bevor Sie diesen Befehl verwenden, müssen Sie den Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren. Wenn Sie diesen Befehl ausgeben, sollte zudem mindestens eine Momentaufnahme im Tivoli Storage Manager FastBack-

Repository für die Tivoli Storage Manager FastBack-Maßnahme vorhanden sein, die archiviert oder gesichert wird.

Windows-BetriebssystemeWenn eine Maßnahmenspezifikation sowohl Windows als auch Linux FastBack-Clients enthält, werden nur die Windows-Datenträger vom Windows-Client für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gesichert oder archiviert.

Linux-BetriebssystemeWenn eine Maßnahmenspezifikation sowohl Windows als auch Linux FastBack-Clients enthält, werden nur die Linux-Datenträger vom Linux-Client für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gesichert oder archiviert.

Tivoli Storage Manager FastBack-Optionen werden je nach der angegebenen Option für die Teilsicherung der neuesten Momentaufnahmen unterstützt:

- Alle Clients und Datenträger, die der FastBack-Maßnahme oder einer Liste von FastBack-Maßnahmen zugeordnet sind.
- Alle Datenträger, die einem bestimmten FastBack-Client oder einer Liste von FastBack-Clients für eine angegebene FastBack-Maßnahme zugeordnet sind.
- Ein bestimmter Datenträger oder Datenträger, die einem bestimmten FastBack-Client für eine angegebene FastBack-Maßnahme zugeordnet sind.

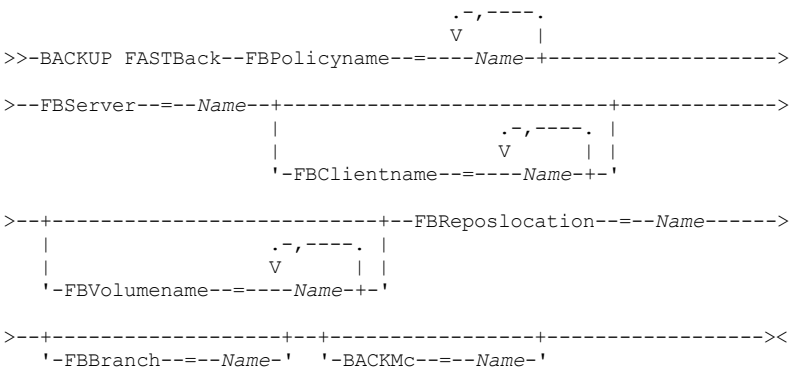
Unterstützte Clients

Linux-BetriebssystemeDieser Befehl ist für Linux x86_64-Clients gültig, die als dedizierte Tivoli Storage Manager FastBack-Proxys konfiguriert sind.

Windows-BetriebssystemeDieser Befehl ist für alle Windows-Clients gültig, die als dedizierte Tivoli Storage Manager FastBack-Proxys konfiguriert sind. Dieser Befehl ist auch für Windows-Clients gültig, die auf der Tivoli Storage Manager FastBack-Server-Workstation oder dem Tivoli Storage Manager FastBack Disaster Recovery Hub installiert sind.

Linux-Betriebssysteme

Syntax

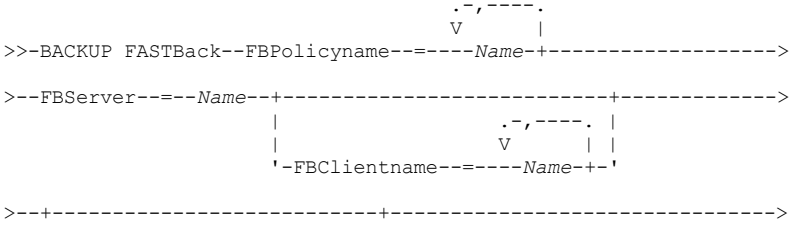


Wichtig:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBCLientName angegeben werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.
7. Sie müssen die Option FBReposLocation angeben.

Windows-Betriebssysteme

Syntax



```
   |                 .-,----. |
   |                 V      | |
   '-FBVolumename--=----Name-+-'

>--+--------------------------+--+------------------+---------->
   '-FBReposlocation--=--Name-'  '-FBBranch--=--Name-'

>--+-----------------+----------------------------------------><
   '-BACKMc--=--Name-'
```

Wichtig:

1. Mindestens ein Wert für FBpolicyName ist immer erforderlich.
2. Sie können bis zu 10 Werte für FBPolicyName angeben, wenn weder für FBClientName noch für FBVolumeName Werte angegeben sind.
3. Wenn Sie einen Wert für FBClientName angeben, darf nur ein Wert für FBPolicyName vorhanden sein.
4. Sie können bis zu 10 Werte für FBClientName angeben, wenn nur ein Wert für PolicyName angegeben ist und keine Werte für FBVolumeName angegeben sind.
5. Wenn Sie die Option FBVolumeName angeben, kann nur ein Wert für FBPolicy und nur ein Wert für FBCLientName angegeben werden.
6. Sie können mehrere Werte für FBVolumeName angeben, wenn Bedingung 5 erfüllt ist.

Tabelle 1. Befehl Backup FastBack: Zugehörige Optionen

Option	Verwendung
fbpolicyname	Befehlszeile und Scheduler.
fbserver	Befehlszeile und Scheduler.
fbclientname	Befehlszeile und Scheduler.
fbvolumename	Befehlszeile und Scheduler.
fbreposlocation	Befehlszeile und Scheduler.
fbbranch	Befehlszeile und Scheduler.
backmc	Befehlszeile und Scheduler.

Beispiele

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeDer Client für Sichern/Archivieren ist auf einer Linux-Proxy-Client-Maschine installiert. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle Linux FastBack-Clients zu sichern, die für die FastBack-Maßnahme Policy1 definiert sind:

```
dsmc backup fastback -fbpolicyname=Policy1
  -fbserver=myfbserver
  -fbreposlocation=myfbserver@WORKGROUP
```

Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

Der FastBack-Servername -myfbserver ist der kurze Hostname des FastBack-Servers, auf dem sich das Repository befindet.

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeDas Repository rep_server1 befindet sich auf dem FastBack Disaster Recovery Hub myFbDrHub.

```
dsmc backup fastback -fbpolicyname="Policy 1"
  -fbserver=myFbDrHub -fbreposlocation=\\myFbDrHub\rep_server1
```

Der FastBack-Servername -myFbDrHub ist der kurze Hostname des FastBack Disaster Recovery Hub-Servers, auf dem sich das Repository befindet.

Die Option -fbreposlocation gibt die Position des Repositorys an. Die Repository-Position ist erforderlich. Wenn Sie die Repository-Position nicht angeben, schlägt der Befehl fehl.

Die Option FBServer sollte in diesem Fall auf den kurzen Hostnamen des FastBack DR Hub verweisen.

Linux-BetriebssystemeBefehlszeile:

Linux-BetriebssystemeAlle Datenträger, die durch die FastBack-Maßnahme mit dem Namen policy1 geschützt sind, für den FastBack-Server mit dem Namen basil sichern:

```
dsmc backup fastback -Fbpolicyname=policy1
  -FBServer=basil -BACKMC="my_tsm_mgmt_class"
  -fbreposlocation=basil@WORKGROUP
```

Windows-BetriebssystemeBefehlszeile:

Windows-BetriebssystemeDer Client für Sichern/Archivieren ist auf dem FastBack-Server installiert. Verwenden Sie diesen Befehl, um alle Tivoli Storage Manager FastBack-Datenträger für alle Windows FastBack-Clients zu sichern, die für die Tivoli Storage Manager

FastBack-Maßnahme Policy1 definiert sind:

```
dsmc backup fastback -fbpolicyname=Policy1
  -fbserver=myfbserver
```

Die Repository-Position ist nicht erforderlich. Wenn Sie die Repository-Position angeben, wird sie ignoriert.

Der FastBack-Servername -myfbserver ist der kurze Hostname des FastBack-Servers, auf dem der Client ausgeführt wird.

 Windows-BetriebssystemeBefehlszeile:

 Windows-BetriebssystemeDer Client für Sichern/Archivieren ist auf dem FastBack Disaster Recovery Hub installiert. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle FastBack-Clients zu sichern, die in der Maßnahme mit dem Namen Policy 1 enthalten sind:

```
dsmc backup fastback -fbpolicyname="Policy 1"
  -fbserver=myFbServer -fbbranch=branch1
```

Die Repository-Position ist nicht erforderlich. Wenn Sie die Repository-Position angeben, wird sie ignoriert.

Der FastBack-Servername myFbServer ist der kurze Hostname des FastBack-Servers, dessen FastBack-Filiale mithilfe der Option FBBranch angegeben wird.

 Windows-BetriebssystemeBefehlszeile:

 Windows-BetriebssystemeDer Client für Sichern/Archivieren ist auf einer dedizierten Proxy-Maschine mit FastBack-Verwaltungsbefehlszeile und FastBack Mount installiert. Der Client stellt eine Verbindung zu dem FastBack-Server-Repository her. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle FastBack-Clients zu sichern, die in der Maßnahme mit dem Namen Policy 1 enthalten sind:

```
dsmc backup fastback -fbpolicyname="Policy 1" -fbserver=myFbServer
  -fbreposlocation=\\myFbServer.company.com\REP
```

Die Repository-Position ist erforderlich.

Der kurze Hostname der Maschine, auf der der FastBack-Server installiert ist, lautet myFbServer.

 Windows-BetriebssystemeBefehlszeile:

 Windows-BetriebssystemeDer Client für Sichern/Archivieren ist auf einer dedizierten Proxy-Maschine mit FastBack-Verwaltungsbefehlszeile und FastBack Mount installiert. Der Client stellt eine Verbindung zu einem Repository einer fernen Filiale auf dem FastBack Disaster Recovery Hub her. Verwenden Sie diesen Befehl, um alle FastBack-Datenträger für alle FastBack-Clients zu sichern, die in der Maßnahme mit dem Namen Policy 1 enthalten sind:

```
dsmc backup fastback -fbpolicyname="Policy 1" -fbserver=myFbServer
  -fbreposlocation=\\myfbdrhub.company.com\REP
  -fbbranch=aFbServerBranch
```

Die Repository-Position ist erforderlich.

Der Wert myFbServer, der mit der Option -fbserver angegeben wird, ist der kurze Hostname des FastBack-Servers, dessen FastBack-Filiale mithilfe der Option FBBranch angegeben wird.

Die Option fbbranch gibt die Filialen-ID des FastBack-Servers auf dem Disaster Recovery Hub an.

 Windows-BetriebssystemeBefehlszeile:

 Windows-BetriebssystemeAlle Datenträger, die durch die FastBack-Maßnahme mit dem Namen policy1 geschützt sind, für den FastBack-Server mit dem Namen basil sichern und die Verwaltungsklasse "my_tsm_mgmt_class" auf die gesicherten Datenträger anwenden:

```
dsmc backup fastback -Fbpolicyname=policy1
  -FBServer=basil -BACKMC="my_tsm_mgmt_class"
```

Zugehörige Konzepte:
Client für die Sicherung und Archivierung von Tivoli Storage Manager FastBack-Daten konfigurieren
Zugehörige Tasks:
Clients für Sichern/Archivieren konfigurieren

Backup Group

Verwenden Sie den Befehl backup group, um eine Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichsursprüngen enthält, zu erstellen und in einem virtuellen Dateibereich auf dem IBM Spectrum Protect-Server zu sichern.

 AIX-BetriebssystemeNur für AIX: Mithilfe der Option `snapshotproviderfs=JFS2` können Sie die Gruppensicherung auf Momentaufnahmebasis aktivieren.

Über eine Gruppensicherung können Sie eine konsistente zeitpunktgesteuerte Sicherung für eine Gruppe von Dateien erstellen, die gemeinsam als logische Einheit verwaltet werden. Für die Objekte in der Gruppe gelten die folgenden Verarbeitungsregeln:

- Erneutes Binden der Verwaltungsklasse für gruppierte Objekte:
  - Während Gesamtsicherungen wird allen Objekten in einer Sicherungsgruppe dieselbe Verwaltungsklasse zugeordnet.
  - Während Differenzsicherungen tritt folgendes Verhalten auf, wenn eine neue Verwaltungsklasse in einer Anweisung include für eine vorhandene Sicherungsgruppe angegeben wird:
    - Alle neuen und geänderten Objekte in der Sicherungsgruppe werden an die neue Verwaltungsklasse gebunden.
    - Alle Mitgliedsobjekte der Gruppe, die nicht geändert werden, erscheinen so, als ob sie nicht an die neue Verwaltungsklasse gebunden wären. Diese unveränderten Objekte sind nicht in den Statistikdaten Gesamtzahl erneut gebundener Objekte enthalten, die nach Beendigung des Befehls Backup Group angezeigt werden.
    - Die unveränderten Objekte werden einer neu erstellten Sicherungsgruppe neu zugeordnet und die neue Sicherungsgruppe wird an die neue Verwaltungsklasse gebunden. Für die unveränderten Gruppenobjekte wird jedoch weiterhin der Name der ursprünglichen Verwaltungsklasse angezeigt.

      Auch wenn für die unveränderten Objekte weiterhin der Name der ursprünglichen Verwaltungsklasse angezeigt wird, sind sie tatsächlich an die neue Verwaltungsklasse der Sicherungsgruppe gebunden.

- Vorhandene Anweisungen exclude für Dateien in der Gruppe werden ignoriert.
- Alle Objekte in der Gruppe werden gemeinsam exportiert.
- Alle Objekte in der Gruppe verfallen gemeinsam wie in der Verwaltungsklasse angegeben. Keine Objekte in der Gruppe verfallen, bevor nicht alle anderen Objekte in der Gruppe verfallen, selbst wenn eine andere Gruppe, zu denen diese Objekte gehören, verfällt.
- Werden vollständige und differenzielle Gruppensicherungen auf eine sequenzielle Einheit ausgeführt, sind die Daten bei der Zurückschreibung an nur zwei Positionen vorhanden. Führen Sie zum Optimieren der Zurückschreibungszeit regelmäßige Gesamtsicherungen aus, um die Daten an eine Position auf dem sequenziellen Datenträger zu sichern.
- Bei einer vollständigen Gruppensicherung werden alle Objekte in der Dateiliste an den Server gesendet. Bei einer differenziellen Gruppensicherung werden nur die Daten, die seit der letzten Gesamtsicherung geändert wurden, an den Server gesendet. Die Objekte in der Dateiliste, die sich seit den letzten Gesamtsicherungen nicht geändert haben, werden als Member der differenziellen Gruppensicherung zugeordnet. Ihre Daten werden jedoch nicht an den Server gesendet, sodass sich die Sicherungszeit verkürzt.

Für den Befehl backup group sind die folgenden Optionen erforderlich:

filelist
: Gibt eine Liste von Dateien an, die einer neuen Gruppe hinzugefügt werden sollen.

groupname
: Gibt den vollständig qualifizierten Namen der Gruppe an, die eine Liste von Dateien enthält.

virtualfsname
: Gibt den Namen des virtuellen Dateibereichs für die Gruppe an, mit der die Operation ausgeführt werden soll. Die Option virtualfsname darf nicht mit einem vorhandenen Dateibereichsnamen übereinstimmen.

mode
: Gibt an, ob alle Dateien in der Dateiliste gesichert werden oder nur die Dateien, die sich seit der letzten Gesamtsicherung geändert haben.

Anmerkung:

1. Wenn eine Datei in der Gruppensicherung fehlschlägt, schlägt die gesamte Gruppensicherung fehl.
2. Verwenden Sie den Befehl query group, um Member einer Gruppensicherung auf dem IBM Spectrum Protect-Server abzufragen.
3. Verwenden Sie den Befehl restore group, um bestimmte Member oder alle Member einer Gruppensicherung auf dem Server zurückzuschreiben.
4. Sofern Sie nicht unter Mac OS X arbeiten, verwenden Sie den Befehl delete group, um eine bestimmte Gruppensicherung vom Server zu löschen.
5. Verwenden Sie den Befehl query filespace, um Namen der virtuellen Dateibereiche für Ihren Knoten anzuzeigen, die auf dem Server gespeichert sind.
6. Eine Gruppensicherung kann zu einem Sicherungssatz hinzugefügt werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDieser Befehl ist für alle UNIX- und Linux-Clients mit Ausnahme von Mac OS X gültig.

 Windows-BetriebssystemeDieser Befehl ist für alle Windows-Clients gültig.

Syntax

```
>>-Backup GRoup-- --Optionen-----------------------------------><
```

Parameter

Tabelle 1. Befehl Backup Group: Zugehörige Optionen

Option	Verwendung

Option	Verwendung
filelist	Nur in der Befehlszeile.
groupname	Nur in der Befehlszeile.
mode	Nur in der Befehlszeile.
AIX-Betriebssysteme snapshotproviderfs	AIX-BetriebssystemeSystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder mit der Option include.fs.
Windows-Betriebssysteme snapshotproviderfs	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.fs.
Windows-Betriebssysteme snapshotproviderimage	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.image.
virtualfsname	Nur in der Befehlszeile.

Beispiele

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeEine Gesamtsicherung aller in der Datei /home/dir1/filelist1 angegebenen Dateien auf den virtuellen Dateibereich mit dem Namen accounting und mit der Hauptmemberdatei /home/group1 ausführen.

Befehl:

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1
-virtualfsname=/virtfs -mode=full
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine Gesamtsicherung aller in der Datei c:\dir1\filelist1 angegebenen Dateien auf den virtuellen Dateibereich mit dem Namen \virtfs und mit der Hauptmemberdatei `group1` ausführen.

Befehl:

```
backup group -filelist=c:\dir1\filelist1 -groupname=group1
-virtualfsname=\virtfs -mode=full
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Backup Image

Mit dem Befehl backup image wird eine Imagesicherung eines oder mehrerer Datenträger auf Ihrem System erstellt.

Mit dem Befehl backup image können Sie NTFS-, ReFS- oder unformatierte (RAW) Datenträger sichern. Wenn ein Datenträger mit NTFS formatiert ist, werden nur die vom Dateisystem verwendeten Blöcke gesichert. Bei ReFS-Datenträgern werden alle Blöcke gesichert.

AIX-BetriebssystemeWenn Sie die Option imagegapsize auf 0 setzen, werden alle Blöcke einschließlich der unbenutzten Blöcke am Ende des Datenträgers gesichert.

AIX-BetriebssystemeWenn Sie ein AIX JFS2-Dateisystem für die Imagesicherung angeben, werden nur die vom Dateisystem verwendeten Blöcke gesichert. Wenn Sie die Option imagegapsize auf null setzen, werden alle Blöcke einschließlich der unbenutzten Blöcke am Ende des Datenträgers gesichert.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAnmerkung:

1. AIX-BetriebssystemeNur für AIX: Standardmäßig ist die Imagesicherung auf Momentaufnahmebasis für JFS2-Datenträger aktiviert. Geben Sie `-snapshotproviderimage=NONE` in diesem Befehl an, um momentaufnahmebasierte Imagesicherungen zu inaktivieren.
2. Linux-BetriebssystemeFür die Linux-Clients wird die Imagesicherung nur auf Partitionen mit der ID 0x83 oder auf logischen Datenträgern unterstützt, die mit dem Linux Logical Volume Manager erstellt wurden. Beim Sichern anderer Partitionen, wie z. B. bei erweiterten Partitionen, die angehängte Dateisysteme oder Datenbankdaten enthalten, kann es zu inkonsistenten Sicherungsdaten kommen, wenn sich die Daten während der Imagesicherungsoperation ändern.
3. Linux-BetriebssystemeFür den Linux-Client wird die Imagesicherung von DASD-Einheiten mit dem Modus 'raw_track_access' unter Linux on z Systems nicht unterstützt.
4. AIX-BetriebssystemeLinux-BetriebssystemeDer Befehl 'backup image' wird nicht auf GPFS-Dateisystemen unterstützt.
5. Die IBM Spectrum Protect-API muss installiert sein, um den Befehl backup image verwenden zu können.
6. AIX-BetriebssystemeWenn Sie das Attribut eines JFS2-Dateisystems in ein von HSM verwaltetes Dateisystem ändern, wird keine Imagesicherung für dieses Dateisystem ausgeführt.

Wichtig: Der Zeitpunkt der letzten Teilsicherung bezieht sich auf die Serverzeit und der Zeitpunkt der letzten Dateiänderung auf die Clientzeit. Sind die Clientzeit und die Serverzeit nicht synchronisiert oder befinden der Client und der Server sich in verschiedenen Zeitzonen, wirkt sich dies auf die Teilsicherung nach Datum und die Imagesicherung mit `mode=incremental` aus.

Der Client sichert die Dateien, deren Änderungsdatum und -zeit (Clientzeit) nach dem Datum und der Zeit der letzten Teilsicherung des Dateisystems liegen, auf dem die Dateien gespeichert werden (Serverzeit).

Liegt die Serverzeit vor der Clientzeit, überspringen Teilsicherungen nach Datum oder Imagesicherungen mit `mode=incremental` die Dateien, die nach der letzten Teilsicherung oder Imagesicherung mit einem Änderungsdatum vor der Zeitmarke der letzten Teilsicherung erstellt oder geändert wurden.

Ist die Clientzeit der Serverzeit voraus, werden alle Dateien erneut gesichert, die vor der letzten Teil- oder Imagesicherung erstellt oder geändert wurden und deren Änderungszeit nach dem Zeitpunkt liegt, den die Zeitmarke der letzten Teilsicherung angibt. Normalerweise würden diese Dateien nicht gesichert, da sie bereits gesichert wurden.

Das Sicherungsdatum kann mit dem Befehl query filespace überprüft werden.

Windows-BetriebssystemeAnmerkung:

1. Das Konto, das den Client für Sichern/Archivieren ausführt, muss über Administratorberechtigung verfügen, damit Imagesicherungen erfolgreich ausgeführt werden können.
2. Die API muss installiert sein, um den Befehl backup image verwenden zu können.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDer Client für Sichern/Archivieren muss den Einheitentyp "unformatierte Einheit" auf der jeweiligen Plattform unterstützen, um eine Imagesicherung einer unformatierten Einheit ausführen zu können. Sie können eine Imagesicherung nur auf lokalen Einheiten ausführen. Gruppeneinheiten oder -dateisysteme sowie Einheiten oder Dateisysteme, die von mindestens zwei Systemen gemeinsam benutzt werden, werden nicht unterstützt. Wenn Sie eine Imagesicherung für ein Dateisystem ausführen wollen, das an eine unformatierte Einheit angehängt ist, muss die unformatierte Einheit unterstützt werden.

Verwenden Sie die Option include.image, um ein Dateisystem oder einen logischen Datenträger für die Imagesicherung einzubeziehen oder um datenträgerspezifische Optionen für die Imagesicherung anzugeben.

Der Befehl backup image verwendet die Option compression.

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Windows-BetriebssystemeDieser Befehl ist für alle Windows-Plattformen gültig.

Syntax

```
>>-Backup Image--+-------------+--------------------------------->
                 '- --Optionen-'

   .---------------------------.
   V                           |
>----+-----------------------+-+-------------------------------><
     '- --Dateispezifikation-'
```

Parameter

Dateispezifikation
: Gibt den Namen eines oder mehrerer logischer Datenträger an. Wenn Sie mehrere Dateisysteme sichern wollen, müssen Sie ihre Namen mit Leerzeichen voneinander trennen. Verwenden Sie keine Mustererkennungszeichen. Wenn Sie keinen Datenträgernamen angeben, werden die mit der Option domain.image angegebenen logischen Datenträger verarbeitet. Wenn Sie die Option domain.image nicht verwenden, um Dateisysteme für die Verarbeitung anzugeben, wird eine Fehlernachricht angezeigt, und es erfolgt keine Imagesicherung.

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDen Dateibereich, über den der logische Datenträger angehängt ist, oder den Namen des logischen Datenträgers angeben. Ist im System ein Dateisystem für einen bestimmten Datenträger konfiguriert, können Sie den Datenträger nicht mit dem Einheitennamen sichern.

  AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeBeispiel: Ist der Dateibereich /dev/lv01 auf dem Datenträger /home angehängt, können Sie `backup image /home` ausgeben; `backup image /dev/lv01` schlägt jedoch mit folgendem Fehler fehl:

  ```
  ANS1063E Ungültiger Pfad angegeben
  ```

  Oracle Solaris-BetriebssystemeAnmerkung: Für Sun-Systeme geben Sie entweder einen Dateisystemnamen oder den Namen einer unformatierten Einheit (des Typs Blockeinheit) an.

  Windows-BetriebssystemeDie Imagesicherung wird nur für einen Datenträger unterstützt, dem ein Mountpunkt oder Laufwerkbuchstabe zugeordnet ist. Ein Datenträger ohne Laufwerkbuchstaben oder Mountpunkt kann nicht gesichert werden.

Tabelle 1. Befehl Backup Image: Zugehörige Optionen

Option	Verwendung
Windows-Betriebssysteme asnodename	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme asnodename	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme compressalways	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Clientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssysteme compressalways	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
compression	Clientoptionsdatei oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme dynamicimage	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMit dem Befehl backup image oder der Option include.image in der Optionsdatei.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme imagegapsize	AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeMit dem Befehl backup image, mit der Option include.image oder in der Optionsdatei.
mode	Nur in der Befehlszeile.
postsnapshotcmd	Mit dem Befehl backup image, mit der Option include.image oder in der Optionsdatei.
presnapshotcmd	Mit dem Befehl backup image, mit der Option include.image oder in der Optionsdatei.
AIX-Betriebssysteme Linux-Betriebssysteme snapshotcachesize	AIX-BetriebssystemeLinux-BetriebssystemeMit dem Befehl backup image, mit der Option include.image oder in der Optionsdatei.
AIX-Betriebssysteme Linux-Betriebssysteme Windows-Betriebssysteme snapshotproviderimage	AIX-BetriebssystemeLinux-BetriebssystemeWindows-BetriebssystemeClientoptionsdatei oder mit der Option include.image.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDen Dateibereich /home/test, über den der logische Datenträger angehängt ist, sichern und eine Imageteilsicherung ausführen, bei der nur neue und geänderte Dateien nach der letzten vollständigen Imagesicherung gesichert werden.

```
dsmc backup image /home/test -mode=incremental
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEinen Datenträger sichern, der keinen Laufwerkbuchstaben hat, aber als Mountpunkt angehängt ist.

```
dsmc backup image m:\mnt\myntfs
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeDas Laufwerk h mithilfe einer Imageteilsicherung sichern. Eine Imageteilsicherung sichert Dateien, die neu sind oder sich seit der letzten vollständigen Imagesicherung geändert haben.

```
dsmc backup image h: -mode=incremental
```

AIX-BetriebssystemeLinux-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeEine statische Imagesicherung des logischen Datenträgers ausführen, der im Verzeichnis /home angehängt ist.

```
dsmc backup image /home -snapshotproviderimage=none
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine Offline-Imagesicherung des Laufwerks f ausführen.

```
dsmc backup image f: -snapshotproviderimage=none
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeEine dynamische Imagesicherung des logischen Datenträgers ausführen, der im Verzeichnis /home angehängt ist.

Befehl: `dsmc backup image /home -dynamicimage=yes`

AIX-BetriebssystemeLinux-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeEine Momentaufnahmeimagesicherung des Verzeichnisses /home ausführen.

```
AIX-BetriebssystemeAIX-Client: dsmc backup image /home
    -snapshotproviderimage=JFS2
Linux-BetriebssystemeLINUX-Client: dsmc backup image /home
    -snapshotproviderimage=LINUX_LVM
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Online-Imagesicherung des Laufwerks f ausführen.

```
dsmc backup image f: -snapshotproviderimage=VSS
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDen unformatierten logischen Datenträger /dev/lv01 sichern.

```
dsmc backup image /dev/lv01
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeDas Laufwerk f sichern, das einem Datenträger zugeordnet ist, der nicht mit einem Dateisystem formatiert wurde.

```
dsmc backup image f:
```

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeStatische, dynamische und Momentaufnahmeimagesicherung
  Die traditionelle Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen.
- Windows-BetriebssystemeOffline- und Online-Imagesicherung
  Die traditionelle offline ausgeführte Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-BetriebssystemeVerwendung der Imagesicherung für die Dateisystemteilsicherung
  Es gibt zwei Methoden, um durch die Verwendung von Imagesicherungen effiziente Teilsicherungen Ihrer Dateisysteme auszuführen. Mithilfe dieser Sicherungsmethoden können Sie eine zeitpunktgesteuerte Zurückschreibung für Ihre Dateisysteme ausführen und den Durchsatz beim Sichern und Zurückschreiben verbessern.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Statische, dynamische und Momentaufnahmeimagesicherung

Die traditionelle Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen.

Verwenden Sie die Option dynamicimage, um den Datenträger im aktuellen Status ohne erneutes Anhängen mit Lesezugriff zu sichern. Die Sicherung kann beschädigt werden, wenn Anwendungen auf den Datenträger schreiben, während die Sicherung ausgeführt wird. Führen Sie in diesem Fall fsck nach einer Zurückschreibung aus.

AIX-BetriebssystemeDie Option dynamicimage wird für JFS2-Datenträger nicht unterstützt.

Linux-BetriebssystemeNur für Linux x86_64-Clients: Standardmäßig führt der Client für Sichern/Archivieren eine Momentaufnahmeimagesicherung von Dateisystemen auf einem logischen Datenträger aus, der von Linux Logical Volume Manager erstellt wurde, während der der Datenträger für andere Systemanwendungen verfügbar ist. Die Momentaufnahmeimagesicherung erfordert einen IBM Spectrum Protect-Server der Version 5.1.

AIX-BetriebssystemeNur für AIX-Clients: Standardmäßig führt der Client für Sichern/Archivieren eine Momentaufnahmeimagesicherung von JFS2-Datenträgern aus, während der der Datenträger für andere Systemanwendungen verfügbar ist. AIX gestattet die Erstellung einer Momentaufnahme eines JFS2-Datenträgers, während er noch online ist. Die Momentaufnahme wird innerhalb derselben Datenträgergruppe wie der Quellendatenträger erstellt. Sie müssen sicherstellen, dass die Datenträgergruppe über genügend freien Plattenspeicherplatz für die Erstellung der Momentaufnahme verfügt. Die Momentaufnahme enthält die alten Datenblöcke; die geänderten Daten werden im Quellendatenträger gespeichert. Geben Sie mit der Option snapshotcachesize im Befehl backup image, in der Datei dsm.sys oder in Verbindung mit der Option include.image eine geeignete Momentaufnahmengröße an, sodass während der Imagesicherung alle alten Datenblöcke gespeichert werden können.

Linux-BetriebssystemeDer Linux Logical Volume Manager gestattet die Erstellung einer Momentaufnahme eines logischen Datenträgers, während der logische Datenträger selbst noch online ist. Die Momentaufnahme wird innerhalb derselben Datenträgergruppe wie der logische Quellendatenträger erstellt. Sie müssen sicherstellen, dass die Datenträgergruppe über genügend freien Plattenspeicherplatz für die Erstellung der Momentaufnahme verfügt. Die Momentaufnahme enthält die alten Datenblöcke; die geänderten Daten werden im logischen

Quellendatenträger gespeichert. Geben Sie mit der Option snapshotcachesize im Befehl backup image, in der Datei dsm.sys oder in Verbindung mit der Option include.image eine geeignete Momentaufnahmengröße an, sodass während der Imagesicherung alle alten Datenblöcke gespeichert werden können. Eine Momentaufnahmengröße von 100 Prozent gewährleistet eine gültige Momentaufnahme.

Windows-Betriebssysteme

Offline- und Online-Imagesicherung

Die traditionelle offline ausgeführte Imagesicherung verhindert während der Operation den Schreibzugriff auf den Datenträger durch andere Systemanwendungen.

Wenn die Unterstützung offener Dateien konfiguriert ist, führt der Client für Sichern/Archivieren eine Momentaufnahmesicherung oder -archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder "im Gebrauch") sind.

Verwenden Sie VSS als Momentaufnahmeprovider für die Unterstützung offener Dateien.

Folgende Hinweise gelten für Offline- und Online-Imagesicherungen:

- Wenn Sie ein Image des Systemlaufwerks erstellen, können Sie es nicht an die ursprüngliche Position zurückschreiben. Beim Zurückschreiben eines Images ist es erforderlich, dass der Client über eine exklusive Sperre des Datenträgers verfügt, auf den zurückgeschrieben wird, d. h. das Systemlaufwerk kann nicht zurückgeschrieben werden, da der Client das Systemlaufwerk nicht sperren kann. Sie können eine Imagesicherung des Systemlaufwerks an eine alternative Position zurückschreiben.
- Das Systemimage kann aufgrund unterschiedlicher Systemkomponentenkonfigurationen in den verschiedenen Komponenten (z. B. Active Directory) inkonsistent sein. Die Konfiguration einiger dieser Komponenten kann die Verwendung verschiedener Datenträger angeben, wobei diese teilweise im Systemlaufwerk, teilweise auf anderen Nicht-Systemlaufwerken installiert sind.
- Installieren Sie das IBM Spectrum Protect-Clientprogramm auf dem Systemlaufwerk. Der Client kann ein Image nicht auf denselben Datenträger zurückschreiben, auf dem auch das Clientprogramm installiert ist.
- Die Imagesicherung wird nur für Datenträger unterstützt, denen ein Mountpunkt oder Laufwerkbuchstabe zugeordnet ist. Ohne Mountpunkt oder Laufwerkbuchstaben führt der Client keine Datenträgersicherung aus.
- Werden bei einer LAN-unabhängigen oder LAN-gestützten Imagesicherung defekte Plattensektoren auf dem Quellenlaufwerk festgestellt, kann es unter Umständen zu einem Datenverlust kommen. In diesem Fall werden defekte Sektoren übersprungen, wenn die Imagedaten auf den IBM Spectrum Protect-Server gesendet werden. Werden bei der Imagesicherung fehlerhafte Plattensektoren festgestellt, wird eine Warnung ausgegeben, nachdem die Imagesicherung beendet ist.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Verwendung der Imagesicherung für die Dateisystemteilsicherung

Es gibt zwei Methoden, um durch die Verwendung von Imagesicherungen effiziente Teilsicherungen Ihrer Dateisysteme auszuführen. Mithilfe dieser Sicherungsmethoden können Sie eine zeitpunktgesteuerte Zurückschreibung für Ihre Dateisysteme ausführen und den Durchsatz beim Sichern und Zurückschreiben verbessern.

Sie können die Sicherung nur auf formatierten Datenträgern und nicht auf unformatierten logischen Datenträgern ausführen. Sie können entweder *Imagesicherung mit Dateisystemteilsicherung* oder *Imagesicherung mit dem Imageteilsicherungsmodus* verwenden, um Imagesicherungen für Datenträger mit angehängten Dateisystemen auszuführen.

Es folgen einige Beispiele für die Verwendung der *Imagesicherung mit Dateisystemteilsicherung*.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

- Eine vollständige Teilsicherung des Dateisystems ausführen: `dsmc incremental /myfilesystem`
- Eine Imagesicherung desselben Dateisystems ausführen: `dsmc backup image /myfilesystem`
- In regelmäßigen Abständen Teilsicherungen ausführen: `dsmc incremental /myfilesystem`

Windows-Betriebssysteme

- Eine vollständige Teilsicherung des Dateisystems ausführen: `dsmc incremental h:`
- Eine Imagesicherung desselben Dateisystems ausführen: `dsmc backup image h:`
- In regelmäßigen Abständen Teilsicherungen ausführen: `dsmc incremental h:`

Sie müssen die nächsten Schritte in der angegebenen Reihenfolge ausführen, um sicherzustellen, dass der Server Hinzufüge- und Löschvorgänge genau aufzeichnet.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeVerwenden Sie diesen Befehl, um das Dateisystem mit exakt dem Status der letzten Teilsicherung zurückzuschreiben: `dsmc restore image /myfilesystem -incremental -deletefiles`.

Windows-BetriebssystemeVerwenden Sie diesen Befehl, um das Dateisystem mit exakt dem Status der letzten Teilsicherung zurückzuschreiben: `dsmc restore image h: -incremental -deletefiles`.

Während der Zurückschreibung führt der Client Folgendes durch:

- Er schreibt das neueste Image auf dem Server zurück.
- Er löscht alle im vorherigen Schritt zurückgeschriebenen Dateien, die auf dem Server inaktiv sind. Dies sind Dateien, die zum Zeitpunkt der Imagesicherung vorhanden waren, aber danach gelöscht und durch eine spätere Teilsicherung aufgezeichnet wurden.
- Er schreibt neue und geänderte Dateien aus den Teilsicherungen zurück.

Wenn Sie die Schritte nicht exakt einhalten, können zwei Dinge passieren:

1. Nach dem Zurückschreiben des ursprünglichen Images werden alle Dateien, die mit dem Befehl incremental gesichert wurden, einzeln zurückgeschrieben.
2. Wird ein Befehl backup image vor einem Befehl incremental ausgeführt, werden Dateien, die aus dem ursprünglichen Image gelöscht wurden, *nicht* aus dem endgültig zurückgeschriebenen Dateisystem gelöscht.

Es folgen einige Beispiele für die Verwendung der *Imagesicherung mit dem Imageteilsicherungsmodus*.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme

- Eine Imagesicherung desselben Dateisystems ausführen: `dsmc backup image /myfilesystem`
- Eine Imageteilsicherung des Dateisystems ausführen: `dsmc backup image /myfilesystem -mode=incremental`

  Hierdurch werden nur die Dateien an den Server gesendet, die seit der letzten Imagesicherung hinzugefügt oder geändert wurden.

- In regelmäßigen Abständen vollständige Imagesicherungen ausführen: `dsmc backup image /myfilesystem`
- Das Image zurückschreiben: `dsmc restore image /myfilesystem -incremental`

  Beim Zurückschreiben ignoriert der Client für Sichern/Archivieren die Option deletefiles, wenn die Sicherungstechnik Image + Imageteilsicherung verwendet wurde. Die Zurückschreibung schließt Dateien ein, die nach der letzten vollständigen Imagesicherung gelöscht wurden, sowie die aktuellsten Versionen von Dateien, die nach der letzten Imagesicherung hinzugefügt oder geändert wurden.

 Windows-Betriebssysteme

- Eine Imagesicherung desselben Dateisystems ausführen: `dsmc backup image h:`
- Eine Imageteilsicherung des Dateisystems ausführen: `dsmc backup image h: -mode=incremental`

  Hierdurch werden nur die Dateien an den Server gesendet, die seit der letzten Imagesicherung hinzugefügt oder geändert wurden.

- In regelmäßigen Abständen vollständige Imagesicherungen ausführen: `dsmc backup image h:`
- Das Image zurückschreiben: `dsmc restore image h: -incremental`

  Beim Zurückschreiben ignoriert der Client für Sichern/Archivieren die Option deletefiles, wenn die Sicherungstechnik Image + Imageteilsicherung verwendet wurde. Die Zurückschreibung schließt Dateien ein, die nach der letzten vollständigen Imagesicherung gelöscht wurden, sowie die aktuellsten Versionen von Dateien, die nach der letzten Imagesicherung hinzugefügt oder geändert wurden.

Anmerkung: In den folgenden Fällen sollten Sie regelmäßig vollständige Imagesicherungen ausführen. Dadurch wird die Zurückschreibungszeit verbessert, da weniger Änderungen von Teilsicherungen angewendet werden.

- Wenn sich ein Dateisystem beträchtlich ändert (mehr als 40%).
- Einmal pro Monat.
- Entsprechend den Anforderungen in Ihrer Umgebung.

Die folgenden Einschränkungen gelten, wenn Sie Imagesicherung mit dem Imageteilsicherungsmodus verwenden:

- Das Dateisystem darf keine früheren, durch den Befehl incremental generierten vollständigen Teilsicherungen aufweisen.
- Durch eine Teilsicherung nach Datum werden Dateien auf dem Server nicht inaktiviert. Daher können beim Zurückschreiben von Dateien keine gelöscht werden.
- Bei der ersten Imagesicherung des Dateisystems wird eine vollständige Imagesicherung ausgeführt.
- Bei Verwendung von mode=*incremental* werden nur Dateien mit einem geänderten Datum und keine Dateien mit geänderten Berechtigungen gesichert.
- Wenn die maximale Kapazität der Dateisysteme bereits oder fast erreicht ist, kann hierdurch eine Bedingung 'Zu wenig Speicherbereich' während der Zurückschreibung auftreten.

 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Backup NAS

Mit dem Befehl backup nas wird eine Imagesicherung eines oder mehrerer Dateisysteme erstellt, die zu einem NAS-Dateiserver (NAS = Network Attached Storage) gehören (wird auch als NDMP-Sicherung bezeichnet). Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.

Der NAS-Dateiserver führt die externe Datenversetzung aus. Ein Serverprozess wird gestartet, um die Sicherung auszuführen.

Verwenden Sie die Option nasnodename, um den Knotennamen für den NAS-Dateiserver anzugeben. Der NAS-Knotenname identifiziert den NAS-Dateiserver für den IBM Spectrum Protect-Server; der NAS-Knotenname muss beim Server registriert sein. Fügen Sie die Option

nasnodename in Ihre Clientoptionsdatei (dsm.opt) ein. Der Wert in der Clientoptionsdatei ist der Standardwert; er kann jedoch in der Befehlszeile überschrieben werden.

Verwenden Sie die Option toc mit dem Befehl backup nas oder der Option include.fs.nas, um anzugeben, ob der IBM Spectrum Protect-Server für jede Dateisystemsicherung Inhaltsverzeichnisinformationen (TOC-Informationen) speichert. Wenn Sie TOC-Informationen speichern, können Sie den Serverbefehl QUERY TOC verwenden, um den Inhalt einer Dateisystemsicherung festzustellen, sowie den Serverbefehl RESTORE NODE, um einzelne Dateien oder Verzeichnisstrukturen zurückzuschreiben.

Sie können auch den IBM Spectrum Protect-Web-Client verwenden, um die gesamte Baumstruktur des Dateisystems zu untersuchen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen. Die Erstellung eines Inhaltsverzeichnisses erfordert, dass Sie das Attribut tocdestination in der Sicherungskopiengruppe für die Verwaltungsklasse definieren, an die dieses Sicherungsimage gebunden wird. Die TOC-Erstellung erfordert während der Sicherungsoperation zusätzliche Verarbeitung, zusätzliche Netzressourcen, zusätzlichen Speicherpoolbereich und möglicherweise einen zusätzlichen Mountpunkt. Wenn Sie keine TOC-Informationen speichern, können Sie über den Befehl RESTORE NODE dennoch einzelne Dateien und Verzeichnisstrukturen zurückschreiben, wenn Sie den vollständig qualifizierten Namen jeder Datei bzw. jedes Verzeichnisses und das Image kennen, in dem das Objekt gesichert wurde.

Die Option toc wird nur für Images unterstützt, die mit Client und Server mit mindestens Version 5.2 gesichert wurden.

Wenn Sie mode =*differential* im Serverbefehl BACKUP NODE oder im Befehl backup nas angeben, ohne dass ein Gesamtimage vorhanden ist, wird angezeigt, dass eine Gesamtsicherung gestartet wurde. Die Verwendung des Serverbefehls QUERY PROCESS zeigt, dass eine Gesamtsicherung in Bearbeitung ist.

Mit der Option mode geben Sie an, ob eine vollständige oder eine differenzielle NAS-Imagesicherung ausgeführt werden soll. Bei einer vollständigen Imagesicherung wird das gesamte Dateisystem gesichert. Der Standardwert ist eine differenzielle NAS-Imagesicherung für Dateien, die sich nach der letzten vollständigen Imagesicherung ändern. Ist keine auswählbare vollständige Imagesicherung vorhanden, erfolgt eine vollständige Imagesicherung. Ist ein Gesamtimage vorhanden, wird bei Angabe von mode =*differential* eine differenzielle Imagesicherung gesendet, unabhängig davon, ob das Image zurückgeschrieben werden kann oder verfallen ist und nur wegen abhängiger differenzieller Images aufbewahrt wird. Wird ein Gesamtimage während einer differenziellen Sicherung gesendet, wird es mithilfe des Severbefehls QUERY NASBACKUP als Gesamtimage angezeigt. Auch der Serverbefehl QUERY NASBACKUP zeigt zurückschreibbare NAS-Images an und "Gesamtimage" oder "differenzielles Image" als Objekttyp.

Mit der Option monitor geben Sie an, ob Sie eine NAS-Imagesicherung eines Dateisystems überwachen und Verarbeitungsinformationen anzeigen wollen.

Mit dem Befehl monitor process können Sie eine Liste aller Prozesse anzeigen, für die eine Verwaltungsbenutzer-ID über eine Berechtigung verfügt. Die Verwaltungsbenutzer-ID sollte mindestens die Clienteignerberechtigung sowohl über den NAS-Knoten als auch den Client-Workstation-Knoten besitzen, der entweder von der Befehlszeile oder vom Web aus verwendet wird.

Mit dem Befehl cancel process können Sie die NAS-Sicherungsverarbeitung stoppen.

Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: `/vol/vol0`.

 Für NAS-Dateisystembezeichnungen in der Befehlszeile müssen geschweifte Klammern {} als Begrenzer um Dateisystemnamen verwendet werden, zum Beispiel `{/vol/vol0}`.

Unterstützte Clients

  Dieser Befehl ist nur für AIX- und Solaris-Clients gültig.

Dieser Befehl ist für alle Windows-Clients gültig.

Syntax

```
                              .---------------------------.
                              V                           |
>>-Backup NAS--+-------------+------ --Dateispezifikation---+--><
               '- --Optionen-'
```

Parameter

Dateispezifikation
: Gibt den Namen eines oder mehrerer Dateisysteme auf dem NAS-Dateiserver an. Wenn Sie diesen Parameter nicht angeben, verarbeitet der Client für Sichern/Archivieren alle Dateisysteme, die durch die Option domain.nas definiert sind.

  Wenn Sie die Option *Dateispezifikation* oder domain.nas nicht angeben, wird der Standardwert all-nas für domain.nas verwendet, und es werden alle Dateisysteme auf dem NAS-Dateiserver gesichert.

Tabelle 1. Befehl Backup NAS: Zugehörige Optionen

Option	Verwendung

Option	Verwendung
mode	Nur in der Befehlszeile.
monitor	Nur in der Befehlszeile.
AIX-Betriebssysteme Oracle Solaris-Betriebssysteme nasnodename	AIX-BetriebssystemeOracle Solaris-BetriebssystemeClientoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssysteme nasnodename	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Oracle Solaris-Betriebssystemetoc	AIX-BetriebssystemeOracle Solaris-BetriebssystemeBefehlszeile oder mit der Option include.fs.nas in Ihrer Clientoptionsdatei (dsm.sys).
Windows-Betriebssystemetoc	Windows-BetriebssystemeBefehlszeile oder mit der Option include.fs.nas in Ihrer Clientoptionsdatei (dsm.opt).

Beispiele

AIX-Betriebssysteme Oracle Solaris-BetriebssystemeTask

AIX-Betriebssysteme Oracle Solaris-BetriebssystemeDie NAS-Imagesicherung des gesamten Dateisystems ausführen.

Befehl: `backup nas -mode=full -nasnodename=nas1 /vol/vol0 /vol/vol2`

Windows-BetriebssystemeTask

Windows-BetriebssystemeDie NAS-Imagesicherung des gesamten Dateisystems ausführen.

Befehl: `backup nas -mode=full -nasnodename=nas1 {/vol/vol0} {/vol/vol2}`

Task

Die NAS-Imagesicherung des gesamten Dateiservers ausführen.

Befehl: `backup nas -nasnodename=nas1`

AIX-Betriebssysteme Oracle Solaris-BetriebssystemeTask

AIX-Betriebssysteme Oracle Solaris-BetriebssystemeDie NAS-Imagesicherung des gesamten Dateisystems ausführen und Inhaltsverzeichnisinformationen (TOC-Informationen) für die Dateisystemsicherung speichern.

Befehl: `backup nas -mode=full -nasnodename=netappsj /vol/vol0 -toc=yes`

Windows-BetriebssystemeTask

Windows-BetriebssystemeDie NAS-Imagesicherung des gesamten Dateisystems ausführen und Inhaltsverzeichnisinformationen (TOC-Informationen) für die Dateisystemsicherung speichern.

Befehl: `backup nas -mode=full -nasnodename=netappsj {/vol/vol0} -toc=yes`

Windows-Betriebssysteme

Backup Systemstate

Verwenden Sie den Befehl backup systemstate, um alle bootfähigen Systemstatus- und Systemservicekomponenten als ein einziges Objekt zu sichern, damit eine konsistente zeitpunktgesteuerte Momentaufnahme des Systemstatus zur Verfügung gestellt wird.

Zu den bootfähigen Systemstatuskomponenten gehören:

- Active Directory (nur Domänencontroller)
- Systemdatenträger (nur Domänencontroller)
- Serverzertifikatsdatenbank
- COM+-Datenbank
- Windows-Registry
- System- und Bootdateien
- ASR-Writer

Zu den Systemservicekomponenten gehören:

- Intelligenter Hintergrundübertragungsdienst (BITS - Background Intelligent Transfer Service)
- Ereignisprotokolle
- RSM-Datenbank (Removable Storage Management)
- Clusterdatenbank (nur Clusterknoten)
- Ferner Speicherservice
- Terminal Server-Lizenzierung
- Windows Management Instrumentation (WMI)

- IIS-Metabasis (IIS = Internet Information Services, Internetinformationsservices)
- DHCP-Datenbank
- Wins-Datenbank

Die Liste der bootfähigen Systemstatus- und Systemservicekomponenten ist dynamisch und kann sich abhängig von installierten Service-Packs und Betriebssystemfeatures ändern. Der Client für Sichern/Archivieren ermöglicht die dynamische Erkennung und Sicherung dieser Komponenten.

Der Systemstatus wird von verschiedenen VSS-Ausgabeprogrammen durch den Typ "bootfähiger Systemstatus" und "Systemservice" dargestellt. Im Hinblick auf die Anzahl Dateien und den Umfang der Daten ist System Writer der größte Bestandteil des Systemstatus. Für System Writer wird standardmäßig eine Teilsicherung ausgeführt. Sie können die Option systemstatebackupmethod verwenden, um Gesamtsicherungen von System Writer auszuführen. Weitere Informationen zu dieser Option finden Sie in Systemstatebackupmethod. Der Client sichert alle anderen Ausgabeprogramme immer vollständig.

Dieser Befehl sichert auch ASR-Daten für Windows-Clients; BIOS- und UEFI-Bootarchitekturen werden unterstützt.

Anmerkung:

1. Die Komponente System- und Bootdateien des Systemstatus wird nur gesichert, wenn ein Member (eine Datei) dieser Komponente sich seit der letzten Sicherung geändert hat. Wenn ein Member sich geändert hat, wird die gesamte Gruppe von Dateien, aus denen sich die Komponente zusammensetzt, gesichert.
2. Der Windows-Client für Sichern/Archivieren lässt die Sicherung einzelner Komponenten nicht zu.
3. Systemstatussicherungen werden standardmäßig an die Standardverwaltungsklasse gebunden. Sollen sie an eine andere Verwaltungsklasse gebunden werden, müssen Sie die Option include.systemstate verwenden; geben Sie all als Muster an und geben Sie den Namen der neuen Verwaltungsklasse an.

   Beispiel: `include.systemstate ALL BASVT2.`

4. Verwenden Sie den Befehl query systemstate, um Informationen zu einer Sicherung des Systemstatus auf dem IBM Spectrum Protect-Server anzuzeigen.
5. Es ist nicht mehr möglich, den Systemstatus auf ein System zurückzuschreiben, das noch online ist. Verwenden Sie stattdessen die ASR-basierte Wiederherstellungsmethode zum Zurückschreiben des Systemstatus im Windows PE-Offlinemodus. Weitere Informationen finden Sie in den folgenden Wiki-Artikeln von IBM Spectrum Protect:
   - Best Practices for Recovering Windows Server 2012 and Windows 8
   - Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1

   Wenn Sie versuchen, den Systemstatus mit dem Befehl dsmc restore systemstate über die GUI des Clients für Sichern/Archivieren oder den Web-Client zurückzuschreiben, wird die folgende Nachricht angezeigt:

```
ANS5189E Die Onlinezurückschreibung des Systemstatus ist veraltet. Verwenden Sie die
    Offline-WinPE-Methode für die Ausführung der Zurückschreibung des Systemstatus.
```

Unterstützte Clients

Dieser Befehl ist für alle unterstützten Windows-Clients gültig.

Syntax

```
>>-Backup SYSTEMSTate-------------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task
: Den Systemstatus sichern.

  Befehl: `backup systemstate`

Linux-Betriebssysteme Windows-Betriebssysteme

Backup VM

Mit dem Befehl backup vm können Sie eine Gesamtsicherung einer virtuellen Maschine starten.
Windows-Betriebssysteme
Mit dem Befehl backup vm können Sie sowohl virtuelle Microsoft Hyper-V-Maschinen als auch virtuelle VMware-Maschinen sichern. Die Informationen für jeden Hypervisor werden in einem eigenen Abschnitt bereitgestellt. Wenn Sie eine virtuelle Maschine sichern, die Teil einer

Hyper-V-Konfiguration ist, müssen Sie den Text unter *Virtuelle VMware-Maschinen sichern* nicht lesen. Wenn Sie eine virtuelle VMware-Maschine sichern, müssen Sie den Text unter *Virtuelle Microsoft Hyper-V-Maschinen sichern* nicht lesen.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Virtuelle VMware-Maschinen sichern

Mit dem Befehl backup vm können Sie virtuelle VMware-Maschinen sichern.

Eine oder mehrere virtuelle Maschinen werden durch den Knotenn der IBM Spectrum Protect-Einheit zum Versetzen von Daten gesichert. Als *Knoten der Einheit zum Versetzen von Daten* wird eine Konfiguration bezeichnet, in der der Client für Sichern/Archivieren auf einem vStorage-Sicherungsserver ausgeführt wird und für den Schutz der virtuellen Maschinen auf einem Virtual Center- oder ESX-/ESXi-Server konfiguriert ist. Sie müssen die virtuelle VMware-Maschine konfigurieren, bevor Sie diesen Befehl verwenden. Informationen zur Konfiguration der virtuellen VMware-Maschine befinden sich in Umgebung für Gesamtsicherungen virtueller VMware-Maschinen vorbereiten. .

Bei einer VM-Gesamtsicherung wird eine Sicherungskopie aller virtuellen Plattenimages und Konfigurationsinformationen einer virtuellen Maschine gespeichert. VM-Gesamtsicherungen ermöglichen eine vollständige Zurückschreibung einer virtuellen Maschine, sie erfordern jedoch mehr Zeit und mehr Speicherbereich auf dem Server als eine Teilsicherung.

Wenn Sie die Option vmenabletemplatebackups auf yes setzen, umfasst eine VM-Sicherungsoperation (backup vm) die virtuellen Schablonenmaschinen, vorausgesetzt, der vStorage-Sicherungsserver ist mit einem vCenter-Server und nicht mit einem ESX- oder ESXi-Host verbunden.

Schlägt eine Momentaufnahme während der Sicherungsverarbeitung fehl, unternimmt der Client noch einen Versuch, die virtuelle VMware-Maschine zu sichern. Die Gesamtzahl der Momentaufnahmeversuche können Sie mit der Option INCLUDE.VMSNAPSHOTATTEMPTS in der Clientoptiondatei definieren.

Datenschutztags werden verwendet, um die Sicherungsmaßnahme virtueller Maschinen in VMware-Objekten zu konfigurieren. Die Tags und Kategorien werden erstellt, wenn Sie eine der folgenden Methoden verwenden:

- Aktivieren Sie mit der Option vmtagdatamover die Tagging-Unterstützung auf dem Knoten der Einheit zum Versetzen von Daten und führen Sie den Befehl backup vm aus.
- Verwenden Sie das IBM Spectrum Protect vSphere-Client-Plug-in, um IBM Spectrum Protect-Sicherungen zu verwalten.
- Führen Sie den Befehl set vmtags auf einem beliebigen Knoten einer Einheit zum Versetzen von Daten aus.

Wenn die Option vmtagdatamover auf *yes* gesetzt wird, werden alle Tags, die einer virtuellen Maschine zugeordnet sind, während der Ausführung von Operationen backup vm gesichert. Die Tags werden zurückgeschrieben, wenn der Befehl restore vm ausgeführt wird. Tags, die anderen Bestandsobjekten zugeordnet sind, werden nicht gesichert und können nicht zurückgeschrieben werden.

Weitere Informationen zu Datenschutztags finden Sie in Übersicht über das Datenschutztagging.

Eine VM-Gesamtsicherung verwendet die VMware-Überwachung geänderter Blöcke (Changed Block Tracking, CBT), um inhaltsgesteuerte Sicherungen (nur verwendete Blöcke) zu erstellen. Der Client aktiviert die Überwachung geänderter Blöcke (CBT) auf einem ESX- oder ESXi-Server, wenn eine Sicherung beginnt. Für VMware CBT ist ein Host mit ESX 4.1 (oder höher) und mit virtueller Hardware 7 (oder höher) erforderlich. Sie können keine inhaltsgesteuerten VM-Teilsicherungen oder VM-Gesamtsicherungen auf virtuellen Maschinen ausführen, die CBT nicht unterstützen.

Wenn CBT aktiviert ist, überwacht es Plattenänderungen, wenn der ESX- oder ESXi-Serverspeicherstack E/A-Operationen auf den folgenden Platten verarbeitet:

- Eine im VMFS gespeicherte virtuelle Platte. Die Platte kann eine iSCSI-Platte, eine lokale Platte oder eine Platte in einem SAN sein.
- Eine im NFS gespeicherte virtuelle Platte.
- Eine RDM-Platte, die sich im Modus für virtuelle Kompatibilität befindet.

Wenn der ESX- oder ESXi-Speicherstack keine E/A-Operationen verarbeitet, kann CBT nicht für die Überwachung von Plattenänderungen verwendet werden. Die folgenden Platten können CBT nicht verwenden:

- Eine RDM-Platte, die sich im Modus für physische Kompatibilität befindet.
- Eine Platte, auf die direkt aus einer virtuellen Maschine heraus zugegriffen wird. vSphere kann beispielsweise keine Änderungen an einer iSCSI-LUN überwachen, auf die ein iSCSI-Initiator in der virtuellen Maschine zugreift.

Vollständige Informationen zu den Anforderungen für die Überwachung geänderter Blöcke (Changed Block Tracking, CBT) finden Sie in der Veröffentlichung *VMware Virtual Disk API Programming Guide* in der VMware-Produktdokumentation. Suchen Sie in dem Handbuch nach "Low Level Backup Procedures" und lesen Sie den Abschnitt "Changed Block Tracking on Virtual Disks".
Bei VMware-Servern, die CBT nicht unterstützen, werden sowohl die verwendeten als auch die nicht verwendeten Bereiche der Platte gesichert; außerdem wird eine Informationsnachricht in der Datei dsmerror.log protokolliert. Verwenden Sie die Option -preview im Befehl backup vm, um den aktuellen CBT-Status anzuzeigen. Der CBT-Status hat drei Werte:

Off

Gibt an, dass der CBT-Konfigurationsparameter (ctkEnabled) in den Konfigurationsparametern der virtuellen Maschine nicht aktiviert ist. Off ist der Standardstatus.

Not Supported
: Gibt an, dass die virtuelle Maschine CBT nicht unterstützt. Sicherungen von ausschließlich geänderten Blöcken sind nicht möglich.

On
: Gibt an, dass die virtuelle Maschine CBT unterstützt und dass CBT in den Konfigurationsparametern der virtuellen Maschine aktiviert ist (ctkEnabled=true).
Der Client aktiviert CBT (Einstellung ctkEnable=true) bei jedem Sicherungsversuch. Nachdem der Client CBT aktiviert hat, bleibt es aktiviert, auch wenn die virtuelle Maschine auf dem IBM Spectrum Protect-Server gelöscht wird. Wenn CBT aktiviert ist, werden nach der Ausführung der ersten VM-Gesamtsicherung nur die geänderten Blöcke auf der Platte gesichert oder zurückgeschrieben.
Wenn Sie keine IBM Spectrum Protect-Sicherungen einer virtuellen Maschine mehr ausführen, können Sie CBT inaktivieren. Für die Inaktivierung von CBT klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, für die Sie CBT im vSphere-Client inaktivieren wollen. Klicken Sie auf Einstellungen editieren > Optionen > Allgemein > Konfigurationsparameter. Setzen Sie dann den Konfigurationsparameter ctkEnabled auf `false`.

Tipp: Sie können die Komprimierungsoption nur dann für Sicherungen verwenden, wenn die Sicherung in einem Speicherpool gespeichert wird, der für die clientseitige Deduplizierung aktiviert wurde.

Windows-BetriebssystemeWeitere Informationen zur Komprimierung finden Sie in Komprimierungs- und Verschlüsselungsverarbeitung.

Windows-BetriebssystemeLinux-BetriebssystemeSie können die Optionen -vmbackuptype und -mode angeben, um festzulegen, wie die Sicherungen ausgeführt werden sollen. Verwenden Sie für VM-Gesamtsicherungen `-vmbackuptype=fullvm` und geben Sie eine der folgenden Optionen für den Modus an:

IFFull
: Modus 'Immer inkrementell - Vollständig'. In diesem Modus wird eine Momentaufnahme aller verwendeten Blöcke auf den Platten einer virtuellen Maschine auf dem Server gesichert. Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware oder IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

IFIncremental
: Immer inkrementell - Inkrementell. In diesem Modus wird eine Momentaufnahme erstellt, die aus den Blöcken besteht, die sich seit der letzten Sicherung geändert haben. Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware oder IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Informationen zur Sicherungsstrategie "Immer inkrementell" finden Sie in IBM Spectrum Protect for Virtual Environments, Data Protection for VMware: Sicherungs- und Zurückschreibungstypen.

Unterstützte Clients

Windows-BetriebssystemeDieser Befehl ist auf unterstützten Windows-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind, der virtuelle VMware-Maschinen schützt.

Linux-BetriebssystemeDieser Befehl ist nur auf unterstützten Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind, der virtuelle VMware-Maschinen schützt.

Syntax

```
                .-,-------.
                V         |
              .---VM-Name-+-.
>>-Backup VM--+-------------+-----------------------------------><

>--+---------------------------------------+---------------------><
   | .-,-------------------------------. |
   | V                                 | |
   '---VM-Name--:vmdk=--Plattenkennsatz-+-'

>--+----------------------+--+------------------------+--------><
   '- -VMBACKUPUPDATEGUID-'  '- -PREView-- --Optionen-'
```

Parameter

VM-Name
: Geben Sie den Namen einer virtuellen Maschine oder die Namen mehrerer virtueller Maschinen an, die gesichert werden soll(en). Der Name ist der Anzeigename der virtuellen Maschine. Trennen Sie die Namen mehrerer virtueller Maschinen durch Kommas. Wenn Sie die Option vmenabletemplatebackups auf yes gesetzt haben, kann *VM-Name* den Namen einer virtuellen Schablonenmaschine angeben, die gesichert werden soll.

  In VMware vCenter dürfen zwei oder mehr virtuelle Maschinen denselben Anzeigenamen haben. Für den Client für Sichern/Archivieren müssen jedoch alle Namen virtueller Maschinen in einer vCenter-Serverkonfiguration eindeutig sein. Damit während der Verarbeitung

keine Fehler auftreten, stellen Sie sicher, dass alle virtuellen Maschinen einen eindeutigen Anzeigenamen haben.

In den Namen virtueller Maschinen, die in diesem Parameter angegeben werden, können Platzhalterzeichen verwendet werden. Die Verarbeitung von Platzhalterzeichen unterscheidet sich jedoch je nach dem verwendeten Sicherungsmodus.

- Für Sicherungen mit den Optionen `mode=iffull` und `mode=ifincremental` können Platzhalterzeichen bei VM-Namensmustern verwendet werden. Zum Beispiel:
  - `backup vm VM_TEST*` umfasst alle virtuellen Maschinen, deren Name mit VM_TEST beginnt.
  - `backup vm VM??` umfasst alle virtuellen Maschinen, deren Name mit den Buchstaben "VM" beginnt, gefolgt von 2 beliebigen Zeichen.

Wenn Sie *VM-Name* nicht angeben, können Sie die virtuelle Maschine mit der Option domain.vmfull identifizieren.

:vmdk=*Plattenkennsatz*

Dieses Schlüsselwort ist eine Erweiterung von *VM-Name*. Es gibt den Kennsatz (Namen) der Platte der virtuellen Maschine an, die in die Sicherungsoperation eingeschlossen werden soll. Sie können eine Platte ausschließen, indem Sie dem Schlüsselwort den Ausschlussoperator (-) voranstellen. Weitere Methoden zum Einschließen oder Ausschließen von Platten für die Verarbeitung finden Sie in Domain.vmfull, Exclude.vmdisk, Include.vmdisk.

-VMBACKUPUPDATEGUID

Für diese Option benötigen Sie eine Lizenzvereinbarung für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Mit dieser Option wird die global eindeutige ID (GUID) für die zu sichernde virtuelle Maschine aktualisiert. Dieser Parameter ist ausschließlich für die Verwendung in dem folgenden Szenario vorgesehen:

Sie möchten eine bereits gesicherte virtuelle Maschine mit dem Namen ORION zurückschreiben. Bevor Sie jedoch das System herunterfahren und die in der Produktionsumgebung ausgeführte Kopie von ORION durch die zurückgeschriebene Kopie ersetzen, möchten Sie die Konfiguration der zurückgeschriebenen virtuellen Maschine überprüfen.

1. Sie schreiben die virtuelle Maschine ORION zurück und ordnen ihr einen neuen Namen zu: `dsmc restore vm Orion -vmname=Orion2`.
2. Sie aktualisieren und überprüfen die virtuelle Maschine ORION2 und stellen fest, dass sie die vorhandene virtuelle Maschine mit dem Namen ORION ersetzen kann.
3. Sie schalten das System aus und löschen ORION.
4. Sie benennen ORION2 in ORION um.
5. Bei der nächsten Sicherung von ORION mit einer immer inkrementellen Gesamtsicherung oder einer immer inkrementellen Teilsicherung fügen Sie dem Befehl backup vm den Parameter -VMBACKUPUPDATEGUID hinzu. Durch diese Option wird die GUID auf dem IBM Spectrum Protect-Server aktualisiert, sodass die neue GUID den gespeicherten Sicherungen für die virtuelle Maschine ORION zugeordnet ist. Die Kette der Teilsicherungen bleibt erhalten; es ist nicht erforderlich, vorhandene Sicherungen zu löschen und durch neue Sicherungen zu ersetzen.

-PREView

Diese Option zeigt Informationen zu einer virtuellen Maschine an, einschließlich der Kennsätze der Festplatten in der virtuellen Maschine und der Verwaltungsklasseninformationen für eine virtuelle Maschine.

Sie können die Plattenkennsätze mit den Schlüsselwörtern `:vmdk=` oder `:-vmdk=` verwenden, um Platten bei einer Sicherungsoperation ein- oder auszuschließen. Das folgende Beispiel zeigt Ausgabe vom Parameter -preview:

```
backup vm vm1 -preview
Gesamtsicherung der virtuellen Maschine 'VM1'

vmName:vm1
VMDK[1]Label: Hard disk 1
VMDK[1]Name: [ds5k_svt_1] tsmcetlnx14/tsmcetlnx14.vmdk
VMDK[1]Status: Included
VMDK[2]Label: Hard disk 2
VMDK[2]Name: [ds5k_svt_1] tsmcetlnx14/tsmcetlnx14_1.vmdk
VMDK[2]Status: Excluded - user,Independent,pRDM
```

Diese `-preview`-Beispielausgabe zeigt, dass VMDK2 von der vorherigen Sicherung ausgeschlossen war. In eine Sicherung eingeschlossene Platten haben den Status `Included` (Eingeschlossen). Von der Sicherung ausgeschlossene Platten haben den Status `Excluded` (Ausgeschlossen), an den sich ein Ursachencode anschließt. Folgende Ursachencodes sind möglich:

user
: Gibt an, dass die Platte übersprungen wurde, weil sie in einer Anweisung domain.vmfull, in der Befehlszeile oder in der Clientoptionsdatei ausgeschlossen wurde.

Independent
: Gibt an, dass die Platte eine unabhängige Platte ist. Unabhängige Platten können nicht Teil einer Momentaufnahme sein, daher werden sie bei VM-Sicherungsoperationen (backup vm) ausgeschlossen. Stellen Sie sicher, dass die Option vmprocessvmwithindependent auf 'yes' gesetzt ist. Andernfalls wird die gesamte virtuelle Maschine bei einer Sicherungsoperation übergangen, wenn sie eine oder mehrere unabhängige Platten enthält.

pRDM
: Gibt an, dass die Platte eine pRDM-Platte ist (pRDM = physical Raw Device Mapping). pRDM-Platten können nicht Teil einer Momentaufnahme sein, daher werden sie bei VM-Sicherungsoperationen (backup vm) ausgeschlossen. Stellen Sie sicher, dass die

Option vmprocessvmwithprdm auf 'yes' gesetzt ist. Andernfalls wird die gesamte virtuelle Maschine von einer Sicherungsoperation übergangen, wenn sie mindestens einen RDM-Datenträger enthält, der im Modus für physische Kompatibilität (pRDM) bereitgestellt wird (RDM = Raw Device Mapping).

In der Ausgabe des Parameters -preview wird auch der Name der Verwaltungsklasse angezeigt, die der virtuellen Maschine zugeordnet ist, sowie Informationen dazu, wo die Verwaltungsklasse definiert wurde. Mithilfe dieser Informationen können Sie überprüfen, ob die Domänen- und Tagwerte für die Verwaltungsklasse korrekt definiert sind. Beispiel:

```
backup vm -preview
Full BACKUP VM der virtuellen Maschinen, die in der Option DOMAIN.VMFULL angegeben sind.

  1. vmName: tag_vm_2
       DomainKeyword:  all-vm
       toolsRunningStatus: guestToolsNotRunning
       toolsVersionStatus: guestToolsNotInstalled
       consolidationNeeded: No
       Change Block Tracking: On
       managementClassName: STANDARD
       managementClassLocation: Node Default

       VMDK[1]Label:   'Hard disk 1' (Hard Disk 1)
       VMDK[1]Name:    '[Raid1-lannds2] tag_vm_2/tag_vm_2.vmdk'
       VMDK[1]Status:  Included
...

12. vmName: vm-jean
       DomainKeyword:  all-vm
       toolsRunningStatus: guestToolsNotRunning
       toolsVersionStatus: guestToolsNotInstalled
       consolidationNeeded: No
       Change Block Tracking: On
       managementClassName: MGMTCLASS1 (invalid)
       managementClassLocation: VM Tag Management Class (IBM Spectrum Protect)

       VMDK[1]Label:   'Hard disk 1' (Hard Disk 1)
       VMDK[1]Name:    '[Raid1-lannds2] vm-jean/vm-jean.vmdk'
       VMDK[1]Status:  Included
```

Hierbei gilt Folgendes:

managementClassName
: Zeigt den Namen der Verwaltungsklasse an, an die die virtuelle Maschine gebunden ist.

  Wird neben dem Namen der Verwaltungsklasse "(invalid)" (ungültig) angezeigt, wurde entweder der Name falsch angegeben oder die Verwaltungsklasse auf dem IBM Spectrum Protect-Server entfernt oder keine Sicherungskopiengruppe in der Verwaltungsklasse auf dem Server gefunden. Wenn der Name der Verwaltungsklasse ungültig ist, schlägt die Sicherungsoperation für die virtuelle Maschine fehl.

managementClassLocation
: Zeigt an, wo die Verwaltungsklasse definiert wurde. Die folgenden Positionen sind möglich:

  Node Default
  : Die Verwaltungsklasse wurde in der Standarddomäne des VMware-Datencenterknotens definiert.

  VMMC option
  : Die Verwaltungsklasse wurde mit der Option vmmc definiert.

  VMCTLMC option
  : Die Verwaltungsklasse wurde mit der Option vmctlmc definiert.

  INCLUDE.VM option
  : Die Verwaltungsklasse wurde mit der Option include.vm definiert.

  VM Tag Management Class (IBM Spectrum Protect)
  : Die Verwaltungsklasse wurde als Tagwert der Tagkategorie `Management Class (IBM Spectrum Protect)` definiert. Tagwerte können mit Datenschutzeinstellungen im IBM Spectrum Protect vSphere-Client-Plug-in im vSphere-Web-Client oder mithilfe von Tools wie beispielsweise VMware vSphere PowerCLI Version 5.5 R2 oder höher festgelegt werden.

Wichtig: Um die durch Tags definierten Verwaltungsklasseninformationen anzuzeigen, müssen Sie die Option vmtagdatamover yes in der Clientoptionsdatei definieren oder den Parameter -vmtagdatamover=yes einschließen, wenn Sie den Befehl dsmc backup vm ausführen. Wenn Sie die Option vmtagdatamover nicht definiert haben oder die Option auf no gesetzt haben, ignoriert der Client alle Tagwerte für die Verwaltungsklasse und zeigt die Verwaltungsklassendefinition an, die in der Standarddomäne des Datencenterknotens, in der Option vmmc oder in der Option include.vm definiert ist.

Rückkehrcodes für Sicherungsoperationen für virtuelle Maschinen

Bei der Beendigung von Sicherungsoperationen für virtuelle Maschinen können die Rückkehrcodes ausgegeben werden, die in der folgenden Tabelle enthalten sind.

Rückkehrcode	Beschreibung

Rückkehrcode	Beschreibung
0	Ein Befehl zum Sichern einer oder mehrerer virtueller Maschinen wurde erfolgreich ausgeführt.
8	Ein Befehl zum Sichern mehrerer virtueller Maschinen wurde nur für einige der virtuellen Maschinen, für die der Befehl galt, erfolgreich ausgeführt. Der Protokolldatei können Sie den Verarbeitungsstatus jeder der virtuellen Maschinen entnehmen, für die der Befehl galt.
12	Gibt an, dass eine der folgenden Fehlerbedingungen aufgetreten ist: • Durch den Sicherungsbefehl konnte keine der virtuellen Maschinen gesichert werden, die Ziele der Sicherungsoperation waren. • Der Sicherungsbefehl ist fehlgeschlagen und wurde gestoppt, bevor alle angegebenen virtuellen Maschinen überprüft wurden. Untersuchen Sie die Protokolldatei, um die Fehlerursache festzustellen.

vStorage API for Data Protection - Beispielbefehle

Eine IFIncremental-Sicherung zweier VMs mit den Namen vm3 und vm4 ausführen.

```
dsmc backup vm vm3,vm4 -vmbackuptype=fullvm -mode=ifincremental
```

Eine IFFull-Sicherung einer VM mit dem Namen vm1 ausführen.

```
dsmc backup vm vm1 -vmbackuptype=fullvm -mode=iffull
```

Eine IFFull-Sicherung einer VM mit dem Namen vm1 ausführen, aber nur 'Festplatte 1' in die Sicherungsoperation einschließen.

```
dsmc backup vm "vm1:vmdk=Festplatte 1" -vmbackuptype=fullvm -mode=iffull
```

Eine immer inkrementelle Sicherung der virtuellen Maschine vm1 ausführen, 'Festplatte 1' und 'Festplatte 4' jedoch von der Sicherungsoperation ausschließen.

```
dcmc backup vm "vm1:-vmdk=Festplatte 1:-vmdk=Festplatte 4"
  -vmbackuptype=fullvm -mode=iffull
```

Eine immer inkrementelle Gesamtsicherung der virtuellen Maschinen mit den Namen vm1 und vm2 ausführen. Auf vm1 nur 'Festplatte 2' und 'Festplatte 3' sichern. Auf vm2 alle virtuellen Platten sichern.

```
dsmc backup vm "vm1:vmdk=Festplatte 2:vmdk=Festplatte 3",
  vm2 -vmbackuptype=fullvm -mode=iffull
```

Parallele immer inkrementelle Gesamtsicherungen der virtuellen VMware-Maschinen ausführen, die mithilfe der Auswahlkriterien (Domänenparameter) in der Anweisung domain.vmfull für die Sicherung ausgewählt werden. Die maximale Anzahl paralleler Sicherungen auf 5 virtuelle Maschinen und 10 Sitzungen setzen und die Sicherungen auf 5 virtuelle Maschinen pro Host und 5 virtuelle Maschinen pro Datenspeicher begrenzen.

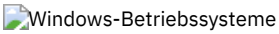
```
dsmc backup vm -vmbackuptype=fullvm -mode=iffull -vmmaxparallel=5
  -vmmaxbackupsessions=10 -vmlimitperhost=5 -vmlimitperdatastore=5
```

Linux-BetriebssystemeWindows-Betriebssysteme

Zugehörige Links für die Sicherung virtueller VMware-Maschinen

- Query VM
- Restore VM
- Domain.vmfull
- Include.vm
- Mbobjrefreshthresh
- Mbpctrefreshthresh
- Mode
- Vmbackdir
- Vmbackuplocation
- Vmbackuptype
- Vmchost
- Vmctlmc
- Vmcpw
- Vmcuser
- Vmlimitperdatastore
- Vmlimitperhost
- Vmmc
- Vmmaxbackupsessions
- Vmmaxparallel
- Vmtagdatamover

- Set vmtags
- Ausschlussoptionen für virtuelle Maschinen
- Einschlussoptionen für virtuelle Maschinen


Windows-Betriebssysteme

Virtuelle Microsoft Hyper-V-Maschinen sichern

Verwenden Sie den Befehl backup vm, um virtuelle Hyper-V-Maschinen zu sichern. Sie können Hyper-V-Gastmaschinen sichern, die auf einer lokalen Platte, auf einer an ein SAN angeschlossenen Platte oder auf einem freigegebenen Clusterdatenträger (Clustervolume) vorhanden sind, oder Gastmaschinen, die sich in einer fernen Dateiserverfreigabe befinden. Ferne Dateiserverfreigaben müssen sich auf einem System mit Windows Server 2012 oder höher befinden.

Sie geben den zu verwendenden Sicherungsmodus an, wenn Sie eine virtuelle Maschine sichern möchten, indem Sie den Parameter -mode in der Befehlszeile angeben. Sie können die Option mode auch in der Clientoptionsdatei definieren. Jeder der folgenden Modi kann angegeben werden:

IFFull
: Modus 'Immer inkrementell - Vollständig'. In diesem Modus wird eine Momentaufnahme aller verwendeten Blöcke auf den Platten einer virtuellen Maschine auf dem Server gesichert. Die Sicherung umfasst Konfigurationsinformationen und alle Platten. Für die Verwendung dieses Modus benötigen Sie eine Lizenz für IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V. Dieser Modus kann nur auf Windows-Clients auf Hyper-V-Hosts verwendet werden, die in Umgebungen mit Windows Server 2012 oder höher ausgeführt werden.

IFIncremental
: Immer inkrementell - Inkrementell. In diesem Modus wird eine Momentaufnahme erstellt, die aus den Blöcken besteht, die seit der letzten Sicherung geändert wurden. Die Sicherung umfasst Konfigurationsinformationen und alle Platten. Für die Verwendung dieses Modus benötigen Sie eine Lizenz für IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V. Dieser Modus kann nur auf Windows-Clients auf Hyper-V-Hosts verwendet werden, die in Umgebungen mit Windows Server 2012 oder höher ausgeführt werden.

Informationen zur Sicherungsstrategie "Immer inkrementell" finden Sie in Sicherungsstrategie "Immer inkrementell".

Unterstützte Clients

Dieser Befehl ist auf unterstützten Windows-Clients gültig, die auf einem Microsoft Hyper-V-Host-Server installiert sind.

Syntax

```
                .-,-------.
               V          |
             .---VM-Name-+-.
>>-Backup VM--+-------------+--+---------------------------------------+-->
                              | .-,-------------------------------. |
                              | V                                 | |
                              '---VM-Name--:vhdx=--Plattenposition-+-'

             .-IFIncremental-.
>-- -MODE = -+---------------+-----------------------------------><
             '-IFFull--------'

>--+----------------------+--+-----------+--+------------------------+-><
   '- -VMBACKUPUPDATEGUID-'  '- -PREview-'  '- -DETail-- --Optionen-'
```

Parameter

VM-Name
: Geben Sie den Namen der virtuellen Maschine an, die gesichert werden soll. Dabei muss die Groß-/Kleinschreibung beachtet werden. Wenn Sie mehrere Namen virtueller Maschinen angeben, müssen Sie die Namen durch Kommas trennen.
In den Namen virtueller Maschinen, die in diesem Parameter angegeben werden, können Platzhalterzeichen verwendet werden. Die Verarbeitung von Platzhalterzeichen unterscheidet sich jedoch je nach dem verwendeten Sicherungsmodus.

  - Für Sicherungen mit den Optionen `mode=iffull` und `mode=ifincremental` können Platzhalterzeichen bei VM-Namensmustern verwendet werden. Zum Beispiel:
    - `backup vm VM_TEST*` umfasst alle virtuellen Maschinen, deren Name mit VM_TEST beginnt.
    - `backup vm VM??` umfasst alle virtuellen Maschinen, deren Name mit den Buchstaben "VM" beginnt, gefolgt von 2 beliebigen Zeichen.

    Geben Sie keinen Namen der virtuellen Maschine an und geben Sie `-mode=ifincremental` oder `-mode=iffull` an, wird anhand der Option domain.vmfull ermittelt, welche virtuellen Maschinen in die Sicherungsoperation einzuschließen sind.

VM-Name:vhdx=*Plattenposition*

Dieser Parameter gibt die Festplatte der virtuellen Maschine (VHDX) an, die in Hyper-V-RCT-VM-Sicherungsoperationen unter Windows Server 2016 eingeschlossen werden soll.

Die Variable *VM-Name* gibt den Namen der zu sichernden VM an. Für die Auswahl von VM-Namen, die einem Muster entsprechen, können Platzhalterzeichen verwendet werden. Ein Stern (*) entspricht einer beliebigen Zeichenfolge. Ein Fragezeichen (?) entspricht einem beliebigen einzelnen Zeichen.

Das Schlüsselwort :vhdx=*Plattenposition* gibt die Position der VM-Platte an, die in die Sicherungsoperation eingeschlossen werden soll. Die Plattenposition wird im Format "*Controllertyp Controllernummer Plattenpositionsnummer_im_Controller*" angegeben. Der Controllertyp muss "SCSI" oder "IDE" lauten. Beispiel:

```
dsmc backup vm "vm1:VHDX=IDE 1 0"
```

Die Informationen über die Plattenposition können Sie im Hyper-V Manager abrufen. Klicken Sie in der Sicht Virtuelle Maschinen mit der rechten Maustaste auf eine virtuelle Maschine und mit der linken Maustaste auf Einstellungen. Suchen Sie im Abschnitt Hardware des Fensters Einstellungen den IDE-Controller oder den SCI-Controller und klicken Sie auf Festplatte, um die Festplatteneinstellungen anzuzeigen. Die Controllernummer und die Plattenposition werden in den Feldern Controller und Position angezeigt. Sie können die Informationen über die Plattenposition auch mit dem Windows PowerShell-Cmdlet Get-VMHardDiskDrive abrufen.

Sie können eine VM-Platte von Sicherungsoperationen ausschließen, indem Sie den Ausschlussoperator (-) vor dem Schlüsselwort vhdx= angeben. Verwenden Sie beispielsweise -vhdx=, um eine VM-Platte von der Sicherungsoperation für eine VM auszuschließen:

```
dsmc backup vm "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

Wenn Sie mehrere einzuschließende oder auszuschließende VM-Platten angeben, müssen das Schlüsselwort vhdx= bzw. -vhdx= und die zugehörigen Werte durch Doppelpunkte ohne Zwischenleerschritte voneinander getrennt werden. Beispiel:

```
dsmc backup vm "*:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

Wenn Sie mehrere VM-Namen und VM-Platten angeben, müssen der VM-Name und die zugehörigen Werte durch Semikolons ohne Zwischenleerschritte voneinander getrennt werden. Beispiel:

```
dsmc backup vm "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1;vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

-VMBACKUPUPDATEGUID

Für diese Option benötigen Sie eine Lizenz für die Verwendung von IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Mit dieser Option wird die global eindeutige ID (GUID) für die zu sichernde virtuelle Maschine aktualisiert. Dieser Parameter ist ausschließlich für die Verwendung in dem folgenden Szenario vorgesehen:

Sie möchten eine bereits gesicherte virtuelle Maschine mit dem Namen ORION zurückschreiben. Bevor Sie jedoch das System herunterfahren und die in der Produktionsumgebung ausgeführte Kopie von ORION durch die zurückgeschriebene Kopie ersetzen, möchten Sie die Konfiguration der zurückgeschriebenen virtuellen Maschine überprüfen.

1. Sie schreiben die virtuelle Maschine ORION zurück und ordnen ihr einen neuen Namen zu: `dsmc restore vm Orion -vmname=Orion2`.
2. Sie aktualisieren und überprüfen die virtuelle Maschine ORION2 und stellen fest, dass sie die vorhandene virtuelle Maschine mit dem Namen ORION ersetzen kann.
3. Sie schalten das System aus und löschen ORION.
4. Sie benennen ORION2 in ORION um.
5. Bei der nächsten Sicherung von ORION mit einer immer inkrementellen Gesamtsicherung oder einer immer inkrementellen Teilsicherung fügen Sie dem Befehl backup vm den Parameter -VMBACKUPUPDATEGUID hinzu. Durch diese Option wird die GUID auf dem IBM Spectrum Protect-Server aktualisiert, sodass die neue GUID den gespeicherten Sicherungen für die virtuelle Maschine ORION zugeordnet ist. Die Kette der Teilsicherungen bleibt erhalten; es ist nicht erforderlich, vorhandene Sicherungen zu löschen und durch neue Sicherungen zu ersetzen.

-PREView

Mit diesem Parameter werden zusätzliche Informationen zu einer virtuellen Maschine angezeigt, einschließlich der Kennsätze der virtuellen Festplatten in der virtuellen Maschine.
Wenn Sie die Option -preview ausgeben, wird die Sicherungsoperation nicht gestartet. Sie müssen den Sicherungsbefehl ohne die Option -preview ausgeben, um die Sicherungsoperation zu starten.
In dem Befehl können Sie sowohl die Option -preview als auch die Option -detail angeben, um Informationen zu Unterplatten anzuzeigen, die bei der Ausführung der Sicherung eingeschlossen werden. Eine Unterplatte ist die AVHDX-Datei, die bei der Erstellung einer Momentaufnahme von einer VHDX-Datei erstellt wird.

Rückkehrcodes für Sicherungsoperationen für virtuelle Maschinen

Bei der Beendigung von Sicherungsoperationen für virtuelle Maschinen können die Rückkehrcodes ausgegeben werden, die in der folgenden Tabelle enthalten sind.

Rückkehrcode	Beschreibung
0	Ein Befehl zum Sichern einer oder mehrerer virtueller Maschinen wurde erfolgreich ausgeführt.

Rückkehrcode	Beschreibung
8	Ein Befehl zum Sichern mehrerer virtueller Maschinen wurde nur für einige der virtuellen Maschinen, für die der Befehl galt, erfolgreich ausgeführt. Der Protokolldatei können Sie den Verarbeitungsstatus jeder der virtuellen Maschinen entnehmen, für die der Befehl galt.
12	Gibt an, dass eine der folgenden Fehlerbedingungen aufgetreten ist: • Durch den Sicherungsbefehl konnte keine der virtuellen Maschinen gesichert werden, die Ziele der Sicherungsoperation waren. • Der Sicherungsbefehl ist fehlgeschlagen und wurde gestoppt, bevor alle angegebenen virtuellen Maschinen überprüft wurden. Untersuchen Sie die Protokolldatei, um die Fehlerursache festzustellen.

Microsoft Hyper-V-Sicherungsbeispiele

Eine immer inkrementelle Teilsicherung einer virtuellen Hyper-V-Maschine mit dem Namen "VM1" starten.

```
dsmc backup vm VM1 -mode=ifincremental
```

Eine immer inkrementelle Teilsicherung aller virtuellen Hyper-V-Maschinen starten, die in der Option domain.vmfull angegeben sind.

```
dsmc backup vm -mode=ifincremental
```

Für Betriebssysteme Windows Server 2016 oder Betriebssysteme einer höheren Version: Mit dem folgenden Befehl werden eine IDE-Platte (mit Controllernummer 1 und Plattenposition 0) und eine SCSI-Platte (mit Controllernummer 0 und Plattenposition 1) von einer immer inkrementellen Hyper-V-RCT-Teilsicherung der virtuellen Maschine "vm2" ausgeschlossen.

```
dsmc backup vm "vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1" -mode=ifincremental
```

Für Betriebssysteme Windows Server 2016 oder Betriebssysteme einer höheren Version: Mit dem folgenden Befehl wird eine Voranzeige einer Hyper-V-RCT-Sicherung der virtuellen Maschine "VM05" aufgerufen:

```
dsmc backup vm VM05 -mode=ifincremental -preview
```

In der Befehlsausgabe werden für den Parameter -preview die VHDX-Kennsätze in der virtuellen Maschine angezeigt. Wenn der Parameter -detail zusammen mit dem Parameter -preview angegeben wird, werden für Hyper-V-RCT-Sicherungen keine zusätzlichen Informationen angezeigt.

```
Befehl 'Backup VM' gestartet. Gesamtzahl zu verarbeitender VMs: 1

  1. VM-Name: VM05

        Domänenschlüsselwort:   VM05
        Modus:                  Immer inkrementell - Inkrementell
        Name des Zielknotens:   NODE14
        Knotenname der Einheit zum Versetzen von Daten: NODE14
        Clusterressource:       Nein

        Platte[1]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05.vhdx
        Kapazität:              15,00 GB
        Größe:                  10,91 GB
        Status:                 Eingeschlossen
        Plattentyp:             VHDX
        Nummer der Unterplatte: 0
        Controllerposition:     IDE 0 0

        Platte[2]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05_Disk2.vhdx
        Kapazität:              2,00 GB
        Größe:                  132,00 MB
        Status:                 Eingeschlossen
        Plattentyp:             VHDX
        Nummer der Unterplatte: 0
        Controllerposition:     SCSI 0 1

Gesamtzahl verarbeiteter virtueller Maschinen: 1
```

Für Windows Server 2012 oder 2012 R2: Mit dem folgenden Befehl wird eine immer inkrementelle Teilsicherung der virtuellen Hyper-V-Maschine "VM3" gestartet:

```
dsmc backup vm VM3 -mode=ifincremental -preview
```

In der Befehlsausgabe werden für den Parameter -preview die VHDX-Kennsätze in der virtuellen Maschine angezeigt:

```
VM-Name: VM3

        Domänenschlüsselwort:   all-vm
```

```
        Modus:                  Immer inkrementell - Inkrementell
        Name des Zielknotens:   NODE1
        Knotenname der Einheit zum Versetzen von Daten: NODE1
        Clusterressource:       Ja

        Platte[1]
        Name: c:\ClusterStorage\Volume1\Hyper-V\VM3\VM3.VHDX
        Kapazität:              40,00 GB
        Größe:                  9,09 GB
        Gesamtsicherung:        Eingeschlossen
        Teilsicherung:          Ausgeschlossen
        Plattentyp:             VHDX
        Nummer der Unterplatte: 1

        Platte[2]
        Name: c:\ClusterStorage\Volume3\Hyper-V\VM3\VM3-DISK2.VHDX
        Kapazität:              127,00 GB
        Größe:                  4,00 MB
        Gesamtsicherung:        Eingeschlossen
        Teilsicherung:          Ausgeschlossen
        Plattentyp:             VHDX
        Nummer der Unterplatte: 1
```

Wenn der Parameter -detail zusammen mit dem Parameter -preview angegeben wird, werden die VHDX-Kennsätze und ihre Unterplatten angezeigt. Die folgende Beispielausgabe wurde abgekürzt, sodass sie nur Informationen zu einer einzigen virtuellen Maschine und Platte zeigt:

```
VM-Name: VM3

        Domänenschlüsselwort:   all-vm
        Modus:                  Immer inkrementell - Inkrementell
        Name des Zielknotens:   NODE1
        Knotenname der Einheit zum Versetzen von Daten: NODE1
        Clusterressource:       Ja

        Platte[1]
        Name: c:\ClusterStorage\Volume1\Hyper-V\VM3\VM3.VHDX
        Kapazität:              40,00 GB
        Größe:                  9,09 GB
        Gesamtsicherung:        Eingeschlossen
        Teilsicherung:          Ausgeschlossen
        Plattentyp:             VHDX
        Nummer der Unterplatte: 1

        Unterplatte[1]
        Name: c:\ClusterStorage\Volume1\Hyper-V\VM3\VM3_9B26166-9C3E.avhdx
        Kapazität:              40,00 GB
        Größe:                  1,25 GB
        Gesamtsicherung:        Eingeschlossen
        Teilsicherung:          Eingeschlossen
        Plattentyp:             AVHDX
```

Beispiele für Hyper-V-Optionsdatei

In dem folgenden Beispiel werden einzelne virtuelle Maschinen in der Clientoptionsdatei angegeben und die Option domain.vmvull wird gezeigt.

```
domain.vmfull vm1,vm2,vm5
```

In den folgenden Beispielen werden mithilfe der Option domain.vmfull bestimmte virtuelle Maschinen verarbeitet.

Für Betriebssysteme Windows Server 2016 oder Betriebssysteme einer höheren Version: In dem folgenden Beispiel wird die Option domain.vmfull wie folgt angegeben:

```
domain.vmfull VM04,VM05
```

Mit dem folgenden Befehl wird eine Voranzeige einer Hyper-V-RCT-Sicherung aller virtuellen Maschinen, die in der Option domain.vmfull angegeben sind, aufgerufen. Mit dem Befehl werden Voranzeigeinformationen zu jeder virtuellen Maschine aufgerufen:

```
dsmc backup vm -mode=iffull -preview
```

Die folgende Ausgabe wird angezeigt:

```
Befehl 'Backup VM' gestartet. Gesamtzahl zu verarbeitender VMs: 2

  1. VM-Name: VM04

        Domänenschlüsselwort:   VM04
        Modus:                  Immer inkrementell - Vollständig
        Name des Zielknotens:   NODE14
        Knotenname der Einheit zum Versetzen von Daten: NODE14
        Clusterressource:       Nein
```

```
        Platte[1]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM04\Virtual Hard Disks\VM04.vhdx
        Kapazität:              36,00 GB
        Größe:                  9,16 GB
        Status:                 Eingeschlossen
        Plattentyp:             VHDX
        Nummer der Unterplatte: 0
        Controllerposition:     IDE 0 0

  2. VM-Name: VM05

        Domänenschlüsselwort:   VM05
        Modus:                  Immer inkrementell - Vollständig
        Name des Zielknotens:   NODE14
        Knotenname der Einheit zum Versetzen von Daten: NODE14
        Clusterressource:       Nein

        Platte[1]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05.vhdx
        Kapazität:              15,00 GB
        Größe:                  10,91 GB
        Status:                 Eingeschlossen
        Plattentyp:             VHDX
        Nummer der Unterplatte: 0
        Controllerposition:     IDE 0 0

        Platte[2]
        Name: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05_Disk2.vhdx
        Kapazität:              2,00 GB
        Größe:                  132,00 MB
        Status:                 Eingeschlossen
        Plattentyp:             VHDX
        Nummer der Unterplatte: 0
        Controllerposition:     SCSI 0 1

Gesamtzahl verarbeiteter virtueller Maschinen: 2
```

Für Windows Server 2012 oder 2012 R2: In dem folgenden Beispiel gibt die Option domain.vmfull diese virtuellen Maschinen an:

```
domain.vmfull BigVM,myGentoox64,HPV2VM3-OLD,Local10
```

Mit dem folgenden Befehl wird eine Voranzeige einer immer inkrementellen Teilsicherungsoperation für alle virtuellen Hyper-V-Maschinen, die in der Option domain.vmfull angegeben sind, aufgerufen. Mit dem Befehl werden Voranzeigeinformationen zu jeder virtuellen Maschine aufgerufen:

```
dsmc backup vm -mode=iffull -preview
```

Die folgende Ausgabe wird angezeigt:

```
1. VM-Name: BigVM

        Domänenschlüsselwort:   all-vm
        Modus:                  Immer inkrementell - Vollständig
        Name des Zielknotens:   MSF
        Knotenname der Einheit zum Versetzen von Daten: MSF
        Clusterressource:       Nein

        Platte[1]
        Name: \\lingonberry\c$\Users\michael\Documents\Storage\BigVM.vhdx
        Kapazität:              5,85 TB
        Größe:                  5,00 MB
        Gesamtsicherung:        Eingeschlossen
        Teilsicherung:          Ausgeschlossen
        Plattentyp:             VHDX
        Nummer der Unterplatte: 0

2. VM-Name: Gentoox64

        Domänenschlüsselwort:   all-vm
        Modus:                  Immer inkrementell - Vollständig
        Name des Zielknotens:   MSF
        Knotenname der Einheit zum Versetzen von Daten: MSF
        Clusterressource:       Nein

3. VM-Name: HPV2VM3-OLD

        Domänenschlüsselwort:   all-vm
        Modus:                  Immer inkrementell - Vollständig
        Name des Zielknotens:   MSF
        Knotenname der Einheit zum Versetzen von Daten: MSF
        Clusterressource:       Nein

4. VM-Name: Local10
```

```
          Domänenschlüsselwort:   all-vm
          Modus:                  Immer inkrementell - Vollständig
          Name des Zielknotens:   MSF
          Knotenname der Einheit zum Versetzen von Daten: MSF
          Clusterressource:       Nein

          Platte[1]
          Name: \\lingonberry\c$\Users\michael\Documents\Storage\Local10.vhdx
          Kapazität:              127,00 GB
          Größe:                  4,00 MB
          Gesamtsicherung:        Eingeschlossen
          Teilsicherung:          Ausgeschlossen
          Plattentyp:             VHDX
          Nummer der Unterplatte: 0

Gesamtzahl verarbeiteter virtueller Maschinen: 4
ANS1900I Rückkehrcode ist 0.
ANS1901I Höchster Rückkehrcode war 0.
```

Zugehörige Links für die Sicherung virtueller Hyper-V-Maschinen

- Detail
- Domain.vmfull
- Mbobjrefreshthresh
- Mbpctrefreshthresh
- Mode
- Query VM
- Restore VM
- Vmbackdir
- Vmbackuptype

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Cancel Process

Der Befehl cancel process zeigt (sofern die NDMP-Unterstützung aktiviert ist) eine Liste der aktuellen NAS-Imagesicherungs- und -zurückschreibungsprozesse an, für die der Benutzer mit Verwaltungsaufgaben die Berechtigung hat. Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.

Aus der Liste kann der Benutzer mit Verwaltungsaufgaben einen Prozess zum Abbrechen auswählen. Die Clienteignerberechtigung ist als Berechtigung ausreichend, um die ausgewählten NAS-Imagesicherungs- oder -zurückschreibungsprozesse abzubrechen.

AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

 AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeDieser Befehl ist nur für AIX-, Linux- und Solaris-Clients gültig.

 Windows-BetriebssystemeDieser Befehl ist für alle Windows-Clients gültig.

Syntax

```
>>-Cancel Process-----------------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task
: Die aktuellen NAS-Imagesicherungs- oder -zurückschreibungsprozesse abbrechen.

  Befehl: `cancel process`

Cancel Restore

Mit dem Befehl cancel restore kann eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt werden.

Sie können nur jeweils eine wiederanlauffähige Zurückschreibungssitzung abbrechen. Führen Sie den Befehl cancel restore erneut aus, um weitere Zurückschreibungen abzubrechen. Zum erneuten Starten wiederanlauffähiger Zurückschreibungssitzungen den Befehl restart restore verwenden.

Verwenden Sie den Befehl cancel restore in den folgenden Fällen:

- Dateien, die von der wiederanlauffähigen Zurückschreibung betroffen sind, können nicht gesichert werden.
- Windows-BetriebssystemeWiederanlauffähige Zurückschreibungssitzungen sollen abgebrochen werden.
- Wiederanlauffähige Zurückschreibungssitzungen sperren den Dateibereich, sodass Dateien nicht von den sequenziellen Serverdatenträgern weg verschoben werden können.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Cancel Restore-------------------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task

Eine Operation zum Zurückschreiben abbrechen.

```
cancel restore
```

Delete Access

Der Befehl delete access löscht Berechtigungsregeln für Dateien, die auf dem Server gespeichert sind.

Wenn Sie eine Berechtigungsregel löschen, wird der Benutzerzugriff für alle Dateien oder Images, die diese Regel angibt, widerrufen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Delete-- --ACcess---------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task

Eine Liste der aktuellen Berechtigungsregeln anzeigen und die zu löschenden Regeln auswählen.

```
delete access
```

Siehe hierzu das folgende Anzeigenbeispiel:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
Index   Art       Knoten  Eigner   Pfad
_____   _______   ______  _____________________
1       Sichern   NODE1   USER1    home/dev/proja/list/
2       Archiv.   NODE3   LUIE     home/fin/budg/depta/
3       Sichern   NODE4   USER2    home/plan/exp/deptc/
```

```
4      Archiv.    NODE5   USER2S  home/mfg/invn/parta/
Index der zu löschenden Regel(n) eingeben oder Abbrechen:
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSollen die Berechtigungsregeln gelöscht werden, die `luie` und `user2s` den Zugriff auf Ihre Dateien oder Images erlauben, geben Sie `2 4` oder `2,4` ein und drücken Sie die `Eingabetaste`.

Windows-Betriebssysteme

```
Index   Art       Knoten  Eigner   Pfad
_____   _______   _____________________________
1       Sichern   node1   daisy    c:\dev\proja\list.c
2       Archiv.   node3   marm     c:\fin\budg\depta.jan
3       Sichern   node4   susie    c:\plan\exp\deptc.feb
4       Archiv.   node5   susies   c:\mfg\invn\parta.wip
Index der zu löschenden Regel(n) eingeben oder Abbrechen:
```

Windows-BetriebssystemeSollen die Berechtigungsregeln gelöscht werden, die `marm` und `susies` den Zugriff auf Ihre Dateien erlauben, geben Sie `2 4` oder `2,4` ein und drücken Sie dann die `Eingabetaste`.

Delete Archive

Mit dem Befehl delete archive können archivierte Dateien aus dem IBM Spectrum Protect-Serverspeicher gelöscht werden. Der Benutzer kann archivierte Dateien nur löschen, wenn ihm der Administrator die entsprechende Berechtigung erteilt hat.

Wichtig: Nach dem Löschen archivierter Dateien können diese nicht mehr abgerufen werden. Daher muss vor dem Löschen sichergestellt werden, dass die Dateien nicht mehr benötigt werden.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Delete ARchive--+-------------+------------------------------>
                   '- --Optionen-'

>--+- --Dateispezifikation--------------------------+----------><
   '- --{--Dateibereichsname--}--Dateispezifikation-'
```

Parameter

Dateispezifikation
: Gibt den Pfad und den Namen der Datei an, die aus dem Speicher gelöscht werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben. Sie können auch die Option filelist verwenden, um eine Liste von Dateien zu verarbeiten. Der Client für Sichern/Archivieren öffnet die Datei, die Sie mit dieser Option angeben, und verarbeitet die darin enthaltene Liste der Dateien dem jeweiligen Befehl entsprechend.
Anmerkung: Wenn *Dateibereichsname* angegeben wird, darf die Dateispezifikation keinen Laufwerkbuchstaben enthalten.

{Dateibereichsname}
: Gibt den Dateibereich (zwischen geschweiften Klammern) auf dem Server an, in dem sich die zu löschende Datei befindet. Dies ist der Name auf dem Workstationlaufwerk, auf dem die Datei archiviert wurde.

  Verwenden Sie Dateibereichsname, wenn der Name geändert wurde oder wenn Sie Dateien löschen, die auf einem anderen Knoten archiviert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.

  Windows-BetriebssystemeSie können einen UNC-Namen angeben; Laufwerkbezeichnungen werden nur für austauschbare Datenträger verwendet.

  Windows-BetriebssystemeSie müssen einen NTFS- oder ReFS-Dateibereichsnamen in Groß-/Kleinschreibung oder in Kleinschreibung angeben, der zwischen Anführungszeichen und geschweiften Klammern steht. Beispiel: `{"NTFSDrive"}`. Hochkommas oder Anführungszeichen sind im Schleifenmodus gültig. Beispielsweise ist sowohl `{"NTFSDrive"}` als auch `{'NTFSDrive'}` gültig. Im Stapelmodus sind nur Hochkommas gültig. Die Einschränkung auf Hochkommas ist im Betriebssystem begründet.

Tabelle 1. Befehl 'Delete Archive': Zugehörige Optionen

Option	Verwendung
dateformat	Clientoptionsdatei (dsm.opt) oder Befehlszeile.

Option	Verwendung
description	Nur in der Befehlszeile.
filelist	Nur in der Befehlszeile.
noprompt	Nur in der Befehlszeile.
numberformat	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
pick	Nur in der Befehlszeile.
subdir	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
timeformat	Clientoptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Datei mit dem Namen `budget` löschen.

```
dsmc delete archive /user/home/proj1/budget
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien löschen, die aus dem Verzeichnis `/user/home/proj1` archiviert wurden und die Dateierweiterung `.txt` haben.

```
dsmc del arch "/user/home/proj1/*.txt"
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDateien löschen, die aus dem Verzeichnis `/user/project` archiviert wurden; dabei die Option pick verwenden, um eine Liste der Archivierungskopien anzuzeigen, die mit der Dateispezifikation übereinstimmen. Aus der Liste können die zu verarbeitenden Versionen ausgewählt werden.

```
dsmc delete archive "/user/project/*" -pick
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAusgewählte Dateien aus der Dateigruppe löschen, die mit der Beschreibung "Monthly Budgets 2010" archiviert wurde und sich in `/user/projects` und dessen Unterverzeichnissen befindet.

```
dsmc delete ar "/user/projects/*" -description="Monthly Budgets 2010" -pick -subdir=yes
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeDateien aus dem Dateibereich `abc` im Verzeichnis `proj` löschen.

```
dsmc delete archive {"abc"}\proj\*
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Datei mit dem Namen `budget` löschen.

```
dsmc delete archive c:\plan\proj1\budget.jan
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeAlle Dateien löschen, die aus dem Verzeichnis `c:\plan\proj1` archiviert wurden und die Dateierweiterung `.txt` haben.

```
delete archive c:\plan\proj1\*.txt
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeDateien löschen, die aus dem Verzeichnis `c:\project` archiviert wurden; dabei die Option pick verwenden, um eine Liste der Archivierungskopien anzuzeigen, die mit der Dateispezifikation übereinstimmen. Aus der Liste können die zu verarbeitenden Versionen ausgewählt werden.

```
dsmc delete archive c:\project\* -pick
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeAusgewählte Dateien aus der Dateigruppe löschen, die mit der Beschreibung "Monthly Budgets 2013" archiviert wurde und sich im Verzeichnis `c:\projects` und dessen Unterverzeichnissen befindet.

```
dsmc delete ar c:\projects\* -description="Monthly Budgets 2013" -pick -subdir=yes
```

Delete Backup

Der Befehl delete backup löscht Dateien, Images und virtuelle Maschinen, die im IBM Spectrum Protect-Serverspeicher gesichert wurden. Ihr Administrator muss Ihnen die Berechtigung zum Löschen von Objekten erteilen.

Wenn Sie Dateien löschen, inaktiviert der IBM Spectrum Protect-Server alle gesicherten Dateien, die den angegebenen Optionen Dateispezifikation und deltype entsprechen. Außerdem ordnet der Server das Inaktivierungsdatum *unendlich-minus* zu, sodass die Dateien nicht mehr für Zurückschreibungen verfügbar sind und bei der nächsten Ausführung des Dateiverfalls sofort gelöscht werden. Die Datei wird erst bei der Ausführung des Verfallsprozesses physisch gelöscht.

Wichtig: Nach dem Löschen von Sicherungsdateien können diese nicht mehr zurückgeschrieben werden. Stellen Sie vor dem Löschen sicher, dass die Sicherungsdateien nicht mehr benötigt werden. Sie werden aufgefordert, die Fortsetzung des Löschvorgangs zu bestätigen. Wenn Sie ja angeben, werden die angegebenen Sicherungsdateien in den Zeitplan zum Löschen aufgenommen und aus dem Serverspeicher entfernt.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Syntax

```
>>-Delete BAckup-- ------------------------------------------->

>--+-------------------------------------------------+---------->
   '-+-Dateispezifikation--------------------------+-'
     '-{--Dateibereichsname--}--Dateispezifikation-'

>--+-------------------------------------------------+---------->
   | .-objtype=FILE------------------------------. |
   '-+-----------------------------------------+-'
     +-objtype=IMAGE-----------------------------+
     '-objtype=VM-+--------------------+- VM-Name-'
                  |         .-BOTH---. |
                  '--FROM -+-SERVER-+-'
                           '-LOCAL--'

   .-deltype=ACTIVE-------.
>--+----------------------+-+----------+----------------------><
   +-+------------------+-+ '-Optionen-'
   | '-deltype=INACTIVE-' |
   '-+--------------+------'
     '-deltype=ALL-'
```

Parameter

Dateibereich/Dateispezifikation
Dateispezifikation
Gibt den Pfad und den Namen der Datei an, die aus dem Speicher gelöscht werden soll. Um eine Datei in einem anderen Dateibereich anzugeben, geben Sie vor dem Dateinamen den Dateibereichsnamen ein. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben. Trennen Sie die Dateispezifikationen durch ein Leerzeichen. Sie können auch die Option filelist verwenden, um eine Liste von Dateien zu verarbeiten. Der Client für Sichern/Archivieren öffnet die Datei, die mit dieser Option angegeben wird, und verarbeitet die darin enthaltene Liste der Dateien dem jeweiligen Befehl entsprechend.
Anmerkung: Wenn *Dateibereichsname* angegeben wird, darf die Dateispezifikation keinen Laufwerkbuchstaben enthalten.

Verwenden Sie bei Angabe von `-deltype=inactive` oder `-deltype=active` Platzhalterzeichen, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.

Geben Sie bei Verwendung von `-deltype=all` ein Verzeichnis an, das ausschließlich aus Platzhalterzeichen besteht.

objtype
Gibt den Typ des zu löschenden Objekts an. Sie können einen der folgenden Werte angeben:

FILE
Gibt an, dass Dateien und Verzeichnisse gelöscht werden sollen. Dieser Wert ist der Standardobjekttyp.
IMAGE
Gibt an, dass eine Imagesicherung gelöscht werden soll. Gibt an, dass eine Imagesicherung gelöscht werden soll. Objtype=image wird unter Mac OS X nicht unterstützt.
VM *VM-Name*

Gibt an, dass Sie mindestens eine Version einer Sicherung einer virtuellen Maschine löschen möchten; die virtuelle Maschine wird durch den Variablenparameter *VM-Name* angegeben. Der Name der virtuellen Maschine darf keine Platzhalterzeichen enthalten.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Wird `objtype=VM` angegeben, kann die Option filelist nicht verwendet werden. Die Angabe von `objtype=VM` ändert das Verhalten der Option `-deltype`. Wird `objtype=vm` angegeben, können Sie entweder `-deltype=active` oder `-deltype=inactive` verwenden. Sie können nicht `-deltype=all` verwenden. Bei Angabe von `-deltype=inactive` wird eine Liste der aktiven und der inaktiven Sicherungen angezeigt. Anhand dieser Liste können Sie die Sicherungen virtueller Maschinen angeben, die gelöscht werden sollen. Sollen nur die aktiven Sicherungen virtueller Maschinen gelöscht werden, verwenden Sie `-deltype=active`.

Wenn Sie `-objtype=VM` angeben, löscht dieser Befehl nur Sicherungen virtueller Maschinen, die mit einem der folgenden Modi erstellt wurden: FULL, IFINCR und IFFULL. Sicherungen, die im vollständigen oder inkrementellen Modus erstellt wurden, wurden mit dem Client der Version 7.1 oder früher erstellt.

Für Sicherungen, die mit Clients der Version 7.1 oder früher erstellt wurden: Einzelne Teilsicherungen (mit `MODE=INCR` erstellte Sicherungen), die nach der Ausführung einer Gesamtsicherung erstellt wurden, können nicht mit diesem Befehl gelöscht werden. Löschen Sie jedoch eine Imagegesamtsicherung einer virtuellen Maschine (mit `MODE=FULL` erstellte Sicherung) und verfügt der Server über Teilsicherungen (`MODE=INCR`), die für diese VM nach der Gesamtsicherung erstellt wurden, werden beim Löschen der VM-Gesamtsicherung auch die Sicherungsdateien gelöscht, die mit `MODE=INCR` erstellt wurden.

Wenn Sie eine aktive Sicherung für eine virtuelle Maschine löschen, wird die neueste inaktive Kopie zur aktiven Sicherung. Wenn Sie die Option -pick oder -inactive angeben, wird nur die von Ihnen angegebene Sicherung gelöscht. Wenn Sie eine mit `MODE=IFINCR` erstellte Sicherung auswählen, wird nur die ausgewählte Teilsicherung gelöscht, andere Teilsicherungen für die virtuelle Maschine werden nicht gelöscht.

-FROM
: Geben Sie die Sicherungsposition oder -positionen an, an denen Sicherungen virtueller Maschinen gelöscht werden sollen. Sie können einen der folgenden Werte angeben:

  SERVER
  : Sicherungen virtueller Maschinen werden vom IBM Spectrum Protect-Server gelöscht.

  LOCAL
  : Gespeicherte Momentaufnahmen virtueller Maschine werden aus dem Hardwarespeicher gelöscht.

  BOTH
  : Sicherungen virtueller Maschinen, die sich auf dem IBM Spectrum Protect-Server befinden, und Momentaufnahmen, die sich im Hardwarespeicher befinden, werden gelöscht. Dies ist der Standardwert.
  Bei Angabe dieses Werts wird eine Liste der Sicherungspositionen angezeigt. Aus der Liste können Sie die Position auswählen, an der Sicherungen virtueller Maschinen gelöscht werden sollen.

deltype
: Gibt den Löschtyp an. Geben Sie einen der folgenden Werte an:

  ACTIVE
  : Es sollen nur aktive Dateiobjekte gelöscht werden. Verzeichnisobjekte werden nicht gelöscht. Dieser Wert ist der Standardlöschtyp.
  Anmerkung: Sind inaktive Objekte vorhanden, nachdem das aktive Objekt gelöscht wurde, wird das aktuellste inaktive Objekt von "inaktiv" in "aktiv" geändert.

  Sollen alle Versionen einer Datei gelöscht werden, setzen Sie zunächst den Befehl delete backup mit `-deltype=inactive` ab und geben Sie anschließend den Befehl mit `-deltype=active` erneut ein.

  INACTIVE
  : Es sollen nur inaktive Dateiobjekte gelöscht werden. Verzeichnisobjekte werden nicht gelöscht.

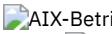
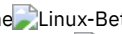
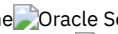
  ALL
  : Alle aktiven und inaktiven Objekte unter einem bestimmten Verzeichnis, einschließlich aller Unterverzeichnisse und der darin enthaltenen Dateien, löschen.
  Anmerkung: Das übergeordnete Verzeichnis der gelöschten Dateien und Unterverzeichnisse wird nicht gelöscht. Wenn Sie `deltype=ALL` angeben, können Sie nicht die Option pick verwenden, da sich `deltype=ALL` und die Option pick gegenseitig ausschließen.

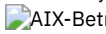
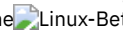
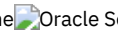
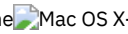
Tabelle 1. Befehl Delete Backup: Zugehörige Optionen

Option	Verwendung
description	Nur in der Befehlszeile.
filelist	Nur in der Befehlszeile.
fromdate	In der Befehlszeile und in der GUI-Suchfunktion.
fromtime	In der Befehlszeile und in der GUI-Suchfunktion.

Option	Verwendung
noprompt	Nur in der Befehlszeile.
pick	Nur in der Befehlszeile.
pitdate	In der Befehlszeile und in der GUI-Suchfunktion.
pittime	In der Befehlszeile und in der GUI-Suchfunktion.
subdir	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
tapeprompt	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
timeformat	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
todate	In der Befehlszeile und in der GUI-Suchfunktion.
totime	In der Befehlszeile und in der GUI-Suchfunktion.

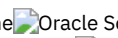
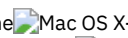
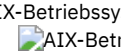
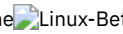
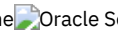
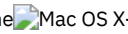
Beispiele

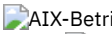
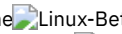
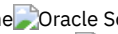




Alle aktiven und inaktiven Dateiobjekte mit dem Namen budget im Verzeichnis /data/plan/proj1 löschen.
Befehle:

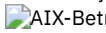
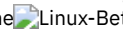
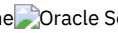
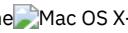
```
delete backup /data/plan/proj1/budget.jan
  -deltype=inactive
delete backup /data/plan/proj1/budget.jan
  -deltype=active
```



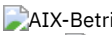
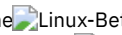
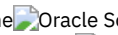






Alle inaktiven Dateien mit der Erweiterung .txt löschen, die im Verzeichnis /data/plan/proj1 und dessen Unterverzeichnissen gesichert wurden.

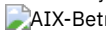
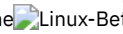
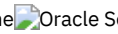
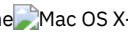
Befehl: `delete backup "/data/plan/proj1/*.txt" -deltype=inactive -subdir=yes`





Ausgewählte aktive Dateien löschen, die im Verzeichnis /home/marymb/project gesichert wurden. Verwenden Sie die Option -pick, um eine Liste der Sicherungskopien anzuzeigen, die mit der Dateispezifikation übereinstimmen. Aus der Liste können Sie die zu löschenden Versionen auswählen.

Befehl: `delete backup "/home/marymb/project/*" -pick`





Alle aktiven und inaktiven Versionen von Dateien und Unterverzeichnissen im Verzeichnis /home/storman/myproject löschen. Anschließend alle aktiven und inaktiven Versionen des Verzeichnisses /user/myproject löschen.
Befehl:

```
delete backup "/home/storman/myproject*"
-deltype=all
```



Alle aktiven Dateiobjekte aus dem Dateibereich abc im Verzeichnis proj löschen.

Befehl: `delete backup {abc}\proj\*`



Alle inaktiven Dateien löschen, deren Name mit .txt endet und die im Verzeichnis c:\plan\proj1 und dessen Unterverzeichnissen gesichert wurden.

Befehl: `delete backup c:\plan\proj1\*.txt -deltype=inactive -subdir=yes`



Ausgewählte aktive Dateien löschen, die im Verzeichnis c:\project gesichert wurden. Verwenden Sie die Option -pick, um eine Liste der Sicherungskopien anzuzeigen, die mit der Dateispezifikation übereinstimmen. Aus der Liste können Sie die zu löschenden Versionen auswählen.

Befehl: `delete backup c:\project\* -pick`

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle aktiven und inaktiven Versionen von Dateien und Unterverzeichnissen im Verzeichnis c:\user\myproject löschen.

Befehl: `delete backup c:\user\myproject\* -deltype=all`

Anmerkung: Die Sicherungsversionen des Verzeichnisobjekts c:\user\myproject werden nicht gelöscht.

Windows-BetriebssystemeTask

Windows-BetriebssystemeDie aktive Sicherung einer virtuellen Maschine mit dem Namen vm1 löschen.

Befehl: `delete backup -objtype=vm vm1`

Anmerkung: Ist mindestens eine inaktive Version dieser Sicherung vorhanden, wird die neueste Version die aktive Version.

Windows-BetriebssystemeTask

Windows-BetriebssystemeMindestens eine Sicherungsversion einer virtuellen Maschine mit dem Namen vm_test löschen.

Befehl: `delete backup -objtype=vm -inactive vm_test`

Anmerkung: Alle Versionen der Sicherungen für diesen VM-Knoten werden in einer Liste angezeigt. Sie wählen die zu löschenden Versionen aus.

Delete Filespace

Mit dem Befehl delete filespace können Dateibereiche im IBM Spectrum Protect-Serverspeicher gelöscht werden. Ein Dateibereich ist ein logischer Speicherbereich auf dem Server, der die gesicherten oder archivierten Dateien enthält.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMac OS X-Betriebssysteme Sie müssen ein berechtigter Benutzer sein, um diesen Befehl verwenden zu können.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme IBM Spectrum Protect ordnet jedem Workstationdateisystem, von dem Sie Dateien sichern oder archivieren, einen separaten Dateibereich auf dem Server zu. Der Dateibereichsname entspricht dem Namen des Dateisystems.

Windows-BetriebssystemeIBM Spectrum Protect ordnet jedem Workstationdateisystem, von dem Sie Dateien sichern oder archivieren, einen separaten Dateibereich auf dem Server zu. Der Dateibereichsname entspricht dem UNC-Namen.

Wenn Sie den Befehl delete filespace eingeben, wird eine Liste Ihrer Dateibereiche angezeigt. Wählen Sie aus dieser Liste den Dateibereich aus, der gelöscht werden soll.

Ihr IBM Spectrum Protect-Administrator muss Ihnen die Berechtigung zum Löschen eines Dateibereichs erteilen. Sie benötigen die Berechtigung BACKDEL, wenn der zu löschende Dateibereich Sicherungsversionen enthält, oder die Berechtigung ARCHDEL, wenn der Dateibereich Archivierungskopien enthält. Enthält der Dateibereich sowohl Sicherungsversionen als auch Archivierungskopien, muss der Benutzer über beide Berechtigungen verfügen.

Wichtig: Beim Löschen eines Dateibereichs werden alle Sicherungsversionen und Archivierungskopien innerhalb dieses Dateibereichs gelöscht. Nach dem Löschen eines Dateibereichs ***können Sie die Dateien nicht zurückschreiben***. Daher muss vor dem Löschen sichergestellt werden, dass die Dateien nicht mehr benötigt werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Mit dem Befehl delete filespace können Sie NAS-Dateibereiche interaktiv aus dem Serverspeicher löschen. Verwenden Sie die Option nasnodename, um den NAS-Dateiserver zu identifizieren. Mit der Option class können Sie die Klasse des zu löschenden Dateibereichs angeben.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Delete Filespace--+-------------+--------------------------><
                     '- --Optionen-'
```

Parameter

Tabelle 1. Befehl Delete Filespace: Zugehörige Optionen

Option	Verwendung

Option	Verwendung
AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-Betriebssystemeclass	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeNur in der Befehlszeile.
detail	Nur in der Befehlszeile.
Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-Betriebssystemenasnodename	Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei oder Befehlszeile.
Windows-Betriebssystemenasnodename	Windows-BetriebssystemeClientoptionsdatei oder Befehlszeile.
Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-Betriebssystemescrolllines	Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei oder Befehlszeile.
Windows-Betriebssystemescrolllines	Windows-BetriebssystemeClientoptionsdatei oder Befehlszeile.
Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-Betriebssystemescrollprompt	Mac OS X-BetriebssystemeAIX-Betriebssysteme Linux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei oder Befehlszeile.
Windows-Betriebssystemescrollprompt	Windows-BetriebssystemeClientsystemoptionsdatei oder Befehlszeile.

Beispiele

Task

Einen Dateibereich löschen.

Befehl: `delete filespace`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme
Task

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Windows-BetriebssystemeAuf dem Server gespeicherte NAS-Dateibereiche aus dem NAS-Dateiserver **dagordon** löschen.

Befehl: `delete filespace -nasnodename=dagordon -class=nas`

Delete Group

Verwenden Sie den Befehl delete group, um eine Gruppensicherung auf dem IBM Spectrum Protect-Server zu löschen.

Nach dem Löschen einer Gruppe verbleibt das Hauptmember (virtualfsname) auf dem IBM Spectrum Protect-Server. Es enthält keine Member (Dateien oder Verzeichnisse), wird aber in einem nachfolgenden Befehl query filespace aufgelistet. Es werden keine Dateien aufgelistet, wenn die Option showmembers hinzugefügt wird. Durch das Löschen einer Gruppe wird der Dateibereich, in dem die Gruppe enthalten ist, nicht entfernt, da er noch andere Gruppen enthalten kann. Verwenden Sie delete filespace, wenn Sie den Dateibereich und alle darin enthaltenen Daten entfernen wollen.

Anmerkung:

1. Verwenden Sie die Option inactive, um sowohl aktive als auch inaktive Gruppensicherungsversionen anzuzeigen. Standardmäßig zeigt der Client aktive Versionen an.
2. Verwenden Sie die Option pick, um eine bestimmte Gruppe auszuwählen, die vom IBM Spectrum Protect-Server gelöscht werden soll.
3. Verwenden Sie die Option noprompt, um die Bestätigungsaufforderung zu unterdrücken, die normalerweise vor dem Löschen einer Gruppensicherungsversion angezeigt wird. Standardmäßig fordert der Client Sie zur Bestätigung auf, bevor die Gruppensicherung gelöscht wird. Mit dieser Option kann die Löschprozedur beschleunigt werden. Die Gefahr, eine Gruppensicherungsversion versehentlich zu löschen, ist hierbei jedoch größer. Diese Option ist mit Vorsicht zu verwenden.
4. Verwenden Sie den Befehl query filespace, um Namen der virtuellen Dateibereiche für Ihren Knoten anzuzeigen, die auf dem Server gespeichert sind.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDieser Befehl ist für alle UNIX- und Linux-Clients gültig, mit Ausnahme von Mac OS X.

Windows-BetriebssystemeDieser Befehl ist für alle Windows-Clients gültig.

Syntax

```
>>-Delete GRoup-- --Dateispezifikation--+-------------+-------><
                                       '- --Optionen-'
```

Parameter

Dateispezifikation
: Gibt den Namen des virtuellen Dateibereichs und den Namen der Gruppe an, die Sie aus dem Serverspeicher löschen wollen.

Tabelle 1. Befehl Delete Group: Zugehörige Optionen

Option	Verwendung
inactive	Nur in der Befehlszeile.
noprompt	Nur in der Befehlszeile.
pick	Nur in der Befehlszeile.
pitdate	Nur in der Befehlszeile.
pittime	Nur in der Befehlszeile.

Beispiele




Task




Die zurzeit aktive Version der Gruppe `/virtfs/group1` löschen.

Befehl:

```
delete group /virtfs/group1
```


Task


Die zurzeit aktive Version der Gruppe `virtfs\group1` löschen.

Befehl:

```
delete group {virtfs}\group1
```




Task




Eine Sicherungsversion der Gruppe `/virtfs/group1` aus einer Liste von aktiven und inaktiven Versionen löschen.

Befehl:

```
delete group /virtfs/group1 -inactive -pick
```


Task


Eine Sicherungsversion der Gruppe `virtfs\group1` aus einer Liste von aktiven und inaktiven Versionen löschen.

Befehl:

```
delete group {virtfs}\group1 -inactive -pick
```

Expire

Mit dem Befehl expire werden die Sicherungsobjekte, die Sie in der Dateispezifikation oder mit der Option filelist angeben, inaktiviert. Sie können eine einzelne Datei als verfallen definieren oder eine Datei, die eine Liste mit Dateien enthält, die als verfallen definiert werden sollen. Wird `OBJTYPE=VM` angegeben, inaktiviert dieser Befehl die aktuelle Sicherung für eine virtuelle Maschine.

Im interaktiven Modus werden Sie durch eine Bedienerführung informiert, bevor Dateien verfallen.

Der Befehl expire entfernt keine Workstationdateien. Wenn eine Datei oder ein Verzeichnis verfällt, die bzw. das auf Ihrer Workstation noch vorhanden ist, wird die Datei bzw. das Verzeichnis während der nächsten Teilsicherung erneut gesichert, sofern Sie das Objekt nicht von der Sicherungsverarbeitung ausschließen.

Wenn ein Verzeichnis verfällt, das aktive Dateien enthält, werden diese Dateien bei einer nachfolgenden Abfrage von der GUI nicht angezeigt. Diese Dateien werden jedoch in der Befehlszeile angezeigt, wenn Sie die korrekte Abfrage mit einem Platzhalterzeichen für das Verzeichnis angeben.





Anmerkung: Da der Befehl expire das Bild des Servers vom Clientdateisystem ändert, ohne das Clientdateisystem zu ändern, ist der Befehl expire für Dateien in einem Dateisystem, das durch den IBM Spectrum Protect-Journaldämon überwacht wird, nicht zulässig.

Anmerkung: Da der Befehl expire das Bild des Servers vom Clientdateisystem ändert, ohne das Clientdateisystem zu ändern, ist der Befehl expire für Dateien in einem Dateisystem, das durch den IBM Spectrum Protect-Journalservice überwacht wird, nicht

zulässig.
AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
              .-OBJTYPE=FILE-- --Dateispezifikation-.
>>-EXPire-- --+-------------------------------------+--+------------------------+-->
                                                      '-OBJTYPE=VM-- --VM-Name-'

>--+----------+-----------------------------------------------><
   '-Optionen-'
```

Parameter

OBJTYPE=FILE Dateispezifikation
: Gibt einen Pfad und Dateinamen an, der verfallen soll. Sie können in diesem Befehl nur eine Dateispezifikation eingeben. Sie können jedoch Platzhalterzeichen verwenden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis auszuwählen. Wenn Sie die Option filelist angeben, wird der in `Dateispezifikation` angegebene Name ignoriert.

OBJTYPE=VM VM-Name
: `VM-Name` gibt den Namen einer virtuellen Maschine an. Die aktive Sicherung für die angegebene virtuelle Maschine verfällt. Der Name der virtuellen Maschine darf keine Platzhalterzeichen enthalten.

  Wird `objtype=VM` angegeben, verfallen durch den Befehl 'expire' nur VM-Gesamtsicherungen (`MODE=FULL` oder `MODE=IFFULL`) für die virtuelle Maschine, die im Parameter `VM-Name` angegeben wird. Sicherungen, die im vollständigen oder inkrementellen Modus erstellt wurden, wurden mit dem Client der Version 7.1 oder früher erstellt.

  Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Tabelle 1. Befehl Expire: Zugehörige Optionen

Option	Verwendung
Windows-Betriebssystemedateformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedateformat	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
filelist	Nur in der Befehlszeile.
noprompt	Nur in der Befehlszeile.
Windows-Betriebssysteme numberformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme numberformat	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
pick	Nur in der Befehlszeile.
Windows-Betriebssystemetimeformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemetimeformat	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
: AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie Dateiletter1.txt im Verzeichnis `home` inaktivieren.

  Befehl: `expire "/home/letter1.txt"`

Windows-BetriebssystemeTask

Windows-BetriebssystemeDie Datei`letter1.txt` im Verzeichnis home inaktivieren.

Befehl: `expire c:\home\letter1.txt`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien im Verzeichnis /admin/mydir inaktivieren.

Befehl: `expire /admin/mydir/*`

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Dateien im Verzeichnis admin\mydir inaktivieren.

Befehl: `expire c:\admin\mydir\*`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien inaktivieren, die in der Datei /home/avi/filelist.txt aufgeführt sind.

Befehl: `expire -filelist=/home/avi/filelist.txt`

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Dateien inaktivieren, die in der Datei `c:\avi\filelist.txt` aufgeführt sind.

Befehl: `expire -filelist=c:\avi\filelist.txt`

Windows-BetriebssystemeTask

Windows-BetriebssystemeDie aktuelle Sicherung der virtuellen Maschine mit dem Namen vm_test inaktivieren.

Befehl: `expire -objtype=VM vm_test`

Help

Verwenden Sie den Befehl help, um Informationen zu Befehlen, Optionen und Nachrichten anzuzeigen.

Tipp: Wenn Sie den Befehl help in der Anfangsbefehlszeile verwenden, wird keine Verbindung zum Server hergestellt und es ist kein Kennwort erforderlich.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Help--+-----------------------------------------+------------><
         +-Befehlsname [Unterbefehlsname]---------+
         +-Optionsname----------------------------+
         +-Abschnittsnummer im Inhaltsverzeichnis-+
         '-[ANS]Nachrichtennummer-----------------'
```

Wenn Sie den Befehl help ohne Argumente eingeben, wird das vollständige Inhaltsverzeichnis angezeigt. Die folgenden Parameter können Sie entweder mit dem ersten Befehl eingeben oder eingeben, wenn HELP eine Bedienerführung anzeigt.

Parameter

Befehlsname [Unterbefehlsname]
: Gibt einen Befehlsnamen und optional einen Unterbefehlsnamen bzw. die entsprechenden Abkürzungen an, beispielsweise backup image oder b i. In letzterem Fall muss die Kombination eindeutig sein. Bei nicht eindeutigen Abkürzungen wird der erste Abschnitt der gesamten Hilfedatei angezeigt, die der Abkürzung entspricht. Dieser Parameter ist optional.

Optionsname
: Gibt den Namen einer Option an, beispielsweise domain oder do. Dieser Parameter ist optional.

Abschnittsnummer im Inhaltsverzeichnis
: Gibt eine Abschnittsnummer im Inhaltsverzeichnis an, beispielsweise 1.5.3. Dieser Parameter ist optional.

[ANS]Nachrichtennummer
: Gibt eine Nachrichtennummer mit oder ohne zugehöriges Präfix an, beispielsweise ans1036 oder 1036. Dieser Parameter ist optional. Der Bewertungscode muss in keinem Fall angegeben werden. Wird ans1036E eingegeben, werden keine Informationen gefunden.

Wichtig: Wenn Sie Argumente eingeben, die diesen Beschreibungen nicht entsprechen, werden möglicherweise unerwartete Ergebnisse (oder keine Ergebnisse) angezeigt. Wenn Sie mehr als zwei Argumente eingeben, wird Ihre Hilfeanforderung zurückgewiesen. Wenn ein Befehlsname und ein Optionsname identisch sind, beispielsweise incremental (Befehl) und incremental (Option), können Sie Hilfe zu der Option aufrufen, indem Sie die entsprechende Abschnittsnummer im Inhaltsverzeichnis eingeben.

Der angeforderte Hilfetext wird je nach der Anzahl der Anzeigezeilen in Ihrem Befehlsfenster in einem Abschnitt oder in mehreren Abschnitten angezeigt. Wenn der Anzeigebereich mit Zeilen gefüllt ist oder wenn das Ende des angeforderten Hilfetexts erreicht ist, werden eine Bedienerführung sowie Anweisungen zu den möglichen Eingaben bei der Bedienerführung angezeigt. Soll mit der Anzeige von Text zu Ihrer aktuellen Auswahl fortgefahren werden, drücken Sie die Eingabetaste oder die Taste `'d'`, um abwärts zu blättern. Um in der aktuellen Auswahl aufwärts zu blättern, drücken Sie die Taste `'u'` und drücken die Eingabetaste. Möglicherweise stehen weitere Auswahlmöglichkeiten zur Verfügung; lesen Sie also die angezeigten Anweisungen.

Für eine ordnungsgemäße Anzeige des Hilfetexts ist eine verwendbare Anzeigebreite von 72 Zeichen erforderlich. Eine Anzeigebreite von weniger als 72 Zeichen hat zur Folge, dass Sätze mit einer Breite von 72 Zeichen in der nächsten Zeile fortgesetzt werden. Dies kann dazu führen, dass nicht der Anfang, sondern ein Abschnitt in der Mitte des Hilfetexts angezeigt wird. Die nicht angezeigten Zeilen können mit der Blätterfunktion der Datenstation angezeigt werden.

Beispiele

Task
: Das Inhaltsverzeichnis der Hilfethemen anzeigen.

  Befehl: `dsmc help`

Task
: Die Informationen in Hilfethema 2.1.2 anzeigen.

  Befehl: `dsmc help 2.1.2`

Task
: Hilfetext zum Befehl archive anzeigen.

  Befehl: `dsmc help archive`

Task
: Hilfetext zu der Nachricht ANS1036 anzeigen.

  Befehl: `dsmc help 1036`

  Befehl: `dsmc help ANS1036`

Incremental

Der Befehl incremental sichert alle neuen oder geänderten Daten an den Positionen, die Sie angeben, sofern Sie sie nicht von den Sicherungsservices ausschließen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Sie können alle neuen oder geänderten Dateien oder Verzeichnisse in der Standardclientdomäne oder in Dateisystemen, Verzeichnissen oder Dateien sichern.

Für eine Teilsicherung ausgewählter Dateien oder Verzeichnisse muss die Dateispezifikation im Befehl angegeben werden. Wenn Sie keine Dateispezifikation eingeben, werden standardmäßig Dateien oder Verzeichnisse in der Standarddomäne gesichert.

AIX-BetriebssystemeNur für AIX: Mithilfe der Option `snapshotproviderfs=JFS2` können Sie die Teilsicherung auf Momentaufnahmebasis aktivieren.

Die folgenden Attribute der Verwaltungsklasse, die der Datei oder dem Verzeichnis zugeordnet ist, bestimmen, ob die Daten gesichert werden:

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme
Häufigkeit
: AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
  Windows-BetriebssystemeDie Anzahl der Tage, die zwischen aufeinanderfolgenden Sicherungen des Objekts vergehen müssen. Das Attribut Häufigkeit gilt nur für eine vollständige Teilsicherung.

  AIX-BetriebssystemeLinux-BetriebssystemeDieses Verwaltungsklassenattribut wird während einer journalbasierten Sicherung ignoriert.

  Windows-BetriebssystemeDieses Verwaltungsklassenattribut wird während einer journalbasierten Sicherung ignoriert.

Modus
: Gibt an, ob sich Änderungen seit der letzten Sicherungsoperation auf die Verarbeitung auswirken. Bei Angabe von `mode=modified` werden nur die Objekte verarbeitet, die sich seit der letzten Sicherungsoperation geändert haben. Bei Angabe von `mode=absolute` wird

jedes Objekt verarbeitet, unabhängig davon, ob sich das Objekt seit der letzten Sicherungsoperation geändert hat.

Wenn als Kopiengruppenmodus modified definiert ist, kann dieser mithilfe der Clientoption absolute außer Kraft gesetzt werden. Weitere Informationen zur Option absolute finden Sie in Absolute.

Durchnummerierung
Ermöglicht oder verhindert die Sicherung von Dateien oder Verzeichnissen gemäß den folgenden Werten:

- Statisch: Damit eine Sicherung erfolgt, dürfen Daten während einer Sicherung oder Archivierung nicht geändert werden.
- Gemeinsam statisch: Ändern sich die Daten in der Datei oder in dem Verzeichnis während der zulässigen Sicherungs- oder Archivierungsversuche, werden sie nicht gesichert oder archiviert. Der Wert der Option changingretries legt fest, wie viele Versuche unternommen werden. Der Standardwert ist 4.
- Dynamisch: Das Objekt wird beim ersten Versuch gesichert oder archiviert, auch wenn sich die Daten während der Verarbeitung ändern.
- Gemeinsam dynamisch: Das Objekt wird beim letzten Versuch gesichert oder archiviert, auch wenn sich die Daten während der Verarbeitung ändern.

Mithilfe der Option include können Sie in einer Einschluss-/Ausschlussliste die Standardverwaltungsklasse für eine Datei oder eine Gruppe von Dateien überschreiben.

Es kann eine vollständige Teilsicherung oder eine Teilsicherung nach Datum ausgeführt werden. Standardwert ist eine vollständige Teilsicherung.

AIX-BetriebssystemeWindows-BetriebssystemeLinux-BetriebssystemeWenn Sie für ein Dateisystem die Journalführung verwenden und das Journal gültig ist, wird bei der vollständigen Teilsicherung eine journalbasierte Sicherung ausgeführt. Es können mehrere journalbasierte Sicherungssitzungen gestartet werden, aber nur eine journalbasierte Sicherungssitzung kann fortgesetzt werden. Alle anderen journalbasierten Sicherungssitzungen, die auf denselben Dateibereich zugreifen müssen, müssen warten, bis die aktuelle journalbasierte Sicherungssitzung beendet ist, bevor die nächste Sitzung fortgesetzt werden kann. Sie können eine vollständige Teilsicherung ohne Journal ausführen, indem Sie die Option nojournal verwenden.

Mit dem Befehl selective kann auch eine selektive Sicherung ausgeführt werden, bei der nur die von Ihnen angegebenen Dateien, Verzeichnisse oder leeren Verzeichnisse gesichert werden, unabhängig davon, ob sie sich geändert haben.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBei einer vollständigen Teilsicherung werden alle neuen Dateien und Verzeichnisse sowie Dateien und Verzeichnisse, die sich seit der letzten Teilsicherung geändert haben, gesichert. Während einer vollständigen Teilsicherung fragt der Client den Server ab. IBM Spectrum Protect verwendet diese Informationen, wenn folgende Aktionen ausgeführt werden:

Windows-BetriebssystemeBei einer vollständigen Teilsicherung werden alle neuen Dateien und Verzeichnisse sowie Dateien und Verzeichnisse, die sich seit der letzten Teilsicherung geändert haben, gesichert. Während einer vollständigen Teilsicherung fragt der Client den Server oder die Journaldatenbank ab. IBM Spectrum Protect verwendet diese Informationen, wenn folgende Aktionen ausgeführt werden:

- Neue Dateien oder Verzeichnisse sichern.
- Dateien oder Verzeichnisse sichern, deren Inhalt sich seit der letzten Sicherung geändert hat.
- Sicherungsversionen auf dem Server für Dateien oder Verzeichnisse, die aus der Workstation gelöscht wurden, als inaktiv markieren.
- Sicherungsversionen erneut an Verwaltungsklassen binden, wenn sich die Zuordnung der Verwaltungsklassen ändert.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Mac OS X-BetriebssystemeAIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

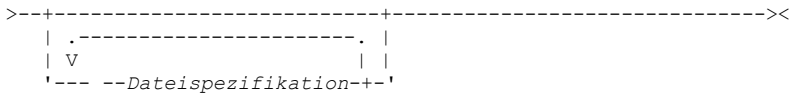
Syntax

```
>>-Incremental--+-------------+---------------------------------->
                '- --Optionen-'

   .-----------------------------.
   V                             |
>----+-------------------------+-+------------------------------><
     +- --Dateispezifikation---+
     '- --"Dateispezifikation"-'
```

Windows-Betriebssysteme

Syntax

```
>>-Incremental--+-------------+---------------------------------->
                '- --Optionen-'
```



Parameter

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDateispezifikation
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt den Pfad und den Namen der Datei an, die gesichert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis auszuwählen. Wenn Sie keine Dateispezifikation angeben, bestimmt die Option domain, was gesichert wird.

Wenn Sie ein Dateisystem angeben, werden alle neuen und geänderten Dateien gesichert. Zusätzlich wird auf dem Server das Datum der letzten Teilsicherung des Dateibereichs aktualisiert. Wenn Sie eine Datei oder ein Verzeichnis angeben, wird das Datum der letzten Teilsicherung nicht aktualisiert. Dies bedeutet, dass die Datei oder das Verzeichnis möglicherweise erneut gesichert wird, wenn eine spätere Sicherung mit der Option incrbydate durchgeführt wird. Bei der Angabe eines Dateisystems müssen Sie das Dateisystem ohne abschließenden Schrägstrich angeben.

Windows-BetriebssystemeDateispezifikation
Windows-BetriebssystemeGibt den Pfad und den Namen der Datei an, die gesichert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis auszuwählen. Sie können so viele Dateispezifikationen angeben wie die verfügbaren Ressourcen oder andere Betriebssystembeschränkungen erlauben. Trennen Sie die Dateispezifikationen durch ein Leerzeichen. Sie können auch die Option filelist verwenden, um eine Liste von Dateien zu verarbeiten. Der Client für Sichern/Archivieren öffnet die Datei, die Sie mit dieser Option angeben, und verarbeitet die darin enthaltene Liste der Dateien dem jeweiligen Befehl entsprechend. Wenn Sie keine Dateispezifikation angeben, bestimmt die Option domain, was gesichert wird.

Wenn Sie ein Dateisystem angeben, werden alle neuen und geänderten Dateien gesichert. Zusätzlich wird auf dem Server das Datum der letzten Teilsicherung des Dateibereichs aktualisiert. Wenn Sie eine Datei oder ein Verzeichnis angeben, wird das Datum der letzten Teilsicherung nicht aktualisiert. Dies bedeutet, dass die Datei oder das Verzeichnis möglicherweise erneut gesichert wird, wenn eine spätere Sicherung mit der Option incrbydate durchgeführt wird. Bei der Angabe eines Dateisystems müssen Sie das Dateisystem ohne abschließenden Schrägstrich angeben.

Tabelle 1. Befehl Incremental: Zugehörige Optionen

Option	Verwendung
absolute	Nur in der Befehlszeile.
Windows-Betriebssystemeautofsrename	Windows-BetriebssystemeNur Clientoptionsdatei (dsm.opt).
Windows-Betriebssystemechangingretries	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-Betriebssystemechangingretries	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDatei dsm.sys oder Befehlszeile.
Windows-Betriebssystemecompressalways	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-Betriebssystemecompressalways	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemecompression	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-Betriebssystemecompression	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDatei dsm.sys innerhalb einer Serverzeilengruppe oder Befehlszeile.
AIX-BetriebssystemeLinux-BetriebssystemeWindows-Betriebssystemedetail	AIX-BetriebssystemeLinux-Betriebssysteme Windows-BetriebssystemeNur in der Befehlszeile.
Linux-BetriebssystemeWindows-Betriebssystemediffsnapshot	Linux-BetriebssystemeWindows-Betriebssysteme Nur in der Befehlszeile.
dirsonly	Nur in der Befehlszeile.
Windows-Betriebssystemedomain	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.

Option	Verwendung
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemedomain	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDatei dsm.sys, Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemeencryptiontype	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe.
Windows-Betriebssystemeencryptiontype	Windows-BetriebssystemeClientoptionsdatei (dsm.opt).
Windows-Betriebssystemeencryptkey	Windows-BetriebssystemeClientoptionsdatei (dsm.opt).
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemeencryptkey	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe.
filelist	Nur in der Befehlszeile.
filesonly	Nur in der Befehlszeile.
incrbydate	Nur in der Befehlszeile.
Windows-Betriebssystememememoryefficientbackup	Windows-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt), Server oder Befehlszeile.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystememememoryefficientbackup	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt), Clientsystemoptionsdatei (dsm.sys), Server oder Befehlszeile.
Windows-Betriebssystemenojournal	Windows-BetriebssystemeNur in der Befehlszeile.
AIX-BetriebssystemeLinux-Betriebssystemenojournal	AIX-BetriebssystemeLinux-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssystemepostsnapshotcmd	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.fs.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssystemepreservelastaccessdate	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemepreservelastaccessdate	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemepresnapshotcmd	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.fs.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMac OS X-Betriebssystemeremoveoperandlimit	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMac OS X-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssystemeresetarchiveattribute	Windows-BetriebssystemeClientoptionsdatei (dsm.opt).
Windows-Betriebssystemeskipntpermissions	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemeskipntsecuritycrc	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Linux-BetriebssystemeWindows-Betriebssystemesnapdiff	Linux-BetriebssystemeWindows-Betriebssysteme Nur in der Befehlszeile.
AIX-BetriebssystemeLinux-Betriebssystemesnapshotcachesize	AIX-BetriebssystemeLinux-Betriebssysteme Clientoptionsdatei (dsm.opt) oder mit der Option include.fs.

Option	Verwendung
AIX-BetriebssystemeWindows-Betriebssystemesnapshotproviderfs	AIX-BetriebssystemeWindows-Betriebssysteme Systemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder mit der Option include.fs.
Windows-Betriebssystemesnapshotproviderimage	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.image.
snapshotroot	Nur in der Befehlszeile.
Windows-Betriebssystemesubdir	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-Betriebssystemesubdir	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme tapeprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-Betriebssystemetapeprompt	AIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Teilsicherung der Clientdomäne ausführen, die in Ihrer Clientbenutzeroptionsdatei (dsm.opt) angegeben ist.

```
Incremental
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Teilsicherung ausführen, bei der alle Dateien in der Domäne gesichert werden, unabhängig davon, ob sie sich seit der lezten Sicherung geändert haben.

```
Incremental -absolute
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine Teilsicherung der Standardclientdomäne ausführen, die in Ihrer Clientoptionsdatei (dsm.opt) angegeben ist.

```
Incremental
```

Windows-BetriebssystemeEine Teilsicherung der Domäne ausführen, die in Ihrer Clientbenutzeroptionsdatei angegeben ist. Mit der Option -absolute wird eine Sicherung aller Dateien in der Domäne erzwungen, auch sie sich seit der letzten Teilsicherung nicht geändert haben.

```
Incremental -absolute
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine Teilsicherung der Laufwerke C, D und E ausführen.

```
incremental c: d: e:
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine Teilsicherung des Verzeichnisses \home\ngai und seines Inhalts im aktuellen Laufwerk ausführen.

```
i \home\ngai\
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Teilsicherung für die Dateisysteme /home, /usr und /proj ausführen.

```
Incremental /home /usr /proj
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Teilsicherung für das Verzeichnis /proj/test ausführen.

```
Incremental /proj/test/
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Teilsicherung nach Datum für das Dateisystem /home ausführen.

```
Incremental -incrbydate /home
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Teilsicherung der Datei abc im Verzeichnis /fs/dir1 ausführen.

```
Incremental -subdir=yes /fs/dir1/abc
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Teilsicherung des Verzeichnisobjekts /fs/dir1, aber nicht für die Dateien im Verzeichnis /fs/dir1 ausführen.

```
Incremental /fs/dir1
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Teilsicherung des Verzeichnisobjekts /fs/dir1, aller Dateien im Verzeichnis fs/dir1 und aller Dateien und Unterverzeichnisse unter /fs/dir1 ausführen.

```
Incremental -subdir=yes /fs/dir1/
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAngenommen, Sie haben eine Momentaufnahme des Dateisystems /usr gestartet und die Momentaufnahme als /snapshot/day1 angehängt. Führen Sie eine Teilsicherung aller Dateien und Verzeichnisse unter der lokalen Momentaufnahme aus und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen /usr.

```
dsmc inc /usr -snapshotroot=/snapshot/day1
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeAngenommen, Sie haben eine Momentaufnahme des Laufwerks C gestartet und die Momentaufnahme als \\florence\c$\snapshots\snapshot.0 angehängt. Führen Sie eine Teilsicherung aller Dateien und Verzeichnisse unter der lokalen Momentaufnahme aus und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen des Laufwerks C:\.

```
dsmc inc c: -snapshotroot=\\florence\c$\snapshots\snapshot.0
```

Linux-BetriebssystemeTask
Linux-BetriebssystemeEine Teilsicherung des Dateisystems /home unter Verwendung der Option snapdiff ausführen und die Option zum Erstellen der Differenzmomentaufnahme angeben. Im folgenden Beispiel ist /home der NFS-Mountpunkt für den Datenträger eines NAS/N-Series-Dateiservers.

```
incremental /home -snapdiff -diffsnapshot=create
```

AIX-BetriebssystemeTask
AIX-BetriebssystemeEine Teilsicherung des Dateisystems /proj unter Verwendung der Option snapdiff ausführen. Die Option zum Verwenden der letzten Momentaufnahme auf dem Dateiserver als Differenzmomentaufnahme angeben. Im folgenden Beispiel ist /proj der NFS-Mountpunkt für den Datenträger eines NAS/N-Series-Dateiservers.

```
incremental /proj -snapdiff -diffsnapshot=latest
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Teilsicherung mit der Option snapdiff auf der Basis einer Momentaufnahme ausführen, die von dem gemeinsam genutzten Netzbereich //homestore.example.com/vol1erstellt wurde, der als Laufwerk H angehängt ist. Dabei ist 'homestore.example.com' ein Dateiserver.

```
incremental -snapdiff H:
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Teilsicherung mit der Option snapdiff auf der Basis einer Momentaufnahme ausführen, die von dem gemeinsam genutzten Netzbereich //homestore.example.com/vol1erstellt wurde, der als Laufwerk H angehängt ist. Dabei ist 'homestore.example.com' ein Dateiserver. Der Wert LATEST der Option -diffsnapshot bedeutet, dass bei der Operation die letzte Momentaufnahme (die aktive Momentaufnahme) für Datenträger H verwendet wird.

```
incremental -snapdiff H: -diffsnapshot=LATEST
```

- Windows-BetriebssystemeUnterstützung offener Dateien
  Wenn die Unterstützung offener Dateien konfiguriert ist, führt der Client für Sichern/Archivieren eine Momentaufnahmesicherung oder -archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder "im Gebrauch") sind.
- Windows-BetriebssystemeJournalbasierte Sicherung
  Wenn der Journalsteuerkomponentenservice installiert und aktiv ist, führt der Befehl incremental standardmäßig eine journalbasierte Sicherung für Dateisysteme aus, die vom Journalsteuerkomponentenservice überwacht werden.
- AIX-BetriebssystemeLinux-BetriebssystemeJournalbasierte Sicherung
  Eine Sicherung für ein bestimmtes Dateisystem ist journalbasiert, wenn der IBM Spectrum Protect-Journaldämon installiert und für die

Aufzeichnung des Dateisystems im Journal konfiguriert wurde und wenn ein gültiges Journal erstellt wurde.

- NTFS- oder ReFS-Datenträgermountpunkte sichern
  Bei einer Teilsicherung eines Dateisystems, in dem ein Datenträgermountpunkt vorhanden ist, sichert IBM Spectrum Protect das Verzeichnis (die Zusammenführung), in dem der Datenträger bereitgestellt wurde; die Daten auf dem bereitgestellten Datenträger werden jedoch nicht traversiert oder gesichert.
-  Windows-BetriebssystemeMicrosoft DFS-Stamm sichern
  Wenn Sie eine Teilsicherung des Microsoft DFS-Stammes mit der Angabe dfsbackupmntpnt=*yes* ausführen, sichert der Client für Sichern/Archivieren nur die Zusammenführungspunkte, *nicht* die Unterverzeichnisstruktur unter den Zusammenführungen.
- Teilsicherung nach Datum
  Bei einer Teilsicherung nach Datum werden neue und geänderte Dateien mit einem Änderungsdatum gesichert, das nach dem Datum der letzten auf dem Server gespeicherten Teilsicherung liegt, sofern die Dateien nicht durch eine **Exclude**-Anweisung von der Sicherung ausgeschlossen sind.
- Lokale Momentaufnahme einem Serverdateibereich zuordnen
  Verwenden Sie die Option snapshotroot im Befehl incremental mit einer Anwendung eines anderen Anbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

 Windows-Betriebssysteme

Unterstützung offener Dateien

Wenn die Unterstützung offener Dateien konfiguriert ist, führt der Client für Sichern/Archivieren eine Momentaufnahmesicherung oder -archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder "im Gebrauch") sind.

Verwenden Sie VSS als Momentaufnahmeprovider. Setzen Sie snapshotproviderimage oder snapshotproviderfs auf VSS.

Anmerkung:

1. Sie können die Option include.fs verwenden, um Momentaufnahmeoptionen pro Dateisystem festzulegen.
2. Die Unterstützung offener Dateien ist nur verfügbar für lokale fixierte Datenträger (entweder an Laufwerkbuchstaben oder Datenträgermountpunkte angehängt), die mit NTFS-Dateisystemen formatiert sind. Diese Unterstützung schließt an ein SAN angeschlossene Datenträger ein, die diese Anforderungen erfüllen.
3. Wenn der Client keine Momentaufnahme erstellen kann, findet eine Übernahme in einer Nicht-OFS-Sicherung statt; dieselbe Sicherungsunterstützung, die erfolgen würde, wenn die OFS-Funktion nicht konfiguriert wäre.
4. Damit die Unterstützung offener Dateien in einer Clusterumgebung aktiviert wird, sollte für alle Systeme im Cluster die OFS-Funktion konfiguriert sein.

 Windows-Betriebssysteme

Journalbasierte Sicherung

Wenn der Journalsteuerkomponentenservice installiert und aktiv ist, führt der Befehl incremental standardmäßig eine journalbasierte Sicherung für Dateisysteme aus, die vom Journalsteuerkomponentenservice überwacht werden.

Der Client für Sichern/Archivieren verwendet nicht die Journalfunktion, die in Windows NTFS- oder ReFS-Dateisysteme oder andere Journaling-Dateisysteme integriert ist.

Die Journalsteuerkomponente zeichnet Änderungen an einem Objekt oder seinen Attributen in einer Journaldatenbank auf. Während einer journalbasierten Sicherung ruft der Client eine Liste der Dateien, die für eine Sicherung ausgewählt werden können, aus der Journaldatenbank ab. Eine regelmäßige Durchführung von Sicherungen bewahrt die Größe des Journals.

Die journalbasierte Sicherung kann die Sicherungsleistung verbessern. Bei einer journalbasierten Sicherung muss der Client nicht die lokalen Dateisysteme durchsuchen oder Informationen vom Server abrufen, um festzustellen, welche Dateien verarbeitet werden müssen. Die journalbasierte Sicherung verringert auch den Datenaustausch im Netz zwischen dem Client und dem Server.

Der Client filtert die Liste mithilfe der aktuellen Einschluss-/Ausschlussliste. IBM Spectrum Protect verarbeitet und aktualisiert die Ergebnisdateien gemäß Maßnahmenvorgaben, wie beispielsweise der Nummerierung, und lässt sie gemäß dieser Vorgaben verfallen. Das Verwaltungsklassenattribut für die Kopienhäufigkeit wird während der journalbasierten Sicherung ignoriert.

Der Journalsteuerkomponentenservice schließt bestimmte Systemdateien (Auslagerungsdatei, Registrierung usw.) von der Aufzeichnung ihrer Änderungen im Journal aus. Da Änderungen dieser Dateien nicht im Journal aufgezeichnet werden, werden diese Dateien vom Client nicht gesichert. Suchen Sie in der Konfigurationsdatei des Journalservice tsmjbbd.ini im Installationsverzeichnis des Clients für Sichern/Archivieren nach bestimmten ausgeschlossenen Systemdateien.

Zur Unterstützung der journalbasierten Sicherung müssen Sie den Journalsteuerkomponentenservice installieren. Verwenden Sie für die Installation dieses Service den Befehl dsmcutil oder den Setup-Assistenten der GUI.

Handelt es sich bei der Dateispezifikation im Befehl incremental um einen Dateibereich, verarbeitet der Client alle Journaleinträge für diesen Dateibereich. Der Client verarbeitet Verzeichnisse und Dateispezifikationen mit Platzhalterzeichen auf dieselbe Weise. Der Client verwendet die Domänenliste, wenn Sie keine Dateispezifikation angeben.

Anmerkung: Die journalbasierte Sicherung wird möglicherweise nicht wieder durch die traditionelle Teilsicherung ersetzt, wenn die Maßnahmendomäne Ihres Knotens auf dem Server geändert wird. Dies ist vom Zeitpunkt der letzten Aktualisierung der Maßnahmengruppe in der Domäne und vom Datum der letzten Teilsicherung abhängig. In diesem Fall müssen Sie eine traditionelle vollständige Teilsicherung erzwingen, um die Dateien erneut an die neue Domäne zu binden. Verwenden Sie die Option nojournal im Befehl incremental, um anzugeben, dass statt der standardmäßigen journalbasierten Sicherung eine traditionelle vollständige Teilsicherung ausgeführt werden soll.

Wenn ein Benutzer eine Datei mit einem langen Namen löscht, übergibt das Windows-Betriebssystem möglicherweise einen Kurznamen (komprimierten Namen) an den Journalsteuerkomponentenservice. Nach dem Löschen des Objekts kann der komprimierte Name erneut verwendet werden, und der Löschhinweis gibt möglicherweise kein eindeutiges Objekt mehr an. Während einer journalbasierten Teilsicherung schlägt der Versuch, die Datei verfallen zu lassen, fehl, da der komprimierte Name dem Server nicht bekannt ist. In diesem Fall wird ein Satz in das Journal eingefügt, der anzeigt, dass das aktuelle Verzeichnis auf dem Server nicht exakt dargestellt ist. Mit der Option incrthreshold können Sie angeben, welche Aktion in diesem Fall ausgeführt wird.

Die Journaldatenbank wird als ungültig betrachtet und der Client kehrt zur traditionellen vollständigen Teilsicherung zurück, wenn eins der folgenden Ereignisse auftritt:

- Der Name eines Journaldateibereichs ändert sich.
- Der Name des Clientknotens ändert sich.
- Der Client nimmt Kontakt zu einem anderen Server auf, um die Sicherung durchzuführen.
- Eine Maßnahmenänderung tritt auf (Aktivierung einer neuen Maßnahmengruppe).
- Das Journal ist beschädigt (Bedingungen 'Kein Speicher mehr', Plattenfehler).
- Der Journalservice ist nicht aktiv.
- Der Journalservice wird aus irgendeinem Grund gestoppt oder gestartet, selbst, wenn er aufgrund eines Warmstarts des Systems erneut gestartet wird.

Die journalbasierte Sicherung unterscheidet sich von der traditionellen vollständigen Teilsicherung wie folgt:

- IBM Spectrum Protect erzwingt keine nicht standardmäßigen Kopienhäufigkeiten (außer 0).
- Attributänderungen an einem Objekt erfordern eine Sicherung des gesamten Objekts.

Sie können die Option nojournal im Befehl incremental verwenden, um anstelle der standardmäßigen journalbasierten Sicherung eine traditionelle vollständige Teilsicherung auszuführen.

Mehrere Sitzungen für journalbasierte Sicherungen sind möglich.

 AIX-Betriebssysteme  Linux-Betriebssysteme

Journalbasierte Sicherung

Eine Sicherung für ein bestimmtes Dateisystem ist journalbasiert, wenn der IBM Spectrum Protect-Journaldämon installiert und für die Aufzeichnung des Dateisystems im Journal konfiguriert wurde und wenn ein gültiges Journal erstellt wurde.

 AIX-BetriebssystemeDie journalbasierte Sicherung wird auf dem AIX-Client für Sichern/Archivieren auf JFS- und JFS2-Dateisystemen unterstützt.

 Linux-BetriebssystemeDie journalbasierte Sicherung wird auf dem Linux-Client für Sichern/Archivieren für Ext2, Ext3, Ext4, XFS, ReiserFS, JFS, VxFS und NSS unterstützt. GPFS wird für journalbasierte Sicherungen unter Linux nicht unterstützt.

Wenn der Journaldämon installiert und aktiv ist, führt der Befehl incremental standardmäßig eine journalbasierte Sicherung für Dateisysteme aus, die vom Dämon der Journalsteuerkomponente überwacht werden. Die folgenden Bedingungen müssen erfüllt sein, damit eine journalbasierte Sicherung erfolgreich ausgeführt werden kann:

- Der Journaldämon muss zum Überwachen des Dateisystems konfiguriert sein, das die Dateien und Verzeichnisse enthält, die gesichert werden.
- Für das Dateisystem, das gesichert wird, muss mindestens eine erfolgreiche vollständige Teilsicherung ausgeführt worden sein.
- Das Dateibereichimage des Dateisystems auf dem Server darf nach der letzten vollständigen Teilsicherung nicht durch einen Verwaltungsbefehl geändert worden sein.
- Die Speicherverwaltungsmaßnahme für die Dateien, die gesichert werden, darf nach der letzten vollständigen Teilsicherung nicht aktualisiert worden sein.

Der Journaldämon zeichnet Änderungen an einem Objekt oder seinen Attributen in einer Journaldatenbank auf. Während einer journalbasierten Sicherung ruft der Client eine Liste der Dateien, die für eine Sicherung ausgewählt werden können, aus der Journaldatenbank ab. Die journalbasierte Sicherung kann die Leistung beim Sichern verbessern, da der Client nicht das lokale Dateisystem durchsuchen oder den Server kontaktieren muss, um festzustellen, welche Dateien verarbeitet werden müssen. Die journalbasierte Sicherung verringert auch den Datenaustausch im Netz zwischen dem Client und dem Server.

Der Client für Sichern/Archivieren filtert die Liste auf der Basis der aktuellen Einschluss-/Ausschlussliste und verarbeitet und aktualisiert die Ergebnisdateien gemäß Maßnahmenvorgaben, wie beispielsweise der Nummerierung, und lässt sie gemäß dieser Vorgaben verfallen. Der Client ignoriert jedoch das Häufigkeitsattribut des Servers während einer journalbasierten Sicherung. Der Grund hierfür ist, dass eine journalbasierte Sicherung die Abfrage der Sicherungsversion beim Server überflüssig macht; daher weiß der Client nicht, wie viele Tage seit der letzten Sicherung der Datei vergangen sind.

Der Journaldämon zeichnet keine Änderungen in speziellen UNIX-Dateien auf.

Der Journaldämon schließt bestimmte Dateien von der Aufzeichnung ihrer Änderungen im Journal aus. Da Änderungen dieser Dateien nicht im Journal aufgezeichnet werden, werden diese Dateien vom Client nicht gesichert. Suchen Sie in der Konfigurationsdatei des Journaldämons, `tsmjbbd.ini`, im Installationsverzeichnis des Clients für Sichern/Archivieren nach bestimmten ausgeschlossenen Systemdateien.

Anmerkung:

1. Wird Antivirensoftware verwendet, unterliegt die journalbasierte Sicherung gewissen Einschränkungen. Bestimmte Antivirensoftware kann fälschlicherweise Änderungsbenachrichtigungen für den IBM Spectrum Protect-Journalservice generieren. Dies hat zur Folge, dass Dateien, die sich nicht geändert haben, bei einer journalbasierten Sicherung fälschlicherweise gesichert werden. Verwenden Sie Norton Anti-Virus Corporate Edition 8.0 oder höher, um diese Probleme zu vermeiden.
2. Eine journalbasierte Sicherung wird möglicherweise nicht wieder durch die traditionelle Teilsicherung ersetzt, wenn die Maßnahmendomäne Ihres Knotens auf dem Server geändert wird. Dies ist vom Zeitpunkt der letzten Aktualisierung der Maßnahmengruppe in der Domäne und vom Datum der letzten Teilsicherung abhängig. In diesem Fall müssen Sie eine traditionelle vollständige Teilsicherung erzwingen, um die Dateien erneut an die neue Domäne zu binden. Verwenden Sie die Option nojournal im Befehl incremental, um anzugeben, dass statt der standardmäßigen journalbasierten Sicherung eine traditionelle vollständige Teilsicherung ausgeführt werden soll.

    AIX-BetriebssystemeFügen Sie unter AIX 6.1 (oder höher) der Datei `tsmjbbd.ini` eine Anweisung zum Ausschließen von Momentaufnahmen hinzu, um zu verhindern, dass interne JFS2-Momentaufnahmeverzeichnisse vom Dämon für die journalbasierte Sicherung überwacht werden. Wenn Sie die Momentaufnahmeverzeichnisse nicht ausschließen, werden die darin enthaltenen Dateien gesichert. Die Sicherung der Momentaufnahmeverzeichnisse ist eine redundante Sicherung, mit der Serverspeicherbereich verschwendet wird.

Unter den folgenden Bedingungen wird die Journaldatenbank als ungültig betrachtet und der Client kehrt zur traditionellen vollständigen Teilsicherung zurück:

- Der Name eines Journaldateibereichs wurde geändert.
- Der Name des Clientknotens wurde geändert.
- Der Client nimmt Kontakt zu einem anderen Server auf, um die Sicherung durchzuführen.
- Es sind Maßnahmenänderungen aufgetreten (Aktivierung einer neuen Maßnahmengruppe).
- Das Journal ist beschädigt (Bedingungen 'Kein Speicher mehr', Plattenfehler).
- Das Journal ist nicht aktiv.

Die journalbasierte Sicherung unterscheidet sich von der traditionellen vollständigen Teilsicherung wie folgt:

- IBM Spectrum Protect erzwingt keine nicht standardmäßigen Kopienhäufigkeiten (außer 0).
- Änderungen in speziellen UNIX-Dateien werden nicht festgestellt.

Sie können die Option nojournal im Befehl incremental verwenden, um anstelle der standardmäßigen journalbasierten Sicherung eine traditionelle vollständige Teilsicherung auszuführen.

 Windows-Betriebssysteme

NTFS- oder ReFS-Datenträgermountpunkte sichern

Bei einer Teilsicherung eines Dateisystems, in dem ein Datenträgermountpunkt vorhanden ist, sichert IBM Spectrum Protect das Verzeichnis (die Zusammenführung), in dem der Datenträger bereitgestellt wurde; die Daten auf dem bereitgestellten Datenträger werden jedoch nicht traversiert oder gesichert.

Wenn z. B. C:\mount ein Mountpunkt ist, werden bei einer Teilsicherung des Laufwerks C:\ nur die Zusammenführung (C:\mount) und nicht die Daten unter C:\mount gesichert.

- Daten auf über NTFS oder ReFS angehängten Datenträgern sichern
  Die Sicherung eines Datenträgers an einem Mountpunkt ist besonders nützlich für Datenträger ohne Laufwerkzuordnung. Wenn für den Verweis auf den am Mountpunkt angehängten Datenträger auch ein Laufwerkbuchstabe verwendet werden kann, muss der Datenträger nicht über den Mountpunkt gesichert werden.

Zugehörige Konzepte:
Mountpunkte für NTFS- oder ReFS-Datenträger zurückschreiben
Daten auf über NTFS angehängten Datenträgern zurückschreiben
Daten auf über NTFS oder ReFS angehängten Datenträgern sichern
 Windows-Betriebssysteme

Microsoft DFS-Stamm sichern

Wenn Sie eine Teilsicherung des Microsoft DFS-Stammes mit der Angabe dfsbackupmntpnt=*yes* ausführen, sichert der Client für Sichern/Archivieren nur die Zusammenführungspunkte, *nicht* die Unterverzeichnisstruktur unter den Zusammenführungen.

Soll die DFS-Verzeichnisstruktur traversiert werden und sollen die Dateien und Unterverzeichnisse aller gefundenen Zusammenführungen gesichert werden, geben Sie die Option dfsbackupmntpnt=*no* an. Sollen sowohl die DFS-Baumstruktur als auch das in der DFS-Baumstruktur enthaltene Datum gesichert werden, müssen Sie zwei Sicherungen ausführen: eine mit der Angabe dfsbackupmntpnt=*yes* und eine mit der Angabe dfsbackupmntpnt =*no*.

Diese Option bleibt bei der Sicherung einzelner Zusammenführungen ohne Wirkung. Die Funktionsweise der Option ***exclude.dir*** ist bei DFS-Zusammenführungen dieselbe wie bei angehängten virtuellen Datenträgern.

Anmerkung: Wird ein DFS-Stamm hinzugefügt oder geändert, wird er vom Client nicht gesichert. Sie müssen den DFS-Stamm in der Option domain in der Clientoptionsdatei (dsm.opt) angeben und zwar unabhängig davon, ob DOMAIN ALL-LOCAL angegeben ist.

Teilsicherung nach Datum

Bei einer Teilsicherung nach Datum werden neue und geänderte Dateien mit einem Änderungsdatum gesichert, das nach dem Datum der letzten auf dem Server gespeicherten Teilsicherung liegt, sofern die Dateien nicht durch eine **Exclude**-Anweisung von der Sicherung ausgeschlossen sind.

Windows-BetriebssystemeWird eine Teilsicherung nach Datum nur für einen Teil eines Dateisystems ausgeführt, wird das Datum der letzten vollständigen Teilsicherung nicht aktualisiert; bei der nächsten Teilsicherung nach Datum werden die Dateien dann wieder gesichert. Das Datum und die Zeit der letzten Teilsicherung des gesamten Dateisystems können mit dem Befehl query filespace bestimmt werden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWird eine Teilsicherung nach Datum nur für einen Teil eines Dateisystems ausgeführt, wird das Datum der letzten vollständigen Teilsicherung nicht aktualisiert; bei der nächsten Teilsicherung nach Datum werden die Dateien dann wieder gesichert. Änderungen der Zugriffssteuerungslisten (ACL) oder der erweiterten Attribute bewirken nicht, dass die Dateien während einer Teilsicherung nach Datum gesichert werden. Das Datum und die Zeit der letzten Teilsicherung des gesamten Dateisystems können mit dem Befehl query filespace bestimmt werden.

Für eine Teilsicherung nach Datum geben Sie die Option incrbydate im Befehl incremental an.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Anders als eine vollständige Teilsicherung hält die Teilsicherung nach Datum den Serverspeicher nicht auf dem aktuellen Stand *aller* Workstationdateien, weil:

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme Windows-BetriebssystemeSicherungsversionen von Dateien, die aus der Workstation gelöscht wurden, hierbei nicht verfallen.
- Sicherungsversionen nicht erneut an eine neue Verwaltungsklasse gebunden werden, wenn sich die Verwaltungsklasse geändert hat.
- Dateien mit geänderten Attributen nur dann gesichert werden, wenn sich auch das Änderungsdatum und die Änderungszeit geändert haben.
- Das Attribut 'Häufigkeit' der Kopiengruppe in den Verwaltungsklassen ignoriert wird.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Aus diesen Gründen sollten bei Zeitmangel für die Ausführung von Sicherungen während der Woche Teilsicherungen nach Datum ausgeführt werden. Am Wochenende, wenn mehr Zeit zur Verfügung steht, kann dann eine vollständige Teilsicherung erfolgen, um den Serverspeicher auf den aktuellen Stand Ihrer Workstationdateien zu bringen.

Wenn der Befehl incremental wegen eines Übertragungs- oder Sitzungsfehlers wiederholt wird, zeigen die Übertragungsstatistiken die Anzahl Bytes an, die der Client während aller Befehlswiederholungen zu übertragen versucht hat. Daher entsprechen die Statistiken für die übertragenen Byte möglicherweise nicht den Dateistatistiken, z. B. für die Dateigröße.

Lokale Momentaufnahme einem Serverdateibereich zuordnen

Verwenden Sie die Option snapshotroot im Befehl incremental mit einer Anwendung eines anderen Anbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind.

Die Option snapshotroot bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

Loop

Der Befehl loop startet eine interaktive Befehlszeilensitzung, die aktiv ist, bis Sie `quit` eingeben.

Wenn für Sie ein Kennwort erforderlich ist, werden Sie zur Eingabe dieses Kennworts aufgefordert, bevor die Eingabeaufforderung für den Schleifenmodus angezeigt wird.
Anmerkung: Es ist nicht möglich, den Schleifenmodus zu aktivieren, ohne dass eine Verbindung zu einem gültigen Server besteht. Eine der Folgen dieses Sachverhalts ist, dass bestimmte Befehle wie beispielsweise `restore backupset -location=file` nur dann in der Anfangsbefehlszeile akzeptiert werden, wenn ein gültiger Server nicht verfügbar ist.

Bei einer interaktiven Befehlszeilensitzung müssen Sie den einzelnen Befehlsnamen nicht die Zeichenfolge **dsmc** und das Kennwort (falls ein Kennwort erforderlich ist) voranstellen.

 Im interaktiven Modus überschreiben die Optionen, die Sie in der Anfangsbefehlszeile eingeben, den Wert, den Sie in Ihrer Clientoptionsdatei (dsm.opt) angegeben haben. Dieser Wert bleibt für die gesamte interaktive Sitzung aktiv, solange er nicht durch einen anderen Wert in einem angegebenen interaktiven Befehl überschrieben wird. Beispiel: Wenn Sie die Option subdir in Ihrer Clientoptionsdatei (dsm.opt) auf *yes* setzen und in der Anfangsbefehlszeile subdir=*no* angeben, bleibt die Einstellung subdir=*no* während der gesamten interaktiven Sitzung aktiv, wenn sie nicht durch den Wert subdir=*yes* in einem angegebenen interaktiven Befehl überschrieben wird. Der Wert subdir=*yes* betrifft jedoch nur den Befehl, in dem er eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf subdir=*no* zurückgesetzt, d. h. auf den Wert, den die Option zu Beginn der interaktiven Sitzung hatte.

    Im interaktiven Modus überschreiben die Optionen, die Sie in der Anfangsbefehlszeile eingeben, den Wert, den Sie in Ihrer Clientbenutzeroptionsdatei (dsm.opt) oder in der Datei dsm.sys angegeben haben. Dieser Wert bleibt für die gesamte interaktive Sitzung aktiv, solange er nicht durch einen anderen Wert in einem angegebenen interaktiven Befehl überschrieben wird. Beispiel: Wenn Sie die Option subdir in Ihrer Clientbenutzeroptionsdatei (dsm.opt) auf *yes* setzen und in der Anfangsbefehlszeile subdir=*no* angeben, bleibt die Einstellung subdir=*no* während der gesamten interaktiven Sitzung aktiv, wenn sie nicht durch den Wert subdir=*yes* in einem angegebenen interaktiven Befehl überschrieben wird. Der Wert subdir=*yes* betrifft jedoch nur den Befehl, in dem er eingegeben wird. Wenn dieser Befehl beendet ist, wird der Wert auf subdir=*no* zurückgesetzt, d. h. auf den Wert, den die Option zu Beginn der interaktiven Sitzung hatte.

Sie können alle gültigen Befehle im interaktiven Modus eingeben, *mit Ausnahme* der Befehle schedule und loop.

Einige Optionen können Sie in der vom Befehl loop erstellten interaktiven Sitzung nicht verwenden; diese werden in der Optionsbeschreibung durch die folgende Anweisung identifiziert: *Diese Option ist nur in der Anfangsbefehlszeile gültig. Im interaktive Modus ist sie nicht gültig.*

    Anmerkung:

1. Im Schleifenmodus wird der Mountpunkt nach einer Zurückschreibungsoperation direkt vom Band nicht freigegeben, falls weitere Zurückschreibungsanforderungen an den Datenträger gestellt werden. Wenn Sie eine Sicherungsoperation in derselben Sitzung anfordern und dieser Mountpunkt der einzig verfügbare ist, stoppt die Sicherungsoperation mit der folgenden Nachricht:

   ```
   Auf Laden von Offlinedatenträger warten
   ```

   In diesem Fall wird der Mountpunkt erst freigegeben, wenn eine der folgenden Bedingungen erfüllt ist:
   - Der Grenzwert der Einheitenklasse MOUNTRETENTION ist erreicht.
   - Das Clientinaktivitätszeitlimit ist erreicht.
   - Die Sitzung dsmc loop wird geschlossen, nachdem die Zurückschreibungsoperation beendet ist. Dies ermöglicht Ihnen den Start einer nachfolgenden Sitzung im Schleifenmodus, um die Sicherungsoperation auszuführen.
2. Im interaktiven Modus können Sie keine Dateispezifikation eingeben, die Sonderzeichen in der Landessprache enthält. Wenn ein Befehl nationale Sonderzeichen enthält, müssen Sie ihn im Stapelmodus verarbeiten, indem Sie dem Befehl den Namen des ausführbaren Programms **dsmc** voranstellen.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-LOOP-------------------------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task

Eine interaktive Befehlszeilensitzung starten.

Befehl: `dsmc`

Geben Sie bei der Eingabeaufforderung `Protect>` einen Befehl ein.

 Zum Beenden einer interaktiven Sitzung geben Sie `quit` ein.

    Es gibt zwei Methoden zum Beenden einer interaktiven Sitzung:

- Geben Sie `quit` ein.
- Wenn Sie editor=*yes* definiert haben, können Sie wie folgt vorgehen:
  1. Drücken Sie die Abbruchtaste (Esc).
  2. Geben Sie Q ein und drücken Sie die Eingabetaste.

   AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeAnmerkung: Die Standardeinstellung ist editor=*yes*.

Anmerkung: Soll ein Befehl dsmc abgebrochen werden, bevor der Client die Verarbeitung beendet hat, geben Sie QQ an der IBM Spectrum Protect-Konsole ein. In vielen, aber nicht in allen Fällen wird der Befehl dadurch abgebrochen.

Macro

Der Befehl macro führt eine Serie von Befehlen aus, die Sie in einer Makrodatei angeben.

Wenn Sie den Befehl macro in einer Makrodatei angeben, können Sie bis zu 10 Befehlsebenen verschachteln.

Kommentarzeilen werden innerhalb der Makrodatei, die Sie für den Befehl macro angeben, nicht unterstützt.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-MAcro-- --Makroname-----------------------------------------><
```

Parameter

Makroname
: Gibt den vollständig qualifizierten Namen der Datei an, in der sich die Befehle befinden.

Beispiele

Das folgende Beispiel zeigt die Verwendung des Befehls macro.

Task
: Dateien in den folgenden Verzeichnissen selektiv sichern:

-  Windows-Betriebssysteme`c:\devel\project\proja`
-  Windows-Betriebssysteme`c:\devel\project\projb`
-  Windows-Betriebssysteme`c:\devel\project\projc`
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme `/devel/project/proja`
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme `/devel/project/projb`
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme `/devel/project/projc`

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
 Windows-Betriebssysteme**Befehl:**`macro backabc.mac`

Dabei enthält `backabc.mac` die folgenden Anweisungen:  AIX-BetriebssystemeLinux-Betriebssysteme
Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

```
Selective /devel/project/proja/
Selective /devel/project/projb/
Selective /devel/project/projc/
```

 Windows-Betriebssysteme

```
selective c:\devel\project\proja\*.*
selective c:\devel\project\projb\*.*
selective c:\devel\project\projc\*.*
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Monitor Process

Der Befehl monitor process zeigt (sofern die NDMP-Unterstützung aktiviert ist) eine Liste der aktuellen NAS-Imagesicherungs- und -zurückschreibungsprozesse an, für die der Benutzer mit Verwaltungsaufgaben die Berechtigung hat. Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.

Der Benutzer mit Verwaltungsaufgaben kann dann einen Prozess für die Überwachung auswählen. Die Clienteignerberechtigung ist als Berechtigung ausreichend, um die ausgewählten NAS-Imagesicherungs- oder -zurückschreibungsprozesse zu überwachen.

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDieser Befehl ist nur für AIX-, Linux- und Solaris-Clients gültig.

 Windows-BetriebssystemeDieser Befehl ist für alle Windows-Clients gültig.

Syntax

```
>>-MONitor Process-----------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task
: Die aktuellen NAS-Imagesicherungs- oder -zurückschreibungsprozesse überwachen.

  Befehl: `monitor process`

Preview Archive

Der Befehl preview archive simuliert einen Archivierungsbefehl, ohne Daten an den Server zu senden.

Der Befehl preview archive generiert eine tabulatorbegrenzte Textdatei, die in ein Tabellenkalkulationsprogramm importiert werden kann. Die Voranzeige enthält Informationen wie z. B., ob die Datei ausgeschlossen oder eingeschlossen ist. Ist die Datei ausgeschlossen, wird das Muster oder die Ursache für den Ausschluss der Datei zusammen mit der Quelle für das Muster aufgeführt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
                                        .- -filter=ALL--.
>>-PREview--Archive--Dateispezifikation--+- -filter=INCL-+------>
                                        '- -filter=EXCL-'

>--+-----------------------+--+-----------+--------------------->
   '- -FILEName= Dateiname-'  '- -CONsole-'

   .- -TRAverse=Yes-.
>--+----------------+-------------------------------------------><
   '- -TRAverse=No--'
```

Parameter

Dateispezifikation
: Gibt den Pfad und den Namen der Datei an, die archiviert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis auszuwählen.

-filter
: Gibt die anzuzeigende Ausgabe an. Sie können eingeschlossene Objekte, ausgeschlossene Objekte oder beides anzeigen.

  ALL
  : Ausgabe für eingeschlossene und ausgeschlossene Objekte anzeigen. Dies ist der Standardwert.

  INCLuded

Nur Ausgabe für eingeschlossene Objekte anzeigen.

EXCLuded
Nur Ausgabe für ausgeschlossene Objekte anzeigen.

-FILEName=
Gibt den Namen der Datei an, in die die durch Tabulatoren getrennte Ausgabe geschrieben werden soll. Der Standardwert ist dsmprev.txt.

-CONsole
Die Ausgabe wird auf die Konsole und in die Datei geschrieben.

-TRAverse
Die Voranzeige für die aktuellen Verzeichnisse und ihre Unterverzeichnisse anzeigen.

Yes
Die Voranzeige für die aktuellen Verzeichnisse und ihre Unterverzeichnisse anzeigen. Dies ist der Standardwert.

No
Die Voranzeige nur für die aktuellen Verzeichnisse und nicht für ihre Unterverzeichnisse anzeigen.

Wichtig: Bei der Angabe von **-traverse** wird keine Voranzeige für Verzeichnisse angezeigt, die mit der Option exclude.dir ausgeschlossen wurden.

Preview Backup

Der Befehl preview backup simuliert einen Sicherungsbefehl, ohne Daten an den Server zu senden.

Der Befehl preview backup generiert eine tabulatorbegrenzte Textdatei, die in ein Tabellenkalkulationsprogramm importiert werden kann. Die Voranzeige enthält Informationen wie z. B., ob die Datei ausgeschlossen oder eingeschlossen ist. Ist die Datei ausgeschlossen, wird das Muster oder die Ursache für den Ausschluss der Datei zusammen mit der Quelle für das Muster aufgeführt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
                                        .- -filter=ALL--.
>>-PREview--backup--Dateispezifikation--+- -filter=INCL-+------->
                                        '- -filter=EXCL-'

>--+-----------------------+--+-----------+--------------------->
   '- -FILEName= Dateiname-'  '- -CONsole-'

   .- -TRAverse=Yes-.
>--+----------------+-------------------------------------------><
   '- -TRAverse=No--'
```

Parameter

Dateispezifikation
Gibt den Pfad und den Namen der Datei an, die gesichert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis auszuwählen.

-filter
Gibt die anzuzeigende Ausgabe an. Sie können eingeschlossene Objekte, ausgeschlossene Objekte oder beides anzeigen.

ALL
Ausgabe für eingeschlossene und ausgeschlossene Objekte anzeigen. Dies ist der Standardwert.

INCLuded
Nur Ausgabe für eingeschlossene Objekte anzeigen.

EXCLuded
Nur Ausgabe für ausgeschlossene Objekte anzeigen.

-FILEName=
Gibt den Namen der Datei an, in die die durch Tabulatoren getrennte Ausgabe geschrieben werden soll. Der Standardwert ist dsmprev.txt.

-CONsole
Die Ausgabe wird auf die Konsole und in die Datei geschrieben.

-TRAverse
Die Voranzeige für die aktuellen Verzeichnisse und ihre Unterverzeichnisse anzeigen.

Yes

Die Voranzeige für die aktuellen Verzeichnisse und ihre Unterverzeichnisse anzeigen. Dies ist der Standardwert.

No
Die Voranzeige nur für die aktuellen Verzeichnisse und nicht für ihre Unterverzeichnisse anzeigen.

Wichtig: Bei der Angabe von **-traverse** wird keine Voranzeige für Verzeichnisse angezeigt, die mit der Option exclude.dir ausgeschlossen wurden.

Query Access

Der Befehl query access zeigt an, welchen Benutzern Zugriff auf Sicherungsversionen und Archivierungskopien bestimmter Dateien erteilt wurde.

Der Client für Sichern/Archivieren zeigt eine Liste der Berechtigungsregeln an, die Sie mit dem Befehl set access oder über die Menüoption Dienstprogramme > Knotenzugriffsliste in der grafischen Benutzerschnittstelle (Graphical User Interface, GUI) des Clients für Sichern/Archivieren definiert haben.

Die folgenden Informationen sind enthalten.

- Die einem Benutzer erteilte Berechtigung zum Zurückschreiben von Sicherungsversionen oder zum Abrufen von Archivierungskopien.
- Der Knotenname des Benutzers, dem die Berechtigung erteilt wurde.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie ID des Benutzers auf dem Knoten, dem die Berechtigung erteilt wurde.
- Die Dateien, auf die der Benutzer Zugriff hat.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query ACcess-------------------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task
Eine Liste der Benutzer anzeigen, die Zugriff auf Ihre Dateien haben.

Befehl: `query access`

Windows-Betriebssysteme

Query Adobjects

Verwenden Sie den Befehl query adobjects, um Informationen zu den gelöschten Objekten anzuzeigen, die sich in der lokalen Active Directory-Domäne befinden.

Auf Clients von Windows Server-Betriebssystemen können Informationen zu Active Directory-Objekten auch von vollständigen Systemstatussicherungen auf dem Server abgerufen werden.

Unterstützte Clients

Dieser Befehl ist nur für Windows Server-Betriebssystemclients gültig.

Syntax

```
>>-Query ADOBJects--+-----------------------------+------------>
                    '- --Quellenpfadspezifikation-'

>--+----------+-------------------------------------------------><
   '-Optionen-'
```

Parameter

Quellenpfadspezifikation
: Gibt das Active Directory-Objekt oder den Container für die Abfrage an. Sie können einen Stern (*) als Platzhalterzeichen angeben. Sie können entweder den vollständigen definierten Namen eines Objekts oder Containers angeben oder nur das Namensattribut (cn oder ou) und dabei Platzhalterzeichen verwenden. Sie können auch die Objekt-GUID in geschweiften Klammern ({}) angeben. Die folgenden Sonderzeichen erfordern ein Escapezeichen, den umgekehrten Schrägstrich (\), wenn sie in dem Namen enthalten sind:

  - \
  - #
  - +
  - =
  - <
  - >

  Beispielsweise wird "`cn=test#`" als "`cn=test\#`" eingegeben.

  Der Client kann keine Objektnamen anzeigen, die einen Stern (*) als Teil des Namens enthalten.

Tabelle 1. Befehl Query Adobjects: Zugehörige Optionen

Option	Verwendung
adlocation	Nur in der Befehlszeile.
dateformat	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
detail	Nur in der Befehlszeile.
pitdate (Option wird ignoriert, wenn adlocation nicht angegeben ist)	Nur in der Befehlszeile.
pittime (Option wird ignoriert, wenn adlocation nicht angegeben ist)	Nur in der Befehlszeile.
scrolllines	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
scrollprompt	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
timeformat	Clientoptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task
: Alle lokalen gelöschten Objekte abfragen.

  Befehl: `query adobjects`

Task
: Alle lokalen gelöschten Objekte für einen Benutzer abfragen, dessen Name mit `Fred` beginnt.

  Befehl: `query adobjects "cn=Fred*" -detail`

Task
: Alle Objekte abfragen, die sich im Container `Users` der Domäne `bryan.test.example.com` auf dem Server befinden.

  Befehl: `query adobjects "cn=Users,DC=bryan,DC=test,DC=ibm,DC=com" -adloc=server`

Task
: Alle lokalen gelöschten Objekte für die Organisationseinheit `testou` abfragen.

  Befehl: `query adobjects "ou=testou"`

Task
: Die lokalen gelöschten Objekte mit der GUID `E079130D-3451-4C69-8349-31747E26C75B` abfragen.

  Befehl: `query adobjects {E079130D-3451-4C69-8349-31747E26C75B}`

Query Archive

Der Befehl query archive zeigt eine Liste Ihrer archivierten Dateien und folgende Informationen zu jeder Datei an: Dateigröße, Archivierungsdatum, Dateispezifikation, Verfallsdatum und Archivierungsbeschreibung.

Wenn Sie die Option detail im Befehl query archive verwenden, zeigt der Client die folgenden zusätzlichen Informationen an:

- Datum der letzten Änderung
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDatum des letzten Zugriffs

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeLetztes Änderungsdatum der Dateiattribute (Dateiindex)
- Windows-BetriebssystemeErstellungsdatum
- Komprimierungstyp
- Verschlüsselungstyp
- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeClientseitige Datendeduplizierung
- Initiierung des Aufbewahrungszeitraums
- Ob die Datei gesperrt ist
- AIX-BetriebssystemeLinux-BetriebssystemeGröße der ACL-Metadaten (IBM Spectrum Scale) für AIX- und Linux-Clients
- AIX-BetriebssystemeLinux-BetriebssystemeServerspeicherinformationen (Datenträgerklasse, Datenträger-ID und Zurückschreibungsreihenfolge) für AIX- und Linux-Clients

Das folgende Beispiel zeigt Beispielausgaben, wenn der Befehl query archive mit der Option detail ausgegeben wird:

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
Größe Archiv.-Datum/-Zeit   Datei - Verfällt am - Beschreibung
---- ------------------ ------------------------------
219 B 08/15/2016 09:32:13 /Volumes/Data/info.txt 08/16/2016
Archivierungsdatum: 08/16/2016
RetInit:STARTED Obj
Held:NO
Geändert: 03/02/2016 19:43:00 Zugegriffen: 03/03/2016 09:31:23
Dateiindex geändert: 03/02/2016 19:43:00
Komprimierungstyp: LZ4  Verschlüsselungstyp: None    Vom Client dedupliziert: YES
ACL-Größe: 0  Datenträgerklasse: Fest  Datenträger-ID: 0008
Zurückschreibungsreihenfolge: 00000000-0000001F-00000000-00600774
```

Windows-Betriebssysteme

```
Größe Archiv.-Datum/-Zeit   Datei - Verfällt am - Beschreibung
---- ------------------ ------------------------------
219 B 03/03/2016 09:32:13 \\halley\m$\tsm620c.0901fa\debug\bin\
winnt_unicode\dsm.opt 03/03/2016
Archivierungsdatum: 03/03/2016
RetInit:STARTED Obj
Held:NO
Geändert: 03/03/2016 19:43:00 Erstellt: 03/01/2016 15:31:23
Komprimierungstyp: LZ4  Verschlüsselungstyp: None  Vom Client dedupliziert: YES
```

Weitere Informationen zum Komprimierungstyp finden Sie in Compression.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query ARchive--+-------------+------------------------------>
                  '- --Optionen-'

>--+- --Dateispezifikation--------------------------+----------->
   '- --{--Dateibereichsname--}--Dateispezifikation-'

>--+- --Dateispezifikation---+--------------------------------><
   '- --"Dateispezifikation"-'
```

Parameter

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDateispezifikation
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt den Pfad und den Namen der Datei an, die abgefragt werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben. Werden Platzhalterzeichen verwendet, muss die Dateispezifikation in Anführungszeichen eingeschlossen werden. Durch Eingabe eines Sterns (*) können alle archivierten Dateien im aktuellen Verzeichnis abgefragt werden.

Windows-BetriebssystemeDateispezifikation
Windows-BetriebssystemeGibt den Pfad und den Namen der Datei an, die abgefragt werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.

Wenn Dateibereichsname angegeben wird, darf die Dateispezifikation keinen Laufwerkbuchstaben enthalten. Laufwerkbezeichnungsnamen werden nur für austauschbare Datenträger verwendet.

Windows-Betriebssysteme{Dateibereichsname}

Windows-BetriebssystemeGibt den Dateibereich (zwischen geschweiften Klammern) auf dem Server an, in dem sich die abzufragende Datei befindet. Der Dateibereich ist der Name auf dem Workstationlaufwerk, auf dem die Datei archiviert wurde. Das folgende Beispiel ist für die Angabe eines UNC-Namens gültig: {'\\machine\C$'}.
Verwenden Sie Dateibereichsname, wenn der Name geändert wurde oder wenn Sie Dateien abfragen, die auf einem anderen Knoten archiviert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.
Anmerkung: Sie müssen einen NTFS-Dateibereichsnamen in Groß-/Kleinschreibung oder in Kleinschreibung angeben, der zwischen Anführungszeichen und geschweiften Klammern steht, beispielsweise {"NTFSDrive"}. Hochkommas oder Anführungszeichen sind im Schleifenmodus gültig. Beispielsweise ist sowohl {"NTFSDrive"} als auch {'NTFSDrive'} gültig. Im Stapelmodus sind nur Hochkommas gültig.

Tabelle 1. Befehl 'Query Archive': Zugehörige Optionen

Option	**Verwendung**
Windows-Betriebssystemedateformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedateformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
description	Nur in der Befehlszeile.
detail	Nur in der Befehlszeile.
dirsonly	Nur in der Befehlszeile.
filelist	Nur in der Befehlszeile.
filesonly	Nur in der Befehlszeile.
fromdate	Nur in der Befehlszeile.
fromnode	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-Betriebssystemefromowner	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-BetriebssystemeNur in der Befehlszeile.
fromtime	Nur in der Befehlszeile.
Windows-Betriebssysteme numberformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme numberformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
querysummary	Nur in der Befehlszeile.
Windows-Betriebssystemescrolllines	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemescrolllines	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme scrollprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme scrollprompt	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemesubdir	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemesubdir	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemetimeformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.

Option	Verwendung
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemetimeformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate	Nur in der Befehlszeile.
totime	Nur in der Befehlszeile.

Beispiele

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeEine Liste aller archivierten Dateien im aktuellen Arbeitsverzeichnis anzeigen.

Befehl: `q archive "*"`

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Liste aller archivierten Dateien im Verzeichnis `c:\proj` anzeigen.

Befehl: `q ar c:\proj\*`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeEine Liste aller archivierten Dateien im Verzeichnis `/devel` und in allen zugehörigen Unterverzeichnissen anzeigen.

Befehl: `query archive "/devel/*" -subdir=yes`

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Liste der archivierten Dateien auf dem Laufwerk `c:` mit der Beschreibung "January Ledgers" anzeigen.

Befehl: `query archive c:\ -su=y -descr="January Ledgers"`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeEine Liste aller archivierten Dateien im aktuellen Verzeichnis anzeigen. Die Datums- und Zeitformate mithilfe der Optionen dateformat und timeformat neu formatieren.

Befehl: `q ar -date=5 -time=1 "*"`

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Liste aller archivierten Dateien im Verzeichnis `c:\proj` anzeigen. Die Datums- und Zeitformate mithilfe der Optionen dateformat und timeformat neu formatieren.

Befehl: `q ar -date=5 -time=4 c:\proj\*`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeEine Liste aller archivierten Dateien im aktuellen Verzeichnis anzeigen. Die Option detail verwenden, um das Datum der letzten Änderung und das Datum des letzten Zugriffs jeder Datei anzuzeigen.

Befehl: `q ar -detail "*"`

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Liste aller archivierten Dateien im Verzeichnis `c:\dir1` anzeigen. Die Option detail verwenden, um das Datum der letzten Änderung und das Erstellungsdatum jeder Datei anzuzeigen.

Befehl: `q ar -detail c:\dir1\*`

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Liste der archivierten Dateien im Verzeichnis `c:\proj` mit der Dateierweiterung `.dev` anzeigen. Die Optionen dateformat und timeformat verwenden.

Befehl: `q ar -date=5 -time=4 c:\proj\*.dev`

Windows-BetriebssystemeTask
Windows-BetriebssystemeKürzlich wurde die Bezeichnung des Laufwerks `c:\` in `store` geändert und einige Dateien archiviert. Gestern wurde die Bezeichnung in `dev` geändert und einige weitere Dateien wurden archiviert. Eine Liste aller Dateien anzeigen, die im Verzeichnis `c:\proj` archiviert wurden, als die Bezeichnung `store` lautete.

Befehl: `q ar {store}\proj\*`

Windows-BetriebssystemeTask

Windows-BetriebssystemeKürzlich wurden von Ihnen Dateien von einer Diskette mit der Bezeichnung `docs` archiviert. Eine Liste aller von Ihnen archivierten Dateien anzeigen.

Befehl: `q ar {docs}\*`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Liste der archivierten Dateien im Verzeichnis `/home/proj` anzeigen, deren Dateiname mit den vier Zeichen `proj` beginnt.

Befehl: `q ar "/home/proj/proj*"`

Query Backup

Der Befehl query backup zeigt eine Liste der Sicherungsversionen Ihrer Dateien an, die auf dem IBM Spectrum Protect-Server gespeichert sind oder sich in einem Sicherungssatz auf dem Server befinden, wenn die Option backupsetname angegeben ist.

Der Befehl zeigt die folgenden Dateiinformationen an:

- Dateispezifikation
- Dateigröße
- Sicherungsdatum
- Ob die Datei aktiv oder inaktiv ist.
- Die der Datei zugeordnete Verwaltungsklasse. Es werden nur die ersten 10 Zeichen des Verwaltungsklassennamens angezeigt.

Wenn Sie die Option detail im Befehl query backup verwenden, zeigt der Client die folgenden zusätzlichen Informationen an:

- Datum der letzten Änderung
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDatum des letzten Zugriffs
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeLetztes Änderungsdatum der Dateiattribute (Dateiindex)
- Windows-BetriebssystemeErstellungsdatum
- Komprimierungstyp
- Verschlüsselungstyp
- Clientseitige Datendeduplizierung
- AIX-BetriebssystemeLinux-BetriebssystemeOb die Datei umgelagert oder vorumgelagert wird. Der Wert `Yes` bedeutet, dass die Datei umgelagert oder vorumgelagert wird. Der Wert `No` bedeutet, dass die Datei nicht umgelagert oder vorumgelagert wird.
- AIX-BetriebssystemeLinux-BetriebssystemeDateiindexnummer
- AIX-BetriebssystemeLinux-BetriebssystemeGröße der ACL-Metadaten (IBM Spectrum Scale)
- AIX-BetriebssystemeLinux-BetriebssystemeServerspeicherinformationen (Datenträgerklasse, Datenträger-ID und Zurückschreibungsreihenfolge

Das folgende Beispiel zeigt Beispielausgaben, wenn der Befehl query backup mit der Option detail ausgegeben wird:

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
      Größe       Sicher.-Datum              Verw.-Kl.            A/I Datei
      ----        -----------                ----------           --- ----
1,500,000  B  08/15/2016 16:01:25             DEFAULT               A  /home/test/mydir/myfile1.txt
    Geändert: 08/15/2016 16:00:10 Zugegriffen: 08/16/2016 15:31:23
Dateiindex geändert: 08/15/2016 16:00:10
Komprimierungstyp: LZ4  Verschlüsselungstyp: None  Vom Client dedupliziert: YES
Umgelagert: NO  Dateiindexnr.: 22691
ACL-Größe: 0  Datenträgerklasse: Fest  Datenträger-ID: 0008
Zurückschreibungsreihenfolge: 00000000-0000001F-00000000-00600774
```

Windows-Betriebssysteme

```
      Größe       Sicher.-Datum              Verw.-Kl.              A/I Datei
      ----        -----------                ----------          --- ----
1.000.000  B  03/15/2016 14:33:17             DEFAULT             A  \\eighth\n$\testdir\myfile1.txt
    Geändert: 03/15/2016 14:31:42        Erstellt: 03/15/2016 14:31:41
Komprimierungstyp: LZ4  Verschlüsselungstyp: None    Vom Client dedupliziert: YES
```

Weitere Informationen zum Komprimierungstyp finden Sie in Compression.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query Backup--+-------------+-------------------------------->
                 '- --Optionen-'

>--+- --Dateispezifikation-------------------------+----------->
   '- --{--Dateibereichsname--}--Dateispezifikation-'

>--+- --Dateispezifikation---+-------------------------------><
   '- --"Dateispezifikation"-'
```

Parameter

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDateispezifikation
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt den Pfad und den Namen der Datei an, die abgefragt werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben. Werden Platzhalterzeichen verwendet, muss die Dateispezifikation in Anführungszeichen eingeschlossen werden. Durch Eingabe eines Sterns (*) können Informationen zu den Sicherungsversionen aller Dateien im aktuellen Verzeichnis angezeigt werden. Verwenden Sie keine Platzhalterzeichen, wenn Sie NAS-Dateisystemimages mit der Optionseinstellung `-class=nas` abfragen.

Windows-BetriebssystemeDateispezifikation
Windows-BetriebssystemeGibt den Pfad und den Namen der Datei an, die abgefragt werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben. Verwenden Sie keine Platzhalterzeichen, wenn Sie NAS-Dateisystemimages mit der Optionseinstellung `-class=nas` abfragen.

Wenn Dateibereichsname angegeben wird, darf die Dateispezifikation keinen Laufwerkbuchstaben enthalten. Laufwerkbezeichnungsnamen werden nur für austauschbare Datenträger verwendet.

Sie können auch den folgenden Wert für *Dateispezifikation* verwenden:

systemstate
: Zeigt die Liste der Sicherungsversionen des Systemstatus unter Windows an.

Windows-Betriebssysteme{Dateibereichsname}
Windows-BetriebssystemeGibt den in geschweifte Klammern eingeschlossenen Dateibereich auf dem Server an, in dem sich die abzufragende Datei befindet. Dies ist die Laufwerkbezeichnung oder der UNC-Name auf dem Workstationlaufwerk, auf dem die Datei gesichert wurde. Das folgende Beispiel zeigt, wie ein UNC-Name angegeben wird: `{'\\machine\C$'}`.

Verwenden Sie *Dateibereichsname*, wenn sich der Name geändert hat oder wenn Dateien abgefragt werden sollen, die auf einem anderen Knoten gesichert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.

Sie müssen einen NTFS- oder ReFS-Dateibereichsnamen in Groß-/Kleinschreibung oder in Kleinschreibung angeben, der zwischen Anführungszeichen und geschweiften Klammern steht. Beispiel: `{"NTFSDrive"}`. Hochkommas oder Anführungszeichen sind im Schleifenmodus gültig. Beispielsweise ist sowohl `{"NTFSDrive"}` als auch `{'NTFSDrive'}` gültig. Im Stapelmodus sind nur Hochkommas gültig.

Tabelle 1. Befehl 'Query Backup': Zugehörige Optionen

Option	Verwendung
backupsetname	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssystemeclass	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWindows-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssystemedateformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedateformat	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
detail	Nur in der Befehlszeile.
dirsonly	Nur in der Befehlszeile.
filelist	Nur in der Befehlszeile.
filesonly	Nur in der Befehlszeile.
fromdate	Nur in der Befehlszeile.
fromowner	Nur in der Befehlszeile.

Option	Verwendung
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-Betriebssystemefromowner	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-BetriebssystemeNur in der Befehlszeile.
fromtime	Nur in der Befehlszeile.
inactive	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme nasnodename	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssysteme nasnodename	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme numberformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme numberformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
pitdate	Nur in der Befehlszeile.
pittime	Nur in der Befehlszeile.
querysummary	Nur in der Befehlszeile.
Windows-Betriebssystemescrolllines	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemescrolllines	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme scrollprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme scrollprompt	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemesubdir	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemesubdir	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemetimeformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemetimeformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate	Nur in der Befehlszeile.
totime	Nur in der Befehlszeile.

Beispiele

Windows-Betriebssysteme`dsmc query backup c:\* -subdir=yes -querysummary`

Windows-Betriebssysteme`dsmc query archive c:\* -subdir=yes -querysummary`

Windows-BetriebssystemeTask

Windows-BetriebssystemeDateien aus dem Verzeichnis `proj` im Dateibereich `abc` abfragen.

```
dsmc query backup {"abc"}\proj\*.*
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Liste aller aktiven und inaktiven Sicherungsversionen der Benutzerdateien im aktuellen Verzeichnis anzeigen.

```
dsmc query backup -inactive "*"
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Liste aller aktiven und inaktiven Sicherungsversionen anzeigen, die aus dem Verzeichnis `c:\proj` gesichert wurden.

```
dsmc q backup -ina c:\proj\*
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Liste aller Ihrer Sicherungen im aktuellen Verzeichnis anzeigen. Die Option detail verwenden, um das Datum der letzten Änderung und das Datum des letzten Zugriffs jeder Datei anzuzeigen.

```
dsmc q backup -detail "*"
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Liste aller Ihrer Sicherungen im Verzeichnis `c:\dir1` anzeigen. Die Option detail verwenden, um das Datum der letzten Änderung und das Erstellungsdatum jeder Datei anzuzeigen.

```
dsmc q backup -detail c:\dir1\*
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Liste aller aktiven und inaktiven Sicherungsversionen anzeigen, die aus dem Verzeichnis `c:\proj` gesichert wurden. Die Datums- und Zeitformate mithilfe der Optionen dateformat und timeformat neu formatieren.

```
dsmc q b -date=5 -time=4 -ina c:\proj\*
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Liste der Dateien anzeigen, die aus dem Verzeichnis `/home/proj` gesichert wurden und deren Dateiname mit proj beginnt.

```
dsmc q b "/home/proj/proj*"
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeEine Liste der aktiven und inaktiven Sicherungsdateiversionen im Dateisystem `/home` anzeigen.

```
dsmc q b -ina -su=yes /home/
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeLetzte Woche wurden von Ihnen Dateien von einer Diskette mit der Bezeichnung **docs** gesichert. Eine Liste dieser Dateien anzeigen.

```
dsmc q b {docs}\*
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDateisystemimages auf dem NAS-Dateiserver 'nas2' abfragen.

```
dsmc query backup -nasnodename=nas2 -class=nas
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeDateisystemimages auf dem NAS-Dateiserver 'nas2' abfragen.

```
dsmc query backup -nasnodename=nas2 -class=nas
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Liste aller Dateien Ihres Laufwerks c anzeigen, die sich im Sicherungssatz `weekly_accounting_data.32145678` befinden.

```
dsmc query backup c:\* -subdir=yes -backupsetname=weekly_accounting_data.32145678
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeInformationen zu allen aktiven und inaktiven Sicherungsversionen des Systemstatus auf dem Server anzeigen.

```
dsmc query backup -ina systemstate
```

- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
  Windows-BetriebssystemeNAS-Dateisystemimages abfragen

Mit dem Befehl query backup können Sie Informationen zu Dateisystemimages, die für einen NAS-Dateiserver gesichert wurden, anzeigen. Der Client fordert Sie zur Eingabe einer Administrator-ID auf.

Query Backupset

Der Befehl query backupset fragt einen Sicherungssatz von einer lokalen Datei, von einer Bandeinheit (falls anwendbar) oder vom IBM Spectrum Protect-Server ab.

Dieser Befehl zeigt den Namen des Sicherungssatzes, das Erstellungsdatum, den Aufbewahrungszeitraum (für einen Sicherungssatz auf dem IBM Spectrum Protect-Server) und die vom Benutzer bereitgestellte Beschreibung an.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

AIX-Betriebssysteme Oracle Solaris-BetriebssystemeBandunterstützung ist nur für AIX- und Oracle Solaris-Clients verfügbar.

Syntax

```
>>-Query BACKUPSET--+----------+--BACKUPSETName=---------------->
                    '-Optionen-'

>--+-Name des Sicherungssatzes-+--+-----------------------+---><
   +-Name der lokalen Datei----+  '-LOCation=--+-server-+-'
   '-Bandeinheit---------------'               +-file---+
                                               '-tape---'
```

Parameter

BACKUPSETName=
: Gibt den Namen des Sicherungssatzes an, der abgefragt werden soll. Den Namen des Sicherungssatzes können Sie mithilfe von Platzhalterzeichen angeben. Wenn Sie Platzhalterzeichen verwenden oder keinen Sicherungssatznamen angeben, werden alle Sicherungssätze angezeigt, deren Eigner Sie sind. Dieser Parameter ist erforderlich.

  AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeWenn ein Sicherungssatz erstellt wird, ordnet der Server Root als Eigner des Sicherungssatzes zu. Bei der Abfrage eines Sicherungssatzes auf dem Server wird der Sicherungssatz für andere Benutzer als Root nicht angezeigt, selbst wenn ihnen der Name des Sicherungssatzes bekannt ist und sie ihn in der Abfrage angeben.

  Der Wert von backupsetname ist von der Position des Sicherungssatzes abhängig und entspricht einer der folgenden drei Auswahlmöglichkeiten:

  backupsetname
  : Gibt den Namen des Sicherungssatzes auf dem Server an. Wird der Parameter location angegeben, müssen Sie `-location=server` angeben.

  Name der lokalen Datei
  : Gibt den Dateinamen des ersten Datenträgers des Sicherungssatzes an. Sie müssen `-location=file` angeben.

  Bandeinheit
  : Gibt den Namen der Bandeinheit an, die den Datenträger des Sicherungssatzes enthält. Sie müssen einen nativen Windows-Einheitentreiber und nicht den von IBM bereitgestellten Einheitentreiber verwenden. Sie müssen `-location=tape` angeben.

LOCation=
: Gibt an, wo der Client für Sichern/Archivieren nach dem Sicherungssatz sucht. Wenn Sie den Parameter location nicht angeben, sucht der Client auf dem IBM Spectrum Protect-Server nach Sicherungssätzen.

  Server
  : Gibt an, dass der Client den Sicherungssatz auf dem Server sucht. Diese Position ist der Standardwert.

  file
  : Gibt an, dass der Client den Sicherungssatz in einer lokalen Datei sucht.

  tape
  : Gibt an, dass der Client den Sicherungssatz auf einer lokalen Bandeinheit sucht.

Tabelle 1. Befehl Query Backupset: Zugehörige Optionen

Option	Verwendung
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedescription	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeNur in der Befehlszeile.

Option	Verwendung
Windows-Betriebssystemedescription	Windows-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssystemescrolllines	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme scrolllines	AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme scrollprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme scrollprompt	AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task
: Alle Sicherungssätze auf dem IBM Spectrum Protect-Server abfragen.

  Befehl: `query backupset -backupsetname=*`

Task
: Einen Sicherungssatz mit dem Namen `monthy_financial_data` auf dem IBM Spectrum Protect-Server abfragen.

  Befehl: `query backupset -backupsetname=monthly_financial_data.12345678`

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeTask
: AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-BetriebssystemeDen Sicherungssatz in der Datei `/home/budget/weekly_budget_data.ost` abfragen.

  Befehl: `dsmc query backupset -backupsetname="/home/budget/weekly_budget_data.ost" -loc=file`

Windows-BetriebssystemeTask
: Windows-BetriebssystemeDen Sicherungssatz in der Datei `c:\budget\weekly_budget_data.ost` abfragen.

  Befehl: `query backupset -backupsetname=c:\budget\weekly_budget_data.ost loc=file`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask
: AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDen Sicherungssatz auf der Bandeinheit /dev/rmt0 abfragen.

  Befehl: `dsmc query backupset -backupsetname=/dev/rmt0 -loc=tape`

Windows-BetriebssystemeTask
: Windows-BetriebssystemeDen Sicherungssatz auf der Bandeinheit \\.\tape0 abfragen.

  Befehl: `dsmc query backupset -backupsetname=\\.\tape0 -loc=tape`

- Query Backupset ohne Parameter backupsetname
  Der Befehl query backupset kann ohne den Parameter backupsetname verwendet werden.

Query Filespace

Der Befehl query filespace zeigt eine Liste der Dateibereiche für einen Knoten an. Die Dateibereiche sind auf dem IBM Spectrum Protect-Server gespeichert oder befinden sich in einem Sicherungssatz auf dem Server, wenn die Option backupsetname angegeben wird. Sie können auch einen einzelnen Dateibereich für die Abfrage angeben.

Ein *Dateibereich* ist ein logischer Speicherbereich auf dem Server, der die gesicherten oder archivierten Dateien enthält. Auf dem Server wird jedem Knoten Ihrer Workstation, von dem Sie Dateien sichern oder archivieren, ein separater Dateibereich zugeordnet.

Auf dem Server wird jedem Dateisystem Ihrer Workstation, von dem Sie Dateien sichern oder archivieren, ein separater Dateibereich zugeordnet. Der Dateibereichsname entspricht dem Namen des Dateisystems.

Windows-BetriebssystemeEin Unicode-Dateibereichsname wird unter Umständen nicht korrekt angezeigt, wenn der Server den Unicode-Namen nicht anzeigen kann. In diesem Fall müssen Sie die Dateibereichskennung (fsID) verwenden, um diese Dateibereiche auf dem Server zu identifizieren. Verwenden Sie den Befehl query filespace mit der Option detail, um die fsID eines Dateibereichs zu bestimmen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query Filespace--+----------------------+--+-------------+-->
                    '- --Dateibereichsname-'  '- --Optionen-'
```

Parameter

Dateibereichsname
: Gibt eine optionale Zeichenfolge an, die Platzhalterzeichen enthalten kann. Mit diesem Argument können Sie eine Untergruppe von Dateibereichen angeben. Standardmäßig werden alle Dateibereiche angezeigt.

Tabelle 1. Befehl Query Filespace: Zugehörige Optionen

Option	Verwendung
backupsetname	Nur in der Befehlszeile.
Windows-Betriebssysteme AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemeclass	Windows-BetriebssystemeAIX-BetriebssystemeLinux-Betriebssysteme Oracle Solaris-BetriebssystemeMac OS X-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssystemedateformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedateformat	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
detail	Nur in der Befehlszeile.
fromnode	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-Betriebssystemefromowner	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeMac OS X-BetriebssystemeNur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme nasnodename	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssysteme nasnodename	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemescrolllines	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemescrolllines	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme scrollprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme scrollprompt	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemetimeformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.

Option	Verwendung
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemetimeformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme Eigene Dateibereiche anzeigen. Die Datums- und Zeitformate mithilfe der Optionen dateformat und timeformat neu formatieren.

```
query filespace -date=5 -time=4
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDen Dateibereich /home anzeigen.

```
query filespace /home
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDateibereichsnamen anzeigen, die das Muster `smith` enthalten.

```
query filespace "*smith*"
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme Einen Dateibereich vom NAS-Dateiserver `nas2` abfragen.

```
query filespace -nasnodename=nas2 -class=nas
```

Windows-BetriebssystemeDen Dateibereich \\florence\c$ anzeigen.

```
query filespace \\florence\c$
```

Windows-BetriebssystemeAlle Dateibereichsnamen auf dem Server anzeigen, die auf `'$'` enden und zu dem System mit dem Namen `florence` gehören.

```
query filespace \\florence\*$
```

Windows-BetriebssystemeDie Dateibereiche im Sicherungssatz `monthly_accounting.23456789` anzeigen.

```
query filespace -backupsetname=monthly_accounting.23456789
```

Detaillierte Dateibereichsinformationen anzeigen, die den Replikationsstatus während einer Übernahme zeigen.

Befehl:

```
query filespace -detail
```

Ausgabe:

```
Nr.  Datum ltzt Teilsich. Typ    FSID  Unicode  Replikation  Dateibereichsname
---  --------------       ------ ----  -------  -----------  --------------
  1  00.00.0000 00:00:00  HFS       3  Yes      Current      /

       Letztes
       Speicherdatum       Server                 Lokal
       ---------------     ------                 -----
                 Sicherungsdaten:    29.04.2013 16:49:55     29.04.2013 16:49:55
               Archivierungsdaten:   Kein Datum verfügbar    Kein Datum verfügbar
```

- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeNAS-Dateibereiche abfragen
  Mit der Option nasnodename identifizieren Sie den abzufragenden NAS-Dateiserver. Bei Verwendung einer interaktiven Befehlszeilensitzung mit einer ID ohne Verwaltungsberechtigung fordert der Client Sie zur Eingabe einer Administrator-ID auf.

Query Group

Verwenden Sie den Befehl query group, um Informationen zu einer Gruppensicherung und ihren Membern anzeigen.

Anmerkung:

1. Verwenden Sie die Option showmembers, um einzelne Member anzuzeigen und auszuwählen, die abgefragt werden sollen. Die Option showmembers ist mit der Option inactive nicht gültig. Um Member in einer Gruppe anzuzeigen, die zurzeit nicht aktiv sind, die Optionen pitdate und pittime verwenden, um das Sicherungsdatum und die Sicherungszeit für das abzufragende Member anzugeben.
2. AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-BetriebssystemeVerwenden Sie den Befehl query filespace, um virtuelle Dateibereichsnamen für Ihren Knoten, die auf dem IBM Spectrum Protect-Server gespeichert sind, anzuzeigen.

3. Wenn Sie eine Gruppengesamtsicherung und eine Gruppendifferenzsicherung ausführen, werden bei einer Abfrage dieser Gruppe mit der Option inactive zwei aktive Sicherungen mit demselben Namen angezeigt, wobei eine den Typ FULL und die andere den Typ DIFF hat.

   Windows-BetriebssystemeDiese Sicherungen inaktivieren alle zuvor ausgeführten Gesamt- und Differenzsicherungen:

   Windows-Betriebssysteme

   ```
   Protect> q group {\fs}\v1 -inactive

   Größe  Sicher.-Datum          Verw.-kl.   A/I Gruppe
   ------ -------------------    ----------  --- ------
    978 B 06/02/2007 11:57:04    DEFAULT      A  FULL \fs\v1
     32 B 06/05/2007 13:52:04    DEFAULT      A  DIFF \fs\v1
   ```

   AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

   ```
   Protect> q group {/fs}/v1 -inactive

   Größe  Sicher.-Datum          Verw.-kl.   A/I Gruppe
   ------ -------------------    ----------  --- ------
    978 B 06/02/2007 11:57:04    DEFAULT      A  FULL /fs/v1
     32 B 06/05/2007 13:52:04    DEFAULT      A  DIFF /fs/v1
   ```

   Fragen Sie eine Gruppensicherung ohne die Option -inactive ab, wird nur die letzte Gruppensicherung angezeigt, die den Typ FULL oder DIFF haben kann:

   Windows-Betriebssysteme

   ```
   Protect> q group {\fs}\v1

   Größe  Sicher.-Datum          Verw.-kl.   A/I Gruppe
   ------ -------------------    ----------  --- ------
     32 B 06/05/2007 13:52:04    DEFAULT      A  DIFF \fs\v1
   ```

   AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

   ```
   Protect> q group {/fs}/v1

   Größe  Sicher.-Datum          Verw.-kl.   A/I Gruppe
   ------ -------------------    ----------  --- ------
     32 B 06/05/2007 13:52:04    DEFAULT      A  DIFF /fs/v1
   ```

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDieser Befehl ist für alle Clients außer Mac OS X gültig.

Windows-BetriebssystemeDieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query GRoup-- --Dateispezifikation--+-------------+--------><
                                       '- --Optionen-'
```

Parameter

Windows-BetriebssystemeDateispezifikation

Windows-BetriebssystemeGibt den Namen des virtuellen Dateibereichs (zwischen geschweiften Klammern) und den Namen der Gruppe auf dem Server für die Abfrage an.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDateispezifikation

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeGibt den Namen des virtuellen Dateibereichs und den Namen der Gruppe auf dem Server für die Abfrage an.

Tabelle 1. Befehl Query Group: Zugehörige Optionen

Option	Verwendung
fromnode	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme fromowner	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeNur in der Befehlszeile.
inactive	Nur in der Befehlszeile.
pitdate	Nur in der Befehlszeile.

Option	Verwendung
pittime	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme showmembers (gilt nicht für Mac OS X)	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeNur in der Befehlszeile.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAlle Gruppen im Dateibereich `/virtfs` anzeigen.

Befehl:

```
query group /virtfs/*
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Gruppen im Dateibereich `virtfs` anzeigen.

Befehl:

```
query group {virtfs}\*
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAktive und inaktive Versionen des Dateibereichs `/virtfs/group1` anzeigen.

Befehl:

```
query group /virtfs/group1 -inactive
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeAktive und inaktive Versionen des Dateibereichs `virtfs\group1` anzeigen.

Befehl:

```
query group {virtfs}\group1 -inactive
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDen Dateibereich `/virtfs/group1` anzeigen. Die Option showmembers verwenden, um eine Liste der Gruppenmember anzuzeigen, aus der Sie abzufragende Member auswählen können.

Befehl:

```
query group /virtfs/group1 -showmembers
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeDen Dateibereich `virtfs\group1` anzeigen. Die Option showmembers verwenden, um eine Liste der Gruppenmember anzuzeigen, aus der Sie abzufragende Member auswählen können.

Befehl:

```
query group {virtfs}\group1 -showmembers
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Query Image

Der Befehl query image zeigt Informationen zu Dateisystemimages an, die auf dem IBM Spectrum Protect-Server gespeichert sind oder sich in einem Sicherungssatz auf dem IBM Spectrum Protect-Server befinden, wenn die Option backupsetname angegeben wurde.

Die folgenden Informationen zu Dateisystemimages werden angezeigt:

- Imagegröße - Die Größe des Datenträgers, der gesichert wurde.
- AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeGespeicherte Größe - Die tatsächliche Größe des Images, das auf dem Server gespeichert wurde. Das auf dem IBM Spectrum Protect-Server gespeicherte Image hat dieselbe Größe wie der Datenträger. Bei Online-Imagesicherungen auf Momentaufnahmebasis kann das gespeicherte Image aufgrund der Größe der Cachedateien größer als das Dateisystem sein. Das auf dem Server gespeicherte Image hat dieselbe Größe wie der Datenträger.
- Windows-BetriebssystemeGespeicherte Größe - Die tatsächliche Größe des Images, das auf dem Server gespeichert wurde. Da bei Imagesicherungen nur die belegten Blöcke in einem Dateisystem gesichert werden können, kann die Größe des auf dem IBM Spectrum Protect-Server gespeicherten Image kleiner sein als die Datenträgergröße. Bei Online-Imagesicherungen kann das gespeicherte Image aufgrund der Größe der Cachedateien größer als das Dateisystem sein.
- Dateisystemtyp
- Sicherungsdatum und -zeit
- Die der Imagesicherung zugeordnete Verwaltungsklasse
- Ob die Imagesicherung eine aktive oder inaktive Kopie ist

- Der Imagename

Anmerkung: Die IBM Spectrum Protect-API muss installiert sein, um den Befehl query image verwenden zu können.

Unterstützte Clients

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDiese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

Windows-BetriebssystemeDieser Befehl ist für alle Windows-Clients gültig.

Syntax

```
>>-Query IMage--+-------------+---------------------------------->
                '- --Optionen-'

>--+- --Name des logischen Datenträgers-+---------------------><
   '- --Dateibereichsname---------------'
```

Parameter

Name des logischen Datenträgers
: Der Name eines logischen Datenträgers, der abgefragt werden soll. Sie müssen den exakten Namen des Images angeben. Platzhalterzeichen sind nicht zulässig. Standardwert ist alle aktiven Images (sofern nicht durch eine oder mehrere Optionen eingeschränkt).

Dateibereichsname
: Der Name des Dateisystems, das abgefragt werden soll.

  Werden der *Name des logischen Datenträgers* und *Dateibereichsname* nicht angegeben, werden alle Images angezeigt.

Tabelle 1. Befehl Query Image: Zugehörige Optionen

Option	**Verwendung**
backupsetname	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme dateformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemedateformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
fromnode	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme fromowner	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeNur in der Befehlszeile.
inactive	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme numberformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme numberformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
pitdate	Nur in der Befehlszeile.
pittime	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme scrolllines	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemescrolllines	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme scrollprompt	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Option	Verwendung
Windows-Betriebssysteme scrollprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme timeformat	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemetimeformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task
Alle gesicherten Images anzeigen.

Befehl: `q image`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAlle gesicherten Images anzeigen, deren Eigner `kutras` auf dem Knoten `avalon` ist.

Befehl: `query image -fromnode=avalon -fromowner=kutras`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeAktive und inaktive Versionen des Images `/usr` anzeigen.

Befehl: `q i /usr -inactive`

Windows-BetriebssystemeTask
Windows-BetriebssystemeAktive und inaktive Versionen des Images `h:` anzeigen.

Befehl: `q im h: -inactive`

Task
Alle Images anzeigen, die sich im Sicherungssatz `weekly_backup_data.32145678` befinden.

Befehl: `query image -backupsetname=weekly_backup_data.32145678`

Query Inclexcl

Mit dem Befehl query inclexcl wird eine Liste der Einschluss-/Ausschlussanweisungen in der Reihenfolge angezeigt, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden. Die Liste zeigt die Optionsart, den Optionsbereich (archive, all, etc.) und den Namen der Quellendatei.

Der Client für Sichern/Archivieren schließt einige Dateien von Dateisystemsicherungs- und -zurückschreibungsoperationen aus. Sie können eine Liste dieser Dateien mit dem Befehl query inclexcl anzeigen. In der Ausgabe des Befehls steht bei diesen Dateien `Betriebssystem` neben dem Pfad.

Sie können die Gültigkeit der gewünschten Muster für die Einschluss-/Ausschlussliste testen, bevor Sie sie tatsächlich in Ihre Optionsdatei einfügen. Siehe die Erläuterung bei *Testmuster*.

Verwenden Sie die Option detail, um die Verwaltungsklasse anzuzeigen, die einer Einschluss-/Ausschlussanweisung zugeordnet ist.

Windows-BetriebssystemeVerwenden Sie die Option display, um die Dateien anzuzeigen, die bei einer Dateisystemsicherungsoperation ein- bzw. ausgeschlossen sind.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme

```
>>-Query INCLexcl-- --+------------+--+----------+-------------><
                      '-Testmuster-'  '- -DETail-'
```

Windows-Betriebssysteme

```
>>-Query INCLexcl--+------------+--+----------+--+-----------------------+-><
                  '-Testmuster-'  '- -DETail-'  |           .-basic---. |
                                                '--DISPLAY=-+-vssexcl-+-'
                                                            '-all-----'
```

Parameter

Testmuster
: Dient zum Testen der Gültigkeit der Muster, die Sie in Ihrer Einschluss-/Ausschlussliste verwenden wollen. Wenn Sie ein Testmuster in diesem Befehl verwenden, geschieht Folgendes:

  - Die interne Einschluss-/Ausschlussliste wird nicht angezeigt
  - Das Muster wird so verarbeitet, als ob es aus einer Einschluss-/Ausschlussanweisung stammte, einschließlich der gesamten üblichen Fehlerprüfung
  - Das Muster wird so angezeigt, wie es in der Einschluss-/Ausschlussliste erscheinen würde

  Wenn das Testmuster fehlerfrei ist, ist das Ergebnis des kompilierten Musters mit dem Testmuster identisch.

-DETail
: Zeigt die Verwaltungsklasse an, die der Einschluss-/Ausschlussanweisung zugeordnet ist.

Windows-Betriebssysteme-DISPLAY=basic | vssexcl | all
: Windows-Betriebssysteme-DISPLAY=basic zeigt die Dateien und Verzeichnisse an, die durch eine der folgenden Methoden ein- oder ausgeschlossen wurden:

  - Die Objekte wurden in der Clientoptionsdatei ein- oder ausgeschlossen.
  - Die Objekte wurden in einer serverseitigen Clientoptionsgruppe ein- oder ausgeschlossen.
  - Die Objekte wurden durch das Betriebssystem ausgeschlossen, weil sie sich im Registrierungsschlüssel `HKEY_LOCAL_MACHINES\SYSTEM\CurrentControlSet\BackupRestore\FilesNotToBackup` befinden.
  - Die Objekte wurden durch den Client explizit ausgeschlossen.

  Dies ist der Standardwert, wenn kein Anzeigewert angegeben wird.
  Windows-Betriebssysteme-DISPLAY=vssexcl zeigt eine Liste mit Dateien an, die von einer Dateisystemsicherung ausgeschlossen sind, da sie eingeschlossen sind, wenn eine Systemstatussicherung ausgeführt wird. Mit einer Systemstatussicherungsoperation (backup systemstate) gesicherte Dateien werden durch den VSS Writer geschützt. Sie können diese Dateien nicht in eine Dateisystemsicherung einschließen, indem Sie sie einer Anweisung include in der Datei dsm.opt oder in der Clientoptionsgruppe hinzufügen.
  Windows-Betriebssysteme-DISPLAY=all zeigt alle Dateien an, die während einer Dateisystemsicherung ein- oder ausgeschlossen sind.

Beispiele

Task
: Eine Datei durch Ausschluss in der Clientoptionsdatei von der Deduplizierung ausschließen:

```
Exclude Dedup *\...\file2
```

Task
: Eine allgemeine Liste der Einschluss-/Ausschlussanweisungen anzeigen. Befehl:

```
query inclexcl
```

Windows-BetriebssystemeTask
: Windows-BetriebssystemeEine Liste der Dateien anzeigen, die von Dateisystemsicherungen ausgeschlossen sind, da sie der VSS Writer in Systemstatussicherungen einschließt.

```
query inclexcl -display=vssexcl
```

Task
: Eine Liste der Einschluss-/Ausschlussanweisungen anzeigen. Die Verwaltungsklasse anzeigen, die jeder Anweisung zugeordnet ist.

```
query inclexcl -detail
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask
: AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDie Gültigkeit des folgenden Musters testen: `/.../?x?/*.log`

```
query inclexcl /.../?x?/*.log
```

Windows-BetriebssystemeTask
: Windows-BetriebssystemeDie Gültigkeit des folgenden Musters testen: `..\?x?\*.log`

```
query inclexcl ..\?x?\*.log
```

Query Mgmtclass

Mit dem Befehl query mgmtclass können Informationen zu den Verwaltungsklassen angezeigt werden, die in der aktiven Maßnahmengruppe verfügbar sind.

Ihr Administrator definiert Verwaltungsklassen. Diese enthalten Attribute, die steuern, ob eine Datei für Sicherungs- oder Archivierungsservices ausgewählt werden kann. Verwaltungsklassen bestimmen außerdem, wie Sicherungen und Archivierungen auf dem Server verwaltet werden.

 Windows-BetriebssystemeDie aktive Maßnahmengruppe enthält eine Standardverwaltungsklasse; sie kann eine beliebige Anzahl zusätzlicher Verwaltungsklassen enthalten. Sie können Dateien bestimmte Verwaltungsklassen zuordnen, indem Sie include-Optionen in der Clientoptionsdatei (dsm.opt) verwenden. Wenn Sie einer Datei keine Verwaltungsklasse zuordnen, wird die Standardverwaltungsklasse verwendet.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDie aktive Maßnahmengruppe enthält eine Standardverwaltungsklasse; sie kann eine beliebige Anzahl zusätzlicher Verwaltungsklassen enthalten. Sie können Dateien bestimmte Verwaltungsklassen zuordnen, indem Sie include-Optionen in der Clientbenutzeroptionsdatei (dsm.opt) verwenden. Wenn Sie einer Datei keine Verwaltungsklasse zuordnen, wird die Standardverwaltungsklasse verwendet.

Wenn Dateien archiviert werden, kann die zugeordnete Verwaltungsklasse mithilfe der Option archmc überschrieben werden.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query Mgmtclass--+-------------+----------------------------><
                    '- --Optionen-'
```

Parameter

Tabelle 1. Befehl Query Mgmtclass: Zugehörige Optionen

Option	Verwendung
detail	Nur in der Befehlszeile.
fromnode	Nur in der Befehlszeile.

Beispiele

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme
Task

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
 Windows-BetriebssystemeStandard- und verfügbare Verwaltungsklassen anzeigen.

Befehl: `query mgmtclass`

Query Node

Der Befehl query node zeigt alle Knoten an, für die eine Verwaltungsbenutzer-ID die Berechtigung zum Ausführen von Operationen hat. Sie werden zur Eingabe der IBM Spectrum Protect-Administrator-ID aufgefordert.

Die Verwaltungsbenutzer-ID sollte mindestens über die Clienteignerberechtigung für den Client-Workstation-Knoten verfügen, der entweder von der Befehlszeile oder vom Web aus verwendet wird.

Sie können mit der Option type die Knotenart angeben, mit der gefiltert werden soll. Die folgenden Werte sind gültig:

-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
  Windows-Betriebssystemenas
- Client
- Server
- any

Der Standardwert ist any.
Anmerkung: Wenn die IBM Spectrum Protect for Virtual Environments: Data Protection for VMware-Lizenzdatei auf einem vStorage-Sicherungsserver installiert ist, wird die auf dem IBM Spectrum Protect-Server gespeicherte Plattformzeichenfolge für jeden Knotennamen, der auf dieser Maschine verwendet wird, auf "TDP VMware" gesetzt. Die Plattformzeichenfolge kann im Kontext von PVU-Berechnungen verwendet

werden. Wird ein Knotenname für die Sicherung der Maschine mit Standardfunktionen des Clients für Sichern/Archivieren verwendet (beispielsweise Sicherung auf Dateiebene oder Imagesicherung), wird diese Plattformzeichenfolge für die Zwecke der PVU-Berechnungen als "client" interpretiert.

Weitere Informationen zu Prozessor-Value-Units finden Sie im Abschnitt *Prozessor-Value-Units schätzen* in der IBM Spectrum Protect-Serverdokumentation.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query Node--+-------------+---------------------------------><
               '- --Optionen-'
```

Parameter

Tabelle 1. Befehl Query Node: Zugehörige Optionen

Option	Verwendung
type	Nur in der Befehlszeile.
Windows-Betriebssystemescrolllines	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemescrolllines	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme scrollprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme scrollprompt	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme
Task

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme
Windows-BetriebssystemeAlle NAS-Knoten anzeigen.

Befehl: `query node -type=nas`

Mac OS X-BetriebssystemeTask

Mac OS X-BetriebssystemeAlle Clientknoten anzeigen, die Clients für Sichern/Archivieren sind.

Befehl: `query node -type=client`

Query Options

Verwenden Sie den Befehl query options, um alle Optionen oder einen Teil Ihrer Optionen und ihre aktuelle Einstellung in Bezug auf den Befehlszeilenclient anzuzeigen.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query Options--+-------------+---- --Muster-----------------><
                 '- --Optionen-'
```

Parameter

Muster
: Eine optionale Zeichenfolge, die Platzhalterzeichen enthalten kann. Mit diesem Argument können Sie eine Untergruppe von Optionen angeben. Standardmäßig werden alle Optionen angezeigt.

Tabelle 1. Befehl Query Options: Zugehörige Optionen

Option	Verwendung
Windows-Betriebssystemescrolllines	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemescrolllines	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme scrollprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme scrollprompt	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task
: Alle Optionen und ihre Werte anzeigen.

```
query options
```

Task
: Nur Optionen anzeigen, die mit der Zeichenfolge *comm* beginnen.

```
query options comm*
```

Task
: Den Wert der Option replace anzeigen.

```
query options replace
```

Task
: Geben Sie den Befehl aus, mit dem alle Optionen und ihre Werte angezeigt werden. Die Übernahmestatusinformationen werden angezeigt.

```
query options
```

Ausgabe:

```
     MYPRIMARYSERVERNAME: SERVER1
     MYREPLICATIONSERVER: TARGET
          REPLSERVERNAME: TARGET
                 Address: 192.0.2.9
                    Port: 1501
                 SSLPort: 1502
                    GUID: 39.5a.da.d1.ae.92.11.e2.82.d3.00.0c.29.2f.07.d3
                    Used: yes
```

Query Restore

Mit dem Befehl query restore kann eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt werden. Die Liste enthält folgende Felder: Eigner, Ersetzen (Ersetz.), Unterverzeichnis (Untver), Pfad beibehalten (Pfad beibeh.), Quelle und Ziel.

Eine wiederanlauffähige Zurückschreibungssitzung wird erstellt, wenn ein Befehl zum Zurückschreiben mit Platzhalterzeichen wegen eines Netzausfalls, Clientfehlers, Serverausfalls oder wegen eines ähnlichen Fehlers fehlschlägt. Wenn ein solcher Fehler auftritt, wird der Dateibereich auf dem Server gesperrt, sodass seine Dateien nicht von den sequenziellen Datenträgern des Servers weg verschoben werden können. Zum Entsperren des Dateibereichs müssen Sie entweder die Zurückschreibung erneut starten und bis zum Ende ausführen (Befehl query restore) oder

die Zurückschreibung abbrechen (Befehl cancel restore). Verwenden Sie query restore, um festzustellen, ob wiederanlauffähige Zurückschreibungssitzungen vorhanden sind und welche Dateien betroffen sind.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query Restore-----------------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

 Windows-BetriebssystemeTask

 Windows-BetriebssystemeDas folgende Beispiel zeigt die Ausgabe des Befehls query restore:

```
--- Informationen zu wiederanlauffähigen Zurückschreibungen ---
Wiederanlauffähige Sitzung: 1
    Startdatum/-zeit: 10/17/2001 15:18:22
             Quelle: {"\\ers\c$"}\data\proposals\*
        Ziel: - nicht vom Benutzer angegeben -

Wiederanlauffähige Sitzung: 2
    Startdatum/-zeit: 10/17/2001 15:20:01
             Quelle: {"\\ers\c$"}\data\spreadsheets\*
        Ziel: - nicht vom Benutzer angegeben -
```

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
Task

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme
Mac OS X-BetriebssystemeDie wiederanlauffähigen Zurückschreibungssitzungen in der Serverdatenbank anzeigen.

Befehl: `query restore`

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Query Schedule

Der Befehl query schedule zeigt die Ereignisse an, die für den Knoten geplant sind. Der Administrator kann Zeitpläne für automatische Sicherungen und Archivierungen erstellen. Zur besseren Arbeitsplanung kann mit diesem Befehl festgestellt werden, wann die nächsten geplanten Ereignisse stattfinden.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query SChedule----------------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task

Geplante Ereignisse anzeigen.

Befehl: `query schedule`

Query Session

Mit dem Befehl query session können Informationen zur Sitzung angezeigt werden, z. B. der aktuelle Knotenname, die Angabe, wann die Sitzung aufgebaut wurde, Serverinformationen und Serververbindungsinformationen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-Query SEssion-------------------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme
Task

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Windows-BetriebssystemeDie Sitzungsinformationen anzeigen.

Befehl: `query session`

Eine Beispielanzeige des Befehls query session:

```
Servername...................: HALLEY_SERVER1
Servertyp....................: Windows
Schutz der Archivaufbewahrung: "Nein"
Serverversion................: Ver. 6, Rel. 2, Stu. 0.0
Datum des letzten Zugriffs...: 03.09.2009 09:08:13
Sicherungsdateien löschen....: "Nein"
Archivierungsdateien löschen.: "Ja"
Deduplizierung...............: "Nur Server"

Knotenname...................: HALLEY
Benutzername.............:
```

Mögliche Werte für die clientseitige Deduplizierung:

- Keine
  - Wird bei Verbindung zu einem IBM Spectrum Protect-Server mit einer niedrigeren Version als 6.1 angezeigt
- Nur Server
- Client oder Server

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme

Eine Beispielanzeige des Befehls query session (LAN-unabhängig):

```
IBM Spectrum Protect-Serververbindungsinformationen

Servername...................: TEMPLAR
Servertyp....................: AIX
Schutz der Archivaufbewahrung: "Nein"
Serverversion................: Ver. 6, Rel. 1, Stu. 4.0
Datum des letzten Zugriffs...: 12.08.10   22:10:15
Sicherungsdateien löschen....: "Nein"
Archivierungsdateien löschen.: "Ja"

Knotenname...................: LAN2
Benutzername.................: root

Speicheragentenname..........: TEMPLAR_STA
Speicheragententyp...........: AIX
Speicheragentversion.........: Ver. 6, Rel. 1, Stu. 3.3
```

Query Systeminfo

Verwenden Sie den Befehl query systeminfo, um Informationen zusammenzustellen und in eine Datei oder an der Konsole auszugeben.

Dieser Befehl ist in erster Linie als Hilfe für die IBM® Unterstützungsfunktion bei der Diagnose von Problemen gedacht. Aber Benutzer, die mit den in diesen Informationen angesprochenen Konzepten vertraut sind, finden ihn möglicherweise auch nützlich.

Wenn Sie die Option console verwenden, wird keine besondere Formatierung der Ausgabe ausgeführt, um die Anzeigenhöhe oder -breite anzupassen. Aus diesem Grund ist die Konsolausgabe wegen ihrer Länge und dem Zeilenumbruch unter Umständen schwierig zu lesen. Wenn die Konsolausgabe schwierig zu lesen ist, können Sie die Option filename mit dem Befehl query systeminfo verwenden. Diese Kombination ermöglicht die Ausgabe in eine Datei, die dann an die IBM Unterstützungsfunktion übergeben werden kann.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
                    .-----------------.
                    V                 |
>>-Query SYSTEMInfo------ --Element---+--+-------------+------->< 
                                       '- --Optionen-'
```

Parameter

Element
: Gibt ein oder mehrere Elemente an, zu denen Informationen zusammengestellt und in der Datei, die Sie über die Option filename angegeben haben, gespeichert oder an der Konsole ausgegeben werden sollen. Standardmäßig werden Informationen zu allen Elementen zusammengestellt.

Sie können Informationen zu einem oder mehreren der folgenden Elemente zusammenstellen:

- DSMOPTFILE - Inhalt der Datei dsm.opt
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDSMSYSFILE - Inhalt der Datei dsm.sys
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeENV - Umgebungsvariablen
- ERRORLOG - Fehlerprotokoll des Clients
- FILE - Attribute für den angegebenen Dateinamen.
- Windows-BetriebssystemeFILESNOTTOBACKUP - Aufzählung des Windows-Registerschlüssels:

  ```
  HKEY_LOCAL_MACHINE\
     SYSTEM\
        CurrentControlSet\
           BackupRestore\
              FilesNotToBackup
  ```

  Dieser Schlüssel gibt diejenigen Dateien an, die nicht gesichert werden sollen. Der Befehl query inclexcl zeigt an, dass diese Dateien vom Betriebssystem ausgeschlossen sind.

- INCLEXCL - Stellt eine Liste der Einschluss/Ausschlussanweisungen in der Reihenfolge zusammen, in der sie bei Sicherungs- und Archivierungsoperationen verarbeitet werden.
- Windows-BetriebssystemeKEYSNOTTORESTORE - Aufzählung des Windows-Registerschlüssels:

  ```
  HKEY_LOCAL_MACHINE\
     SYSTEM\
        ControlSet001\
           BackupRestore\
              KeysNotToRestore
  ```

  Dieser Schlüssel gibt diejenigen Windows-Registerschlüssel, an die nicht zurückgeschrieben werden sollen.

- Windows-BetriebssystemeMSINFO - Windows-Systeminformationen (Ausgabe von MSINFO32.EXE).
- OPTIONS - Optionen
- Windows-BetriebssystemeOSINFO - Name und Version des Clientbetriebssystems
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeOSINFO - Name und Version des Clientbetriebssystems (umfasst ULIMIT-Informationen für UNIX)
- POLICY - Speicherauszug der Maßnahmengruppe
- Windows-BetriebssystemeREGISTRY - IBM Spectrum Protect-bezogene Windows-Registry-Einträge.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeSCHEDLOG - Inhalt des Planungsprotokolls (normalerweise dsmsched.log).

- Windows-BetriebssystemeSFP - Liste der Dateien, die durch Windows-Systemdateischutz geschützt sind, und für jede Datei die Anzeige, ob diese Datei vorhanden ist. Diese Dateien werden als Teil des Systemobjekts SYSFILES gesichert.
- Windows-BetriebssystemeSFP=<*Dateiname*> - Zeigt an, ob die angegebene Datei (*Dateiname*) durch den Windows-Systemdateischutz geschützt ist. Zum Beispiel:

  ```
  SFP=C:\WINNT\SYSTEM32\MSVCRT.DLL
  ```

- Windows-BetriebssystemeSYSTEMSTATE - Informationen zum Windows-Systemstatus
- AIX-BetriebssystemeCLUSTER - AIX-Clusterinformationen
- Windows-BetriebssystemeCLUSTER - Windows-Clusterinformationen
- ENCRYPT - Verfügbare Verschlüsselungsverfahren

Anmerkung:

1. AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeVerwenden Sie die Option filename, um den Namen einer Datei anzugeben, in der die Informationen zu den angegebenen Elementen gespeichert werden sollen. Wenn Sie keinen Dateinamen angeben, werden die Informationen standardmäßig in der Datei /Library/Application Support/tivoli/tsm/client/ba/bin/dsminfo.txt (für Mac OS X) oder dsminfo.txt (für andere UNIX- und Linux-Systeme) gespeichert.
2. Windows-BetriebssystemeVerwenden Sie die Option filename, um den Namen einer Datei anzugeben, in der die Informationen zu den angegebenen Elementen gespeichert werden sollen. Wird kein Dateiname angegeben, werden die Informationen standardmäßig in der Datei dsminfo.txt gespeichert.
3. Verwenden Sie die Option console, wenn die Informationen an der Konsole ausgegeben werden sollen.

Tabelle 1. Befehl Query Systeminfo: Zugehörige Optionen

Option	Verwendung
console	Nur in der Befehlszeile.
filename	Nur in der Befehlszeile.

Beispiele

Task

Den Inhalt der Datei dsm.opt und der IBM Spectrum Protect-Fehlerprotokolldatei zusammenstellen und in der Datei `tsminfo.txt` speichern.

Befehl: `query systeminfo dsmoptfile errorlog -filename=tsminfo.txt`

Windows-Betriebssysteme

Query Systemstate

Verwenden Sie den Befehl query systemstate, um Informationen zu einer Sicherung des Systemstatus anzuzeigen, die auf dem IBM Spectrum Protect-Server gespeichert ist oder sich in einem Sicherungssatz auf dem IBM Spectrum Protect-Server befindet, wenn die Option backupsetname angegeben wurde.

In der Ausgabe ist angegeben, ob das Objekt aktiv ("A") oder inaktiv ("I") ist. Inaktive Objekte werden nur aufgelistet, wenn die Option inactive mit dem Befehl angegeben wird. Der Client für Sichern/Archivieren unter Windows unterstützt das Standard- und das detaillierte Format.

Unterstützte Clients

Dieser Befehl ist nur für unterstützte Windows-Clients gültig.

Syntax

```
>>-Query SYSTEMSTate--+-----------+---------------------------><
                      '- Optionen-'
```

Parameter

Tabelle 1. Befehl Query Systemstate: Zugehörige Optionen

Option	Verwendung
backupsetname	Nur in der Befehlszeile.

Option	Verwendung
dateformat	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
inactive	Nur in der Befehlszeile.
numberformat	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
pitdate	Nur in der Befehlszeile.
pittime	Nur in der Befehlszeile.
showmembers	Nur in der Befehlszeile.
timeformat	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
detail	Nur in der Befehlszeile.

Beispiele

Task
Informationen über die aktive Sicherung des Systemstatus auf dem IBM Spectrum Protect-Server anzeigen.

Befehl: `query systemstate`

Task
Informationen über die aktive Sicherung des Systemstatus auf dem IBM Spectrum Protect-Server anzeigen.

Befehl: `query systemstate -detail`

Task
Informationen zur aktiven Sicherung des Systemstatus abfragen, die sich im Sicherungssatz `daily_backup_data.12345678` befindet.

Befehl: `query systemstate -backupsetname=daily_backup_data.12345678`

Task
Zum Anzeigen von Informationen zu Active Directory geben Sie den folgenden Befehl ein: `query systemstate -detail`.

Suchen Sie in der Ausgabe nach Informationen zu Active Directory.

Linux-Betriebssysteme Windows-Betriebssysteme

Query VM

Verwenden Sie den Befehl query VM, um die erfolgreichen Sicherungen von virtuellen Maschinen (VMs) aufzulisten und zu verifizieren.

Windows-Betriebssysteme
Mit dem Befehl query VM können Sie feststellen, welche virtuellen Microsoft Hyper-V-Maschinen und virtuellen VMware-Maschinen auf dem Server gesichert wurden. Die Informationen für jeden Hypervisor werden in einem eigenen Abschnitt bereitgestellt. Wenn Sie Sicherungen von virtuellen Hyper-V-Maschinen abfragen, können Sie den Text *Query VM für virtuelle VMware-Maschinen* überspringen. Wenn Sie Sicherungen von virtuellen VMware-Maschinen abfragen, müssen Sie den Text *Query VM für virtuelle Hyper-V-Maschinen* nicht lesen.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Linux-Betriebssysteme Windows-Betriebssysteme

Query VM für virtuelle VMware-Maschinen

Verwenden Sie den Befehl query vm, um festzustellen, welche virtuellen VMware-Maschinen gesichert wurden.

Unterstützte Clients

Linux-BetriebssystemeDieser Befehl ist auf Linux-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Windows-BetriebssystemeDieser Befehl ist auf Windows-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind.

Syntax

```
>>-Query VM-- --VM-Name--+--------------------+--+----------+---><
```

```
|        .-BOTH---. |  '-Optionen-'
'--FROM -+-SERVER-+-'
         '-LOCAL--'
```

Parameter

VM-Name
: Gibt den Hostnamen der virtuellen Maschine an, die abgefragt werden soll. Wenn Sie den Namen der virtuellen Maschine nicht angeben, zeigt der Befehl alle VM-Sicherungen auf dem IBM Spectrum Protect-Server an.

-FROM
: Gibt die Sicherungsposition oder -positionen an, die abgefragt werden sollen. Sie können einen der folgenden Werte angeben:

  SERVER
  : Die Abfrage ist auf Sicherungen beschränkt, die sich auf dem IBM Spectrum Protect-Server befinden.

  LOCAL
  : Die Abfrage ist auf gespeicherte Momentaufnahmen beschränkt, die sich im Hardwarespeicher befinden.

  BOTH
  : Mit der Abfrage werden sowohl Informationen für Sicherungen, die sich auf dem IBM Spectrum Protect-Server befinden, als auch Informationen für Sicherungen, die sich im Hardwarespeicher befinden, aufgelistet. Dies ist der Standardwert.

Tabelle 1. Befehl Query VM: Zugehörige Optionen für Abfragen virtueller VMware-Maschinen

Option	Verwendung
detail Gültig für vmbackuptype=fullvm Windows-BetriebssystemeGültig für -vmrestoretype	Befehlszeile
inactive Gültig für vmbackuptype=fullvm	Befehlszeile
pitdate Gültig für vmbackuptype=fullvm	Befehlszeile
pittime Gültig für vmbackuptype=fullvm	Befehlszeile
vmbackuptype	Befehlszeile oder Clientoptionsdatei
vmchost	Befehlszeile oder Clientoptionsdatei
vmcpw	Befehlszeile oder Clientoptionsdatei
vmcuser	Befehlszeile oder Clientoptionsdatei

Linux-BetriebssystemeWindows-Betriebssysteme

Beispiele für Query VM (VMware)

Die folgenden Beispiele zeigen die Verwendung des Befehls query VM mit und ohne Angabe der Option -detail.

Linux-BetriebssystemeWindows-BetriebssystemeVM-Gesamtsicherung
Linux-BetriebssystemeWindows-Betriebssysteme

```
q vm devesx04-24 -ina
VM-Gesamtsicherung auf virtueller Maschine abfragen

 Nr. Sicherungsdatum     Verw.-Klasse Größe     Typ      A/I Position  Virtuelle Maschine
---  -------------------  ----------  --------  ------   --- --------  ---------------
  1  07.12.2016 14:45:24  DDMGMT      47,85 GB  IFFULL    I  SERVER    devesx04-24
  2  14.12.2016 17:38:05  DDMGMT      47,85 GB  IFINCR    A  SERVER    devesx04-24
  3  23.01.2017 14:07:44  DDMGMT      47,85 GB  SNAPSHOT  I  LOCAL     devesx04-24
  4  01.02.2017 08:59:52  DDMGMT      47,85 GB  SNAPSHOT  A  LOCAL     devesx04-24
ANS1900I Rückkehrcode ist 0.
```

Linux-BetriebssystemeWindows-BetriebssystemeVM-Gesamtsicherung mit der Option -detail
Linux-BetriebssystemeWindows-Betriebssysteme

```
q vm devesx04-24 -ina -detail
VM-Gesamtsicherung auf virtueller Maschine abfragen

 Nr. Sicherungsdatum     Verw.-Klasse Größe     Typ      A/I Position  Virtuelle Maschine
---  -------------------  ----------  --------  ------   --- --------  ---------------
```

```
  1  07.12.2016 14:45:24  DDMGMT      47,85 GB  IFFULL    I  SERVER    devesx04-24
        Größe dieser Teilsicherung: nicht zutreffend
        Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0
        Zusätzliches Datenvolumen: 0
        IBM Spectrum Protect-Objektfragmentierung: 0
        Sicherung ist dargestellt durch: 79 TSM-Objekte
        Art des Anwendungsschutzes: VMware
        Momentaufnahmetyp: VMware Tools
        Platte[1]Kennsatz: Festplatte 1
        Platte[1]Name:     [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204
af/devesx04-24-000003.vmdk
        Platte[1]Status:   Geschützt
        Platte[2]Kennsatz: Festplatte 2
        Platte[2]Name:     [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204
af/devesx04-24_1-000003.vmdk
        Platte[2]Status:   Geschützt
        Platte[3]Kennsatz: Festplatte 3
        Platte[3]Name:     [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204
af/devesx04-24_2-000003.vmdk
        Platte[3]Status:   Geschützt
  2  14.12.2016 17:38:05  DDMGMT        47,85 GB  IFINCR    A  SERVER    devesx04-24
        Größe dieser Teilsicherung: 186,43 MB
        Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1
        Zusätzliches Datenvolumen: 0
        IBM Spectrum Protect-Objektfragmentierung: 2
        Sicherung ist dargestellt durch: 119 TSM-Objekte
        Art des Anwendungsschutzes: VMware
        Momentaufnahmetyp: VMware Tools
        Platte[1]Kennsatz: Festplatte 1
        Platte[1]Name:     [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204
af/devesx04-24-000006.vmdk
        Platte[1]Status:   Geschützt
        Platte[2]Kennsatz: Festplatte 2
        Platte[2]Name:     [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204
af/devesx04-24_1-000006.vmdk
        Platte[2]Status:   Geschützt
        Platte[3]Kennsatz: Festplatte 3
        Platte[3]Name:     [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204
af/devesx04-24_2-000006.vmdk
        Platte[3]Status:   Geschützt
  3  23.01.2017 14:07:44  DDMGMT        47,85 GB  SNAPSHOT  I  LOCAL     devesx04-24
        Größe dieser Teilsicherung: nicht zutreffend
        Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0
        Zusätzliches Datenvolumen: 0
        IBM Spectrum Protect-Objektfragmentierung: 0
        Sicherung ist dargestellt durch: 0 TSM-Objekte
        Art des Anwendungsschutzes: VMware
        Momentaufnahmetyp: VMware Tools
  4  01.02.2017 08:59:52  DDMGMT        47,85 GB  SNAPSHOT  A  LOCAL     devesx04-24
        Größe dieser Teilsicherung: nicht zutreffend
        Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0
        Zusätzliches Datenvolumen: 0
        IBM Spectrum Protect-Objektfragmentierung: 0
        Sicherung ist dargestellt durch: 0 TSM-Objekte
        Art des Anwendungsschutzes: VMware
        Momentaufnahmetyp: VMware Tools
------------------------------------------------------------------------------
        Alle Durchschnittswerte werden nur für oben angezeigte immer inkrementelle
        Sicherungen berechnet.
        Durchschnittsgröße der Teilsicherung: 186,43 MB
        Durchschnittliche Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1
        Durchschnittsaufwand für zusätzliche Daten: 0
        Durchschnittliche Objektfragmentierung: 0
        Durchschnittliche Anzahl Objekte pro Sicherung: 49
ANS1900I Rückkehrcode ist 0.
```

 Der folgende Befehl gibt eine Liste der virtuellen Maschinen zurück, die eine Sofortzurückschreibungsoperation ausführen.

```
q vm * -vmrestoretype=instantrestore
```

 Alle virtuellen VMware-Maschinen abfragen, die mit `-vmbacktype=fullvm` gesichert wurden:

```
q vm * -vmbackuptype=fullvm
```

Query VM für virtuelle Microsoft Hyper-V-Maschinen

Verwenden Sie den Befehl query vm, um festzustellen, welche virtuellen Hyper-V-Maschinen gesichert wurden.

Unterstützte Clients

Dieser Befehl ist auf Windows-Clients gültig, die auf einem Hyper-V-Hostsystem installiert sind.

Syntax

```
>>-Query VM-- --VM-Name--+----------+-------------------------><
                         '-Optionen-'
```

Parameter

VM-Name
: Gibt den Hostnamen der virtuellen Maschine an, die abgefragt werden soll. Beim Namen der virtuellen Maschine muss die Groß-/Kleinschreibung beachtet werden. Wenn Sie einen VM-Namen in dem Befehl angeben, darf der Name keine Platzhalterzeichen enthalten.
  Wenn Sie den Namen der virtuellen Maschine nicht angeben, zeigt der Befehl alle VM-Sicherungen auf dem IBM Spectrum Protect-Server an.

Windows-Betriebssysteme

Tabelle 2. Befehl Query VM: Zugehörige Optionen für Abfragen virtueller Hyper-V-Maschinen

Option	Verwendung
detail	Befehlszeile. Zeigt die Details zu jeder Platte (Kennsatz, Name) und ihren Status (geschützt oder ausgeschlossen) sowie Leistungsstatistik für immer inkrementelle Sicherungen an.
inactive	Befehlszeile
pitdate	Befehlszeile
pittime	Befehlszeile

Windows-Betriebssysteme

Beispiele

Task
: Alle virtuellen Maschinen auflisten, die von Data Protection for Microsoft Hyper-V auf dem Hyper-V-Host gesichert wurden.

```
dsmc query vm
```

Windows-Betriebssysteme

Beispiele für Query VM (Hyper-V)

Das folgende Beispiel zeigt einen Befehl query VM, mit dem Übersichtsdaten zu allen virtuellen Hyper-V-Maschinen angezeigt, die gesichert wurden.

```
dsmc query vm

VM-Gesamtsicherung auf virtueller Maschine abfragen

 Nr. Sicherungsdatum     Verw.-Klasse Größe     Typ      A/I Position  Virtuelle Maschine
---  ------------------  ----------  --------  ------   --- --------  ---------------
  1  19.03.2017 17:54:34  STANDARD    17,00 GB  IFFULL    A  SERVER    DeptA_VM05
  2  20.03.2017 01:51:34  STANDARD    15,00 GB  IFINCR    A  SERVER    DeptA_VM_W2k08R2
  3  20.03.2017 01:46:19  STANDARD    36,00 GB  IFFULL    A  SERVER    DeptA_VM04
```

Mit dem folgenden Befehl query VM mit der Option -detail werden detaillierte Informationen zu virtuellen Hyper-V-Maschinen angezeigt, die gesichert wurden. Die detaillierte Ausgabe umfasst den Typ der ausgeführten Sicherung, die Größe der virtuellen Maschine, Informationen zu ihren Platten und statistische Daten.

```
dsmc query vm -detail

VM-Gesamtsicherung auf virtueller Maschine abfragen

 Nr. Sicherungsdatum     Verw.-Klasse Größe        Typ      A/I Position  Virtuelle Maschine
---  ------------------  ----------  -----------  ------   --- --------  ---------------
  1  19.03.2017 17:54:34  STANDARD       17,00 GB  IFFULL    A  SERVER    DeptA_VM05
        Größe dieser Teilsicherung: nicht zutreffend
        Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0
        Zusätzliches Datenvolumen: 0
        IBM Spectrum Protect-Objektfragmentierung: 0
```

```
        Sicherung ist dargestellt durch: 99 IBM Spectrum Protect-Objekte
        Art des Anwendungsschutzes: nicht zutreffend
        Die Sicherung ist komprimiert: Nein
        Die Sicherung ist dedupliziert: Nein
        Momentaufnahmetyp: Hyper-V RCT - anwendungskonsistent
        Platte[1]Name: DeptA_VM05.vhdx
        Platte[1]Position: IDE 0 0
        Platte[1]Status: Geschützt
        Platte[2]Name: DeptA_VM05_Disk2.vhdx
        Platte[2]Position: SCSI 0 1
        Platte[2]Status: Geschützt
        Platte[3]Name:  Platte 7 2,00 GB Bus 0 LUN 4 Ziel 0
        Platte[3]Position: SCSI 0 0
        Platte[3]Status: übersprungen: Physische Platte
        Platte[4]Name:  Platte 8 2,50 GB Bus 0 LUN 5 Ziel 0
        Platte[4]Position: SCSI 0 2
        Platte[4]Status: Übersprungen: Physische Platte
  2  20.03.2017 01:51:34  STANDARD       15,00 GB  IFINCR    A  SERVER    DeptA_VM_W2k08R2
        Größe dieser Teilsicherung: 544,00 KB
        Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1
        Zusätzliches Datenvolumen: 0
        IBM Spectrum Protect-Objektfragmentierung: 2
        Sicherung ist dargestellt durch: 37 IBM Spectrum Protect-Objekte
        Art des Anwendungsschutzes: nicht zutreffend
        Die Sicherung ist komprimiert: Nein
        Die Sicherung ist dedupliziert: Nein
        Momentaufnahmetyp: Hyper-V RCT - absturzkonsistent
        Platte[1]Name: DeptA_VM_W2k08R2.vhdx
        Platte[1]Position: IDE 0 0
        Platte[1]Status: Geschützt
  3  20.03.2017 01:46:19  STANDARD       36,00 GB  IFFULL    A  SERVER    DeptA_VM04
        Größe dieser Teilsicherung: nicht zutreffend
        Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0
        Zusätzliches Datenvolumen: 0
        IBM Spectrum Protect-Objektfragmentierung: 0
        Sicherung ist dargestellt durch: 79 IBM Spectrum Protect-Objekte
        Art des Anwendungsschutzes: nicht zutreffend
        Die Sicherung ist komprimiert: Nein
        Die Sicherung ist dedupliziert: Nein
        Momentaufnahmetyp: Hyper-V RCT - anwendungskonsistent
        Platte[1]Name: DeptA_VM04.vhdx
        Platte[1]Position: IDE 0 0
        Platte[1]Status: Geschützt
--------------------------------------------------------------------------------
        Alle Durchschnittswerte werden nur für oben angezeigte immer inkrementelle
        Sicherungen berechnet.
        Durchschnittsgröße der Teilsicherung: 544,00 KB
        Durchschnittliche Anzahl Teilsicherungen seit letzter Gesamtsicherung: 0
        Durchschnittsaufwand für zusätzliche Daten: 0
        Durchschnittliche Objektfragmentierung: 0
        Durchschnittliche Anzahl Objekte pro Sicherung: 71
```

Die detaillierte Ausgabe umfasst auch den Momentaufnahmetyp und Datenträgerinformationen wie die folgenden:

Momentaufnahmetyp
: Der Typ der Momentaufnahme, der während der VM-Sicherungsoperation erstellt wurde:

  Hyper-V RCT - anwendungskonsistent
  : Eine stillgelegte Momentaufnahme, die mit Hyper-V Resilient Change Tracking (RCT) unter Windows Server 2016 erstellt wurde.

  Hyper-V RCT - absturzkonsistent
  : Eine nicht stillgelegte Momentaufnahme, die mit Hyper-V RCT unter Windows Server 2016 erstellt wurde.

  Hyper-V VSS
  : Eine Momentaufnahme, die mit dem Volumeschattenkopiedienst (Volume Shadow Copy Service, VSS) unter Windows Server 2012 oder Windows Server 2012 R2 erstellt wurde.

Platte[*n*]Position
: Die Plattenposition der VM-Platte *n*; dabei ist *n* eine Zahl. Die Plattenposition besteht aus dem Plattencontrollertyp ("IDE" oder "SCSI") gefolgt von der Controllernummer und der Einheitenpositionsnummer.

Platte[*n*]Status
: Der Sicherungsstatus der VM-Platte *n*; dabei ist *n* eine Zahl.

  Geschützt
  : Gibt an, dass die Daten auf der VM-Platte gesichert werden.

  Übersprungen: Nach Benutzer ausgeschlossen
  : Gibt an, dass die VM-Platte während Sicherungsoperationen wie durch die Option exclude.vmdisk angegeben ausgeschlossen wird. Weitere Informationen finden Sie in Exclude.vmdisk.

  Übersprungen: Physische Platte

Gibt an, dass es sich bei der VM-Platte um eine physische Platte (Durchgriffsplatte) handelt, deren Daten nicht gesichert werden. Es werden nur die Plattenkonfigurationsinformationen gesichert. Weitere Informationen finden Sie in Vmprocessvmwithphysdisks.

Das folgende Beispiel zeigt die Syntax, die verwendet werden muss, um die detaillierte Ausgabe für eine bestimmte virtuelle Maschine mit dem Namen `DeptA_VM_W2k08R2` aufzulisten.

```
dsmc query vm DeptA_VM_W2k08R2 -detail

VM-Gesamtsicherung auf virtueller Maschine abfragen

 Nr. Sicherungsdatum     Verw.-Klasse Größe        Typ      A/I Position  Virtuelle Maschine
---  ------------------  ----------  -----------  ------   --- --------  ---------------
  1  20.03.2017 01:51:34  STANDARD       15,00 GB  IFINCR    A  SERVER    DeptA_VM_W2k08R2
        Größe dieser Teilsicherung: 544,00 KB
        Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1
        Zusätzliches Datenvolumen: 0
        IBM Spectrum Protect-Objektfragmentierung: 2
        Sicherung ist dargestellt durch: 37 IBM Spectrum Protect-Objekte
        Art des Anwendungsschutzes: nicht zutreffend
        Die Sicherung ist komprimiert: Nein
        Die Sicherung ist dedupliziert: Nein
        Momentaufnahmetyp: Hyper-V RCT - absturzkonsistent
        Platte[1]Name: Jimmy_VM_Windows2008R2.vhdx
        Platte[1]Position: IDE 0 0
        Platte[1]Status: Geschützt
--------------------------------------------------------------------------------
        Alle Durchschnittswerte werden nur für oben angezeigte immer inkrementelle
        Sicherungen berechnet.
        Durchschnittsgröße der Teilsicherung: 544,00 KB
        Durchschnittliche Anzahl Teilsicherungen seit letzter Gesamtsicherung: 1
        Durchschnittsaufwand für zusätzliche Daten: 0
        Durchschnittliche Objektfragmentierung: 2
        Durchschnittliche Anzahl Objekte pro Sicherung: 37
```

Restart Restore

Mit dem Befehl restart restore kann eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt werden.

Sie können nur jeweils eine wiederanlauffähige Zurückschreibungssitzung erneut starten. Führen Sie den Befehl restart restore erneut aus, um weitere Zurückschreibungen erneut zu starten.

Bei der erneut gestarteten Zurückschreibung werden dieselben Optionen wie bei der fehlgeschlagenen Zurückschreibung verwendet. Die erneut gestartete Zurückschreibung wird an dem Punkt fortgesetzt, an dem die Zurückschreibung zuvor fehlgeschlagen ist.

Zum Abbrechen wiederanlauffähiger Zurückschreibungssitzungen den Befehl cancel restore verwenden. Den Befehl restart restore in folgenden Fällen verwenden:

- Wiederanlauffähige Zurückschreibungssitzungen sperren den Dateibereich auf dem Server, sodass Dateien nicht von den sequenziellen Serverdatenträgern weg verschoben werden können.
- Dateien, die von der wiederanlauffähigen Zurückschreibung betroffen sind, können nicht gesichert werden.

Optionen der fehlgeschlagenen Sitzung überlagern neue oder geänderte Optionen für die erneut gestartete Sitzung.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-RESTArt Restore-----------------------------------------------><
```

Parameter

Für diesen Befehl gibt es keine Parameter.

Beispiele

Task
: Eine Zurückschreibungssitzung erneut starten.

Befehl: `restart restore`

Restore

Mit dem Befehl restore werden Kopien der Sicherungsversionen Ihrer Dateien vom IBM Spectrum Protect-Server oder aus einem Sicherungssatz abgerufen.

Zum Zurückschreiben der Dateien müssen die Verzeichnisse oder die ausgewählten Dateien angegeben oder die Dateien aus einer Liste ausgewählt werden. Dateien können in das Verzeichnis zurückgeschrieben werden, aus dem sie gesichert wurden, oder in ein anderes Verzeichnis. Der Client für Sichern/Archivieren verwendet die Option preservepath mit dem Wert subtree als Standardwert zum Zurückschreiben von Dateien.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAnmerkung:

1. Für UNIX- und Linux-Systeme: Wird eine symbolische Verbindung erstellt, wird ihre Änderungszeit auf die aktuelle Systemzeit gesetzt. Diese Zeit kann nicht geändert werden. Wenn eine symbolische Verbindung zurückgeschrieben wird, werden daher Datum und Uhrzeit der Zurückschreibung als ihr Änderungsdatum und ihre Änderungszeit festgelegt und nicht das Datum und die Uhrzeit der Verbindung bei ihrer Sicherung. Folglich sichert der Client die symbolische Verbindung während der nächsten Teilsicherung, weil sich ihre Änderungszeit seit der letzten Sicherung geändert hat.

Windows-BetriebssystemeAnmerkung:

1. Wenn Sie ein Verzeichnis zurückschreiben, werden das Datum und die Uhrzeit der Zurückschreibung als Änderungsdatum und Änderungszeit festgelegt und nicht das Datum und die Uhrzeit des Verzeichnisses bei seiner Sicherung. Die Ursache dafür ist, dass der Client zuerst die Verzeichnisse zurückschreibt und anschließend die Dateien zu den Verzeichnissen hinzufügt.
2. Wird versucht, eine Datei zurückzuschreiben, deren Name mit dem Kurznamen einer vorhandenen Datei identisch ist, tritt ein Fehler auf. Wenn Sie beispielsweise versuchen, eine Datei, der ausdrücklich der Name ABCDEF~1.DOC zugeordnet wurde, in ein Verzeichnis zurückzuschreiben, in dem sich eine Datei mit dem Namen abcdefghijk.doc befindet, schlägt die Zurückschreibung fehl, weil das Windows-Betriebssystem die Datei mit dem Namen abcdefghijk.doc dem Kurznamen ABCDEF~1.DOC gleichsetzt. Die Zurückschreibungsfunktion behandelt dies als doppelte Datei.
   Wenn dieser Fehler auftritt, kann er mit einer der folgenden Maßnahmen korrigiert werden:
   - Die Datei mit dem Kurzdateinamen an eine andere Position zurückschreiben.
   - Die Zurückschreibung stoppen und den Namen der vorhandenen Datei ändern.
   - Die Unterstützung für Kurzdateinamen auf Windows inaktivieren.
   - Keine Dateinamen verwenden, die mit der Kurzdateinamenskonvention unverträglich sind, z. B. ABCDEF~1.DOC.

Wenn Sie beim Zurückschreiben eines bestimmten Pfads und einer bestimmten Datei die Option subdir auf yes setzen, führt der Client eine rekursive Zurückschreibung aller Unterverzeichnisse unter diesem Pfad und aller Instanzen der angegebenen Datei durch, die sich unter allen diesen Unterverzeichnissen befinden.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWenn Sie ein vollständiges Verzeichnis oder eine vollständige Verzeichnisstruktur zurückschreiben und nicht die Option inactive, latest, pick, todate und fromdate im Befehl restore angeben, verfolgt der Client, welche Objekte zurückgeschrieben werden. Wird der Zurückschreibungsprozess unterbrochen, kann er mithilfe des Befehls restart restore am Unterbrechungspunkt erneut gestartet werden. Es können mehrere wiederanlauffähige Zurückschreibungssitzungen erstellt werden. Zurückschreibungssitzungen können nur dann erneut gestartet werden, wenn die Dateispezifikation ausschließlich aus Platzhalterzeichen besteht. Für eine wiederanlauffähige Zurückschreibungssitzung kann beispielsweise Folgendes eingegeben werden:

```
dsmc rest /home/* -sub=yes
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie Eingabe für eine nicht wiederanlauffähige Zurückschreibungssitzung sieht wie folgt aus:

```
dsmc rest "/Users/user1/file?.c" -sub=yes
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeMit dem Befehl query restore wird eine Liste der wiederanlauffähigen Zurückschreibungssitzungen des Benutzers in der Serverdatenbank angezeigt. Es können keine weiteren Sicherungen des Dateisystems ausgeführt werden, bis die wiederanlauffähige Zurückschreibung mit dem Befehl restart restore abgeschlossen oder mit dem Befehl cancel restore abgebrochen wird.

```
dsmc rest "/Users/user1/file?.c" -sub=yes
```

Windows-BetriebssystemeWeitere Informationen finden Sie im Artikel Q121007 der Microsoft Knowledge Base mit dem Titel *How to Disable the 8.3 Name Creation on NTFS Partitions*.

Windows-BetriebssystemeWird der Befehl restore wegen eines Übertragungs- oder Sitzungsfehlers wiederholt, zeigen die Übertragungsstatistiken die Byte an, die der Client während aller Befehlswiederholungen zu übertragen versucht hat. Daher entsprechen die Statistiken für die übertragenen Byte möglicherweise nicht den Dateistatistiken, z. B. für die Dateigröße.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
            .- --FILE-.
>>-REStore--+---------+--+-------------+------------------------>
                         '- --Optionen-'

>--+- --Quellendateispezifikation-------------------------+---->
   '- --{--Dateibereichsname--}--Quellendateispezifikation-'

>--+- --Quellendateispezifikation---+-------------------------->
   '- --"Quellendateispezifikation"-'

>--+---------------------------+------------------------------->
   '- --Zieldateispezifikation-'

>--+-----------------------------------------------+------------>
   '-BACKUPSETName=--+-Name des Sicherungssatzes-+-'
                     +-Name der lokalen Datei----+
                     '-Bandeinheit---------------'

>--+-----------------------+---------------------------------><
   '-LOCation=--+-server-+-'
                +-file---+
                '-tape---'
```

Parameter

file

Dieser Parameter gibt an, dass die Quellendateispezifikation ein expliziter Dateiname ist. Dieser Parameter ist erforderlich, wenn ein Dateiname aus dem aktuellen Pfad zurückgeschrieben wird, kein relativer oder absoluter Pfad angegeben wird und der Dateiname mit einem der reservierten Schlüsselwörter des Befehls restore, wie z. B. restore backupset, unverträglich ist.

Quellendateispezifikation

Gibt den Pfad und den Namen der Datei im Speicher an, die zurückgeschrieben werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.

 Windows-BetriebssystemeAnmerkung: Wenn Dateibereichsname angegeben wird, darf die Dateispezifikation keinen Laufwerkbuchstaben enthalten.

{Dateibereichsname}

Gibt den in geschweiften Klammern eingeschlossenen Dateibereich auf dem Server an, in dem sich die zurückzuschreibenden Dateien befinden. Dies ist der Name auf dem Workstationlaufwerk, auf dem die Dateien gesichert wurden.

Geben Sie den Dateibereichsnamen an, wenn sich die Laufwerkbezeichnung geändert hat oder wenn Sie Dateien zurückschreiben, die auf einem anderen Knoten gesichert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.

 Windows-BetriebssystemeAnmerkung: Sie müssen einen NTFS- oder ReFS-Dateibereichsnamen in Groß-/Kleinschreibung oder in Kleinschreibung angeben, der zwischen Anführungszeichen und geschweiften Klammern steht. Beispiel: {"NTFSDrive"}. Hochkommas oder Anführungszeichen sind im Schleifenmodus gültig. Beispielsweise ist sowohl {"NTFSDrive"} als auch {'NTFSDrive'} gültig. Im Stapelmodus sind nur Hochkommas gültig. Die Einschränkung auf Hochkommas ist im Betriebssystem begründet.

Zieldateispezifikation

Gibt den Pfad und den Dateinamen für das Ziel der zurückgeschriebenen Dateien an. Wenn Sie kein Ziel angeben, schreibt der Client die Dateien in den ursprünglichen Quellenpfad zurück.

 Windows-BetriebssystemeBeachten Sie bei der Eingabe der Zieldateispezifikation Folgendes:

- Wenn die Quellendateispezifikation eine einzelne Datei benennt, kann die Zieldateispezifikation eine Datei oder ein Verzeichnis sein. Wenn Sie eine einzelne Datei zurückschreiben, kann die Spezifikation wahlweise mit einem Dateinamen enden, wenn die zurückgeschriebene Datei einen neuen Namen erhalten soll.
- Wenn die Quellendateispezifikation Platzhalterzeichen enthält oder wenn `subdir=yes` angegeben wird, muss die Zieldateispezifikation ein Verzeichnis sein und mit einem Verzeichnisbegrenzer (\) enden.

Anmerkung: Falls der Zielpfad oder ein Teil davon nicht vorhanden ist, wird er vom Client erstellt.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeAnmerkung: Wenn Sie kein Ziel angeben, stellt der Client fest, ob das ursprüngliche Dateisystem erreicht werden kann. Kann das ursprüngliche Dateisystem nicht erreicht werden, schreibt der Client die Datei nicht zurück. In diesem Fall können Sie ein anderes Ziel angeben und den Befehl wiederholen.

BACKUPSETName=

Gibt den Namen eines Sicherungssatzes an. Dieser Parameter ist optional. Wenn Sie den Parameter backupsetname im Befehl restore angeben, können Sie nicht die Option pick verwenden.

Der Wert von backupsetname ist von der Position des Sicherungssatzes abhängig und entspricht einer der folgenden Optionen:

backupsetname

Gibt den Namen des Sicherungssatzes auf dem IBM Spectrum Protect-Server an. Wird der Parameter location angegeben, müssen Sie `-location=server` angeben. Ist der Sicherungssatz im IBM Spectrum Protect-Serverspeicher gespeichert, muss der Sicherungssatz über ein Inhaltsverzeichnis verfügen.

Name der lokalen Datei
: Gibt den Dateinamen des ersten Datenträgers des Sicherungssatzes an. Sie müssen `-location=file` angeben.

Bandeinheit
: Gibt den Namen der Bandeinheit an, die den Datenträger des Sicherungssatzes enthält. Sie müssen einen von Windows bereitgestellten Einheitentreiber und nicht den von IBM bereitgestellten Einheitentreiber verwenden. Sie müssen `-location=tape` angeben.

LOCation=
: Gibt an, wo der Client nach dem Sicherungssatz sucht. Wenn Sie den Parameter location nicht angeben, sucht der Client auf dem IBM Spectrum Protect-Server nach Sicherungssätzen.

Server
: Gibt an, dass der Client den Sicherungssatz auf dem Server sucht. Dies ist die Standardposition.

file
: Gibt an, dass der Client den Sicherungssatz in einer lokalen Datei sucht.

tape
: Gibt an, dass der Client den Sicherungssatz auf einer lokalen Bandeinheit sucht.

Tabelle 1. Befehl Restore: Zugehörige Optionen

Option	**Verwendung**
Windows-Betriebssystemeasrmode	Windows-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssystemedateformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedateformat	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
dirsonly	Nur in der Befehlszeile.
filelist	Nur in der Befehlszeile.
filesonly	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme followsymbolic	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
fromdate	Nur in der Befehlszeile.
fromnode	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-Betriebssystemefromowner	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeMac OS X-BetriebssystemeNur in der Befehlszeile.
fromtime	Nur in der Befehlszeile.
ifnewer	Nur in der Befehlszeile.
inactive	Nur in der Befehlszeile.
latest	Nur in der Befehlszeile.
Windows-Betriebssysteme numberformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme numberformat	AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
pick Anmerkung: Wenn Sie den Parameter backupsetname im Befehl restore angeben, können Sie nicht die Option pick verwenden.	Nur in der Befehlszeile.

Option	Verwendung
pitdate	Nur in der Befehlszeile.
pittime	Nur in der Befehlszeile.
preservepath	Nur in der Befehlszeile.
Windows-Betriebssystemereplace	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemereplace	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme skipntpermissions	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme skipntsecuritycrc	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemesubdir	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemesubdir	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme tapeprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme tapeprompt	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemetimeformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemetimeformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate	Nur in der Befehlszeile.
totime	Nur in der Befehlszeile.

Beispiele

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeEine einzelne Datei mit dem Namen `budget` im Verzeichnis `/Users/user1/Documents` zurückschreiben.

```
restore /home/devel/projecta/budget
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine einzelne Datei mit dem Namen `budget.fin` zurückschreiben.

```
restore c:\devel\projecta\budget.fin
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeEine einzelne Datei mit dem Namen `budget` zurückschreiben, die sich im aktuellen Verzeichnis befindet.

```
restore file budget
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine einzelne Datei mit dem Namen `budget.fin` zurückschreiben, die sich im aktuellen Verzeichnis befindet.

```
restore file budget.fin
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeDateien aus dem Verzeichnis `proj` im Dateibereich `abc` zurückschreiben.

```
rest {"abc"}\proj\*.*
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien mit der Dateierweiterung `.c` aus dem Verzeichnis `/home/devel/projecta` zurückschreiben.

```
restore "/home/devel/projecta/*.c"
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeAlle Dateien mit der Dateierweiterung `.c` aus dem Verzeichnis `c:\devel\projecta` zurückschreiben.

```
rest c:\devel\projecta\*.c
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeAlle Dateien mit der Erweiterung `.c` aus dem Verzeichnis `\devel\projecta` zurückschreiben, das sich im Dateibereich `winnt` befindet.

```
rest {winnt}\devel\projecta\*.c
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeAlle Dateien mit der Dateierweiterung `.c` aus dem Verzeichnis `c:\devel\projecta` in das Verzeichnis `c:\newdevel\projectn\projecta` zurückschreiben. Ist das Verzeichnis `projectn` oder `projectn\projecta` nicht vorhanden, wird es erstellt.

```
restore c:\devel\projecta\*.c c:\newdevel\projectn\
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDateien im Verzeichnis `/user/project` zurückschreiben. Mithilfe der Optionen pick und inactive aktive und inaktive Sicherungsversionen auswählen.

```
restore "/user/project/*" -pick -inactive
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeDateien im Verzeichnis `c:\project` zurückschreiben. Mithilfe der Optionen pick und inactive aktive und inaktive Sicherungsversionen auswählen.

```
restore c:\project\* -pi -ina
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien aus dem Verzeichnis `/home/devel/projecta`, deren Name auf `.c` endet, in das Verzeichnis `/home/newdevel/projectn/projecta` zurückschreiben. Ist das Verzeichnis `projectn` oder `projectn/projecta` nicht vorhanden, wird es erstellt.

```
restore "/home/devel/projecta/*.c" /home/newdevel/projectn/
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien im Verzeichnis `/home/mydir` mit ihrem Status am 17. August 2002 um 13:00 Uhr zurückschreiben.

```
restore -pitd=8/17/2002 -pitt=13:00:00 /home/mydir/
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeAlle Dateien im Verzeichnis `c:\mydir` mit ihrem Status am 17. August 2002 um 13:00 Uhr zurückschreiben.

```
restore -pitd=8/17/2002 -pitt=13:00:00 c:\mydir\
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Objekte im Verzeichnis `/home/myid/` zurückschreiben. Da diese Zurückschreibungsoperation ausschließlich aus Platzhalterzeichen besteht, wird eine wiederanlauffähige Zurückschreibungssitzung erstellt, falls der Zurückschreibungsprozess unterbrochen wird.

```
res "/home/myid/*"
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeEine Datei aus dem umbenannten Dateibereich `\\Ihr-Knoten\h$_OLD` an ihre ursprüngliche Position zurückschreiben. Geben Sie sowohl die Quelle als auch das Ziel wie folgt ein:

```
res \\Ihr-Knoten\h$_OLD\docs\myresume.doc h:\docs\
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien im Verzeichnis `/home/mydir` mit ihrem Status am 17. August 2002 um 13:00 Uhr zurückschreiben.

```
restore -pitd=8/17/2002 -pitt=13:00:00 /home/mydir/
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeAlle Dateien im Verzeichnis `c:\mydir` mit ihrem Status am 17. August 2002 um 13:00 Uhr zurückschreiben.

```
restore -pitd=8/17/2002 -pitt=13:00:00 c:\mydir\
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine einzelne Datei mit dem Namen `budget.fin` zurückschreiben, die sich in dem Sicherungssatz `daily_backup_data.12345678` befindet.

```
restore c:\projecta\budget.fin -backupsetname=daily_backup_data.12345678 -location=server
```

- Mountpunkte für NTFS- oder ReFS-Datenträger zurückschreiben
  Wenn ein Dateisystem zurückgeschrieben wird, das einen Datenträgerladepunkt enthält, wird nur der Mountpunkt (Verzeichnis) zurückgeschrieben. Die Daten auf dem Datenträger, der in diesem Verzeichnis angehängt ist, werden nicht zurückgeschrieben.
- Windows-BetriebssystemeMicrosoft DFS-Zusammenführungen zurückschreiben
  Zum Zurückschreiben von Microsoft DFS-Zusammenführungen müssen Sie den Microsoft DFS-Stamm zurückschreiben.
- Windows-BetriebssystemeAktive Dateien zurückschreiben
  Werden die aktive Version und die inaktive Version einer Datei mit der Option replace zurückgeschrieben, wird nur die zuletzt zurückgeschriebene Datei ersetzt.
- Windows-BetriebssystemeZurückschreibungen mit Universal Naming Convention
  Für die Speicherung von Dateien auf dem IBM Spectrum Protect-Server verwendet der Client die Windows Universal Naming Convention (UNC - allgemeine Namenskonvention), nicht den Laufwerkbuchstaben. Der UNC-Name ist der Netzname der Datei. Der Systemname ist Teil des UNC-Namens. Lautet Ihr Systemname beispielsweise STAR und der Dateiname c:\doc\h2.doc, lautet der UNC-Name \\star\c$\doc\h2.doc.
- Mac OS X-BetriebssystemeWindows-BetriebssystemeAus nicht Unicode-fähigen Dateibereichen zurückschreiben
  Wenn Sie aus Dateibereichen zurückschreiben wollen, die nicht Unicode-fähig sind, müssen Sie die Quelle auf dem Server und ein Ziel auf dem Client angeben, bevor Sie den Client mit Unicode-Unterstützung installieren.
- Windows-BetriebssystemeBenannte Datenströme zurückschreiben
  Der Client für Sichern/Archivieren schreibt benannte Datenströme nur auf Dateibasis zurück.
- Windows-BetriebssystemeDateien mit freien Bereichen zurückschreiben
  Wenn Sie Dateien mit freien Bereichen in ein Nicht-NTFS- oder Nicht-ReFS-Dateisystem zurückschreiben, geben Sie als Wert des IBM Spectrum Protect-Serverübertragungszeitlimits (idletimeout) den Maximalwert 255 an, um eine Zeitlimitüberschreitung der Clientsitzung zu vermeiden.

Windows-Betriebssysteme

Mountpunkte für NTFS- oder ReFS-Datenträger zurückschreiben

Wenn ein Dateisystem zurückgeschrieben wird, das einen Datenträgerladepunkt enthält, wird nur der Mountpunkt (Verzeichnis) zurückgeschrieben. Die Daten auf dem Datenträger, der in diesem Verzeichnis angehängt ist, werden nicht zurückgeschrieben.

Ein Mountpunkt kann auch einzeln zurückgeschrieben werden. Beispiel: C:\mount ist ein Mountpunkt, der als Teil des Laufwerks C:\ auf dem System STORMAN gesichert wurde. Dieser Mountpunkt kann mit dem folgenden Befehl zurückgeschrieben werden:

```
dsmc restore {\\storman\c$}\mount
```

Die geschweiften Klammern ({ }) sind erforderlich, wenn Sie auch die Daten auf dem angehängten Datenträger an dem Mountpunkt gesichert haben. Ohne die geschweiften Klammern schreibt der Client Daten aus dem Dateibereich mit dem der Dateispezifikation entsprechenden längsten Namen zurück. Wenn Sie die Daten über den Mountpunkt gesichert haben, werden die Sicherungen in einem Dateibereich mit dem Namen \\storman\c$\mount gespeichert. Mit den geschweiften Klammern wird angegeben, dass die Daten aus dem Dateibereich \\storman\c$ zurückgeschrieben werden sollen.
Der Mountpunkt kann nicht zurückgeschrieben werden, wenn eine der folgenden Bedingungen zutrifft:

- Der Mountpunkt ist bereits vorhanden.
- Ein dem Mountpunktnamen entsprechendes nicht leeres Verzeichnis ist vorhanden.
- Eine dem Mountpunktnamen entsprechende Datei ist vorhanden.

- Daten auf über NTFS angehängten Datenträgern zurückschreiben
  Der Mountpunkt muss vorhanden sein, damit die Daten auf dem angehängten Datenträger an ihre ursprüngliche Position zurückgeschrieben werden können.

Zugehörige Konzepte:
Daten auf über NTFS angehängten Datenträgern zurückschreiben
NTFS- oder ReFS-Datenträgermountpunkte sichern
Daten auf über NTFS oder ReFS angehängten Datenträgern sichern
Windows-Betriebssysteme

Microsoft DFS-Zusammenführungen zurückschreiben

Zum Zurückschreiben von Microsoft DFS-Zusammenführungen müssen Sie den Microsoft DFS-Stamm zurückschreiben.

Wird der Zusammenführungspunkt selbst ausgewählt, schreibt der Client für Sichern/Archivieren Daten unter der Zusammenführung, aber nicht die Zusammenführung selbst zurück. Wird ein Zusammenführungspunkt ausgewählt, der unter dem DFS-Stamm nicht mehr vorhanden ist, erstellt der Client vor dem Zurückschreiben von Daten ein lokales Verzeichnis unter dem DFS-Stamm mit demselben Namen wie die Zusammenführung.

Windows-Betriebssysteme

Aktive Dateien zurückschreiben

Werden die aktive Version und die inaktive Version einer Datei mit der Option replace zurückgeschrieben, wird nur die zuletzt zurückgeschriebene Datei ersetzt.

Windows-Betriebssysteme

Zurückschreibungen mit Universal Naming Convention

Für die Speicherung von Dateien auf dem IBM Spectrum Protect-Server verwendet der Client die Windows Universal Naming Convention (UNC - allgemeine Namenskonvention), nicht den Laufwerkbuchstaben. Der UNC-Name ist der Netzname der Datei. Der Systemname ist Teil des UNC-Namens. Lautet Ihr Systemname beispielsweise STAR und der Dateiname c:\doc\h2.doc, lautet der UNC-Name \\star\c$\doc\h2.doc.

Wenn Sie Dateien auf dasselbe System zurückschreiben, von dem sie gesichert wurden, können Sie den lokalen Laufwerkbuchstaben oder den UNC-Namen für die Datei angeben. Jeder der beiden folgenden Befehle schreibt c:\doc\h2.doc an die ursprüngliche Position zurück:

```
dsmc restore c:\doc\h2.doc
dsmc restore \\star\c$\doc\h2.doc
```

Wenn Sie Dateien auf ein System mit einem anderen Namen zurückschreiben, müssen Sie den UNC-Namen für die Datei angeben. Dies gilt auch, wenn auf dasselbe physische System zurückgeschrieben wird, dessen Name sich seit der Sicherung jedoch geändert hat.
Wenn Sie beispielsweise c:\doc\h2.doc auf System STAR sichern und auf System METEOR zurückschreiben wollen, müssen Sie den UNC-Namen für die Datei angeben. Sie müssen außerdem ein Ziel für die Zurückschreibung angeben. Das ist erforderlich, weil die Datei standardmäßig an ihre ursprüngliche Position (auf System STAR) zurückgeschrieben wird. Damit die Datei auf das System METEOR zurückgeschrieben wird, können Sie einen der folgenden Befehle auf METEOR ausführen:

```
dsmc restore \\star\c$\doc\h2.doc c:\
dsmc restore \\star\c$\doc\h2.doc \\meteor\c$\
```

Mac OS X-BetriebssystemeWindows-Betriebssysteme

Aus nicht Unicode-fähigen Dateibereichen zurückschreiben

Wenn Sie aus Dateibereichen zurückschreiben wollen, die nicht Unicode-fähig sind, müssen Sie die Quelle auf dem Server und ein Ziel auf dem Client angeben, bevor Sie den Client mit Unicode-Unterstützung installieren.

Mac OS X-BetriebssystemeAnmerkung: Dieser Unicode-Abschnitt gilt nur für Mac OS X.

Windows-BetriebssystemeWenn Sie aus Dateibereichen zurückschreiben wollen, die nicht Unicode-fähig sind, müssen Sie die Quelle auf dem Server und ein Ziel auf dem Client angeben. Beispiel: Sie haben Ihre Platte `H` mit dem Namen `\\Ihr-Knoten\h$` gesichert, bevor Sie den Client mit Unicode-Unterstützung installiert haben. Nach der Installation geben Sie den folgenden Befehl für eine selektive Sicherung ein:

Windows-Betriebssysteme

```
sel h:\logs\*.log
```

Mac OS X-BetriebssystemeBeispiel: Angenommen, `Jaguar` ist der Name Ihrer Startplatte und Sie sichern alle `.log`-Dateien im Verzeichnis `/Users/user5/Documents`. Bevor die Sicherung stattfindet, benennt der Server den Dateibereich in `Jaguar_OLD` um. Bei der Sicherung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen `/` gestellt. Der neue Unicode-fähige Dateibereich enthält nun nur das Verzeichnis `/Users/user5/Documents` und die Dateien `*.log`, die in der Operation angegeben wurden.

Mac OS X-BetriebssystemeWenn eine Datei aus dem *umbenannten* (alten) Dateibereich an die ursprüngliche Position zurückgeschrieben werden soll, müssen Sie sowohl die Quelle als auch das Ziel wie folgt eingeben:

```
restore Jaguar_OLD/Users/user5/Documents
  /mylog.log /Users/user5/Documents/
```

Windows-BetriebssystemeBevor die Sicherung stattfindet, benennt der Server den Dateibereich in `\\Ihr-Knoten\h$_OLD` um. Bei der Sicherung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen `\\Ihr-Knoten\h$` gestellt. Dieser Dateibereich enthält nun nur das Verzeichnis `\logs` und die Dateien `*.log`. Wenn eine Datei aus dem (alten) *umbenannten* Dateibereich an ihre ursprüngliche Position zurückgeschrieben werden soll, müssen Sie sowohl die Quelle als auch das Ziel wie folgt eingeben:

```
restore \\Ihr-Knoten\h$_OLD\docs\myresume.doc h:\docs\
```

Windows-Betriebssysteme

Benannte Datenströme zurückschreiben

Der Client für Sichern/Archivieren schreibt benannte Datenströme nur auf Dateibasis zurück.

Windows-Verzeichnisse können benannte Datenströme enthalten. Benannte Datenströme, die einem Verzeichnis zugeordnet sind, werden während einer Operation zum Zurückschreiben immer überschrieben (unabhängig vom Wert der Prompt-Option).


Windows-Betriebssysteme

Dateien mit freien Bereichen zurückschreiben

Wenn Sie Dateien mit freien Bereichen in ein Nicht-NTFS- oder Nicht-ReFS-Dateisystem zurückschreiben, geben Sie als Wert des IBM Spectrum Protect-Serverübertragungszeitlimits (idletimeout) den Maximalwert 255 an, um eine Zeitlimitüberschreitung der Clientsitzung zu vermeiden.

Der Client für Sichern/Archivieren ist auf das Zurückschreiben von Dateien mit freien Bereichen beschränkt, deren Größe kleiner als 4 GB ist.

Die folgenden Probleme treten auf, wenn mehr Daten zurückgeschrieben werden als das Microsoft-Datenträgerkontingent zulässt:

- Wenn der Benutzer, der die Zurückschreibung ausführt, ein Datenträgerkontingent hat (er gehört beispielsweise zur Gruppe 'Sicherungsoperatoren'), schreibt der Client keine Daten zurück, die das Datenträgerkontingent des Benutzers, der die Zurückschreibung ausführt, überschreiten, und zeigt die Nachricht "Platte voll" an.
- Wenn der Benutzer, der die Zurückschreibung ausführt, kein Datenträgerkontingent hat (er gehört beispielsweise zur Gruppe 'Administratoren'), schreibt der Client alle Daten zurück und überträgt die Eigentumsrechte der Dateien, die das Datenträgerkontingent des ursprünglichen Eigners überschreiten, an den Benutzer, der die Zurückschreibung ausführt (in diesem Fall an den Administrator).


Windows-Betriebssysteme

Restore Adobjects

Verwenden Sie den Befehl restore adobjects, um einzelne Active Directory-Objekte aus dem lokalen Container für gelöschte Objekte zurückzuschreiben.

Auf Windows Server-Plattformen ausgeführte Clients für Sichern/Archivieren können einzelne Active Directory-Objekte aus vollständigen Systemstatussicherungen zurückschreiben, die auf dem IBM Spectrum Protect gespeichert sind.

Unterstützte Clients

Dieser Befehl ist für Windows Server-Betriebssystemclients gültig.

Syntax

```
>>-Restore ADOBJects--+-------------------------+-------------->
                      '-Quellenpfadspezifikation-'

>--+----------+-------------------------------------------------><
   '-Optionen-'
```

Parameter

Quellenpfadspezifikation
: Gibt das Active Directory-Objekt oder den Container für die Zurückschreibung an. Wird ein Container angegeben, wird auch sein Inhalt zurückgeschrieben. Sie können entweder den vollständigen definierten Namen eines Objekts oder Containers angeben oder nur das Namensattribut ('cn' oder 'ou') und dabei Platzhalterzeichen verwenden. Die folgenden Sonderzeichen erfordern ein Escapezeichen, den umgekehrten Schrägstrich (\), wenn sie in dem Namen enthalten sind:

  - \
  - #
  - +
  - =
  - <
  - >

  Beispielsweise wird "`cn=test#`" als "`cn=test\#`" eingegeben.

  Der Client kann keine Objektnamen anzeigen, die einen Stern (*) als Teil des Namens enthalten.

  Verwenden Sie keine Platzhalterzeichen, wenn Sie einen definierten Namen angeben.

Tabelle 1. Befehl Restore Adobjects: Zugehörige Optionen

Option	Verwendung
adlocation	Nur in der Befehlszeile.

Option	Verwendung
dateformat (Die Option wird ignoriert, wenn adlocation nicht angegeben ist.)	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
pitdate (Die Option wird ignoriert, wenn adlocation nicht angegeben ist.)	Nur in der Befehlszeile.
pittime (Die Option wird ignoriert, wenn adlocation nicht angegeben ist.)	Nur in der Befehlszeile.
replace	Clientoptionsdatei (dsm.opt) oder Befehlszeile.
timeformat (Die Option wird ignoriert, wenn adlocation nicht angegeben ist.)	Clientoptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task
Ein bestimmtes gelöschtes Active Directory-Objekt zurückschreiben.

Befehl: `restore adobj "CN=Administrator,CN=Users,DC=bryan,DC=test,DC=ibm,DC=com"`

Task
Alle gelöschten Objekte zurückschreiben, die ursprünglich im Container 'Users' enthalten waren.

Befehl: `restore adobj "CN=Users,DC=bryan,DC=test,DC=ibm,DC=com"`

Task
Einzelne Active Directory-Objekte vom IBM Spectrum Protect-Server zurückschreiben. Verwenden Sie die Optionen pitdate und pittime, um eine Auswahl aus einer Liste neuerer und älterer Sicherungsversionen zu treffen.
Befehl: `restore adobj "cn=guest" -adloc=server -pitdate=03/17/2008 -pittime=11:11:11`

Task
Alle gelöschten Benutzer zurückschreiben, deren Name mit `Fred` beginnt.

Befehl: `restore adobjects "cn=Fred*"`

Task
Alle gelöschten Organisationseinheiten mit dem Namen `testou` zurückschreiben.

Befehl: `restore adobjects "ou=testou"`

Restore Backupset

Der Befehl restore backupset schreibt einen Sicherungssatz vom IBM Spectrum Protect-Server, von einer lokalen Datei oder von einer lokalen Bandeinheit zurück. Sie können den vollständigen Sicherungssatz oder in einigen Fällen bestimmte Dateien in dem Sicherungssatz zurückschreiben.

AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-REStore Backupset-------------------------------------------->

>--+-------------------------------------------------------+------->
   '-+---------------------+--Quellendateispezifikation-'
     '-{Dateibereichsname}-'

>--+-------------------------+--+----------+--------------------->
   '-Zieldateispezifikation-'  '-Optionen-'

>-- -BACKUPSETName= --+-Name des Sicherungssatzes-+------------->
                       +-Name der lokalen Datei----+
                       '-Bandeinheit---------------'

>--+--------------------------+-------------------------------><
   '- -LOCation= --+-server-+-'
                   +-file---+
```

```
'-tape---'
```

Parameter

{Dateibereichsname}
Gibt den in geschweiften Klammern eingeschlossenen Dateibereich auf dem Server an, in dem sich die zurückzuschreibenden Dateien befinden. Dies ist der Name des Workstationlaufwerks, auf dem die Dateien gesichert wurden, oder der Name des virtuellen Dateibereichs für eine Gruppe.

Geben Sie einen Dateibereichsnamen an, wenn Sie einen Sicherungssatz zurückschreiben, der eine Gruppe enthält.

Geben Sie einen Dateibereichsnamen an, wenn die *Quellendateispezifikation* auf dem Zielcomputer nicht vorhanden ist. Diese Situation kann eintreten, wenn sich die Laufwerkbezeichnung geändert hat oder wenn Sie Dateien zurückschreiben, die auf einem anderen Knoten gesichert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.

Windows-BetriebssystemeAnmerkung: Sie müssen einen NTFS- oder ReFS-Dateibereichsnamen in Groß-/Kleinschreibung oder in Kleinschreibung angeben, der zwischen Anführungszeichen und geschweiften Klammern steht. Beispiel: {"NTFSDrive"}. Hochkommas oder Anführungszeichen sind im Schleifenmodus gültig. Beispielsweise ist sowohl {"NTFSDrive"} als auch {'NTFSDrive'} gültig. Im Stapelmodus sind nur Hochkommas gültig. Die Einschränkung auf Hochkommas ist im Betriebssystem begründet.

Quellendateispezifikation
Gibt den Quellenpfad eines Teils des Sicherungssatzes an. Standardmäßig wird der gesamte Sicherungssatz zurückgeschrieben.

Zieldateispezifikation
Gibt den Zielpfad für die zurückgeschriebenen Dateien an. Wird keine *Quellendateispezifikation* angegeben, können Sie keine *Zieldateispezifikation* angeben. Wenn Sie kein Ziel angeben, schreibt der Client für Sichern/Archivieren die Dateien in den ursprünglichen Quellenpfad zurück. Wenn Sie mehrere Dateien zurückschreiben, muss die Dateispezifikation mit einem Verzeichnisbegrenzer (/) enden. Andernfalls geht der Client davon aus, dass der letzte Name ein Dateiname ist, und meldet einen Fehler. Wenn Sie eine einzelne Datei zurückschreiben, kann die Zieldateispezifikation optional mit einem Dateinamen enden, wenn die zurückgeschriebene Datei einen neuen Namen erhalten soll. Ist die *Quellendateispezifikation* nicht auf der Zielworkstation vorhanden, müssen Sie eine *Zieldateispezifikation* angeben.

-BACKUPSETName=
Gibt den Namen des Sicherungssatzes an, mit dem eine Zurückschreibungsoperation ausgeführt werden soll. Den Namen des Sicherungssatzes können Sie nicht mithilfe von Platzhalterzeichen angeben. Der Wert von *backupsetname* ist von der Position des Sicherungssatzes abhängig und entspricht einer der folgenden Auswahlmöglichkeiten:

Name des Sicherungssatzes
Gibt den Namen des Sicherungssatzes auf dem Server an, von dem eine Operation zum Zurückschreiben ausgeführt werden soll. Wird die Option location angegeben, müssen Sie `-location=server` angeben.

Name der lokalen Datei
Gibt den Dateinamen des ersten Datenträgers des Sicherungssatzes an. Sie müssen `-location=file` angeben.

Bandeinheit
Gibt den Namen der Bandeinheit an, die den Datenträger des Sicherungssatzes enthält. Sie müssen einen von Windows bereitgestellten Einheitentreiber und nicht den von IBM bereitgestellten Einheitentreiber verwenden. Sie müssen `-location=tape` angeben.

-LOCation=
Gibt die Position des Sicherungssatzes an. Wenn Sie den Parameter location nicht angeben, sucht der Client auf dem IBM Spectrum Protect-Server nach Sicherungssätzen. Wenn Sie den Parameter 'location' angeben, muss der Wert einer der folgenden drei Auswahlmöglichkeiten entsprechen.

server
Gibt an, dass der Sicherungssatz sich auf dem IBM Spectrum Protect-Server befindet. Server ist die Standardposition.

file
Gibt an, dass der Sicherungssatz sich auf einem verfügbaren Dateisystem befindet.

tape
Gibt an, dass der Sicherungssatz sich auf einer verfügbaren Bandeinheit befindet.

Tabelle 1. Befehl Restore Backupset: Zugehörige Optionen

Option	Verwendung
dirsonly	Nur in der Befehlszeile.
filesonly	Nur in der Befehlszeile.
ifnewer	Nur in der Befehlszeile.
preservepath	Nur in der Befehlszeile.
 Windows-Betriebssystemequiet	 Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.

Option	Verwendung
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemequiet	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemereplace	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemereplace	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme skipntpermissions	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemesubdir	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemesubdir	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

Task

Den gesamten Sicherungssatz mit dem Namen monthly_financial_data.87654321 vom Server zurückschreiben.

```
dsmc restore backupset
  -backupsetname=monthly_financial_data.87654321
   -loc=server
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDen gesamten Sicherungssatz zurückschreiben, der in der Datei /home/budget/weekly_budget_data.ost enthalten ist.

```
dsmc restore backupset
  -backupsetname="/home/budget/weekly_budget_data.ost"
   -loc=file
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDen gesamten Sicherungssatz von der Einheit /dev/rmt0 zurückschreiben.

```
dsmc restore backupset
  "-backupsetname=/dev/rmt0" -loc=tape
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDie einzelne Datei mit dem Namen /home/jones/budget.dev von der Einheit /dev/rmt0 in den ursprünglichen Quellenpfad zurückschreiben.

```
dsmc restore backupset
  -backupsetname=/dev/rmt0 "/home/jones/budget.dev"
   -loc=tape
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien im Verzeichnis budget mit der Dateierweiterung .txt von den Bändern auf der Einheit /dev/rmt0 in den ursprünglichen Quellenpfad zurückschreiben.

```
dsmc restore backupset "/home/budget/*.txt"
  -backupsetname=/dev/rmt0 -loc=tape
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDen gesamten Sicherungssatz zurückschreiben, der in der lokalen Datei "/home/jones/bset01.file" enthalten ist.

```
dsmc restore backupset
  -backupsetname="/home/jones/bset01.file"
   -loc=file
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeGruppen aus dem Sicherungssatz mybackupset.12345678 auf dem IBM Spectrum Protect-Server in das Verzeichnis /home/devel/projectb zurückschreiben. Der virtuelle Dateibereich der Gruppen ist accounting.

```
dsmc restore backupset {/accounting}/*
   /home/devel/projectb/
  -backupsetname=mybackupset.12345678 -loc=server
   -subdir=yes
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeGruppen aus dem lokalen Sicherungssatz mybackupset.ost in das Verzeichnis /home/devel/projectb/ zurückschreiben. Der virtuelle Dateibereich der Gruppen ist accounting.

```
dsmc restore backupset {/accounting}/*
   /home/devel/projectb/
   -backupsetname=mybackupset.ost
   -loc=server -subdir=yes
```

 Windows-BetriebssystemeTask

 Windows-BetriebssystemeDen gesamten Sicherungssatz von der Einheit \\.\tape0 zurückschreiben.

```
dsmc restore backupset
  -backupsetname=\\.\tape0 -loc=tape
```

 Windows-BetriebssystemeTask

 Windows-BetriebssystemeGruppen aus dem Sicherungssatz mybackupset.12345678 auf dem IBM Spectrum Protect-Server in das Verzeichnis c:\newdevel\projectn zurückschreiben. Der virtuelle Dateibereich der Gruppen ist accounting.

```
dsmc restore backupset {accounting}\*
   c:\newdevel\projectn\
   -backupsetname=mybackupset.12345678
   -loc=server -subdir=yes
```

 Windows-BetriebssystemeTask

 Windows-BetriebssystemeDen gesamten Sicherungssatz zurückschreiben, der in der Datei c:\budget\weekly_budget_data.ost enthalten ist.

```
dsmc restore backupset
  -backupsetname=c:\budget\weekly_budget_data.ost
  -loc=file
```

 Windows-BetriebssystemeTask

 Windows-BetriebssystemeDas Verzeichnis \budget\ und seine Unterverzeichnisse aus dem Sicherungssatz zurückschreiben, der in der Datei c:\budget\weekly_budget_data.ost enthalten ist.

```
dsmc restore backupset m:\budget\*
  -backupsetname=c:\budget\weekly_budget_data.ost
  -loc=file -subdir=yes
```

 Windows-BetriebssystemeTask

 Windows-BetriebssystemeDie Datei \budget\salary.xls aus dem Sicherungssatz zurückschreiben, der in der Datei c:\budget\weekly_budget_data.ost enthalten ist.

```
dsmc restore backupset m:\budget\salary.xls
  -backupsetname=c:\budget\weekly_budget_data.ost
  -loc=file -subdir=yes
```

- Sicherungssätze zurückschreiben: Hinweise und Einschränkungen
  In diesem Abschnitt sind einige Hinweise und Einschränkungen aufgeführt, die Sie beim Zurückschreiben von Sicherungssätzen beachten müssen.
-  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme
   Windows-BetriebssystemeSicherungssätze in einer SAN-Umgebung zurückschreiben
  Sie können Sicherungssätze auf folgende Weise in einem Speicherbereichsnetz (SNA) zurückschreiben:
- Restore Backupset ohne Parameter backupsetname
  Der Befehl restore backupset kann ohne den Parameter backupsetname verwendet werden.

Sicherungssätze zurückschreiben: Hinweise und Einschränkungen

In diesem Abschnitt sind einige Hinweise und Einschränkungen aufgeführt, die Sie beim Zurückschreiben von Sicherungssätzen beachten müssen.

Hinweise für das Zurückschreiben von Sicherungssätzen

Beachten Sie beim Zurückschreiben von Sicherungssätzen die folgenden Hinweise:

- Wenn das zurückzuschreibende Objekt auf einem Clientknoten generiert wurde, dessen Name sich von Ihrem aktuellen Knotennamen unterscheidet, geben Sie in allen Zurückschreibungsbefehlen den ursprünglichen Knotennamen im Parameter filespacename an.

- Ist das Zurückschreiben eines Sicherungssatzes von einem austauschbaren Datenträger nicht möglich, ist zusammen mit dem IBM Spectrum Protect-Administrator zu überprüfen, ob der austauschbare Datenträger auf einer Einheit erstellt wurde, auf der ein kompatibles Format verwendet wurde.
- Wenn Sie den Befehl restore backupset in der Anfangsbefehlszeile mit dem Parameter `-location=tape` oder `-location=file` verwenden, versucht der Client nicht, eine Verbindung zum IBM Spectrum Protect-Server herzustellen.
- Beim Zurückschreiben einer Gruppe aus einem Sicherungssatz:
  - Die gesamte Gruppe bzw. alle Gruppen im virtuellen Dateibereich werden zurückgeschrieben. Wenn sich in einem virtuellen Dateibereich mehrere Gruppen befinden, ist es nicht möglich, durch Angabe des Gruppennamens eine einzige Gruppe zurückzuschreiben. Es ist nicht möglich, durch Angabe eines Dateipfads eine Gruppe teilweise zurückzuschreiben.
  - Geben Sie eine Gruppe über einen der folgenden Werte an:
    - Geben Sie den Namen des virtuellen Dateibereichs mit dem Parameter Dateibereichsname an.
    - Verwenden Sie die Option subdir, um Unterverzeichnisse einzuschließen.
- Eine begrenzte Unterstützung wird für das Zurückschreiben von Sicherungssätzen auf Bandeinheiten bereitgestellt, die an das Clientsystem angeschlossen sind. Sie müssen immer einen nativen Einheitentreiber verwenden, der vom Hersteller der Einheit bereitgestellt wird. Der Einheitentreiber, der von IBM für die Verwendung mit dem IBM Spectrum Protect-Server bereitgestellt wird, kann nicht auf dem Clientsystem zum Zurückschreiben lokaler Sicherungssätze benutzt werden.
- Mac OS X-BetriebssysemeAIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssystemeEnthält ein Sicherungssatz Dateien von mehreren Eignern, ist der Sicherungssatz selbst Eigentum der Rootbenutzer-ID und er wird Benutzer-IDs ohne Rootberechtigung nicht angezeigt. In diesem Fall können Benutzer-IDs ohne Rootberechtigung ihre Dateien zurückschreiben, indem sie den Namen des Sicherungssatzes vom IBM Spectrum Protect-Administrator anfordern. Andere Benutzer als Root können nur eigene Dateien zurückschreiben.
- Mac OS X-BetriebssysemeAIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-Betriebssysteme Windows-BetriebssystemeSoll die grafische Benutzerschnittstelle des Clients einen Sicherungssatz von einer lokalen Einheit zurückschreiben, ohne dass eine Serververbindung erforderlich ist, verwenden Sie die Option localbackupset.

Einschränkungen beim Zurückschreiben von Sicherungssätzen

Beachten Sie beim Zurückschreiben von Sicherungssätzen die folgenden Einschränkungen:

- Sicherungssatzdaten, die mit der API gesichert wurden, können weder zurückgeschrieben noch verwendet werden.
- AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeWindows-BetriebssystemeMit dem Befehl restore backupset können Sie keine Imagedaten aus einem Sicherungssatz zurückschreiben. Imagedaten aus einem Sicherungssatz können Sie nur mit dem Befehl restore image zurückschreiben.
- AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeWindows-BetriebssystemeSie können keine Imagedaten aus einem lokalen Sicherungssatz (`location=tape` oder `location=file`) zurückschreiben. Imagedaten aus einem Sicherungssatz können Sie nur vom IBM Spectrum Protect-Server zurückschreiben.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssysemeWindows-Betriebssysteme

Sicherungssätze in einer SAN-Umgebung zurückschreiben

Sie können Sicherungssätze auf folgende Weise in einem Speicherbereichsnetz (SNA) zurückschreiben:

- Befindet sich der Sicherungssatz auf einer an ein SAN angeschlossenen Speichereinheit, geben Sie die Einheit mit dem Parameter *filename* an und verwenden die Option location=*tape*, soweit zutreffend. Der Client für Sichern/Archivieren schreibt den Sicherungssatz direkt von der an das SAN angeschlossenen Speichereinheit zurück und erzielt bei der Zurückschreibung eine hohe Geschwindigkeit. AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssystemeAnmerkung: Sie müssen sicherstellen, dass in dem an das SAN angeschlossenen Bandlaufwerk das korrekte Band geladen ist, bevor Sie den Befehl restore ausgeben. Der Client für Sichern/Archivieren initiiert einen SCSI-Kassettenwechsler nicht dazu, das Band automatisch zu laden.
- Befindet sich der Sicherungssatz nicht auf einem lokalen Datenträger oder auf einer an ein SAN angeschlossenen Speichereinheit, können Sie den Sicherungssatz mit der Option backupsetname angeben. Verwenden Sie die Option location=*server*, um den Sicherungssatz direkt vom Server mithilfe des LAN zurückzuschreiben.

Restore Backupset ohne Parameter backupsetname

Der Befehl restore backupset kann ohne den Parameter backupsetname verwendet werden.

Die bevorzugte Syntax für den Befehl restore backupset erfordert den Parameter backupsetname. Vor der Einführung des Parameters backupsetname hat der Client für Sichern/Archivieren beim Zurückschreiben von Sicherungssätzen eine andere Syntax verwendet. Die vorherige Syntax wird zwar unterstützt, es wird jedoch empfohlen, wann immer möglich die Syntax zu verwenden, die den Parameter backupsetname erfordert. Die vorherige Syntax wird für die Fälle dokumentiert, in denen sie nicht durch die bevorzugte Syntax ersetzt werden kann.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssysemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-REStore Backupset-------------------------------------------->

>--+-------------------------------------------------------+------->
   '-+---------------------+--Quellendateispezifikation-'
     '-{Dateibereichsname}-'

>--+------------------------+--+----------+--------------------->
   '-Zieldateispezifikation-'  '-Optionen-'

>--+-Name des Sicherungssatzes-+--+-----------------------+---><
   +-Name der lokalen Datei----+  '-LOCation=--+-server-+-'
   '-Bandeinheit---------------'               +-file---+
                                               '-tape---'
```

Parameter

Optionen
: Alle Optionen, die für die bevorzugte Syntax von restore backupset gültig sind, sind auch für die vorherige Syntax von restore backupset gültig.

{Dateibereichsname}
: Gibt den in geschweiften Klammern eingeschlossenen Dateibereich auf dem Server an, in dem sich die zurückzuschreibenden Dateien befinden. Dies ist der Name des Workstationlaufwerks, auf dem die Dateien gesichert wurden, oder der Name des virtuellen Dateibereichs für eine Gruppe.

  Geben Sie einen Dateibereichsnamen an, wenn Sie einen Sicherungssatz zurückschreiben, der eine Gruppe enthält.

  Geben Sie einen Dateibereichsnamen an, wenn die *Quellendateispezifikation* auf dem Zielcomputer nicht vorhanden ist. Diese Situation kann eintreten, wenn sich die Laufwerkbezeichnung geändert hat oder wenn Sie Dateien zurückschreiben, die auf einem anderen Knoten gesichert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.

  Windows-BetriebssystemeAnmerkung: Sie müssen einen NTFS- oder ReFS-Dateibereichsnamen in Groß-/Kleinschreibung oder in Kleinschreibung angeben, der zwischen Anführungszeichen und geschweiften Klammern steht. Beispiel: {"NTFSDrive"}. Hochkommas oder Anführungszeichen sind im Schleifenmodus gültig. Beispielsweise ist sowohl {"NTFSDrive"} als auch {'NTFSDrive'} gültig. Im Stapelmodus sind nur Hochkommas gültig. Die Einschränkung auf Hochkommas ist im Betriebssystem begründet.

Quellendateispezifikation
: Gibt den Quellenpfad eines Teils des Sicherungssatzes an. Standardmäßig wird der gesamte Sicherungssatz zurückgeschrieben.

Zieldateispezifikation
: Gibt den Zielpfad für die zurückgeschriebenen Dateien an. Wird keine *Quellendateispezifikation* angegeben, können Sie keine *Zieldateispezifikation* angeben. Wenn Sie kein Ziel angeben, schreibt der Client die Dateien in den ursprünglichen Quellenpfad zurück. Wenn Sie mehrere Dateien zurückschreiben, muss die Dateispezifikation mit einem Verzeichnisbegrenzer (/) enden. Andernfalls geht der Client davon aus, dass der letzte Name ein Dateiname ist, und meldet einen Fehler. Wenn Sie eine einzelne Datei zurückschreiben, kann die Zieldateispezifikation optional mit einem Dateinamen enden, wenn die zurückgeschriebene Datei einen neuen Namen erhalten soll. Ist die *Quellendateispezifikation* auf der Zielworkstation nicht vorhanden, müssen Sie die *Zieldateispezifikation* angeben.

Name des Sicherungssatzes
: Gibt den Namen des Sicherungssatzes auf dem IBM Spectrum Protect-Server an. Wird der Parameter location angegeben, müssen Sie `-location=server` angeben.

Name der lokalen Datei
: Gibt den Dateinamen des ersten Datenträgers des Sicherungssatzes an. Sie müssen `-location=file` angeben.

Bandeinheit
: Gibt den Namen der Bandeinheit an, die den Datenträger des Sicherungssatzes enthält. Sie müssen einen von Windows bereitgestellten Einheitentreiber und nicht den von IBM bereitgestellten Einheitentreiber verwenden. Sie müssen `-location=tape` angeben.

LOCation=
: Gibt die Position des Sicherungssatzes an. Wenn Sie den Parameter location nicht angeben, sucht der Client auf dem IBM Spectrum Protect-Server nach Sicherungssätzen. Wenn Sie den Parameter 'location' angeben, muss der Wert einer der folgenden drei Auswahlmöglichkeiten entsprechen.

  server
  : Gibt an, dass der Sicherungssatz sich auf dem Server befindet. Server ist die Standardposition.

  file
  : Gibt an, dass der Sicherungssatz sich auf einem verfügbaren Dateisystem befindet.

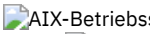
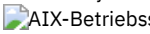
  tape
  : Gibt an, dass der Sicherungssatz sich auf einer verfügbaren Bandeinheit befindet.

Beispiele

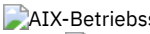
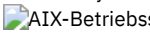
Task

Den gesamten Sicherungssatz mit dem Namen `monthly_financial_data.87654321` vom Server zurückschreiben.

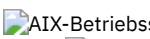
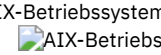
```
dsmc restore backupset monthly_financial_data.87654321 -loc=server
```


Task

Den gesamten Sicherungssatz zurückschreiben, der in der Datei `/home/budget/weekly_budget_data.ost` enthalten ist.

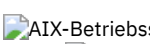
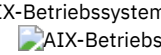
```
dsmc restore backupset "/home/budget/weekly_budget_data.ost" -loc=file
```


Task

Den gesamten Sicherungssatz von der Einheit `/dev/rmt0` zurückschreiben.

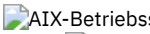
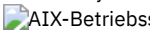
```
dsmc restore backupset "/dev/rmt0" -loc=tape
```


Task

Die einzelne Datei mit dem Namen `/home/jones/budget.dev` von der Einheit `/dev/rmt0` in den ursprünglichen Quellenpfad zurückschreiben.

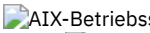
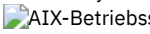
```
dsmc restore backupset /dev/rmt0 "/home/jones/budget.dev" -loc=tape
```


Task

Alle Dateien im Verzeichnis budget mit der Dateierweiterung `.txt` von dem Band/den Bändern auf der Einheit `/dev/rmt0` in den ursprünglichen Quellenpfad zurückschreiben.

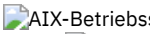
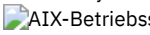
```
dsmc restore backupset /dev/rmt0 "/home/budget/*.txt" -loc=tape
```


Task

Den gesamten Sicherungssatz zurückschreiben, der in der lokalen Datei "`/home/jones/bset01.file`" enthalten ist.

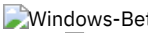
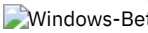
```
dsmc restore backupset "/home/jones/bset01.file" -loc=file
```


Task

Gruppen aus dem Sicherungssatz `mybackupset.12345678` auf dem IBM Spectrum Protect-Server in das Verzeichnis `/home/devel/projectb` zurückschreiben. Der virtuelle Dateibereich der Gruppen ist `accounting`.

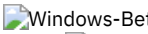
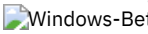
```
dsmc restore backupset mybackupset.12345678 {/accounting}/* /home/devel/projectb/ -loc=server -subdir=yes
```


Task

Gruppen aus dem lokalen Sicherungssatz `mybackupset.ost` in das Verzeichnis `/home/devel/projectb/` zurückschreiben. Der virtuelle Dateibereich der Gruppen ist `accounting`.

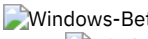
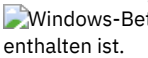
```
dsmc restore backupset mybackupset.ost {/accounting}/* /home/devel/projectb/ -loc=server -subdir=yes
```


Task

Den gesamten Sicherungssatz von der Einheit `\\.\tape0` zurückschreiben.

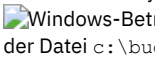
```
dsmc restore backupset \\.\tape0 -loc=tape
```


Task

Gruppen aus dem Sicherungssatz `mybackupset.12345678` auf dem IBM Spectrum Protect-Server in das Verzeichnis `c:\newdevel\projectn` zurückschreiben. Der virtuelle Dateibereich der Gruppen ist `accounting`.

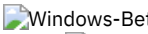
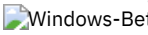
```
dsmc restore backupset mybackupset.12345678 {accounting}\* c:\newdevel\projectn\ -loc=server -subdir=yes
```


Task

Den gesamten Sicherungssatz zurückschreiben, der in der Datei `c:\budget\weekly_budget_data.ost` enthalten ist.

```
dsmc restore backupset c:\budget\weekly_budget_data.ost -loc=file
```


Task

Das Verzeichnis `\budget\` und seine Unterverzeichnisse aus dem Sicherungssatz zurückschreiben, der in der Datei `c:\budget\weekly_budget_data.ost` enthalten ist.

```
dsmc restore backupset c:\budget\weekly_budget_data.ost m:\budget\* -loc=file -subdir=yes
```


Task

Die Datei `\budget\salary.xls` aus dem Sicherungssatz zurückschreiben, der in der Datei `c:\budget\weekly_budget_data.ost` enthalten ist.

```
dsmc restore backupset c:\budget\weekly_budget_data.ost m:\budget\salary.xls -loc=file -subdir=yes
```

Restore Group

Verwenden Sie den Befehl restore group, um bestimmte Member oder alle Member einer Gruppensicherung zurückzuschreiben.

Anmerkung:

1. Verwenden Sie die Option pick, um eine Liste der Gruppen anzuzeigen, aus der Sie eine zurückzuschreibende Gruppe auswählen können.
2. Verwenden Sie die Option showmembers in Verbindung mit der Option pick, um einzelne oder mehrere Member einer Gruppe anzuzeigen und zurückzuschreiben. In diesem Fall wählen Sie zunächst die Gruppe aus, von der Sie Member zurückschreiben wollen, und anschließend wählen Sie ein oder mehrere Member der Gruppe aus, die zurückgeschrieben werden sollen.
3. Sie können eine Gruppe aus einem Sicherungssatz zurückschreiben.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDieser Befehl ist für alle Clients außer Mac OS X gültig.

 Windows-BetriebssystemeDieser Befehl ist für alle Clients gültig.

Syntax

```
>>-REStore GRoup--+----------+----Quelle----+------+-----------><
                  '-Optionen-'               '-Ziel-'
```

Parameter

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeQuelle
 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeGibt den Namen des virtuellen Dateibereichs und den Gruppennamen auf dem Server für die Zurückschreibung an.

 Windows-BetriebssystemeQuelle
 Windows-BetriebssystemeGibt den Namen des virtuellen Dateibereichs (zwischen geschweiften Klammern) und den Namen der Gruppe auf dem Server an, die zurückgeschrieben werden soll.

Ziel
Gibt den Pfad für das Ziel der Gruppe bzw. eines oder mehrerer Mitglieder der Gruppe an. Wenn kein Ziel angegeben wird, schreibt der Client die Dateien an die ursprüngliche Position zurück.

Tabelle 1. Befehl Restore Group: Zugehörige Optionen

Option	Verwendung
backupsetname	Nur in der Befehlszeile.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme followsymbolic	 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.
fromdate	Nur in der Befehlszeile.
fromnode	Nur in der Befehlszeile.
 AIX-Betriebssysteme Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssystemefromowner	 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeNur in der Befehlszeile.
fromtime	Nur in der Befehlszeile.
ifnewer	Nur in der Befehlszeile.
inactive	Nur in der Befehlszeile.
latest	Nur in der Befehlszeile.
pick	Nur in der Befehlszeile.
pitdate	Nur in der Befehlszeile.
pittime	Nur in der Befehlszeile.
preservepath	Nur in der Befehlszeile.
 Windows-Betriebssystemereplace	 Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.

Option	Verwendung
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssystemereplace	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Clientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemeshowmembers	Windows-BetriebssystemeNur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme showmembers (gilt nicht für Mac OS X)	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssysteme skipntpermissions	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme skipntsecuritycrc	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemesubdir	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssystemesubdir	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemetapeprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme tapeprompt	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate	Nur in der Befehlszeile.
totime	Nur in der Befehlszeile.

Beispiele

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeAlle Member der Gruppensicherung `/virtfs/group1` an ihre ursprüngliche Position auf dem Clientsystem zurückschreiben.

Befehl:

```
restore group /virtfs/group1
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Member der Gruppensicherung `virtfs\group1` an ihre ursprüngliche Position auf dem Clientsystem zurückschreiben.

Befehl:

```
restore group {virtfs}\group1
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeAlle Gruppen im virtuellen Dateibereich `/virtfs` anzeigen. Die Option showmembers verwenden, um eine Liste der Gruppenmember anzuzeigen, aus der Sie zurückzuschreibende Member auswählen können.

Befehl:

```
restore group /virtfs/
  * -pick -showmembers
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Gruppen im virtuellen Dateibereich `virtfs` anzeigen. Die Option showmembers verwenden, um eine Liste der Gruppenmember anzuzeigen, aus der Sie zurückzuschreibende Member auswählen können.

Befehl:

```
restore group {virtfs}\
  * -pick -showmembers
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeEine Liste der Gruppen im virtuellen Dateibereich `/virtfs` anzeigen, aus der Sie eine oder mehrere zurückzuschreibende Gruppen auswählen können.

Befehl:

```
restore group /virtfs/* -pick
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine Liste der Gruppen im virtuellen Dateibereich `virtfs` auswählen, aus der Sie eine oder mehrere zurückzuschreibende Gruppen auswählen können.

Befehl:

```
restore group {virtfs}\* -pick
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Restore Image

Mit dem Befehl restore image wird ein Dateisystemimage oder das Image eines unformatierten Datenträgers zurückgeschrieben, das mithilfe des Befehls backup image gesichert wurde.

Bei der Zurückschreibung wird das Sicherungsimage vom IBM Spectrum Protect-Server oder aus einem Sicherungssatz vom IBM Spectrum Protect-Server abgerufen, wenn die Option backupsetname angegeben ist. Dieser Befehl kann ein aktives Basisimage oder ein zeitpunktgesteuertes Basisimage mit zugeordneten Teilaktualisierungen zurückschreiben.

Anmerkung:

1. Windows-BetriebssystemeDas Konto, das den Client für Sichern/Archivieren ausführt, muss über Administratorberechtigung verfügen, damit Imagezurückschreibungen erfolgreich ausgeführt werden können.
2. AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDie Verwendung der Option incremental im Befehl restore image zur Ausführung einer dynamischen Imagesicherung wird nicht unterstützt.
3. Wenn Sie IBM Spectrum Protect HSM for Windows oder IBM Spectrum Protect for Space Management verwenden, eine Dateisystemimagesicherung zurückschreiben und die Ausführung eines Abgleichs planen, müssen Sie die Dateien zurückschreiben, die nach der Imagesicherung gesichert wurden. Andernfalls verfallen umgelagerte Dateien, die nach der Imagesicherung erstellt wurden, im HSM-Archivierungsspeicher auf dem IBM Spectrum Protect-Server.

Sie können mit der Option verifyimage im Befehl restore image angeben, dass die Feststellung von defekten Sektoren auf dem Zieldatenträger aktiviert werden soll. Werden defekte Sektoren auf dem Zieldatenträger festgestellt, gibt der Client eine Warnung auf der Konsole und im Fehlerprotokoll aus.

Befinden sich defekte Sektoren auf dem Zieldatenträger, können Sie die Option imagetofile im Befehl restore image verwenden, um anzugeben, dass das Quellenimage in eine Datei zurückgeschrieben werden soll. Später können Sie ein Datenkopierprogramm Ihrer Wahl verwenden, um das Image von der Datei auf einen Plattendatenträger zu übertragen.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeHinweise:

- Die API muss installiert sein, um den Befehl restore image verwenden zu können.
- Oracle Solaris-BetriebssystemeDie Imagezurückschreibung wird für das Sun-Dateisystem QFS nicht unterstützt.
- Linux-BetriebssystemeDie Imagezurückschreibung wird für GPFS-Dateisysteme unter Linux x86_64, Linux on POWER und Linux on System z nicht unterstützt.
- Linux-BetriebssystemeAuf Linux-Systemen verwenden einige Dateisysteme (z. B. ext2, ext3, ext4, btrfs und xfs) eine UUID (Universally Unique Identifier), um sich selbst im Betriebssystem zu identifizieren. Wenn Sie eine Imagesicherung eines solchen Datenträgers erstellen und an eine andere Position zurückschreiben, kann es sein, dass es zwei Datenträger mit derselben UUID gibt. Wenn Sie Ihre Dateisysteme mit einer UUID in /etc/fstab definieren, denken Sie daran, dass der Client für Sichern/Archivieren das zurückgeschriebene Dateisystem unter Umständen wegen eines UUID-Konflikts nicht korrekt anhängen kann. Um diese Situation zu vermeiden, sollten Sie das Image an seine ursprüngliche Position zurückschreiben. Wenn Sie es an eine andere Position zurückschreiben müssen, ändern Sie die UUID des ursprünglichen oder des zurückgeschriebenen Datenträgers, bevor Sie das zurückgeschriebene Dateisystem anhängen. Informationen zur Änderung einer UUID finden Sie in der Linux-Dokumentation. Möglicherweise müssen Sie auch die Datei /etc/fstab manuell bearbeiten, damit der ursprüngliche Datenträger und/oder der zurückgeschriebene Datenträger angehängt werden können.
- Wenn Sie die Option pick verwenden, werden die folgenden Informationen für Dateisystemimages angezeigt, die vom Client gesichert wurden:
  - Imagegröße
  - Gespeicherte Größe - Dieser Wert ist die tatsächliche Größe des Images, das auf dem IBM Spectrum Protect-Server gespeichert ist. Das auf dem Server gespeicherte Image hat dieselbe Größe wie der Datenträger.
  - Dateisystemtyp
  - Sicherungsdatum und -zeit
  - Die den Imagesicherungen zugeordnete Verwaltungsklasse
  - Ob die Imagesicherung eine aktive oder inaktive Kopie ist
  - Der Imagename
- Sollte ein zurückgeschriebenes Image aus irgendeinem Grund beschädigt sein, können Sie versuchen, es mit dem Tool fsck zu reparieren.

Windows-BetriebssystemeHinweise:

- Die IBM Spectrum Protect-API muss installiert sein, um den Befehl restore image verwenden zu können.
- Sie können ein NTFS- oder ReFS-Dateisystem auf einen FAT32-Datenträger zurückschreiben und umgekehrt.
- Der Zieldatenträger, auf den Sie zurückschreiben, muss vorhanden und mindestens so groß wie der Ausgangsdatenträger sein.
- Der physische Aufbau des Zieldatenträgers (einheitenübergreifend, gespiegelt) kann abweichen.
- Der Zieldatenträger wird mit den in der Imagesicherung enthaltenen Daten überschrieben.

- Sie müssen einen Zieldatenträger nicht formatieren, bevor Sie eine Imagesicherung zurückschreiben, die ein Dateisystem enthält.
- Der Client erfordert eine exklusive Sperre des Zieldatenträgers, auf den Sie zurückschreiben. Bei einer Zurückschreibungsoperation wird der Datenträger vom Client gesperrt, zurückgeschrieben, entsperrt, abgehängt und angehängt. Während des Zurückschreibungsprozesses ist der Zieldatenträger nicht für andere Anwendungen verfügbar.
- Wenn Sie die Option pick verwenden, werden die folgenden Informationen für vom Client gesicherte Dateisystemimages angezeigt:
  - Imagegröße
  - Gespeicherte Größe - Dieser Wert ist die tatsächliche Größe des Images, das auf dem Server gespeichert wurde. Die Option imagegapsize kann definiert werden, damit nur verwendete Blöcke in einem Dateisystem gesichert werden. Daher kann die Größe des auf dem Server gespeicherten Images kleiner als die Datenträgergröße sein. Bei Online-Imagesicherungen kann das gespeicherte Image aufgrund der Größe der Cachedateien größer als das Dateisystem sein.
  - Dateisystemtyp
  - Sicherungsdatum und -zeit
  - Die der Imagesicherung zugeordnete Verwaltungsklasse
  - Ob die Imagesicherung eine aktive oder inaktive Kopie ist
  - Der Imagename
- Falls ein zurückgeschriebenes Image beschädigt ist, verwenden Sie das Dienstprogramm chkdsk, um nach defekten Sektoren zu suchen und diese zu reparieren (sofern der zurückgeschriebene Datenträger nicht unformatiert (RAW) ist).

Unterstützte Clients

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeDiese Option ist für AIX-, Linux- und Oracle Solaris-Clients gültig.

 Windows-BetriebssystemeDieser Befehl ist für alle Windows-Clients gültig.

Syntax

```
>>-REStore Image--+-------------+------------------------------->
                  '- --Optionen-'

>--+- --Quellendateispezifikation---+--------------------------->
   '- --"Quellendateispezifikation"-'

>--+----------------------------+------------------------------><
   '- --Zieldateispezifikation-'
```

Parameter

Quellendateispezifikation
: Der Name eines Quellenimagedateisystems, das zurückgeschrieben werden soll. Es kann nur ein einzelnes Quellenimage angegeben werden. Platzhalterzeichen sind nicht zulässig.

AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeZieldateispezifikation
: AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeGibt den Namen eines vorhandenen angehängten Dateisystems oder den Pfad und Dateinamen an, in das/den das Quellendateisystem zurückgeschrieben wird. Standardwert ist die ursprüngliche Position des Dateisystems.

 Windows-BetriebssystemeZieldateispezifikation
:  Windows-BetriebssystemeGibt den Namen eines vorhandenen angehängten Dateisystems oder den Pfad und Dateinamen an, in das/den das Quellendateisystem zurückgeschrieben wird. Standardwert ist die ursprüngliche Position des Dateisystems. Sie können ein NTFS- oder ReFS-Dateisystem auf einen FAT32-Datenträger zurückschreiben und umgekehrt.

Tabelle 1. Befehl Restore Image: Zugehörige Optionen

Option	Verwendung
backupsetname	Nur in der Befehlszeile.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme dateformat	 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
 Windows-Betriebssystemedateformat	 Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
deletefiles	Nur in der Befehlszeile.
fromnode	Nur in der Befehlszeile.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme fromowner	 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-BetriebssystemeNur in der Befehlszeile.

Option	Verwendung
imagetofile	Nur in der Befehlszeile.
inactive	Nur in der Befehlszeile.
incremental	Nur in der Befehlszeile.
noprompt	Nur in der Befehlszeile.
pick	Nur in der Befehlszeile.
pitdate	Nur in der Befehlszeile.
pittime	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme timeformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Clientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemetimeformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
verifyimage	Nur in der Befehlszeile.

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDurch den Befehl restore image wird der Zieldateibereich nicht definiert oder angehängt. Der Zieldatenträger muss vorhanden und groß genug für die Quelle sein und wenn er ein Dateisystem enthält, muss er angehängt sein. Wenn eine Imagesicherung ein Dateisystem enthält und an eine andere Position zurückgeschrieben wird, müssen folgende Punkte beachtet werden:

Windows-BetriebssystemeDurch den Befehl restore image wird der Zieldateibereich nicht definiert oder angehängt. Der Zieldatenträger muss vorhanden und groß genug für die Quelle sein und wenn er ein Dateisystem enthält, muss er angehängt sein. Der Zieldatenträger muss einem Laufwerkbuchstaben zugeordnet sein. Wenn eine Imagesicherung ein Dateisystem enthält und an eine andere Position zurückgeschrieben wird, müssen folgende Punkte beachtet werden:

- Ist der Zieldatenträger kleiner als der Quellendatenträger, schlägt die Operation fehl.
- AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeWenn der Zieldatenträger größer als die Quelle ist, geht die Größendifferenz nach der Zurückschreibungsoperation verloren. Der verlorene Speicherbereich kann durch Vergrößern des Datenträgers wiederhergestellt werden, wodurch sich auch der zurückgeschriebene Datenträger vergrößert.
- Windows-BetriebssystemeWenn der Zieldatenträger größer als die Quelle ist, geht die Größendifferenz nach der Zurückschreibungsoperation verloren. Befindet sich der Zieldatenträger auf einer dynamischen Platte, kann der verlorene Speicherbereich durch Vergrößern des Datenträgers wiederhergestellt werden. Die Vergrößerung des Datenträgers bewirkt, dass sich auch der zurückgeschriebene Datenträger vergrößert.

Beispiele

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeTask
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDas Verzeichnis `/home/test`, über das der logische Datenträger angehängt wird, an seine ursprüngliche Position zurückschreiben.

Befehl: `dsmc rest image /home/test`

Windows-BetriebssystemeTask
Windows-BetriebssystemeDas Laufwerk `e:` an seine ursprüngliche Position zurückschreiben.

Befehl: `dsmc rest image e:`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeTask
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDas Verzeichnis `/home/proj`, über das der logische Datenträger angehängt wird, an seine ursprüngliche Position zurückschreiben und die auf dem Server aufgezeichneten Änderungen aus der letzten Teilsicherung des ursprünglichen Images anwenden. Die Änderungen schließen das Löschen von Dateien ein.

Befehl: `dsmc restore image /home/proj -incremental -deletefiles`

Windows-BetriebssystemeTask
Windows-BetriebssystemeDas Laufwerk `h:` an seine ursprüngliche Position zurückschreiben und die auf dem Server aufgezeichneten Änderungen aus der letzten Teilsicherung des ursprünglichen Images anwenden. Die Änderungen schließen das Löschen von Dateien ein.

Befehl: `dsmc restore image h: -incremental -deletefiles`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeTask
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-BetriebssystemeDas Dateisystem `/usr` an seine ursprüngliche Position zurückschreiben. Verwenden Sie die Option verifyimage, um die Feststellung von defekten Sektoren auf dem Zieldatenträger zu aktivieren.

Befehl: `dsmc restore image /usr -verifyimage`

Windows-BetriebssystemeTask

Windows-BetriebssystemeDas Laufwerk `d:` an seine ursprüngliche Position zurückschreiben. Verwenden Sie die Option verifyimage, um die Feststellung von defekten Sektoren auf dem Zieldatenträger zu aktivieren.

Befehl: `dsmc restore image d: -verifyimage`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeSind defekte Sektoren auf dem Zieldatenträger vorhanden, die Option imagetofile verwenden, um das Dateisystem `/usr` in die Datei `/home/usr.img` zurückzuschreiben, sodass Datenverlust vermieden wird.

Befehl: `dsmc restore image /usr /home/usr.img -imagetofile`

Windows-BetriebssystemeTask

Windows-BetriebssystemeSind defekte Sektoren auf dem Zieldatenträger vorhanden, die Option imagetofile verwenden, um das Laufwerk `d:` in die Datei `e:\diskD.img` zurückzuschreiben, sodass Datenverlust vermieden wird.

Befehl: `dsmc restore image d: e:\diskD.img -imagetofile`

Windows-BetriebssystemeTask

Windows-BetriebssystemeDas Laufwerk `e:` aus dem Sicherungssatz `weekly_backup_data.12345678` an seine ursprüngliche Position zurückschreiben.

Befehl: `restore image e: -backupsetname=weekly_backup_data.12345678`

AIX-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme

Restore NAS

Mit dem Befehl restore nas wird das Image eines Dateisystems zurückgeschrieben, das zu einem NAS-Dateiserver gehört. Wenn Sie eine interaktive Befehlszeilensitzung mit einer ID ohne Verwaltungsberechtigung verwenden, werden Sie zur Eingabe einer Administrator-ID aufgefordert.

Der NAS-Dateiserver führt die Gerätedatenversetzung aus. Ein Serverprozess führt die Zurückschreibung durch.

Wenn Sie die Option toc im Befehl backup nas oder mit der Option include.fs.nas verwendet haben, um Inhaltsverzeichnisinformationen (TOC-Informationen) für jede Dateisystemsicherung zu speichern, können Sie über den Serverbefehl QUERY TOC den Inhalt einer Dateisystemsicherung ermitteln und über den Serverbefehl RESTORE NODE einzelne Dateien oder Verzeichnisstrukturen zurückschreiben. Sie können auch den Web-Client verwenden, um die gesamte Baumstruktur des Dateisystems zu untersuchen und zurückzuschreibende Dateien und Verzeichnisse auszuwählen. Werden keine TOC-Informationen gespeichert, können Sie über den Befehl RESTORE NODE dennoch einzelne Dateien und Verzeichnisstrukturen zurückschreiben, wenn Ihnen der vollständig qualifizierte Name jeder Datei bzw. jedes Verzeichnisses und des Image bekannt ist, in dem das Objekt gesichert wurde.

AIX-BetriebssystemeOracle Solaris-BetriebssystemeVerwenden Sie die Option nasnodename, um den Knotennamen für den NAS-Dateiserver anzugeben. Der NAS-Knotenname identifiziert den NAS-Dateiserver für den IBM Spectrum Protect-Server. Sie müssen den NAS-Knotennamen im Server registrieren. Fügen Sie die Option nasnodename in Ihre Clientsystemoptionsdatei (dsm.sys) ein. Der Wert in der Clientsystemoptionsdatei ist der Standardwert, dieser Wert kann jedoch in der Befehlszeile überschrieben werden.

Windows-BetriebssystemeVerwenden Sie die Option nasnodename, um den Knotennamen für den NAS-Dateiserver anzugeben. Der NAS-Knotenname identifiziert den NAS-Dateiserver für den IBM Spectrum Protect-Server. Sie müssen den NAS-Knotennamen im Server registrieren. Fügen Sie die Option nasnodename in Ihre Clientoptionsdatei (dsm.opt) ein. Der Wert in der Clientoptionsdatei ist der Standardwert, dieser Wert kann jedoch in der Befehlszeile überschrieben werden.

Sie können mit der Option pick eine Liste der NAS-Images anzeigen, deren Eigner der angegebene NAS-Knoten ist. In dieser Liste können Sie Images zum Zurückschreiben auswählen. Wenn Sie mit der Option pick mehrere Images zum Zurückschreiben auswählen, dürfen Sie nicht die Option monitor verwenden; sonst werden die Zurückschreibungen serialisiert. Wenn Sie beim Zurückschreiben mehrerer Images mehrere Zurückschreibungsprozesse gleichzeitig starten wollen, dürfen Sie nicht monitor=`yes` angeben.

Mit der Option monitor geben Sie an, ob Sie eine NAS-Imagezurückschreibung eines Dateisystems überwachen und Verarbeitungsinformationen anzeigen wollen.

Mit dem Befehl monitor process können Sie eine Liste der aktuellen Zurückschreibungsprozesse für alle NAS-Knoten anzeigen, für die Ihre Verwaltungsbenutzer-ID eine Berechtigung hat. Die Verwaltungsbenutzer-ID sollte mindestens die Clienteignerberechtigung sowohl über den NAS-Knoten als auch den Client-Workstation-Knoten besitzen, der entweder von der Befehlszeile oder vom Web aus verwendet wird.

Mit dem Befehl cancel process können Sie die NAS-Zurückschreibungsverarbeitung stoppen.

AIX-BetriebssystemeOracle Solaris-BetriebssystemeUnabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: `/vol/vol0`.

Windows-BetriebssystemeFür eine NAS-Dateisystemspezifikation werden folgende Konventionen verwendet:

- Unabhängig von der Clientplattform wird in NAS-Dateisystemspezifikationen der Schrägstrich (/) als Trennzeichen verwendet. Zum Beispiel: /vol/vol0.
- Für NAS-Dateisystembezeichnungen in der Befehlszeile müssen geschweifte Klammern {} als Begrenzer um Dateisystemnamen verwendet werden. Zum Beispiel: {/vol/vol0}.

 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme  Windows-Betriebssysteme

Unterstützte Clients

 AIX-Betriebssysteme  Oracle Solaris-BetriebssystemeDieser Befehl ist nur für AIX- und Solaris-Clients gültig.

 Windows-BetriebssystemeDieser Befehl ist für alle Windows-Clients gültig.

Syntax

```
>>-REStore NAS--+-------------+--------------------------------->
                '- --Optionen-'

>---- --Quellendateispezifikation------------------------------->

>--+---------------------------+-------------------------------><
   '- --Zieldateispezifikation-'
```

Parameter

Quellendateispezifikation
: Gibt den Namen des NAS-Dateisystemimages an, das Sie zurückschreiben wollen. Dieser Parameter ist erforderlich, wenn Sie nicht die Option pick verwenden, um eine Liste der NAS-Images zur Auswahl anzuzeigen. Sie können keine Platzhalterzeichen verwenden, wenn Sie die Quellendateispezifikation angeben.

Zieldateispezifikation
: Gibt den Namen eines vorhandenen angehängten Dateisystems auf der NAS-Einheit an, über das das Image zurückgeschrieben werden soll. Dieser Parameter ist optional. Standardwert ist die ursprüngliche Position des Dateisystems auf der NAS-Einheit.

Tabelle 1. Befehl Restore NAS: Zugehörige Optionen

Option	Verwendung
 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme dateformat	AIX-BetriebssystemeOracle Solaris-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
 Windows-Betriebssystemedateformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
inactive	Nur in der Befehlszeile.
mode	Nur in der Befehlszeile.
monitor	Nur in der Befehlszeile.
 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme nasnodename	AIX-BetriebssystemeOracle Solaris-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
 Windows-Betriebssysteme nasnodename	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme numberformat	AIX-BetriebssystemeOracle Solaris-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
 Windows-Betriebssysteme numberformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
pick	Nur in der Befehlszeile.
pitdate	Nur in der Befehlszeile.
pittime	Nur in der Befehlszeile.
 AIX-Betriebssysteme  Oracle Solaris-Betriebssysteme timeformat	AIX-BetriebssystemeOracle Solaris-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
 Windows-Betriebssystemetimeformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

AIX-BetriebssystemeOracle Solaris-BetriebssystemeTask
AIX-BetriebssystemeOracle Solaris-BetriebssystemeDas NAS-Dateisystemimage /vol/vol1 in das Dateisystem /vol/vol2 auf dem NAS-Dateiserver `nas1` zurückschreiben.

Befehl: `restore nas -nasnodename=nas1 /vol/vol1 /vol/vol2`

Windows-BetriebssystemeTask
Windows-BetriebssystemeDas NAS-Dateisystemimage /vol/vol1 in das Dateisystem /vol/vol2 auf dem NAS-Dateiserver `nas1` zurückschreiben.

Befehl: `restore nas -nasnodename=nas1 {/vol/vol1} {/vol/vol2}`

Task
Inaktive NAS-Images zurückschreiben.

Befehl: `restore nas -nasnodename=nas2 -pick -inactive`

Windows-Betriebssysteme

Restore Systemstate

Der Befehl restore systemstate ist für Onlinezurückschreibungsoperationen des Systemstatus veraltet.

Einschränkung:
Es ist nicht mehr möglich, den Systemstatus auf ein System zurückzuschreiben, das noch online ist. Verwenden Sie stattdessen die ASR-basierte Wiederherstellungsmethode zum Zurückschreiben des Systemstatus im Windows PE-Offlinemodus. Weitere Informationen finden Sie in den folgenden Wiki-Artikeln von IBM Spectrum Protect:

- Best Practices for Recovering Windows Server 2012 and Windows 8
- Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1

Wenn Sie versuchen, den Systemstatus mit dem Befehl dsmc restore systemstate über die GUI des Clients für Sichern/Archivieren oder den Web-Client zurückzuschreiben, wird die folgende Nachricht angezeigt:

```
ANS5189E Die Onlinezurückschreibung des Systemstatus ist veraltet. Verwenden Sie die
    Offline-WinPE-Methode für die Ausführung der Zurückschreibung des Systemstatus.
```

Linux-BetriebssystemeWindows-Betriebssysteme

Restore VM

Mit dem Befehl restore vm können Sie eine virtuelle Maschine zurückschreiben, die zuvor gesichert wurde.

Windows-Betriebssysteme
Mit dem Befehl restore VM können sowohl virtuelle Microsoft Hyper-V-Maschinen als auch virtuelle VMware-Maschinen zurückgeschrieben werden. Die Informationen für jeden Zurückschreibungstyp werden in einem eigenen Abschnitt bereitgestellt. Wenn Sie eine virtuelle Maschine zurückschreiben, die Teil einer Hyper-V-Konfiguration ist, können Sie den Text *Restore VM für virtuelle VMware-Maschinen* überspringen. Wenn Sie eine virtuelle VMware-Maschine zurückschreiben, müssen Sie den Text *Restore VM für virtuelle Hyper-V-Maschinen* nicht lesen.

Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments ausgeführt wird.

Linux-BetriebssystemeWindows-Betriebssysteme

Restore VM für virtuelle VMware-Maschinen

Mit dem Befehl Restore VM können Sie virtuelle VMware-Maschinen oder Schablonen virtueller VMware-Maschinen zurückschreiben.

Wenn der Client für Sichern/Archivieren auf einem separaten System installiert ist, das als vStorage-Sicherungsserver konfiguriert ist, können Sie vollständige Sicherungen virtueller Maschinen auf den ESX- oder ESXi-Server zurückschreiben, von dem sie stammen, oder auf einen anderen Server. Soll eine vollständige Sicherung einer virtuellen Maschine auf einen anderen Server zurückgeschrieben werden, verwenden Sie die Option -host. Der Client für Sichern/Archivieren kopiert die Daten vom IBM Spectrum Protect-Server über das LAN oder das SAN. Der Client schreibt die Daten dann direkt auf den ESX-Server, indem die in der Clientoptionsdatei angegebene Transportmethode verwendet wird.

Bei der Zurückschreibung einer vollständigen Sicherung einer virtuellen Maschine wird eine neue virtuelle Maschine erstellt. Die Konfigurationsinformationen und der Inhalt der neuen Maschine sind mit den Konfigurationsinformationen und dem Inhalt zum Zeitpunkt der Sicherung identisch. Alle Platten der virtuellen Maschine werden bis zum angegebenen Zeitpunkt als virtuelle Platten in der neu erstellten virtuellen Maschine zurückgeschrieben.

Wenn Sie eine bestimmte Platte mit der :vmdk=-Syntax zurückschreiben, wird eine vorhandene virtuelle Maschine mit den Daten der angegebenen virtuellen Platten aktualisiert. Nur die angegebenen Platten werden auf die vorhandene virtuelle Maschine zurückgeschrieben;

andere Platten in der virtuellen Maschine werden nicht geändert. Die vorhandene virtuelle Maschine, auf die die Platte zurückgeschrieben wird, muss ausgeschaltet werden, bevor Sie die Zurückschreibungsoperation einleiten.

Um eine neue virtuelle Maschine zu erstellen, geben Sie den Parameter -vmname und einen Namen für die neue virtuelle Maschine an. Mit dem Parameter -vmname wird eine neue virtuelle Maschine mit einer Konfiguration erstellt, die mit der Konfiguration zum Zeitpunkt der Sicherung identisch ist. Wird auch die :vmdk=-Syntax angegeben, werden Daten auf alle Platten zurückgeschrieben, die in den Parametern :vmdk= enthalten sind; Platten, die nicht eingeschlossen sind, werden zwar zurückgeschrieben, aber nur als unformatierte Platten, die keine Daten enthalten.

Virtuelle Maschinen werden in ihren ursprünglichen Ressourcenpool, Cluster oder Ordner zurückgeschrieben, wenn die Container vorhanden sind. Wenn während einer Zurückschreibungsoperation das Ziel (vCenter- oder ESXi-Host) die erforderlichen Container nicht aufweist, wird die virtuelle Maschine in die Standardposition auf der höchsten Ebene auf dem ESXi-Zielhost zurückgeschrieben. Wenn Sie eine virtuelle Maschine mithilfe des Befehlszeilenclients zurückschreiben und wenn die virtuelle Maschine nicht an ihre ursprüngliche Position zurückgeschrieben werden kann, wird eine Informationsnachricht (ANS2091I) angezeigt. Wenn Sie eine virtuelle Maschine mithilfe der Java™-GUI zurückschreiben und wenn die virtuelle Maschine nicht an ihre ursprüngliche Position zurückgeschrieben werden kann, wird die Informationsnachricht nicht angezeigt. Die virtuelle Maschine wird jedoch trotzdem in die Standardposition auf der höchsten Ebene zurückgeschrieben.

Datenschutztags, die mit dem Befehl backup vm gesichert wurden, werden mit der virtuellen Maschine zurückgeschrieben. Datenschutztags werden verwendet, um virtuelle Maschinen von Sicherungen auszuschließen und die Aufbewahrungsmaßnahme für Sicherungen anzugeben.

 Windows-BetriebssystemeGesamtsicherungen virtueller Maschinen, die zuvor mit VMware Consolidated Backup (VCB) erstellt wurden, können dennoch zurückgeschrieben werden, indem die ursprünglichen VCB-Zurückschreibungsschritte verwendet werden. Informationen zum Zurückschreiben von Gesamtsicherungen virtueller Maschinen, die mit VCB erstellt wurden, finden Sie in Mit VMware Consolidated Backup erstellte vollständige VM-Sicherungen zurückschreiben. Wenn Sie eine virtuelle Maschine mit VCB zurückschreiben, versetzen Sie die zurückgeschriebenen Dateien mit dem VMware-Konvertierungsprogramm auf dem Client in einen aktiven Status auf einem VMware-Server. Wenn der Client für Sichern/Archivieren auf einer virtuellen Maschine ausgeführt wird und Sie eine Sicherung der Dateien der virtuellen Maschine auf Dateiebene mit dem Client der Version 7.1 oder früher ausgeführt hatten, können Sie die Sicherungsversionen mithilfe der Befehlszeilenschnittstelle oder der Java-GUI auf die virtuelle Maschine zurückschreiben.

Unterstützte Clients

 Linux-BetriebssystemeDieser Befehl ist auf unterstützten Linux-Clients gültig, die auf einem vStorage-Sicherungsserver für eine virtuelle VMware-Maschine installiert sind.

 Windows-BetriebssystemeDieser Befehl ist auf unterstützten Windows-Clients gültig, die auf einem vStorage-Sicherungsserver für eine virtuelle VMware-Maschine installiert sind.

Syntax

```
>>-REStore VM--VM-Quellenspezifikation-------------------------->

   .-----------------------------.
   V .-:vmdk=all-vmdk---------. |
>----+-------------------------+-+------------------------------>
     +-:vmdk=cnfg-------------+
     +-:vmdk=Plattenkennsatz--+
     '-:-vmdk=Plattenkennsatz-'

>--+-----------------------------------------------+-------------->
   +- -- -VMNAme="neuer_VM-Name" [* <Zeitmarke>]-+
   +- --DATACENTER="eigenes_Datacenter"----------+
   +- --HOST="eigener_Host"----------------------+
   '- --DATASTORE="eigener_Datenspeicher"--------'

>--+-------------+--+------------------------+-----------------><
   '- --Optionen-'  '-Zieldateispezifikation-'
```

Parameter

Alle Parameter, die Leerzeichen enthalten, müssen in Anführungszeichen (" ") eingeschlossen werden.

VM-Quellenspezifikation
: Gibt den Namen der virtuellen Maschine (oder der VM-Schablone) an, die zurückgeschrieben werden soll.

VMNAme *Zeitmarke
: Gibt den neuen Namen der virtuellen Maschine nach der Zurückschreibung an, wenn nicht der über *VM-Quellenspezifikation* angegebene Name verwendet werden soll.
Sie können das Symbol * (Stern) als Platzhalterzeichen verwenden, um den Namen der zurückgeschriebenen virtuellen Maschine darzustellen. Indem gültige Zeichen vor oder hinter dem Stern angegeben werden, kann ein Präfix oder Suffix für den Namen der zurückgeschriebenen virtuellen Maschine erstellt werden.
Die folgenden Zeichen werden in Namen zurückgeschriebener virtueller Maschinen nicht unterstützt: <q>:;'\"*?,<>/\\|. Ein Zurückschreibungsbefehl, der nicht unterstützte Zeichen enthält, schlägt mit Fehlernachricht ANS9117E fehl.

VMWare unterstützt keine Namen virtueller Maschinen mit einer Länge von mehr als 80 Zeichen.
Eine Zeitmarkenoption, die das Datum und die Uhrzeit der Zurückschreibung aufzeichnet, kann an den Namen der zurückgeschriebenen virtuellen Maschine angehängt werden. Die Optionsausgabe verwendet die in der Optionsdatei definierten Formate für DATEFORMAT und TIMEFORMAT für die Angabe der Zeitmarkenzeichenfolge. In den von den Zeitmarkenparametern zurückgegebenen Datumsangaben wird ein Gedankenstrich als Trennzeichen verwendet.
Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, oder bei Angabe von LOCAL für den Parameter FROM nicht gültig.

DATACENTER
Gibt den Namen des Datencenters, in das die virtuelle Maschine zurückgeschrieben werden soll, gemäß Definition in vSphere vCenter an. Wenn das Datencenter in einem Ordner enthalten ist, müssen Sie die Option -datacenter angeben, wenn Sie die virtuelle Maschine zurückschreiben, und die Ordnerstruktur des Datencenters in den Datencenternamen einschließen. Die folgende Syntax ist beispielsweise gültig:

```
-datacenter=Ordnername/Datencentername
```

Wenn Sie eine virtuelle Maschine mithilfe der grafischen Benutzerschnittstelle zurückschreiben, müssen Sie die virtuelle Maschine an eine andere Position zurückschreiben. Erfolgt die Zurückschreibung an die ursprüngliche Position, kann der Ordnername des Datencenters nicht angegeben werden. Ohne einen Ordnernamen zum Lokalisieren des ursprünglichen Datencenters schlägt die Zurückschreibungsoperation fehl.

Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

HOST
Gibt den Domänennamen des ESX-Host-Servers an, auf den zurückgeschrieben wird (wie in vSphere vCenter definiert).
Bei diesem Parameter muss die Groß-/Kleinschreibung beachtet werden und sein Wert muss mit dem Hostnamen übereinstimmen, der im VMware vSphere-Web-Client angezeigt wird. Um den Hostnamen im vSphere-Web-Client zu bestätigen, wählen Sie einen Host aus und klicken Sie auf Verwalten > Netzbetrieb > TCP/IP-Konfiguration > DNS.
Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

DATASTORE
Gibt den VMware-Datenspeicher an, in den die virtuelle Maschine zurückgeschrieben werden soll. Der Datenspeicher kann sich auf einer SAN-, NAS- oder iSCSI-Einheit oder auf einem virtuellen VMware-Datenträger (VVOL) befinden. Sie können nur einen Datenspeicher angeben, wenn Sie eine virtuelle Maschine zurückschreiben. Wenn Sie keinen Parameter datastore angeben, wird die VMDK-Datei der virtuellen Maschine in den Datenspeicher zurückgeschrieben, in dem sie sich befunden hat, als die Sicherung erstellt wurde.
Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

Windows-Betriebssysteme*Zieldateispezifikation*

Windows-Betriebssysteme Dieser Parameter ist nur für VMware-VCB-Zurückschreibungen gültig. Er gibt die Position an, an der vollständige VCB-Imagedateien für virtuelle Maschinen zurückgeschrieben werden. Wird diese Option nicht angegeben, wird die Option vmbackdir verwendet.

:vmdk=all-vmdk
Diese Option gibt an, dass alle virtuellen Platten (Dateien *.vmdk) bei der Zurückschreibung der virtuellen Maschine eingeschlossen werden. Dies ist der Standardwert.
Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

:vmdk=cnfg
Diese Option gibt an, dass die Konfigurationsinformationen der virtuellen Maschine zurückgeschrieben werden. Die Konfigurationsinformationen werden immer zurückgeschrieben, wenn eine neue virtuelle Maschine erstellt wird. Standardmäßig wird die Konfiguration jedoch nicht zurückgeschrieben, wenn Sie eine vorhandene virtuelle Maschine mit ausgewählten virtuellen Platten aktualisieren.
Normalerweise schlägt das Zurückschreiben von Konfigurationsinformationen auf eine vorhandene virtuelle Maschine fehl, weil ein Konflikt zwischen den zurückgeschriebenen Konfigurationsinformationen und den Konfigurationsinformationen der vorhandenen virtuellen Maschine auftritt. Verwenden Sie diese Option, wenn die vorhandene Konfigurationsdatei einer virtuellen Maschine auf dem ESX-Server gelöscht wurde und die gesicherte Konfiguration verwendet werden soll, um die Datei erneut zu erstellen.
Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

:vmdk=*Plattenkennsatz*
Mit dieser Option wird der Plattenkennsatz der virtuellen Platten angegeben, die bei der Zurückschreibungsoperation berücksichtigt werden sollen. Sie geben diese Option nur an, wenn Sie Daten selektiv von bestimmten Platten zurückschreiben wollen.
Anmerkung: Beim Befehl Restore VM müssen die Kennsatznamen der vmdk-Dateien, die bei einer Zurückschreibungsoperation für virtuelle Maschinen (Restore VM) eingeschlossen werden sollen (Parameter :vmdk=), als Kennsatznamen in der englischen Sprache genauso angegeben werden, wie sie in der Ausgabe des Befehls `Backup VM VM-Name -preview` angezeigt werden. Beispiele für die englischen VMDK-Kennsätze sind "Hard Disk 1", "Hard Disk 2" usw.
Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

:-vmdk=*Plattenkennsatz*
Mit dieser Option wird der Plattenkennsatz mindestens einer virtuellen Platte angegeben, die von der Zurückschreibungsoperation ausgeschlossen werden soll.
Anmerkung: Beim Befehl Restore VM müssen die Kennsatznamen der vmdk-Dateien, die bei einer Zurückschreibungsoperation für virtuelle Maschinen (Restore VM) ausgeschlossen werden sollen (Parameter :-vmdk=), als Kennsatznamen in der englischen Sprache genauso angegeben werden, wie sie in der Ausgabe des Befehls `Backup VM VM-Name -preview` angezeigt werden. Beispiele für die englischen VMDK-Kennsätze sind "Hard Disk 1", "Hard Disk 2" usw.
Anmerkung: Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

Tabelle 1. Befehl Restore VM: Zugehörige Optionen für die Zurückschreibung virtueller VMware-Maschinen

Option	Verwendung
datacenter	Befehlszeile oder Optionsdatei. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
datastore	Befehlszeile oder Optionsdatei. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
host	Befehlszeile oder Optionsdatei. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
inactive	Befehlszeile.
pick	Befehlszeile. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
pitdate	Befehlszeile. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
pittime	Befehlszeile. Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.
Windows-Betriebssystemevmautostartvm Dieser Parameter ist nur gültig, wenn instantaccess als Wert für vmrestoretype angegeben wird.	Windows-BetriebssystemeBefehlszeile oder Clientoptionsdatei
vmbackdir	Befehlszeile oder Clientoptionsdatei
vmbackuplocation	Befehlszeile
vmbackuptype	Befehlszeile oder Clientoptionsdatei
vmdefaultdvportgroup	Befehlszeile oder Clientoptionsdatei
vmdefaultdvswitch	Befehlszeile oder Clientoptionsdatei
vmdefaultnetwork	Befehlszeile oder Clientoptionsdatei
vmdiskprovision Dieser Parameter ist nur gültig, wenn instantrestore als Wert für vmrestoretype angegeben wird.	Befehlszeile oder Clientoptionsdatei
Windows-Betriebssystemevmiscsiserveraddress Dieser Parameter ist nur gültig, wenn instantaccess oder instantrestore als Wert für vmrestoretype angegeben wird.	Windows-BetriebssystemeBefehlszeile oder Clientoptionsdatei
vmmaxrestoresessions	Befehlszeile oder Clientoptionsdatei
Windows-Betriebssystemevmrestoretype	Windows-BetriebssystemeBefehlszeile.
Windows-Betriebssystemevmtempdatastore Dieser Parameter ist nur gültig, wenn instantrestore als Wert für vmrestoretype angegeben wird.	Windows-BetriebssystemeBefehlszeile oder Clientoptionsdatei
vmvstortransport	Befehlszeile oder Clientoptionsdatei Dieser Parameter ist für die Zurückschreibung virtueller VMware-Maschinen, die mit VCB gesichert wurden, nicht gültig.

Beispiele

Windows-BetriebssystemeTask

Windows-BetriebssystemeInformationen zur Ausführung einer Sofortzurückschreibungs- oder Sofortzugriffsoperation über die Befehlszeile finden Sie in Szenarios für die Ausführung des vollständigen VM-Sofortzugriffs (Instant Access) und der vollständigen VM-Sofortzurückschreibung (Instant Restore) über die Befehlszeile des Clients für Sichern/Archivieren.

Task

Die neueste Sicherungsversion von `eigene_VM` mit dem ursprünglichen Namen zurückschreiben. Die VMware-Verwaltungsschnittstelle verwenden, um die ursprüngliche virtuelle Maschine zu löschen, bevor sie mit dieser Syntax zurückgeschrieben wird.

```
dsmc restore vm eigene_VM
```

Task

Die neueste Sicherungsversion von *eigene_VM* auf eine neue Maschine zurückschreiben, die mit dem Namen "Testmaschine" erstellt wird. Im Befehl sind für das Zurückschreibungsziel das Datencenter, der ESX-Host und der Datenspeicher angegeben.

```
dsmc restore vm eigene_VM -vmname="Testmaschine"
  -datacenter="eigenes_Datacenter" -host="eigener_Host"
   -datastore="eigener_Datenspeicher"
```

Task

Die neueste Sicherungsversion von *eigene_VM* mit dem neuen Namen *eigene_VM_nach_Zurückschreibung* zurückschreiben.

```
dsmc restore vm eigene_VM -vmname="*_nach_Zurückschreibung"
  -datacenter="eigenes_Datacenter" -host="eigener_Host"
   -datastore="eigener_Datenspeicher"
```

Task

Die neueste Sicherungsversion von *eigene_VM* mit einem neuen Namen zurückschreiben, der Datum und Uhrzeit ähnlich wie in dem Beispiel *eigene_VM_03-22-2017_14-41-24* anzeigt.

```
dsmc restore vm eigene_VM -vmname="*_<Zeitmarke>"
  -datacenter="eigenes_Datacenter" -host="eigener_Host"
   -datastore="eigener_Datenspeicher"
```

Task

Die neueste Sicherungsversion von *eigene_VM* zurückschreiben. Die Zurückschreibung in ein Datencenter mit dem Namen *eigenes_Datacenter* ausführen. Das Datencenter befindet sich in vCenter; der relative Pfad in vCenter lautet dirA/datacenters/.

```
dsmc restore vm eigene_VM -vmname="Testmaschine"
  -datacenter="dirA/datacenters/eigenes_Datencenter"
  -host="eigener_Host" -datastore="eigener_Datenspeicher"
```

Task

Eine Schablone für virtuelle Maschinen an dieselbe Position und mit demselben Namen zurückschreiben.

```
dsmc restore vm VM-Schablonenname
```

Task

Eine Schablone für virtuelle Maschinen an eine andere Position zurückschreiben.

```
dsmc restore vm VM-Schablonenname-vmname=neuer_Name
  -datastore=neuer_Datenspeicher -host=neuer_Host
   -datacenter=neues_Datencenter
```

Task

Nur Festplatte 2 und Festplatte 3 auf die vorhandene virtuelle Maschine mit dem Namen vm1 zurückschreiben.

```
dsmc restore vm "vm1:vmdk=Festplatte 2:vmdk=Festplatte 3"
```

Task

Alle Platten auf die vorhandene virtuelle Maschine mit dem Namen vm1 zurückschreiben, aber die Daten von Festplatte 4 nicht zurückschreiben.

```
dsmc restore vm "vm1:-vmdk=Festplatte 4"
```

Task

Nur die Daten von Festplatte 1 auf die vorhandene virtuelle Maschine vm1 zurückschreiben, ohne Konfigurationsinformationen zu aktualisieren.
Anmerkung: Wenn Sie eine vorhandene virtuelle Maschine zurückschreiben, ist das Standardverhalten, die Konfigurationsinformationen nicht zu aktualisieren.

```
dsmc restore vm "vm1:vmdk=Festplatte 1:-vmdk=cnfg"
```

Task

Alle Platten auf die vorhandene virtuelle Maschine mit dem Namen vm1 zurückschreiben.

```
dsmc restore vm "vm1:vmdk=all-vmdk"
```

Dieser Befehl aktualisiert alle virtuellen Platten auf einer vorhandenen virtuellen Maschine mit dem Namen vm1. Hierbei besteht ein Unterschied zu der mit `dsmc restore vm vm1` ausgeführten Aktion, bei der eine neue virtuelle Maschine mit dem Namen vm1 erstellt wird (vm1 darf nicht vorhanden sein, damit `dsmc restore vm vm1` erfolgreich ist).

Task

Maximal drei Sitzungen für Zurückschreibungsoperationen für virtuelle Platten in der VM vm1 festlegen:

```
dsmc restore vm vm1 -vmmaxrestoresessions=3
```

Wichtig: Für virtuelle Windows-Maschinen: Wenn Sie versuchen, eine vollständige VM-Zurückschreibung einer Sicherung mit Anwendungsschutz auszuführen, die mit zwei oder mehr Versuchen zur Erstellung einer Momentaufnahme erstellt wurde, ist die Momentaufnahme des Systemproviders auf der zurückgeschriebenen virtuellen Maschine (VM) vorhanden. Während die Anwendung Daten auf die Platte schreibt, wächst der Schattenspeicherbereich, bis nicht mehr genügend Plattenspeicher verfügbar ist.

Im Allgemeinen darf, wenn während einer Sicherung Anwendungsschutz verwendet wurde, nur die Zurückschreibung mit Anwendungsschutz verwendet werden. Wenn Sie die Anwendung zurückschreiben, wird der Datenträger automatisch zurückgesetzt. Wenn Sie jedoch die vollständige virtuelle Maschine zurückschreiben müssen, müssen Sie die Schattenkopie zurücksetzen oder löschen.

Stellen Sie nach der Zurückschreibung der gesamten virtuellen Maschine sicher, dass die Zurückschreibung erfolgreich war und die Daten nicht beschädigt sind. Wenn die Daten nicht beschädigt sind, löschen Sie die Schattenkopie. Wenn die Daten beschädigt sind, setzen Sie die Schattenkopie zurück, um die Datenintegrität wiederherzustellen.

Sie können die Schattenkopie, die gelöscht oder zurückgesetzt werden soll, mithilfe der Datei dsmShadowCopyID.txt im Stammverzeichnis jedes zurückgeschriebenen Datenträgers bestimmen. Diese Datei enthält die Momentaufnahme-IDs der Schattenkopien, die während der Versuche zur Erstellung einer Momentaufnahme erstellt wurden. Mit dem diskshadow-Befehl delete shadows können Sie diese IDs löschen; mit dem Befehl revert können Sie die Schattenkopie zurücksetzen. Nachdem das Löschen oder Zurücksetzen abgeschlossen ist, können Sie auch die Datei dsmShadowCopyID.txt löschen.

Weitere Informationen finden Sie in INCLUDE.VMSNAPSHOTATTEMPTS.

Windows-Betriebssysteme

Restore VM für virtuelle Microsoft Hyper-V-Maschinen

Mit dem Befehl Restore VM können Sie Hyper-V-Gastmaschinen zurückschreiben. Sie können Hyper-V-Gastmaschinen auf eine lokale Platte, auf eine Platte mit SAN-Anschluss, einen freigegebenen Clusterdatenträger (freigegebenes Clustervolume) oder in eine ferne Dateiserverfreigabe zurückschreiben. Ferne Dateiserverfreigaben müssen sich auf einem System mit Windows Server 2012 oder höher befinden.

Wenn die virtuelle Maschine, die Sie zurückschreiben, vorhanden ist, beendet der Client für Sichern/Archivieren sie und löscht alle Dateien, aus denen die virtuelle Maschine besteht. Der Client schreibt sie dann aus dem Image zurück, das auf dem IBM Spectrum Protect-Server gespeichert ist. Wenn die virtuelle Maschine zu einem Windows Server 2012-Cluster gehört, wird sie im Cluster in den Offlinestatus versetzt. Dadurch wird die virtuelle Maschine gestoppt. Anschließend werden die Dateien gelöscht und der Client schreibt die virtuelle Maschine aus der IBM Spectrum Protect-Sicherung zurück.

Tipp: Auch wenn der Client die virtuelle Maschine vor dem Löschen abschaltet, ist das manuelle Abschalten der virtuellen Maschine vor der Ausführung des Befehls Restore VM zu empfehlen, um alle aktiven Anwendungsaktivitäten ordnungsgemäß zu stoppen. Schreiben Sie anschließend die virtuelle Maschine mit dem Befehl Restore VM so zurück, dass ihr Inhalt und ihre Konfiguration mit dem Stand bei ihrer Sicherung identisch sind.

Unterstützte Clients

Dieser Befehl ist auf unterstützten Windows-Clients gültig, die auf einem Hyper-V-Hostsystem installiert sind.

Syntax

```
>>-REStore VM-- --VM-Quellenspezifikation----------------------->

>--+-----------------------------------------------------+-------->
   '- -targetpath=--Pfad--+--------------------------+-'
                          '- -vmname=--neuer_VM-Name-'

>--+-----------------+-----------------------------------------><
   '-+-------------+-'
     '- --Optionen-'
```

Parameter

Alle Parameter, die Leerzeichen enthalten, müssen in Anführungszeichen (" ") eingeschlossen werden.
Der Parameter *VM-Quellenspezifikation* ist erforderlich. Die anderen Parameter sind optional. Bestimmen Sie anhand der folgenden Szenarios die zu verwendenden Parameter:

- Um die virtuelle Maschine unter Verwendung des ursprünglichen Namens der virtuellen Maschine in den ursprünglichen Pfad zurückzuschreiben, verwenden Sie nur den Parameter *VM-Quellenspezifikation*. Die virtuelle Maschine wird mit ihrer ursprünglichen VMware-GUID zurückgeschrieben.
- Um die virtuelle Maschine unter Verwendung des ursprünglichen Namens der virtuellen Maschine in einen Alternativpfad zurückzuschreiben, verwenden Sie die Parameter *VM-Quellenspezifikation* und -targetpath. Die virtuelle Maschine mit mit einer neuen VMware-GUID in den angegebenen Pfad zurückgeschrieben. Die virtuelle Maschine im ursprünglichen Pfad wird nicht gelöscht.
- Um die virtuelle Maschine unter Verwendung eines neuen Namens für die virtuelle Maschine in einen Alternativpfad zurückzuschreiben, verwenden Sie die Parameter *VM-Quellenspezifikation*, -targetpath und -vmname. Die virtuelle Maschine wird mit dem neuen Namen und einer neuen VMware-GUID in den angegebenen Pfad zurückgeschrieben. Die virtuelle Maschine mit dem ursprünglichen Namen im ursprünglichen Pfad wird nicht gelöscht.

Der Parameter -vmname ist nur für die Zurückschreibung virtueller Maschinen gültig, die mit dem Modus `iffull` oder `ifincremental` gesichert wurden. Dieser Parameter wird für virtuelle Maschinen ignoriert, die mit dem Modus `full` oder `incremental`, die beide in früheren

Produktreleases bereitgestellt wurden, gesichert wurden.

VM-Quellenspezifikation
Gibt den Namen der virtuellen Maschine an, die zurückgeschrieben werden soll. Beim Namen der virtuellen Maschine muss die Groß-/Kleinschreibung beachtet werden. Sie können keine Platzhalterzeichen im Namen der virtuellen Maschine verwenden.

-targetpath=*Pfad*
Gibt den Pfad an, in den die virtuelle Maschine zurückgeschrieben werden soll.
Dieser Parameter ist erforderlich, wenn der Parameter -vmname verwendet wird; in allen anderen Fällen ist er optional. Verwenden Sie diesen Parameter, um die virtuelle Maschine in einen Alternativpfad zurückzuschreiben.

-vmname=*neuer_VM-Name*
Gibt einen neuen Namen für die virtuelle Maschine an. Der Name kann 1-100 Zeichen enthalten. Die folgenden Zeichen sind nicht gültig: `\ / : ; , * ? " ' < > |`
Dieser Parameter erfordert den Parameter -targetpath.

Tabelle 2. Befehl 'Restore VM': Zugehörige Optionen für die Zurückschreibung virtueller Hyper-V-Maschinen

Option	Verwendung
inactive	Befehlszeile:
pick	Befehlszeile:
pitdate	Befehlszeile:
pittime	Befehlszeile:
replace	Befehlszeile, Clientoptionsdatei oder Profileditor des Clients
vmbackdir	Befehlszeile, Clientoptionsdatei

Beispiele

Task
Die neueste Sicherungsversion einer virtuellen Maschine mit dem Namen VM1 auf das Laufwerk und in den Pfad zurückschreiben, von dem sie gesichert wurde.

```
dsmc restore vm VM1
```

Task
Die neueste Sicherungsversion einer virtuellen Maschine mit dem Namen vm1 auf das Laufwerk und in den Pfad zurückschreiben, von dem sie gesichert wurde. Die vorhandene virtuelle Maschine ohne Anzeige einer Bestätigung ersetzen.

```
dsmc restore vm vm1 -replace=yes
```

Task
Die gesicherte virtuelle Maschine mit dem Namen VM1 unter einem neuen Namen (vm2) zurückschreiben:

```
dsmc restore vm VM1 -VmName=vm2
```

Task
Die gesicherte virtuelle Maschine mit dem Namen vm1 zurückschreiben und ihr einen neuen Namen (vm2) zuordnen. Falls die virtuelle Maschine vm2 bereits vorhanden ist, eine Bestätigungsanforderung vor dem Überschreiben ausgeben.

```
dsmc restore vm vm1 -VmName=vm2 -replace=prompt
```

Task
Die virtuelle Maschine mit dem Namen vm1 auf ein bestimmtes Laufwerk und in einen bestimmten Pfad zurückschreiben, ohne die virtuelle Maschine umzubenennen:

```
dsmc restore vm vm1 -targetpath="E:\New Path"
```

Task
Die virtuelle Maschine mit dem Namen vm1 in einen neuen Pfad zurückschreiben und in vm2 umbenennen:

```
dsmc restore vm vm1 -VmName=vm2 -targetpath=F:\NewPath
```

Task
Die Optionen -pick und -inactive verwenden, um aktive und inaktive Sicherungen für eine virtuelle Maschine mit dem Namen vm1 anzuzeigen. Sie wählen die zurückzuschreibende Sicherung in einer Liste aus:

```
dsmc restore vm vm1 -pick -inactive
```

Retrieve

Mit dem Befehl retrieve können Kopien archivierter Dateien vom IBM Spectrum Protect-Server abgerufen werden. Es können bestimmte Dateien oder vollständige Verzeichnisse abgerufen werden.

Mit der Option description können die Beschreibungen angegeben werden, die den abzurufenden Dateien zugeordnet sind.

Verwenden Sie die Option pick, um eine Liste Ihrer Archivierungen anzuzeigen, aus der Sie eine Archivierung zum Abrufen auswählen können.

Rufen Sie die Dateien in dasselbe Verzeichnis ab, in dem sie archiviert wurden, oder in ein anderes Verzeichnis. Der Client für Sichern/Archivieren verwendet die Option preservepath mit dem Wert subtree als Standardwert für das Zurückschreiben von Dateien.

 Mac OS X-BetriebssystemeAnmerkung: Wird ein Verzeichnis abgerufen, werden das Datum und die Uhrzeit des Abrufs als Änderungsdatum und Änderungszeit festgelegt und nicht das Datum und die Uhrzeit des Verzeichnisses bei seiner Archivierung. Die Ursache dafür ist, dass der Client für Sichern/Archivieren zuerst die Verzeichnisse abruft und anschließend die Dateien zu den Verzeichnissen hinzufügt.
 Windows-BetriebssystemeAnmerkung:

1. Wird ein Verzeichnis abgerufen, werden das Datum und die Uhrzeit des Abrufs als Änderungsdatum und Änderungszeit festgelegt und nicht das Datum und die Uhrzeit des Verzeichnisses bei seiner Archivierung. Die Ursache dafür ist, dass der Client für Sichern/Archivieren zuerst die Verzeichnisse abruft und anschließend die Dateien zu den Verzeichnissen hinzufügt.
2. Wird versucht, eine Datei abzurufen, deren Name mit dem Kurznamen einer vorhandenen Datei identisch ist, tritt ein Fehler auf. Wenn Sie beispielsweise versuchen, eine Datei, der ausdrücklich der Name ABCDEF~1.DOC zugeordnet wurde, in ein Verzeichnis abzurufen, in dem sich eine Datei mit dem Namen abcdefghijk.doc befindet, schlägt der Abruf fehl, weil das Windows-Betriebssystem die Datei mit dem Namen abcdefghijk.doc dem Kurznamen ABCDEF~1.DOC gleichsetzt. Die Abruffunktion behandelt dies als doppelte Datei.
   Wenn dieser Fehler auftritt, kann er mit einer der folgenden Maßnahmen korrigiert werden:
   - Die Datei mit dem angegebenen Kurzdateinamen an eine andere Position abrufen.
   - Den Abruf stoppen und den Namen der vorhandenen Datei ändern.
   - Die Unterstützung für Kurzdateinamen auf Windows inaktivieren.
   - Keine Dateinamen verwenden, die mit der Kurzdateinamenskonvention unverträglich sind. Verwenden Sie z. B. nicht ABCDEF~1.DOC.

 Windows-BetriebssystemeDer Workstationname ist Bestandteil des Dateinamens. Daher muss ein Ziel angegeben werden, wenn Dateien auf einer Workstation archiviert werden und auf einer anderen Workstation abgerufen werden sollen. Dies gilt auch, wenn auf derselben physischen Workstation abgerufen wird, die Workstation jedoch einen neuen Namen hat. Soll beispielsweise die Datei c:\doc\h2.doc in ihr Ursprungsverzeichnis auf der Workstation mit dem Namen 'star' abgerufen werden, geben Sie Folgendes ein:

```
dsmc retrieve c:\doc\h2.doc \\star\c$\
```

Die Workstation 'star' wurde umbenannt und der neue Name lautet 'meteor'. Um die Datei c:\doc\h2.doc nach 'meteor' abzurufen, geben Sie Folgendes ein:

```
dsmc retrieve c:\doc\h2.doc \\meteor\c$\
```

Folgende Eingabe ist auch möglich:

```
dsmc retrieve c:\doc\h2.doc \\star\c$\
```

Beide Befehle können verwendet werden, da die lokale Workstation (in diesem Fall meteor) angenommen wird, wenn kein Workstationname im Befehl angegeben wird.
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

 Mac OS X-Betriebssysteme  AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme

Syntax

```
>>-RETrieve--+-------------+-------------------------------------->
             '- --Optionen-'

>--+- --Quellendateispezifikation---+--------------------------->
   '- --"Quellendateispezifikation"-'

>--+---------------------------+------------------------------><
   '- --Zieldateispezifikation-'
```

 Windows-Betriebssysteme

Syntax

```
>>-RETrieve--+-------------+-------------------------------------->
```

```
              '- --Optionen-'

>--+- --Quellendateispezifikation--------------------------+---->
   '- --{--Dateibereichsname--}--Quellendateispezifikation-'

>--+---------------------------+-------------------------------><
   '- --Zieldateispezifikation-'
```

Parameter

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeQuellendateispezifikation
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt den Pfad und den Namen der Datei an, die abgerufen werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.

Windows-BetriebssystemeQuellendateispezifikation
Windows-BetriebssystemeGibt den Pfad und den Namen der Datei an, die abgerufen werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.
Anmerkung: Wenn Dateibereichsname angegeben wird, darf die Dateispezifikation keinen Laufwerkbuchstaben enthalten.

Windows-Betriebssysteme{Dateibereichsname}
Windows-BetriebssystemeGibt den in geschweiften Klammern eingeschlossenen Dateibereich auf dem Server an, in dem sich die abzurufenden Dateien befinden. Dieser Name ist die Laufwerkbezeichnung des Workstationlaufwerks, aus dem die Dateien archiviert wurden.
Sie verwenden den Dateibereichsnamen, wenn sich die Laufwerkbezeichnung geändert hat oder wenn Sie Dateien abrufen, die aus einem anderen Knoten archiviert wurden, dessen Laufwerkbezeichnungen sich von Ihren unterscheiden.
Anmerkung: Sie müssen einen NTFS- oder ReFS-Dateibereichsnamen in Groß-/Kleinschreibung oder in Kleinschreibung angeben, der zwischen Anführungszeichen und geschweiften Klammern steht. Beispiel: *{"NTFSDrive"}*. Hochkommas oder Anführungszeichen sind im Schleifenmodus gültig. Beispielsweise ist sowohl *{"NTFSDrive"}* als auch *{'NTFSDrive'}* gültig. Im Stapelmodus sind nur Hochkommas gültig. Die Einschränkung auf Hochkommas ist im Betriebssystem begründet.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeZieldateispezifikation
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeGibt den Pfad und Dateinamen an, in dem die Dateien gespeichert werden sollen. Wenn Sie kein Ziel angeben, schreibt der Client die Dateien in den ursprünglichen Quellenpfad zurück.
Anmerkung: Wenn Sie kein Ziel angeben, stellt der Client für Sichern/Archivieren fest, ob das ursprüngliche Dateisystem erreicht werden kann. Kann das ursprüngliche Dateisystem nicht erreicht werden, schreibt der Client die Datei nicht zurück.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeDieser Fehler kann auch auftreten, wenn Sie die Option virtualmountpoint aus der Datei dsm.sys entfernen. In diesem Fall können Sie ein anderes Ziel angeben oder die ursprüngliche Option virtualmountpoint in die Datei dsm.sys zurückschreiben, den Client erneut starten und den Befehl wiederholen.

Windows-BetriebssystemeZieldateispezifikation
Windows-BetriebssystemeGibt den Pfad und Dateinamen an, in dem die Dateien gespeichert werden sollen. Wenn Sie kein Ziel angeben, schreibt der Client die Dateien in den ursprünglichen Quellenpfad zurück.
Beachten Sie bei der Eingabe der Zieldateispezifikation Folgendes:

- Wenn die Quellendateispezifikation eine einzelne Datei benennt, kann die Zieldateispezifikation eine Datei oder ein Verzeichnis sein.
- Wenn die Quellendateispezifikation Platzhalterzeichen enthält oder wenn Sie die Option `subdir=yes` angeben, muss die Zieldateispezifikation ein Verzeichnis sein und mit einem Verzeichnisbegrenzer (\) enden.

Anmerkung: Falls der Zielpfad oder ein Teil davon nicht vorhanden ist, wird er vom Client erstellt.

Tabelle 1. Befehl Retrieve: Zugehörige Optionen

Option	**Verwendung**
Windows-Betriebssystemedateformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemedateformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
description	Nur in der Befehlszeile.
dirsonly	Nur in der Befehlszeile.
filelist	Nur in der Befehlszeile.
filesonly	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme followsymbolic	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Option	Verwendung
fromdate	Nur in der Befehlszeile.
fromnode	Nur in der Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-Betriebssystemefromowner	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-BetriebssystemeNur in der Befehlszeile.
fromtime	Nur in der Befehlszeile.
ifnewer	Nur in der Befehlszeile.
pick	Nur in der Befehlszeile.
preservepath	Nur in der Befehlszeile.
Windows-Betriebssystemereplace	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemereplace	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme skipntpermissions	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme skipntsecuritycrc	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemesubdir	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemesubdir	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme tapeprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme tapeprompt	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssystemetimeformat	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemetimeformat	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
todate	Nur in der Befehlszeile.
totime	Nur in der Befehlszeile.

Beispiele

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeEine einzelne Datei mit dem Namen budget abrufen.

```
retrieve /home/devel/projecta/budget
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine einzelne Datei mit dem Namen budget.fin abrufen.

```
ret c:\devel\projecta\budget.fin
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAlle Dateien mit der Erweiterung .c aus dem Verzeichnis /home/devel/projecta abrufen.

```
retrieve "/home/devel/projecta/*.c"
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Dateien mit der Erweiterung .c aus dem Verzeichnis c:\devel\projecta abrufen.

```
ret c:\devel\projecta\*.c
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Dateien mit der Dateierweiterung .c aus dem Verzeichnis \devel\projecta im Dateibereich winnt abrufen.

```
ret {winnt}\devel\projecta\*.c
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien im Verzeichnis /home abrufen.

```
retrieve /home/
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Dateien im Verzeichnis c:\devel abrufen.

```
ret c:\devel\*
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeDateien aus dem Verzeichnis proj im Dateibereich abc abrufen.

```
ret {abc}\proj\*.*
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien mit der Dateierweiterung .c aus dem Verzeichnis /home/devel/projecta in das Verzeichnis /home/newdevel/projectn/projecta abrufen. Ist das Verzeichnis /projectn oder /projectn/projecta nicht vorhanden, wird es erstellt.

```
retrieve "/home/devel/projecta/*.c" /home/newdevel/projectn/
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeAlle Dateien mit der Dateierweiterung .c aus dem Verzeichnis c:\devel\projecta in das Verzeichnis c:\newdevel\projectn\projecta abrufen. Ist das Verzeichnis \projectn oder \projectn\projecta nicht vorhanden, wird es erstellt.

```
ret c:\devel\projecta\*.c c:\newdevel\projectn\
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDateien im Verzeichnis /user/project abrufen. Die Option pick verwenden.

```
ret "/user/project/*" -pick
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeDateien im Verzeichnis c:\project abrufen. Die Option pick verwenden.

```
ret c:\project\* -pick
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien abrufen, die aus dem Verzeichnis /proj mit der Beschreibung "2012 survey results" archiviert wurden.

```
retrieve "/proj/*" -desc="2012 survey results"
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie archivierte Datei /home/devel/budget mit der Beschreibung "my budget" auf das Bandlaufwerk /dev/rmt1 abrufen.

```
mkfifo fifo
dd if=fifo of=/dev/rmt1&
dsmc retrieve -replace=yes -description="mybudget"
/home/devel/budget fifo
```

Mac OS X-BetriebssystemeTask

Mac OS X-BetriebssystemeEine Datei aus dem umbenannten Dateibereich Jaguar_OLD an ihre ursprüngliche Position abrufen. Geben Sie sowohl die Quelle als auch das Ziel wie folgt ein:

```
ret Jaguar_OLD/user5/Documents/myresume.doc /Users/user5/Documents/
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeEine Datei aus dem umbenannten Dateibereich \\Ihr-Knoten\h$_OLD an ihre ursprüngliche Position abrufen. Geben Sie sowohl die Quelle als auch das Ziel wie folgt ein:

```
ret \\your-node\h$_OLD\docs\myresume.doc h:\docs\
```

- Mac OS X-BetriebssysemeWindows-BetriebssystemeArchivierungen aus nicht Unicode-fähigen Dateibereichen abrufen
  Wenn Sie Archivierungen aus Dateibereichen abrufen wollen, die vom Unicode-fähigen Client umbenannt wurden, müssen Sie die Quelle auf dem Server und ein Ziel auf dem Client angeben.
- Windows-BetriebssystemeBenannte Datenströme abrufen
  Der Client für Sichern/Archivieren ruft benannte Datenströme nur auf Dateibasis ab.
- Windows-BetriebssystemeDateien mit freien Bereichen abrufen
  Wenn Sie Dateien mit freien Bereichen in ein Nicht-NTFS- oder Nicht-ReFS-Dateisystem abrufen, geben Sie als Wert des Serverübertragungszeitlimits (IDLETIMEOUT) den Maximalwert 255 an, um eine Zeitlimitüberschreitung der Clientsitzung zu vermeiden.

Mac OS X-BetriebssysemeWindows-Betriebssysteme

Archivierungen aus nicht Unicode-fähigen Dateibereichen abrufen

Wenn Sie Archivierungen aus Dateibereichen abrufen wollen, die vom Unicode-fähigen Client umbenannt wurden, müssen Sie die Quelle auf dem Server und ein Ziel auf dem Client angeben.

Mac OS X-BetriebssysemeDieser Abschnitt gilt nur für Mac OS X. Beispiel: Angenommen, `Jaguar` ist der Name Ihrer Startplatte und Sie archivieren alle .log-Dateien im Verzeichnis /Users/user5/Documents. Bevor die Archivierung stattfindet, benennt der Server den Dateibereich in `Jaguar_OLD` um. Bei der Archivierung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen `/` gestellt. Der neue Unicode-fähige Dateibereich enthält jetzt nur das Verzeichnis Users/user5/Documents und die Dateien *.log, die in der Operation angegeben wurden.

Mac OS X-BetriebssysemeWenn eine Datei aus dem *umbenannten* (alten) Dateibereich an die ursprüngliche Position abgerufen werden soll, müssen Sie sowohl die Quelle als auch das Ziel wie folgt eingeben:

Windows-BetriebssystemeWenn Sie Archivierungen aus Dateibereichen abrufen wollen, die vom Unicode-fähigen Client umbenannt wurden, müssen Sie die Quelle auf dem Server und ein Ziel auf dem Client angeben. Beispiel: Sie haben Dateien von Ihrer H-Platte mit dem Namen \\Ihr-Knoten\h$ archiviert, bevor Sie den Client installierten. Nach der Installation geben Sie den folgenden Archivierungsbefehl aus:

```
arc h:\logs\*.log
```

Windows-BetriebssystemeBevor die Archivierung stattfindet, benennt der Server den Dateibereich in `\\Ihr-Knoten\h$_OLD` um. Bei der Archivierung werden die in der aktuellen Operation angegebenen Daten in den Unicode-fähigen Dateibereich mit dem Namen `\\Ihr-Knoten\h$` gestellt. Dieser Dateibereich enthält nun nur das Verzeichnis `\logs` und die Dateien `*.log`. Wenn eine Datei aus dem (alten) *umbenannten* Dateibereich an ihre ursprüngliche Position abgerufen werden soll, müssen Sie sowohl die Quelle als auch das Ziel wie folgt eingeben:

```
retrieve \\Ihr-Knoten\h$_OLD\docs\myresume.doc h:\docs\
```

Windows-Betriebssysteme

Benannte Datenströme abrufen

Der Client für Sichern/Archivieren ruft benannte Datenströme nur auf Dateibasis ab.

Verzeichnisse in Windows-Systemen können benannte Datenströme enthalten. Benannte Datenströme, die einem Verzeichnis zugeordnet sind, werden während eines Abrufs immer überschrieben (unabhängig vom Wert der Option prompt).

Windows-Betriebssysteme

Dateien mit freien Bereichen abrufen

Wenn Sie Dateien mit freien Bereichen in ein Nicht-NTFS- oder Nicht-ReFS-Dateisystem abrufen, geben Sie als Wert des Serverübertragungszeitlimits (IDLETIMEOUT) den Maximalwert 255 an, um eine Zeitlimitüberschreitung der Clientsitzung zu vermeiden.

Die folgenden Probleme treten auf, wenn mehr Daten zurückgeschrieben werden als das Microsoft-Datenträgerkontingent zulässt:

- Wenn der Benutzer, der den Abruf ausführt, ein Datenträgerkontingent hat (er gehört beispielsweise zur Gruppe 'Sicherungsoperatoren'), ruft der Client für Sichern/Archivieren keine Daten ab, die das Datenträgerkontingent des Benutzers, der den Abruf ausführt, überschreiten, und zeigt die Nachricht "Platte voll" an.
- Wenn der Benutzer, der den Abruf ausführt, kein Datenträgerkontingent hat (er gehört beispielsweise zur Gruppe 'Administratoren'), ruft der Client für Sichern/Archivieren alle Daten ab und überträgt die Eigentumsrechte der Dateien, die das Datenträgerkontingent des ursprünglichen Eigners überschreiten, an den Benutzer, der den Abruf ausführt (in diesem Fall an den Administrator).

Schedule

Mit dem Befehl schedule kann der Client-Scheduler auf Ihrer Workstation gestartet werden. Der Client-Scheduler muss aktiv sein, damit geplante Arbeit gestartet werden kann.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-Betriebssysteme**Berechtigter Benutzer:** Der Befehl schedule startet den Client-Scheduler auf Ihrer Workstation. Der Client-Scheduler muss aktiv sein, damit geplante Arbeit gestartet werden kann.

Anmerkung:

1. Der Befehl schedule kann nicht verwendet werden, wenn die Option managedservices auf `schedule` gesetzt ist. .
2. Mac OS X-BetriebssysemeNur für Mac OS X: Geben Sie zur Verwendung des Befehls schedule die Option managedservices `none` in der Datei dsm.sys an.
3. Dieser Befehl ist nur in der Anfangsbefehlszeile gültig. Im interaktive Modus oder in einer Makrodatei ist er nicht gültig.

Windows-BetriebssysemeIst die Option schedmode auf "polling" (Sendeaufruf) gesetzt, fragt der Client-Scheduler den Server nach der Anzahl Stunden, die Sie mit der Option queryschedperiod in Ihrer Clientoptionsdatei (dsm.opt) angegeben haben, nach geplanten Ereignissen ab. Wird die Option queryschedperiod vom Administrator für alle Knoten definiert, überschreibt diese Einstellung die Einstellung des Clients.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssysemeIst die Option schedmode auf "polling" (Sendeaufruf) gesetzt, fragt der Client-Scheduler den Server nach der Anzahl Stunden, die Sie mit der Option queryschedperiod in Ihrer Clientbenutzeroptionsdatei (dsm.opt) angegeben haben, nach geplanten Ereignissen ab. Wird die Option queryschedperiod vom Administrator für alle Knoten definiert, überschreibt diese Einstellung die Einstellung des Clients.

Windows-BetriebssysemeWird TCP/IP-Übertragung verwendet, kann der Server der Workstation auch mitteilen, wann ein geplantes Ereignis ausgeführt werden muss. In diesem Fall müssen Sie die Option schedmode in der Clientoptionsdatei (dsm.opt) oder im Befehl schedule auf prompted setzen.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssysemeWird TCP/IP-Übertragung verwendet, kann der Server der Workstation auch mitteilen, wann ein geplantes Ereignis ausgeführt werden muss. In diesem Fall müssen Sie die Option schedmode in der Clientbenutzeroptionsdatei (dsm.opt) oder im Befehl schedule auf prompted setzen.

Windows-BetriebssysemeNach dem Starten des Client-Schedulers bleibt dieser solange aktiv und startet geplante Ereignisse, bis die Tastenkombination Strg+Untbr gedrückt, die Workstation erneut gestartet oder ganz ausgeschaltet wird.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssysemeMac OS X-Betriebssysteme Sie können die Option sessioninitiation im Befehl schedule verwenden, um zu steuern, ob der Server oder der Client Sitzungen durch eine Firewall einleiten soll.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssysemeNach dem Starten des Client-Schedulers bleibt dieser so lange aktiv und startet geplante Ereignisse, bis Sie die Tastenkombination Strg+C drücken, den Schedulerprozess mit dem UNIX-Befehl kill stoppen oder die Workstation erneut starten bzw. ausschalten, um ihn zu beenden.

Mac OS X-BetriebssysemeNach dem Starten des Client-Schedulers bleibt dieser so lange aktiv und startet geplante Ereignisse, bis die Sie die Tastenkombination Strg+C drücken, die Taste Q zweimal drücken oder die Workstation erneut starten bzw. ausschalten, um ihn zu beenden.

AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssysemeWindows-Betriebssysteme Anmerkung: Dieser Befehl kann *nicht* im interaktiven Modus eingegeben werden.
AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-BetriebssysemeMac OS X-BetriebssysemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-SCHedule--+-------------+-----------------------------------><
             '- --Optionen-'
```

Parameter

Tabelle 1. Befehl Schedule: Zugehörige Optionen

Option	Verwendung
Windows-Betriebssysteme maxcmdretries	Windows-BetriebssysemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme maxcmdretries	AIX-BetriebssysemeLinux-BetriebssysemeOracle Solaris-Betriebssysteme Mac OS X-BetriebssysemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssystemepassword	Windows-BetriebssysemeClientoptionsdatei (dsm.opt)

Option	Verwendung
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemepassword	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt)
Windows-Betriebssysteme queryschedperiod	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme queryschedperiod	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssystemeretryperiod	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemeretryperiod	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssysteme schedlogname	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme schedlogname	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssystemeschedmode	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme schedmode	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssysteme sessioninitiation	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme sessioninitiation	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
Windows-Betriebssysteme tcpclientport	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme tcpclientport	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.

Beispiele

Mac OS X-Betriebssysteme Windows-BetriebssystemeTask

Mac OS X-Betriebssysteme Windows-BetriebssystemeDen Client-Scheduler starten.

Befehl: `dsmc sch -password=notell`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeFür AIX: Den Scheduler beim Systemstart starten, indem Sie den folgenden Befehl in die Datei /etc/inittab eingeben. Stellen Sie sicher, dass die Option ***passwordaccess*** auf *generate* gesetzt ist.

Befehl: `tsm::once:/usr/bin/dsmc sched > /dev/null 2>&1 #TSM`

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDen Scheduler interaktiv starten und im Hintergrund ausführen.

Befehl: `nohup dsmc sched 2> /dev/null &`

Windows-BetriebssystemeWenn Sie den Befehl schedule ausführen, werden alle Nachrichten zu geplanter Arbeit an die Datei `dsmsched.log` gesendet oder an die Datei, die Sie mit der Option schedlogname in Ihrer Clientoptionsdatei (dsm.opt) angeben. Wenn Sie für den Dateinamen in der Option schedlogname keinen Verzeichnispfad angeben, wird die Datei `dsmsched.log` im aktuellen Arbeitsverzeichnis gespeichert.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWenn Sie den Befehl schedule ausführen, werden alle Nachrichten zu geplanter Arbeit an die Datei `dsmsched.log` gesendet oder an die Datei, die Sie mit der Option schedlogname in Ihrer Clientsystemoptionsdatei (dsm.sys) angeben. Wenn Sie für den Dateinamen in der Option schedlogname keinen Verzeichnispfad angeben, wird die Datei `dsmsched.log` im aktuellen Arbeitsverzeichnis gespeichert. Dies gilt jedoch nicht für Mac OS X. Bei Mac OS X befindet sich die Datei `dsmsched.log` im Verzeichnis `/Library/Logs/tivoli/tsm/`.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Wichtig: Geben Sie in der Umgebungsvariablen DSM_LOG den Namen eines Verzeichnisses an, in dem die Standardberechtigungen den erforderlichen Zugriff gestatten, um Fehler bei Protokollschreiboperationen und den Verarbeitungsabbruch in bestimmten Fällen zu vermeiden.

Selective

Der Befehl selective sichert vom Benutzer angegebene Dateien. Werden diese Dateien beschädigt oder gehen sie verloren, können sie durch Sicherungsversionen vom Server ersetzt werden.

Wenn Sie eine selektive Sicherung ausführen, sind alle Dateien Sicherungskandidaten, sofern Sie sie nicht von der Sicherung ausschließen oder sie nicht den Anforderungen der Verwaltungsklasse in Bezug auf die Durchnummerierung entsprechen.

Während einer selektiven Sicherung werden Kopien der Dateien an den Server gesendet, auch wenn sie sich seit der letzten Sicherung nicht geändert haben. Aus diesem Grund können mehrere Kopien derselben Datei auf dem Server vorhanden sein. In diesem Fall sind möglicherweise nicht so viele verschiedene Versionen der Datei auf dem Server vorhanden, wie beabsichtigt war. Das Versionslimit könnte durch identische Dateien erreicht worden sein. Um dieses Problem zu vermeiden, können Sie mithilfe des Befehls incremental ausschließlich neue und geänderte Dateien sichern.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme Sie können einzelne Dateien oder Verzeichnisse selektiv sichern. Zum Sichern von Gruppen zusammengehöriger Dateien können außerdem Platzhalterzeichen verwendet werden.

Wenn Sie beim Sichern eines bestimmten Pfads und einer bestimmten Datei die Option subdir auf yes setzen, sichert der Client rekursiv alle Unterverzeichnisse unter diesem Pfad und alle Instanzen der angegebenen Datei, die sich unter allen diesen Unterverzeichnissen befinden.

Während einer selektiven Sicherung kann ein Verzeichnispfad gesichert werden, auch wenn die spezifische Datei für die Sicherung nicht gefunden wird. Beispielsweise sichert der folgende Befehl `dir1` und `dir2`, auch wenn die Datei `bogus.txt` nicht vorhanden ist.

Mac OS X-Betriebssysteme

```
selective /Users/user1/Documents/dir1/bogus.txt
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme

```
selective "/dir1/dir2/bogus.txt"
```

Windows-Betriebssysteme

```
selective c:\dir1\dir2\bogus.txt
```

Wenn der Befehl selective wegen eines Übertragungs- oder Sitzungsfehlers wiederholt wird, zeigen die Übertragungsstatistiken die Anzahl Byte an, die der Client während *aller* Befehlswiederholungen zu übertragen versucht. Daher entsprechen die Statistiken für die übertragenen Byte möglicherweise nicht den Dateistatistiken, z. B. für die Dateigröße.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeSie können mit der Option removeoperandlimit angeben, dass die Beschränkung auf 20 Operanden entfernt wird. Geben Sie die Option removeoperandlimit mit dem Befehl selective an, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
              .---------------------------.
              V                           |
>>-Selective------ --Dateispezifikation---+--+-------------+---><
```

Parameter

Dateispezifikation

Gibt den Pfad und den Namen der Datei an, die gesichert werden soll. Es können Platzhalterzeichen verwendet werden, um eine Dateigruppe oder alle Dateien in einem Verzeichnis anzugeben.
Sollen mehrere Dateispezifikationen angegeben werden, trennen Sie die einzelnen Spezifikationen durch ein Leerzeichen voneinander. Werden mehrere Dateispezifikationen angegeben und haben mindestens zwei der Spezifikationen gemeinsame übergeordnete Verzeichnisse, kann es vorkommen, dass die gemeinsamen Verzeichnisobjekte mehrmals gesichert werden. Die Bedingungen, unter denen dieses Verhalten auftritt, sind laufzeitabhängig; das Verhalten selbst hat jedoch keine nachteiligen Auswirkungen.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeLautet die Dateispezifikation beispielsweise /home/amr/ice.doc /home/amr/fire.doc, könnten /home und /home/amr zweimal gesichert werden. Die Dateiobjekte, ice.doc und fire.doc, werden nur einmal gesichert.

 Windows-BetriebssystemeLautet die Dateispezifikation beispielsweise C:\proposals\drafts\ice.doc C:\proposals\drafts\fire.doc, könnten C:\proposals und C:\proposals\drafts zweimal gesichert werden. Die Dateiobjekte, ice.doc und fire.doc, werden nur einmal gesichert.

Wenn Sie verhindern wollen, dass das gemeinsame übergeordnete Verzeichnis mehrmals angegeben wird, verwenden Sie separate, nicht überlappende selective-Befehle, um jede Dateispezifikation zu sichern.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeWenn Sie ein Dateisystem sichern, geben Sie einen abschließenden Schrägstrich an (/home/).
 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeEs gilt eine Begrenzung auf 20 Operanden. Diese Begrenzung verhindert, dass sehr viele Sitzungen geöffnet werden, wenn die Platzhalterzeichen vom Befehlsprozessor der UNIX-Shell erweitert werden. Sie können verhindern, dass aufgrund der Shellerweiterung der Grenzwert von 20 Operanden überschritten wird, indem Sie am Anfang und am Ende der Dateispezifikationen, die Platzhalterzeichen enthalten ("home/docs/*"), Anführungszeichen eingeben.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Mac OS X-Betriebssysteme  Oracle Solaris-BetriebssystemeSie können mit der Option removeoperandlimit angeben, dass die Beschränkung auf 20 Operanden entfernt wird. Wenn Sie die Option removeoperandlimit angeben, wird die Beschränkung auf 20 Operanden nicht umgesetzt und nur durch die verfügbaren Ressourcen oder andere Begrenzungen des Betriebssystems eingeschränkt. Entfernen Sie beispielsweise die Begrenzung auf 20 Operanden, um 21 Dateispezifikationen zu sichern:

```
selective -removeoperandlimit filespec1 filespec2 ... filespec21
```

 Windows-BetriebssystemeWenn Sie ein Dateisystem sichern, geben Sie einen abschließenden Schrägstrich an (C:\).
 Windows-BetriebssystemeSie können so viele Dateispezifikationen angeben wie die verfügbaren Ressourcen oder andere Betriebssystembeschränkungen erlauben.
Sie können die Option filelist anstelle von Dateispezifikationen verwenden, um anzugeben, welche Dateien bei dieser Operation berücksichtigt werden sollen. Diese beiden Methoden schließen sich jedoch gegenseitig aus. Sie können nicht sowohl Dateispezifikationsparameter angeben als auch die Option filelist verwenden. Wenn die Option filelist angegeben wird, werden alle angegebenen Dateispezifikationen ignoriert.

Tabelle 1. Befehl Selective: Zugehörige Optionen

Option	Verwendung
 Windows-Betriebssysteme changingretries	 Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme changingretries	 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeClientsystemoptionsdatei (dsm.sys) oder Befehlszeile.
 Windows-Betriebssysteme compressalways	 Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme compressalways	 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
 Windows-Betriebssysteme compression	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.

Option	Verwendung
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme compression	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
dirsonly	Nur in der Befehlszeile.
filelist	Nur in der Befehlszeile.
filesonly	Nur in der Befehlszeile.
Windows-Betriebssysteme postsnapshotcmd	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.fs.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme preservelastaccessdate	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme preservelastaccessdate	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme presnapshotcmd	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.fs.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-Betriebssysteme removeoperandlimit	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Mac OS X-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssysteme skipntpermissions	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme skipntsecuritycrc	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme snapshotcachesize	AIX-Betriebssysteme Linux-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.fs.
AIX-Betriebssysteme snapshotproviderfs	AIX-BetriebssystemeSystemoptionsdatei (dsm.sys) innerhalb einer Serverzeilengruppe oder mit der Option include.fs.
Windows-Betriebssysteme snapshotproviderfs	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder mit der Option include.fs.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-Betriebssysteme snapshotroot	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Windows-BetriebssystemeNur in der Befehlszeile.
Windows-Betriebssystemesubdir	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssystemesubdir	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.
Windows-Betriebssysteme tapeprompt	Windows-BetriebssystemeClientoptionsdatei (dsm.opt) oder Befehlszeile.
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme tapeprompt	AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeClientbenutzeroptionsdatei (dsm.opt) oder Befehlszeile.

Beispiele

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDie Datei `proja` im Verzeichnis `/home/devel` sichern.

Befehl: `selective /home/devel/proja`

Windows-BetriebssystemeTask
Windows-BetriebssystemeDie Datei `proja.dev` im Verzeichnis `c:\devel` sichern.

Befehl: `sel c:\devel\proja.dev`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien im Verzeichnis `/home/devel` sichern, deren Dateiname mit `proj` beginnt.

Befehl: `selective "/home/devel/proj*"`

Windows-BetriebssystemeTask
Windows-BetriebssystemeAlle Dateien im Verzeichnis `c:\devel` sichern, deren Dateiname mit `proj` beginnt.

Befehl: `sel c:\devel\proj*.*`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAlle Dateien im Verzeichnis `/home/devel` sichern, deren Dateiname mit `proj` beginnt. Die einzelne Datei mit dem Namen `budget` im Verzeichnis `/user/home` sichern.

Befehl: `selective "/home/devel/proj*" /user/home/budget`

Windows-BetriebssystemeTask
Windows-BetriebssystemeAlle Dateien im Verzeichnis `c:\devel` sichern, deren Dateiname mit `proj` beginnt. Alle Dateien mit der Dateierweiterung `.fin` im Verzeichnis `c:\planning` sichern.

Befehl: `sel c:\devel\proj* c:\planning\*.fin`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDas Dateisystem `/home` sichern.

Befehl: `selective /home/ -subdir=yes`

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeAngenommen, Sie haben eine Momentaufnahme des Dateisystems `/usr` gestartet und die Momentaufnahme als `/snapshot/day1` angehängt. Führen Sie eine selektive Sicherung der Verzeichnisbaumstruktur `/usr/dir1/sub1` aus der lokalen Momentaufnahme durch und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnames `/usr`.

Befehl: `dsmc sel "/usr/dir1/sub1/*" -subdir=yes -snapshotroot=/snapshot/day1`

Windows-BetriebssystemeTask
Windows-BetriebssystemeAngenommen, Sie haben eine Momentaufnahme des Laufwerks `C:\` gestartet und die Momentaufnahme als `\\florence\c$\snapshots\snapshot.0` angehängt. Führen Sie eine selektive Sicherung der Verzeichnisbaumstruktur `c:\dir1\sub1` aus der lokalen Momentaufnahme durch und verwalten Sie sie auf dem IBM Spectrum Protect-Server unter dem Dateibereichsnamen `C:\`.

Befehl: `dsmc sel c:\dir1\sub1\* -subdir=yes -snapshotroot=\\florence\c$\snapshots\snapshot.0`

- Windows-BetriebssystemeUnterstützung offener Dateien
  Wenn die Unterstützung offener Dateien konfiguriert ist, führt der Client für Sichern/Archivieren eine Momentaufnahmesicherung oder -archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder "im Gebrauch") sind.
- Lokale Momentaufnahme einem Serverdateibereich zuordnen
  Verwenden Sie die Option snapshotroot im Befehl selective mit einer Anwendung eines unabhängigen Softwareanbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind. Die Option snapshotroot bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

Windows-Betriebssysteme

Unterstützung offener Dateien

Wenn die Unterstützung offener Dateien konfiguriert ist, führt der Client für Sichern/Archivieren eine Momentaufnahmesicherung oder -archivierung der Dateien aus, die von anderen Anwendungen gesperrt (oder "im Gebrauch") sind.

Verwenden Sie VSS als Momentaufnahmeprovider. Setzen Sie snapshotproviderimage oder snapshotproviderfs auf VSS.

Anmerkung:

1. Sie können die Option include.fs verwenden, um Momentaufnahmeoptionen pro Dateisystem festzulegen.
2. Die Unterstützung offener Dateien ist nur verfügbar für lokale fixierte Datenträger (entweder an Laufwerkbuchstaben oder Datenträgermountpunkte angehängt), die mit NTFS- oder ReFS-Dateisystemen formatiert sind. Diese Unterstützung schließt an ein SAN angeschlossene Datenträger ein, die diese Anforderungen erfüllen.
3. Wenn der Client keine Momentaufnahme erstellen kann, findet eine Übernahme in einer Nicht-OFS-Sicherung statt; dieselbe Sicherungsunterstützung, die erfolgen würde, wenn die OFS-Funktion nicht konfiguriert wäre.
4. Damit die Unterstützung offener Dateien in einer Clusterumgebung aktiviert wird, sollte für alle Systeme im Cluster die OFS-Funktion konfiguriert sein.

Lokale Momentaufnahme einem Serverdateibereich zuordnen

Verwenden Sie die Option snapshotroot im Befehl selective mit einer Anwendung eines unabhängigen Softwareanbieters, die eine Momentaufnahme eines logischen Datenträgers bereitstellt, um die Daten der lokalen Momentaufnahme den realen Dateibereichsdaten zuzuordnen, die auf dem IBM Spectrum Protect-Server gespeichert sind. Die Option snapshotroot bietet keine Funktionen zur Erstellung einer Datenträgermomentaufnahme, sondern ausschließlich Funktionen zur Verwaltung von Daten, die durch Erstellen einer Datenträgermomentaufnahme generiert werden.

AIX-BetriebssystemeNur für AIX: Sie können eine selektive Sicherung auf Momentaufnahmebasis ausführen, indem Sie die Option snapshotproviderfs=*JFS2* angeben.

Set Access

Der Befehl set access erteilt Benutzern an anderen Knoten Zugriff auf Ihre Sicherungsversionen und Archivierungskopien.

Sie können den Befehl set access auch verwenden, um Benutzern an anderen Knoten Zugriff auf Ihre Sicherungsimages zu erteilen.

Sie können einem anderen Benutzer Zugriff auf eine bestimmte Datei oder ein bestimmtes Image, auf mehrere Dateien oder Images oder auf alle Dateien in einem Verzeichnis erteilen. Erteilen Sie einem anderen Benutzer die Zugriffsberechtigung, kann dieser Benutzer Ihre Objekte zurückschreiben oder abrufen. In dem Befehl muss angegeben werden, ob der Zugriff auf Archivierungskopien oder auf Sicherungsversionen erteilt wird.

Linux-BetriebssystemeWindows-BetriebssystemeBei virtuellen VMware-Maschinen können Sie einem Benutzer auf einem anderen Knoten Zugriff auf die Sicherungen einer bestimmten virtuellen Maschine erteilen.

Wenn ein Knoten auf einen anderen IBM Spectrum Protect-Server exportiert wird, können sich die Zugriffsregeln auf dem importierenden Server ändern. Wird eine Zugriffsregel auf alle Dateibereiche auf dem exportierenden Server angewendet, wird die Zugriffsregel auf dem importierenden Server auf die importierten Dateibereiche beschränkt. Die Dateibereiche in der Zugriffsregel auf dem importierenden Server werden aus Sicherheitsgründen beschränkt. Darüber hinaus erkennen die Zugriffsregeln das erste Auftreten eines Platzhalterzeichens in der Dateispezifikation beim Zurückschreiben oder beim Abruf nicht. Dies bedeutet, dass Unterverzeichnisse ignoriert werden, wenn Sie in der Dateispezifikation für eine Zurückschreibung oder einen Abruf ein Platzhalterzeichen verwenden.

Tipp: Wenn Sie einen Knoten auf einen anderen IBM Spectrum Protect-Server exportieren, dürfen Sie kein einzelnes Platzhalterzeichen als Dateispezifikation in der Zugriffsregel verwenden. Erstellen Sie stattdessen eine Zugriffsregel für jeden Dateibereich.
Anmerkung: Es ist nicht möglich, mit einem einzigen Befehl die Zugriffsberechtigung für Sicherungen und Archivierungen zu erteilen.

Mac OS X-BetriebssystemeWindows-BetriebssystemeWenn ein vorhandener Dateibereich während der Unicode-Konvertierung umbenannt wird, gelten die für den Dateibereich definierten Zugriffsregeln weiterhin für den ursprünglichen Dateibereich. Für den neuen Unicode-Dateibereich müssen jedoch neue Zugriffsregeln definiert werden.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-SET Access--+- --Archive-+----------------------------------->
               '- --Backup--'

>--+- --Dateispezifikation--------------------------+----------->
   +- --{--Dateibereichsname--}--Dateispezifikation-+
   +-Image-DS-----------------------------------+
   '-TYPE=VM-- --VM-Name----------------------------'

>-- --Knoten--+-------------+----------------------------------><
             '- --Benutzer-'
```

Parameter

Archive
Erteilt Zugriff auf archivierte Dateien oder Images.

Backup
Erteilt Zugriff auf Sicherungsversionen von Dateien oder Images.

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme*Dateispezifikation*
 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeGibt den Pfad, die Datei, das Image oder das Verzeichnis an, für den/die/das Sie dem anderen Knoten oder Benutzer Zugriff erteilen. Verwenden Sie Platzhalterzeichen, um Gruppen von Dateien oder Images oder alle Dateien in einem Verzeichnis, alle Objekte in einer Verzeichnisverzweigung oder alle Objekte in einem Dateisystem anzugeben. Mit einem einzelnen Stern "*" als Dateispezifikation können Sie die Zugriffsberechtigung für alle Dateien oder Images erteilen, deren Eigner Sie sind und die auf dem Server gesichert wurden. Wenn der Befehl `set access backup "*" Knoten` eingegeben wird, erfolgt keine Überprüfung auf dem Server; es wird davon ausgegangen, dass mindestens ein Objekt gesichert wurde.

Wird die Zugriffsberechtigung für eine Ebene des aktuellen Arbeitsverzeichnisses erteilt, muss nur die Ebene angegeben werden. Wird die Zugriffsberechtigung für Objekte erteilt, die sich nicht in einer Verzeichnisebene des aktuellen Arbeitsverzeichnisses befinden, müssen Sie den vollständigen Pfad angeben. Für die Dateispezifikation, für die eine Zugriffsberechtigung erteilt wurde, muss mindestens eine Sicherungsversion oder eine Archivierungskopie (Datei oder Verzeichnis) auf dem Server vorhanden sein.

Sollen alle Dateien in einem bestimmten Verzeichnis angegeben werden, geben Sie `/home/mine/proj1/*` in die Befehlszeile ein.

Um die Zugriffsberechtigung für alle Objekte unter einer bestimmten Ebene zu erteilen, geben Sie einen Stern, ein Verzeichnisbegrenzungszeichen und einen Stern am Ende der Dateispezifikation an. Soll beispielsweise Zugriff auf alle Objekte unter `home/test` erteilt werden, verwenden Sie die Dateispezifikation `home/test/*/*`.

Wichtig: Durch die Verwendung des Formats `/*/*` alleine erteilen Sie keinen Zugriff auf Objekte in dem angegebenen Verzeichnis, sondern nur auf Objekte in den Verzeichnissen unter dem angegebenen Verzeichnis.

Für das Stammverzeichnis sind die Regeln im Wesentlichen identisch. Geben Sie `/*` in einem Befehl set access und `/*/*` in einem weiteren Befehl set access an, wenn ein anderer Benutzer Zugriff auf alle Dateien und Verzeichnisse in und unter dem Stammverzeichnis haben soll. Die erste Angabe `/*` erteilt Zugriff auf alle Verzeichnisse und alle Dateien im Stammverzeichnis. Die zweite Angabe `/*` erteilt Zugriff auf alle Verzeichnisse und Dateien unter dem Stammverzeichnis.

Beispiel:

- Ihre Verzeichnisstruktur besteht aus mehreren Ebenen: `/home/sub1/subsub1`.
- Das Verzeichnis `/home` enthält die Dateien `h1.txt` und `h2.txt`.
- Das Verzeichnis `/home/sub1` enthält die Datei `s1.htm`.
- Das Verzeichnis `/home/sub1/sub2` enthält die Datei `ss1.cpp`.

Soll Zugriff auf alle Dateien im Verzeichnis `/home/sub1/sub2` erteilt werden, geben Sie Folgendes ein:

```
set access backup /home/sub1/sub2/* * *
```

Soll Zugriff nur auf die Dateien im Verzeichnis `/home` erteilt werden, geben Sie Folgendes ein:

```
set access backup /home/* * *
```

Soll Zugriff auf alle Dateien in allen Verzeichnissen in und unter dem Verzeichnis `/home` erteilt werden, geben Sie Folgendes ein:

```
set access backup /home/* * *
set access backup /home/*/* * *
```

 Windows-Betriebssysteme*Dateispezifikation*
 Windows-BetriebssystemeGibt den Pfad, die Datei, das Image oder das Verzeichnis an, für den/die/das Sie dem anderen Knoten oder Benutzer Zugriff erteilen. Verwenden Sie Platzhalterzeichen, um Gruppen von Dateien oder Images oder alle Dateien in einem Verzeichnis, alle Objekte in einer Verzeichnisverzweigung oder alle Objekte in einem Laufwerk anzugeben. Platzhalterzeichen können jedoch nicht dazu verwendet werden, alle Laufwerke anzugeben. Mit einem einzelnen Stern "*" als Dateispezifikation können Sie die Zugriffsberechtigung für alle Dateien oder Images erteilen, deren Eigner Sie sind und die auf dem Server gesichert wurden. Wenn der Befehl `set access backup "*" Knoten` eingegeben wird, erfolgt keine Überprüfung auf dem Server; es wird davon ausgegangen, dass mindestens ein Objekt gesichert wurde.

Wird die Zugriffsberechtigung für eine Ebene des aktuellen Arbeitsverzeichnisses erteilt, muss nur die Ebene angegeben werden. Wird die Zugriffsberechtigung für Objekte erteilt, die sich nicht in einer Verzeichnisebene des aktuellen Arbeitsverzeichnisses befinden, müssen Sie den vollständigen Pfad angeben. Für die Dateispezifikation, für die eine Zugriffsberechtigung erteilt wurde, muss mindestens eine Sicherungsversion oder eine Archivierungskopie (Datei oder Verzeichnis) auf dem Server vorhanden sein.

Sollen alle Dateien in einem bestimmten Verzeichnis angegeben werden, geben Sie `d:\test\mine\proj1\*` in die Befehlszeile ein.

Um die Zugriffsberechtigung für alle Objekte unter einer bestimmten Ebene zu erteilen, geben Sie einen Stern, ein Verzeichnisbegrenzungszeichen und einen Stern am Ende der Dateispezifikation an. Soll beispielsweise Zugriff auf alle Objekte unter `d:\test` erteilt werden, verwenden Sie die Dateispezifikation `d:\test\*\*`.

Wichtig: Durch die Verwendung des Formats `\*\*` alleine erteilen Sie keinen Zugriff auf Objekte in dem angegebenen Verzeichnis, sondern nur auf Objekte in den Verzeichnissen unter dem angegebenen Verzeichnis.

Für das Stammverzeichnis sind die Regeln im Wesentlichen identisch. Geben Sie `\*` in einem Befehl set access und `\*\*` in einem weiteren Befehl set access an, wenn ein anderer Benutzer Zugriff auf alle Dateien und Verzeichnisse in und unter dem Stammverzeichnis haben soll. Die erste Angabe `\*` erteilt Zugriff auf alle Verzeichnisse und alle Dateien im Stammverzeichnis. Die zweite Angabe `\*` erteilt Zugriff auf alle Verzeichnisse und Dateien unter dem Stammverzeichnis.

Anmerkung:

1. Der Dateibereichsname wird verwendet, wenn sich die Laufwerkbezeichnung geändert hat.
2. Wenn Dateibereichsname angegeben wird, darf die Dateispezifikation keinen Laufwerkbuchstaben enthalten.

Beispiel:

- Ihre Verzeichnisstruktur besteht aus mehreren Ebenen: `d:\test\sub1\subsub1`.
- Das Verzeichnis `d:\test` enthält die Dateien `h1.txt` und `h2.txt`.
- Das Verzeichnis `d:\test\sub1` enthält die Datei `s1.htm`.
- Das Verzeichnis `d:\test\sub1\sub2` enthält die Datei `ss1.cpp`.

Soll Zugriff auf alle Dateien im Verzeichnis `d:\test\sub1\sub2` erteilt werden, geben Sie Folgendes ein:

```
set access backup d:\test\sub1\sub2\* * *
```

Soll Zugriff nur auf die Dateien im Verzeichnis `d:\test` erteilt werden, geben Sie Folgendes ein:

```
set access backup d:\test\* * *
```

Soll Zugriff auf alle Dateien in allen Verzeichnissen in und unter dem Verzeichnis `d:\test` erteilt werden, geben Sie Folgendes ein:

```
set access backup d:\test\* * *
set access backup d:\test\*\* * *
```

Windows-Betriebssysteme{Dateibereichsname}
Windows-BetriebssystemeGibt den in geschweiften Klammern eingeschlossenen Namen des Dateibereichs auf dem Server an, in dem sich die Dateien befinden, für die die Zugriffsberechtigung erteilt werden soll. Dieser Name ist die Laufwerkbezeichnung des Workstationlaufwerks, aus dem die Datei gesichert oder archiviert wurde. Der Dateibereichsname wird verwendet, wenn sich die Laufwerkbezeichnung geändert hat.

Image-DS
Der Name des Imagedateisystems, das gemeinsam benutzt werden soll. Durch die Angabe eines Sterns (*) wird der Zugriff auf alle Images des Eigners ermöglicht, der die Zugriffsberechtigung erteilt.

Linux-BetriebssystemeWindows-Betriebssysteme-TYPE=VM *VM-Name*
Linux-BetriebssystemeWindows-BetriebssystemeDieser Parameter ist erforderlich, wenn Sie diesen Befehl verwenden, um einem anderen Benutzer Zugriff auf Sicherungen der virtuellen VMware-Maschine zu erteilen. Die Option *VM-Name* kann nur verwendet werden, wenn -TYPE=VM angegeben wird; *VM-Name* ist der Name der virtuellen VMware-Maschine, der Sie Zugriff erteilen.

Knoten
Gibt den Clientknoten des Benutzers an, dem der Zugriff erteilt werden soll. Es können Platzhalterzeichen verwendet werden, wenn der Zugriff für mehrere Knoten mit ähnlichen Knotennamen erteilt werden soll. Mit einem Stern (*) wird allen Knoten der Zugriff erteilt.

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeBenutzer
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDieser optionale Parameter schränkt den Zugriff auf den benannten Benutzer auf dem angegebenen Knoten ein. Soll jeder berechtigte Benutzer Zugriff auf Ihre gesicherten oder archivierten Daten erhalten, geben Sie root als Benutzer an.

Beispiele

Windows-BetriebssystemeTask
Windows-BetriebssystemeDem Benutzer an node_2 die Berechtigung zum Zurückschreiben aller Dateien mit der Erweiterung `.c` aus dem Verzeichnis `c:\devel\proja` erteilen.

```
set access backup c:\devel\proja\*.c node_2
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDem Benutzer an `node_2` die Berechtigung zum Zurückschreiben der Datei `budget` aus dem Verzeichnis `/home/user` erteilen.

```
set access backup /home/user/budget node_2
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeTask
AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeDem Knoten `node_3` die Berechtigung zum Abrufen aller Dateien im Verzeichnis `/home/devel/proja` erteilen.

```
set ac archive /home/devel/proja/ node_3
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeDem Benutzer an `node_3` die Berechtigung zum Abrufen aller Dateien im Verzeichnis `c:\devel` erteilen, jedoch keinen Zugriff auf Dateien in Unterverzeichnissen von `c:\devel`, wie `c:\devel\proj`, erlauben.

```
set access archive c:\devel\* node_3
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Task
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeAllen Knoten, deren Name mit `bldgb` endet, die Berechtigung zum Zurückschreiben aller Sicherungsversionen aus Verzeichnissen mit dem Dateibereichsnamen `project` erteilen.

```
set ac b "{project}/*" "*bldgb"
```

Windows-Betriebssysteme Task
Windows-BetriebssystemeAllen Knoten, deren Name mit `bldgb` endet, die Berechtigung zum Zurückschreiben aller Sicherungsversionen aus allen Verzeichnissen auf Laufwerk `d:` erteilen. Laufwerk `d:` hat den Dateibereichsnamen `project`.

```
set ac b {project}\*\* *bldgb
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Task
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeJedem berechtigten Benutzer auf node1 die Berechtigung zum Abrufen aller Dateien im Verzeichnis /home/devel/projb erteilen.

```
set access archive /home/devel/projb/ node1 root
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-Betriebssysteme Task
AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeBenutzer serena auf `node_5` die Berechtigung zum Zurückschreiben aller Images des im Verzeichnis `/home/devel/proja` angehängten Dateibereichs erteilen.

```
set acc backup "home/devel/proja/*/*" node_5 serena
```

Linux-Betriebssysteme Windows-Betriebssysteme Task
Linux-Betriebssysteme Windows-BetriebssystemeDem Knoten myOtherNode die Berechtigung zum Zurückschreiben von Dateien erteilen, die von der virtuellen VMware-Maschine myTestVM gesichert wurden.

```
set access backup -TYPE=VM myTestVM myOtherNode
```

Set Event

Mit dem Befehl set event können Sie die Umstände für das Löschen archivierter Daten angeben.

Den Befehl set event können Sie für folgende Aktionen verwenden:

- Die Löschung von Daten am Ende ihrer zugeordneten Aufbewahrungsdauer verhindern (Löschen unzulässig)
- Den Verfall wie von der Archivierungskopiengruppe definiert zulassen (eine Löschsperre freigeben)
- Die Uhr für den Verfall starten, wenn ein bestimmtes Ereignis eintritt (den Server benachrichtigen, dass ein Ereignis eingetreten ist)

Betroffene Objekte können wie folgt angegeben werden: über eine Standarddateispezifikation (einschließlich Platzhalterzeichen), über eine Liste von Dateien, deren Namen in der mit der Option filelist angegebenen Datei stehen, oder über eine Gruppe archivierter Dateien, deren Beschreibung mit der Option description angegeben ist.

Anmerkung: Wird nur eine <Dateispezifikation> verwendet, sind alle archivierten Kopien von Dateien oder Ordnern betroffen, die mit der Dateispezifikation übereinstimmen. Wenn Sie bestimmte Versionen einer Datei berücksichtigen wollen, verwenden Sie die Option -pick und wählen Sie aus der angezeigten Liste aus.

Interaktion mit Servern einer älteren Version

Wird der Befehl set event auf einem Client mit Verbindung zu einem Server ausgegeben, der keine ereignisgesteuerten Maßnahmen unterstützt (vor IBM Spectrum Protect 5.2.2), wird der Befehl mit einer Fehlernachricht zurückgewiesen, die besagt, dass der aktuelle Server keine ereignisgesteuerten Maßnahmen unterstützt.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Syntax

```
>>-SET Event---- -TYPE=---+-Hold--------------+------------------>
                          +-Release-----------+
                          '-Activateretention-'

>-- --<Dateispezifikation>-------------------------------------->
```

```
>-- -- -filelist=<Dateispezifikation>-- -- -description=-------->

>-- -pick-------------------------------------------------------><
```

Parameter

TYPE=

Gibt die Einstellung des Ereignistyps an. Dieser Parameter muss angegeben werden.

hold

Verhindert, dass das Objekt gelöscht wird (unabhängig von der Verfallsmaßnahme).

release

Ermöglicht einen normalen ereignisgesteuerten Verfall.

activateretention

Sendet ein Signal an den Server, dass das steuernde Ereignis eingetreten ist, und startet die Uhr für den Verfall.

-pick

Stellt eine Liste von Objekten zur Verfügung, die der Benutzer auswählen kann, um das Ereignis auf sie anzuwenden.

Die folgenden Optionen können ebenfalls verwendet werden; sie dienen ihrem üblichen Zweck:

- Dateformat
- Numberformat
- Noprompt
- Subdir
- Timeformat

Beispiele

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeTask

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-BetriebssystemeDas folgende Beispiel zeigt die ausführliche Ausgabe und Statistikausgabe des Befehls set event für `set event type=hold /home/accounting/ledgers/*05.books` bei erneut gebundenen Objekten an (im Gegensatz zu archivierten oder anderen Objekten).

```
Erneut binden--> 274 /home/accounting/ledgers/
  jan05.books
Erneut binden--> 290 /home/accounting/ledgers/
  feb05.books

Gesamtzahl archivierter Objekte:             0
Gesamtzahl fehlgeschlagener Objekte:             0
Gesamtzahl erneut gebundener Objekte:        2
Gesamtzahl übertragener Byte:               0  B
Datenübertragungszeit:                          0,00 Sek.
Datenübertragungsgeschwindigkeit im Netz:       0,00 KB/Sek.
Datenübertragungsgeschwindigkeit Gesamt:  0,00 KB/Sek.
Objekte komprimiert um:                          0%
Verarbeitungszeit:                  00:00:02
```

 Windows-BetriebssystemeTask

 Windows-BetriebssystemeDas folgende Beispiel zeigt die ausführliche Ausgabe und Statistikausgabe des Befehls set event für `set event type=hold \\user\c$\tsm521\debug\bin\winnt_unicode\dsm.opt` bei erneut gebundenen Objekten an (im Gegensatz zu archivierten oder anderen Objekten).

```
Erneut binden--> 274 \\user\c$\tsm521\debug\
  bin\winnt_unicode\dsm.opt
Erneut binden--> 290 \\user\c$\tsm521\debug\
  bin\winnt_unicode\dsm.opt

Gesamtzahl geprüfter Objekte:               2
Gesamtzahl archivierter Objekte:             0
Gesamtzahl aktualisierter Objekte:               0
Gesamtzahl erneut gebundener Objekte:        2
Gesamtzahl gelöschter Objekte:                   0
Gesamtzahl verfallener Objekte:                  0
Gesamtzahl fehlgeschlagener Objekte:             0
Gesamtzahl übertragener Byte:               0  B
Datenübertragungszeit:                          0,00 Sek.
Datenübertragungsgeschwindigkeit im Netz:       0,00 KB/Sek.
```

```
Datenübertragungsgeschwindigkeit Gesamt:  0,00 KB/Sek.
Objekte komprimiert um:                       0%
Verarbeitungszeit:                  00:00:02
```

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeTask

AIX-Betriebssysteme Linux-Betriebssysteme Oracle Solaris-Betriebssysteme Mac OS X-BetriebssystemeDie Option -pick in dem 'set event'-Befehl `set event type=activate /user/tsm521/common/unix` zeigt den Ereignistyp anstelle des Befehlsnamens:

```
Fenster PICK mit Blätterfunktion - Aufbewahrungsereignis: ACTIVATE

Nr.  Archiv.-Datum/-Zeit      Dateigröße  Datei
-------------------------------------------------
1. | 05.08.2003 08:47:46        766  B   /user/tsm521
                                          /common/unix
2. | 01.08.2003 10:38:11        766  B   /user/tsm521
                                          /common/unix
3. | 05.08.2003 08:47:46       5,79 KB   /user/tsm521
                                          /common/unix
4. | 01.08.2003 10:38:11       5,79 KB   /user/tsm521
                                          /common/unix
5. | 05.08.2003 08:47:46      10,18 KB   /user/tsm521
                                          /common/unix
```

Windows-BetriebssystemeTask

Windows-BetriebssystemeDie Option -pick in dem 'set event'-Befehl `set event type=activate \user\c$\tsm521\common\winnt` zeigt den Ereignistyp anstelle des Befehlsnamens:

```
Fenster PICK mit Blätterfunktion - Aufbewahrungsereignis: ACTIVATE

Nr.  Archiv.-Datum/-Zeit      Dateigröße  Datei
-------------------------------------------------------------
1. | 05.08.2003 08:47:46        766  B   \\user\c$\tsm521
                                            \common\winnt
2. | 01.08.2003 10:38:11        766  B   \\user\c$\tsm521
                                            \common\winnt
3. | 05.08.2003 08:47:46       5,79 KB   \\user\c$\tsm521
                                            \common\winnt
4. | 01.08.2003 10:38:11       5,79 KB   \\user\c$\tsm521
                                            \common\winnt
5. | 05.08.2003 08:47:46      10,18 KB   \\user\c$\tsm521
                                            \common\winnt
```

Linux-Betriebssysteme Windows-Betriebssysteme

Set Netappsvm

Der Befehl set netappsvm ordnet die Berechtigungsnachweise für Anmeldung eines Cluster-Management-Servers, die im Befehl set password angegeben werden, einer NetApp Storage Virtual Machine und dem Daten-SVM-Namen (Data Vserver) zu (SVM = Storage Virtual Machine). Sie müssen diesen Befehl eingeben, bevor Sie eine Momentaufnahmedifferenzteilsicherung eines NetApp-Clusterdatenträgers erstellen können.

Dieser Befehl wird normalerweise nur einmal eingegeben. Die Parameter werden gespeichert und bei der nächsten Sicherung eines Clusterdatenträgers, der von der Storage Virtual Machine verwaltet wird, wiederverwendet. Wenn Sie eine Storage Virtual Machine zu einem anderen Cluster-Management-Server verschieben, müssen Sie diesen Befehl erneut eingeben und den neuen Cluster-Management-Server angeben. Falls erforderlich, ändern Sie die Berechtigungsnachweise für Anmeldung mit dem Befehl set password.

Unterstützte Clients

Linux-Betriebssysteme Dieser Befehl ist für Linux-Clients für Sichern/Archivieren gültig, die Momentaufnahmedifferenzsicherungen von Clustered Data ONTAP-C-Mode-Dateiserverdatenträgern ausführen.

Windows-Betriebssysteme Dieser Befehl ist für Windows-Clients gültig, die Momentaufnahmedifferenzsicherungen von Clustered Data ONTAP-C-Mode-Dateiserverdatenträgern ausführen.

Syntax

```
>>-SET NETAPPSVM--+-SVM-Hostname--CMS-Hostname--SVM-Name-+-----><
                  '- -remove--SVM-Hostname---------------'
```

Parameter

SVM-Hostname
Gibt für die Datenträger, die Sie schützen wollen, den Hostnamen oder die IP-Adresse der Storage Virtual Machine an, die die Datenträger und logischen Schnittstellen (LIFs) verwaltet.

CMS-Hostname
Gibt den Hostnamen oder die IP-Adresse des Cluster-Management-Servers an. Geben Sie denselben Hostnamen an, den Sie bei Verwendung des Befehls set password für die Erstellung der Berechtigungsnachweise für Anmeldung für diesen Cluster-Management-Server angegeben haben.

SVM-Name
Gibt den Namen der Daten-SVM an, die den angehängten Datenträger verwaltet. Wenden Sie sich an den NetApp SVM-Administrator, um den Namen der Daten-SVM, die der virtuellen Maschinen zugeordnet ist, zu erhalten.

-remove *SVM-Hostname*
Hebt die Zuordnung zwischen der SVM und dem Cluster-Management-Server, dem sie zuvor zugeordnet war, auf. Geben Sie einen SVM-Hostnamen an.

Sie können diesen Parameter angeben, wenn Sie eine Storage Virtual Machine versehentlich einem 7-Mode-Dateiserver zugeordnet haben. Wenn Sie einen 7-Mode-Dateiserver entfernen und anschließend einen Cluster-Management-Server zuordnen, definieren Sie die Anmeldeberechtigungsnachweise für den Cluster-Management-Server mit dem Befehl set password.

Beispiele

Die Berechtigungsnachweise und den Zugriff auf eine Storage Virtual Machine konfigurieren:

```
set netappsvm svm_example.com cms_filer1.example.com svm_2
dsmc set password cms_filer1.example.com user_name password
```

Für die Storage Virtual Machine erstellte Zuordnungen entfernen:

```
set netappsvm -remove svm_example.com
```

Zugehörige Tasks:
Clustered Data ONTAP NetApp-Dateiserverdatenträger schützen
AIX-Betriebssysteme Linux-Betriebssysteme Mac OS X-Betriebssysteme Oracle Solaris-Betriebssysteme Windows-Betriebssysteme

Set Password

Mit dem Befehl set password können Sie das IBM Spectrum Protect-Kennwort für Ihre Workstation ändern oder die Berechtigungsnachweise definieren, mit denen auf einen anderen Server zugegriffen wird.

Wenn Sie das alte und das neue Kennwort bei der Eingabe des Befehls set password weglassen, werden Sie einmal zur Eingabe des alten Kennworts und zweimal zur Eingabe des neuen Kennworts aufgefordert.

Die maximale Kennwortlänge beträgt 63 Zeichen. Kennwortbedingungen variieren, abhängig davon, wo die Kennwörter gespeichert und verwaltet werden, und abhängig von der Version des IBM Spectrum Protect-Servers, zu dem Ihr Client die Verbindung herstellt.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie einen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden
Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Bei den Kennwörtern muss die Groß-/Kleinschreibung beachtet werden. Außerdem können die Kennwörter weiteren Einschränkungen aufgrund von LDAP-Richtlinien unterliegen.

Wenn Ihr IBM Spectrum Protect-Server die Version 6.3.3 oder höher aufweist und Sie keinen LDAP-Verzeichnisserver zum Authentifizieren von Kennwörtern verwenden
Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

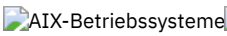
```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Kennwörter werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.

Wenn Ihr IBM Spectrum Protect-Server eine Version vor Version 6.3.3 aufweist
Verwenden Sie die folgenden Zeichen, um ein Kennwort zu erstellen:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
_ - & + .
```

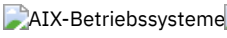
Kennwörter werden in der IBM Spectrum Protect-Serverdatenbank gespeichert. Bei diesen Kennwörtern muss die Groß-/Kleinschreibung nicht beachtet werden.


Hinweis:

Schließen Sie in der Befehlszeile alle Parameter, die mindestens ein Sonderzeichen enthalten, in Anführungszeichen ein. Ohne Anführungszeichen können die Sonderzeichen als Shell-Escapezeichen, als Dateiumleitungszeichen oder als andere Zeichen, die eine Bedeutung für das Betriebssystem haben, interpretiert werden.

Auf Windows-Systemen:
Schließen Sie die Befehlsparameter in Anführungszeichen (") ein.

Beispiel für die Befehlszeile:
```
dsmc set password "t67@#$%^&" "pass2><w0rd"
```



Auf AIX-, Linux- und Solaris-Systemen:
Schließen Sie die Befehlsparameter in Hochkommas (') ein.

Beispiel für die Befehlszeile:
```
dsmc set password -type=vmguest 'Win 2012 SQL' 'tsml2dag\administrator' '7@#$%^&7'
```

Anführungszeichen sind nicht erforderlich, wenn Sie ein Kennwort mit Sonderzeichen in einer Optionsdatei eingeben.

Unterstützte Clients

Dieser Befehl ist für alle Clients gültig.

Die folgenden Parameter gelten für VMware-Operationen, die nur verfügbar sind, wenn Sie den Client als eine Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware verwenden.

- TYPE=DOMAIN
- TYPE=VM
- TYPE=VMGUEST

Syntax

```
>>-SET Password--+--------------------------------+------------>
                 '-altes_Kennwort--neues_Kennwort-'

>--+-----------------------------------------------------+----->
   '-anderer_Server--andere_Benutzer-ID--anderes_Kennwort-'

   .-TYPE=TSM-----------.
>--+--------------------+---------------------------------------><
   +-TYPE=DOMAIN--------+
   +-TYPE=FASTBack------+
   +-TYPE=FILER---------+
   +-TYPE=VM------------+
   '-TYPE=VMGUEST ALLVM-'
```

Parameter

altes_Kennwort
Gibt das aktuelle Kennwort für die Workstation an.

neues_Kennwort
Gibt das neue Kennwort für die Workstation an.

anderer_Server andere_Benutzer-ID anderes_Kennwort
Diese drei Parameter geben die Attribute an, mit denen der Client auf einen anderen Server, wie beispielsweise einen Dateiserver oder einen ESXi-Host, zugreift.

anderer_Server
Gibt den Hostnamen oder die IP-Adresse des Servers an, auf den der Client zum Schutz von Dateien zugreifen kann.

andere_Benutzer-ID
Die Benutzer-ID eines Kontos auf dem Server, mit der sich der Client bei dem anderen Server anmeldet. Das Konto muss über die erforderlichen Berechtigungen für die Operationen verfügen, die ausgeführt werden, sobald der Benutzer am anderen Server angemeldet ist.

anderes_Kennwort

Das Kennwort, das der Benutzer-ID auf dem anderen Server zugeordnet ist.

TYPE

Gibt an, ob dieses Kennwort für den Client für Sichern/Archivieren oder für einen anderen Servertyp gilt.

Verwenden Sie `TYPE=TSM`, um das Kennwort für Ihren Client für Sichern/Archivieren anzugeben. Der Standardtyp ist `TYPE=TSM`.

 Mit `TYPE=DOMAIN` können Sie die Berechtigungsnachweise des Windows-Domänenadministrators definieren, um Benutzern die Anmeldung bei einem fernen Windows-Proxy-Knoten (die Dateizurückschreibungsschnittstelle) zur Ausführung von Dateizurückschreibungsoperationen zu ermöglichen. Diese Option erfordert eine Lizenz für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.
Verwenden Sie für den Befehl set password -type=domain das folgende Format:

```
set password -type=domain -validate Administratorname Kennwort
```

Hierbei gilt Folgendes:

VALidate
: Prüft die Berechtigungsnachweise des Windows-Domänenadministrators, bevor sie gespeichert werden. . Wenn die Überprüfung fehlschlägt, werden die Berechtigungsnachweise nicht gespeichert und Benutzer können sich nicht bei der Dateizurückschreibungsschnittstelle anmelden. Der Parameter validate ist nur in Verbindung mit dem Parameter `TYPE=DOMAIN` gültig.

Administratorname
: Gibt den Kontonamen eines Domänenadministrators an. Der Kontoname muss den Windows-Domänennamen und die Administrator-ID enthalten. Der Kontoname muss das folgende Format haben:

  ```
  Domänenname\Administrator-ID
  ```

Kennwort
: Gibt das Kennwort an, das dem angegebenen Domänenadministratorkonto zugeordnet ist.

Weitere Informationen zu den Konfigurationsvoraussetzungen für ferne Mount-Proxy-Knoten finden Sie in der IBM Spectrum Protect for Virtual Environments: Data Protection for VMware-Dokumentation.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Verwenden Sie `TYPE=FastBack` auf Linux- und Windows-Clients, um die Tivoli Storage Manager FastBack-Berechtigungsnachweise zu speichern, die für das Bereitstellen und das Aufheben der Bereitstellung der FastBack-Datenträger auf dem Windows FastBack Disaster Recovery Hub-Server erforderlich sind.

Die Kennwortdatei auf dem vStorage-Sicherungsserver muss entweder über die Windows-Administrator-ID für das VMware Virtual Center-System oder über die UNIX-Benutzer-ID für einen bestimmten ESX-Server verfügen. Für eine Proxy-Sicherung für FastBack muss die Kennwortdatei die FastBack-Administrator-ID und das zugehörige Kennwort enthalten. Hier einige Beispiele:

```
dsmc set password 192.0.2.24 admin admin 123 -type=fastback

dsmc set password 192.0.2.24 WORKGROUP:admin admin 123 -type=fastback

dsmc set password windserv administrator windpass4 -type=fastback
```

Wichtig: Sie müssen die Benutzerberechtigungsnachweise, die für das Bereitstellen und das Aufheben der Bereitstellung von FastBack-Datenträgern in einem Repository erforderlich sind, für den Client für Sichern/Archivieren definieren, bevor Sie den FastBack-Unterbefehl für die Sicherung/Archivierung eingeben. Verwenden Sie die Option fbserver zum Definieren der Berechtigungsnachweise.
Es folgt eine Kurzbeschreibung der verschiedenen Konfigurationen und der erforderlichen Berechtigungsnachweise:

- Der Client für Sichern/Archivieren ist auf einem dedizierten vStorage-Sicherungsserver installiert. Der Client auf dem vStorage-Sicherungsserver muss eine Verbindung zu mehreren gemeinsam genutzten Repositorys im Netz herstellen.

Führen Sie die folgenden Schritte für jedes der gemeinsam genutzten Repositorys im Netz aus, mit denen der Client verbunden ist:

1. Konfigurieren Sie das Repository mit FastBack Manager für den fernen Netzzugriff. Siehe die Tivoli Storage Manager FastBack-Produktdokumentation im IBM® Knowledge Center unter http://www.ibm.com/support/knowledgecenter/SS9NU9/welcome.

   Bei dieser Prozedur wird ein Domänenname und eine Benutzer-ID sowie ein Kennwort für die gemeinsame Nutzung im Netz erstellt, sodass eine ferne Verbindung zu dem Repository hergestellt werden kann.

2. Geben Sie auf der Workstation des Clients für Sichern/Archivieren manuell den folgenden Befehl ein:

   ```
   dsmc set password type=fastback FBServer Domäne:Benutzer-ID_für_Netzzugriff
      Kennwort_für_Netzzugriff
   ```

   Die Option fbserver gibt den kurzen Hostnamen der FastBack-Server-Workstation an. Für den FastBack DR Hub gibt die Option fbserver den Kurznamen der Workstation an, auf der der DR Hub installiert ist.

   Benutzer-ID_für_Netzzugriff ist entweder die Windows-Administrator-ID oder das FastBack-Verwaltungskennwort.

Domäne ist der Domänenname der Benutzer-ID.

Kennwort_für_Netzzugriff ist entweder die Windows-Administrator-ID oder das FastBack-Verwaltungskennwort.

3. Diese Berechtigungsnachweise werden auf der Basis des kurzen Hostnamens abgerufen, den Sie mit der Option fbserver angeben.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Verwenden Sie `TYPE=FILER` auf Linux- und Windows-Systemen, um anzugeben, dass dieses Kennwort für Momentaufnahmedifferenzoperationen auf einem Dateiserver gilt.

Bei `TYPE=FILER` müssen Sie den Namen des Dateiservers sowie die Benutzer-ID und das Kennwort angeben, mit denen auf den Dateiserver zugegriffen wird. Beispiel: `dsmc set password -type=filer myfiler filerid filerpasswd`.

Wenn Sie `TYPE=FILER` angeben, wird das Kennwort in der Kennwortdatei (TSM.sth) gespeichert, ohne zu überprüfen, ob das Kennwort gültig ist. Kennwörter, die mit `TYPE=FILER` gespeichert wurden, können von mehreren Clientknoten gemeinsam genutzt werden. Ein von Knoten NODE_A gespeichertes Kennwort kann beispielsweise von NODE_B verwendet werden. Für jeden Dateiserver wird nur ein Satz Berechtigungsnachweise gespeichert.

 Linux-Betriebssysteme  Windows-Betriebssysteme

Verwenden Sie `TYPE=VM`, um ein Kennwort zu definieren, das für die Anmeldung bei einem ESX- oder vCenter-Server verwendet wird.

```
dsmc SET PASSWORD -type=VM Hostname Administrator Kennwort
```

Hierbei gilt Folgendes:

Hostname
: Gibt den VMware VirtualCenter- oder ESX-Server an, der gesichert, zurückgeschrieben oder abgefragt werden soll. Dieser Hostname muss der in der Option vmchost verwendeten Hostnamenssyntax entsprechen. Das heißt, wenn in vmchost kein Hostname, sondern eine IP-Adresse verwendet wird, muss in diesem Befehl die IP-Adresse und kein kurzer Hostname und kein vollständig qualifizierter Hostname angegeben werden.

Administrator
: Gibt das für die Anmeldung beim ESXi-Host benötigte Konto an.

Kennwort
: Gibt das Kennwort an, das dem Anmeldekonto zugeordnet ist, das Sie für den vCenter- oder ESXi-Administrator angegeben haben.

  Verwenden Sie den Profileditor, um die Optionen vmchost, vmcuser und vmcpw zu definieren.

  Sie können die Option vmchost auch in der Clientoptionsdatei definieren und anschließend mit dem Befehl set password diesen Hostnamen dem Administratorkonto und dem Kennwort des Administratorkontos zuordnen, mit denen die Anmeldung bei diesem Host ausgeführt wird. Beispiel: `set password TYPE=VM myvmchost.example.com Administratorname Administratorkennwort`.

 Linux-Betriebssysteme  Windows-Betriebssysteme
Verwenden Sie `TYPE=VMGUEST` auf Linux- und Windows-Clients, wenn Sie die Option INCLUDE.VMTSMVSS zum Schutz einer virtuellen Maschine verwenden. Verwenden Sie für den Befehl set password das folgende Format:

```
set password -type=vmguest VM-Gastmaschine Administrator Kennwort
```

Hierbei gilt Folgendes:

VM-Gastmaschine
: Gibt den Namen der virtuellen Gastmaschine an, die Sie schützen wollen.

Administrator
: Gibt das für die Anmeldung bei der VM-Gastmaschine benötigte Konto an.

Kennwort
: Gibt das Kennwort an, das dem Anmeldekonto zugeordnet ist.

Wenn Sie sich bei mehreren virtuellen Maschinen, die durch die Option INCLUDE.VMTSMVSS geschützt werden, mit denselben Berechtigungsnachweisen anmelden, können Sie das Kennwort für alle virtuellen Maschinen durch Angabe des Parameters ALLVM definieren. Der Parameter ALLVM bewirkt, dass bei der Anmeldung des Clients bei jeder Gastmaschine, die in einer Option INCLUDE.VMTSMVSS enthalten ist, dieselben Berechtigungsnachweise verwendet werden. Der folgende Befehl ist ein Beispiel für die Verwendung von ALLVM. In diesem Beispiel werden der Benutzername "Administrator" und das Kennwort "Password" für die Anmeldung bei jeder virtuellen Maschine verwendet, die Sie in einer Option INCLUDE.VMTSMVSS angegeben haben:

```
set password -type=vmguest ALLVM Administrator Password
```

Sie können auch eine Kombination aus gemeinsam genutzten und individuellen Berechtigungsnachweisen definieren. Wenn beispielsweise die meisten virtuellen Maschinen in Ihrer Umgebung dieselben Berechtigungsnachweise verwenden, aber einige virtuelle Maschinen andere Berechtigungsnachweise verwenden, können Sie mehrere Befehle set password verwenden, um die Berechtigungsnachweise anzugeben. Beispiel: Angenommen, die meisten virtuellen Maschinen verwenden "Administrator1" als Anmeldenamen und "Password1" als Kennwort. Außerdem wird angenommen, dass eine virtuelle Maschine mit dem Namen VM2

"Administrator2" als Anmeldename und "Password2" als Kennwort verwendet. Die folgenden Befehle werden verwendet, um die Berechtigungsnachweise für dieses Szenario zu definieren:

- `set password -type=vmguest ALLVM Administrator1 Password1` (definiert die Berechtigungsnachweise für die meisten virtuellen Maschinen).
- `set password -type=vmguest VM2 Administrator2 Password2` (definiert eindeutige Berechtigungsnachweise für VM2).

Beispiele

Bei den folgenden Beispielen wird der Befehl set password verwendet.

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeWindows-Betriebssysteme
Task

AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-Betriebssysteme
Windows-BetriebssystemeDas Kennwort von `osecret` in `nsecret` ändern.

```
set password osecret nsecret
```

 AIX-Betriebssysteme  Linux-Betriebssysteme  Oracle Solaris-Betriebssysteme  Mac OS X-Betriebssysteme  Windows-Betriebssysteme
Task

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Windows-BetriebssystemeEine Benutzer-ID und ein Kennwort für den Root auf dem Dateiserver `myFiler.example.com` definieren.

```
dsmc set password -type=filer myFiler.example.com root
```

```
Bitte Kennwort für Benutzer-ID "root@myFiler.example.com" eingeben: ******** Zur Bestätigung das Kennwort
erneut eingeben: ******** ANS0302I Erfolgreich ausgeführt.
```

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-BetriebssystemeWindows-Betriebssysteme
Task

AIX-BetriebssystemeLinux-BetriebssystemeOracle Solaris-BetriebssystemeMac OS X-Betriebssysteme
Windows-BetriebssystemeEine Benutzer-ID und ein Kennwort für den Root auf dem Dateiserver `myFiler.example.com` definieren.

```
dsmc set password -type=filer myFiler.example.com root secret
```

Linux-BetriebssystemeWindows-BetriebssystemeTask
Linux-BetriebssystemeWindows-BetriebssystemeEine Benutzer-ID und ein Kennwort für den FastBack-Server `myFastBackServer` definieren. Verwenden Sie die Option -fbserver in den Befehlen archive fastback und backup fastback für den Servernamen.

Linux-Betriebssystemedsmc set password -type=FASTBack myFastBackServer myUserId 'pa$sword'
Windows-Betriebssystemedsmc set password -type=FASTBack myFastBackServer myUserId "pa$sword"

Wichtig:

1. Der Befehl `dsmc set password -type=fastback` muss auf einer dedizierten Client-Proxy-Workstation für jedes FastBack-Repository, zu dem der Client für Sichern/Archivieren eine Verbindung herstellen soll, einmal wiederholt werden.
2. Für gemeinsam genutzte Repositorys im Netz geben Sie den Befehl `dsmc set password -type=fastback` im folgenden Format aus: `dsmc set password -type=fastback myFBServer domainName:userId password`.

   Der angegebene Servername, `myFBServer` in diesem Beispiel, muss mit dem Namen übereinstimmen, der in der Option -fbserver in einem Befehl backup fastback oder archive fastback angegeben wird.

3. Für den FastBack-Server oder den FastBack Disaster Recovery Hub muss die angegebene Benutzer-ID mit dem zugehörigen Kennwort über FastBack-Administratorberechtigungen verfügen. Sie müssen den Befehl `dsmc set password -type=fastback` einmal für jedes Repository einer Filiale des FastBack-Servers auf dem FastBack DR Hub ausgeben, zu dem der Client für Sichern/Archivieren eine Verbindung herstellen soll.

Linux-BetriebssystemeTask
Linux-BetriebssystemeDer Client für Sichern/Archivieren stellt eine Verbindung zu dem FastBack-Server-Repository mit dem kurzen Hostnamen `myFBServer` her. `USERID` ist die FastBack-Netzbenutzer-ID, die über Schreib-/Lesezugriff auf die Repository-Freigabe verfügt. `DOMAIN` ist die Domäne, zu der die Benutzer-ID gehört. `myNetworkPass` ist das entsprechende Kennwort für die Benutzer-ID.

```
dsmc set password -type=fastback myFbServer DOMAIN:USERID myNetworkPass
```

Linux-BetriebssystemeTask
Linux-BetriebssystemeDer Client für Sichern/Archivieren stellt eine Verbindung zu einem Repository auf einer DR Hub-Maschine mit dem kurzen Hostnamen `myFbDrHub` her. Die Benutzer-ID ist die Windows-Administrator-ID. `DOMAIN` ist die Domäne, zu der die DR Hub-Maschine gehört. `myNetworkPass` ist das entsprechende Kennwort für die Administrator-ID.

```
dsmc set password -type=fastback myFbDrHub DOMAIN:administrator adminPasswd
```

Windows-BetriebssystemeTask
Windows-BetriebssystemeDie Berechtigungsnachweise des Windows-Domänenadministrators, die Benutzer für die Anmeldung bei der Dateizurückschreibungsschnittstelle benötigen, definieren und die Windows-Domänenberechtigungsnachweise speichern. In diesem

Beispiel hat die Windows-Domäne, in der alle Benutzerkonten registriert werden, den Namen `example_domain`. `Kev_the_admin` ist die ID des Windows-Domänenadministrators und `pas$word!` ist das entsprechende Kennwort für den Administrator.

```
dsmc set password -type=domain -val "example_domain\Kev_the_admin" "pas$word!"
```

 Linux-Betriebssysteme  Windows-Betriebssysteme

Set vmtags

Mit dem Befehl set vmtags werden Datenschutztags und Kategorien erstellt, die VMware-Bestandsobjekten hinzugefügt werden können. Sie können IBM Spectrum Protect-Sicherungen virtueller Maschinen in diesen VMware-Objekten verwalten, indem Sie die Tags mit Tools wie beispielsweise VMware vSphere PowerCLI Version 5.5 R2 oder höher angeben.

 Dieses Feature ist nur verfügbar, wenn der Client als Einheit zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware ausgeführt wird.

Wenn Sie das IBM Spectrum Protect vSphere-Client-Plug-in zum Verwalten von Sicherungen verwenden, müssen Sie nicht zuerst den Befehl set vmtags ausführen. Die Tags und Kategorien werden für Sie erstellt.

Wenn Sie Scripts schreiben, um diese Tags auf VMware-Bestandsobjekte anzuwenden, müssen Sie den Befehl set vmtags nur einmal ausgeben, damit Datenschutztags erstellt werden, bevor sie dem VMware-Bestand hinzugefügt werden.

Sie können Sicherungen virtueller Maschinen auf den folgenden VMware-Bestandsobjektebenen verwalten:

- Datencenter
- Ordner (Ordner 'Host' und 'Cluster' sowie Ordner 'VM' und 'Schablone')
- Host
- Host-Cluster
- Ressourcenpool
- Virtuelle Maschine

Die Liste der unterstützten Tags finden Sie in "Unterstützte Datenschutztags".

Bei Tags, die sich auf Zeitpläne beziehen, müssen sich die virtuellen Maschinen in einer Schutzgruppe befinden, die durch einen Zeitplan geschützt wird. Eine Schutzgruppe besteht aus den virtuellen Maschinen in einem Container, denen der Tag `Schedule (IBM Spectrum Protect)` zugeordnet ist.

Nach der Ausführung des Befehls set vmtags können Sie die Tags VMware-Objekten zuordnen, um den Schutz virtueller Maschinen zu steuern. Sie können beispielsweise virtuelle Maschinen in Services für geplante Sicherungen einschließen oder von ihnen ausschließen, die Aufbewahrungsmaßnahme für Sicherungen angeben, die Datenkonsistenz von Momentaufnahmen festlegen oder die zu schützenden Platten der virtuellen Maschinen auswählen.

Wenn die Datenschutztags bereits vorhanden sind, werden die Tags bei der Ausführung des Befehls set vmtags nicht erneut erstellt.

Wenn Sie einen Upgrade von einer Vorgängerversion der Einheit zum Versetzen von Daten durchführen, werden bei der erneuten Ausführung des Befehls set vmtags alle neuen Tags erstellt, die in der neuen Version der Einheit zum Versetzen von Daten verfügbar sind.

Voraussetzungen: Bevor Sie den Befehl set vmtags ausführen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der VMware vCenter-Server muss über Version 6.0 Update 1 oder eine höhere Version verfügen.
- Die Option vmchost muss in der Datei dsm.opt auf Windows-Einheiten zum Versetzen von Daten oder in der Datei dsm.sys auf Linux-Einheiten zum Versetzen von Daten konfiguriert werden. Der Benutzername und das Kennwort, die dem Wert für vmchost zugeordnet sind, müssen ebenfalls definiert werden. Falls noch nicht definiert, können Sie den Befehl dsmc set password verwenden, um den Benutzernamen und das Kennwort zu definieren.

Unterstützte Clients

 LinuxBetriebssystemeDieser Befehl ist nur auf unterstützten Linux x86_64-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind, der VMware-Assets schützt.

 WindowsBetriebssystemeDieser Befehl ist auf unterstützten Windows 64-Bit-Clients gültig, die auf einem vStorage-Sicherungsserver installiert sind, der VMware-Assets schützt.

Syntax

```
>>-SET VMTAGS-------------------------------------------------><
```

Parameter

Für diesen Befehl sind keine Parameter erforderlich.

Beispiele

Task

Erstellung von Datenschutztags und Kategorien, die VMware-Bestandsobjekten hinzugefügt werden können:

```
dsmc set vmtags
```

- Linux-BetriebssystemeWindows-BetriebssystemeÜbersicht über das Datenschutztagging
  Um den Datenschutz für virtuelle Maschinen zu verwalten, können Sie VMware-Bestandsobjekten IBM Spectrum Protect-Tags zuordnen. Sie können VMware-Objekten Tags zuordnen, indem Sie Datenschutzeinstellungen im IBM Spectrum Protect vSphere-Client-Plug-in des vSphere-Web-Clients angeben. Wenn Sie das IBM Spectrum Protect vSphere-Client-Plug-in nicht verwenden, können Sie Tags mithilfe von Scripting-Tools wie VMware Power CLI zuordnen.

Zugehörige Konzepte:
Verwaltungsklassen und Kopiengruppen
Zugehörige Verweise:
Unterstützte Datenschutztags
Vmchost
Vmtagdatamover
Set Password
Windows-Betriebssysteme

IBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service

Die folgenden Client-Services können installiert werden, wenn Sie den Client für Sichern/Archivieren installieren oder das IBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service nach der Installation des Clients für Sichern/Archivieren verwenden:

- Scheduler für Sichern/Archivieren
- Clientakzeptor
- Ferner Clientagent
- Journalsteuerkomponente

Weitere Informationen zur Verwendung des IBM Spectrum Protect-Konfigurationsdienstprogramms für den Client-Service für die Installation von Client-Services finden Sie in den zugehörigen Informationen zur Verwendung des Befehls dsmcutil.

- Windows-BetriebssystemeService 'Scheduler für Sichern/Archivieren' installieren
  Sie können entweder die GUI des Clients für Sichern/Archivieren oder das IBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service verwenden, um den Scheduler zu installieren.
- Windows-BetriebssystemeBefehl dsmcutil
  Mit dem IBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service, dsmcutil, können Services des Clients für Sichern/Archivieren auf lokalen und fernen Windows-Workstations installiert werden.

Zugehörige Konzepte:
Befehl dsmcutil
Windows-Betriebssysteme

Service 'Scheduler für Sichern/Archivieren' installieren

Sie können entweder die GUI des Clients für Sichern/Archivieren oder das IBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service verwenden, um den Scheduler zu installieren.

Informationen zu diesem Vorgang

- Klicken Sie in der GUI des Clients für Sichern/Archivieren auf Dienstprogramme und dann auf Setup-Assistent. Wählen Sie die Option Hilfe zum Konfigurieren des Client-Schedulers aus.
- Wenn Sie über ein Konto verfügen, das zur Gruppe 'Administratoren/Domänen-Admins' gehört, können Sie das IBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service verwenden, um Client-Services sowohl auf lokalen als auch auf fernen Windows-Workstations zu konfigurieren.

- Windows-BetriebssystemeKonfigurationsdienstprogramm für den Client-Service verwenden (Windows)
  In diesem Abschnitt werden die Schritte bereitgestellt, die Sie ausführen müssen, um mit dem Konfigurationsdienstprogramm für den Client-Service Sicherungen zu automatisieren, vorhandene Scheduler-Services zu verwalten, einen neuen Scheduler zu erstellen und einen Clientakzeptor für die Verwaltung des Schedulers zuzuordnen.

Windows-Betriebssysteme

Befehl dsmcutil

Mit dem IBM Spectrum Protect-Konfigurationsdienstprogramm für den Client-Service, dsmcutil, können Services des Clients für Sichern/Archivieren auf lokalen und fernen Windows-Workstations installiert werden.

Mit dem Befehl dsmcutil können Sie die folgenden Client-Services installieren:

- Scheduler für Sichern/Archivieren
- Clientakzeptor
- Ferner Clientagent
- Journalsteuerkomponente

Das Konfigurationsdienstprogramm für den Client-Service muss von einem Konto ausgeführt werden, das zur Gruppe 'Administratoren/Domänen-Admins' gehört. Die Syntax des Befehls sieht wie folgt aus:

```
                          .-SCHEDuler---.
>>-dsmcutil-- --Befehl--+-Service-----+------------------------><
                        +-CAD---------+
                        +-JOURnal-----+
                        '-REMOTEagent-'
```

Anmerkung: Die mit dsmcutil-Befehlen angegebenen Optionen überschreiben die Optionen, die Sie in Ihrer Optionsdatei (dsm.opt) angeben.

Das Konto, das das Dienstprogramm ausführt, muss über geeignete Benutzerberechtigungen für die Installation von Services und die Aktualisierung der Windows-Registrierung auf der Zielworkstation verfügen.

Wird eine ferne Workstation angegeben, muss das Konto dazu berechtigt sein, eine Verbindung zu der Windows-Registrierung der angegebenen Workstation herzustellen.

Anmerkung: Für die hier aufgeführten Befehle und Optionen steht die Mindestabkürzung, die Sie eingeben können, in Großbuchstaben.

- Windows-BetriebssystemeDsmcutil-Befehle: Erforderliche Optionen und Beispiele
  Dieser Abschnitt enthält Referenzinformationen für die dsmcutil-Befehle und Beispiele.
- Windows-BetriebssystemeGültige dsmcutil-Optionen
  In diesem Abschnitt sind die gültigen **dsmcutil**-Optionen aufgelistet, die Sie bei der Verwendung des Scheduler-Service angeben können.

Zugehörige Konzepte:
IBM Spectrum Protect-Client konfigurieren
Windows-Betriebssysteme

Dsmcutil-Befehle: Erforderliche Optionen und Beispiele

Dieser Abschnitt enthält Referenzinformationen für die dsmcutil-Befehle und Beispiele.

Mit dem Befehl INSTall werden Services des Clients für Sichern/Archivieren installiert und konfiguriert.

INSTall Scheduler

Installiert und konfiguriert den IBM Spectrum Protect-Scheduler-Service.

Die folgenden Optionen sind für den Befehl INSTall erforderlich:

- /name:*Servicename*
- /password:*Kennwort*
- /clusternode:Yes | No (erforderlich, falls Microsoft Cluster Server (MSCS) oder Veritas Cluster Server (VCS) ausgeführt wird)
- /clustername:*Clustername* (erforderlich, falls MSCS oder VCS ausgeführt wird)

Einschränkung: Geben Sie keinen Clusternamen mit mehr als 64 Zeichen an. Wenn Sie mehr als 64 Zeichen angeben und Veritas Storage Foundation mit hoher Verfügbarkeit oder eine Microsoft Cluster Server-Konfiguration verwenden, können Sie den Scheduler-Service möglicherweise nicht installieren oder starten.

Die Option /clientdir:*Clientverzeichnis* kann ebenfalls verwendet werden; Standardwert ist das aktuelle Verzeichnis.

Die folgenden Dateien müssen in dem durch *Clientverzeichnis* angegebenen Verzeichnis vorhanden sein:

- dsmcsvc.exe
- dscdeu.txt
- dsm.opt
- dsmntapi.dll
- tsmutil1.dll

Anmerkung: Wenn der Service auf einer fernen Workstation installiert wird, sollte der vollständig qualifizierte Clientverzeichnispfad relativ zur Zielworkstation angegeben werden. UNC-Namen sind für das lokale Systemkonto nicht zulässig. Auf einer Workstation können mehrere Services

installiert werden.
Tipp: In den Befehlen, die in den folgenden Beispielen angegeben werden, wird das Standardverzeichnis des Clientinstallationsprogramms (C:\program files\tivoli\tsm\baclient) verwendet. Wenn Sie den Client in einem anderen Verzeichnis installiert haben, müssen Sie den Standardpfad durch Ihren angepassten Installationspfad ersetzen. Wenn der Pfad ein Leerzeichen enthält, muss er in Anführungszeichen eingeschlossen werden (z. B. "C:\program files\tivoli\tsm\baclient").

Task
: Einen Scheduler-Service mit dem Namen `Zentraler TSM-Scheduler` auf der lokalen Workstation installieren. Der Service soll automatisch beim Systemstart gestartet werden. Alle erforderlichen Dateien müssen sich im aktuellen Verzeichnis befinden und die Clientoptionsdatei muss auf den IBM Spectrum Protect-Server verweisen, auf dem Knoten ALPHA1 mit dem Kennwort `nodepw` definiert ist. Der Server wird kontaktiert, um zu prüfen, ob der angegebene Knoten und das zugehörige Kennwort gültig sind. Wenn das Kennwort auf seine Gültigkeit hin überprüft wurde, wird es im Kennwortspeicher generiert (verschlüsselt):
Befehl:

```
dsmcutil install scheduler /name:"Zentraler TSM-Scheduler"
/node:ALPHA1 /password:Knotenkennwort /autostart:yes
```

Task
: Einen Scheduler-Service mit dem Namen `Zentraler TSM-Scheduler` auf der fernen Workstation PDC installieren. Der Service soll automatisch beim Systemstart gestartet werden. Die erforderlichen Dateien für den Scheduler-Service und die angegebene Optionsdatei müssen sich auf der fernen Workstation im Verzeichnis `C:\program files\tivoli\tsm\baclient` befinden. Das Kennwort wird verschlüsselt in den Kennwortspeicher aufgenommen. Der IBM Spectrum Protect-Server wird nicht kontaktiert, um das Kennwort zu prüfen.
Befehl:

```
dsmcutil install scheduler /name:"Zentraler TSM-Scheduler"
/machine:PDC /clientdir:"c:\program files\tivoli\tsm\baclient"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
/node:PDC /validate:no /autostart:yes /password:nodepassword
```

Task
: Einen Scheduler-Service mit dem Namen `Zentraler TSM-Scheduler` auf der fernen Workstation PDC installieren. Der Service soll automatisch beim Systemstart gestartet werden. Die erforderlichen Dateien für den Scheduler-Service und die angegebene Optionsdatei müssen sich auf der fernen Workstation im Verzeichnis `C:\program files\tivoli\tsm\baclient` befinden. Das Kennwort wird verschlüsselt in den Kennwortspeicher aufgenommen. Der IBM Spectrum Protect-Server, der sich am angegebenen TCP/IP-Host und -Anschluss befindet, wird kontaktiert, um das Kennwort auf seine Gültigkeit hin zu überprüfen.
Befehl:

```
dsmcutil install scheduler /name:"Zentraler TSM-Scheduler"
/machine:PDC /clientdir:"c:\program files\tivoli\tsm\baclient"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
/node:PDC /autostart:yes /password:Knotenkennwort
/commmethod:tcpip /commserver:alpha1.example.com
/commport:1521
```

Task
: Den Service `Zentraler TSM-Scheduler` auf einem einzigen Knoten in einem MSCS- oder VCS-Cluster installieren. Stellen Sie für *group-a* von Workstation *node-1* aus sicher, dass *node-1* derzeit Eigner von *group-a* ist, und geben Sie dann den folgenden Befehl aus.

  Befehl:

  Befehl:

```
dsmcutil install scheduler /name:"Zentraler TSM-Scheduler:
group-a" /clientdir:"c:\program files\tivoli\tsm\baclient"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
/node:mscs-cluster-group-a /password:n
/validate:no /autostart:yes /startnow:yes
/clusternode:yes /clustername:mscs-cluster
```

INSTall CAD

Installiert und konfiguriert den Clientakzeptorservice. Erforderliche Optionen sind:

- /name:*Servicename*
- /node:*Knotenname*
- /password:*Kennwort*

Andere gültige Optionen sind:

- /optfile:*Optionsdatei*
- /httpport:*HTTP-Anschluss*
- /webports:*Webanschlüsse*

Task

Einen Clientakzeptorservice mit dem Namen `TSM CAD` installieren. Der Clientakzeptor verwendet den Knoten *test*, um die Verbindung zum IBM Spectrum Protect-Server herzustellen. Verwenden Sie die Optionsdatei `c:\program files\tivoli\tsm\baclient\dsm.opt`, um die Verbindung zum Server herzustellen.
Befehl:

```
dsmcutil install cad /name:"TSM-CAD" /node:test /password:test
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
```

INSTall Journal

Installiert einen Journalsteuerkomponentenservice auf allen Windows-Clients. Es wird eine Journaldatenbank erstellt, in der die Informationen gespeichert werden, anhand derer der Client vor Beginn einer Operation festlegt, welche Dateien für die Sicherung auswählbar sind.

Sie können gegebenenfalls die Option nojournal im Befehl incremental verwenden, um anzugeben, dass Sie eine traditionelle vollständige Teilsicherung ausführen wollen.

Der Journalsteuerkomponentenservice hat den Namen `TSM-Journalservice` und verwendet die Konfigurationsdatei `tsmjbbd.ini` aus dem Installationsverzeichnis des Clients für Sichern/Archivieren.

Anmerkung: Der Journalservice wird in einer Microsoft Cluster Server-Umgebung unterstützt. Es können mehrere Journalservices installiert werden, indem mithilfe der Journalkonfigurationseinstellung JournalPipe und den Clientoptionen eindeutige Pipenamen angegeben werden.

Für diesen Befehl stehen keine Optionen zur Verfügung.

Task
Journalsteuerkomponentenservice (`TSM-Journalservice`) installieren.
Befehl:

```
dsmcutil install journal
```

INSTall REMOTEAgent

Installiert und konfiguriert einen Service 'Ferner Clientagent'. Erforderliche Optionen sind:

- /name:*Servicename*
- /node:*Knotenname*
- /password:*Kennwort*
- /partnername:*Partnerservicename*

Andere gültige Optionen sind:

- /optfile:*Optionsdatei*

Task
Einen fernen Clientagentenservice mit dem Namen `TSM AGENT` installieren. Der ferne Clientagent verwendet den Knoten *test*, um die Verbindung zum IBM Spectrum Protect-Server herzustellen. Die Optionsdatei C:\program files\tivoli\tsm\baclient\dsm.opt wird zum Herstellen der Verbindung verwendet. Der Partnerclientakzeptorservice hat den Namen `TSM-CAD`.
Befehl:

```
dsmcutil install remoteagent /name:"TSM-AGENT" /node:test
/password:test /optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
/partnername:"TSM-CAD"
```

Anmerkung: Sowohl der Agentenservice für den fernen Client als auch der Clientakzeptorservice muss so installiert sein, dass er den Web-Client ausführt. Der Clientakzeptorservice muss vor dem Agentenservice für den fernen Client installiert werden. Geben Sie den Namen des Partnerclientakzeptorservice über die Option /partnername: an.

REMove

Entfernt einen installierten Client-Service. Die erforderliche Option ist /name:*Servicename*.

Task
Den angegebenen Scheduler-Service aus der lokalen Workstation entfernen.
Befehl:

```
dsmcutil remove /name:"Zentraler TSM-Scheduler"
```

Task
Den Journalsteuerkomponentenservice (TSM-Journalservice) von der lokalen Workstation entfernen.
Befehl:

```
dsmcutil remove /name:"TSM-Journalservice"
```

UPDate

Aktualisiert die Registrierungswerte für den Scheduler-Service. Für diesen Befehl ist die Option /name:*Servicename* erforderlich; außerdem müssen die zu aktualisierenden Registrierungswerte angegeben werden. Andere gültige Optionen sind:

- /clientdir:*Clientverzeichnis*
- /optfile::*Optionsdatei*
- /eventlogging:Yes | No
- /node:*Knotenname*
- /autostart:Yes | No
- /clusternode:Yes | No (erforderlich, falls MSCS oder VCS ausgeführt wird)
- /clustername:*Clustername* (erforderlich, falls MSCS oder VCS ausgeführt wird)

Task

Clientverzeichnis und Optionsdatei für den angegebenen Scheduler-Service aktualisieren. Alle erforderlichen Client-Servicedateien müssen sich im angegebenen Verzeichnis befinden.
Anmerkung: Die Übertragungsoptionen, die in diesem dsmcutil-Befehl angegeben werden, haben Vorrang vor den Optionen in der Clientoptionsdatei.
Befehl:

```
dsmcutil update /name:"Zentraler TSM-Scheduler"
/clientdir:"c:\program files\tivoli\tsm\baclient"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
```

Task

Angegebenen Scheduler-Service so aktualisieren, dass er das TCP/IP-Protokoll verwendet, um eine Verbindung zu dem IBM Spectrum Protect-Server mit dem angegebenen Hostnamen an dem angegebenen Anschluss herzustellen.
Befehl:

```
dsmcutil update /name:"Zentraler TSM-Scheduler"
/commserver:nt1.example.com /commport:1521 /commmethod:
tcpip
```

UPDate CAD

Aktualisiert die Registrierungswerte für den Clientakzeptorservice. Für diesen Befehl ist die Option /name:*Servicename* erforderlich; außerdem müssen die zu aktualisierenden Registrierungswerte angegeben werden. Andere gültige Optionen sind:

- /node:*Knotenname*
- /password:*Kennwort*
- /optfile:*Optionsdatei*
- /httpport:*HTTP-Anschluss*
- /webports:*Webanschlüsse*
- /cadschedname:*Schedulername*

Task

Clientakzeptorservice so aktualisieren, dass er das angegebene Clientkennwort und die angegebene Optionsdatei verwendet. Alle erforderlichen Client-Servicedateien müssen sich im angegebenen Verzeichnis befinden.
Befehl:

```
dsmcutil update cad /name:"TSM-CAD" /password:test
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
```

UPDate REMOTEAgent

Aktualisiert die Registrierungswerte des Agentenservice für den fernen Client. Für diesen Befehl ist die Option /name:*Servicename* erforderlich; außerdem müssen die zu aktualisierenden Registrierungswerte angegeben werden. Andere gültige Optionen sind:

- /node:*Knotenname*
- /password:*Kennwort*
- /optfile:*Optionsdatei*
- /partnername:*Partnerservicename*

Task

Einen fernen Clientagentenservice mit dem Namen `TSM-AGENT` aktualisieren. Der ferne Clientagentenservice verwendet den Knoten *test*, um die Verbindung zum IBM Spectrum Protect-Server herzustellen. Die Optionsdatei C:\program files\tivoli\tsm\baclient\dsm.opt wird zum Herstellen der Verbindung zum Server verwendet. Der Partnerclientakzeptorservice hat den Namen `TSM-CAD`.
Befehl:

```
dsmcutil update remoteagent /name:"TSM-AGENT" /node:test
/password:test /optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
/partnername:"TSM-CAD"
```

Scheduler abfragen

Registrierungswerte für den Scheduler-Service abfragen. Erforderliche Optionen sind: /name:*Servicename*. Andere gültige Optionen sind:

- /machine:*Machinenname*
- /clientdir
- /optfile
- /eventlogging
- /node
- /commmethod
- /commport
- /commserver
- /errorlog
- /schedlog

Anmerkung: Geben Sie keinen Wert für die nicht erforderlichen Optionen an. Der Client gibt die entsprechenden Registrierungswerte für den von Ihnen angegebenen Scheduler-Service zurück.

Task
: Registrierungseinstellungen für den von Ihnen angegebenen Scheduler-Service abfragen.
Befehl:

```
dsmcutil query /name:"Zentraler TSM-Scheduler"
```

Task
: Registrierungseinstellung für das Clientverzeichnis für den von Ihnen angegebenen Scheduler-Service abfragen.
Befehl:

```
dsmcutil query /name:"Zentraler TSM-Scheduler"
```

Query CAD

Fragt die Registrierungswerte für den Clientakzeptorservice ab. Für diesen Befehl ist die Option /name:*Servicename* erforderlich. Andere gültige Optionen sind:

- /machine:*Machinenname*
- /node
- /optfile
- /httpport
- /webports
- /clientdir
- /partnername

Anmerkung: Geben Sie keinen Wert für diese Optionen an.

Task
: Registrierungseinstellungen für den von Ihnen angegebenen Clientakzeptorservice abfragen.
Befehl:

```
dsmcutil query cad /name:"TSM CAD"
```

Query Journal

Den Journalsteuerkomponentenservice, `TSM-Journalservice`, auf einem Windows-System abfragen. Für diesen Befehl stehen keine Optionen zur Verfügung.

Task
: Den Journalsteuerkomponentenservice, `TSM-Journalservice`, abfragen.
Befehl:

```
dsmcutil query journal
```

Query REMOTEAgent

Fragt die Registrierungswerte für den Agentenservice für den fernen Client ab. Für diesen Befehl ist die Option /name:*Servicename* erforderlich. Andere gültige Optionen sind:

- /machine:*Machinenname*
- /node
- /optfile
- /partnername
- /clientdir

Anmerkung: Geben Sie keinen Wert für diese Optionen an.

Task

Registrierungseinstellungen für den angegebenen Agentenservice für den fernen Client abfragen.
Befehl:

```
dsmcutil query remoteagent /name:"TSM AGENT"
```

List

Listet die installierten Client-Services auf. Es sind keine Optionen erforderlich.

Task

Die installierten Services des Clients für Sichern/Archivieren auf der lokalen Workstation suchen und auflisten.
Befehl:

```
dsmcutil list
```

Task

Die installierten Services des Clients für Sichern/Archivieren auf der fernen Workstation PDC auflisten.
Befehl:

```
dsmcutil list /MACHINE:PDC
```

START

Mit dem Befehl Start kann ein Client-Service gestartet werden. Für den Befehl Start ist die Option /name:*Servicename* erforderlich.

Task

Den Journalsteuerkomponentenservice, `TSM-Journalservice`, starten.
Befehl:

```
dsmcutil start /name:"TSM-Journalservice"
```

STOP

Mit dem Befehl Stop kann ein Client-Service gestoppt werden. Für den Befehl Stop ist die Option /name:*Servicename* erforderlich.

Task

Den Journalsteuerkomponentenservice, `TSM-Journalservice`, stoppen.
Befehl:

```
dsmcutil stop /name:"TSM-Journalservice"
```

UPDATEPW

Ein verschlüsseltes IBM Spectrum Protect-Kennwort generieren. Für den Befehl UPDATEPW sind die Optionen /node:*Knotenname*, /password:*Kennwort* und /commserver:*Servername* erforderlich. Wenn die Option clusternode auf YES gesetzt ist, ist der Parameter /optfile: ebenfalls erforderlich.

Wahlweise können Sie auch folgende Optionen verwenden:

- /validate:Yes | No
- /clusternode:Yes | No (erforderlich, falls MSCS oder VCS ausgeführt wird)
- /clustername:*Clustername* (erforderlich, falls MSCS oder VCS ausgeführt wird)
- /force:Yes | No
- /optfile: (für Operationen ohne Cluster)
- /commmethod:
- /commport:

Das Kennwort wird vom IBM Spectrum Protect-Server geprüft, wenn /validate:Yes angegeben ist. Das Kennwort wird auf dem Server aktualisiert, wenn Sie /updateonserver:Yes angeben. Bei Angabe dieser Option müssen Sie das aktuelle Kennwort mit der Option /oldpassword: angeben.

Task

Das verschlüsselte Kennwort für den angegebenen Knoten aktualisieren. Das Kennwort soll auf dem angegebenen IBM Spectrum Protect-Server, der sich beim angegebenen TCP/IP-Hostnamen und -Anschluss befindet, geprüft und aktualisiert werden.
Befehl:

```
dsmcutil updatepw /node:alpha1 /commMethod:tcpip
/commServer:alpha1.example.com /commPort:1500
/password:neues_Kennwort /oldpassword:altes_Kennwort /updateonserver:yes
/validate:yes /optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
```

ADDACE

Gewährt Zugriff auf das Kennwort des IBM Spectrum Protect-Clients für Sichern/Archivieren und auf die Client-SSL-Zertifikate für Benutzer ohne Administratorberechtigung.

Ab IBM Spectrum Protect Version 8.1.2 wird eine strengere Zugriffssteuerung für den IBM Spectrum Protect-Kennwortspeicher in Windows-Betriebssystemen durchgesetzt. Standardmäßig haben nur die Konten 'Administrator', 'SYSTEM' und 'Lokales System' Zugriff den Kennwortspeicher und die SSL-Zertifikate.

Sie können den Befehl addace verwenden, um die Zugriffssteuerungsliste zu ändern, damit weitere Benutzer (z. B. Benutzer ohne Verwaltungsaufgaben) oder Prozesse (z. B. die IBM Spectrum Protect Data Protection-Clientprozesse) auf den Kennwortspeicher und die SSL-Zertifikate zugreifen können.

Die folgenden Optionen sind erforderlich:

- -entity:*Benutzer | Gruppe*
- -object:ALL | *KNOTENNAME* | *Pfad*\TSM.* | *Pfad*\spclient.*

Dabei gilt:

Benutzer | Gruppe
: Der Windows-Benutzer oder die Windows-Benutzergruppe, dem bzw. der Schreib-/Lesezugriffsberechtigung für den Kennwortspeicher erteilt wird.

ALL
: Gewährt Zugriff auf alle Kennwortdateien und SSL-Zertifikate in den Unterverzeichnissen des Verzeichnisses C:\ProgramData\Tivoli\TSM\baclient.

KNOTENNAME
: Gewährt Zugriff auf alle Kennwortdateien und SSL-Zertifikate in den Unterverzeichnissen des Verzeichnisses C:\ProgramData\Tivoli\TSM\baclient\Nodes*Knotenname*.

Pfad\TSM.* | *Pfad*\spclient.*
: Gewährt für Clusterkennwörter, die in einem Verzeichnis für gemeinsam genutzte Ressourcen vorhanden sein können, Zugriff auf die Kennwort- oder Zertifikatsdateien in einem bestimmten Verzeichnis für einen Knoten.

Weitere Informationen zu den sicheren Kennwortpositionen unter Windows finden Sie in Sicherer Kennwortspeicher.
Tipp: Mit dem Befehl dsmcutil deleteace kann der Zugriff auf Kennwortdateien und SSL-Zertifikate entzogen werden.

Task
: Nachdem Sie als Administrator den Client für Sichern/Archivieren installiert und konfiguriert haben, müssen Sie der Benutzerin ohne Verwaltungsaufgaben 'Susan' auf Ihrem Windows-System eine Zugriffsberechtigung für die Kennwortdateien und SSL-Zertifikate auf dem Clientknoten Alpha1 erteilen.
Befehl:

```
dsmcutil addace -entity:Susan -object:Alpha1
```

Task
: Ein Benutzer ohne Verwaltungsaufgaben von IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server hat die IBM Spectrum Protect-Kennwörter konfiguriert, aber auch der Administrator muss auf die Kennwörter zugreifen können. Der Benutzer von Data Protection for Microsoft SQL Server gibt den folgenden Befehl aus, um dem Administrator Zugriffsberechtigung für die Kennwortdateien zu erteilen:
Befehl:

```
dsmcutil addace -entity:Administrator -object:all
```

Task
: Während einer Clusterkonfiguration muss der Windows-Administrator dem Clusterknoten clusnode_A Zugriffsberechtigung für die Client-SSL-Zertifikate erteilen.
Befehl:

```
dsmcutil addace -entity:Group_A
-object:C:\ProgramData\Tivoli\TSM\baclient\Nodes\clusnode_A\spclient.*
```

Wenn sich die Clientzertifikate nicht an der Standardposition (C:\ProgramData\Tivoli\TSM\baclient\Nodes\clusnode_A\) befinden, befinden sie sich in demselben Verzeichnis wie die Datei dsm.opt.

DELETEACE

Entzieht Zugriff auf das Kennwort des IBM Spectrum Protect-Clients für Sichern/Archivieren und auf die Client-SSL-Zertifikate für Benutzer ohne Administratorberechtigung.

Sie können den Befehl deleteace verwenden, um die Zugriffssteuerungsliste zu ändern und den Zugriff auf den Kennwortspeicher und die SSL-Zertifikate für Benutzer (z. B. Benutzer ohne Verwaltungsaufgaben) oder Prozesse (z. B. die IBM Spectrum Protect Data Protection-Clientprozesse) aufzuheben.

Die folgenden Optionen sind erforderlich:

- -entity:*Benutzer | Gruppe*

- -object:ALL | *KNOTENNAME* | *Pfad*\TSM.* | *Pfad*\spclient.*

Dabei gilt:

Benutzer | Gruppe
: Der Windows-Benutzer oder die Windows-Benutzergruppe, dem bzw. der der Zugriff auf den Kennwortspeicher und die Clientzertifikate entzogen wird.

ALL
: Entzieht den Zugriff auf alle Kennwortdateien und SSL-Zertifikate in den Unterverzeichnissen des Verzeichnisses C:\ProgramData\Tivoli\TSM\baclient.

KNOTENNAME
: Entzieht den Zugriff auf alle Kennwortdateien und SSL-Zertifikate in den Unterverzeichnissen des Verzeichnisses C:\ProgramData\Tivoli\TSM\baclient\Nodes*Knotenname*.

Pfad\TSM.* | *Pfad*\spclient.*
: Entzieht für Clusterkennwörter, die in einem Verzeichnis für gemeinsam genutzte Ressourcen vorhanden sein können, den Zugriff auf die Kennwort- oder Zertifikatsdateien in einem bestimmten Verzeichnis für einen Knoten.

Weitere Informationen zu den sicheren Kennwortpositionen unter Windows finden Sie in Sicherer Kennwortspeicher.
Tipp: Mit dem Befehl dsmcutil addace kann der Zugriff auf Kennwortdateien und SSL-Zertifikate gewährt werden.

Task
: Die Benutzerin ohne Verwaltungsaufgaben 'Susan' hat Ihr Unternehmen vor zwei Tagen verlassen und als Administrator müssen Sie die Zugriffsberechtigung für die Kennwortdateien und SSL-Zertifikate auf dem Clientknoten `Alpha1` entziehen.
Befehl:

```
dsmcutil deleteace -entity:Susan -object:Alpha1
```

Task
: Der Clusterknoten `clusnode_Z` wird aus der Clusterkonfiguration entfernt und benötigt keinen Zugriff mehr auf die Client-SSL-Zertifikate. Geben Sie den folgenden Befehl aus, um die Zugriffsberechtigung für `clusnode_Z` zu entziehen:
Befehl:

```
dsmcutil deleteace -entity:Group_Z
-object:C:\ProgramData\Tivoli\TSM\baclient\Nodes\clusnode_Z\spclient.*
```

Wenn sich die Clientzertifikate nicht an der Standardposition (C:\ProgramData\Tivoli\TSM\baclient\Nodes\clusnode_Z\) befinden, befinden sie sich in demselben Verzeichnis wie die Datei dsm.opt.

Zugehörige Konzepte:
Journalbasierte Sicherung
Zugehörige Tasks:
Gültige dsmcutil-Optionen
Zugehörige Verweise:
Incremental
Windows-Betriebssysteme

Gültige dsmcutil-Optionen

In diesem Abschnitt sind die gültigen **dsmcutil**-Optionen aufgelistet, die Sie bei der Verwendung des Scheduler-Service angeben können.

Informationen zu diesem Vorgang

/autostart:[Yes|No]
: Gibt an, ob der Scheduler-Service automatisch beim Systemstart gestartet werden soll. Der Standardwert ist *No*.

/cadschedname:Schedulername
: Gibt den Namen des Scheduler-Service an, der mit dem Clientakzeptor verwaltet werden soll. Verwenden Sie diese Option, wenn die Option ***managedservices*** in der Clientoptionsdatei dsm.opt auf *schedule* gesetzt ist. Sie können diese Option nur beim Clientakzeptorservice angeben.

/clientdir:Clientverzeichnis
: Der vollständig qualifizierte Verzeichnispfad, bei dem sich die Dateien für den Client-Service befinden. Dieses Verzeichnis sollte relativ zur Zielworkstation angegeben werden, auf der der Service installiert ist. UNC-Namen sind nicht zulässig, wenn das lokale Systemkonto auf Anmelden gesetzt ist. Standardwert ist das aktuelle Verzeichnis.

/clustername:Clustername
: Diese Option ersetzt die Option ***/group***.

Die Option ***/clustername*** gibt den Clusternamen an, zu dem das System gehört. Sie können den Clusternamen auf eine der folgenden Arten bestimmen:

- Führen Sie in MSCS den MSCS-Befehl CLUSTER /LIST von der Befehlszeile aus oder verwenden Sie das Dienstprogramm Clusteradministrator. Wenn das Dienstprogramm Clusteradministrator gestartet wird, erscheint eine baumähnliche Struktur, an deren Spitze der Clustername steht.

- Verwenden Sie in VCS die VCS-Clustermanager - Java™-Konsole oder öffnen Sie die Datei main.cf im Verzeichnis %VCS_HOME%\config.
- Verwenden Sie in VCS den folgenden Befehl:

  ```
  haclus -display
  ```

Einschränkung: Geben Sie keinen Clusternamen mit mehr als 64 Zeichen an. Wenn Sie mehr als 64 Zeichen angeben und Veritas Storage Foundation mit hoher Verfügbarkeit oder eine Microsoft Cluster Server-Konfiguration verwenden, können Sie den Scheduler-Service von IBM Spectrum Protect möglicherweise nicht installieren oder starten.

Diese Option muss zusammen mit der Option ***/clusternode***:Yes verwendet werden. Diese Option muss angegeben werden, wenn der Befehl INSTALL in einer Clusterumgebung verwendet wird. Sie muss außerdem angegeben werden, wenn mit dem Befehl UPDATE die Clustereinstellungen geändert werden (***/clusternode*** und ***/clustername***).

Diese Option kann auch angegeben werden, wenn der Befehl UPDATEPW in einer Clusterumgebung verwendet wird. In der Regel ist dies nicht erforderlich. Wenn jedoch für einen bestimmten Knoten mehrere Scheduler-Services mit unterschiedlichen Clustereinstellungen definiert sind, kann das Dienstprogramm nicht bestimmen, welche Einstellungen korrekt sind. In diesem Fall korrigieren Sie die Diskrepanzen zwischen den Services.

Alternativ dazu können Sie diese Option mit ***/clusternode***: Yes und ***/force***:Yes angeben, um das Dienstprogramm zu zwingen, das Kennwort mit den angegebenen Clustereinstellungen anzuzeigen oder zu aktualisieren.

Diese Option ist nicht erforderlich, wenn ***/clusternode*** :No angegeben ist.

/clusternode:Yes|No
Gibt an, ob die Unterstützung für Clusterressourcen aktiviert werden soll. Der Standardwert ist *No*. Sie müssen MSCS oder VCS ausführen, um ***/clusternode***:Yes angeben zu können. Diese Option muss angegeben werden, wenn der Befehl INSTALL in einer Clusterumgebung verwendet wird. Sie muss außerdem angegeben werden, wenn mit dem Befehl UPDATE die Clustereinstellungen geändert werden (***/clusternode*** , ***/clustername***).

Diese Option kann auch angegeben werden, wenn der Befehl UPDATEPW in einer Clusterumgebung verwendet wird. In der Regel ist dies nicht erforderlich. Wenn jedoch für einen bestimmten Knoten mehrere Scheduler-Services mit unterschiedlichen Clustereinstellungen definiert sind, kann das Dienstprogramm nicht bestimmen, welche Einstellungen korrekt sind. In diesem Fall korrigieren Sie die Diskrepanzen zwischen den Services.

Alternativ dazu können Sie diese Option mit ***/clustername*** und ***/force***:Yes angeben, um das Dienstprogramm zu zwingen, das Kennwort mit den angegebenen Clustereinstellungen anzuzeigen oder zu aktualisieren. Wenn ***/clusternode*** :No angegeben wird, ist ***/clustername*** nicht erforderlich.

/commmethod:Protokoll
Gibt das Clientübertragungsprotokoll an, über das mit dem IBM Spectrum Protect-Server kommuniziert werden soll. Gültige Protokolle sind: TCP/IP und Benannte Pipes. Wenn Sie keinen Wert angeben, wird der Wert aus der Clientoptionsdatei abgerufen oder auf den standardmäßig vorgegebenen Wert für den Client gesetzt. Sie können diese Option auch in Verbindung mit dem Befehl UPDATEPW verwenden, um ein Übertragungsprotokoll anzugeben, mit dem beim Aktualisieren von Kennwörtern die Verbindung zu einem Server hergestellt wird.

/commport:Serveranschluss
Gibt den protokollspezifischen IBM Spectrum Protect-Serveranschluss an. Für TCP/IP ist dies der Anschluss beim angegebenen Hostnamen. Wird für diese Option kein Wert angegeben, wird der Wert aus der Clientoptionsdatei abgerufen oder auf den standardmäßig vorgegebenen Wert für den Client gesetzt. Sie können diese Option auch in Verbindung mit dem Befehl UPDATEPW verwenden, um einen protokollspezifischen Serveranschluss anzugeben, zu dem die Verbindung beim Aktualisieren von Kennwörtern hergestellt wird.

/commserver:Servername
Gibt den protokollspezifischen IBM Spectrum Protect-Servernamen an. Abhängig vom verwendeten Protokoll, kann es sich dabei um einen TCP/IP-Hostnamen oder einen Namen für benannte Pipes handeln. Wird für diese Option kein Wert angegeben, wird der Wert aus der Clientoptionsdatei abgerufen oder auf den standardmäßig vorgegebenen Wert für den Client gesetzt.

Sie können diese Option auch in Verbindung mit dem Befehl UPDATEPW verwenden, um einen protokollspezifischen Servernamen anzugeben, zu dem die Verbindung beim Aktualisieren von Kennwörtern hergestellt wird.

/copyfiles
Gibt an, dass die Serviceinstallation vor der Installation an eine andere Position kopiert wird. Mit der Option ***/srcdir*** kann der vollständig qualifizierte Quellenpfad angegeben werden.

/errorlog:Fehlerprotokoll
Gibt den vollständig qualifizierten Namen des Clientfehlerprotokolls an.

/eventlogging:[Yes|No]
Aktiviert oder deaktiviert das ausführliche Protokollieren für den angegebenen Scheduler-Service. Der Standardwert ist *Yes*.

/force:[Yes|No]
Diese Option kann auch angegeben werden, wenn der Befehl UPDATEPW in einer Clusterumgebung verwendet wird. In der Regel ist dies nicht erforderlich. Wenn jedoch für einen bestimmten Knoten mehrere Scheduler-Services mit unterschiedlichen Clustereinstellungen definiert sind, kann das Dienstprogramm nicht bestimmen, welche Einstellungen korrekt sind. In diesem Fall korrigieren Sie die Diskrepanzen zwischen den Services.

Alternativ dazu können Sie diese Option mit ***/clusternode*** und ***/clustername*** angeben (wenn ***/clusternode***:Yes angegeben wird), um das Dienstprogramm zu zwingen, das Kennwort mit den angegebenen Clustereinstellungen anzuzeigen oder zu aktualisieren.

/httpport:HTTP-Anschluss
Gibt eine TCP/IP-Anschlussadresse für den Web-Client an.
/machine:Einheitenname
Gibt den Namen der fernen Workstation an, zu der eine Verbindung hergestellt wird.
/name:Servicename
Gibt den Namen des Client-Service an. Wenn der Name eingebettete Leerzeichen enthält, muss er in Anführungszeichen gesetzt werden.
/node:Knotenname
Gibt den IBM Spectrum Protect-Knotennamen an, den der Client-Service beim Herstellen der Verbindung zum IBM Spectrum Protect-Server verwendet. Er wird auch beim Anzeigen oder Aktualisieren des IBM Spectrum Protect-Kennworts verwendet. Der Standardwert ist der Workstationname.
/ntaccount:NT-Konto
Gibt das Windows-Konto an, mit dem sich der Service anmeldet.
/ntdomain:NT-Domäne
Gibt die Windows-Domäne an, mit der sich der Service anmeldet.
/ntpassword:NT-Kennwort
Gibt das Windows-Kennwort für das Konto an, mit dem sich der Service anmeldet.
/oldpassword:altes Kennwort
Das aktuelle Kennwort des IBM Spectrum Protect-Servers. Wird in Zusammenhang mit der Option /updateonserver verwendet, wenn ein Kennwort auf dem Server aktualisiert wird.
/optfile:Optionsdatei
Der vollständig qualifizierte Pfad der Clientoptionsdatei. Dabei handelt es sich um die Optionsdatei, die der angegebene Client-Service zum Herstellen der Verbindung zum IBM Spectrum Protect-Server verwendet. Das Dienstprogramm verwendet diese Datei auch zum Herstellen der Verbindung zum IBM Spectrum Protect-Server, um Kennwörter zu prüfen und zu aktualisieren. Bitte beachten: Obwohl diese Option die Standardoptionsdatei im aktuellen Verzeichnis (dsm.opt) überschreibt, erfordert die IBM Spectrum Protect-API, dass eine Standardoptionsdatei im aktuellen Verzeichnis vorhanden ist. UNC-Namen sind nicht zulässig, wenn das lokale Systemkonto auf Anmelden gesetzt ist. Der Standardwert ist die Datei dsm.opt im Verzeichnis ***/clientdir***.
/partnername:Partnerservicename
Diese Option wird bei der Installation eines Agentenservice für den fernen Client verwendet, um den Partnerclientakzeptorservice anzugeben.
/password:Kennwort
Das IBM Spectrum Protect-Kennwort, das generiert und verschlüsselt wird.
/schedlog:Planungsprotokoll
Gibt den vollständig qualifizierten Namen des Clientplanungsprotokolls an.
/srcdir:Pfadname
Verwenden Sie diese Option in Verbindung mit der Option ***/copyfiles*** für die Angabe des vollständig qualifizierten Quellenpfads, um die Serviceinstallation vor der Installation des Service an eine andere Position zu kopieren.
/startnow:[Yes|No]
Gibt an, ob dsmcutil den angegebenen Service nach der Ausführung des Befehls starten soll; der Standardwert lautet *Yes*. Wenn Sie ***No*** angeben, müssen Sie den Service manuell über das Applet für Servicesystemsteuerung oder den Befehl NET START **Name des Service** starten.
/updateonserver:[Yes|No]
Gibt an, ob das angegebene Kennwort auf dem IBM Spectrum Protect-Server aktualisiert wird. Muss zusammen mit der Option ***/oldpassword*** verwendet werden.
/validate:[Yes|No]
Gibt an, ob beim Anzeigen oder Aktualisieren des verschlüsselten Kennworts eine Überprüfung durchgeführt werden soll. Der Standardwert ist *Yes*.
/webports:Web-Anschlüsse
Gibt die TCP/IP-Anschlussnummer an, die vom Clientakzeptorservice und dem Web-Client-Agentenservice für die Kommunikation mit der Web-GUI verwendet wird.

Dokumentation für Clients für Sichern/Archivieren in PDF-Dateien

Die im IBM Knowledge Center verfügbaren Informationen zu Clients für Sichern/Archivieren stehen auch in Form von PDF-Dateien zur Verfügung.

- AIX-BetriebssystemeLinux-BetriebssystemeMac OS X-BetriebssystemeOracle Solaris-BetriebssystemeClients für Sichern/Archivieren Installations- und Benutzerhandbuch
- Windows-BetriebssystemeClients für Sichern/Archivieren Installations- und Benutzerhandbuch
- Clientnachrichten und API-Rückkehrcodes

Zugehörige Konzepte:
IBM Spectrum Protect-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)
Zugehörige Tasks:
Clients für Sichern/Archivieren konfigurieren
IBM Spectrum Protect-Clients für Sichern/Archivieren
Zugehörige Verweise:

Optionen und Befehle des Clients für Sichern/Archivieren
Zugehörige Informationen:
Schutz für Workstations und Dateiserver

Lösungen mit der Anwendungsprogrammierschnittstelle entwickeln

Die Anwendungsprogrammierschnittstelle (API) von IBM Spectrum Protect befindet sich im selben Paket wie der Client für Sichern/Archivieren von IBM Spectrum Protect. Mit der API können Sie Geschäftsanwendungen, wie beispielsweise Datenbanken, in der IBM Spectrum Protect-Umgebung schützen.

- Neuerungen für die IBM Spectrum Protect-API
  Enthält Informationen zu neuen und geänderten Funktionen. Lesen Sie vor der Installation des Produkts die Releaseinformationen.
- API installieren
  Informationen zum Installieren der Anwendungsprogrammierschnittstelle (API) von IBM Spectrum Protect werden in den Installationsverfahren für den Client für Sichern/Archivieren bereitgestellt.
- Übersicht über die API
  Die Anwendungsprogrammierschnittstelle (API) von IBM Spectrum Protect ermöglicht einem Anwendungsclient die Verwendung von Speicherverwaltungsfunktionen.
- API-Musteranwendung erstellen und ausführen
  Das API-Paket enthält Musteranwendungen, die die API-Funktionsaufrufe im Kontext veranschaulichen. Installieren Sie eine Musteranwendung und schauen Sie sich den Quellcode an, um sich mit der Verwendung der Funktionsaufrufe vertraut zu machen.
- Hinweise zum Entwerfen einer Anwendung
  Wenn Sie eine Anwendung entwerfen, müssen Sie über Kenntnisse über viele Aspekte der API verfügen.
- Erläuterungen zur Interoperabilität
  Bei der API unterscheidet man zwei Typen von Interoperabilität: Interoperabilität zwischen dem Client für Sichern/Archivieren und den API-Anwendungen sowie Interoperabilität zwischen verschiedenen Betriebssystemen.
- Verwendung der API mit Unicode
  Die IBM Spectrum Protect-API unterstützt Unicode UCS-2, eine Doppelbyte-Codepage mit fester Länge, die Codepunkte für alle bekannten Codepages, wie z. B. Japanisch, Chinesisch oder Deutsch, enthält. Sie unterstützt bis zu 65.535 eindeutige Codepunkte.
- API-Funktionsaufrufe
- Quellendatei mit API-Rückkehrcodes: dsmrc.h
  Die Headerdatei dsmrc.h enthält alle Rückkehrcodes, die die API an eine Anwendung zurückgeben kann.
- Quellendateien für API-Typdefinitionen
- Quellendatei mit den API-Funktionsdefinitionen
  Dieser Anhang enthält die Headerdatei dsmapifp.h mit den Funktionsdefinitionen für die API.
- API-Rückkehrcodereferenz

Zugehörige Konzepte:
IBM Tivoli Storage Manager-Clients für Sichern/Archivieren
Zugehörige Verweise:
PDF-Dateien zum Drucken

Neuerungen für die IBM Spectrum Protect-API

Enthält Informationen zu neuen und geänderten Funktionen. Lesen Sie vor der Installation des Produkts die Releaseinformationen.

- API-Aktualisierungen
  Lesen Sie die Informationen zu neuen Funktionen und Aktualisierungen für die Anwendungsprogrammierschnittstelle (API) in IBM Spectrum Protect Version 8.1. In
- Releaseinformationen für die Anwendungsprogrammierschnittstelle Version 8.1 von IBM Spectrum Protect
  Die Anwendungsprogrammierschnittstelle (API) Version 8.1 von IBM Spectrum Protect ist verfügbar. Dieses Dokument enthält wichtige Installationsinformationen. Außerdem finden Sie in diesem Dokument Produktaktualisierungen, Kompatibilitätsanforderungen, Einschränkungen und bekannte Probleme.
- Readme-Dateien für Fixpacks der Anwendungsprogrammierschnittstelle von IBM Spectrum Protect Version 8.1
  Readme-Dateien für die Fixpacks für die Anwendungsprogrammierschnittstelle (API) von IBM Spectrum Protect Version 8.1 sind bei einem Fixpack-Update in der Unterstützungswissensbasis verfügbar.
- Neueste Dokumentationsaktualisierungen
  Aktualisierungen für die Dokumentation der IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) können vorgenommen werden, nachdem die Dokumentation im IBM® Knowledge Center veröffentlicht wurde.

API-Aktualisierungen

Lesen Sie die Informationen zu neuen Funktionen und Aktualisierungen für die Anwendungsprogrammierschnittstelle (API) in IBM Spectrum Protect Version 8.1. In

Release	Neue Funktionen und Aktualisierungen

Release	Neue Funktionen und Aktualisierungen
8.1.2	Erweiterte Clientsicherheitseinstellungen Ab IBM Spectrum Protect Version 8.1.2 werden im Client für Sichern/Archivieren mehrere Änderungen eingeführt, um eine Zusammenarbeit mit dem IBM Spectrum Protect-Server der Version 8.1.2 zu ermöglichen, der Erweiterungen zur Verbesserung der Sicherheit für die Kommunikation zwischen Client und Server bereitstellt. Weitere Informationen finden Sie in Aktualisierungen für den Client für Sichern/Archivieren. Der Trusted Communication Agent (TCA) wird nicht mehr verwendet Aufgrund der erweiterten Kommunikation, die in IBM Spectrum Protect Version 8.1.2 eingeführt wird, ist der Trusted Communication Agent (TCA) nicht mehr verfügbar. Weitere Informationen finden Sie in: • Sicherer Kennwortspeicher • Benutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen Wartungsaktualisierungen Die API-Dokumentation wurde aktualisiert, um Wartungsaktualisierungen einzuschließen.
8.1.0	IBM® Tivoli Storage Manager heißt künftig IBM Spectrum Protect. IBM Spectrum Protect Version 8.1 ist die nächste Generation von Tivoli Storage Manager. Dieses neue Release stellt mehr als nur eine Namensänderung in der Benutzerschnittstelle und Dokumentation dar. Es ist eine Weiterentwicklung auf eine höhere Ebene des Datenschutzes, mit dem die komplexen Anforderungen der heutigen Zeit erfüllt werden sollen. Weitere Informationen finden Sie in Lernen Sie IBM Spectrum Protect kennen. Mit dem Serverbefehl REGISTER NODE wird eine Benutzer-ID mit Administratorberechtigung nicht mehr standardmäßig erstellt Ab IBM Spectrum Protect Version 8.1 wird mit dem Serverbefehl REGISTER NODE nicht automatisch eine Benutzer-ID mit Administratorberechtigung erstellt, die mit dem Knotennamen übereinstimmt. Mit dieser Produktaktualisierung soll die Benutzerauthentifizierung bei einem Lightweight Directory Access Protocol-Server (LDAP-Server) optimiert werden. Diese Produktaktualisierung hat keine Auswirkungen auf vorhandene Clientknoten, aber sie kann sich auf den Prozess zum Registrieren neuer Clientknoten, einschließlich Knoten für IBM Spectrum Protect-Clients für Sichern/Archivieren, auswirken. In einigen Fällen müssen Sie möglicherweise eine Benutzer-ID mit Administratorberechtigung erstellen, wenn Sie einen Knoten registrieren. Sie können die Benutzer-ID mit Administratorberechtigung erstellen, indem Sie den Befehl REGISTER NODE ausgeben und den Parameter USERID angeben. Informationen zu den betroffenen Clienttypen finden Sie in Technote 7048963. Weitere Informationen zum Erstellen einer Benutzer-ID mit Administratorberechtigung finden Sie in Benutzer mit Verwaltungsaufgaben mit Clienteignerberechtigung erstellen. Verwendung und Unterstützung von Clientbetriebssystemen wurde eingestellt Um die Vorteile der neuen Produktfunktionen zu nutzen, installieren Sie den Client für Sichern/Archivieren der Version 8.1 und die API auf einem der unterstützten Betriebssysteme. Die aktuelle Liste der unterstützten Betriebssysteme finden Sie in Technote 1243309. Die folgenden Betriebssysteme werden vom Client für Sichern/Archivieren nicht mehr unterstützt: • Windows 32-Bit-Betriebssysteme (Client und API). • Betriebssysteme Windows Server 2008, Windows Server 2008 R2, Windows 7 und Windows 8. • HP-UX-Betriebssysteme. Sie können weiterhin die IBM Spectrum Protect-API auf einem HP-UX-Betriebssystem verwenden. Installationsanweisungen finden Sie in HP-UX Itanium 2-API installieren. • Linux on Power Systems (Big Endian). Sie können weiterhin die IBM Spectrum Protect-API unter Linux on Power Systems (Big Endian) verwenden. Installationsanweisungen finden Sie in API unter Linux on Power Systems (Big Endian) installieren. • Solaris SPARC-Betriebssysteme. Sie können weiterhin die IBM Spectrum Protect-API auf Solaris SPARC-Betriebssystemen verwenden. Anweisungen zur Installation der API finden Sie im Abschnitt Oracle Solaris-Client installieren.

Releaseinformationen für die Anwendungsprogrammierschnittstelle Version 8.1 von IBM Spectrum Protect

Die Anwendungsprogrammierschnittstelle (API) Version 8.1 von IBM Spectrum Protect ist verfügbar. Dieses Dokument enthält wichtige Installationsinformationen. Außerdem finden Sie in diesem Dokument Produktaktualisierungen, Kompatibilitätsanforderungen, Einschränkungen und bekannte Probleme.

Inhalt

- Beschreibung
- Ankündigung
- Kompatibilität mit früheren Versionen
- Systemvoraussetzungen
- API installieren
- Aktualisierungen, Einschränkungen und bekannte Probleme

Beschreibung

Die Anwendungsprogrammierschnittstelle (API) von IBM Spectrum Protect ermöglicht einem Anwendungsclient die Verwendung von Speicherverwaltungsfunktionen. Die API umfasst Funktionsaufrufe, die Sie in einer Anwendung zur Ausführung der folgenden Operationen verwenden können:

- Sitzung starten oder beenden
- Objekten Verwaltungsklassen zuordnen, bevor sie auf einem Server gespeichert werden
- Objekte auf einem Server sichern oder archivieren
- Objekte von einem Server zurückschreiben oder abrufen
- Server nach Informationen zu gespeicherten Objekten abfragen
- Dateibereiche verwalten
- Aufbewahrungsereignisse senden

Die API wird von Softwareentwicklern zum Erstellen neuer Anwendungen verwendet, die mit IBM Spectrum Protect arbeiten.

Die Veröffentlichung *IBM Spectrum Protect Verwendung der Anwendungsprogrammierschnittstelle* stellt Informationen zur Verwendung der IBM Spectrum Protect-API bereit.

Die IBM Spectrum Protect-API ist auf den folgenden Betriebssystemen verfügbar:

- HP-UX
- IBM® AIX
- Linux
- Mac OS X
- Microsoft Windows 64-Bit-Betriebssysteme
- Oracle Solaris

Eine Liste der APARs, die in diesem Release behoben wurden, finden Sie in Technote 1993247.

Ankündigung

Die Ankündigung für die IBM Spectrum Protect-Produktfamilie der Version 8.1 enthält die folgenden Informationen:

- Detaillierte Produktbeschreibung, einschließlich einer Beschreibung der neuen Funktionen
- Produktpositionierungsanweisung
- Details zu Produktauswahl und Bestellung
- Internationale Kompatibilitätsinformationen

Führen Sie die folgenden Schritte aus, um nach der Produktankündigung zu suchen:

1. Rufen Sie die Produktankündigungswebsite auf.
2. Geben Sie in das Feld Search for die Produkt-ID (PID) für Ihr Produkt ein. Die PID für IBM Spectrum Protect ist 5725-W98.
3. Wählen Sie im Feld Information Type den Eintrag Announcement letters aus und klicken Sie auf Search.
4. Wählen Sie in der Liste Search in den Eintrag Product Number aus.
5. Optional: Wählen Sie im Teilfenster Refine Your Search auf der linken Seite des Fensters das Land aus, in dem Sie sich befinden.
6. Wählen Sie im Bereich Sort by den Eintrag Newest first aus.

Kompatibilität mit früheren Versionen

Informationen zur Kompatibilität mit früheren Versionen befinden sich in IBM Spectrum Protect Server/Client Compatibility and Upgrade Considerations.

Systemvoraussetzungen

Informationen zur Hardware- und Softwarekompatibilität finden Sie in dem detaillierten Dokument zu den Systemvoraussetzungen auf den folgenden Webseiten:

Apple Macintosh Client Requirements
: Technote 1053584

HP-UX Itanium API Requirements
: Technote 1197146

IBM AIX Client Requirements
: Technote 1052226

Linux on Power Systems Client Requirements
: Technote 1169963

Linux x86_64 Client Requirements
: Technote 1052223

Linux on z Systems Client Requirements
: Technote 1066436

Microsoft Windows Client Requirements
: Technote 1197133

Oracle Solaris SPARC API Requirements
: Technote 1052211

Oracle Solaris x86_64 Client Requirements
: Technote 1232956

API installieren

Installationsanweisungen finden Sie in API installieren.

Aktualisierungen, Einschränkungen und bekannte Probleme

Dokumentationsaktualisierungen, Einschränkungen und bekannte Probleme sind als technische Hinweise in der Unterstützungswissensbasis im IBM Support Portal for IBM Spectrum Protect dokumentiert. Werden Probleme erkannt und gelöst, wird die Wissensbasis vom IBM Software Support aktualisiert. Durchsuchen Sie die Wissensbasis, um Fehlerumgehungen oder Lösungen für Probleme zu finden.

Einschränkungen und bekannte Probleme
: Einschränkungen und bekannte Probleme, die die IBM Spectrum Protect-API Version 8.1 betreffen, befinden sich in Technote 1993248.

Dokumentationsaktualisierungen
: Informationen, die zum Zeitpunkt der Veröffentlichung nicht zur Verfügung standen, befinden sich in den Dokumentationsaktualisierungen in Technote 7048957.

Readme-Dateien für Fixpacks der Anwendungsprogrammierschnittstelle von IBM Spectrum Protect Version 8.1

Readme-Dateien für die Fixpacks für die Anwendungsprogrammierschnittstelle (API) von IBM Spectrum Protect Version 8.1 sind bei einem Fixpack-Update in der Unterstützungswissensbasis verfügbar.

Readme-Dateien für Fixpacks für die API von IBM Spectrum Protect Version 8.1 anzeigen

Neueste Dokumentationsaktualisierungen

Aktualisierungen für die Dokumentation der IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) können vorgenommen werden, nachdem die Dokumentation im IBM® Knowledge Center veröffentlicht wurde.

Informationen zu den neuesten Dokumentationsaktualisierungen finden Sie in Technote 7048957 im IBM Support Portal.

API installieren

Informationen zum Installieren der Anwendungsprogrammierschnittstelle (API) von IBM Spectrum Protect werden in den Installationsverfahren für den Client für Sichern/Archivieren bereitgestellt.

- Tivoli Storage Manager-Clients für Sichern/Archivieren installieren (UNIX, Linux und Windows)

Übersicht über die API

Die Anwendungsprogrammierschnittstelle (API) von IBM Spectrum Protect ermöglicht einem Anwendungsclient die Verwendung von Speicherverwaltungsfunktionen.

Die API umfasst Funktionsaufrufe, die Sie in einer Anwendung zur Ausführung der folgenden Operationen verwenden können:

- Sitzung starten oder beenden
- Objekten Verwaltungsklassen zuordnen, bevor sie auf einem Server gespeichert werden
- Objekte auf einem Server sichern oder archivieren
- Objekte von einem Server zurückschreiben oder abrufen
- Server nach Informationen zu gespeicherten Objekten abfragen
- Dateibereiche verwalten
- Aufbewahrungsereignisse senden

Wenn Sie als Anwendungsentwickler die API installieren, erhalten Sie die Dateien, die ein Endbenutzer einer Anwendung benötigt:

- die gemeinsam genutzte Bibliothek der API
- die Nachrichtendatei
- die Musterclientoptionsdateien
- den Quellcode für die API-Headerdateien, die Ihre Anwendung benötigt
- den Quellcode für eine Musteranwendung und die Makefile zum Erstellen dieser Anwendung

Bei 64-Bit-Anwendungen sollten alle Kompilierungen unter Verwendung von Compileroptionen ausgeführt werden, die die 64-Bit-Unterstützung ermöglichen. Beispielsweise sollte '-q64' verwendet werden, wenn API-Anwendungen unter AIX erstellt werden, und '-m64' sollte unter Linux verwendet werden. Die Mustermakefiles enthalten weitere Informationen.

Wichtig: Wenn Sie die API installieren, stellen Sie sicher, dass alle Dateien dieselbe Version haben.

Informationen zur Installation der API finden Sie in Installation der IBM Spectrum Protect-Clients für Sichern/Archivieren.

Verweise auf UNIX und Linux schließen die Betriebssysteme AIX, HP-UX, Linux, Mac OS X und Oracle Solaris ein.

- Erläuterungen zu Konfigurations- und Optionsdateien
  Konfigurations- und Optionsdateien definieren die Bedingungen und Einschränkungen, unter denen die Sitzung ausgeführt wird.
- API-Umgebung konfigurieren
  Die API verwendet eindeutige Umgebungsvariablen, um Dateien zu lokalisieren. Sie können für API-Anwendungen andere Dateien verwenden als die, die vom Client für Sichern/Archivieren verwendet werden. Anwendungen können mithilfe des Funktionsaufrufs dsmSetup die Werte überschreiben, die in den Umgebungsvariablen definiert sind.

Erläuterungen zu Konfigurations- und Optionsdateien

Konfigurations- und Optionsdateien definieren die Bedingungen und Einschränkungen, unter denen die Sitzung ausgeführt wird.

Als Administrator oder Endbenutzer können Sie Optionswerte für Folgendes definieren:

- Konfiguration der Verbindung zu einem Server
- Steuerung, welche Objekte an den Server gesendet werden, und Festlegung der Verwaltungsklasse, der sie zugeordnet sind

Sie definieren Optionen in einer oder zwei Dateien, wenn Sie die API auf Ihrer Workstation installieren.

Unter den Betriebssystemen UNIX und Linux sind die Optionen in zwei Optionsdateien gespeichert:

- dsm.opt - die Clientoptionsdatei
- dsm.sys - die Clientsystemoptionsdatei

Unter anderen Betriebssystemen enthält die Clientoptionsdatei (dsm.opt) alle Optionen.

Einschränkung: Die API unterstützt nicht die folgenden Optionen des Clients für Sichern/Archivieren:

- autofsrename
- changingretries
- domain
- eventlogging
- groups
- subdir
- users
- virtualmountpoint

Sie können auch Optionen im Funktionsaufruf dsmInitEx angeben. Verwenden Sie den Parameter für die Optionszeichenfolge oder den Parameter für die API-Konfigurationsdatei.

Dieselbe Option kann aus mehreren Konfigurationsquellen stammen. In diesem Fall hat die Quelle mit der höchsten Priorität Vorrang. In Tabelle 1 ist die Prioritätsreihenfolge aufgelistet.

Tabelle 1. Konfigurationsquellen in absteigender Prioritätsreihenfolge

Priorität	UNIX und Linux	Windows	Beschreibung
1	dsm.sys (Datei) (Clientsystemoptionen)	nicht zutreffend	Diese Datei enthält Optionen, die ein Systemadministrator ausschließlich für UNIX und Linux definiert. Tipp: Wenn Ihre Datei dsm.sys Serverzeilengruppen enthält, stellen Sie sicher, dass in allen Zeilengruppen für die Option passwordaccess derselbe Wert angegeben ist (entweder prompt oder generate).

Priorität	UNIX und Linux	Windows	Beschreibung
2	Optionszeichenfolge (Clientoptionen)	Optionszeichenfolge (alle Optionen)	Eine dieser Optionen wird wirksam, wenn sie als Parameter an einen Aufruf dsmInitEx übergeben wird. Die Liste kann Clientoptionen wie compressalways, servername (nur UNIX und Linux) oder tcpserveraddr (nicht UNIX) enthalten. Mithilfe der API-Optionszeichenfolge kann ein Anwendungsclient Änderungen an den Optionswerten in der API-Konfigurationsdatei und der Clientoptionsdatei durchführen. Beispielsweise kann Ihre Anwendung den Endbenutzer abfragen, ob Komprimierung erforderlich ist. Abhängig von den Benutzeraktionen können Sie eine API-Optionszeichenfolge mit dieser Option erstellen und in den Aufruf dsmInitEx übergeben. Informationen zum Format der API-Optionszeichenfolge finden Sie in dsmInitEx. Sie können diesen Parameter auch auf NULL setzen. Dies gibt an, dass für diese Sitzung keine API-Optionszeichenfolge vorhanden ist.
3	API-Konfigurationsdatei (Clientoptionen)	API-Konfigurationsdatei (alle Optionen)	Die Werte, die Sie in der API-Konfigurationsdatei definieren, überschreiben die Werte, die Sie in der Clientoptionsdatei definieren. Definieren Sie die Optionen in der API-Konfigurationsdatei mit geeigneten Werten für die IBM Spectrum Protect-Sitzung des Benutzers. Die Werte werden wirksam, wenn der Name der API-Konfigurationsdatei als Parameter in dem Aufruf dsmInitEx übergeben wird. Sie können diesen Parameter auch auf NULL setzen. Dies gibt an, das für diese Sitzung keine API-Konfigurationsdatei vorhanden ist.
4	Datei dsm.opt (Clientoptionen)	Datei dsm.opt (alle Optionen)	Unter den Betriebssystemen UNIX und Linux enthält die Datei dsm.opt nur die Benutzeroptionen. Unter anderen Betriebssystemen enthält die Datei dsm.opt alle Optionen. Um die Optionen in diesen Dateien zu überschreiben, führen Sie die in dieser Tabelle beschriebenen Verfahren aus.

Zugehörige Konzepte:
Verarbeitungsoptionen

API-Umgebung konfigurieren

Die API verwendet eindeutige Umgebungsvariablen, um Dateien zu lokalisieren. Sie können für API-Anwendungen andere Dateien verwenden als die, die vom Client für Sichern/Archivieren verwendet werden. Anwendungen können mithilfe des Funktionsaufrufs dsmSetup die Werte überschreiben, die in den Umgebungsvariablen definiert sind.

Tipp: Unter Windows ist das Standardinstallationsverzeichnis %SystemDrive%\Programme\Common Files\Tivoli\TSM\api.
In Tabelle 1 sind die API-Umgebungsvariablen nach Betriebssystem aufgelistet.

Tabelle 1. API-Umgebungsvariablen

Variablen	UNIX und Linux	Windows
DSMI_CONFIG	Der vollständig qualifizierte Name für die Clientoptionsdatei (dsm.opt).	Der vollständig qualifizierte Name für die Clientoptionsdatei (dsm.opt).
DSMI_DIR	Verweist auf den Pfad, der dsm.sys, das Unterverzeichnis en_US und alle anderen Sprachen für die Unterstützung in der Landessprache enthält. Das Unterverzeichnis en_US muss dsmclientV3.cat enthalten.	Verweist auf den Pfad, der dscenu.txt und alle Nachrichtendateien für die Unterstützung in der Landessprache enthält.
DSMI_LOG	Verweist auf den Pfad für die Datei dsierror.log.	Verweist auf den Pfad für die Datei dsierror.log. Wenn die Clientoption errorlogname (Fehlerprotokollname) definiert ist, überschreibt die durch diese Option angegebene Position das mit DSMI_LOG angegebene Verzeichnis.

API-Musteranwendung erstellen und ausführen

Das API-Paket enthält Musteranwendungen, die die API-Funktionsaufrufe im Kontext veranschaulichen. Installieren Sie eine Musteranwendung und schauen Sie sich den Quellcode an, um sich mit der Verwendung der Funktionsaufrufe vertraut zu machen.

Wählen Sie eines der folgenden API-Musteranwendungspakete aus:

- Paket für interaktive Einzelthread-Anwendung (dapi*)
- Paket für Multithread-Anwendung (callmt*)
- Testanwendung für logische Objektgruppierung (dsmgrp*)
- Musteranwendung für ereignisgesteuerte Aufbewahrungsdauer (callevnt)
- Musteranwendung für Status 'Löschen unzulässig' (callhold)
- Musteranwendung für Aufbewahrungsschutz für Daten (callret)
- Musterprogramm für IBM Spectrum Protect-Datenpuffer (callbuff)

Schauen Sie sich als Einstieg die Prozedur zum Erstellen der Musteranwendung dapismp für Ihre Plattform an:

- Für UNIX- und Linux-Anwendungen siehe Quellendateien für die UNIX- oder Linux-Musteranwendung.
- Für Windows-Anwendungen siehe 64-Bit-Musteranwendung von Windows.

Die Musteranwendung dapismp erstellt eigene Datenströme, wenn Objekte gesichert oder archiviert werden. Es werden keine Objekte aus dem Dateisystem auf der lokalen Festplatte gelesen oder in dieses Dateisystem geschrieben. Der Objektname entspricht keiner Datei auf Ihrer Workstation. Mit der "Seedzeichenfolge", die Sie ausgeben, wird ein Muster generiert, das verifiziert werden kann, wenn das Objekt zurückgeschrieben oder abgerufen wird. Befolgen Sie, nachdem Sie die Musteranwendung kompiliert und **dapismp** zum Starten der Musteranwendung ausgeführt haben, die Anweisungen, die am Bildschirm angezeigt werden.

- Quellendateien für die UNIX- oder Linux-Musteranwendung
  Um die UNIX- oder Linux-Musteranwendung zu erstellen und auszuführen, müssen Sie sicherstellen, dass bestimmte Quellendateien vorhanden sind. Sobald Sie die Musteranwendung erstellt haben, können Sie die Anwendung kompilieren und ausführen.
- 64-Bit-Musteranwendung von Windows
  Um die Musteranwendung für Microsoft Windows-64-Bit-Systeme zu erstellen und auszuführen, müssen Sie die IBM Spectrum Protect-API installieren und sicherstellen, dass bestimmte Quellendateien vorhanden sind.

Quellendateien für die UNIX- oder Linux-Musteranwendung

Um die UNIX- oder Linux-Musteranwendung zu erstellen und auszuführen, müssen Sie sicherstellen, dass bestimmte Quellendateien vorhanden sind. Sobald Sie die Musteranwendung erstellt haben, können Sie die Anwendung kompilieren und ausführen.

Die Dateien, die in Tabelle 1 aufgelistet sind, umfassen die Quellendateien und anderen Dateien, die Sie zum Erstellen der Musteranwendung benötigen, die Teil des API-Pakets ist.

Tabelle 1. Erforderliche Dateien für das Erstellen der UNIX- oder Linux-API-Musteranwendung

Dateinamen		**Beschreibung**
README_api_enu		Readme-Datei
dsmrc.h dsmapitd.h dsmapips.h dsmapifp.h release.h		Headerdatei für Rückkehrcodes Headerdatei für allgemeine Typdefinitionen Headerdatei für betriebssystemspezifische Typdefinitionen Headerdatei für Funktionsprototypen Headerdatei für Releasewerte
dapibkup.c dapidata.h dapiinit.c dapint64.h dapint64.c dapipref.c dapiproc.c dapiproc.h	dapipw.c dapiqry.c dapirc.c dapismp.c dapitype.h dapiutil.h dapiutil.c	Module für die befehlszeilengesteuerte Musteranwendung
makesmp[64].*xxx*		Makefile zum Erstellen von dapismp für Ihr Betriebssystem. *xxx* gibt das Betriebssystem an.
callmt1.c callmt2.c		Multithread-Musterdateien
callmtu1.c callmtu2.c		Multithread-Unicode-Musterdateien
libApiDS.xx libApiDS64.xx oder libApiTSM64.xx		Gemeinsam genutzte Bibliothek (das Suffix ist plattformabhängig)

Dateinamen		Beschreibung
dsmgrp.c callevnt.c callhold.c callret.c callbuff.c dpsthread.c		Musterdateien für Gruppierung Musterquellcode für Maßnahme für ereignisgesteuerte Aufbewahrungsdauer Musterquellcode für Status 'Löschen unzulässig' Musterquellcode für Aufbewahrungsschutz für Daten

- UNIX- oder Linux-Musteranwendung erstellen
  Sie erstellen die API-Musteranwendung dapismp unter Verwendung eines Compilers für Ihr Betriebssystem.

64-Bit-Musteranwendung von Windows

Um die Musteranwendung für Microsoft Windows-64-Bit-Systeme zu erstellen und auszuführen, müssen Sie die IBM Spectrum Protect-API installieren und sicherstellen, dass bestimmte Quellendateien vorhanden sind.

Einschränkungen:

- Die besten Ergebnisse werden bei Verwendung von dynamischem Laden erzielt. Nehmen Sie als Beispiel die Datei dynaload.c und die Implementierung im Mustercode.
- Dateien für die Musteranwendung befinden sich in den folgenden Verzeichnissen:

  api64\obj
  : Enthält die Objektdateien des API-Musterprogramms.

  api64\samprun
  : Enthält das Musterprogramm dapismp. Das Musterprogramm enthält das Ausführungsverzeichnis.

- Die DLL-Datei tsmapi64.dll ist eine 64-Bit-DLL-Datei.
- Verwenden Sie Microsoft C/C++ Compiler Version 15 und die Makefile makesmp64.mak, um die API-Musteranwendung dapismp zu kompilieren. Möglicherweise müssen Sie die Makefiles an Ihre Umgebung anpassen, insbesondere die Bibliothek oder die Einschlussverzeichnisse.
- Führen Sie nach der Kompilierung der Anwendung die Musteranwendung durch Ausgabe des Befehls **dapismp** im Verzeichnis api64\samprun aus.
- Wählen Sie aus der Liste der angezeigten Optionen aus. Führen Sie die Anmeldeaktion aus, bevor Sie andere Aktionen ausführen.
- Geben Sie vor dem Dateibereichsnamen, dem übergeordneten und dem untergeordneten Namen bei der Eingabe immer den korrekten Pfadbegrenzer (\) als Präfix an, z. B. \eigenerDateibereich. Sie müssen dieses Präfix auch verwenden, wenn Sie den Stern (*) als Platzhalterzeichen angeben.

Für Windows-Betriebssysteme sind die für das Erstellen der Musteranwendung erforderlichen Quellendateien in Tabelle 1 aufgelistet. Die Musteranwendung ist im API-Paket enthalten. Außerdem befindet sich dort eine vorkompilierte ausführbare Datei (dapismp.exe).

Tabelle 1. Dateien für das Erstellen der Windows-64-Bit-API-Musteranwendung

Dateinamen	Beschreibung
api.txt	Readme-Datei
tsmapi64.dll	API-DLLs
dsmrc.h dsmapitd.h dsmapips.h dsmapifp.h dsmapidl.h release.h	Headerdatei für Rückkehrcodes Headerdatei für allgemeine Typdefinitionen Headerdatei für betriebssystemspezifische Typdefinitionen Headerdatei für Funktionsprototypen Dynamisch geladene Headerdatei für Funktionsprototypen Headerdatei für Releasewerte
dapidata.h dapint64.h dapitype.h dapiutil.h	Headerdateien für Quellcode
tsmapi64.lib	Implizite Bibliothek

Dateinamen	Beschreibung
dapibkup.c dapiinit.c dapint64.c dapipref.c dapiproc.c dapiproc.h dapipw.c dapiqry.c dapirc.c dapismp64.c dapiutil.c dynaload.c	Quellcodedateien für dapismp.exe
makesmpx64.mak (Windows x64) makesmp64.mak (Windows IA64)	Makefile zum Erstellen von Musteranwendungen
callmt1.c callmt2.c callmtu164.c callmtu264.c dpsthread.c	Multithread-Musterdateien Musterdatei mit Quellcode
callevnt.c callhold.c callret.c callbuff.c	Quellcode für Maßnahme für ereignisgesteuerte Aufbewahrungsdauer Musterquellcode für Status 'Löschen unzulässig' Musterquellcode für Aufbewahrungsschutz für Daten Musterquellcode für gemeinsam genutzten Puffer (keine Kopie).

Hinweise zum Entwerfen einer Anwendung

Wenn Sie eine Anwendung entwerfen, müssen Sie über Kenntnisse über viele Aspekte der API verfügen.

Lesen Sie die folgenden Abschnitte, um ein Verständnis für die API zu entwickeln:

- Größenbeschränkungen bestimmen
- API-Versionssteuerung verwalten
- Multithreading verwenden
- Signale und Signalhandler
- Sitzung starten oder beenden
- Objektnamen und -IDs
- Zugriff auf Kennwortdateien steuern
- Zugriff auf Objekte als Sitzungseigner
- Knoten- und eignerübergreifender Zugriff auf Objekte
- Dateibereiche verwalten
- Objekte Verwaltungsklassen zuordnen
- Verfall/Löschen anhalten und freigeben
- IBM Spectrum Protect-System abfragen
- Daten an einen Server senden
- Beispielablaufdiagramme für Sicherung und Archivierung
- Dateigruppierung
- Zustandsdiagrammzusammenfassung für die IBM Spectrum Protect-API

Wenn Sie Ihre Anwendung entwerfen, lesen Sie die Hinweise in Tabelle 1. Startstrukturen mit memset-Feldern werden möglicherweise in nachfolgenden Releases geändert. Der Wert für stVersion erhöht sich mit jeder Produkterweiterung.

Tabelle 1. API: Hinweise zum Entwerfen von Anwendungen

Entwurfselement	Hinweise
Ländereinstellung definieren	Die Anwendung muss die Ländereinstellung festlegen, bevor die API aufgerufen wird. Wenn Sie den Standardwert für die Ländereinstellung verwenden möchten, fügen Sie der Anwendung den folgenden Code hinzu: `setlocale(LC_ALL,"");` Soll ein anderer Wert für die Ländereinstellung definiert werden, verwenden Sie denselben Aufruf mit der entsprechenden Ländereinstellung im zweiten Parameter. Überprüfen Sie die Spezifikationen in der Dokumentation für jedes von Ihnen verwendete Betriebssystem.

Entwurfselement	Hinweise

Sitzungssteuerung	Wenden Sie die folgenden Richtlinien für die Sitzungssteuerung an:
	
	• Weisen Sie jedem von Ihnen verwendeten Produkt des IBM Spectrum Protect-Clients für Sichern/Archivieren und des IBM Spectrum Protect-API-Clients einen eindeutigen Knotennamen zu. Die folgenden Produkte sind Beispiele für diese Clients:
	  ◦ IBM Spectrum Protect for Mail
	  ◦ oder IBM Spectrum Protect HSM for Windows
	• Verwenden Sie während einer Sicherungs- und Zurückschreibungsprozedur einen konsistenten Eignernamen.
	• Verwenden Sie zum Steuern des Zugriffs auf die geschützte Kennwortdatei die Option passwordaccess.
	• Stellen Sie sicher, dass Datenversetzungssitzungen enden, wenn die Task abgeschlossen ist, sodass Einheiten auf dem Server für die Verwendung durch andere Sitzungen freigegeben werden.
	• Verwenden Sie den Funktionsaufruf dsmSetup mit aktiviertem Flag multithread, um LAN-unabhängige Datenübertragung zu gestatten.
	• Wenn Sie unter AIX Multithread-Anwendungen oder LAN-unabhängige Operationen verwenden, insbesondere auf Multiprozessormaschinen, setzen Sie in der Umgebung die Umgebungsvariable AIXTHREAD_SCOPE vor dem Starten der Anwendung auf S, um Leistung und Zeitplanung zu verbessern. Beispiel:
	
	`EXPORT AIXTHREAD_SCOPE=S`
	
	Wenn AIXTHREAD_SCOPE auf S gesetzt ist, werden mit Standardattributen erstellte Benutzerthreads in den systemweiten Zuteilungsbereich gestellt. Wenn ein Benutzerthread mit systemweitem Zuteilungsbereich erstellt wird, wird er an einen Kernel-Thread gebunden und vom Kernel geplant. Der zugrunde liegende Kernel-Thread wird mit keinem anderen Benutzerthread gemeinsam genutzt. Weitere Informationen zu dieser Umgebungsvariablen finden Sie hier:
	
	Multithreading verwenden
	
	• Stellen Sie sicher, dass eine API-Funktion nicht gleichzeitig von mehreren Threads in einer Sitzung aufgerufen wird. Anwendungen, die mehrere Threads mit derselben Sitzungskennung verwenden, müssen die API-Aufrufe synchronisieren. Verwenden Sie beispielsweise einen mutex, um API-Aufrufe zu synchronisieren:
	  ◦ getTSMMutex()
	  ◦ TSM-API-Aufruf ausgeben
	  ◦ releaseTSMMutex()
	Verwenden Sie diese Methode nur, wenn die Threads eine Kennung gemeinsam nutzen. Sie können parallele API-Funktionsaufrufe verwenden, wenn die Aufrufe unterschiedliche Sitzungskennungen verwenden.
	• Implementieren Sie für das Versetzen von Daten ein Konsumenten-/Produzentenmodell mit Threads. Die API-Aufrufe sind synchron und die Aufrufe der Funktionen dsmGetData und dsmSendData blockieren, bis sie beendet sind. Bei Verwendung eines Konsumenten-/Produzentenmodells kann die Anwendung den nächsten Puffer lesen, während sie auf das Netz wartet. Die Entkopplung von Datenlese-/-schreiboperationen und Netzoperationen verbessert außerdem die Leistung, wenn ein Netzengpass oder Verzögerungen vorliegen. Im Allgemeinen gilt:
	
	`Data thread <---> shared queue of buffers <---> communication thread (issue calls to the IBM Spectrum Protect API)`
	
	• Verwenden Sie dieselbe Sitzung für mehrere Operationen, um einen erhöhten Systemaufwand zu vermeiden. Implementieren Sie für Anwendungen, die viele kleine Objekte bearbeiten, die Anwendung von Sitzungspools, sodass dieselbe Sitzung von mehreren kleinen Operationen verwendet werden kann. Systemaufwand ist mit dem Öffnen und Schließen einer Sitzung mit dem IBM Spectrum Protect-Server verbunden. Der Aufruf `dsmInit/dsmInitEX` ist serialisiert, sodass auch in einer Multithread-Anwendung nicht mehrere Threads gleichzeitig angemeldet sein können. Außerdem sendet die API während der Anmeldung eine Reihe von einmaligen Abfragen an den Server, sodass der Server alle Operationen ausführen kann. Diese Abfragen umfassen Maßnahmen, Optionen, Dateibereiche und die lokale Konfiguration.

Entwurfselement	Hinweise
Operationsfolge	Der IBM Spectrum Protect-Server sperrt Datenbankeinträge im Dateibereich während einiger Operationen. Für das Entwerfen von IBM Spectrum Protect-API-Anwendungen gelten folgende Regeln: • Abfragen sperren den Dateibereich während der gesamten Transaktion. • Die Abfragesperre kann mit anderen Abfrageoperationen gemeinsam genutzt werden, so dass mehrere Abfrageoperationen in demselben Dateibereich gleichzeitig ausgeführt werden können. • Die folgenden Operationen werden zum Ändern der IBM Spectrum Protect-Serverdatenbank verwendet (DB Chg): Senden, Abrufen, Umbenennen, Aktualisieren und Löschen. • Die Beendigung einer DB Chg-Operation erfordert eine Dateibereichssperre während der Datenbankänderung am Ende der Transaktion. • Es können mehrere DB Chg-Operationen in demselben Dateibereich gleichzeitig ausgeführt werden. Es kann eine Verzögerung beim Warten auf die Sperre am Ende der Transaktion auftreten. • Die Abfragesperre kann nicht mit DB Chg-Operationen gemeinsam genutzt werden. Eine DB Chg-Operation verzögert den Anfang einer Abfrage in demselben Dateibereich. Daher sollten Sie Ihre Anwendungen so gestalten, dass Abfragen von DB Chg-Operationen in demselben Dateibereich getrennt und serialisiert werden.
Objektbenennung	Beachten Sie beim Benennen von Objekten die folgenden Faktoren: • Die spezifischen Objektnamen sind die übergeordneten und untergeordneten Objektnamen. Enthält der Name eine eindeutige Kennung, z. B. eine Datumszeitmarke, sind Sicherungsobjekte immer aktiv. Die Objekte verfallen nur, wenn sie durch den Funktionsaufruf dsmDeleteObj als inaktiv markiert werden. • Durch die Zurückschreibungsmethode für Objekte wird die Art der Namensformatierung für einfache Abfragen festgelegt. Wenn Sie eine Zurückschreibung von Teilobjekten durchführen wollen, können Sie keine Komprimierung verwenden. Verwenden Sie die Funktion dsmSendObj objAttr objCompressed=bTrue zum Unterdrücken der Komprimierung.
Objektgruppierung	Gruppieren Sie Objekte logisch durch die Verwendung von Dateibereichen. Ein Dateibereich ist ein Container auf dem Server, der eine Gruppierungskategorie für die Objekte darstellt. Die API fragt während der ersten Anmeldung und auch während der Abfragen alle Dateibereiche ab, sodass die Anzahl der Dateibereiche eingeschränkt werden muss. Es ist eine realistische Annahme, dass eine Anwendung 20 bis 100 Dateibereiche pro Knoten aufbaut. Die API kann mehr Dateibereiche verarbeiten, aber jeder Dateibereich stellt einen Aufwand für das System dar. Verwenden Sie das Objekt `Verzeichnis` in der Anwendung, um eine differenziertere Trennung zu erreichen.
Objektbearbeitung	Speichern Sie keine `objectID`-Werte zur Verwendung in späteren Zurückschreibungen. Die Persistenz dieser Werte ist während der Lebensdauer des Objekts nicht garantiert. Achten Sie während einer Zurückschreibung besonders auf die Zurückschreibungsreihenfolge. Sortieren Sie nach der Abfrage anhand dieses Werts, bevor die Zurückschreibung ausgeführt wird. Wenn Sie mehrere Typen serieller Datenträger verwenden, greifen Sie in separaten Sitzungen auf die verschiedenen Datenträgertypen zu. Weitere Informationen finden Sie im folgenden Thema: Objekte nach Zurückschreibungsreihenfolge auswählen und sortieren
Verwaltungsklasse	Überlegen Sie, wie viel Kontrolle die Anwendung über die Verwaltungsklasse haben muss, die den Anwendungsobjekten zugeordnet ist. Sie können Einschlussanweisungen definieren oder einen Namen im Funktionsaufruf dsmSendObj angeben.
Objektgröße	IBM Spectrum Protect benötigt eine Größenschätzung für jedes Objekt. Überlegen Sie, wie Ihre Anwendung die Größe eines Objekts schätzt. Eine zu hohe Schätzung der Objektgröße ist besser als eine zu niedrige.

- Größenbeschränkungen bestimmen
  Bestimmte Datenstrukturen oder Felder in der API unterliegen Größenbeschränkungen. Bei diesen Strukturen handelt es sich häufig um Namen oder andere Textfelder, die eine vordefinierte Länge nicht überschreiten dürfen.
- API-Versionssteuerung verwalten
  Für alle APIs gibt es eine Form der Versionssteuerung. Die von Ihnen in Ihrer Anwendung verwendete API-Version muss mit der Version der API-Bibliothek kompatibel sein, die auf der Benutzerworkstation installiert ist.
- Multithreading verwenden
  Die Multithread-API ermöglicht Anwendungen das Erstellen mehrerer Sitzungen mit dem IBM Spectrum Protect-Server innerhalb desselben Prozesses. Die API kann erneut aufgerufen werden. Alle Aufrufe können in unterschiedlichen Threads parallel ausgeführt werden.
- Signale und Signalhandler
  Die Anwendung verarbeitet Signale vom Benutzer oder vom Betriebssystem. Wenn der Benutzer die Tastenanschlagfolge Strg+C drückt, muss die Anwendung das Signal abfangen und Aufrufe dsmTerminate für jeden aktiven Thread senden. Rufen Sie dann dsmCleanUp auf, um die Anwendung zu beenden. Wenn Sitzungen nicht korrekt geschlossen werden, können auf dem Server nicht erwartete Ergebnisse auftreten.
- Sitzung starten oder beenden
  IBM Spectrum Protect ist ein sitzungsbasiertes Produkt und alle Aktivitäten müssen innerhalb einer IBM Spectrum Protect-Sitzung

ausgeführt werden. Zum Starten einer Sitzung startet die Anwendung den Aufruf dsmInitEx. Dieser Aufruf muss vor jedem anderen API-Aufruf ausgeführt werden, der nicht dsmQueryApiVersionEx, dsmQueryCliOptions oder dsmSetUp ist.

- Objektnamen und -IDs
  Der IBM Spectrum Protect-Server ist ein Objektspeicherserver, dessen Funktion in erster Linie darin besteht, benannte Objekte effizient zu speichern und abzurufen. Die Objekt-ID ist für jedes Objekt eindeutig und bleibt dem Objekt während der gesamten Lebensdauer zugeordnet, *es sei denn*, das Objekt wird exportiert oder importiert.
- Zugriff auf Objekte als Sitzungseigner
  Jedem Objekt ist ein Eignername zugeordnet. Die Regeln, die festlegen, auf welche Objekte zugegriffen wird, sind von dem Eignernamen abhängig, der beim Starten einer Sitzung verwendet wird. Steuern Sie mithilfe dieses Werts für den Sitzungseigner den Zugriff auf das Objekt.
- Knoten- und eignerübergreifender Zugriff auf Objekte
  Drei Funktionsaufrufe unterstützen knoten- und eignerübergreifenden Zugriff auf derselben Plattform: **dsmSetAccess**, **dsmDeleteAccess** und **dsmQueryAccess**. Diese Funktionen in Verbindung mit den Zeichenfolgeoptionen *-fromnode* und *-fromowner*, die in **dsmInitEx** übergeben werden, gestatten einen vollständigen knotenübergreifenden Abfrage-, Zurückschreibungs- und Abrufprozess über die API.
- Dateibereiche verwalten
  Da Dateibereiche für den Betrieb des Systems wichtig sind, wird eine separate Gruppe von Aufrufen zum Registrieren, Aktualisieren und Löschen von Dateibereichs-IDs verwendet. Bevor Sie Objekte, die einem Dateibereich auf dem System zugeordnet sind, speichern können, müssen Sie den Dateibereich zunächst bei IBM Spectrum Protect registrieren.
- Objekte Verwaltungsklassen zuordnen
  Ein wichtiges Merkmal von IBM Spectrum Protect ist die Verwendung von Maßnahmen (Verwaltungsklassen), die definieren, wie Objekte im IBM Spectrum Protect-Speicher gespeichert und verwaltet werden. Ein Objekt wird bei seiner Sicherung oder Archivierung einer Verwaltungsklasse zugeordnet.
- Verfall/Löschen anhalten und freigeben
  Sie können das Löschen und den Verfall bestimmter Archivierungsobjekte als Reaktion auf eine anstehende oder laufende Aktion, die das Anhalten bestimmter Daten erfordert, anhalten. Falls eine Aktion eingeleitet wird, die möglicherweise Zugriff auf Daten erfordert, müssen diese Daten verfügbar sein, bis die Aktion abgeschlossen ist und der Zugriff auf die Daten im Rahmen dieses Prozesses nicht mehr erforderlich ist. Nachdem festgestellt wurde, dass die Aussetzung nicht mehr erforderlich ist (Freigabe), wird die normale Zeitplanung für Löschen und Verfall über den ursprünglichen Aufbewahrungszeitraum wieder aufgenommen.
- IBM Spectrum Protect-System abfragen
  Die API enthält mehrere Abfragen, beispielsweise eine Verwaltungsklassenabfrage, die von Anwendungen verwendet werden können.
- Servereffizienz
  Beachten Sie diese Richtlinien beim Abrufen von Objekten vom IBM Spectrum Protect-Server oder beim Senden von Objekten an den Server.
- Daten an einen Server senden
  Die API ermöglicht Anwendungsclients das Senden von Daten oder benannten Objekten und ihrer zugehörigen Daten in IBM Spectrum Protect-Serverspeicher.
- API für das Senden von Leistungsdaten an die Clientleistungsüberwachung konfigurieren
  Die Clientleistungsüberwachung ist eine Komponente des Tivoli Storage Manager Administration Center, die zum Anzeigen von Leistungsdaten verwendet wird, die von der API erfasst wurden. Die Clientleistungsüberwachung zeichnet Leistungsdaten für Clientsicherungs-, -archivierungs- und -zurückschreibungsoperationen auf und zeigt diese Daten an.
- Objekte an den Server senden
  Anwendungsclients können Daten oder benannte Objekte und ihre zugehörigen Daten mithilfe der API-Sicherungs- und -Archivierungsfunktionen in IBM Spectrum Protect-Speicher senden. Die Sicherungs- und Archivierungskomponenten des Systems ermöglichen die Verwendung unterschiedlicher Verwaltungsprozeduren für Daten, die in den Speicher gesendet werden.
- Datendeduplizierung
  Die Datendeduplizierung ist eine Methode zum Verringern des Speicherbedarfs, indem redundante Daten eliminiert werden.
- Anwendungsübernahme
  Wenn der IBM Spectrum Protect-Server wegen einer Betriebsunterbrechung nicht mehr verfügbar ist, können Anwendungen, die die API verwenden, für die Datenwiederherstellung automatisch eine Übernahme auf einem Sekundärserver durchführen.
- Beispielablaufdiagramme für Sicherung und Archivierung
  Der Entwurf der API basiert auf direkten Logikabläufen und klaren Übergängen zwischen den verschiedenen Zuständen des Anwendungsclients. Aufgrund dieser deutlichen Zustandsübergänge werden Logik- und Programmfehler frühzeitig im Entwicklungszyklus abgefangen und somit Qualität und Zuverlässigkeit des Systems erheblich verbessert.
- Dateigruppierung
  Die IBM Spectrum Protect-API verfügt über ein Protokoll zum Gruppieren logischer Dateien, mit dem mehrere einzelne Objekte in Gruppen zusammengefasst werden. Sie können diese Gruppen auf dem Server als eine logische Gruppe referenzieren und verwalten. Bei einer logischen Gruppe müssen alle Gruppenmitglieder und der Gruppenleiter zu demselben Knoten und Dateibereich auf dem Server gehören.
- Daten von einem Server empfangen
  Anwendungsclients können Daten oder benannte Objekte und ihre zugehörigen Daten aus IBM Spectrum Protect-Speicher über die Zurückschreibungs- und Abruffunktionen empfangen. Die Zurückschreibungsfunktion greift auf Objekte zu, die zuvor gesichert wurden; die Abruffunktion greift auf Objekte zu, die zuvor archiviert wurden.
- Objekte auf dem Server aktualisieren und löschen
  Ihre API-Anwendungen können Objekte, die archiviert oder gesichert wurden, mithilfe des Funktionsaufrufs **dsmUpdateObj** oder **dsmUpdateObjEx** aktualisieren. Verwenden Sie beide Aufrufe nur im Sitzungsstatus und aktualisieren Sie jeweils nur ein einziges Objekt. Verwenden Sie **dsmUpdateObjEx**, um mehrere Archivierungsobjekte zu aktualisieren, die denselben Namen enthalten.
- Ereignisse protokollieren
  Eine API-Anwendung kann Ereignisnachrichten an zentralen Positionen protokollieren. Die Anwendung kann die Protokollierung an den IBM Spectrum Protect-Server und/oder die lokale Maschine übertragen. Der Funktionsaufruf dsmLogEventEx wird in einer Sitzung

ausgeführt. Um Nachrichten anzuzeigen, die auf dem Server protokolliert sind, verwenden Sie den Befehl query actlog über den Verwaltungsclient.
- Zustandsdiagrammzusammenfassung für die IBM Spectrum Protect-API
  Überprüfen Sie alle Überlegungen beim Erstellen Ihrer eigenen Anwendung mit der IBM Spectrum Protect-API mithilfe dieses Zustandsdiagramms mit der Zusammenfassung einer vollständigen Anwendung.

Größenbeschränkungen bestimmen

Bestimmte Datenstrukturen oder Felder in der API unterliegen Größenbeschränkungen. Bei diesen Strukturen handelt es sich häufig um Namen oder andere Textfelder, die eine vordefinierte Länge nicht überschreiten dürfen.

Die folgenden Felder sind Beispiele für Datenstrukturen mit Größenbeschränkungen:

- Anwendungstyp
- Archivierungsbeschreibung
- Ziel für Kopiengruppe
- Kopiengruppenname
- Dateibereichsinformationen
- Verwaltungsklassenname
- Objekteignername
- Kennwort

Diese Grenzwerte sind als Konstanten in der Headerdatei dsmapitd.h definiert. Jede Speicherzuordnung basiert auf diesen Konstanten und nicht auf von Ihnen eingegebenen Werten. Weitere Informationen finden Sie in Quellendateien für API-Typdefinitionen.

API-Versionssteuerung verwalten

Für alle APIs gibt es eine Form der Versionssteuerung. Die von Ihnen in Ihrer Anwendung verwendete API-Version muss mit der Version der API-Bibliothek kompatibel sein, die auf der Benutzerworkstation installiert ist.

dsmQueryApiVersionEx sollte der erste API-Aufruf sein, den Sie bei Verwendung der API eingeben. Dieser Aufruf führt die folgenden Tasks aus:

- bestätigt, dass die API-Bibliothek auf dem System des Endbenutzers installiert und verfügbar ist.
- gibt den Versionsstand der API-Bibliothek zurück, auf die die Anwendung zugreift.

Die API ist auf Aufwärtskompatibilität angelegt. Für ältere Versionen oder Releases der API-Bibliothek geschriebene Anwendungen funktionieren ordnungsgemäß, wenn Sie eine höhere Version ausführen.

Die Bestimmung des Releases der API-Bibliothek ist sehr wichtig, weil einige Releases einen anderen Speicherbedarf und andere Datenstrukturdefinitionen haben können. Abwärtskompatibilität ist unwahrscheinlich. Informationen zu Ihrer Plattform finden Sie in Tabelle 1.

Tabelle 1. Plattformkompatibilitätsinformationen

Plattform	Beschreibung
Windows	Die Nachrichtendateien müssen dieselbe Version wie die Bibliothek (DLL) haben.
UNIX oder Linux	Die API-Bibliothek und die Nachrichtendateien müssen dieselbe Version haben.

Der Aufruf **dsmQueryApiVersionEx** gibt die Version der API-Bibliothek zurück, die auf der Endbenutzerworkstation installiert ist. Dann können Sie den zurückgegebenen Wert mit der Version der API vergleichen, die der Anwendungsclient verwendet.

Die API-Versionsnummer des Anwendungsclients wird als Gruppe von vier in dsmapitd.h definierten Konstanten in den kompilierten Objektcode eingegeben:

```
DSM_API_VERSION
DSM_API_RELEASE
DSM_API_LEVEL
DSM_API_SUB_LEVEL
```

Siehe Quellendateien für API-Typdefinitionen.

Die API-Version des Anwendungsclients sollte kleiner-gleich der Version der API-Bibliothek sein, die auf dem Benutzersystem installiert ist. Beachten Sie alle anderen Bedingungen. Sie können den Aufruf **dsmQueryApiVersionEx** jederzeit eingeben, unabhängig davon, ob die API-Sitzung gestartet wurde oder nicht.

Von der API verwendete Datenstrukturen enthalten ebenfalls Versionssteuerungsinformationen. Strukturen enthalten Versionsinformationen als erstes Feld. Wenn Erweiterungen an Strukturen vorgenommen werden, wird die Versionsnummer erhöht. Wenn Sie das Versionsfelds initialisieren, verwenden Sie den definierten Strukturversionswert in dsmapitd.h.

Abbildung 1 zeigt die Typdefinition der Struktur dsmApiVersionEx aus der Headerdatei dsmapitd.h. In dem Beispiel wird dann eine globale Variable mit dem Namen ***apiLibVer*** definiert. Außerdem wird die Verwendung in einem Aufruf an **dsmQueryApiVersionEx** gezeigt, mit dem die Version der API-Bibliothek des Endbenutzers zurückgegeben wird. Schließlich wird der zurückgegebene Wert mit der API-Versionsnummer des Anwendungsclients verglichen.

Abbildung 1. Beispiel für das Abrufen des Versionsstands der API

```
typedef struct
{
        dsUint16_t     stVersion;              /* Strukturversion              */
        dsUint16_t version;       /* API-Version                       */
        dsUint16_t release;       /* API-Release                       */
        dsUint16_t level;         /* API-Stand                         */
        dsUint16_t subLevel;      /* API-Unterstufe                    */
} dsmApiVersionEx;

dsmApiVersionEx apiLibVer;

memset(&apiLibVer,0x00,sizeof(dsmApiVersionEx));
dsmQueryApiVersionEx(&apiLibVer);

/* Kompatibilitätsproblemprüfung */
dsInt16_t appVersion= 0, libVersion = 0;
  appVersion=(DSM_API_VERSION * 10000)+(DSM_API_RELEASE * 1000) +
              (DSM_API_LEVEL * 100) + (DSM_API_SUBLEVEL);
  libVersion = (apiLibVer.version * 10000) + (apiLibVer.release * 1000) +
                  (apiLibVer.level * 100) + (apiLibVer.subLevel);
   if (libVersion < appVersion)
   {
      printf("\n************************************************************\n");
      printf("Die IBM Spectrum Protect-Bibliothek ist niedriger als die Anwendungsversion.\n");
      printf("Installieren Sie die aktuelle Bibliotheksversion.\n");
      printf("************************************************************\n");
      return 0;
   }

printf("* API Library Version = %d.%d.%d.%d  *\n",
     apiLibVer.version,
     apiLibVer.release,
     apiLibVer.level,
     apiLibVer.subLevel);
```

Multithreading verwenden

Die Multithread-API ermöglicht Anwendungen das Erstellen mehrerer Sitzungen mit dem IBM Spectrum Protect-Server innerhalb desselben Prozesses. Die API kann erneut aufgerufen werden. Alle Aufrufe können in unterschiedlichen Threads parallel ausgeführt werden.

Tipp: Wenn Sie Anwendungen ausführen, die eine Multithread-API voraussetzen, verwenden Sie den Aufruf **dsmQueryAPIVersionEx**.

Um die API im Multithread-Modus auszuführen, setzen Sie den Wert *mtflag* im Aufruf **dsmSetUp** auf DSM_MULTITHREAD. Der Aufruf **dsmSetUp** muss der erste Aufruf nach dem Aufruf **dsmQueryAPIVersionEx** sein. Dieser Aufruf muss zurückkehren, bevor ein Thread den Aufruf **dsmInitEx** aufruft. Nachdem die Ausführung aller Threads beendet ist, geben Sie einen Aufruf **dsmCleanUp** ein. Der primäre Prozess darf nicht enden, bevor nicht die Verarbeitung aller Threads abgeschlossen ist. Siehe callmt1.c in der Musteranwendung.

Einschränkung: Der Standardmodus für die API ist der Einzelthread-Modus. Wenn eine Anwendung **dsmSetUp** nicht mit der Angabe DSM_MULTITHREAD für den Wert *mtflag* aufruft, erlaubt die API für jeden Prozess nur eine einzige Sitzung.

Sobald der Aufruf **dsmSetUp** erfolgreich ausgeführt wurde, kann die Anwendung mehrere Threads starten und mehrere Aufrufe **dsmInitEx** ausführen. Jeder Aufruf **dsmInitEx** gibt eine Kennung für diese Sitzung zurück. Alle nachfolgenden Aufrufe in diesem Thread für diese Sitzung müssen diesen Wert für die Kennung verwenden. Bei bestimmten Werten handelt es sich um prozessweite Umgebungsvariablen (Werte, die im Aufruf **dsmSetUp** definiert werden). Bei jedem Aufruf **dsmInitEx** werden die Optionen erneut syntaktisch analysiert. Jeder Thread kann mit unterschiedlichen Optionen ausgeführt werden, indem eine Überschreibungsdatei oder eine Optionszeichenfolge im Aufruf **dsmInitEx** angegeben wird. Damit können unterschiedliche Threads auf verschiedenen Servern ausgeführt werden oder verschiedene Knotennamen verwenden.

Empfehlung: Definieren Sie bei HP den Thread-Stack mit 64 KB oder höher. Der Standardwert für den Thread-Stack (32 KB) ist möglicherweise nicht hoch genug.

Um Anwendungsbenutzern die Verwendung einer LAN-unabhängigen Sitzung zu ermöglichen, geben Sie **dsmSetUp** *mtFlag DSM_MULTITHREAD* in Ihrer Anwendung an. Dies ist selbst dann erforderlich, wenn es sich bei der Anwendung um eine Einzelthread-Anwendung handelt. Mit diesem Flag wird das für die LAN-unabhängige Schnittstelle von IBM Spectrum Protect erforderliche Threading aktiviert.

Signale und Signalhandler

Die Anwendung verarbeitet Signale vom Benutzer oder vom Betriebssystem. Wenn der Benutzer die Tastenanschlagfolge Strg+C drückt, muss die Anwendung das Signal abfangen und Aufrufe dsmTerminate für jeden aktiven Thread senden. Rufen Sie dann dsmCleanUp auf, um die Anwendung zu beenden. Wenn Sitzungen nicht korrekt geschlossen werden, können auf dem Server nicht erwartete Ergebnisse auftreten.

Die Anwendung erfordert Signalhandler, wie beispielsweise SIGPIPE und SIGUSR1, für Signale, die die Beendigung der Anwendung zur Folge haben. Die Anwendung empfängt dann den Rückkehrcode von der API. Um beispielsweise SIGPIPE zu ignorieren, fügen Sie Ihrer Anwendung die

folgende Anweisung hinzu: `signal(SIGPIPE, SIG_IGN)`. Nachdem diese Angabe hinzugefügt wurde, wird die Anwendung bei einer unterbrochenen Pipe nicht mehr beendet, sondern der korrekte Rückkehrcode zurückgegeben.

Sitzung starten oder beenden

IBM Spectrum Protect ist ein sitzungsbasiertes Produkt und alle Aktivitäten müssen innerhalb einer IBM Spectrum Protect-Sitzung ausgeführt werden. Zum Starten einer Sitzung startet die Anwendung den Aufruf dsmInitEx. Dieser Aufruf muss vor jedem anderen API-Aufruf ausgeführt werden, der nicht dsmQueryApiVersionEx, dsmQueryCliOptions oder dsmSetUp ist.

Die Funktion dsmQueryCliOptions kann nur vor dem Aufruf dsmInitEx aufgerufen werden. Die Funktion gibt die Werte wichtiger Optionen zurück, beispielsweise Optionsdateien, Komprimierungseinstellungen und Kommunikationsparameter. Der Aufruf dsmInitEx richtet eine Sitzung mit dem Server gemäß den Angaben in den Parametern ein, die in dem Aufruf übergeben werden oder die in der Optionsdatei definiert sind.

Der Clientknotenname, der Eignername und die Kennwortparameter werden an den Aufruf dsmInitEx übergeben. Beim Eignernamen muss die Groß-/Kleinschreibung beachtet werden, beim Knotennamen und Kennwort nicht. Die Anwendungsclientknoten müssen im Server registriert werden, bevor eine Sitzung gestartet wird.

Jedes Mal, wenn ein API-Anwendungsclient eine Sitzung mit dem Server startet, wird der Clientanwendungstyp im Server registriert. Geben Sie als Wert für den Anwendungstyp immer eine Abkürzung für das Betriebssystem an, da dieser Wert in das Plattformfeld auf dem Server eingegeben wird. Die maximale Länge für die Zeichenfolge ist DSM_MAX_PLATFORM_LENGTH.

Der Funktionsaufruf dsmInitEx richtet die IBM Spectrum Protect-Sitzung mit der API-Konfigurationsdatei und -Optionsliste des Anwendungsclients ein. Der Anwendungsclient kann mit der API-Konfigurationsdatei und -Optionsliste eine Reihe von IBM Spectrum Protect-Optionen definieren. Diese Werte überschreiben die während der Installation in den Benutzerkonfigurationsdateien definierten Werte. Benutzer können die vom Administrator definierten Optionen nicht ändern. Wenn der Anwendungsclient keine bestimmte Konfigurationsdatei und Optionsliste hat, können Sie für diese beiden Parameter NULL angeben. Weitere Informationen zu Konfigurationsdateien finden Sie hier:

Erläuterungen zu Konfigurations- und Optionsdateien

Der Funktionsaufruf dsmInitEx richtet die IBM Spectrum Protect-Sitzung ein. Dabei werden Parameter verwendet, die eine erweiterte Überprüfung ermöglichen.

Überprüfen Sie den Funktionsaufruf dsmInitEx und den Informationsrückkehrcode dsmInitExOut. Der Administrator hat die letzte Sitzung abgebrochen, wenn der Rückkehrcode ok ist (RC=ok) und der Informationsrückkehrcode (infoRC) DSM_RC_REJECT_LASTSESS_CANCELED lautet. Soll die aktuelle Sitzung sofort beendet werden, rufen Sie dsmTerminate auf.

Der Aufruf dsmQuerySessOptions gibt dieselben Felder wie der Aufruf dsmQueryCliOptions zurück. Der Aufruf kann nur in einer Sitzung gesendet werden. Die Werte geben die Clientoptionen wieder, die während dieser Sitzung gültig sind (Werte aus Optionsdateien und alle Überschreibungswerte aus dem Aufruf dsmInitEx).

Nach dem Start einer Sitzung kann die Anwendung einen Aufruf dsmQuerySessInfo senden, um die für diese Sitzung definierten Serverparameter zu bestimmen. Mit diesem Aufruf werden Elemente wie die Maßnahmendomäne und Transaktionsgrenzwerte an die Anwendung zurückgegeben.

Beenden Sie Sitzungen mit einem Aufruf **dsmTerminate**. Alle Verbindungen zum Server werden beendet und alle Ressourcen, die dieser Sitzung zugeordnet sind, werden freigegeben.

Ein Beispiel für das Starten und Beenden einer Sitzung finden Sie hier:

Abbildung 1

In dem Beispiel wird eine Reihe von globalen und lokalen Variablen definiert, die in Aufrufen dsmInitEx und dsmTerminate verwendet werden. Im Aufruf dsmInitEx wird ein Verweis auf `dsmHandle` als Parameter verwendet, während im Aufruf dsmTerminate `dsmHandle` als Parameter verwendet wird. Das Beispiel in Abbildung 2 zeigt die Details von rcApiOut an. Die Funktion rcApiOut ruft die API-Funktion dsmRCMsg auf, die einen Rückkehrcode in eine Nachricht umsetzt. Der Aufruf rcApiOut gibt dann die Nachricht für den Benutzer aus. Eine Version von rcApiOut ist in der API-Musteranwendung enthalten. Die Funktion dsmApiVersion ist eine Typdefinition, die sich in der Headerdatei dsmapitd.h befindet.

- Sitzungssicherheit
  Das sitzungsbasierte System IBM Spectrum Protect verfügt über Sicherheitskomponenten, die Anwendungen das Starten von Sitzungen auf sichere Art und Weise ermöglichen. Diese Sicherheitsmaßnahmen verhindern den unbefugten Zugriff auf den Server und unterstützen die Gewährleistung der Systemintegrität.
- Zugriff auf Kennwortdateien steuern
  Um den Zugriff auf die geschützten Kennwortdateien auf UNIX- und Linux-Systemen zu steuern, können Sie sich als berechtigter Benutzer anmelden und die Option passwordaccess auf generate setzen.
- Benutzer mit Verwaltungsaufgaben mit Clienteignerberechtigung erstellen
  Ein Benutzer mit Verwaltungsaufgaben mit Clienteignerberechtigung kann Parameter im Funktionsaufruf dsmInitEx definieren, um Sitzungen zu starten. Dieser Benutzer kann als "Benutzer mit Verwaltungsaufgaben" mit Sicherungs- und Zurückschreibungsberechtigung für die definierten Knoten arbeiten.

Sitzungssicherheit

Das sitzungsbasierte System IBM Spectrum Protect verfügt über Sicherheitskomponenten, die Anwendungen das Starten von Sitzungen auf sichere Art und Weise ermöglichen. Diese Sicherheitsmaßnahmen verhindern den unbefugten Zugriff auf den Server und unterstützen die Gewährleistung der Systemintegrität.

Jede Sitzung, die mit dem Server gestartet wird, muss einen Anmeldeprozess durchlaufen und erfordert ein Kennwort. Wenn das Kennwort zusammen mit dem Knotennamen des Clients angegeben wird, ist beim Herstellen der Verbindung zum Server die korrekte Berechtigung gewährleistet. Der Anwendungsclient stellt der API dieses Kennwort zum Starten der Sitzung zur Verfügung.

Es gibt zwei Methoden der Kennwortverarbeitung: *passwordaccess=prompt* und *passwordaccess=generate*. Wenn Sie die Option *passwordaccess=prompt* verwenden, müssen Sie den Kennwortwert bei jedem Aufruf von **dsmInitEx** angeben. Sie können auch den Knotennamen und Eignernamen im **dsmInitEx**-Aufruf angeben.

Jedem Kennwort ist eine Ablaufzeit zugeordnet. Wenn ein **dsmInitEx**-Aufruf mit einem Rückkehrcode wegen eines abgelaufenen Kennworts (DSM_RC_REJECT_VERIFIER_EXPIRED) fehlschlägt, muss der Anwendungsclient den Aufruf dsmChangePW mit der Kennung eingeben, die von **dsmInitEx** zurückgegeben wird. Dadurch wird das Kennwort aktualisiert, bevor die Sitzung erfolgreich eingerichtet werden kann. Das Beispiel in Abbildung 3 zeigt die Vorgehensweise bei der Änderung eines Kennworts mithilfe von **dsmChangePW**. Der Anmeldeeigner muss eine Rootbenutzer-ID oder eine ID des berechtigten Benutzers verwenden, um das Kennwort ändern zu können.

Bei der zweiten Methode, *passwordaccess=generate*, wird der Kennwortwert in einer Datei verschlüsselt und gespeichert. Der Knotenname und Eignername können nicht im Aufruf **dsmInitEx** angegeben werden und die Systemstandardwerte werden verwendet. Dadurch wird die Sicherheit der Kennwortdatei gewährleistet. Wenn das Kennwort abläuft, erstellt der Parameter generate ein neues und aktualisiert die Kennwortdatei automatisch.

Hinweise:

1. Wenn zwei verschiedene physische Maschinen über denselben IBM Spectrum Protect-Knotennamen verfügen oder wenn auf einem Knoten mehrere Pfade mit mehreren Serverzeilengruppen definiert sind, funktioniert *passwordaccess=generate* möglicherweise nur für die Zeilengruppe, die nach dem Ablauf der Kennwortgültigkeit als Erstes verwendet wird. Während des ersten Client/Server-Kontakts muss der Benutzer dasselbe Kennwort für jede Serverzeilengruppe separat angeben und für jede Zeilengruppe wird eine Kopie des Kennworts separat gespeichert. Wenn das Kennwort abläuft, wird ein neues Kennwort für die Zeilengruppe generiert, die eine Verbindung des ersten Client/Server-Kontakts herstellt. Alle nachfolgenden Versuche, eine Verbindung über andere Serverzeilengruppen herzustellen, schlagen fehl, weil es keine logische Verbindung zwischen den jeweiligen Kopien des alten Kennworts und der aktualisierten Kopie gibt, die von der Zeilengruppe generiert wird, die nach dem Ablauf der Kennwortgültigkeit als Erstes verwendet wird. In diesem Fall müssen Sie die Kennwörter vor dem Ablauf oder nach dem Ablauf als Wiederherstellungsmaßnahme dieser Situation wie folgt aktualisieren:
    a. Führen Sie **dsmadmc** aus und aktualisieren Sie das Kennwort auf dem Server.
    b. Führen Sie **dsmc -servername=stanza1** aus und verwenden Sie das neue Kennwort, um einen ordnungsgemäßen Eintrag zu generieren.
    c. Führen Sie **dsmc -servername=stanza2** aus und verwenden Sie das neue Kennwort, um einen ordnungsgemäßen Eintrag zu generieren.
2. Für UNIX oder Linux: Nur der Rootbenutzer oder ein berechtigter Benutzer kann das Kennwort ändern, wenn *passwordaccess=prompt* verwendet wird. Nur der Rootbenutzer oder ein berechtigter Benutzer kann die Kennwortdatei starten, wenn *passwordaccess=generate* verwendet wird.
   Einschränkung: Die Optionen users und groups werden nicht erkannt.

Eine Anwendung kann den Benutzerzugriff mit anderen Mitteln beschränken, z. B. durch Zugriffsfilter.

Anwendungen, die mehrere IP-Verbindungen zu einem einzelnen IBM Spectrum Protect-Server verwenden, sollten denselben Knotennamen und dasselbe IBM Spectrum Protect-Clientkennwort für jede Sitzung verwenden. Gehen Sie wie folgt vor, um diese Unterstützung zu aktivieren:

1. Definieren Sie eine IBM Spectrum Protect-Serverzeilengruppe in der Datei dsm.sys.
2. Geben Sie für die Verbindungen, die nicht die IP-Standardadresse verwenden, die Optionswerte für die *TCPserver*-Adresse und *TCPport* im Aufruf **dsmInitEx** an.

Diese Werte überschreiben die IP-Verbindungsdaten, aber die Sitzung verwendet weiterhin dieselben Knoten- und Kennwortinformationen der Zeilengruppe in dsm.sys.

Anmerkung: Knoten in einem Cluster verwenden ein Kennwort gemeinsam.
Abbildung 1. Beispiel für das Starten und Beenden einer Sitzung

```
dsmApiVersionEx * apiApplVer;
char           *node;
char           *owner;
char           *pw;
char           *confFile = NULL;
char           *options = NULL;
dsInt16_t      rc = 0;
dsUint32_t     dsmHandle;
dsmInitExIn_t  initIn;
dsmInitExOut_t initOut;
char           *userName;
char           *userNamePswd;

memset(&initIn, 0x00, sizeof(dsmInitExIn_t));
memset(&initOut, 0x00, sizeof(dsmInitExOut_t));
```

```
memset(&apiApplVer,0x00,sizeof(dsmapiVersionEx));
apiApplVer.version = DSM_API_VERSION; /* Set the applications compile */
apiApplVer.release = DSM_API_RELEASE;  /* time version. */
apiApplVer.level   = DSM_API_LEVEL;
apiApplVer.subLevel= DSM_API_SUBLEVEL;

printf("Doing signon for node %s, owner %s, with password %s\n", node,owner,pw);

initIn.stVersion = dsmInitExInVersion;
initIn.dsmApiVersionP = &apiApplVer
initIn.clientNodeNameP = node;
initIn.clientOwnerNameP = owner ;
initIn.clientPasswordP = pw;
initIn.applicationTypeP = "Sample-API AIX";
initIn.configfile = confFile;
initIn.options = options;
initIn.userNameP = userName;
initIn.userPasswordP = userNamePswd;
rc = dsmInitEx(&dsmHandle, &initIn, &initOut);

if (rc == DSM_RC_REJECT_VERIFIER_EXPIRED)
{
   printf("*** Password expired. Select Change Password.\n");
   return(rc);
}
else if (rc)
{
   printf("*** Init failed: ");
   rcApiOut(dsmHandle, rc);   /* Call function to print error message */
   dsmTerminate(dsmHandle);    /* clean up memory blocks */
   return(rc);
}
```

Abbildung 2. Details für rcApiOut

```
void rcApiOut (dsUint32_t handle, dsInt16_t rc)
{
     char *msgBuf ;

     if ((msgBuf = (char *)malloc(DSM_MAX_RC_MSG_LENGTH+1)) == NULL)
     {
          printf("Abort:  Not enough memory.\n") ;
          exit(1) ;
      }

      dsmRCMsg(handle, rc, msgBuf);
      printf("
      free(msgBuf) ;
      return;
}
```

Abbildung 3. Beispiel für eine Kennwortänderung

```
printf("Enter your current password:");
gets(current_pw);
printf("Enter your new password:");
gets(new_pw1);
printf("Enter your new password again:");
gets(new_pw2);
/* If new password entries don't match, try again or exit. */
/* If they do match, call dsmChangePW. */

rc = dsmChangePW(dsmHandle,current_pw,new_pw1);
if (rc)
{
   printf("*** Password change failed.  Rc =
}
   else
{
   printf("*** Your new password has been accepted and updated.\n");
}
return 0;
```

Zugriff auf Kennwortdateien steuern

Um den Zugriff auf die geschützten Kennwortdateien auf UNIX- und Linux-Systemen zu steuern, können Sie sich als berechtigter Benutzer anmelden und die Option passwordaccess auf generate setzen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um passwordaccess auf generate zu setzen:

1. Geben Sie beim Schreiben der Anwendung einen Aufruf dsmSetUp an, der *argv[0]* übergibt. *Argv[0]* enthält den Namen der Anwendung, mit der die API aufgerufen wird. Die Anwendung kann durch einen berechtigten Benutzer ausgeführt werden, der Administrator muss jedoch den Anmeldenamen für den berechtigten Benutzer festlegen.
2. Setzen Sie das Bit für die aktuelle Benutzer-ID (Bit S) für die ausführbare Anwendung auf Ein. Der Eigner der ausführbaren Datei der Anwendung kann dann zu einem berechtigten Benutzer werden und eine Kennwortdatei erstellen, Kennwörter aktualisieren und Anwendungen ausführen. Der Eigner der ausführbaren Datei der Anwendung muss mit der Benutzer-ID übereinstimmen, die das Programm ausführt. In dem folgenden Beispiel ist `user1` der *`Benutzer`* und `applA` der Name der ausführbaren Datei der Anwendung; `user1` hat Schreib-/Lesezugriff auf das Verzeichnis /home/user1. Die ausführbare Datei `applA` hat die folgenden Berechtigungen:

   ```
   -rwsr-xr-x user1    group1   applA
   ```

3. Weisen Sie die Benutzer der Anwendung an, für die Anmeldung den Namen des berechtigten Benutzers zu verwenden. IBM Spectrum Protect prüft, ob die Anmelde-ID mit dem Eigner der ausführbaren Anwendung übereinstimmt, bevor der Zugriff auf die geschützte Kennwortdatei erlaubt wird.
4. Setzen Sie die Option passworddir in der Datei dsm.sys so, dass sie auf ein Verzeichnis verweist, für das dieser Benutzer über Schreib-/Lesezugriff verfügt. Geben Sie beispielsweise die folgende Zeile in der Serverzeilengruppe der Datei dsm.sys ein:

   ```
   passworddir /home/user1
   ```

5. Erstellen Sie die Kennwortdatei und stellen Sie sicher, dass der berechtigte Benutzer Eigner der Datei ist.
6. Melden Sie sich als `user1` an und führen Sie `applA` aus.
7. Rufen Sie dsmSetUp auf und übergeben Sie *argv*.

Benutzer mit Verwaltungsaufgaben mit Clienteignerberechtigung erstellen

Ein Benutzer mit Verwaltungsaufgaben mit Clienteignerberechtigung kann Parameter im Funktionsaufruf dsmInitEx definieren, um Sitzungen zu starten. Dieser Benutzer kann als "Benutzer mit Verwaltungsaufgaben" mit Sicherungs- und Zurückschreibungsberechtigung für die definierten Knoten arbeiten.

Vorgehensweise

Führen Sie auf dem Server die folgenden Schritte aus, um die Clienteignerberechtigung zu erhalten:

1. Definieren Sie den Benutzer mit Verwaltungsaufgaben:

   ```
   REGister Admin Administratorname Kennwort
   ```

   Dabei gilt Folgendes:
   - *Administratorname* ist der Name des Benutzers mit Verwaltungsaufgaben.
   - *Kennwort* ist das Administratorkennwort.
2. Definieren Sie die Berechtigungsstufe. Benutzer mit System- oder Maßnahmenberechtigung verfügen auch über Clienteignerberechtigung.

   ```
   Grant Authority Administratorname Klassen Berechtigung node
   ```

   Dabei gilt Folgendes:
   - *Administratorname* ist der Benutzer mit Verwaltungsaufgaben.
   - *Klassen* ist der Knoten.
   - *Berechtigung* hat eine der folgenden Berechtigungsstufen:
     - `owner`: vollständige Sicherungs- und Zurückschreibungsberechtigung für den Knoten
     - `node`: einzelner Knoten
     - `domain`: Gruppe von Knoten
3. Definieren Sie den Zugriff auf einen einzelnen Knoten.

   ```
   Register Node Knotenname Kennwort
   userid=Benutzer-ID
   ```

   Dabei gilt Folgendes:
   - *Knotenname* ist der Clientbenutzerknoten
   - *Kennwort* ist das Kennwort für den Clientbenutzerknoten
   - *Benutzer-ID* ist der Name des Benutzers mit Verwaltungsaufgaben

Ergebnisse

Wenn die Anwendung den Benutzer mit Verwaltungsaufgaben verwendet, wird die Funktion dsmInitEx mit den Parametern userName und userNamePswd aufgerufen.

```
dsmInitEx
                    clientNodeName = NULL
                    clientOwnerName = NULL
      clientPassword = NULL
```

```
userName = 'Name des Benutzers mit Verwaltungsaufgaben'
userNamePswd = 'Kennwort des Benutzers mit Verwaltungsaufgaben'
```

Sie können Option passwordaccess auf generate oder prompt setzen. Mit jedem der Parameter wird über den Wert userNamePswd die Sitzung gestartet. Wenn die Sitzung gestartet wird, kann ein Sicherungs- oder Zurückschreibungsprozess für diesen Knoten ausgeführt werden.

Objektnamen und -IDs

Der IBM Spectrum Protect-Server ist ein Objektspeicherserver, dessen Funktion in erster Linie darin besteht, benannte Objekte effizient zu speichern und abzurufen. Die Objekt-ID ist für jedes Objekt eindeutig und bleibt dem Objekt während der gesamten Lebensdauer zugeordnet, *es sei denn*, das Objekt wird exportiert oder importiert.

Um diese Voraussetzung zu erfüllen, verfügt IBM Spectrum Protect über zwei Hauptspeicherbereiche, Datenbank und Datenspeicher.

- Die Datenbank enthält alle Metadaten wie den Namen und die Attribute, die den Objekten zugeordnet sind.
- Der Datenspeicher enthält die Objektdaten. Der Datenspeicher ist eigentlich eine Speicherhierarchie, die der Systemadministrator definiert. Daten werden abhängig von Kosten und Zugriffsanforderungen entweder effizient auf Onlinedatenträgern oder auf Offlinedatenträgern gespeichert und verwaltet.

Jedem Objekt, das auf dem Server gespeichert ist, ist ein Name zugeordnet. Der Client steuert die folgenden Schlüsselkomponenten dieses Namens:

- Dateibereichsname
- Übergeordneter Name
- Untergeordneter Name
- Objekttyp

Beim Treffen von Entscheidungen in Bezug auf die Benennung von Objekten für eine Anwendung muss unter Umständen ein externer Name für die vollständigen Objektnamen beim Endbenutzer verwendet werden. Der Endbenutzer muss unter Umständen das Objekt in einer Ein- oder Ausschlussanweisung angeben, wenn die Anwendung ausgeführt wird. Die genaue Syntax des Objektnamens in diesen Anweisungen ist plattformabhängig. Unter dem Betriebssystem Windows wird der Laufwerkbuchstabe, der dem Dateibereich zugeordnet ist und nicht der Dateibereichsname selbst in der Ein- oder Ausschlussanweisung verwendet.

Der Wert für die Objekt-ID, der beim Erstellen des Objekts zugeordnet wurde, ist möglichweise nicht derselbe wie bei der Ausführung eines Zurückschreibungsprozesses. Anwendungen sollten den Objektnamen speichern und dann abfragen, um die aktuelle Objekt-ID abzurufen, bevor eine Zurückschreibung ausgeführt wird.

- Dateibereichsname
  Der Dateibereichsname ist eine der wichtigsten Speicherkomponenten. Dabei kann es sich um den Namen eines Dateisystems, eines Plattenlaufwerks oder eines anderen übergeordneten Qualifikationsmerkmals handeln, mit dem zusammengehörige Daten gruppiert werden.
- Übergeordnete und untergeordnete Namen
  Zwei weitere Komponenten des Objektnamens sind das Qualifikationsmerkmal für den übergeordneten Namen und das Qualifikationsmerkmal für den untergeordneten Namen. Das Qualifikationsmerkmal für den übergeordneten Namen ist der Verzeichnispfad, in den das Objekt gehört; das Qualifikationsmerkmal für den untergeordneten Namen ist der eigentliche Name des Objekts in diesem Verzeichnispfad.
- Objekttyp
  Der Objekttyp identifiziert das Objekt entweder als eine Datei oder als ein Verzeichnis. Eine Datei ist ein Objekt, das sowohl Attribute als auch Binärdaten enthält; ein Verzeichnis ist ein Objekt, das nur Attribute enthält.

Dateibereichsname

Der Dateibereichsname ist eine der wichtigsten Speicherkomponenten. Dabei kann es sich um den Namen eines Dateisystems, eines Plattenlaufwerks oder eines anderen übergeordneten Qualifikationsmerkmals handeln, mit dem zusammengehörige Daten gruppiert werden.

IBM Spectrum Protect identifiziert mithilfe des Dateibereichs das Dateisystem oder das Plattenlaufwerk, auf dem sich die Daten befinden. So ist es möglich, Aktionen für alle Entitäten in einem Dateibereich auszuführen, z. B. Abfragen aller Objekte in einem bestimmten Dateibereich. Da der Dateibereich eine derart wichtige Komponente der Namenskonvention von IBM Spectrum Protect ist, verwenden Sie spezielle Aufrufe zum Registrieren, Aktualisieren, Abfragen und Löschen von Dateibereichen.

Der Server verfügt auch über Verwaltungsbefehle, um die Dateibereiche in jedem Knoten in IBM Spectrum Protect-Speicher abzufragen und, falls erforderlich, zu löschen. Allen Daten, die vom Anwendungsclient gespeichert werden, muss ein Dateibereichsname zugeordnet sein. Wählen Sie den Namen mit Bedacht, um ähnliche Daten im System zu gruppieren.

Um mögliche Kollisionen zu verhindern, dürfen die Dateibereichsnamen, die ein Anwendungsclient auswählt, nicht mit den Namen übereinstimmen, die ein Client für Sichern/Archivieren verwenden würde. Der Anwendungsclient muss seine Dateibereichsnamen publizieren, damit Endbenutzer die Objekte für Einschluss-/Ausschlussanweisungen, falls erforderlich, identifizieren können.

Anmerkung: Auf Windows-Plattformen ist einem Dateibereich ein Laufwerkbuchstabe zugeordnet. Wenn Sie einen Dateibereich registrieren oder aktualisieren, müssen Sie den Laufwerkbuchstaben angeben. Da die Einschluss-/Ausschlussliste auf den Laufwerkbuchstaben Bezug nimmt,

müssen Sie jeden Laufwerkbuchstaben mit seinem zugehörigen Dateibereich protokollieren. In dem Musterprogramm dapismp ist der Laufwerkbuchstabe standardmäßig auf "G" gesetzt.

Weitere Informationen zu den Musterprogrammen finden Sie in API-Musteranwendung erstellen und ausführen.

Übergeordnete und untergeordnete Namen

Zwei weitere Komponenten des Objektnamens sind das Qualifikationsmerkmal für den übergeordneten Namen und das Qualifikationsmerkmal für den untergeordneten Namen. Das Qualifikationsmerkmal für den übergeordneten Namen ist der Verzeichnispfad, in den das Objekt gehört; das Qualifikationsmerkmal für den untergeordneten Namen ist der eigentliche Name des Objekts in diesem Verzeichnispfad.

Wenn der Dateibereichsname, der übergeordnete Name und der untergeordnete Name verknüpft werden, müssen sie einen syntaktisch korrekten Namen auf dem Betriebssystem bilden, auf dem der Client ausgeführt wird. Es ist nicht erforderlich, dass der Name als ein Objekt auf dem System vorhanden ist oder den tatsächlichen Daten im lokalen Dateisystem ähnelt. Der Name muss jedoch den Standardbenennungsregeln entsprechen, damit er von den Aufrufen **dsmBindMC** korrekt verarbeitet werden kann. Überlegungen zur Benennung in Bezug auf die Maßnahmenverwaltung finden Sie in Erläuterungen zu Sicherungs- und Archivierungsobjekten.

Objekttyp

Der Objekttyp identifiziert das Objekt entweder als eine Datei oder als ein Verzeichnis. Eine Datei ist ein Objekt, das sowohl Attribute als auch Binärdaten enthält; ein Verzeichnis ist ein Objekt, das nur Attribute enthält.

Tabelle 1 zeigt den Anwendungsclient-Code für Objektnamen nach Plattform.

Tabelle 1. Beispiele für Anwendungsobjektnamen nach Plattform

Plattform	**Client-Code für Objektname**
UNIX oder Linux	/myfs/highlev/lowlev
Windows	"myvol\\highlev\\lowlev" Anmerkung: Auf einer Windows-Plattform wird ein doppelter umgekehrter Schrägstrich in einen einfachen umgekehrten Schrägstrich umgesetzt, da ein umgekehrter Schrägstrich das Escapezeichen ist. Auf der UNIX- oder Linux-Plattform beginnen Dateibereichsnamen mit einem Schrägstrich, während sie auf der Windows-Plattform nicht mit einem Schrägstrich beginnen dürfen.

Zugriff auf Objekte als Sitzungseigner

Jedem Objekt ist ein Eignername zugeordnet. Die Regeln, die festlegen, auf welche Objekte zugegriffen wird, sind von dem Eignernamen abhängig, der beim Starten einer Sitzung verwendet wird. Steuern Sie mithilfe dieses Werts für den Sitzungseigner den Zugriff auf das Objekt.

Der Sitzungseigner wird während des Aufrufs **dsmInitEx** im Parameter *clientOwnerNameP* festgelegt. Wenn Sie eine Sitzung mit **dsmInitEx** unter Angabe des Eignernamens *NULL* starten und *passwordaccess=prompt* verwenden, wird diesem Sitzungseigner Sitzungsberechtigung (Root- oder berechtigter Benutzer) zugeordnet. Dies trifft auch zu, wenn Sie sich mit einer Rootbenutzer-ID oder einer ID des berechtigten Benutzers anmelden und *passwordaccess=generate* verwenden. Während einer auf diese Weise gestarteten Sitzung können Sie jede Aktion für jedes Objekt ausführen, dessen Eigner dieser Knoten ist; dies ist unabhängig vom tatsächlichen Eigner dieses Objekts.

Wenn eine Sitzung mit einem bestimmten Eignernamen gestartet wird, kann die Sitzung nur Aktionen für Objekte ausführen, denen dieser Objekteignername zugeordnet ist. Allen Sicherungen oder Archivierungen in dem System muss dieser Eignername zugeordnet sein. Alle Abfragen, die ausgeführt werden, geben nur die Werte zurück, denen dieser Eignername zugeordnet ist. Der Wert für den Objekteigner wird während des Aufrufs **dsmSendObj** im Feld **owner** der Struktur **ObjAttr** festgelegt. Bei einem Eignernamen muss die Groß-/Kleinschreibung beachtet werden. In Tabelle 1 sind die Bedingungen zusammengefasst, unter denen ein Benutzer Zugriff auf ein Objekt hat.

Tabelle 1. Zusammenfassung des Benutzerzugriffs auf Objekte

Sitzungseigner	**Objekteigner**	**Benutzerzugriff**
NULL (Root, Systemeigner)	" " (leere Zeichenfolge)	Ja
NULL	Bestimmter Name	Ja
Bestimmter Name	" " (leere Zeichenfolge)	Nein
Bestimmter Name	Derselbe Name	Ja
Bestimmter Name	Anderer Name	Nein

Knoten- und eignerübergreifender Zugriff auf Objekte

Drei Funktionsaufrufe unterstützen knoten- und eignerübergreifenden Zugriff auf derselben Plattform: **dsmSetAccess**, **dsmDeleteAccess** und **dsmQueryAccess**. Diese Funktionen in Verbindung mit den Zeichenfolgeoptionen *-fromnode* und *-fromowner*, die in **dsmInitEx** übergeben

werden, gestatten einen vollständigen knotenübergreifenden Abfrage-, Zurückschreibungs- und Abrufprozess über die API.

Benutzer A auf Knoten A verwendet beispielsweise den Funktionsaufruf **dsmSetAccess**, um Benutzer B auf Knoten B Zugriff auf seine Sicherungen unter dem Dateibereich /db zu geben. Die Zugriffsregel wird wie folgt angezeigt:

ID	Typ	Knoten	Benutzer	Pfad
1	Sicherung	Knoten B	Benutzer B	/db/*/*

Wenn sich Benutzer B bei Knoten B anmeldet, lautet die Optionszeichenfolge für **dsmInitEx**:

```
-fromnode=nodeA -fromowner=userA
```

Diese Optionen werden für diese Sitzung definiert. Alle Abfragen greifen auf die Dateibereiche und Dateien des Knotens A zu. Sicherungen und Archivierungen sind nicht zulässig. Aus den Dateibereichen, auf die Benutzer B Zugriff hat, sind nur Abfrage-, Zurückschreibungs- und Abrufprozesse zulässig. Wenn die Anwendung versucht, bei einer Anmeldung mit einer definierten Option *-fromnode* oder *-fromowner* eine Operation mit **dsmBeginTxn** auszuführen (z. B. Sicherung oder Aktualisierung), schlägt dsmBeginTxn mit dem Rückkehrcode DSM_RC_ABORT_NODE_NOT_AUTHORIZED fehl. Weitere Informationen finden Sie bei den einzelnen Funktionsaufrufen und in dsmInitEx.
Tipp: Unter UNIX und Linux können Sie *–fromowner=root* in der Optionszeichenfolge angeben, die im Funktionsaufruf **dsmInitEx** übergeben wird. Dadurch erhalten Benutzer ohne Rootberechtigung Zugriff auf Dateien des Root, wenn ein set access ausgeführt wurde.

Verwenden Sie die Option *asnodename* in der Optionszeichenfolge **dsmInitEx** mit der entsprechenden Funktion, um Daten unter dem Zielknotennamen auf dem IBM Spectrum Protect-Server zu sichern, zu archivieren, zurückzuschreiben, abzurufen, abzufragen oder zu löschen. Informationen zur Aktivierung dieser Option finden Sie in Mehrere Knoten mit Clientknoten-Proxy-Unterstützung sichern.

Dateibereiche verwalten

Da Dateibereiche für den Betrieb des Systems wichtig sind, wird eine separate Gruppe von Aufrufen zum Registrieren, Aktualisieren und Löschen von Dateibereichs-IDs verwendet. Bevor Sie Objekte, die einem Dateibereich auf dem System zugeordnet sind, speichern können, müssen Sie den Dateibereich zunächst bei IBM Spectrum Protect registrieren.

Führen Sie diese Task mithilfe des Aufrufs dsmRegisterFS aus. Weitere Informationen zu Objektnamen und -IDs finden Sie in Objektnamen und -IDs.

Die Dateibereichs-ID ist das Qualifikationsmerkmal der höchsten Ebene in einer dreiteiligen Namenshierarchie. Die Gruppierung zusammengehöriger Daten in einem Dateibereich erleichtert die Verwaltung dieser Daten erheblich. Beispielsweise kann entweder der Anwendungsclient oder der IBM Spectrum Protect-Serveradministrator einen Dateibereich und alle Objekte in diesem Dateibereich löschen.

Dateibereiche ermöglichen es dem Anwendungsclient außerdem, dem Server Informationen zu dem Dateibereich bereitzustellen, die der Administrator dann abfragen kann. Diese Informationen werden bei der Abfrage in der Struktur qryRespFSData zurückgegeben und umfassen die folgenden Dateisysteminformationen:

Typ	Definition
fstype	Der Dateibereichstyp. Dieses Feld ist eine Zeichenfolge, die vom Anwendungsclient definiert wird.
fsAttr[Plattform].fsInfo	Ein Feld für Clientinformationen, das für clientspezifische Daten verwendet wird.
capacity	Der gesamte Speicherbereich in dem Dateibereich.
occupancy	Die Größe des Speicherbereichs, der momentan in dem Dateibereich belegt ist.
backStartDate	Die Zeitmarke, die angibt, wann die letzte Sicherung gestartet wurde (durch Senden eines Aufrufs dsmUpdateFS festgelegt).
backCompleteDate	Die Zeitmarke, die angibt, wann die letzte Sicherung beendet wurde (durch Senden eines Aufrufs dsmUpdateFS festgelegt).

Die Verwendung von 'capacity' und 'occupancy' ist vom Anwendungsclient abhängig. Einige Anwendungen benötigen möglicherweise keine Informationen zur Größe des Dateibereichs; in diesem Fall kann für diese Felder standardmäßig 0 angenommen werden. Weitere Informationen zum Abfragen von Dateibereichen finden Sie in IBM Spectrum Protect-System abfragen.

Nachdem ein Dateibereich beim System registriert wurde, können Sie jederzeit Objekte sichern oder archivieren. Rufen Sie dsmUpdateFS auf, um die Felder 'occupancy' und 'capacity' des Dateibereichs nach einer Sicherungs- oder Archivierungsoperation zu aktualisieren. Dieser Aufruf stellt sicher, dass die Werte für Belegung (occupancy) und Kapazität (capacity) des Dateisystems aktuell sind. Sie können auch die Felder fsinfo, backupstart und backupcomplete aktualisieren.

Wenn Sie das Datum ihrer letzten Sicherungen überwachen möchten, geben Sie einen Aufruf dsmUpdateFS ein, bevor Sie die Sicherung starten. Setzen Sie die Aktualisierungsaktion auf DSM_FSUPD_BACKSTARTDATE. Dies zwingt den Server, das Feld backStartDate des Dateibereichs auf die aktuelle Uhrzeit zu setzen. Nachdem die Sicherung für diesen Dateibereich abgeschlossen ist, geben Sie einen Aufruf dsmUpdateFS mit der Angabe DSM_FSUPD_BACKCOMPLETEDATE für die Aktualisierungsaktion ein. Dieser Aufruf erstellt am Ende der Sicherung eine Zeitmarke.

Wenn ein Dateibereich nicht mehr benötigt wird, können Sie ihn mit dem Befehl dsmDeleteFS löschen. Auf einem UNIX- oder Linux-Betriebssystem können nur Rootbenutzer oder berechtigte Benutzer Dateibereiche löschen.

Die Beispiele in Abbildung 1 veranschaulichen die Verwendung der drei Dateibereichsaufrufe für UNIX oder Linux. Ein Beispiel für die Verwendung der drei Dateibereichsaufrufe für Windows enthält der Code des auf Ihrem System installierten Beispielprogramms.
Abbildung 1. Beispiel für die Verwendung von drei Dateibereichen, Teil 1

```
/* Den Dateibereich registrieren, sofern dies noch nicht erfolgt ist. */

dsInt16        rc;
regFSData    fsData;
char         fsName[DSM_MAX_FSNAME_LENGTH];
char         smpAPI[] = "Muster-API";

strcpy(fsName,"/home/tallan/text");
memset(&fsData,0x00,sizeof(fsData));
fsData.stVersion = regFSDataVersion;
fsData.fsName = fsName;
fsData.fsType = smpAPI;
strcpy(fsData.fsAttr.unixFSAttr.fsInfo,"FsInfo für Muster-API");
fsData.fsAttr.unixFSAttr.fsInfoLength =
       strlen(fsData.fsAttr.unixFSAttr.fsInfo) + 1;
fsData.occupancy.hi=0;
fsData.occupancy.lo=100;
fsData.capacity.hi=0;
fsData.capacity.lo=300;

rc = dsmRegisterFS(dsmHandle,fsData);
if (rc == DSM_RC_FS_ALREADY_REGED) rc = DSM_RC_OK;  /* bereits ausgeführt */
if (rc)
{
   printf("Dateibereichsregistrierung fehlgeschlagen: ");
   rcApiOut(dsmHandle, rc);
   free(bkup_buff);
   return (RC_SESSION_FAILED);
}
```

Abbildung 2. Beispiel für die Verwendung von drei Dateibereichen, Teil 2

```
/* Dateibereich aktualisieren. */

dsmFSUpd     updFilespace;         /* Aktual. des Dateibereichs */

updFilespace.stVersion = dsmFSUpdVersion;
updFilespace.fsType = 0;             /* keine Änderung */
updFilespace.occupancy.hi = 0;
updFilespace.occupancy.lo = 50;
updFilespace.capacity.hi = 0;
updFilespace.capacity.lo = 200;
strcpy(updFilespace.fsAttr.unixFSAttr.fsInfo,
       "Aktualisierung für Dateibereich") ;
updFilespace.fsAttr.unixFSAttr.fsInfoLength =
       strlen(updFilespace.fsAttr.unixFSAttr.fsInfo);

updAction = DSM_FSUPD_FSINFO |
            DSM_FSUPD_OCCUPANCY |
            DSM_FSUPD_CAPACITY;

rc = dsmUpdateFS (handle,fsName,&updFilespace,updAction);
printf("dsmUpdateFS rc=%d\n", rc);
```

Abbildung 3. Beispiel für die Verwendung von drei Dateibereichen, Teil 3

```
/* Dateibereich löschen. */

printf("\nDateibereich wird gelöscht
rc = dsmDeleteFS (dsmHandle,fsName,DSM_REPOS_ALL);
if (rc)
{
   printf(" FEHLGESCHLAGEN!!! ");
   rcApiOut(dsmHandle, rc);
}
else printf("  OK!\n");
```

Objekte Verwaltungsklassen zuordnen

Ein wichtiges Merkmal von IBM Spectrum Protect ist die Verwendung von Maßnahmen (Verwaltungsklassen), die definieren, wie Objekte im IBM Spectrum Protect-Speicher gespeichert und verwaltet werden. Ein Objekt wird bei seiner Sicherung oder Archivierung einer Verwaltungsklasse zugeordnet.

Diese Verwaltungsklasse legt Folgendes fest:

- Wie viele Versionen des Objekts aufbewahrt werden, wenn es gesichert wird
- Wie lange Archivierungskopien aufbewahrt werden
- An welcher Position das Objekt in der Speicherhierarchie auf dem Server eingefügt werden soll

Verwaltungsklassen bestehen sowohl aus Sicherungskopiengruppen als auch aus Archivierungskopiengruppen. Eine Kopiengruppe besteht aus einer Reihe von Attributen, die die Verwaltungsmaßnahmen für ein Objekt definieren, das gesichert oder archiviert wird. Wenn eine Sicherungsoperation ausgeführt wird, werden die Attribute in der Sicherungskopiengruppe angewendet. Wenn eine Archivierungsoperation ausgeführt wird, werden die Attribute in der Archivierungskopiengruppe angewendet.

Die Sicherungs- oder Archivierungskopiengruppe in einer bestimmten Verwaltungsklasse kann leer oder NULL sein. Wird ein Objekt an die NULL-Sicherungskopiengruppe gebunden, kann dieses Objekt nicht gesichert werden. Wird ein Objekt an die NULL-Archivierungskopiengruppe gebunden, kann dieses Objekt nicht archiviert werden.

Da die Verwendung einer Maßnahme ein sehr wichtiger Bestandteil von IBM Spectrum Protect ist, ist es für die API erforderlich, dass allen Objekten, die an den Server gesendet werden, zunächst mithilfe des Aufrufs **dsmBindMC** eine Verwaltungsklasse zugeordnet wird. Mit der IBM Spectrum Protect-Software können Sie eine Einschluss-/Ausschlussliste für die Verwaltungsklassenbindung verwenden. Der Aufruf **dsmBindMC** verwendet die aktuelle Einschluss-/Ausschlussliste, um die Verwaltungsklassenbindung durchzuführen.

Einschlussanweisungen (include) können eine bestimmte Verwaltungsklasse einem Sicherungs- oder Archivierungsobjekt zuordnen. Ausschlussanweisungen (exclude) können die Sicherung von Objekten, aber nicht die Archivierung von Objekten verhindern.

Für die API ist erforderlich, dass **dsmBindMC** vor der Sicherung oder Archivierung eines Objekts aufgerufen wird. Der Aufruf **dsmBindMC** gibt eine mcBindKey-Struktur zurück, die Informationen zu Verwaltungsklassen und Kopiengruppen enthält, die dem Objekt zugeordnet sind. Überprüfen Sie das Ziel für die Kopiengruppe, bevor eine Sendeoperation ausgeführt wird. Wenn Sie mehrere Objekte in einer einzigen Transaktion senden, müssen die Objekte dasselbe Ziel für Kopiengruppe haben. Der Funktionsaufruf **dsmBindMC** gibt folgende Informationen zurück:

Tabelle 1. Im Aufruf dsmBindMC zurückgegebene Informationen

Informationen	**Beschreibung**
Verwaltungsklasse	Der Name der Verwaltungsklasse, die dem Objekt zugeordnet wurde. Der Anwendungsclient kann den Aufruf **dsmBeginQuery** senden, um alle Attribute dieser Verwaltungsklasse zu bestimmen.
Sicherungskopiengruppe	Gibt Auskunft darüber, ob eine Sicherungskopiengruppe für diese Verwaltungsklasse vorhanden ist. Wenn eine Sicherungsoperation ausgeführt wird und keine Sicherungskopiengruppe vorhanden ist, kann dieses Objekt nicht an den Speicher gesendet werden. Sie empfangen einen Fehlercode, wenn Sie eine Sendeoperation mit dem Aufruf **dsmSendObj** auszuführen versucht haben.
Kopienzielort für Sicherungen	Dieses Feld gibt den Speicherpool an, an den die Daten gesendet werden. Wenn Sie eine Sicherungstransaktion mit mehreren Objekten ausführen, müssen alle Kopienzielorte innerhalb dieser Transaktion identisch sein. Wenn ein Objekt andere Kopienzielorte als vorherige Objekte in der Transaktion hat, beenden Sie die aktuelle Transaktion und beginnen Sie eine neue Transaktion, damit Sie das Objekt senden können. Sie empfangen einen Fehlercode, wenn Sie versuchen, Objekte innerhalb derselben Transaktion an verschiedene Kopienzielorte zu senden.
Archivierungskopiengruppe	Gibt Auskunft darüber, ob eine Archivierungskopiengruppe für diese Verwaltungsklasse vorhanden ist. Wenn eine Archivierungsoperation ausgeführt wird und keine Archivierungskopiengruppe vorhanden ist, kann dieses Objekt nicht an den Speicher gesendet werden. Sie empfangen einen Fehlercode, wenn Sie eine Sendeoperation mit dem Aufruf **dsmSendObj** auszuführen versucht haben.
Kopienzielort für Archivierungen	Dieses Feld gibt den Speicherpool an, an den die Daten gesendet werden. Wenn Sie eine Archivierungstransaktion mit mehreren Objekten ausführen, müssen alle Kopienzielorte innerhalb dieser Transaktion identisch sein. Wenn ein Objekt andere Kopienzielorte als vorherige Objekte in der Transaktion hat, beenden Sie die aktuelle Transaktion und beginnen Sie eine neue Transaktion, bevor Sie das Objekt senden. Sie empfangen einen Fehlercode, wenn Sie versuchen, Objekte innerhalb derselben Transaktion an verschiedene Kopienzielorte zu senden.

Sicherungskopien eines Objekts können an eine andere Verwaltungsklasse erneut gebunden werden, wenn eine nachfolgende Sicherung mit demselben Objektnamen ausgeführt wird, in der eine andere als die ursprüngliche Verwaltungsklasse verwendet wird. Wenn Sie beispielsweise ObjektA sichern und an Verwaltungsklasse1 binden und später ObjektA sichern und an Verwaltungsklasse2 binden, werden bei der aktuellsten Sicherung alle inaktiven Kopien an Verwaltungsklasse2 erneut gebunden. Die in Verwaltungsklasse2 definierten Parameter steuern dann alle Kopien. Wenn sich der Zielort ändert, werden die Daten jedoch nicht versetzt.

Sie können Sicherungskopien auch mit dem Aufruf **dsmUpdateObj** oder **dsmUpdateObjEx** mit der Aktion DSM_BACKUPD_MC an eine andere Verwaltungsklasse erneut binden.

- Verwaltungsklassen abfragen
  Anwendungen können Verwaltungsklassen abfragen, um zu bestimmen, welche Verwaltungsklasse für einen bestimmten Knoten gültig sind, und um zu bestimmen, welche Attribute sich in der Verwaltungsklasse befinden.

Zugehörige Verweise:
Option Deduplication

Verfall/Löschen anhalten und freigeben

Sie können das Löschen und den Verfall bestimmter Archivierungsobjekte als Reaktion auf eine anstehende oder laufende Aktion, die das Anhalten bestimmter Daten erfordert, anhalten. Falls eine Aktion eingeleitet wird, die möglicherweise Zugriff auf Daten erfordert, müssen diese Daten verfügbar sein, bis die Aktion abgeschlossen ist und der Zugriff auf die Daten im Rahmen dieses Prozesses nicht mehr erforderlich ist. Nachdem festgestellt wurde, dass die Aussetzung nicht mehr erforderlich ist (Freigabe), wird die normale Zeitplanung für Löschen und Verfall über den ursprünglichen Aufbewahrungszeitraum wieder aufgenommen.

Vorbereitende Schritte

Überprüfen Sie, ob der Server lizenziert ist, indem Sie einen Testaufruf dsmRetentionEvent ausgeben:

1. Führen Sie eine Abfrage nach einem einzelnen Objekt aus, das angehalten werden soll, und rufen Sie die ID ab.
2. Setzen Sie den Aufruf dsmBeginTxn, den Aufruf dsmRetentionEvent mit der Angabe Hold und den Aufruf dsmEndTxn ab.
3. Ist der Server nicht lizenziert, empfangen Sie ein Votum 'abort' (Abbrechen) mit dem Ursachencode `DSM_RC_ABORT_LICENSE_VIOLATION`.

Einschränkungen:

1. Sie können in einer einzigen Transaktion nicht mehrere Aufrufe dsmRetentionEvent absetzen.
2. Es ist nicht möglich, das Anhalten eines Objekts anzufordern, das bereits angehalten ist.

Vorgehensweise

1. Führen Sie die folgenden Schritte aus, um Objekte anzuhalten:
   a. Fragen Sie den Server nach allen Objekten ab, die angehalten werden sollen. Rufen Sie die Objekt-ID für jedes Objekt ab.
   b. Setzen Sie zunächst einen Aufruf dsmBeginTxn und dann einen Aufruf dsmRetentionEvent mit der Liste der Objekte ab, gefolgt von einem Aufruf dsmEventType: eventHoldObj. Überschreitet die Anzahl Objekte den Wert von maxObjPerTxn, müssen Sie mehrere Transaktionen verwenden.
   c. Verwenden Sie die Antwort `qryRespArchiveData` im Funktionsaufruf dsmGetNextQObj, um zu bestätigen, dass die Objekte angehalten wurden. Überprüfen Sie den Wert von `objHeld` in `qryRespArchiveData`.
2. Führen Sie die folgenden Schritte aus, um Objekte freizugeben:
   a. Fragen Sie den Server nach allen angehaltenen Objekten ab, die freigegeben werden sollen. Rufen Sie die Objekt-ID für jedes Objekt ab.
   b. Setzen Sie zunächst einen Aufruf dsmBeginTxn und dann einen Aufruf dsmRetentionEvent mit der Liste der Objekte ab, gefolgt von einem Aufruf dsmEventType: eventReleaseObj. Überschreitet die Anzahl Objekte den Wert von `maxObjPerTxn`, müssen Sie mehrere Transaktionen verwenden.
   c. Verwenden Sie die Antwort qryRespArchiveData im Funktionsaufruf dsmGetNextQObj, um zu überprüfen, ob die angehaltenen Objekte freigegeben wurden. Überprüfen Sie den Wert von objHeld in qryRespArchiveData.

- Aufbewahrungsschutz für Archivierungsdaten
  Von IBM Spectrum Protect gesteuerte Daten können nicht durch Agenten ohne entsprechende Berechtigung, wie beispielsweise eine Person oder ein Programm, geändert werden. Dieser Schutz erstreckt sich auf das Löschen von Daten (z. B. Archivierungsobjekte) durch einen Agenten vor Ablauf des Aufbewahrungszeitraums.

IBM Spectrum Protect-System abfragen

Die API enthält mehrere Abfragen, beispielsweise eine Verwaltungsklassenabfrage, die von Anwendungen verwendet werden können.

Vorgehensweise

Alle Abfragen, die den Aufruf dsmBeginQuery verwenden, beinhalten die folgenden Schritte:

1. Aufruf dsmBeginQuery mit dem geeigneten Abfragetyp senden:
   - Sicherung
   - Archivierung
   - Aktive gesicherte Objekte
   - Dateibereich
   - Verwaltungsklasse

   Der Aufruf dsmBeginQuery informiert die API über das Datenformat, das vom Server zurückgegeben wird. Die entsprechenden Felder können in die Datenstrukturen eingefügt werden, die über die dsmGetNextQObj-Aufrufe übergeben werden. Der Aufruf zum Beginnen der Abfrage (begin query) ermöglicht dem Anwendungsclient außerdem, den Geltungsbereich der Abfrage festzulegen, indem die Parameter ordnungsgemäß im Aufruf 'begin query' angegeben werden.
   Einschränkung: Auf UNIX- und Linux-Systemen kann nur der Rootbenutzer aktive gesicherte Objekte abfragen. Dieser Abfragetyp wird als "Direktaufruf" bezeichnet.
2. Geben Sie den Aufruf dsmGetNextQObj ein, um jeden Datensatz aus der Abfrage abzurufen. Dieser Aufruf übergibt einen Puffer, der groß genug ist, um die aus der Abfrage zurückgegebenen Daten aufzunehmen. Jeder Abfragetyp hat eine entsprechende Datenstruktur für die

zurückgegebenen Daten. Dem Abfragetyp 'Sicherung' beispielsweise ist die Struktur qryRespBackupData zugeordnet, die gefüllt wird, wenn der Aufruf dsmGetNextQObj gesendet wird.

3. Der Aufruf dsmGetNextQObj gibt in der Regel einen der folgenden Codes zurück:
   - `DSM_RC_MORE_DATA`: Senden Sie den Aufruf dsmGetNextQObj erneut.
   - `DSM_RC_FINISHED`: Es sind keine weitere Daten vorhanden. Senden Sie den Aufruf dsmEndQuery.
4. Senden Sie den Aufruf dsmEndQuery. Wenn alle Abfragedaten abgerufen wurden bzw. keine weiteren Abfragedaten benötigt werden, geben Sie den Aufruf dsmEndQuery ein, um den Abfrageprozess zu beenden. Die API löscht alle verbleibenden Daten aus dem Abfragedatenstrom und gibt alle für die Abfrage genutzten Ressourcen frei.

Ergebnisse

Abbildung 1 zeigt das Zustandsdiagramm für Abfrageoperationen.
Abbildung 1. Zustandsdiagramm für allgemeine Abfragen

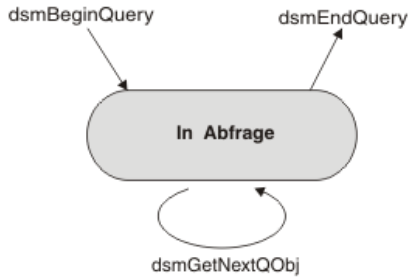
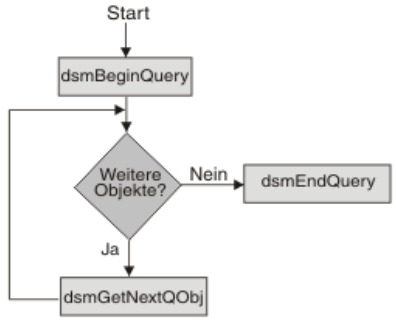


Abbildung 2 zeigt das Ablaufdiagramm für Abfrageoperationen.
Abbildung 2. Ablaufdiagramm für allgemeine Abfragen



- Beispiel für das Abfragen des Systems
  In diesem Beispiel für eine Verwaltungsklassenabfrage werden die Werte aller Felder in den Sicherungs- und Archivierungskopiengruppe für eine bestimmte Verwaltungsklasse gedruckt.

Servereffizienz

Beachten Sie diese Richtlinien beim Abrufen von Objekten vom IBM Spectrum Protect-Server oder beim Senden von Objekten an den Server.

- Wenn Sie Objekte vom IBM Spectrum Protect-Server abrufen, beachten Sie folgende Richtlinien:
  - Rufen Sie Daten in der Zurückschreibungsreihenfolge ab, die vom IBM Spectrum Protect-Server bereitgestellt wird. Die Zurückschreibungsreihenfolge ist insbesondere bei Bandeinheiten wichtig, da das Abrufen von Daten, die sich nicht in der korrekten Reihenfolge befinden, das Zurückspulen und Laden von Bändern zur Folge haben kann.
  - Selbst wenn die Daten auf einer Platteneinheit gespeichert sind, können Sie Zeit sparen, wenn beim Abrufen die Reihenfolge eingehalten wird.
  - Führen Sie so viel Arbeit wie möglich in einer einzigen IBM Spectrum Protect-Serversitzung aus.
  - Starten und stoppen Sie keine Mehrfachsitzungen.
- Wenn Sie Objekte an den IBM Spectrum Protect-Server senden, beachten Sie folgende Richtlinien:
  - Senden Sie mehrere Objekte in einer einzigen Transaktion.
  - Vermeiden Sie es, ein einziges Objekt pro Transaktion zu senden; dies gilt insbesondere dann, wenn die Daten direkt an eine Bandeinheit gesendet werden. Im Rahmen der Bandeinheitentransaktion wird sichergestellt, dass die Daten in den Arbeitsspeicherpuffern des Bands auf Datenträger geschrieben werden.

Zugehörige Konzepte:
Objekte nach Zurückschreibungsreihenfolge auswählen und sortieren
Zugehörige Informationen:
Sitzung starten oder beenden

Daten an einen Server senden

Die API ermöglicht Anwendungsclients das Senden von Daten oder benannten Objekten und ihrer zugehörigen Daten in IBM Spectrum Protect-Serverspeicher.

Tipp: Sie können Daten entweder sichern oder archivieren. Führen Sie alle Sendeoperationen innerhalb einer Transaktion aus.

- Das Transaktionsmodell
  Die während einer Sicherungs- oder Archivierungsoperation an den IBM Spectrum Protect-Speicher gesendeten Daten werden innerhalb einer Transaktion gesendet. Ein Transaktionsmodell stellt ein hohes Maß an Datenintegrität bereit, bedingt jedoch einige Einschränkungen, die ein Anwendungsclient berücksichtigen muss.
- Dateizusammenfassung
  IBM Spectrum Protect-Server verwenden eine Funktion, die als Dateizusammenfassung bezeichnet wird. Bei der Dateizusammenfassung werden alle Objekte, die in einer einzigen Transaktion gesendet werden, zusammen gespeichert; dadurch wird Speicherbereich eingespart und die Leistung verbessert. Sie können die Objekte weiterhin einzeln abfragen und zurückschreiben.
- LAN-unabhängige Datenübertragung
  Die API kann die Vorteile der LAN-unabhängigen Datenübertragung nutzen, wenn die Option **dsmSetUp** für Multithreading auf ON gesetzt ist. Die API gibt das Vorhandensein eines LAN-unabhängigen Ziels in der **Query Mgmt Class**-Antwortstruktur **archDetailCG** oder **backupDetailCG** im Feld **bLanFreeDest** zurück.
- Gleichzeitiges Schreiben
  IBM Spectrum Protect-Serverspeicherpools können so konfiguriert werden, dass sie während einer Sicherung oder Archivierung gleichzeitig in einen primären Speicherpool und in einen oder mehrere Kopienspeicherpools schreiben. Verwenden Sie diese Konfiguration zum Erstellen mehrerer Kopien des Objekts.
- API-Leistung verbessern
  Sie können die Leistung der API mithilfe der Clientoptionen tcpbuffsize und tcpnodelay sowie dem API-Parameter DataBlk verbessern.

Das Transaktionsmodell

Die während einer Sicherungs- oder Archivierungsoperation an den IBM Spectrum Protect-Speicher gesendeten Daten werden innerhalb einer Transaktion gesendet. Ein Transaktionsmodell stellt ein hohes Maß an Datenintegrität bereit, bedingt jedoch einige Einschränkungen, die ein Anwendungsclient berücksichtigen muss.

Starten Sie eine Transaktion durch einen Aufruf von **dsmBeginTxn** und beenden Sie eine Transaktion durch einen Aufruf von **dsmEndTxn**. Eine einzelne Transaktion ist eine atomare Aktion. Die innerhalb der Grenzen einer Transaktion gesendeten Daten werden entweder am Ende der Transaktion auf dem System festgeschrieben oder rückgängig gemacht, wenn die Transaktion vorzeitig endet.

Transaktionen können aus Sendeoperationen für Einzelobjekte oder aus Sendeoperationen für mehrere Objekte bestehen. Um die Systemleistung durch Verringerung des Systemaufwands zu verbessern, sollten Sie kleinere Objekte in einer Transaktion mit mehreren Objekten senden. Der Anwendungsclient bestimmt, ob einzelne oder mehrere Transaktionen angemessen sind.

Senden Sie alle Objekte in einer Transaktion mit mehreren Objekten an dasselbe Kopienziel. Wenn Sie ein Objekt an ein anderes Ziel als das vorherige Objekt senden müssen, beenden Sie die aktuelle Transaktion und starten Sie eine neue. Innerhalb der neuen Transaktion können Sie das Objekt an das neue Kopienziel senden.
Anmerkung: Objekte, die keine Bitdaten enthalten (*sizeEstimate=0*), werden nicht auf Kopienzielkonsistenz überprüft.

IBM Spectrum Protect begrenzt die Anzahl Objekte, die in einer Transaktion mit mehreren Objekten gesendet werden können. Diesen Grenzwert finden Sie, wenn Sie **dsmQuerySessInfo** aufrufen und das Feld **maxObjPerTxn** überprüfen. Dieses Feld enthält den Wert der auf Ihrem Server definierten Option *TXNGroupmax*.

Der Anwendungsclient muss die innerhalb einer Transaktion gesendeten Objekte überwachen, um im Fall einer vorzeitigen Beendigung der Transaktion eine Wiederholung oder Fehlerbehandlung ausführen zu können. Der Server oder der Client kann eine Transaktion jederzeit stoppen. Der Anwendungsclient muss darauf vorbereitet sein, nicht selbst gestartete plötzliche Transaktionsbeendigungen zu bearbeiten.

Dateizusammenfassung

IBM Spectrum Protect-Server verwenden eine Funktion, die als Dateizusammenfassung bezeichnet wird. Bei der Dateizusammenfassung werden alle Objekte, die in einer einzigen Transaktion gesendet werden, zusammen gespeichert; dadurch wird Speicherbereich eingespart und die Leistung verbessert. Sie können die Objekte weiterhin einzeln abfragen und zurückschreiben.

Um diese Funktion verwenden zu können, müssen alle Objekte in einer Transaktion denselben Dateibereichsnamen haben. Wenn sich der Dateibereichsname in einer Transaktion ändert, schließt der Server das vorhandene zusammengefasste Objekt und beginnt ein neues.

LAN-unabhängige Datenübertragung

Die API kann die Vorteile der LAN-unabhängigen Datenübertragung nutzen, wenn die Option **dsmSetUp** für Multithreading auf ON gesetzt ist. Die API gibt das Vorhandensein eines LAN-unabhängigen Ziels in der **Query Mgmt Class**-Antwortstruktur **archDetailCG** oder **backupDetailCG** im Feld **bLanFreeDest** zurück.

Sie können LAN-unabhängige Operationen auf Plattformen verwenden, die vom Speicheragenten unterstützt werden. Die Macintosh-Plattform ist ausgeschlossen.

LAN-unabhängige Informationen werden in den folgenden Ausgabestrukturen bereitgestellt. Die Ausgabestruktur (**dsmEndGetDataExOut_t**) für **dsmEndGetData** umfasst das Feld **totalLFBytesRecv**. Dies ist die Gesamtanzahl empfangener LAN-unabhängiger Byte. Die Ausgabestruktur (**dsmEndSendObjExOut_t**) für **dsmEndSendObjEx** umfasst das Feld **totalLFBytesSent**. Dies ist die Gesamtanzahl gesendeter LAN-unabhängiger Byte.

Zugehörige Informationen:
LAN-unabhängige Datenversetzung: Übersicht über den Speicheragenten

Gleichzeitiges Schreiben

IBM Spectrum Protect-Serverspeicherpools können so konfiguriert werden, dass sie während einer Sicherung oder Archivierung gleichzeitig in einen primären Speicherpool und in einen oder mehrere Kopienspeicherpools schreiben. Verwenden Sie diese Konfiguration zum Erstellen mehrerer Kopien des Objekts.

Wenn eine Operation für gleichzeitiges Schreiben fehlschlägt, kann der Rückkehrcode für die Funktion **dsmEndTxn** `DSM_RC_ABORT_STGPOOL_COPY_CONT_NO` lauten; dies gibt an, dass der Schreibvorgang in einen der Kopienspeicherpools fehlgeschlagen ist und die Option COPYCONTINUE für den IBM Spectrum Protect-Speicherpool auf NO gesetzt wurde. Die Anwendung wird beendet und der Fehler muss vom IBM Spectrum Protect-Serveradministrator behoben werden.

Weitere Informationen zum Konfigurieren von Operationen für gleichzeitiges Schreiben finden Sie in der Dokumentation für den IBM Spectrum Protect-Server.

API-Leistung verbessern

Sie können die Leistung der API mithilfe der Clientoptionen tcpbuffsize und tcpnodelay sowie dem API-Parameter DataBlk verbessern.

Tabelle 1 enthält eine Beschreibung der Aktionen, die Sie zum Verbessern der API-Leistung durchführen können.

Tabelle 1. Optionen zum Sichern/Archivieren und der API-Parameter zum Verbessern der Leistung

Optionen des Clients für Sichern/Archivieren	**Beschreibung**
tcpbuffsize	Gibt die Größe des TCP-Puffers an. Der Standardwert ist 31 KB. Setzen Sie zur Verbesserung der Leistung den Wert auf 32 KB.
tcpnodelay	Sie gibt an, ob kleine Puffer statt angehalten zu werden an den Server gesendet werden sollten. Setzen Sie diese Option für alle Plattformen auf *yes*. Diese Option ist nur für Windows und AIX gültig.
API-Parameter	**Beschreibung**
DataBlk	Dieser Parameter wird im Funktionsaufruf **dsmSendData** verwendet, um die Größe des Anwendungspuffers zu bestimmen. Die besten Ergebnisse können Sie erzielen, wenn Sie für den Parameter ein Vielfaches des Wertes von *tcpbuffsize* verwenden und dann den Wert von tcpbuffsize minus 4 Byte angeben. Geben Sie beispielsweise für diesen Parameter den Wert 28 an, wenn tcpbuffsize einen Wert von 32 KB hat.

Jeder Aufruf dsmSendData erfolgt synchron und kehrt erst zurück, nachdem für die in dataBlkPtr an die API übertragenen Daten eine Flushoperation in das Netz ausgeführt wurde. Die API fügt jedem Transaktionspuffer, der in das Netz gestellt wird, 4 Byte Systemaufwand hinzu.

Hat beispielsweise der Transaktionspuffer eine Größe von 32 KB und der DataBlk-Anwendungspuffer eine Größe von 31 KB, passt jeder DataBlk-Anwendungspuffer in einen Kommunikationspuffer und es kann sofort eine Flushoperation ausgeführt werden. Wenn der DataBlk-Anwendungspuffer jedoch exakt 32 KB hat, sind, da die API pro Transaktionspuffer 4 Byte hinzufügt, zwei Flushoperationen erforderlich: eine mit 32 KB und eine mit 4 Byte. Wird die Option tcpnodelay auf no gesetzt, kann die Flushoperation für die 4 Byte bis zu 200 Millisekunden dauern.

API für das Senden von Leistungsdaten an die Clientleistungsüberwachung konfigurieren

Die Clientleistungsüberwachung ist eine Komponente des Tivoli Storage Manager Administration Center, die zum Anzeigen von Leistungsdaten verwendet wird, die von der API erfasst wurden. Die Clientleistungsüberwachung zeichnet Leistungsdaten für Clientsicherungs-, -archivierungs- und -zurückschreibungsoperationen auf und zeigt diese Daten an.

Bei aktivierter Leistungsüberwachung können Sie Leistungsdaten anzeigen, die von der API unter Verwendung der Leistungsüberwachung erfasst werden. Die Leistungsüberwachung ist im Tivoli Storage Manager Administration Center verfügbar. Ab Version 7.1 ist die Komponente Administration Center nicht mehr in Tivoli Storage Manager oder in den IBM Spectrum Protect-Verteilungen enthalten. Wenn Sie ein Administration Center haben, das mit einem vorherigen Serverrelease installiert wurde, können Sie es weiterhin zum Anzeigen von Leistungsdaten verwenden. Wenn Sie über kein installiertes Administration Center verfügen, können Sie die zuvor freigegebene Version von ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/admincenter/v6r3/ herunterladen. Informationen zur Verwendung der Leistungsüberwachung finden Sie in der Dokumentation zu Tivoli Storage Manager Version 6.3.

- Optionen für die Clientleistungsüberwachung konfigurieren
  Sie aktivieren IBM Spectrum Protect-Clients für die Verwendung der Leistungsüberwachung, indem Sie Parameter in der Clientoptionsdatei angeben. Sie geben diese Optionen für jeden Client an, der überwacht werden soll.

Objekte an den Server senden

Anwendungsclients können Daten oder benannte Objekte und ihre zugehörigen Daten mithilfe der API-Sicherungs- und -Archivierungsfunktionen in IBM Spectrum Protect-Speicher senden. Die Sicherungs- und Archivierungskomponenten des Systems ermöglichen die Verwendung unterschiedlicher Verwaltungsprozeduren für Daten, die in den Speicher gesendet werden.

Das Attribut für die Größenschätzung ist eine Schätzung der Gesamtgröße des Datenobjekts, das an den Server gesendet werden soll. Wenn der Anwendung die exakte Objektgröße nicht bekannt ist, geben Sie für *sizeEstimate* einen höheren Schätzwert an. Wenn die Schätzung kleiner als die tatsächliche Größe ist, nutzt der IBM Spectrum Protect-Server zusätzliche Ressourcen für die Handhabung zusätzlicher Bereichszuordnungen.

Hinweise:

- Diese Größe sollte so genau wie möglich geschätzt werden. Der Server verwendet dieses Attribut für die effiziente Bereichszuordnung und Objektpositionierung in seinen Speicherressourcen.
- Wenn die Schätzung kleiner als die tatsächliche Größe ist, ordnet ein Server, der Caching verwendet, keinen zusätzlichen Speicherbereich zu und stoppt die Sendeoperation.

Möglicherweise treten Probleme auf, wenn der Wert für *sizeEstimate* viel zu groß ist. Unter Umständen ist auf dem Server nicht genügend Speicherbereich für die geschätzte Größe, aber für die tatsächliche Größe verfügbar. Es ist auch möglich, dass der Server langsamere Einheiten verwendet.

Sie können Objekte, deren Größe 2 Gigabyte überschreitet, sichern oder archivieren. Die Objekte können komprimiert oder unkomprimiert sein.

Um eine Sendeoperation zu starten, rufen Sie **dsmSendObj** auf. Sind mehr Daten verfügbar, als in einer einzigen Operation gesendet werden können, können Sie **dsmSendData** wiederholt aufrufen, um die verbleibenden Informationen zu übertragen. Rufen Sie **dsmEndSendObj** auf, um die Sendeoperation abzuschließen.

- Erläuterungen zu Sicherungs- und Archivierungsobjekten
  Die Sicherungskomponente des IBM Spectrum Protect-Systems unterstützt mehrere Versionen benannter Objekte, die auf dem Server gespeichert sind.
- Komprimierung
  Konfigurationsoptionen auf einem bestimmten Knoten legen in Verbindung mit der dsmSendObj-Option objCompressed fest, ob IBM Spectrum Protect das Objekt während eines Sendevorgangs komprimiert. Außerdem werden Objekte mit einer Größenschätzung (sizeEstimate), die DSM_MIN_COMPRESS_SIZE unterschreitet, nie komprimiert.
- Pufferkopieneliminierung
  Mit der Pufferkopieneliminierungsfunktion wird die Kopie von Datenpuffern zwischen einer Anwendung und dem IBM Spectrum Protect-Server entfernt, was eine bessere Prozessorauslastung zur Folge hat. Den größten Effekt hat dieses Konzept in einer LAN-unabhängigen Umgebung.
- API-Verschlüsselung
  Es stehen zwei Verfahren zum Verschlüsseln von Daten zur Verfügung: die anwendungsverwaltete Verschlüsselung und die IBM Spectrum Protect-Clientverschlüsselung.

Erläuterungen zu Sicherungs- und Archivierungsobjekten

Die Sicherungskomponente des IBM Spectrum Protect-Systems unterstützt mehrere Versionen benannter Objekte, die auf dem Server gespeichert sind.

Jedes Objekt, das auf dem Server gesichert wird und dessen Name mit dem Namen eines Objekts übereinstimmt, das bereits von diesem Client auf dem Server gespeichert ist, unterliegt der Versionssteuerung. Bei Objekten wird von einem aktiven oder inaktiven Status auf dem Server ausgegangen. Die neueste Kopie eines Objekts auf dem Server, die nicht inaktiviert wurde, ist im aktiven Status. Jedes andere Objekt mit demselben Namen wird als inaktiv betrachtet, unabhängig davon, ob es sich um eine ältere Version oder um eine inaktivierte Kopie handelt. Verwaltungsklassenkonstrukte definieren verschiedene Verwaltungskriterien. Sie werden aktiven und inaktiven Objekten auf dem Server zugeordnet.

Tabelle 1 enthält die für den aktiven und den inaktiven Status gültigen Kopiengruppenfelder.

Tabelle 1. Felder für Sicherungskopiengruppen

Feld	Beschreibung
VEREXISTS	Die Anzahl inaktiver Versionen, wenn aktive Versionen vorhanden sind.
VERDELETED	Die Anzahl inaktiver Versionen, wenn keine aktiven Versionen vorhanden sind.
RETEXTRA	Die Aufbewahrungsdauer für inaktive Versionen in Tagen.
RETONLY	Die Aufbewahrungsdauer für die letzten inaktiven Versionen in Tagen, wenn keine aktiven Versionen vorhanden sind.

Wenn jede Sicherungsversion einen eindeutigen Namen hat, z. B. eine Zeitmarke im Namen, findet die Versionssteuerung nicht automatisch statt: jedes Objekt ist aktiv. Aktive Objekte verfallen nie, daher wäre es die Aufgabe einer Anwendung, diese mit dem Aufruf **dsmDeleteObj** zu inaktivieren. In dieser Situation wäre es für die Anwendung erforderlich, dass die inaktivierten Objekte so bald wie möglich verfallen. Der Benutzer würde eine Sicherungskopiengruppe mit VERDELETED=0 und RETONLY=0 definieren.

Die Archivierungskomponente des IBM Spectrum Protect-Systems erlaubt die Speicherung von Objekten auf dem Server mit Steuerangaben für den Aufbewahrungs- oder Verfallszeitraum anstelle der Versionssteuerung. Jedes gespeicherte Objekt ist eindeutig, auch wenn sein Name mit einem bereits archivierten Objekt übereinstimmt. Bei Archivierungsobjekten ist den Metadaten ein Beschreibungsfeld zugeordnet, mit dem während einer Abfrage ein bestimmtes Objekt identifiziert werden kann.

Jedem Objekt auf dem IBM Spectrum Protect-Server wird eine eindeutige Objekt-ID zugewiesen. Die Persistenz des ursprünglichen Werts wird während der Lebensdauer eines Objekts nicht garantiert (insbesondere nach einem Export oder Import). Daher sollte eine Anwendung die ursprüngliche Objekt-ID zur Verwendung in zukünftigen Zurückschreibungen nicht abfragen und speichern. Stattdessen sollte eine Anwendung den Objektnamen und das Einfügedatum speichern. Sie können mit diesen Informationen während einer Zurückschreibung Objekte abfragen und das Einfügedatum verifizieren. Dann kann das Objekt mit der aktuellen Objekt-ID zurückgeschrieben werden.

Komprimierung

Konfigurationsoptionen auf einem bestimmten Knoten legen in Verbindung mit der dsmSendObj-Option objCompressed fest, ob IBM Spectrum Protect das Objekt während eines Sendevorgangs komprimiert. Außerdem werden Objekte mit einer Größenschätzung (sizeEstimate), die DSM_MIN_COMPRESS_SIZE unterschreitet, nie komprimiert.

Wenn das Objekt bereits komprimiert ist (objCompressed=bTrue), wird es nicht noch einmal komprimiert. Wenn es nicht komprimiert ist, trifft IBM Spectrum Protect die Entscheidung, ob das Objekt komprimiert werden soll, anhand der Werte der Komprimierungsoption, die vom Administrator und in den API-Konfigurationsquellen definiert ist.

Der Administrator kann die Komprimierungsschwellenwerte auf dem Server mit dem Befehl register node ändern (compression=yes, no oder Vom Client bestimmt). Bei Angabe von Vom Client bestimmt wird das Komprimierungsverhalten durch den Wert der Komprimierungsoption in den Konfigurationsquellen bestimmt.

Bei einigen Datentypen, z. B. bereits komprimierte Daten, kann die Datengröße sogar zunehmen, wenn sie mit dem Komprimierungsalgorithmus verarbeitet werden. In diesem Fall wird der Rückkehrcode DSM_RC_COMPRESS_GREW generiert. Wenn Sie feststellen, dass dieser Fall eintreten könnte, Sie die Sendeoperation aber dennoch fortsetzen wollen, teilen Sie den Endbenutzern mit, folgende Option in ihrer Optionsdatei anzugeben:

```
COMPRESSAlways Yes
```

Wenn Sie während der Ausführung der Funktion dsmSendData bei aktivierter Komprimierung den Rückkehrcode DSM_RC_COMPRESS_GREW empfangen, möchten Sie eventuell von vorn beginnen und das Objekt ohne Komprimierung erneut senden. Um dies durchzusetzen, setzen Sie ObjAttr.objCompressed in dsmSendObj auf bTrue.

Informationen zum tatsächlichen Komprimierungsverhalten während einer dsmSendObj-Operation werden durch den Aufruf dsmEndSendObjEx zurückgegeben. objCompressed gibt an, ob die Komprimierung durchgeführt wurde. totalBytesSent ist die Anzahl der von der Anwendung gesendeten Byte. totalCompressedSize ist die Anzahl Byte nach der Komprimierung. Der Aufruf dsmEndSendObjEx verfügt außerdem über ein Feld totalLFBytesSent, das die Gesamtanzahl der LAN-unabhängig gesendeten Byte enthält.

Achtung: Soll Ihre Anwendung eine Zurückschreibung oder einen Abruf von Teilobjekten ausführen, können die Daten während des Sendevorgangs nicht komprimiert werden. Um dies durchzusetzen, setzen Sie ObjAttr.objCompressed in dsmSendObj auf bTrue.

- Komprimierungstyp
  Der vom Client verwendete Komprimierungstyp wird durch die während der Sicherungs- oder Archivierungsverarbeitung verwendete Kombination von Komprimierung und clientseitiger Datendeduplizierung bestimmt.

Pufferkopieneliminierung

Mit der Pufferkopieneliminierungsfunktion wird die Kopie von Datenpuffern zwischen einer Anwendung und dem IBM Spectrum Protect-Server entfernt, was eine bessere Prozessorauslastung zur Folge hat. Den größten Effekt hat dieses Konzept in einer LAN-unabhängigen Umgebung.

Die Puffer für die Datenversetzung werden von IBM Spectrum Protect zugeordnet und ein Verweis wird an die Anwendung zurückgegeben. Die Anwendung stellt die Daten in den bereitgestellten Puffer und dieser Puffer wird über die Übertragungsschichten unter Verwendung gemeinsam genutzten Speichers an den Speicheragenten übergeben. Die Daten werden dann auf die Bandeinheit versetzt, wodurch Datenkopien eliminiert werden. Diese Funktion kann mit Sicherungs- oder Archivierungsoperationen verwendet werden.

Achtung: Wenn Sie diese Methode verwenden, müssen Sie besonderes Augenmerk auf die korrekte Pufferhandhabung und die Größe der Puffer legen. Die Puffer werden gemeinsam von den Komponenten genutzt und jede Speicherüberschreibung aufgrund eines Programmierfehlers hat schwerwiegende Fehler zur Folge.

Die gesamte Aufruffolge für die Sicherung/Archivierung ist wie folgt:

```
dsmInitEx (UseTsmBuffers = True, numTsmBuffers
= [wie viele von IBM Spectrum Protect zugeordnete Puffer die Anwendung zuordnen muss])
```

```
dsmBeginTxn
für jedes Objekt in der Transaktion
  dsmBindMC
    dsmSendObject
      dsmRequestBuffer
      dsmSendBufferData (sendet und gibt den verwendeten Puffer frei)
    dsmEndSendObjEx
dsmEndTxn
für jeden noch angehaltenen Puffer
      dsmReleaseBuffer
dsmTerminate
```

Die Funktion dsmRequestBuffer kann mehrfach aufgerufen werden bis zu der Höhe des Wertes, der durch die Option numTsmBuffers angegeben wird. Die Anwendung kann über zwei Threads verfügen: einen Produzententhread, der Puffer mit Daten füllt, und einen Konsumententhread, der diese Puffer mit dem Aufruf dsmSendBufferData an IBM Spectrum Protect sendet. Wenn ein Aufruf dsmRequestBuffer ausgegeben und dadurch der in numTsmBuffers angegebene Wert erreicht wird, wird der Aufruf dsmRequestBuffer so lange blockiert, bis ein Puffer freigegeben wird. Die Freigabe des Puffers kann erfolgen durch Aufrufen von dsmSendBufferData, wodurch ein Puffer gesendet und freigegeben wird, oder durch Aufrufen von dsmReleaseBuffer. Weitere Informationen finden Sie unter callbuff.c im API-Musterverzeichnis.

Tritt an irgendeinem Punkt beim Senden ein Fehler auf, muss die Anwendung alle angehaltenen Puffer freigeben und die Sitzung beenden. Beispiel:

```
  Bei Fehler
    für jeden von der Anwendung angehaltenen Datenpuffer
      dsmReleaseBuffer aufrufen
  dsmTerminate
```

Wenn dsmTerminate von einer Anwendung aufgerufen wird und noch ein Puffer angehalten ist, wird die API nicht verlassen. Der folgende Code wird zurückgegeben: `DSM_RC_CANNOT_EXIT_MUST_RELEASE_BUFFER`. Wenn die Anwendung den Puffer nicht freigeben kann, muss sie den Prozess verlassen, um eine Bereinigung zu erzwingen.

- Pufferkopieneliminierung und Zurückschreibung und Abruf
  Der IBM Spectrum Protect-Server steuert das in den Puffer zu übertragende Datenvolumen, basierend auf der Bandzugriffsoptimierung beim Zurückschreiben und Abrufen. Diese Methode ist weniger vorteilhaft für die Anwendung als die normale Methode zum Abrufen von Daten. Prüfen Sie bei der Prototyperstellung die Leistung der Pufferkopieneliminierungsmethode und verwenden Sie diese Methode nur, wenn Sie eine nennenswerte Verbesserung erkennen.

API-Verschlüsselung

Es stehen zwei Verfahren zum Verschlüsseln von Daten zur Verfügung: die anwendungsverwaltete Verschlüsselung und die IBM Spectrum Protect-Clientverschlüsselung.

Wählen und verwenden Sie nur eines dieser Verfahren zum Verschlüsseln von Daten. Die Verfahren schließen sich gegenseitig aus. Wenn Sie Daten mit beiden Verfahren verschlüsseln, können Sie einige Daten nicht zurückschreiben oder abrufen. Beispiel: Angenommen, eine Anwendung verwendet die anwendungsverwaltete Verschlüsselung zum Verschlüsseln von Objekt A und verwendet anschließend die IBM Spectrum Protect-Clientverschlüsselung zum Verschlüsseln von Objekt B. Wenn die Anwendung für eine Zurückschreibungsoperation festlegt, dass die IBM Spectrum Protect-Clientverschlüsselung verwendet werden soll, und versucht, beide Objekte zurückzuschreiben, kann nur Objekt B zurückgeschrieben werden. Objekt A kann nicht zurückgeschrieben werden, weil es von der Anwendung und nicht vom Client verschlüsselt wurde.

Unabhängig vom verwendeten Verschlüsselungsverfahren muss IBM Spectrum Protect die Kennwortauthentifizierung aktivieren. Standardmäßig verwendet der Server `SET AUTHENTICATION ON`.

Die API verwendet entweder die 128-Bit-AES-Verschlüsselung oder die 256-Bit-AES-Verschlüsselung. Die 256-Bit-AES-Datenverschlüsselung stellt eine höhere Datenverschlüsselungsebene als die 128-Bit-AES-Datenverschlüsselung bereit. Mit 256-Bit-AES-Verschlüsselung gesicherte Dateien können nicht mit einem Client, der eine ältere Version aufweist, zurückgeschrieben werden. Die Verschlüsselung kann mit oder ohne Komprimierung aktiviert werden. Wenn Sie mit Verschlüsselung arbeiten, können Sie nicht die Zurückschreibung von Teilobjekten und keine Abruf- und Pufferkopieneliminierungsfunktionen verwenden.

- Anwendungsverwaltete Verschlüsselung
  Bei der anwendungsverwalteten Verschlüsselung stellt die Anwendung der API das Schlüsselkennwort (unter Verwendung des Schlüssels DSM_ENCRYPT_USER) zur Verfügung und die Anwendung ist für die Verwaltung des Schlüsselkennworts zuständig.
- IBM Spectrum Protect-Clientverschlüsselung
  Die IBM Spectrum Protect-Clientverschlüsselung verwendet den vom Wert DSM_ENCRYPT_CLIENTENCRKEY verwalteten Schlüssel, um Ihre Daten zu schützen. Die Clientverschlüsselung ist transparent für die Anwendung, von der die API verwendet wird. Allerdings sind Zurückschreibungs- und Abrufoperationen von Teilobjekten für verschlüsselte oder komprimierte Objekte nicht möglich.

Anwendungsverwaltete Verschlüsselung

Bei der anwendungsverwalteten Verschlüsselung stellt die Anwendung der API das Schlüsselkennwort (unter Verwendung des Schlüssels DSM_ENCRYPT_USER) zur Verfügung und die Anwendung ist für die Verwaltung des Schlüsselkennworts zuständig.

Achtung: Wenn der Verschlüsselungsschlüssel nicht gespeichert wird und Sie den Schlüssel vergessen, können Ihre Daten nicht wiederhergestellt werden.

Die Anwendung stellt das Schlüsselkennwort im Aufruf dsmInitEx bereit und muss das korrekte Schlüsselkennwort zum Zeitpunkt der Zurückschreibung bereitstellen.

Achtung: Wenn das Schlüsselkennwort verloren geht, gibt es keine Möglichkeit, die Daten zurückzuschreiben.

Für Sicherungs- und Zurückschreibungsoperationen (oder Archivierungs- und Abrufoperationen) für dasselbe Objekt muss dasselbe Schlüsselkennwort verwendet werden. Dieses Verfahren ist nicht von der Version des IBM Spectrum Protect-Servers abhängig. Zum Konfigurieren dieses Verfahrens müssen in der Anwendung folgende Schritte ausgeführt werden:

1. Die Variable bEncryptKeyEnabled muss im Aufruf dsmInitEx auf bTrue gesetzt werden und die Variable encryptionPasswordP muss auf eine Zeichenfolge mit dem Schlüsselkennwort für die Verschlüsselung verweisen.
2. Die Option include.encrypt muss für die Objekte auf encrypt gesetzt werden. Um beispielsweise alle Daten zu verschlüsseln, definieren Sie Folgendes:

   ```
   include.encrypt /.../* (UNIX)
   ```

   und

   ```
   include.encrypt *\...\* (Windows)
   ```

   Geben Sie Folgendes an, um das Objekt /FS1/DB2/FULL zu verschlüsseln:

   ```
   include.encrypt /FS1/DB2/FULL
   ```

3. Unter Windows muss in der Optionszeichenfolge, die im Aufruf dsmInitEx an die API übergeben wird, ENCRYPTKEY=PROMPT|SAVE festgelegt werden. Diese Option kann auch in dsm.opt (Windows) oder dsm.sys (UNIX oder Linux) angegeben werden.

Standardmäßig wird die Option encryptkey auf prompt gesetzt. Diese Einstellung stellt sicher, dass der Schlüssel nicht automatisch gespeichert wird. Wird für encryptkey 'save' angegeben, wird der Schlüssel von IBM Spectrum Protect auf der lokalen Maschine gespeichert; in diesem Fall ist jedoch nur ein einziger Schlüssel für alle IBM Spectrum Protect-Operationen mit demselben Knotennamen gültig.

Nachdem ein Objekt gesendet wurde, gibt dsmEndSendObjEx an, ob ein Objekt verschlüsselt wurde und welches Verfahren verwendet wurde. Gültige Werte im Feld *encryptionType*:

- DSM_ENCRYPT_NO
- DSM_ENCRYPT_USER
- DSM_ENCRYPT_CLIENTENCRKEY

In der folgenden Tabelle sind die API-Verschlüsselungstypen, Voraussetzungen und verfügbaren Funktionen aufgelistet.

Tabelle 1. API-Verschlüsselungstypen, Voraussetzungen und verfügbare Funktionen

Typ	**Voraussetzungen**	**Verfügbare Funktion**
ENCRYPTIONTYPE	Keine	Festlegen von ENCRYPTIONTYPE in der Optionszeichenfolge, die unter Windows im Aufruf dsmInitEx an die API übergeben wird. Der Standardwert ist ENCRYPTIONTYPE=AES128.
EncryptKey=save	Keine	API und Sicherung/Archivierung
EncryptKey=prompt	Keine	API und Sicherung/Archivierung
EncryptKey=generate	Keine	API und Sicherung/Archivierung
EnableClientEncryptKey	Keine	Nur API

Anmerkung: Es wird empfohlen, auf dem Server die Authentifizierung auf ON zu setzen. Wird die Authentifizierung auf OFF gesetzt, wird der Schlüssel nicht verschlüsselt, während die Daten verschlüsselt werden. Diese Vorgehensweise wird jedoch nicht empfohlen.

Tabelle 2 zeigt, wie sowohl berechtigte Benutzer als auch nicht berechtigte Benutzer Daten während einer Sicherungs- oder Zurückschreibungsoperation abhängig von dem für die Option passwordaccess angegebenen Wert verschlüsseln oder entschlüsseln können. Die Datei TSM.PWD muss vorhanden sein, damit die folgenden Operationen von berechtigten und nicht berechtigten Benutzern ausgeführt werden können. Der berechtigte Benutzer erstellt die Datei TSM.PWD und setzt die Option encryptkey auf 'save' und die Option passwordaccess auf 'generate'.

Tabelle 2. Verschlüsselung oder Entschlüsselung von Daten mit einem anwendungsverwalteten Schlüssel unter UNIX oder Linux

Operation	**Option passwordaccess**	**Option encryptkey**	**Ergebnis**
Sicherung durch berechtigten Benutzer	generate	save	Daten verschlüsselt.
	generate	prompt	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.

Operation	Option passwordaccess	Option encryptkey	Ergebnis
	prompt	save	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
	prompt	prompt	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
Zurückschreibung durch berechtigten Benutzer	generate	save	Daten verschlüsselt.
	generate	prompt	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
	prompt	save	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
	prompt	prompt	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
Sicherung durch nicht berechtigten Benutzer	generate	save	Daten verschlüsselt.
	generate	prompt	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
	prompt	save	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
	prompt	prompt	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
Zurückschreibung durch nicht berechtigten Benutzer	generate	save	Daten verschlüsselt.
	generate	prompt	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
	prompt	save	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.
	prompt	prompt	Daten verschlüsselt, wenn encryptionPasswordP ein Verschlüsselungskennwort enthält.

IBM Spectrum Protect-Clientverschlüsselung

Die IBM Spectrum Protect-Clientverschlüsselung verwendet den vom Wert DSM_ENCRYPT_CLIENTENCRKEY verwalteten Schlüssel, um Ihre Daten zu schützen. Die Clientverschlüsselung ist transparent für die Anwendung, von der die API verwendet wird. Allerdings sind Zurückschreibungs- und Abrufoperationen von Teilobjekten für verschlüsselte oder komprimierte Objekte nicht möglich.

Sowohl bei der IBM Spectrum Protect-Clientverschlüsselung als auch bei der anwendungsverwalteten Verschlüsselung bezieht sich das Verschlüsselungskennwort auf einen Zeichenfolgewert, mit dem der tatsächliche Verschlüsselungsschlüssel generiert wird. Der Wert für die Option für das Verschlüsselungskennwort kann 1 bis 63 Zeichen lang sein, aber der daraus generierte Schlüssel hat immer eine Länge von 8 Byte bei 56-Bit-DES, 16 Byte bei 128-Bit-AES und 32 Byte bei 256-Bit-AES.

Achtung: Wenn der Verschlüsselungsschlüssel nicht verfügbar ist, können Daten weder zurückgeschrieben noch abgerufen werden. Wenn Sie ENABLECLIENTENCRYPTKEY für die Verschlüsselung verwenden, wird der Verschlüsselungsschlüssel in der Serverdatenbank gespeichert. Für Objekte, die dieses Verfahren verwenden, muss die Serverdatenbank vorhanden sein und die korrekten Werte für die Objekte enthalten, damit eine ordnungsgemäße Zurückschreibung möglich ist. Stellen Sie sicher, dass Sie Ihre Serverdatenbank häufig sichern, um einen Datenverlust zu verhindern.

Dies ist im Hinblick auf die Implementierung das einfachere Verfahren; dabei wird jeweils ein Verschlüsselungszufallsschlüssel pro Sitzung generiert und auf dem IBM Spectrum Protect-Server mit dem Objekt in der Serverdatenbank gespeichert. Während der Zurückschreibung wird der gespeicherte Schlüssel für die Entschlüsselung verwendet. Bei der Verwendung dieses Verfahrens ist IBM Spectrum Protect für die Verwaltung des Schlüssels zuständig; die Anwendung muss sich überhaupt nicht damit befassen. Da der Schlüssel in der Serverdatenbank gespeichert ist, muss eine gültige IBM Spectrum Protect-Datenbank für eine Zurückschreibungsoperation eines verschlüsselten Objekts vorhanden sein. Wenn der Schlüssel zwischen der API und dem Server übertragen wird, wird er ebenfalls verschlüsselt. Die Übertragung des Schlüssels ist sicher; wenn der Schlüssel in der Datenbank des IBM Spectrum Protect-Servers gespeichert wird, wird er verschlüsselt. Die einzige Zeit, während der der Schlüssel im Exportdatenstrom nicht verschlüsselt ist, ist beim Export der Daten eines Knotens zwischen Servern.

Gehen Sie wie folgt vor, um die IBM Spectrum Protect-Clientverschlüsselung zu aktivieren:

1. Geben Sie -ENABLECLIENTENCRYPTKEY=YES in der Optionszeichenfolge an, die im Aufruf dsmInitEx an die API übergeben wird, oder geben Sie die Option in der Systemoptionsdatei dsm.opt (Windows) bzw. dsm.sys (UNIX oder Linux) an.
2. Geben Sie include.encrypt für die Objekte an, die verschlüsselt werden sollen. Um beispielsweise alle Daten zu verschlüsseln, definieren Sie Folgendes:

```
include.encrypt /.../* (UNIX)
```

und

```
include.encrypt *\...\* (Windows)
```

Geben Sie Folgendes an, um das Objekt /FS1/DB2/FULL zu verschlüsseln:

```
include.encrypt /FS1/DB2/FULL
```

Datendeduplizierung

Die Datendeduplizierung ist eine Methode zum Verringern des Speicherbedarfs, indem redundante Daten eliminiert werden.

Übersicht

Bei IBM Spectrum Protect sind zwei Typen von Datendeduplizierung verfügbar: *clientseitige Datendeduplizierung* und *serverseitige Datendeduplizierung*.

Als *clientseitige Datendeduplizierung* wird ein Datendeduplizierungsverfahren bezeichnet, das der Client für Sichern/Archivieren verwendet, um bei der Sicherungs- und Archivierungsverarbeitung redundante Daten zu entfernen, bevor die Daten an den IBM Spectrum Protect-Server übertragen werden. Mithilfe der clientseitigen Datendeduplizierung kann das Datenvolumen, das über ein lokales Netz gesendet wird, reduziert werden.

Die *serverseitige Datendeduplizierung* ist ein Datendeduplizierungsverfahren, das vom Server ausgeführt wird. Der IBM Spectrum Protect-Administrator kann die zu verwendende Position für die Datendeduplizierung (Client oder Server) mit dem Parameter DEDUP im Serverbefehl REGISTER NODE oder UPDATE NODE angeben.

Erweiterungen

Mit der clientseitigen Datendeduplizierung haben Sie folgende Möglichkeiten:

- Bestimmte Dateien auf einem Client von der Datendeduplizierung ausschließen.
- Einen Cache für die Datendeduplizierung aktivieren, der den Datenaustausch im Netz zwischen dem Client und dem Server reduziert. Der Cache enthält Bereiche, die in vorherigen Teilsicherungsoperationen an den Server gesendet wurden. Anstatt den Server nach dem Vorhandensein eines Bereichs abzufragen, fragt der Client seinen Cache ab.

  Eine Größe und Position für einen Client-Cache angeben. Wird eine Inkonsistenz zwischen dem Server und dem lokalen Cache festgestellt, wird der lokale Cache entfernt und erneut gefüllt.

  Anmerkung: Für Anwendungen, die die IBM Spectrum Protect-API verwenden, darf der Datendeduplizierungscache wegen möglicher Sicherungsfehler nicht verwendet werden, die verursacht werden, wenn der Cache nicht mit dem IBM Spectrum Protect-Server synchron ist. Wenn mehrere, gleichzeitig ablaufende Sitzungen des Clients für Sichern/Archivieren konfiguriert sind, muss für jede Sitzung ein separater Cache konfiguriert werden.
- Sowohl die clientseitige Datendeduplizierung als auch die Komprimierung aktivieren, um das vom Server gespeicherte Datenvolumen zu reduzieren. Jeder Bereich wird komprimiert, bevor er an den Server gesendet wird. Der Kompromiss liegt zwischen Speichereinsparungen und der Verarbeitungsleistung, die zum Komprimieren der Clientdaten erforderlich ist. Im Allgemeinen gilt: Wenn Sie Daten auf dem Clientsystem komprimieren und deduplizieren, ist etwa zweimal so viel Verarbeitungsleistung wie für die Datendeduplizierung allein erforderlich.

  Der Server kann mit deduplizierten, komprimierten Daten arbeiten. Außerdem können Clients für Sichern/Archivieren vor Version 6.2 deduplizierte, komprimierte Daten zurückschreiben.

Die clientseitige Datendeduplizierung verwendet den folgenden Prozess:

- Der Client erstellt Bereiche. *Bereiche* sind Teile von Dateien, die mit anderen Dateibereichen verglichen werden, um Duplikate zu identifizieren.
- Der Client und der Server arbeiten zusammen, um doppelte Bereiche zu identifizieren. Der Client sendet Bereiche, die nicht doppelt sind, an den Server.
- Nachfolgende clientseitige Datendeduplizierungsoperationen erstellen neue Bereiche. Einige oder alle dieser Bereiche können mit den Bereichen übereinstimmen, die in vorherigen Datendeduplizierungsoperationen erstellt und an den Server gesendet wurden. Übereinstimmende Bereiche werden nicht erneut an den Server gesendet.

Vorteile

Die clientseitige Datendeduplizierung bietet mehrere Vorteile:

- Sie kann das über das lokale Netz (LAN) gesendete Datenvolumen reduzieren.
- Die zum Identifizieren doppelter Daten erforderliche Verarbeitungsleistung wird vom Server auf Clientknoten verlagert. Die serverseitige Datendeduplizierung ist für Speicherpools, die für die Deduplizierung aktiviert sind, immer aktiviert. Dateien, die sich in den Speicherpools befinden, die für die Deduplizierung aktiviert sind, und die vom Client dedupliziert wurden, erfordern jedoch keine zusätzliche Verarbeitung.

- Die zum Entfernen doppelter Daten auf dem Server erforderliche Verarbeitungsleistung wird eliminiert. Dadurch werden Speichereinsparungen auf dem Server sofort wirksam.

Die clientseitige Datendeduplizierung hat einen möglichen Nachteil. Der Server verfügt erst dann über vollständige Kopien von Clientdateien, *wenn* Sie die primären Speicherpools, die die clientseitigen Bereiche enthalten, in einem nicht dedupizierten Kopienspeicherpool sichern. (*Bereiche* sind Teile einer Datei, die während des Prozesses für die Datendeduplizierung erstellt werden.) Während der Speicherpoolsicherung in einem nicht dedupizierten Speicherpool werden clientseitige Bereiche in aneinandergrenzenden Dateien neu erstellt.

Standardmäßig müssen primäre Speicherpools mit sequenziellem Zugriff, die für die Datendeduplizierung definiert sind, in nicht dedupizierten Kopienspeicherpools gesichert werden, bevor sie zurückgefordert und doppelte Daten entfernt werden können. Mit dem Standardwert wird sichergestellt, dass der Server immer über Kopien vollständiger Dateien in einem primären Speicherpool oder einem Kopienspeicherpool verfügt.

Wichtig: Eine weitere Datenreduktion wird erzielt, wenn Sie die clientseitige Datendeduplizierung zusammen mit der Komprimierung aktivieren. Jeder Bereich wird komprimiert, bevor er an den Server gesendet wird. Bei der Komprimierung wird Speicherbereich eingespart, die Verarbeitungszeit auf der Client-Workstation verlängert sich jedoch.

Die folgenden Optionen gelten für die Datendeduplizierung:

- Deduplication
- Dedupcachepath
- Dedupcachesize
- Enablededupcache
- Exclude.dedup
- Include.dedup

- Clientseitige Datendeduplizierung der API
  Die *clientseitige Datendeduplizierung* wird von der API auf dem Client für Sichern/Archivieren verwendet, um redundante Daten während der Sicherungs- und Archivierungsverarbeitung zu entfernen, bevor die Daten an den IBM Spectrum Protect übertragen werden.
- Serverseitige Datendeduplizierung
  Die serverseitige Datendeduplizierung ist eine Datendeduplizierung, die vom Server ausgeführt wird.

Clientseitige Datendeduplizierung der API

Die *clientseitige Datendeduplizierung* wird von der API auf dem Client für Sichern/Archivieren verwendet, um redundante Daten während der Sicherungs- und Archivierungsverarbeitung zu entfernen, bevor die Daten an den IBM Spectrum Protect übertragen werden.

Die clientseitige Datendeduplizierung wird von der API verwendet, um redundante Daten während der Sicherungs- und Archivierungsverarbeitung zu entfernen, bevor die Daten an den IBM Spectrum Protect-Server übertragen werden. Mithilfe der clientseitigen Datendeduplizierung kann das Datenvolumen, das über ein lokales Netz gesendet wird, reduziert werden. Mithilfe der clientseitigen Datendeduplizierung kann auch der Speicherbereich des IBM Spectrum Protect-Servers reduziert werden.

Wenn der Client für die clientseitige Datendeduplizierung aktiviert ist und Sie eine Sicherungs- oder Archivierungsoperation ausführen, werden die Daten als Bereiche an den Server gesendet. Wenn die nächste Sicherungs- oder Archivierungsoperation ausgeführt wird, identifizieren der Client und der Server die Datenbereiche, die bereits gesichert oder archiviert wurden, und es werden nur die eindeutigen Datenbereiche an den Server gesendet.

Bei der clientseitigen Datendeduplizierung müssen der Server und die API Version 6.2 oder höher haben.

Bevor Sie die clientseitige Datendeduplizierung zum Sichern oder Archivieren Ihrer Dateien verwenden, muss das System die folgenden Voraussetzungen erfüllen:

- Für den Client muss die Option deduplication aktiviert sein.
- Der Server muss den Client mit dem Parameter DEDUP=CLIENTORSERVER im Befehl REGISTER NODE oder UPDATE NODE für die clientseitige Datendeduplizierung aktivieren.
- Das Speicherpoolziel für die Daten muss ein für die Datendeduplizierung aktivierter Speicherpool sein. Der für die Datendeduplizierung aktivierte Speicherpool darf nur den Einheitentyp FILE haben.
- Stellen Sie sicher, dass die Dateien an die korrekte Verwaltungsklasse gebunden sind.
- Eine Datei kann von der clientseitigen Datendeduplizierungsverarbeitung ausgeschlossen werden. Standardmäßig sind alle Dateien eingeschlossen.
- Dateien müssen größer als 2 KB sein.
- Der Server kann die maximale Transaktionsgröße für die Datendeduplizierung begrenzen, indem die Option CLIENTDEDUPTXNLIMIT auf dem Server gesetzt wird. Informationen zu dieser Option finden Sie in der Dokumentation für den Server.

Ist eine dieser Voraussetzungen nicht erfüllt, werden die Daten normal, d. h. ohne clientseitige Datendeduplizierung verarbeitet.

Nachfolgend einige der Einschränkungen, die für die Datendeduplizierung gelten:

- LAN-unabhängige Datenversetzung und clientseitige Datendeduplizierung schließen sich gegenseitig aus. Wenn Sie sowohl LAN-unabhängige Datenversetzung als auch clientseitige Datendeduplizierung aktivieren, werden LAN-unabhängige Datenversetzungsoperationen ausgeführt und die clientseitige Datendeduplizierung wird ignoriert.

- Verschlüsselung und clientseitige Datendeduplizierung schließen sich gegenseitig aus. Wenn Sie sowohl Verschlüsselung als auch clientseitige Datendeduplizierung aktivieren, werden Verschlüsselungsoperationen ausgeführt und die clientseitige Datendeduplizierung wird ignoriert. Verschlüsselte Dateien und Dateien, die für die clientseitige Datendeduplizierung auswählbar sind, können in derselben Operation verarbeitet werden, die Verarbeitung erfolgt jedoch in unterschiedlichen Transaktionen.
  Voraussetzungen:
  1. In jeder Transaktion müssen entweder alle Dateien für die Datendeduplizierung eingeschlossen oder von der Datendeduplizierung ausgeschlossen werden. Sind in einer Transaktion diese Dateien gemischt, schlägt die Transaktion fehl und von der API wird der Rückkehrcode `DSM_RC_NEEDTO_ENDTXN` zurückgegeben.
  2. Verwenden Sie Speichereinheitenverschlüsselung zusammen mit clientseitiger Datendeduplizierung. Da SSL in Kombination mit clientseitiger Deduplizierung verwendet wird, ist keine Clientverschlüsselung erforderlich.
- Die folgenden Funktionen sind für die clientseitige Datendeduplizierung nicht verfügbar:
  - HSM-Client (HSM = IBM Spectrum Protect for Space Management)
  - API-Puffer für gemeinsamen Zugriff
  - NAS
  - Subdateisicherung
- Pufferkopieneliminierung kann nicht mit Datenkonvertierungen wie Komprimierung, Verschlüsselung und Datendeduplizierung verwendet werden.
- Wenn Sie die clientseitige Deduplizierung verwenden, erkennt und unterlässt die API (mit RC=254) Sicherungen von Dateibereichen, die auf dem Server als verfallen markiert sind, während Daten an den Server gesendet werden. Soll die Operation wiederholt werden, müssen Sie diese Programmierung in die aufrufende Anwendung einschließen.
- Operationen für gleichzeitiges Schreiben auf dem Server haben Vorrang vor der clientseitigen Datendeduplizierung. Sind Operationen für gleichzeitiges Schreiben aktiviert, erfolgt keine clientseitige Datendeduplizierung.
  Einschränkung: Ist die clientseitige Datendeduplizierung aktiviert, ist für die API keine Wiederherstellung von einem Zustand möglich, bei dem kein Speicherbereich mehr im Zielpool des Servers verfügbar ist, selbst wenn ein nächster Pool definiert ist. Der Ursachencode DSM_RS_ABORT_DESTINATION_POOL_CHANGED zum Stoppen wird zurückgegeben und die Operation schlägt fehl. Es gibt zwei Möglichkeiten zur Wiederherstellung in dieser Situation:
  1. Bitten Sie den Administrator, dem ursprünglichen Dateipool weitere Arbeitsdatenträger hinzuzufügen.
  2. Wiederholen Sie die Operation mit inaktivierter Datendeduplizierung.

Für noch geringere Anforderungen an die Bandbreite können Sie einen lokalen Cache für die Datendeduplizierung aktivieren. Der lokale Cache verhindert, dass Abfragen an den IBM Spectrum Protect-Server gesendet werden. Der Standardwert für ENABLEDEDUPCACHE ist NO, d. h., der Cache ist mit dem Server synchron. Wenn der Cache mit dem Server nicht synchron ist, sendet die Anwendung alle Daten erneut. Wenn Ihre Anwendung eine fehlgeschlagene Transaktion wiederholen kann und der lokale Cache verwendet werden soll, setzen Sie die Option ENABLEDEDUPCACHE in der Datei dsm.opt (Windows) oder in der Datei dsm.sys (UNIX) auf YES.

Am Ende einer Zurückschreibung wird, wenn *alle* Daten über die API zurückgeschrieben wurden und das Objekt vom Client dedupliziert wurde, ein End-to-End-Digest berechnet und mit dem zum Zeitpunkt der Sicherung berechneten Wert verglichen. Stimmen diese Werte nicht überein, wird der Fehler DSM_RC_DIGEST_VALIDATION_ERROR zurückgegeben. Wenn eine Anwendung diesen Fehler empfängt, sind die Daten beschädigt. Dieser Fehler kann auch die Folge eines temporären Fehlers im Netz sein; wiederholen Sie in diesem Fall die Zurückschreibung oder den Abruf.

Das folgende Beispiel zeigt den Befehl zum Abfragen der Sitzung mit Datendeduplizierungsinformationen:

```
Werte für dsmQuerySessInfo:
Serverinformationen:
Servername: SERVER1
Server-Host: AVI
Server-Port: 1500
Serverdatum: 2009/10/6 20:48:51
Servertyp: Windows
Serverversion: 6.2.0.0
Aufbewahrungsschutz für Archivierung (Server): NEIN
Clientinformationen:
Clientknotentyp: API Test1
Begrenzer für Dateibereich (Client): :
Begrenzer für HL & LL (Client): \
Clientkomprimierung: Vom Client bestimmt (3u)
Archivierung löschen (Client): Client kann archivierte Objekte löschen
Sicherung löschen (Client): Client kann Sicherungsobjekte NICHT löschen
Maximale Anzahl Objekte in Transaktion mit mehreren Objekten: 4096
LAN-unabhängig aktiviert: NEIN
Deduplizierung: Client oder Server
Allgemeine Sitzungsinformationen:
Knoten: AVI
Eigner:
API-Konfigurationsdatei:
```

Das folgende Beispiel zeigt den Befehl zum Abfragen der Verwaltungsklasse mit Datendeduplizierungsinformationen:

```
Maßnahmeninformationen:
Domänenname: DEDUP
Name der Maßnahmengruppe: DEDUP
Maßnahmenaktivierungsdatum: 0/0/0 0:0:0
Standardverwaltungsklasse: DEDUP
Aufbewahrungszeitraum für Sicherung: 30 Tage
```

```
Aufbewahrungszeitraum für Archivierung: 365 Tage
Verwaltungsklasse 1:
Name: DEDUP
Beschreibung: Deduplizierung - Standardwerte
Name der Sicherungskopiengruppe: STANDARD
Häufigkeit: 0
Versionsdaten vorhanden: 2
Versionsdaten gelöscht: 1
Extraversionen aufbewahren: 30
Nur Versionen aufbewahren: 60
Kopienziel: AVIFILEPOOL
LAN-unabhängiges Ziel: NEIN
Daten deduplizieren: JA

Name der Archivierungskopiengruppe: STANDARD
Häufigkeit: 10000
Versionen aufbewahren: 365
Kopienziel: AVIFILEPOOL
LAN-unabhängiges Ziel: NEIN
Anfangsversion aufbewahren: CREATE
Mindestversionen aufbewahren: 65534
Daten deduplizieren: JA
```

- Dateien von der Datendeduplizierung ausschließen
  Falls gewünscht, können Sie Sicherungs- oder Archivierungsdateien von der Datendeduplizierung ausschließen.
- Dateien für die Datendeduplizierung einschließen
  Falls gewünscht, können Sie Sicherungs- oder Archivierungsdateien für die Datendeduplizierung einschließen.

Zugehörige Verweise:
Option Deduplication
Option exclude
Option dedupcachepath
Option dedupcachesize
Option enablededupcache
Option ieobjtype

Dateien von der Datendeduplizierung ausschließen

Falls gewünscht, können Sie Sicherungs- oder Archivierungsdateien von der Datendeduplizierung ausschließen.

Um Dateien von der Datendeduplizierungsverarbeitung auszuschließen, führen Sie diese Schritte aus:

1. Definieren Sie die Option exclude.dedup für die Objekte, die ausgeschlossen werden sollen.

   Um beispielsweise alle Deduplizierungsdaten für UNIX-Systeme auszuschließen, definieren Sie Folgendes:

   ```
   exclude.dedup /.../*
   ```

2. Um alle Deduplizierungsdaten für Windows-Systeme auszuschließen, definieren Sie Folgendes:

   ```
   exclude.dedup *\...\*
   ```

Wichtig: Wenn ein Objekt an einen Datendeduplizierungspool gesendet wird, erfolgt selbst dann eine Datendeduplizierung auf dem Server, wenn das Objekt von der clientseitigen Datendeduplizierung ausgeschlossen ist.

Dateien für die Datendeduplizierung einschließen

Falls gewünscht, können Sie Sicherungs- oder Archivierungsdateien für die Datendeduplizierung einschließen.

Um die Liste der einzuschließenden Dateien einzugrenzen, kann die Option include.dedup zusammen mit der Option exclude.dedup verwendet werden.

Standardmäßig werden alle auswählbaren Objekte für die Datendeduplizierung eingeschlossen.

Nachfolgend einige Beispiele für UNIX und Linux:

```
exclude.dedup /FS1/.../*

include.dedup /FS1/archive/*
```

Nachfolgend einige Beispiele für Windows:

```
exclude.dedup E:\myfiles\...\*

include.dedup E:\myfiles\archive\*
```

Serverseitige Datendeduplizierung

Die serverseitige Datendeduplizierung ist eine Datendeduplizierung, die vom Server ausgeführt wird.

Der IBM Spectrum Protect-Administrator kann die zu verwendende Position für die Datendeduplizierung (Client oder Server) mit dem Parameter DEDUP im Serverbefehl REGISTER NODE oder UPDATE NODE angeben.

In einem Speicherpool (Dateipool), der für die Datendeduplizierung aktiviert ist, wird nur eine einzige Instanz eines Datenbereichs aufbewahrt. Andere Instanzen desselben Datenbereichs werden durch einen Verweis auf die aufbewahrte Instanz ersetzt.

Weitere Informationen zur serverseitigen Datendeduplizierung finden Sie in der Dokumentation für den IBM Spectrum Protect-Server.

Anwendungsübernahme

Wenn der IBM Spectrum Protect-Server wegen einer Betriebsunterbrechung nicht mehr verfügbar ist, können Anwendungen, die die API verwenden, für die Datenwiederherstellung automatisch eine Übernahme auf einem Sekundärserver durchführen.

Der IBM Spectrum Protect-Server, zu dem der Client und die API während des normalen Produktionsprozesses eine Verbindung herstellen, wird als *Primärserver* bezeichnet. Wenn der Primärserver für die Knotenreplikation konfiguriert ist, wird er auch als *Quellenreplikationsserver* bezeichnet. Die Clientknotendaten auf dem Quellenreplikationsserver können auf den *Zielreplikationsserver* repliziert werden. Dieser Server wird auch als *Sekundärserver* bezeichnet und er ist der Server, auf dem der Client automatisch eine Übernahme durchführt, wenn der Primärserver ausfällt.

Der Client und die API müssen für die automatisierte Clientübernahme konfiguriert und mit einem Server der Version 7.1 (oder einer höheren Version) verbunden sein, der Clientknotendaten repliziert. Die Konfiguration für die API ist dieselbe wie die Konfiguration für den Client für Sichern/Archivieren.

Im normalen Betrieb werden Verbindungsdaten für den Sekundärserver automatisch während des Anmeldeprozesses vom Primärserver an den Client gesendet. Die Informationen zum Sekundärserver werden automatisch in der Clientoptionsdatei gespeichert.

Die Clientanwendung versucht bei jeder Anmeldung beim IBM Spectrum Protect-Server, den Primärserver anzusprechen. Wenn der Primärserver nicht verfügbar ist, führt die Anwendung, unter Verwendung der Informationen zum Sekundärserver in der Clientoptionsdatei, eine Übernahme auf dem Sekundärserver durch. Im Übernahmemodus kann die Anwendung den Sekundärserver abfragen und replizierte Daten zurückschreiben oder abrufen.

Sie müssen die Anwendung mindestens einmal auf dem Primärserver sichern. Die API kann nur dann eine Übernahme auf dem Sekundärserver zum Wiederherstellen von Daten durchführen, wenn die Daten vom Clientknoten vom Primärserver auf den Sekundärserver repliziert wurden.

- Übernahmestatusinformationen
  Die API stellt Statusinformationen bereit, die von Anwendungen verwendet werden können, um den Übernahmestatus und den Status replizierter Clientdaten auf dem Sekundärserver festzustellen.

Zugehörige Konzepte:
Konfiguration und Verwendung der automatisierten Clientübernahme

Beispielablaufdiagramme für Sicherung und Archivierung

Der Entwurf der API basiert auf direkten Logikabläufen und klaren Übergängen zwischen den verschiedenen Zuständen des Anwendungsclients. Aufgrund dieser deutlichen Zustandsübergänge werden Logik- und Programmfehler frühzeitig im Entwicklungszyklus abgefangen und somit Qualität und Zuverlässigkeit des Systems erheblich verbessert.

Sie können beispielsweise einen Aufruf **dsmSendObj** erst absetzen, wenn eine Transaktion gestartet wurde und zuvor ein Aufruf **dsmBindMC** für das Objekt, das gesichert wird, erfolgt ist.

Abbildung 1 zeigt das Zustandsdiagramm für die Ausführung von Sicherungs- oder Archivierungsoperationen innerhalb einer Transaktion. Der Pfeil, der von "In 'Objekt senden'" auf **dsmEndTxn** zeigt, gibt an, dass ein Aufruf **dsmEndTxn** nach einem Aufruf **dsmSendObj** oder **dsmSendData** gestartet werden kann. Dies kann ausgeführt werden, wenn während des Sendevorgangs eines Objekts eine Fehlerbedingung aufgetreten ist und die gesamte Operation gestoppt werden soll. In diesem Fall müssen Sie für das Votum DSM_VOTE_ABORT angeben. Rufen Sie jedoch unter normalen Umständen **dsmEndSendObj** auf, bevor Sie die Transaktion beenden.

Abbildung 1. Zustandsdiagramm für Sicherungs- und Archivierungsoperationen

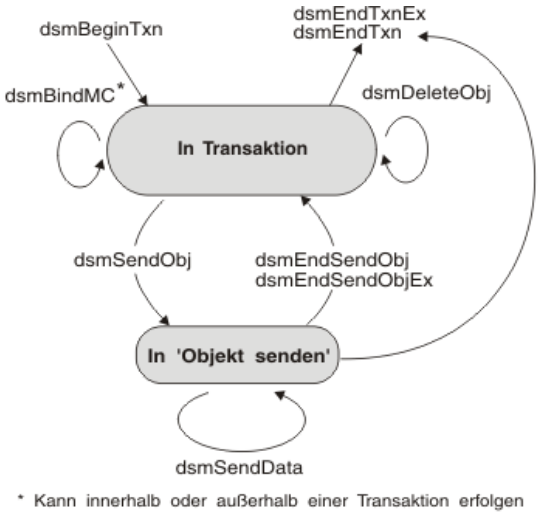
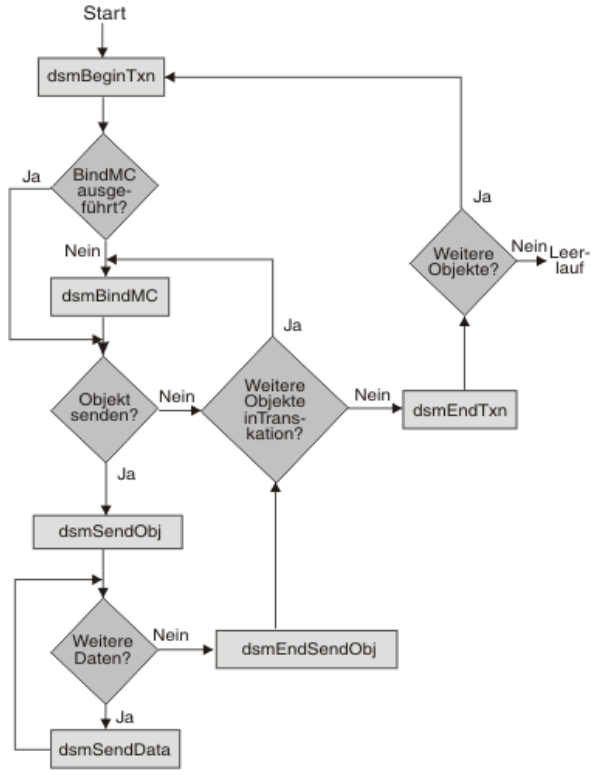


Abbildung 2 zeigt das Ablaufdiagramm für die Ausführung von Sicherungs- oder Archivierungsoperationen innerhalb einer Transaktion.

Abbildung 2. Ablaufdiagramm für Sicherungs- und Archivierungsoperationen



Das wichtigste Merkmal in diesen beiden Diagrammen ist die Schleife zwischen den folgenden API-Aufrufen innerhalb einer Transaktion:

- **dsmBindMC**
- **dsmSendObj**
- **dsmSendData**
- **dsmEndSendObj**

Der Aufruf **dsmBindMC** ist insofern einzigartig, als Sie ihn innerhalb oder außerhalb einer Transaktionsgrenze starten können. Sie können ihn auch, falls erforderlich, von einer anderen Transaktion aus starten. Einzige Voraussetzung für den Aufruf **dsmBindMC** ist, dass er vor der Sicherung oder Archivierung eines Objekts erfolgt. Wenn das Objekt, das gesichert oder archiviert wird, keiner Verwaltungsklasse zugeordnet ist, wird von **dsmSendObj** ein Fehlercode zurückgegeben. In dieser Situation wird die Transaktion beendet, indem **dsmEndTxn** aufgerufen wird. (Diese Fehlerbedingung wird in dem Ablaufdiagramm nicht gezeigt.)

Das Ablaufdiagramm veranschaulicht, wie eine Anwendung Transaktionen mit mehreren Objekten verwenden würde. Es zeigt, wo Entscheidungspunkte gesetzt werden können, um festzulegen, ob das Objekt, das gesendet wird, in die Transaktion passt oder ob eine neue Transaktion gestartet werden muss.

- Codebeispiel für API-Funktionen, mit denen Daten zum IBM Spectrum Protect-Speicher gesendet werden
  Dieses Beispiel veranschaulicht die Verwendung von API-Funktionen, mit denen Daten an IBM Spectrum Protect-Speicher gesendet werden. Der Aufruf **dsmSendObj** erscheint in einer Anweisung 'switch', sodass verschiedene Parameter abhängig davon, ob eine Sicherungs- oder Archivierungsoperation ausgeführt wird, aufgerufen werden können.

Dateigruppierung

Die IBM Spectrum Protect-API verfügt über ein Protokoll zum Gruppieren logischer Dateien, mit dem mehrere einzelne Objekte in Gruppen zusammengefasst werden. Sie können diese Gruppen auf dem Server als eine logische Gruppe referenzieren und verwalten. Bei einer logischen Gruppe müssen alle Gruppenmitglieder und der Gruppenleiter zu demselben Knoten und Dateibereich auf dem Server gehören.

Jede logische Gruppe hat einen Gruppenleiter. Wenn der Gruppenleiter gelöscht wird, wird auch die Gruppe gelöscht. Sie können kein Mitglied löschen, das zu einer Gruppe gehört. Der Verfall aller Mitglieder in einer Gruppe ist vom Gruppenleiter abhängig. Ist beispielsweise ein Mitglied für den Verfall markiert, verfällt es erst, wenn auch der Gruppenleiter verfällt. Ist ein Mitglied jedoch nicht für den Verfall markiert und der Gruppenleiter verfällt, verfallen auch alle Mitglieder.

Dateigruppen enthalten nur Sicherungsdaten und können keine Archivierungsdaten enthalten. Für Archivierungsobjekte kann über das Feld **Archivierungsbeschreibung** eine Art von Gruppierung erfolgen, sofern eine Anwendung dies erfordert.

Mit dem Aufruf **dsmGroupHandler** werden die Operationen gruppiert. Die Funktion **dsmGroupHandler** muss innerhalb einer Transaktion aufgerufen werden. Die meisten Fehlerbedingungen für Gruppen werden entweder in Aufrufen **dsmEndTxn** oder **dsmEndTxnEx** abgefangen.

Die `Ausgabe`struktur in **dsmEndTxnEx** enthält ein neues Feld, **groupLeaderObjId**. Dieses Feld enthält die Objekt-ID des Gruppenleiters, wenn eine Gruppe in dieser Transaktion geöffnet wurde. Eine Gruppe kann transaktionsübergreifend erstellt werden. Eine Gruppe wird erst festgeschrieben oder gespeichert, wenn auf dem Server eine Operation zum Schließen ausgeführt wird. Bei der Funktion **dsmGroupHandler** handelt es sich um eine Schnittstelle, die fünf verschiedene Operationen akzeptieren kann. Diese umfassen:

- DSM_GROUP_ACTION_OPEN
- DSM_GROUP_ACTION_CLOSE
- DSM_GROUP_ACTION_ADD
- DSM_GROUP_ACTION_ASSIGNTO
- DSM_GROUP_ACTION_REMOVE

In Tabelle 1 sind die Aktionen für den Funktionsaufruf **dsmGroupHandler** aufgelistet:

Tabelle 1. Funktion dsmGroupHandler

Aktion	Beschreibung
OPEN	Mit der Aktion OPEN wird eine Gruppe erstellt. Das nächste Objekt, das gesendet wird, wird der Gruppenleiter. Der Gruppenleiter darf keinen Inhalt haben. Alle Objekte nach dem ersten Objekt werden Mitglieder, die der Gruppe hinzugefügt werden. Um eine Gruppe zu erstellen, öffnen Sie eine Gruppe und übergeben Sie eine eindeutige Zeichenfolge, um die Gruppe zu identifizieren. Diese eindeutige Kennung ermöglicht es, mehrere Gruppen mit demselben Namen zu öffnen. Das nächste Objekt, das gesendet wird, nachdem die Gruppe geöffnet wurde, ist der Gruppenleiter. Alle anderen Objekte, die gesendet werden, sind Gruppenmitglieder.
CLOSE	Mit der Aktion CLOSE wird eine offene Gruppe festgeschrieben und gespeichert. Um die Gruppe zu schließen, übergeben Sie den Objektnamen und die eindeutige Zeichenfolge, die in der Operation zum Öffnen verwendet wird. Die Anwendung muss auf offene Gruppen prüfen und diese, falls erforderlich, schließen oder löschen. Eine Gruppe wird erst festgeschrieben oder gespeichert, wenn sie geschlossen wird. Eine Aktion CLOSE schlägt unter den folgenden Bedingungen fehl: • Die Gruppe, die Sie zu schließen versuchen, hat denselben Namen wie eine vorhandene offene Gruppe. • Zwischen der aktuellen geschlossenen Gruppe und der neuen Gruppe mit demselben Namen, die geschlossen werden soll, besteht eine Inkompatibilität in Bezug auf die Verwaltungsklasse. Führen Sie in diesem Fall die folgenden Schritte aus: 1. Fragen Sie die vorherige geschlossene Gruppe ab. 2. Wenn die Verwaltungsklasse der vorhandenen geschlossenen Gruppe nicht mit der Verwaltungsklasse übereinstimmt, die der aktuellen offenen Gruppe zugeordnet ist, geben Sie einen Funktionsaufruf **dsmUpdateObject** des Typs DSM_BACKUPD_MC aus. Mit diesem Befehl wird die vorhandene Gruppe mit der neuen Verwaltungsklasse aktualisiert. 3. Rufen Sie die Aktion CLOSE auf.
ADD	Mit der Aktion ADD wird ein Objekt einer Gruppe hinzugefügt. Alle Objekte, die nach der Aktion ADD gesendet werden, werden der Gruppe zugeordnet.
ASSIGNTO	Mit der Aktion ASSIGNTO wird dem Client die Zuordnung von Objekten, die auf dem Server vorhanden sind, zu der deklarierten Peergruppe ermöglicht. Mit dieser Transaktion wird die Peergruppenbeziehung definiert. Die Aktion ASSIGNTO entspricht mit Ausnahme der folgenden Punkte der Aktion ADD: • Die Aktion ADD findet Anwendung auf Objekte in unvollständigen Transaktionen. • Die Aktion ASSIGNTO findet Anwendung auf ein Objekt, das sich auf dem Server befindet.

Aktion	Beschreibung
REMOVE	Mit der Aktion REMOVE wird ein Mitglied oder eine Liste mit Mitgliedern aus einer Gruppe entfernt. Ein Gruppenleiter kann nicht aus einer Gruppe entfernt werden. Ein Gruppenmitglied muss entfernt werden, bevor es gelöscht werden kann.

Verwenden Sie die folgenden Abfragetypen für die Gruppenunterstützung:

- **qtBackupGroups**
- **qtOpenGroups**

Mit **qtBackupGroups** werden Gruppen abgefragt, die geschlossen sind, während mit **qtOpenGroups** Gruppen abgefragt werden, die offen sind. Für den Abfragepuffer für die neuen Typen gibt es die Felder **groupLeaderObjId** und **objType**. Die Abfrage wird abhängig von den Werten für diese beiden Felder unterschiedlich ausgeführt. Die folgende Tabelle zeigt einige Abfragemöglichkeiten:

Tabelle 2. Beispiele für Abfragen

groupLeaderObjId.hi	groupLeaderObjId.lo	objType	Ergebnis
0	0	NULL	Gibt eine Liste aller Gruppenleiter zurück.
grpLdrObjId.hi	grpLdrObjId.lo	0	Gibt eine Liste für alle Gruppenmitglieder zurück, die dem angegebenen Gruppenleiter (**grpLdrObjId**) zugeordnet sind.
grpLdrObjId.hi	grpLdrObjId.lo	objType	Gibt unter Verwendung von **BackQryRespEnhanced3** eine Liste für jedes Gruppenmitglied zurück, das dem angegebenen Gruppenleiter (**grpLdrObjId**) zugeordnet ist und einen übereinstimmenden Objekttyp (**objType**) hat.

Die Antwortstruktur (**qryRespBackupData**) von **dsmGetNextQObj** umfasst zwei Felder für die Gruppenunterstützung:

- **isGroupLeader**
- **isOpenGroup**

Bei diesen Feldern handelt es sich um boolesche Flags. Das folgende Beispiel zeigt das Erstellen der Gruppe, das Hinzufügen von Mitgliedern zu der Gruppe und das Schließen der Gruppe, um diese auf dem IBM Spectrum Protect-Server festzuschreiben.
Abbildung 1. Beispiel für Pseudocode zum Erstellen einer Gruppe

```
dsmBeginTxn
                dsmGroupHandler (PEER, OPEN, leader, uniqueId)
        dsmBeginSendObj
                dsmEndSendObj
dsmEndTxnEx (mit objId des Leiters)
Schleife für mehrere Transaktionen
{
        dsmBeginTxn
                                dsmGroupHandler (PEER, ADD, member, groupLeaderObjID)
                                Schleife für mehrere Objekte
                {
                        dsmBeginSendObj
                                                Schleife für Daten
                        {
                                dsmSendData
                        }
                        dsmEndSendObj
                }
        dsmEndTxn
}
dmBeginTxn
                dsmGroupHandler(CLOSE)
dsmEndTxn
```

Beispielcode können Sie dem Musterprogramm für eine Gruppe, dsmgrp.c, entnehmen, das sich im API-Verzeichnis sampsrc befindet.

Daten von einem Server empfangen

Anwendungsclients können Daten oder benannte Objekte und ihre zugehörigen Daten aus IBM Spectrum Protect-Speicher über die Zurückschreibungs- und Abruffunktionen empfangen. Die Zurückschreibungsfunktion greift auf Objekte zu, die zuvor gesichert wurden; die Abruffunktion greift auf Objekte zu, die zuvor archiviert wurden.

Einschränkung: Die API kann nur Objekte zurückschreiben und abrufen, die mithilfe von API-Aufrufen gesichert oder archiviert wurden.

Zurückschreibungs- und Abruffunktionen starten beide mit einer Abfrageoperation. Abhängig davon, ob die Daten ursprünglich gesichert oder archiviert wurden, gibt die Abfrage unterschiedliche Informationen zurück. Beispielsweise gibt eine Abfrage für Sicherungsobjekte Informationen zurück, die angeben, ob ein Objekt aktiv oder inaktiv ist, während eine Abfrage für Archivierungsobjekte Informationen wie Objektbeschreibungen zurückgibt. Beide Abfragen geben Objekt-IDs zurück, mit deren Hilfe das Objekt auf dem Server eindeutig identifiziert wird.

- Zurückschreibung oder Abruf von Teilobjekten
  Der Anwendungsclient kann nur einen Teil des Objekts empfangen. Das wird als Zurückschreibung von Teilobjekten bzw. Abruf von Teilobjekten bezeichnet.
- Daten zurückschreiben oder abrufen
  Nachdem eine Abfrage ausgeführt und eine Sitzung mit dem IBM Spectrum Protect-Server hergestellt wurde, können Sie eine Prozedur zum Zurückschreiben oder Abrufen von Daten ausführen.
- Beispielablaufdiagramme für Zurückschreibung und Abruf
  Mithilfe eines Zustandsdiagramms und eines Ablaufdiagramms kann die Ausführung von Zurückschreibungs- oder Abrufoperationen veranschaulicht werden.
- Codebeispiel für das Empfangen von Daten von einem Server
  Dieses Beispiel veranschaulicht die API-Funktion zum Abrufen von Daten aus IBM Spectrum Protect-Speicher

Zurückschreibung oder Abruf von Teilobjekten

Der Anwendungsclient kann nur einen Teil des Objekts empfangen. Das wird als Zurückschreibung von Teilobjekten bzw. Abruf von Teilobjekten bezeichnet.

Achtung: Eine Teilzurückschreibung oder ein Teilabruf komprimierter oder verschlüsselter Objekte führt zu unvorhersehbaren Ergebnissen.
Anmerkung: Wenn Sie Ihre Anwendung zur Verwendung einer Zurückschreibung oder eines Abruf von Teilobjekten codieren, können Sie Daten während des Sendevorgangs nicht komprimieren. Um dies durchzusetzen, setzen Sie *ObjAttr.objCompressed* auf *bTrue*.
Um eine Zurückschreibung oder einen Abruf von Teilobjekten durchzuführen, ordnen Sie die beiden folgenden Datenfelder jedem **GetList**-Eintrag des Objekts zu:

offset
: Die relative Byteadresse des Objekts, ab der Daten zurückgegeben werden sollen.

length
: Die Anzahl der zurückzugebenden Objektbyte.

Verwenden Sie DSM_MAX_PARTIAL_GET_OBJ, um die maximale Anzahl der Objekte zu bestimmen, die eine Zurückschreibung oder einen Abruf von Teilobjekten für eine bestimmte **dsmBeginGetData**-Liste durchführen können.

Die folgenden, im Aufruf **dsmBeginGetData** verwendeten Datenfelder legen fest, welcher Abschnitt des Objekts zurückgeschrieben oder abgerufen wird:

- Sind die relative Adresse und die Länge null, wird das gesamte Objekt aus dem IBM Spectrum Protect-Speicher zurückgeschrieben oder abgerufen.
- Ist die relative Adresse größer als null, die Länge aber null, wird das Objekt ab der relativen Adresse bis zum Ende zurückgeschrieben oder abgerufen.
- Ist die Länge größer als null, wird nur der Abschnitt des Objekts ab der relativen Adresse mit der angegebenen Länge zurückgeschrieben oder abgerufen.

Daten zurückschreiben oder abrufen

Nachdem eine Abfrage ausgeführt und eine Sitzung mit dem IBM Spectrum Protect-Server hergestellt wurde, können Sie eine Prozedur zum Zurückschreiben oder Abrufen von Daten ausführen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Daten zurückzuschreiben oder abzurufen:

1. Fragen Sie den IBM Spectrum Protect-Server nach Sicherungs- oder Archivierungsdaten ab.
2. Legen Sie die Objekte fest, die zurückgeschrieben oder vom Server abgerufen werden sollen.
3. Sortieren Sie die Objekte anhand des Felds Zurückschreibungsreihenfolge.
4. Senden Sie den Aufruf dsmBeginGetData mit der Liste der Objekte, auf die zugegriffen werden soll.
5. Senden Sie den Aufruf dsmGetObj, um jedes Objekt vom System abzurufen. Unter Umständen sind mehrere Aufrufe dsmGetData für jedes Objekt erforderlich, um alle zugehörigen Objektdaten abzurufen. Senden Sie den Aufruf dsmEndGetObj, nachdem alle Daten für ein Objekt abgerufen wurden.
6. Senden Sie den Aufruf dsmEndGetData, nachdem alle Daten für alle Objekte empfangen wurden, oder um die Empfangsoperation zu beenden.

- Server abfragen
  Fragen Sie vor dem Beginn einer Zurückschreibungs- oder Abrufoperationen zunächst den IBM Spectrum Protect-Server ab, um die Objekte zu bestimmen, die aus dem Speicher abgerufen werden können.
- Objekte nach Zurückschreibungsreihenfolge auswählen und sortieren
  Nachdem die Sicherungs- oder Archivabfrage ausgeführt wurde, muss der Anwendungsclient bestimmen, welche Objekte (sofern vorhanden) zurückgeschrieben oder abgerufen werden sollen.
- Aufruf dsmBeginGetData starten
  Nachdem Sie die zu empfangenden Objekte ausgewählt und sortiert haben, übergeben Sie sie für eine Zurückschreibungs- oder

Abrufoperation an IBM Spectrum Protect. Mit dem Aufruf **dsmBeginGetData** wird eine Zurückschreibungs- oder Abrufoperationen gestartet. Die Objekte werden in der von Ihnen angeforderten Reihenfolge an den Anwendungsclient zurückgegeben.

- Jedes zurückzuschreibende oder abzurufende Objekt empfangen
  Nachdem der Aufruf dsmBeginGetData gesendet wurde, können Sie eine Prozedur ausführen, um jedes Objekt, das vom Server gesendet wird, zu empfangen.

Server abfragen

Fragen Sie vor dem Beginn einer Zurückschreibungs- oder Abrufoperationen zunächst den IBM Spectrum Protect-Server ab, um die Objekte zu bestimmen, die aus dem Speicher abgerufen werden können.

Um die Abfrage zu senden, muss die Anwendung die Parameterlisten und Strukturen für den Aufruf dsmBeginQuery verwenden. Die Struktur muss den Dateibereich, den die Abfrage prüft, und Musterübereinstimmungseinträge für die Felder für den übergeordneten Namen und den untergeordneten Namen umfassen. Wenn die Sitzung mit dem Wert NULL für den Eignernamen initialisiert wurde, müssen Sie das Feld für den Eigner nicht angeben. Wenn die Sitzung jedoch mit einem expliziten Eignernamen initialisiert wurde, werden nur Objekte zurückgegeben, denen dieser Eignername zugeordnet ist.

Die zeitpunktgesteuerte Abfrage BackupQuery stellt eine Momentaufnahme des Systems zu einem bestimmten Zeitpunkt bereit. Indem Sie ein gültiges Datum angeben, können Sie alle Dateien abfragen, die bis zu diesem Zeitpunkt gesichert wurden. Selbst wenn ein Objekt über eine aktive Sicherung eines späteren Datums verfügt, überschreibt der Zeitpunktwert einen Objektstatus (objState), sodass die vorherige inaktive Kopie zurückgegeben wird. Weitere Informationen enthält das folgende Beispiel: pitDate.

Eine Abfrage gibt alle Informationen zurück, die mit dem Objekt gespeichert sind, sowie die Informationen in der folgenden Tabelle.

Tabelle 1. Zurückgegebene Informationen der Abfrage des Servers

Feld	Beschreibung
`copyId`	Die Werte `copyIdHi` und `copyIdLo` geben eine aus 8 Byte bestehende Zahl an, die dieses Objekt für diesen Knoten im IBM Spectrum Protect-Speicher eindeutig kennzeichnet. Fordern Sie mithilfe dieser ID ein bestimmtes Objekt im Speicher für die Zurückschreibungs- oder Abrufverarbeitung an.
`restoreOrderExt`	Der Wert für `restoreOrderExt` gibt an, wie Objekte aus IBM Spectrum Protect-Speicher auf möglichst effiziente Art und Weise empfangen werden können. Sortieren Sie die Objekte für die Zurückschreibung anhand dieses Werts, um sicherzustellen, dass Bänder nur einmal geladen und von vorne nach hinten gelesen werden.

Sie müssen einen Teil oder alle Abfrageinformationen für die spätere Verarbeitung aufbewahren. Sie müssen die Felder `copyId` und `restoreOrderExt` aufbewahren, da sie für die eigentliche Zurückschreibungsoperation benötigt werden. Sie müssen auch alle anderen Informationen aufbewahren, die erforderlich sind, um eine Datendatei zu öffnen oder ein Ziel zu identifizieren.

Rufen Sie dsmEndQuery auf, um die Abfrageoperation zu beenden.

Objekte nach Zurückschreibungsreihenfolge auswählen und sortieren

Nachdem die Sicherungs- oder Archivabfrage ausgeführt wurde, muss der Anwendungsclient bestimmen, welche Objekte (sofern vorhanden) zurückgeschrieben oder abgerufen werden sollen.

Anschließend sortieren Sie die Objekte in aufsteigender Reihenfolge. Diese Sortierung ist sehr wichtig für die Leistung der Zurückschreibungsoperation. Durch das Sortieren der Objekte anhand der Felder **restoreOrderExt** wird sichergestellt, dass die Daten vom Server in der effizientesten Reihenfolge gelesen werden.

Alle Daten auf Platte werden zuerst zurückgeschrieben, gefolgt von den Daten in Datenträgerklassen, die das Laden von Datenträgern (wie z. B. Bändern) erfordern. Über das Feld **restoreOrderExt** wird außerdem sichergestellt, dass beim Lesen der Daten auf Band die korrekte Verarbeitungsreihenfolge (vom Anfang des Bands bis zum Ende des Bands) eingehalten wird.

Eine korrekte Sortierung anhand des Felds **restoreOrderExt** bedeutet, dass keine doppelten Bandladevorgänge und kein unnötiges Zurückspulen von Bändern erfolgen.

Ein Wert ungleich null im Feld **restoreOrderExt**.top korreliert mit einer eindeutigen Einheit mit seriellem Zugriff auf dem IBM Spectrum Protect-Server. Da eine Einheit mit seriellem Zugriff nur jeweils von einer einzigen Sitzung bzw. einem einzigen Mountpunkt verwendet werden kann, muss die Anwendung - wenn sie mehrere Sitzungen verwendet - sicherstellen, dass Zurückspeicherungen mit demselben Wert für **restoreOrderExt**.top nicht gleichzeitig erfolgen. Andernfalls kann die erste Sitzung zwar auf die Objekte zugreifen, die anderen Sitzungen müssen jedoch warten, bis die erste Sitzung beendet ist und die Einheit verfügbar wird.

Das nachfolgende Beispiel zeigt die Sortierung von Objekten anhand von Feldern für die **Zurückschreibungsreihenfolge**.

Abbildung 1. Objekte anhand der Felder für die Zurückschreibungsreihenfolge sortieren

```
typedef struct {
dsStruct64_t      objId;
dsUint160_t      restoreOrderExt;
```

```
}  SortOrder;               /* für Sortierung verwendete Struktur */

=====================================================================
/* Der Code für die Sortierung beginnt hier */
dsmQueryType      queryType;
qryBackupData     queryBuffer;
DataBlk           qDataBlkArea;
qryRespBackupData qbDataArea;
dsInt16_t   rc;
dsBool_t  done = bFalse;
int i = 0;
int qry_item;
SortOrder  sortorder[100]; /* Sortierung kann zur Zeit nur für bis
                              100 Einträge erfolgen. Definieren Sie
                              die Array-Größe wie erforderlich.   */
/*--------------------------------------------------------------------+
| ANMERKUNG: Stellen Sie sicher, dass die korrekten
|  Initialisierungen für queryType, queryBuffer, qDataBlkAre
|  und qbDataArea ausgeführt wurden.
|
--------------------------------------------------------------------*/

   qDataBlkArea.bufferPtf = (char*) &qbDataArea;

   rc = dsmBeginQuery(dsmHandle, queryType, (void *) &queryBuffer);

   /*---------------------------------------+
   | Rückkehrcode von dsmBeginQuery überprüfen
   +---------------------------------------*/
   while (!done)
   {
      rc = dsmGetNextQObj(dsmHandle, &qDataBlkArea);
 if ((rc == DSM_RC_MORE_DATA) ||
          (rc == DSM_RC_FINISHED))
           &&( qDataBlkArea.numBytes))
      {
         /*****************************************/
         /* Übertrag. von restoreOrderExt und objId*/
         /*****************************************/
         sortorder[i].restoreOrderExt = qbDataArea.restoreOrderExt;
         sortorder[i].objId = qbDataArea.objId;

      } /*  if ((rc == DSM_RC_MORE_DATA) || (rc == DSM_RC_FINISHED)) */
         else
      {
          done = bTrue;
          /*****************************/
          /* Entspr. Aktion ausführen */
          /*****************************/
      }

      i++;
      qry_item++;

   } /* while (!done) */
   rc = dsmEndQuery(dsmHandle);
  /* Rückkehrcode überprüfen */
   /*****************************************************/
   /* Sortierung des Arrays mit qsort. Nach dem Aufruf  */
   /* wird sortorder anhand des Felds restoreOrderExt   */
   /* sortiert.                                         */
   /*****************************************************/

   qsort(sortorder, qry_item, sizeof(SortOrder), SortRestoreOrder);

 /*--------------------------------------------------------------------+
| ANMERKUNG: Stellen Sie sicher, dass sortierte Objekt-IDs
|       extrahiert werden und in jeder gewünschten Datenstruktur
|       gespeichert werden.
--------------------------------------------------------------------*/

/*--------------------------------------------------------------------+
| int SortRestoreOrder(SortOrder *a, SortOrder *b)
|
| Mit dieser Funktion werden Felder restoreOrder aus zwei
| Strukturen miteinander verglichen.
| if (a > b)
|   return(GREATERTHAN);
|| if (a < b)
|   return(LESSTHAN);
|| if (a == b)
```

```
|   return(EQUAL);
|+-------------------------------------------------------------------*/
int SortRestoreOrder(SortOrder *a, SortOrder *b)
{
    if (a->restoreOrderExt.top > b->restoreOrderExt.top)
       return(GREATERTHAN);
    else if (a->restoreOrderExt.top < b->restoreOrderExt.top)
       return(LESSTHAN);
    else if (a->restoreOrderExt.hi_hi > b->restoreOrderExt.hi_hi)
       return(GREATERTHAN);
    else if (a->restoreOrderExt.hi_hi < b->restoreOrderExt.hi_hi)
       return(LESSTHAN);
    else if (a->restoreOrderExt.hi_lo > b->restoreOrderExt.hi_lo)
       return(GREATERTHAN);
    else if (a->restoreOrderExt.hi_lo < b->restoreOrderExt.hi_lo)
       return(LESSTHAN);
     else if (a->restoreOrderExt.lo_hi > b->restoreOrderExt.lo_hi)
       return(GREATERTHAN);
    else if (a->restoreOrderExt.lo_hi < b->restoreOrderExt.lo_hi)
       return(LESSTHAN);
    else if (a->restoreOrderExt.lo_lo > b->restoreOrderExt.lo_lo)
       return(GREATERTHAN);
    else if (a->restoreOrderExt.lo_lo < b->restoreOrderExt.lo_lo)
       return(LESSTHAN);
       else
       return(EQUAL);
}
```

Aufruf dsmBeginGetData starten

Nachdem Sie die zu empfangenden Objekte ausgewählt und sortiert haben, übergeben Sie sie für eine Zurückschreibungs- oder Abrufoperation an IBM Spectrum Protect. Mit dem Aufruf **dsmBeginGetData** wird eine Zurückschreibungs- oder Abrufoperationen gestartet. Die Objekte werden in der von Ihnen angeforderten Reihenfolge an den Anwendungsclient zurückgegeben.

Geben Sie die Informationen für diese beiden Parameter in diesen Aufrufen an:

mountWait
: Über diesen Parameter wird dem Server mitgeteilt, ob der Anwendungsclient auf das Laden von Offlinedatenträgern wartet, um Daten für ein Objekt abzurufen, oder ob dieses Objekt während der Verarbeitung der Zurückschreibungs- oder Abrufoperationen übersprungen werden soll.

dsmGetObjListP
: Dieser Parameter ist eine Datenstruktur, die das Feld **objId** enthält, das eine Liste aller Objekt-IDs ist, die zurückgeschrieben oder abgerufen werden. Jedes Feld **objId** ist einer Struktur **partialObjData** zugeordnet, die beschreibt, ob das gesamte über **objId** angegebene Objekt oder nur ein bestimmter Teil des Objekts abgerufen wird.

  Jedes Feld **objId** hat eine Länge von acht Byte, sodass eine einzige Zurückschreibungs- oder Abrufanforderung tausende von Objekten enthalten kann. Die Anzahl Objekte, die in einem einzigen Aufruf angefordert werden können, ist auf DSM_MAX_GET_OBJ oder DSM_MAX_PARTIAL_GET_OBJ beschränkt.

Jedes zurückzuschreibende oder abzurufende Objekt empfangen

Nachdem der Aufruf dsmBeginGetData gesendet wurde, können Sie eine Prozedur ausführen, um jedes Objekt, das vom Server gesendet wird, zu empfangen.

Informationen zu diesem Vorgang

Der Rückkehrcode DSM_RC_MORE_DATA gibt an, dass ein Puffer zurückgegeben wurde und Sie dsmGetData erneut aufrufen müssen. Überprüfen Sie DataBlk.numBytes auf die tatsächliche Anzahl zurückgegebener Byte.

Wenn Sie alle Daten für ein Objekt abrufen, müssen Sie einen Aufruf dsmEndGetObj senden. Wenn weitere Objekte empfangen werden sollen, senden Sie dsmGetObj erneut.

Wenn Sie den Prozess stoppen möchten, um beispielsweise alle verbleibenden Daten im Zurückschreibungsdatenstrom für alle noch nicht empfangenen Objekte zu löschen, senden Sie den Aufruf dsmEndGetData. Dieser Aufruf führt für die Daten, die vom Server an den Client gesendet werden, eine Flushoperation aus. Die Ausführung mithilfe dieser Methode kann jedoch einige Zeit in Anspruch nehmen. Wenn Sie eine Zurückschreibungsoperation beenden möchten, schließen Sie die Sitzung mithilfe von dsmTerminate.

Vorgehensweise

1. Senden Sie den Aufruf dsmGetObj, um das Objekt, das Sie aus dem Datenstrom angefordert haben, zu identifizieren und den ersten Datenblock, der dem Objekt zugeordnet ist, abzurufen.
2. Senden Sie, falls erforderlich, weitere Aufrufe dsmGetData, um die verbleibenden Objektdaten abzurufen.

Beispielablaufdiagramme für Zurückschreibung und Abruf

Mithilfe eines Zustandsdiagramms und eines Ablaufdiagramms kann die Ausführung von Zurückschreibungs- oder Abrufoperationen veranschaulicht werden.

Der Pfeil, der von "In 'Objekt abrufen'" auf **dsmEndGetData** zeigt, gibt an, dass ein Aufruf **dsmEndGetData** nach einem Aufruf **dsmGetObj** oder dsmGetData gesendet werden kann. Dies ist möglicherweise erforderlich, wenn während des Abrufs eines Objekts aus IBM Spectrum Protect-Speicher eine Fehlerbedingung aufgetreten ist und die Operation gestoppt werden soll. Rufen Sie jedoch unter normalen Umständen zunächst **dsmEndGetObj** auf.

Abbildung 1. Zustandsdiagramm für Zurückschreibungs- und Abrufoperationen

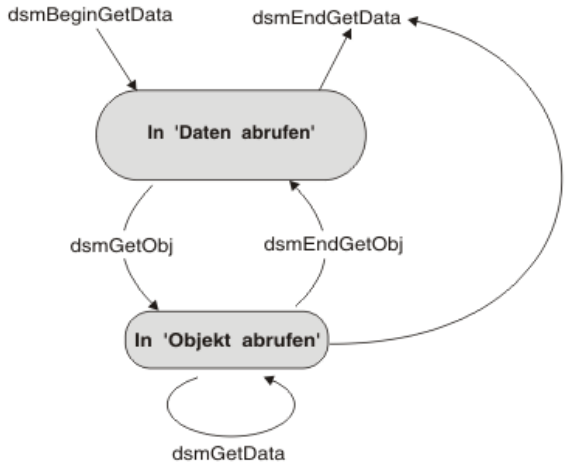
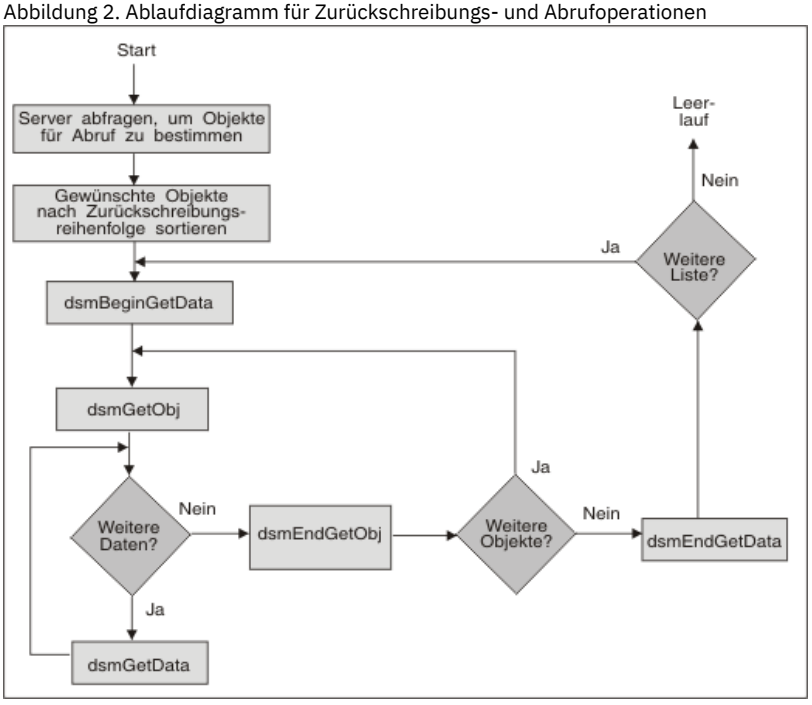


Abbildung 2 zeigt das Ablaufdiagramm für die Ausführung von Zurückschreibungs- oder Abrufoperationen.

Abbildung 2. Ablaufdiagramm für Zurückschreibungs- und Abrufoperationen



Codebeispiel für das Empfangen von Daten von einem Server

Dieses Beispiel veranschaulicht die API-Funktion zum Abrufen von Daten aus IBM Spectrum Protect-Speicher

Der Funktionsaufruf **dsmBeginGetData** erscheint in einer Anweisung 'switch', sodass verschiedene Parameter abhängig davon, ob eine Zurückschreibungs- oder Abrufoperationen ausgeführt wird, aufgerufen werden können. Der Funktionsaufruf **dsmGetData** erfolgt innerhalb einer Schleife, die wiederholt Daten vom Server abruft, bis ein Flag gesetzt wird, das der Programmausführung das Verlassen der Schleife ermöglicht.

Abbildung 1. Beispiel für das Empfangen von Daten von einem Server

```
/* Aufruf dsmBeginQuery und Erstellen einer verketteten Liste mit     */
/* zurückzuschreibenden Objekten.                                     */
/* Verarbeitung dieser Liste zum Erstellen der korrekten Liste für    */
/* die Aufrufe GetData.                                               */
/* Definieren der Struktur getList zum Verweisen auf diese Liste.     */
/* Dieses Beispiel dient zur Ausführung eines Abrufs von Teilobjekten.*/
/* Um nur vollständige Objekte abzurufen, muss Folgendes definiert    */
/* werden:                                                            */
/*       getList.stVersion = dsmGetListVersion;                       */
/*       getList.partialObjData = NULL;                               */
dsmGetList getList;
getList.stVersion = dsmGetListPORVersion;   /* Strukturversion        */
getList.numObjId  = items;               /* Anzahl Einträge in Liste  */
getList.objId     = (ObjID *)rest_ibuff;
                                    /* Liste der Objekt-IDs für Zu-
                                       rückschreibung                 */
getList.partialObjData = (PartialObjData *) part_ibuff;
                                     /* Liste der Teilobjektdaten    */
switch(get_type)
{
   case (Restore_Get) :
     rc = dsmBeginGetData(dsmHandle,bFalse,gtBackup,&getList);
     break;
   case (Retrieve_Get) :
     rc = dsmBeginGetData(dsmHandle,bFalse,gtArchive,&getList);
     break;
   default : ;
}
if (rc)
{
   printf("*** dsmBeginGetData fehlgeschlagen: ");
   rcApiOut(dsmHandle, rc);
   return rc;
}
/* Jedes Objekt aus der Liste abrufen und überprüfen, ob es auf dem */
/* Server vorhanden ist. Ist dies der Fall, Strukturen mit Objekt-  */
/* attributen für Datenprüfungen initialisieren. Anschließend       */
/* dsmGetObj aufrufen.                                                 */
 rc = dsmGetObj(dsmHandle,objId,&dataBlk);
done = bFalse;
while(!done)
{
   if (   (rc == DSM_RC_MORE_DATA)
       || (rc == DSM_RC_FINISHED))
   {
      if (rc == DSM_RC_MORE_DATA)
      {
         dataBlk.numBytes = 0;
         rc = dsmGetData(dsmHandle,&dataBlk);
      }
         else
         done = bTrue;
   }
      else
   {
      printf("*** dsmGetObj oder dsmGetData fehlgeschlagen: ");
      rcApiOut(dsmHandle, rc);
      done = bTrue;
   }
} /* while */
rc = dsmEndGetObj(dsmHandle);
/* check rc from dsmEndGetObj */
/* check rc from dsmEndGetData */
rc = dsmEndGetData(dsmHandle);
return 0;
```

Objekte auf dem Server aktualisieren und löschen

Ihre API-Anwendungen können Objekte, die archiviert oder gesichert wurden, mithilfe des Funktionsaufrufs **dsmUpdateObj** oder **dsmUpdateObjEx** aktualisieren. Verwenden Sie beide Aufrufe nur im Sitzungsstatus und aktualisieren Sie jeweils nur ein einziges Objekt. Verwenden Sie **dsmUpdateObjEx**, um mehrere Archivierungsobjekte zu aktualisieren, die denselben Namen enthalten.

Um ein Archivierungsobjekt auszuwählen, setzen Sie den Funktionsaufruf **dsmSendType** auf **stArchive**.

- Mit **dsmUpdateObj** wird nur das letzte Archivierungsobjekt mit dem zugeordneten Namen aktualisiert.
- Mit **dsmUpdateObjEx** kann jedes archivierte Objekt durch Angabe der korrekten Objekt-ID aktualisiert werden.

Bei einem archivierten Objekt kann die Anwendung die folgenden Felder aktualisieren:

- Beschreibung

- Objektinformationen
- Eigner

Um ein Sicherungsobjekt auszuwählen, setzen Sie **dsmSendType** auf **stBackup**. Bei gesicherten Objekten wird nur die aktive Kopie aktualisiert.

Bei einem gesicherten Objekt kann die Anwendung die folgenden Felder aktualisieren:

- Verwaltungsklasse
- Objektinformationen
- Eigner

- Objekte vom Server löschen
  API-Anwendungen können Aufrufe ausführen, um entweder Objekte, die archiviert wurden, zu löschen oder um Objekte, die gesichert wurden, zu inaktivieren. Das Löschen archivierter Objekte ist von der Knotenberechtigung abhängig, die bei der Registrierung des Knotens durch den Administrator erteilt wurde. Administratoren können festlegen, dass Knoten Archivierungsobjekte löschen können.

Ereignisse protokollieren

Eine API-Anwendung kann Ereignisnachrichten an zentralen Positionen protokollieren. Die Anwendung kann die Protokollierung an den IBM Spectrum Protect-Server und/oder die lokale Maschine übertragen. Der Funktionsaufruf dsmLogEventEx wird in einer Sitzung ausgeführt. Um Nachrichten anzuzeigen, die auf dem Server protokolliert sind, verwenden Sie den Befehl query actlog über den Verwaltungsclient.

Verwenden Sie die IBM Spectrum Protect-Clientoption errorlogretention, um die Clientfehlerprotokolldatei zu bereinigen, wenn die Anwendung zahlreiche Clientnachrichten in das Clientprotokoll schreibt (dsmLogType ist entweder logLocal oder logBoth).

Weitere Informationen zu IBM Spectrum Protect-Protokollen finden Sie in der Dokumentation für den IBM Spectrum Protect-Server.

Zustandsdiagrammzusammenfassung für die IBM Spectrum Protect-API

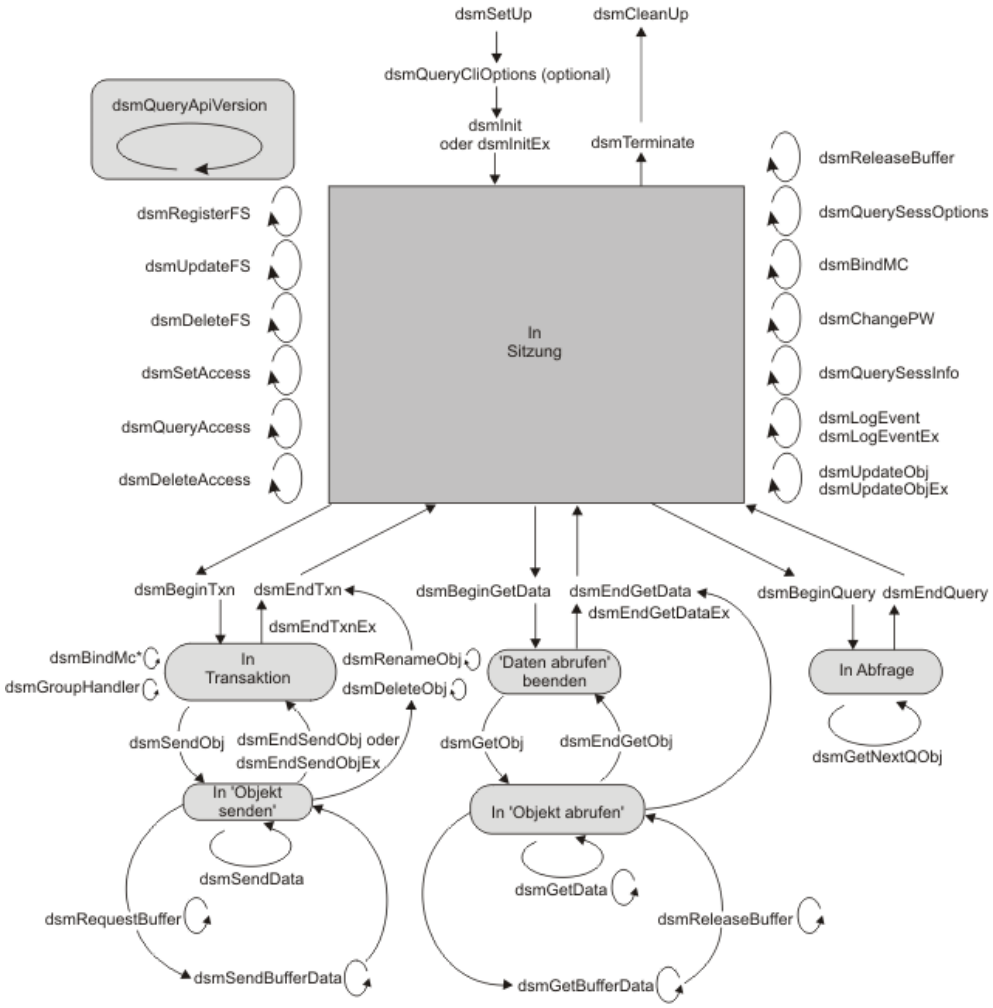
Überprüfen Sie alle Überlegungen beim Erstellen Ihrer eigenen Anwendung mit der IBM Spectrum Protect-API mithilfe dieses Zustandsdiagramms mit der Zusammenfassung einer vollständigen Anwendung.

Abbildung 1 zeigt das Zustandsdiagramm für die API. Sie enthält alle zuvor angezeigten Zustandsdiagramme sowie verschiedene andere Aufrufe, die zuvor nicht angezeigt wurden.

Wichtige Punkte in diesem Diagramm umfassen:

- **dsmQueryApiVersionEx** kann jederzeit aufgerufen werden. Dieser Funktion ist kein Zustand zugeordnet. Ein Beispiel finden Sie in Abbildung 1.
- Rufen Sie **dsmQueryCliOptions** nur vor einem Aufruf **dsmInitEx** auf.
- Verwalten Sie Dateibereiche mithilfe von **dsmRegisterFS**, **dsmUpdateFS** und **dsmDeleteFS**. Diese Aufrufe erfolgen innerhalb eines inaktiven Sitzungsstatus. Fragen Sie Dateibereiche mithilfe des Aufrufs **dsmBeginQuery** ab. Weitere Informationen zu Dateibereichsaufrufen finden Sie in Dateibereiche verwalten.
- Senden Sie den Aufruf **dsmBindMC** innerhalb eines inaktiven Sitzungsstatus oder innerhalb eines Transaktionsstatus 'Objekt senden'. Siehe das Beispiel in Abbildung 1.
- Senden Sie den Aufruf **dsmChangePW** innerhalb eines inaktiven Sitzungsstatus.
  Anmerkung: Wenn der Aufruf **dsmInitEx** einen Rückkehrcode zurückgibt, der angibt, dass ein Kennwort abgelaufen ist, muss der Aufruf **dsmChangePW** vor dem Start einer gültigen Sitzung erfolgen. Abbildung 3 zeigt ein Beispiel für die Verwendung von **dsmChangePW**.
- Gibt ein Aufruf einen Fehler zurück, ändert sich der Zustand nicht. Wenn beispielsweise **dsmGetObj** einen Fehler zurückgibt, lautet der Zustand weiterhin "In 'Daten abrufen'" und ein Aufruf **dsmEndGetObj** stellt einen Fehler in der Aufruffolge dar.

Abbildung 1. Zusammenfassungszustandsdiagramm für die API



* Kann innerhalb oder außerhalb einer Transaktion erfolgen

Erläuterungen zur Interoperabilität

Bei der API unterscheidet man zwei Typen von Interoperabilität: Interoperabilität zwischen dem Client für Sichern/Archivieren und den API-Anwendungen sowie Interoperabilität zwischen verschiedenen Betriebssystemen.

- Interoperabilität des Clients für Sichern/Archivieren
  Die Befehlszeile für Sichern/Archivieren kann auf API-Objekte zugreifen, um begrenzte Interoperabilität zur Verfügung zu stellen. Das Anzeigen von API-Objekten und der Zugriff auf API-Objekte ist nur über den Befehlszeilenclient für Sichern/Archivieren und nicht über eine der grafischen Benutzerschnittstellen möglich. Der Befehlszeilenclient für Sichern/Archivieren kann nur den Dateiinhalt uns sonst nichts zurückschreiben. Daher sollten Sie ihn nur für eine Wiederherstellungsoperation verwenden.
- Interoperabilität zwischen Betriebssystemen
  Die IBM Spectrum Protect-API unterstützt die plattformübergreifende Interoperabilität. Anwendungen auf einem UNIX- oder Linux-System können Operationen für Dateibereiche und Objekte ausführen, die von einem Windows-System gesichert werden. Analog kann ein Windows-System Operationen für Dateibereiche und Objekte ausführen, die auf einem UNIX- oder Linux-System gesichert werden.
- Mehrere Knoten mit Clientknoten-Proxy-Unterstützung sichern
  Sicherungen mehrerer Knoten, die Speicher gemeinsam nutzen, können auf dem IBM Spectrum Protect-Server auf einen gemeinsamen Zielknotennamen konsolidiert werden. Diese Methode ist hilfreich, wenn sich das System, das die Sicherung ausführt, im Laufe der Zeit ändern kann, beispielsweise im Fall eines Clusters. Sie können auch die Option asnodename zum Zurückschreiben von Daten von einem anderen System verwenden als demjenigen, das die Sicherung ausgeführt hat.

Interoperabilität des Clients für Sichern/Archivieren

Die Befehlszeile für Sichern/Archivieren kann auf API-Objekte zugreifen, um begrenzte Interoperabilität zur Verfügung zu stellen. Das Anzeigen von API-Objekten und der Zugriff auf API-Objekte ist nur über den Befehlszeilenclient für Sichern/Archivieren und nicht über eine der grafischen Benutzerschnittstellen möglich. Der Befehlszeilenclient für Sichern/Archivieren kann nur den Dateiinhalt uns sonst nichts zurückschreiben. Daher sollten Sie ihn nur für eine Wiederherstellungsoperation verwenden.

Die folgenden Befehlszeilenaktionen sind verfügbar:

- Delete archive
- Delete filespace
- Query
- Restore
- Retrieve
- Set access

Die Pfadinformationen sind tatsächliche Verzeichnisse für Objekte des Clients für Sichern/Archivieren. Die Pfadinformationen der API-Objekte dagegen haben möglicherweise keine Beziehung zu vorhandenen Verzeichnissen, der Pfad kann völlig frei erfunden sein. Die Interoperabilität ändert diesen Aspekt dieser Objekttypen nicht. Um dieses Feature erfolgreich einsetzen zu können, halten Sie die Bedingungen und Konventionen ein.

Anmerkungen:

1. Es gibt keine Interoperabilität zwischen dem Client für Sichern/Archivieren und API-Objekten, die auf einem Aufbewahrungsschutzserver gespeichert sind.
2. Sie können nicht mit den grafischen Benutzerschnittstellen des Clients für Sichern/Archivieren auf Dateien zugreifen, die mit dem API-Client gespeichert wurden. Sie können auf diese Dateien nur über die Befehlszeile zugreifen.

- Benennung von API-Objekten
  Erstellen Sie eine konsistente Namenskonvention für API-Objektnamen. Die Namenskonvention muss den Dateibereichsnamen, das übergeordnete Qualifikationsmerkmal und das untergeordnete Qualifikationsmerkmal berücksichtigen. Der Dateibereichsname und die übergeordneten Qualifikationsmerkmale können sich auf tatsächliche Verzeichnisnamen beziehen. Jeder Objektname kann aus mehreren Verzeichnisnamen bestehen, die für das untergeordnete Qualifikationsmerkmal gelten.
- Für die API verwendbare Befehle des Clients für Sichern/Archivieren
  Sie können eine Untergruppe der Befehle des Clients für Sichern/Archivieren in einer Anwendung verwenden. Sie können beispielsweise Objekte, deren Eigner andere Benutzer sind, auf demselben Knoten oder auf einem anderen Knoten anzeigen und verwalten.

Benennung von API-Objekten

Erstellen Sie eine konsistente Namenskonvention für API-Objektnamen. Die Namenskonvention muss den Dateibereichsnamen, das übergeordnete Qualifikationsmerkmal und das untergeordnete Qualifikationsmerkmal berücksichtigen. Der Dateibereichsname und die übergeordneten Qualifikationsmerkmale können sich auf tatsächliche Verzeichnisnamen beziehen. Jeder Objektname kann aus mehreren Verzeichnisnamen bestehen, die für das untergeordnete Qualifikationsmerkmal gelten.

Am einfachsten ist es, als untergeordnetes Qualifikationsmerkmal den Namen des Objekts ohne Verzeichnisinformationen als Präfix zu verwenden. Weitere Informationen finden Sie in Objektnamen und -IDs.

Dateibereichsnamen müssen vollständig qualifiziert sein, wenn von der API oder der Befehlszeile für Sichern/Archivieren auf sie Bezug genommen wird. Registrieren Sie beispielsweise unter einem Betriebssystem UNIX oder Linux die folgenden Dateibereiche:

- `/a`
- `/a/b`

Wenn Sie auf `/a` Bezug nehmen, werden Objekte angezeigt, die sich nur auf Dateibereich `/a` beziehen. Wenn Objekte angezeigt werden sollen, die sich auf `/a/b` beziehen, müssen Sie `/a/b` als Dateibereichsnamen angeben.

Wenn Sie, nachdem Sie beide Dateibereiche registriert haben, Objekt `b` in Dateibereich `/a` sichern, werden bei einer Abfrage für `/a/b` weiterhin Objekte angezeigt, die sich nur auf Dateibereich `/a/b` beziehen.

Eine Ausnahme von dieser Einschränkung sind Dateibereichsreferenzen, wenn Sie versuchen, Dateibereiche mit der API abzufragen oder zu löschen. In beiden Fällen müssen die Dateibereichsnamen nicht vollständig qualifiziert sein, wenn ein Platzhalterzeichen verwendet wird. Beispielsweise bezieht sich `/a*` sowohl auf `/a` als auch auf `/a/b`.
Tipp: Wenn Interoperabilität für Sie wichtig ist, geben Sie keine Dateibereichsnamen an, die sich überschneiden.

Schließen Sie bei Windows-Systemen die Dateibereichsnamen für API-Objekte in geschweifte Klammern `{ }` ein, wenn der Zugriff auf die Objekte über die Befehlszeilenschnittstelle für Sichern/Archivieren erfolgt. Windows-Betriebssysteme setzen Dateibereichsnamen automatisch in Großbuchstaben um, wenn die Namen registriert werden oder auf sie Bezug genommen wird. Diese automatische Funktion gibt es jedoch nicht für die restliche Objektnamensspezifikation. Wird vollständige Interoperabilität gewünscht, geben Sie beim Sichern von API-Objekten das übergeordnete Qualifikationsmerkmal und das untergeordnete Qualifikationsmerkmal in der Anwendung in Großbuchstaben an. Wenn Ihre Anwendung übergeordnete Qualifikationsmerkmale (Verzeichnisnamen) und untergeordnete Qualifikationsmerkmale (Dateinamen) vor dem Senden von Objekten an den Server nicht in Großbuchstaben umsetzt, können Sie über den Client für Sichern/Archivieren nicht direkt über den Namen auf die Objekte zugreifen.

Wenn beispielsweise ein Objekt auf dem Server als {"Dateibereichsname"}\TEST\MYDIRNAME\file.txt gespeichert ist, können Sie das Objekt file.txt nicht direkt zurückschreiben oder abfragen, weil Ihre Anwendung den Dateinamen nicht in Großbuchstaben umgesetzt hat, bevor die Datei auf den Server kopiert wurde. Die einzige Möglichkeit, mit diesen Objekten zu arbeiten, besteht in der Verwendung von Platzhalterzeichen. Beispielsweise muss ein Benutzer des Clients für Sichern/Archivieren bei einer Abfrage von \TEST\MYDIRNAME\file.txt Platzhalterzeichen für alle Teile des Objektnamens verwenden, die nicht in Großbuchstaben umgesetzt wurden, bevor sie an den Server gesendet wurden. Der folgende Befehl muss verwendet werden, um diese Datei file.txt abzufragen:

```
dsmc query backup {"Dateibereichsname"}\TEST\MYDIRNAME\*
```

Wenn auch noch andere Qualifikationsmerkmale in Kleinschreibung gespeichert wurden, müssen auch sie unter Verwendung von Platzhalterzeichen abgefragt werden. Verwenden Sie beispielsweise zum Abfragen eines Objekts, das als {"Dateibereichsname"}\TEST\mydirname\file.txt gespeichert wurde, den folgenden Befehl:

```
dsmc query backup {"Dateibereichsname"}\TEST\*\*
```

Die nachfolgenden Beispiele veranschaulichen diese Konzepte. Weder in Windows- noch in UNIX- oder Linux-Umgebungen müssen Sie das vollständige übergeordnete oder untergeordnete Qualifikationsmerkmal angeben. Wenn Sie nicht das vollständige Qualifikationsmerkmal angeben, müssen Sie allerdings das Platzhalterzeichen verwenden.

Plattform	**Beispiel**
Windows	Um alle gesicherten Dateien im Dateibereich `MYFS` abzufragen, geben Sie die folgende Zeichenfolge ein: `dsmc q ba "{MYFS}\*\*"` Sie müssen für jedes übergeordnete und untergeordnete Qualifikationsmerkmal mindestens 1 Stern (*) verwenden.
UNIX oder Linux	Um alle gesicherten Dateien im Dateibereich `/A` abzufragen, geben Sie die folgende Zeichenfolge ein: `dsmc q ba "/A/*/*"` Sie müssen für jedes übergeordnete und untergeordnete Qualifikationsmerkmal mindestens 1 Stern (*) verwenden.

Für die API verwendbare Befehle des Clients für Sichern/Archivieren

Sie können eine Untergruppe der Befehle des Clients für Sichern/Archivieren in einer Anwendung verwenden. Sie können beispielsweise Objekte, deren Eigner andere Benutzer sind, auf demselben Knoten oder auf einem anderen Knoten anzeigen und verwalten.

Gehen Sie wie folgt vor, um Objekte, deren Eigner andere Benutzer sind, auf demselben Knoten oder auf einem anderen Knoten anzuzeigen und zu verwalten:

1. Erteilen Sie Zugriff mit dem Befehl set access.
2. Geben Sie den Eigner und den Knoten an. Verwenden Sie die Optionen *fromowner* und *fromnode* über die Befehlszeile für Sichern/Archivieren, um den Eigner und den Knoten anzugeben. Beispiel:

   ```
   dsmc q ba "/A/*/*" -fromowner=anderer_Eigner -fromnode=anderer_Knoten
   ```

Tabelle 1 enthält die Befehle, die Sie für API-Objekte verwenden können.

Tabelle 1. Für API-Objekte verwendbare Befehle des Clients für Sichern/Archivieren

Befehl	**Beschreibung**
Delete Archive	Archivierte Dateien, deren Eigner der aktuelle Benutzer ist, können gelöscht werden. Die Einstellungen des Befehls set access haben keinen Einfluss auf diesen Befehl.
Delete Filespace	Der Befehl delete filespace wirkt sich auf API-Objekte aus.
Query	Über die Befehlszeile für Sichern/Archivieren können Sie gesicherte und archivierte API-Objekte und Objekte, deren Eigner andere Benutzer sind oder die sich auf anderen Knoten befinden, abfragen. Informationen zum Abfragen von API-Objekten finden Sie in Benennung von API-Objekten. Verwenden Sie die vorhandene Option *–fromowner*, um Objekte abzufragen, deren Eigner ein anderer Benutzer ist und für die die set access-Berechtigung erteilt wurde. Verwenden Sie die vorhandene Option *–fromnode*, um Objekte abzufragen, die sich auf einem anderen Knoten befinden und für die die set access-Berechtigung erteilt wurde. Weitere Informationen finden Sie in dsmInitEx.

Befehl	Beschreibung
Restore Retrieve	Anmerkung: Verwenden Sie diese Befehle nur in Ausnahmesituationen. Mit dem anwendungsverwalteten Schlüssel verschlüsselte API-Objekte können zurückgeschrieben oder abgerufen werden, wenn der Verschlüsselungsschlüssel bekannt oder in der Kennwortdatei bzw. im Registry gespeichert ist. Mit der transparenten Verschlüsselung verschlüsselte API-Objekte können nicht mit dem Client für Sichern/Archivieren zurückgeschrieben oder abgerufen werden. Diese Befehle geben Daten als Bitdateien zurück, die mit Standarddateiattributen erstellt werden. Sie können API-Objekte, deren Eigner andere Benutzer sind oder die von einem anderen Knoten stammen, zurückschreiben oder abrufen. Der Befehl set access legt fest, welche Objekte in Frage kommen.
Set Access	Mit dem Befehl set access können Benutzer API-Objekte verwalten, deren Eigner ein anderer Benutzer ist oder die von einem anderen Knoten stammen.

Interoperabilität zwischen Betriebssystemen

Die IBM Spectrum Protect-API unterstützt die plattformübergreifende Interoperabilität. Anwendungen auf einem UNIX- oder Linux-System können Operationen für Dateibereiche und Objekte ausführen, die von einem Windows-System gesichert werden. Analog kann ein Windows-System Operationen für Dateibereiche und Objekte ausführen, die auf einem UNIX- oder Linux-System gesichert werden.

Informationen zu diesem Vorgang

Standardmäßig sind die Namen von Objekten aus einem UNIX-System mit den Namen von Objekten aus anderen UNIX-Systemen kompatibel. Standardmäßig sind die Namen von Objekten aus Windows-Systemen nicht mit den Namen von Objekten aus UNIX-Systemen kompatibel. Die Benennung von Objekten in IBM Spectrum Protect-Dateibereichen wird durch mehrere Parameter gesteuert. Wenn Sie eine Anwendung ordnungsgemäß konfigurieren, können die Namen von Objekten verwendet werden, die sowohl auf Windows-Systemen als auch auf UNIX-Systemen ausgeführt werden. Verwenden Sie für die Sicherung und Zurückschreibung von Objekten dieselben Parameter.
Einschränkung: Eine Windows-Anwendung, die Unicode verwendet, erstellt einen Dateibereich, der nicht mit Anwendungen kompatibel ist, die auf UNIX-Systemen ausgeführt werden.

Vorgehensweise

Führen Sie die folgenden Konfigurationstasks aus, um Interoperabilität zu erzielen:

1. Erstellen Sie eine konsistente Namenskonvention. Wählen Sie ein Zeichen für den Verzeichnisbegrenzer aus, zum Beispiel einen normalen Schrägstrich (/) oder einen umgekehrten Schrägstrich (\). Das als Verzeichnisbegrenzer verwendete Zeichen muss vor dem Dateibereichsnamen, vor dem übergeordneten Qualifikationsmerkmal bzw. vor dem untergeordneten Qualifikationsmerkmal stehen.
2. Wenn Sie dsmInitEx aufrufen, setzen Sie den Wert für das Feld dirDelimiter auf das als Verzeichnisbegrenzer zu verwendende Zeichen und setzen Sie bCrossPlatform auf bTrue.
3. Setzen Sie das Flag useUnicode auf bFalse, wenn Sie die IBM Spectrum Protect-Schnittstelle verwenden. Unicode-Dateinamen sind nicht mit Nicht-Unicode-Dateinamen kompatibel.

Mehrere Knoten mit Clientknoten-Proxy-Unterstützung sichern

Sicherungen mehrerer Knoten, die Speicher gemeinsam nutzen, können auf dem IBM Spectrum Protect-Server auf einen gemeinsamen Zielknotennamen konsolidiert werden. Diese Methode ist hilfreich, wenn sich das System, das die Sicherung ausführt, im Laufe der Zeit ändern kann, beispielsweise im Fall eines Clusters. Sie können auch die Option asnodename zum Zurückschreiben von Daten von einem anderen System verwenden als demjenigen, das die Sicherung ausgeführt hat.

Informationen zu diesem Vorgang

Verwenden Sie die Option asnodename in der dsmInitEx-Optionszeichenfolge, um Daten unter dem Zielknotennamen auf dem IBM Spectrum Protect-Server zu sichern, zu archivieren, zurückzuschreiben, abzurufen, abzufragen oder zu löschen. Sie können die Option asnodename auch in der Datei dsm.opt oder dsm.sys angeben.

Einschränkung: Verwenden Sie Zielknoten nicht als traditionelle Knoten, besonders dann nicht, wenn Sie Ihre Dateien verschlüsseln, bevor Sie auf dem Server sichern.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um diese Option zu aktivieren:

1. Installieren Sie den API-Client auf allen Knoten in einer gemeinsam genutzten Datenumgebung.
2. Falls noch nicht geschehen, registrieren Sie jeden Knoten beim IBM Spectrum Protect-Server. Registrieren Sie den gemeinsamen Zielknotennamen, der von allen in Ihrer gemeinsam genutzten Datenumgebung verwendeten Agentenknoten gemeinsam genutzt werden soll.

3. Registrieren Sie jeden Agentenknoten in der gemeinsam genutzten Datenumgebung beim Server. Der Agentenknotenname wird für die Authentifizierung verwendet. Es werden keine Daten unter Verwendung des Agentenknotennamens gespeichert, wenn die Option asnodename verwendet wird.
4. Bitten Sie Ihren Administrator, allen Knoten in der gemeinsam genutzten Umgebung mit dem Befehl grant proxynode Proxy-Berechtigung zu erteilen, damit sie auf den Zielknotennamen auf dem IBM Spectrum Protect-Server zugreifen können.
5. Verwenden Sie den Verwaltungsclientbefehl query proxynode, um die Clientknoten anzuzeigen, die die Berechtigung zum Ausführen von Clientoperationen für einen anderen Knoten haben. Diese Berechtigung wird mit dem Befehl grant proxynode erteilt. Oder verwenden Sie den Befehl dsmQuery mit dem Abfragetyp qtProxyNodeAuth, um die Knoten anzuzeigen, an die der vorliegende Knoten weiterleiten kann.
6. Wenn die Anwendung mit Benutzerverschlüsselung für Daten arbeitet (nicht TSMENCRKEY), müssen Sie sicherstellen, dass alle Knoten denselben Verschlüsselungsschlüssel verwenden. Sie müssen denselben Verschlüsselungsschlüssel für alle Dateien verwenden, die in der Umgebung mit gemeinsam genutzten Knoten gesichert werden.

Zugehörige Tasks:
Daten mit Proxy-Unterstützung für Clientknoten sichern (UNIX- und Linux-Systeme)
Daten mit Proxy-Unterstützung für Clientknoten sichern (Windows-Systeme)

Verwendung der API mit Unicode

Die IBM Spectrum Protect-API unterstützt Unicode UCS-2, eine Doppelbyte-Codepage mit fester Länge, die Codepunkte für alle bekannten Codepages, wie z. B. Japanisch, Chinesisch oder Deutsch, enthält. Sie unterstützt bis zu 65.535 eindeutige Codepunkte.

Einschränkung: Diese Funktion ist nur unter Windows verfügbar.

Bei Verwendung von Unicode kann Ihre Anwendung Dateinamen in jedem Zeichensatz auf derselben Maschine sichern und zurückschreiben. Beispielsweise können Sie auf einer Maschine, auf der Englisch installiert ist, Dateinamen in jeder anderen Sprachencodepage sichern und zurückschreiben.

- Situationen für die Verwendung von Unicode
  Sie können Ihre Anwendung, die mehrere Sprachen unterstützt, vereinfachen, indem Sie eine Unicode-Anwendung schreiben und die Vorteile der Unicode-Schnittstelle von IBM Spectrum Protect nutzen.
- Unicode konfigurieren
  Um Unicode konfigurieren und verwenden zu können, müssen Sie eine bestimmte Prozedur ausführen, damit die API einen Unicode-Dateibereich auf dem Server registriert und alle Dateinamen in diesem Dateibereich Unicode-Zeichenfolgen werden.

Situationen für die Verwendung von Unicode

Sie können Ihre Anwendung, die mehrere Sprachen unterstützt, vereinfachen, indem Sie eine Unicode-Anwendung schreiben und die Vorteile der Unicode-Schnittstelle von IBM Spectrum Protect nutzen.

Verwenden Sie die Unicode-Schnittstelle von IBM Spectrum Protect, wenn eine der folgenden Bedingungen erfüllt ist:

- Ihre Anwendung wurde bereits für Unicode kompiliert und wurde in einen Mehrbytezeichensatz (MBCS) konvertiert, bevor die IBM Spectrum Protect-API aufgerufen wurde.
- Sie schreiben eine neue Anwendung und Ihre Anwendung soll Unicode unterstützen.
- Ihre Anwendung verwendet eine Zeichenfolge, die von einem Betriebssystem oder einer anderen Anwendung, das bzw. die Unicode verwendet, an die Anwendung übergeben wurde.

Wenn Unicode nicht benötigt wird, ist es nicht erforderlich, die Anwendung erneut zu kompilieren.

Die API verwendet weiterhin die dsm-Schnittstelle. Das API-SDK enthält die Musterprogramme callmtu1.c und callmtu2.c, die die Verwendung der Unicode-API veranschaulichen. Kompilieren Sie diese Programme mithilfe von **makemtu**.

Unicode konfigurieren

Um Unicode konfigurieren und verwenden zu können, müssen Sie eine bestimmte Prozedur ausführen, damit die API einen Unicode-Dateibereich auf dem Server registriert und alle Dateinamen in diesem Dateibereich Unicode-Zeichenfolgen werden.

Einschränkung: Sie können Unicode-Dateinamen und andere Dateinamen nicht in demselben Dateibereich speichern.

1. Kompilieren Sie den Code mit dem Flag -DUNICODE.
2. Alle Zeichenfolgen in Ihrer Anwendung müssen wchar-Zeichenfolgen sein.
3. Folgen Sie den Strukturen in der Datei tsmapitd.h und den Funktionsdefinitionen in der Datei tsmapifp.h für Aufrufe an die API.
4. Setzen Sie das Flag *useUnicode* im Funktionsaufruf **tsmInitEx** auf *bTrue*. Jeder neue Dateibereich wird als Unicode-Dateibereich registriert.

Wenn Sie Daten an bereits registrierte Nicht-Unicode-Dateibereiche senden, sendet die API Dateinamen weiterhin als Nicht-Unicode. Benennen Sie die alten Dateibereiche auf dem Server in fsname_old um und starten Sie einen neuen Unicode-Dateibereich für neue Daten. Die API schreibt Nicht-Unicode-Daten aus den alten Dateibereichen zurück. Verwenden Sie das Feld **bIsUnicode** in der Struktur **tsmQryRespFSData**, die in einem Abfragedateibereich zurückgegeben wird, um festzustellen, ob es sich um einen Unicode-Dateibereich handelt.

Jeder Funktionsaufruf **dsmXXX** verfügt über einen entsprechenden Funktionsaufruf **tsmXXX**. Der Unterschied zwischen beiden sind die verwendeten Strukturen. Alle Strukturen des Funktionsaufrufs **tsmXXX** haben den Typ dsChar_t für Zeichenfolgewerte, wenn sie mit dem UNICODE-Flag kompiliert werden. dsChar_r wird wchar zugeordnet. Es gibt keinen anderen Unterschied zwischen diesen Schnittstellen. Einschränkung: Verwenden Sie entweder die eine Schnittstelle oder die andere. Kombinieren Sie nicht die Schnittstellen des Funktionsaufrufs **dsmXXX** und des Funktionsaufrufs **tsmXXX**. Stellen Sie sicher, dass Sie die IBM Spectrum Protect-Strukturen und IBM Spectrum Protect-Versionsdefinitionen verwenden.

Einige Konstanten werden weiterhin in der Datei dsmapitd.h definiert, daher benötigen Sie beim Kompilieren sowohl die Datei dsmapitd.h als auch die Datei tsmapitd.h.

Sie können die IBM Spectrum Protect-Schnittstelle auf anderen Betriebssystemen verwenden, z. B. UNIX oder Linux. Auf diesen Betriebssystemen wird der Typ dsChar_t jedoch char zugeordnet, weil Unicode nur unter Windows unterstützt wird. Sie können nur eine einzige Variante der Anwendung schreiben und auf mehreren Betriebssystemen mithilfe der IBM Spectrum Protect-Schnittstelle kompilieren. Verwenden Sie die IBM Spectrum Protect-Schnittstelle, wenn Sie eine neue Anwendung schreiben.

Wenn Sie ein Upgrade einer vorhandenen Anwendung durchführen:

1. Konvertieren Sie die Strukturen und Aufrufe des Funktionsaufrufs **dsmXXX** in die IBM Spectrum Protect-Schnittstelle
2. Migrieren Sie vorhandene Dateibereiche
3. Sichern Sie neue Dateibereiche mit der Einstellung *true* für das Flag *useUnicode*

Anmerkung: Sobald Sie mithilfe eines Clients mit Unicode-Unterstützung auf einen Knoten zugegriffen haben, können Sie mit einer älteren Version der API oder mit einer API aus einem anderen Betriebssystem keine Verbindung zu demselben Knoten herstellen. Wenn Ihre Anwendung plattformübergreifende Funktionalität verwendet, dürfen Sie das Flag Unicode nicht verwenden. Es gibt keine plattformübergreifende Unterstützung zwischen Unicode- und Nicht-Unicode-Betriebssystemen.

Wenn Sie das Flag *useUnicode* aktivieren, werden alle Zeichenfolgestrukturen als Unicode-Zeichenfolgen behandelt. Auf dem Server sind nur die folgenden Felder wahre Unicode-Felder:

- Dateibereichsname
- Obere Ebene
- Untere Ebene
- Archivierungsbeschreibung

Alle übrigen Felder werden in MBCS in der lokalen Codepage konvertiert, bevor sie an den Server gesendet werden. Felder wie Knotenname sind wchar-Zeichenfolgen. Sie müssen in der aktuellen Ländereinstellung gültig sein. Sie können beispielsweise auf einem japanischen System Dateien mit chinesischen Namen sichern, der Knotenname muss jedoch eine gültige japanische Zeichenfolge sein. Die Optionsdatei bleibt in der aktuellen Codepage. Wenn Sie eine Einschluss-/Ausschlussliste in Unicode erstellen müssen, verwenden Sie die Option *inclexcl* mit einem Dateinamen und erstellen Sie eine Unicode-Datei, die Unicode-Muster enthält.

Zugehörige Verweise:
Option inclexcl

API-Funktionsaufrufe

In Tabelle 1 wird eine alphabetische Liste der API-Funktionsaufrufe mit einer Kurzbeschreibung und der Angabe, wo detaillierte Informationen zu dem Funktionsaufruf gefunden werden können, bereitgestellt. Die Liste umfasst Folgendes:

Element	Beschreibung
Zweck	Beschreibt den Funktionsaufruf.
Syntax	Enthält den tatsächlichen C-Code für den Funktionsaufruf. Dieser Code wurde aus der UNIX- oder Linux-Version der Headerdatei dsmapifp.h kopiert. . Siehe Quellendatei mit den API-Funktionsdefinitionen. Diese Datei unterscheidet sich geringfügig von der Datei auf anderen Betriebssystemen. Anwendungsprogrammierer für andere Betriebssysteme müssen in Bezug auf die exakte Syntax der API-Definitionen Ihre Version der Headerdatei dsmapifp.h überprüfen.
Parameter	Beschreibt jeden Parameter in dem Funktionsaufruf und kennzeichnet ihn abhängig von seiner Verwendung als Eingabe (E) oder Ausgabe (A). Einige Parameter sind sowohl als Eingabe als auch als Ausgabe (E/A) gekennzeichnet. Die Datentypen, auf die in diesem Abschnitt Bezug genommen wird, sind in der Headerdatei dsmapitd.h definiert. Siehe Quellendateien für API-Typdefinitionen.
Rückkehrcodes	Enthält eine Liste der Rückkehrcodes, die für den Funktionsaufruf spezifisch sind. Allgemeine Systemfehler wie Kommunikationsfehler, Serverfehler oder Benutzerfehler, die in jedem Aufruf auftreten können, sind nicht aufgelistet. Die Rückkehrcodes sind in der Headerdatei dsmrc.h definiert. Siehe Quellendatei mit API-Rückkehrcodes: dsmrc.h.

Tabelle 1. API-Funktionsaufrufe

Funktionsaufruf und Link	Beschreibung
dsmBeginGetData	Startet eine Zurückschreibungs- oder Abrufoperation für eine Liste mit Objekten im Speicher.
dsmBeginQuery	Startet für IBM Spectrum Protect eine Anforderung zum Abfragen von Informationen.

Funktionsaufruf und Link	Beschreibung
dsmBeginTxn	Startet eine oder mehrere Transaktionen, die eine vollständige Aktion starten. Entweder werden alle Aktionen erfolgreich ausgeführt oder keine wird erfolgreich ausgeführt.
dsmBindMC	Ordnet eine Verwaltungsklasse dem Objekt zu, das übergeben wird, bzw. bindet eine Verwaltungsklasse an dieses Objekt.
dsmChangePW	Ändert ein IBM Spectrum Protect-Kennwort.
dsmCleanUp	Dieser Aufruf wird verwendet, wenn **dsmSetUp** aufgerufen wurde.
dsmDeleteAccess	Löscht aktuelle Berechtigungsregeln für Sicherungsversionen oder archivierte Kopien Ihrer Objekte.
dsmDeleteFS	Löscht einen Dateibereich aus dem Speicher.
dsmDeleteObj	Inaktiviert Sicherungsobjekte oder löscht Archivierungsobjekte im Speicher.
dsmEndGetData	Beendet eine **dsmBeginGetData**-Sitzung, mit der Objekte aus dem Speicher abgerufen werden.
dsmEndGetDataEx	Gibt die Gesamtanzahl gesendeter LAN-unabhängiger Byte an.
dsmEndGetObj	Beendet eine **dsmGetObj**-Sitzung, mit der Daten für ein bestimmtes Objekt abgerufen werden.
dsmEndQuery	Gibt das Ende einer Aktion **dsmBeginQuery** an.
dsmEndSendObj	Gibt das Ende der Daten an, die in den Speicher gesendet werden.
dsmEndSendObjEx	Gibt Komprimierungsangaben und die Anzahl gesendeter Byte an.
dsmEndTxn	Beendet eine IBM Spectrum Protect-Transaktion.
dsmEndTxnEx	Stellt Informationen zur Objekt-ID des Gruppenleiters für die Verwendung im Aufruf **dsmGroupHandlerfunction** bereit.
dsmGetData	Ruft einen Bytestrom mit Daten aus IBM Spectrum Protect ab und stellt ihn in den Puffer des Aufrufenden.
dsmGetBufferData	Ruft einen von IBM Spectrum Protect zugeordneten Datenpuffer aus dem IBM Spectrum Protect-Server ab.
dsmGetNextQObj	Ruft die nächste Abfrageantwort aus einem vorherigen Aufruf **dsmBeginQuery** ab und stellt ihn in den Puffer des Aufrufenden.
dsmGetObj	Ruft die angeforderten Objektdaten aus dem Datenstrom ab und stellt sie in den Puffer des Aufrufenden.
dsmGroupHandler	Führt abhängig von der bereitgestellten Eingabe eine Aktion für eine logische Dateigruppe aus.
dsmInit	Startet eine API-Sitzung und verbindet den Client mit Speicher.
dsmInitEx	Startet eine API-Sitzung unter Verwendung der zusätzlichen Parameter, die eine erweiterte Überprüfung ermöglichen.
dsmLogEvent	Protokolliert eine Benutzernachricht in der Serverprotokolldatei und/oder im lokalen Fehlerprotokoll.
dsmLogEventEx	Protokolliert eine Benutzernachricht in der Serverprotokolldatei und/oder im lokalen Fehlerprotokoll.
dsmQueryAccess	Fragt den Server nach allen Zugriffsberechtigungsregeln für Sicherungsversionen oder archivierte Kopien Ihrer Objekte ab.
dsmQueryApiVersion	Führt eine Abfrageanforderung für die API-Bibliotheksversion aus, auf die der Anwendungsclient zugreift.
dsmQueryApiVersionEx	Führt eine Abfrageanforderung für die API-Bibliotheksversion aus, auf die der Anwendungsclient zugreift.
dsmQueryCliOptions	Fragt wichtige Optionswerte in der Benutzeroptionsdatei ab.
dsmQuerySessInfo	Startet eine Anforderung zum Abfragen von Informationen an IBM Spectrum Protect, die sich auf die Operation der angegebenen Sitzung in **dsmHandle** beziehen.
dsmQuerySessOptions	Fragt wichtige Optionswerte ab, die in der angegebenen Sitzung in **dsmHandle** gültig sind.
dsmRCMsg	Ruft den Nachrichtentext ab, der einem API-Rückkehrcode zugeordnet ist.
dsmRegisterFS	Registriert einen neuen Dateibereich beim Server.
dsmReleaseBuffer	Gibt einen von IBM Spectrum Protect zugeordneten Puffer zurück.

Funktionsaufruf und Link	Beschreibung
dsmRenameObj	Benennt den übergeordneten oder untergeordneten Objektnamen um.
dsmRequestBuffer	Ruft einen von IBM Spectrum Protect zugeordneten Puffer für die Pufferkopieneliminierung ab.
dsmRetentionEvent	Sendet im Rahmen einer Aufbewahrungsereignisoperation, die für die in der Liste angegebenen Objekte ausgeführt werden soll, eine Liste mit Objekt-IDs an den Server.
dsmSendBufferData	Sendet Daten aus einem von IBM Spectrum Protect zugeordneten Puffer.
dsmSendData	Sendet einen Bytestrom mit Daten über einen Puffer an IBM Spectrum Protect.
dsmSendObj	Startet eine Anforderung zum Senden eines einzelnen Objekts in Speicher.
dsmSetAccess	Erteilt anderen Benutzern oder Knoten Zugriff auf Sicherungsversionen oder archivierte Kopien Ihrer Objekte, Zugriff auf alle Ihre Objekte oder Zugriff auf eine ausgewählte Gruppe von Objekten.
dsmSetUp	Überschreibt Umgebungsvariablenwerte.
dsmTerminate	Beendet eine Sitzung mit dem Server und bereinigt die IBM Spectrum Protect-Umgebung.
dsmUpdateFS	Aktualisiert einen Dateibereich im Speicher.
dsmUpdateObj	Aktualisiert die objInfo-Informationen, die einem aktiven Sicherungsobjekt zugeordnet sind, das sich bereits auf dem Server befindet, oder aktualisiert archivierte Objekte.
dsmUpdateObjEx	Aktualisiert die objInfo-Informationen, die einem bestimmten Archivierungsobjekt zugeordnet sind, selbst dann, wenn mehrere Objekte mit demselben Namen vorhanden sind, oder aktualisiert aktive Sicherungsobjekte.

- dsmBeginGetData
  Mit dem Funktionsaufruf **dsmBeginGetData** wird eine Zurückschreibungs- oder Abrufoperationen für eine Liste mit Objekten im Speicher gestartet. Diese Liste mit Objekten ist in der Struktur **dsmGetList** enthalten. Die Anwendung erstellt diese Liste mit Werten aus der Abfrage, die einem Aufruf **dsmBeginGetData** voranging.
- dsmBeginQuery
  Mit dem Funktionsaufruf dsmBeginQuery wird eine Anforderung zur Abfrage von Informationen zu Daten, Dateibereichen und Verwaltungsklassen an den Server gestartet.
- dsmBeginTxn
  Mit dem Funktionsaufruf **dsmBeginTxn** werden eine oder mehrere IBM Spectrum Protect-Transaktionen gestartet, die eine vollständige Aktion starten; entweder werden alle Aktionen erfolgreich ausgeführt oder es wird keine Aktion erfolgreich ausgeführt. Eine Aktion kann entweder ein einzelner Aufruf oder eine Serie von Aufrufen sein. Beispielsweise kann ein Aufruf **dsmSendObj**, auf den eine Reihe von Aufrufen **dsmSendData** folgt, als eine einzige Aktion betrachtet werden. In ähnlicher Weise wird ein Aufruf **dsmSendObj** mit **dataBlkPtr**, der einen Datenbereich angibt, der das zu sichernde Objekt enthält, ebenso als eine einzige Aktion betrachtet.
- dsmBindMC
  Mit den Funktionsaufruf **dsmBindMC** wird eine Verwaltungsklasse dem übergebenen Objekt zugeordnet bzw. an es gebunden. Das Objekt wird über die Einschluss-/Ausschlussliste übergeben, auf die in der Optionsdatei verwiesen wird. Wird in der Einschlussliste keine Übereinstimmung für eine bestimmte Verwaltungsklasse gefunden, wird die Standardverwaltungsklasse zugeordnet. Über die Ausschlussliste können Objekte von einer Sicherung ausgeschlossen werden, aber nicht von einer Archivierung.
- dsmChangePW
  Mit dem Funktionsaufruf **dsmChangePW** wird ein IBM Spectrum Protect-Kennwort geändert. Bei einem Mehrbenutzerbetriebssystem wie UNIX oder Linux kann dieser Aufruf nur vom Rootbenutzer oder vom berechtigten Benutzer verwendet werden.
- dsmCleanUp
  Der Funktionsaufruf **dsmCleanUp** wird verwendet, wenn **dsmSetUp** aufgerufen wurde. Der Funktionsaufruf **dsmCleanUp** sollte aufgerufen werden, nachdem **dsmTerminate** aufgerufen wurde. Nachdem **dsmCleanUp** aufgerufen wurde, können keine anderen Aufrufe erfolgen.
- dsmDeleteAccess
  Mit dem Funktionsaufruf **dsmDeleteAccess** werden aktuelle Berechtigungsregeln für Sicherungsversionen oder archivierte Kopien Ihrer Objekte gelöscht. Wenn Sie eine Berechtigungsregel löschen, entziehen Sie den Zugriff, den ein Benutzer auf alle in der Regel angegebenen Dateien hat.
- dsmDeleteFS
  Mit dem Funktionsaufruf **dsmDeleteFS** wird ein Dateibereich aus dem Speicher gelöscht. Um einen Dateibereich löschen zu können, muss Ihnen der IBM Spectrum Protect-Administrator die korrekten Berechtigungen erteilen. Rufen Sie **dsmQuerySessInfo** auf, um zu bestimmen, ob Sie über die erforderlichen Berechtigungen verfügen. Dieser Funktionsaufruf gibt eine Datenstruktur des Typs *ApiSessInfo* zurück, die zwei Felder, *archDel* und *backDel*, enthält.
- dsmDeleteObj
  Mit dem Funktionsaufruf **dsmDeleteObj** werden Sicherungsobjekte inaktiviert oder gelöscht oder Archivierungsobjekte im Speicher gelöscht. Beim Typ **dtBackup** wird nur die momentan aktive Sicherungskopie inaktiviert. Beim Typ **dtBackupID** wird das Objekt mit der jeweils angegebenen Objekt-ID vom Server gelöscht. Rufen Sie diese Funktion innerhalb einer Transaktion auf.
- dsmEndGetData
  Mit dem Funktionsaufruf **dsmEndGetData** wird eine **dsmBeginGetData**-Sitzung, mit der Objekte aus Speicher abgerufen werden, beendet.

- dsmEndGetDataEx
  Mit dem Funktionsaufruf **dsmEndGetDataEx** wird die Gesamtanzahl gesendeter LAN-unabhängiger Byte angegeben. Er ist eine Erweiterung des Funktionsaufrufs **dsmEndGetData**.
- dsmEndGetObj
  Mit dem Funktionsaufruf **dsmEndGetObj** wird eine **dsmGetObj**-Sitzung, mit der Daten für ein bestimmtes Objekt abgerufen werden, beendet.
- dsmEndQuery
  Mit dem Funktionsaufruf **dsmEndQuery** wird das Ende einer Aktion **dsmBeginQuery** angegeben. Der Anwendungsclient sendet einen Aufruf **dsmEndQuery**, um eine Abfrage abzuschließen. Dieser Aufruf wird entweder gesendet, nachdem alle Abfrageantworten über **dsmGetNextQObj** abgerufen wurden, oder er wird gesendet, um eine Abfrage zu beenden, bevor alle Daten zurückgegeben werden.
- dsmEndSendObj
  Mit dem Funktionsaufruf **dsmEndSendObj** wird das Ende der Daten angegeben, die in den Speicher gesendet werden.
- dsmEndSendObjEx
  Mit dem Funktionsaufruf **dsmEndSendObjEx** werden zusätzliche Informationen in Bezug auf die Anzahl verarbeiteter Byte bereitgestellt. Die Informationen umfassen: Gesamtanzahl gesendeter Byte, Komprimierungsangaben, LAN-unabhängige Byte und Angaben zur Deduplizierung.
- dsmEndTxn
  Mit dem Funktionsaufruf dsmEndTxn wird eine IBM Spectrum Protect-Transaktion beendet. Geben Sie den Funktionsaufruf dsmEndTxn zusammen mit dsmBeginTxn an, um den Aufruf oder die Gruppe von Aufrufen, die als eine Transaktion betrachtet werden, zu identifizieren. Der Anwendungsclient kann im Aufruf dsmEndTxn angeben, ob die Transaktion festgeschrieben oder beendet werden muss.
- dsmEndTxnEx
  Mit dem Funktionsaufruf **dsmEndTxnEx** werden Informationen zur Objekt-ID des Gruppenleiters zur Verwendung im Funktionsaufruf **dsmGroupHandler** bereitgestellt. Er ist eine Erweiterung des Funktionsaufrufs **dsmEndTxn**.
- dsmGetData
  Mit dem Funktionsaufruf **dsmGetData** wird ein Bytestrom mit Daten von IBM Spectrum Protect abgerufen und in den Puffer des Aufrufenden gestellt. Der Anwendungsclient ruft **dsmGetData** auf, wenn weitere Daten für den Empfang von einem vorherigen Aufruf **dsmGetObj** oder **dsmGetData** verfügbar sind.
- dsmGetBufferData
  Mit dem Funktionsaufruf **dsmGetBufferData** wird ein Bytestrom mit Daten über einen Puffer von IBM Spectrum Protect empfangen. Nach jedem Aufruf muss die Anwendung die Daten kopieren und den Puffer über einen Aufruf **dsmReleaseBuffer** freigeben. Wenn die Anzahl Puffer, die von der Anwendung angehalten wurden, dem im Aufruf **dsmInitEx** für 'numTsmBuffers' angegebenen Wert entspricht, blockt die Funktion **dsmGetBufferData** das Senden von Daten, bis ein Aufruf **dsmReleaseBuffer** gesendet wird.
- dsmGetNextQObj
  Mit dem Funktionsaufruf dsmGetNextQObj wird die nächste Abfrageantwort von einem vorherigen Aufruf dsmBeginQuery abgerufen und in den Puffer des Aufrufenden gestellt.
- dsmGetObj
  Mit dem Funktionsaufruf **dsmGetObj** werden die angeforderten Objektdaten aus dem IBM Spectrum Protect-Datenstrom abgerufen und in den Puffer des Aufrufenden gestellt. Der Aufruf **dsmGetObj** verwendet die Objekt-ID, um das nächste Objekt oder das nächste Teilobjekt aus dem Datenstrom abzurufen.
- dsmGroupHandler
  Mit dem Funktionsaufruf **dsmGroupHandler** wird abhängig von der bereitgestellten Eingabe eine Aktion für eine logische Dateigruppe ausgeführt. Der Client fasst eine Reihe einzelner Objekte in einer Gruppe zusammen, um diese auf dem IBM Spectrum Protect-Server als logische Gruppe zu referenzieren und zu verwalten.
- dsmInit
  Mit dem Funktionsaufruf **dsmInit** wird eine API-Sitzung gestartet und der Client mit IBM Spectrum Protect-Speicher verbunden. Für den Anwendungsclient kann jeweils nur eine einzige Sitzung zu einem bestimmten Zeitpunkt aktiv sein. Um eine weitere Sitzung mit anderen Parametern zu öffnen, beenden Sie die aktuelle Sitzung zunächst mit dem Aufruf **dsmTerminate**.
- dsmInitEx
  Mit dem Funktionsaufruf dsmInitEx wird eine API-Sitzung gestartet, wobei die zusätzlichen Parameter für die erweiterte Prüfung verwendet werden.
- dsmLogEvent
  Mit dem Funktionsaufruf **dsmLogEvent** wird eine Benutzernachricht (ANE4991I) in der Serverprotokolldatei und/oder im lokalen Fehlerprotokoll protokolliert. Eine Struktur des Typs **logInfo** wird in dem Aufruf übergeben. Dieser Aufruf muss während des Zustands **InSession** innerhalb einer Sitzung ausgeführt werden. Er darf nicht in einer Sende-, Abruf- oder Abfrageoperation ausgeführt werden. Um Nachrichten abzurufen, die auf dem Server protokolliert sind, verwenden Sie den Befehl **query actlog** über den Verwaltungsclient.
- dsmLogEventEx
  Mit dem Funktionsaufruf dsmLogEventEx wird eine Benutzernachricht in der Serverprotokolldatei und/oder im lokalen Fehlerprotokoll protokolliert. Dieser Aufruf muss während des Zustands InSession innerhalb einer Sitzung ausgeführt werden. Der Aufruf kann nicht in einem Sende-, Abruf- oder Abfrageaufruf durchgeführt werden.
- dsmQueryAccess
  Mit dem Funktionsaufruf **dsmQueryAccess** wird der Server nach allen Zugriffsberechtigungsregeln für Sicherungsversionen oder archivierte Kopien Ihrer Objekte abgefragt. Ein Verweis auf ein Array von Zugriffsregeln wird an den Aufruf übergeben und das fertige Array zurückgegeben. Es wird ein Verweis auf die Anzahl Regeln übergeben, um anzugeben, wie viele Regeln das Array enthält.
- dsmQueryApiVersion
  Mit dem Funktionsaufruf **dsmQueryApiVersion** wird eine Abfrageanforderung für die API-Bibliotheksversion ausgeführt, auf die der Anwendungsclient zugreift.
- dsmQueryApiVersionEx
  Mit dem Funktionsaufruf **dsmQueryApiVersionEx** wird eine Abfrageanforderung für die API-Bibliotheksversion ausgeführt, auf die der

Anwendungsclient zugreift.

- dsmQueryCliOptions
  Mit dem Funktionsaufruf **dsmQueryCliOptions** werden wichtige Optionswerte in der Benutzeroptionsdatei abgefragt. Eine Struktur des Typs **optStruct** wird in dem Aufruf übergeben und enthält die Informationen. Dieser Aufruf wird ausgeführt, bevor **dsmInitEx** aufgerufen wird; er legt die Konfiguration vor der Sitzung fest.
- dsmQuerySessInfo
  Mit dem Funktionsaufruf **dsmQuerySessInfo** wird eine Anforderung zum Abfragen von Informationen an IBM Spectrum Protect gestartet, die sich auf die Operation der angegebenen Sitzung in **dsmHandle** beziehen. Eine Struktur des Typs **ApiSessInfo** wird in dem Aufruf übergeben; sie enthält alle verfügbaren eingegebenen sitzungsbezogenen Informationen. Dieser Aufruf wird nach einem erfolgreichen Aufruf **dsmInitEx** gestartet.
- dsmQuerySessOptions
  Mit dem Funktionsaufruf dsmQuerySessOptions werden wichtige Optionswerte, die in der in dsmHandle angegebenen Sitzung gültig sind, abgefragt. Eine Struktur des Typs `optStruct` wird in dem Aufruf übergeben und enthält die Informationen.
- dsmRCMsg
  Mit dem Funktionsaufruf dsmRCMsg wird der Nachrichtentext abgerufen, der einem API-Rückkehrcode zugeordnet ist.
- dsmRegisterFS
  Mit dem Funktionsaufruf **dsmRegisterFS** wird ein neuer Dateibereich beim IBM Spectrum Protect-Server registriert. Bevor Sie Daten in einem Dateibereich sichern können, müssen Sie diesen zuvor registrieren.
- dsmReleaseBuffer
  Mit der Funktion **dsmReleaseBuffer** wird ein Puffer an IBM Spectrum Protect zurückgegeben. **dsmReleaseBuffer** wird von der Anwendung aufgerufen, nachdem ein Aufruf **dsmGetDataEx** erfolgt ist und die Anwendung alle Daten aus dem Puffer übertragen hat und zum Freigeben des Puffers bereit ist. **dsmReleaseBuffer** erfordert den Aufruf **dsmInitEx** unter Angabe von ***btrue*** für *UseTsmBuffers* und einem Wert ungleich null für *numTsmBuffers*. **dsmReleaseBuffer** sollte auch aufgerufen werden, wenn der Aufruf **dsmTerminate** unmittelbar bevorsteht und die Anwendung Datenpuffer noch nicht freigegeben hat.
- dsmRenameObj
  Mit dem Funktionsaufruf **dsmRenameObj** wird der übergeordnete oder untergeordnete Objektname umbenannt. Übergeben Sie bei Sicherungsobjekten den aktuellen Objektnamen und Änderungen für über- oder untergeordnete Objektnamen. Übergeben Sie bei Archivierungsobjekten den aktuellen Objektdateibereichsnamen und die Objekt-ID sowie Änderungen für über- oder untergeordnete Objektnamen. Verwenden Sie diesen Funktionsaufruf in Aufrufen **dsmBeginTxn** und **dsmEndTxn**.
- dsmRequestBuffer
  Mit der Funktion **dsmRequestBuffer** wird ein Puffer an IBM Spectrum Protect zurückgegeben. **dsmRequestBuffer** wird von der Anwendung aufgerufen, nachdem ein Aufruf **dsmGetDataEx** erfolgt ist und die Anwendung alle Daten aus dem Puffer übertragen hat und zum Freigeben des Puffers bereit ist.
- dsmRetentionEvent
  Mit dem Funktionsaufruf **dsmRetentionEvent** wird im Rahmen einer Aufbewahrungsereignisoperation, die für die in der Liste angegebenen Objekte ausgeführt werden soll, eine Liste mit Objekt-IDs an den IBM Spectrum Protect-Server gesendet. Verwenden Sie diesen Funktionsaufruf in Aufrufen **dsmBeginTxn** und **dsmEndTxn**.
- dsmSendBufferData
  Mit dem Funktionsaufruf **dsmSendBufferData** wird ein Bytestrom mit Daten über einen in einem vorherigen Aufruf **dsmReleaseBuffer** bereitgestellten Puffer an IBM Spectrum Protect gesendet. Der Anwendungsclient kann jeden Typ von Daten zum Speichern auf dem Server übergeben. In der Regel (aber nicht ausschließlich) handelt es sich bei diesen Daten um Dateidaten. Sie können **dsmSendBufferData** mehrmals aufrufen, wenn der Bytestrom mit Daten, den Sie senden, groß ist. Der Puffer wird unabhängig davon, ob der Aufruf erfolgreich ausgeführt wird oder fehlschlägt, freigegeben.
- dsmSendData
  Mit dem Funktionsaufruf **dsmSendData** wird ein Bytestrom mit Daten über einen Puffer an IBM Spectrum Protect gesendet. Der Anwendungsclient kann jeden Typ von Daten zum Speichern auf dem Server übergeben. In der Regel (aber nicht ausschließlich) handelt es sich bei diesen Daten um Dateidaten. Sie können **dsmSendData** mehrmals aufrufen, wenn der Bytestrom mit Daten, der gesendet werden soll, groß ist.
- dsmSendObj
  Mit dem Funktionsaufruf **dsmSendObj** wird eine Anforderung zum Senden eines einzelnen Objekts in Speicher gestartet. Aufgrund von Leistungsaspekten können mehrere Aufrufe **dsmSendObj** und zugehörige Aufrufe **dsmSendData** innerhalb der Grenzen einer Transaktion ausgeführt werden.
- dsmSetAccess
  Mit dem Funktionsaufruf **dsmSetAccess** wird anderen Benutzern oder Knoten Zugriff auf Sicherungsversionen oder archivierte Kopien Ihrer Objekte, Zugriff auf alle Ihre Objekte oder Zugriff auf eine ausgewählte Gruppe von Objekten erteilt. Wenn Sie einem anderen Benutzer Zugriff erteilen, kann dieser Benutzer Ihre Dateien abfragen, zurückschreiben oder abrufen. Dieser Befehl unterstützt Platzhalterzeichen für die folgenden Felder: *fs*, *hl*, *ll*, *node*, *owner*.
- dsmSetUp
  Mit dem Funktionsaufruf **dsmSetUp** werden Umgebungsvariablenwerte überschrieben. Rufen Sie **dsmSetUp** auf, bevor Sie **dsmInitEx** aufrufen. Die Werte, die in der Struktur **envSetUp** übergeben wurden, überschreiben alle vorhandenen Umgebungsvariablen oder Standardwerte. Wenn Sie NULL für ein Feld angeben, werden die Werte aus der Umgebung übernommen. Wenn Sie keinen Wert definieren, werden die Werte aus den Standardwerden übernommen.
- dsmTerminate
  Mit dem Funktionsaufruf **dsmTerminate** wird eine Sitzung mit dem IBM Spectrum Protect-Server beendet und die IBM Spectrum Protect-Umgebung bereinigt.
- dsmUpdateFS
  Mit dem Funktionsaufruf dsmUpdateFS wird ein Dateibereich im IBM Spectrum Protect-Speicher aktualisiert. Diese Aktualisierung stellt sicher, das der Administrator über einen aktuellen Satz Ihres Dateibereichs verfügt.

- dsmUpdateObj
  Mit dem Funktionsaufruf **dsmUpdateObj** werden die Metainformationen aktualisiert, die einem aktiven Sicherungs- oder Archivierungsobjekt zugeordnet sind, das sich bereits auf dem Server befindet. Der Aufruf hat keine Auswirkungen auf die Anwendungsbitdaten. Um ein Objekt aktualisieren zu können, müssen Sie einen bestimmten Namen ohne Platzhalterzeichen angeben. Um ein archiviertes Objekt zu aktualisieren, setzen Sie **dsmSendType** auf **stArchive**. Es wird nur das letzte benannte Archivierungsobjekt aktualisiert.
- dsmUpdateObjEx
  Mit dem Funktionsaufruf **dsmUpdateObjEx** werden die Metainformationen aktualisiert, die einem aktiven Sicherungs- oder Archivierungsobjekt zugeordnet sind, das sich auf dem Server befindet. Der Aufruf hat keine Auswirkungen auf die Anwendungsbitdaten. Um ein Objekt aktualisieren zu können, müssen Sie einen Namen ohne Platzhalterzeichen angeben; Sie können auch die Objekt-ID angeben, um ein bestimmtes archiviertes Objekt zu aktualisieren. Bei der Angabe des Namens können Sie keine Platzhalterzeichen verwenden. Um ein Sicherungsobjekt zu aktualisieren, setzen Sie den Parameter **dsmSendType** auf **stBackup**. Um ein archiviertes Objekt zu aktualisieren, setzen Sie den Parameter **dsmSendType** auf **stArchive**.

Zugehörige Verweise:
API-Rückkehrcodes

dsmBeginGetData

Mit dem Funktionsaufruf **dsmBeginGetData** wird eine Zurückschreibungs- oder Abrufoperationen für eine Liste mit Objekten im Speicher gestartet. Diese Liste mit Objekten ist in der Struktur **dsmGetList** enthalten. Die Anwendung erstellt diese Liste mit Werten aus der Abfrage, die einem Aufruf **dsmBeginGetData** voranging.

Der Aufrufende muss die Felder für die Zurückschreibungsreihenfolge aus der Objektabfrage verwenden, um die Liste, die in diesem Aufruf enthalten ist, zu sortieren. Damit wird sichergestellt, dass die Objekte so effizient wie möglich aus dem Speicher zurückgeschrieben werden, ohne dass Datenbänder zurückgespult oder erneut geladen werden müssen.

Beim Abrufen vollständiger Objekte ist das Maximum für *dsmGetList.numObjID* DSM_MAX_GET_OBJ. Beim Abrufen von Teilobjekten ist das Maximum DSM_MAX_PARTIAL_GET_OBJ.

Geben Sie nach dem Aufruf **dsmBeginGetData** einen oder mehrere Aufrufe **dsmGetObj** an, um jedes Objekt in der Liste abzurufen. Nachdem das jeweilige Objekt abgerufen wurde und keine weiteren Daten für das Objekt erforderlich sind, wird der Aufruf **dsmEndGetObj** gesendet.

Nachdem alle Objekte abgerufen wurden oder wenn der Aufruf **dsmEndGetObj** abgebrochen wird, wird der Aufruf **dsmEndGetData** gesendet. Sie können dann den Zyklus erneut starten.

Syntax

```
dsInt16_t dsmBeginGetData (dsUint32_t       dsmHandle,
   dsBool_t     mountWait,
   dsmGetType   getType,
   dsmGetList  *dsmGetObjListP);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.

dsBool_t mountWait (I)
: Ein boolescher Wert von 'true' oder 'false' gibt an, ob der Anwendungsclient auf das Laden von Offlinedatenträgern wartet, wenn die erforderlichen Daten momentan offline sind. Hat 'mountWait' den Wert 'true', wartet die Anwendung auf das Laden der erforderlichen Datenträger durch den Server. Die Anwendung wartet, bis die Datenträger geladen sind oder die Anforderung abgebrochen wird.

dsmGetType getType (I)
: Ein Aufzählungstyp, der aus gtBackup und gtArchive besteht und angibt, welcher Typ von Objekt abgerufen werden soll.

dsmGetList *dsmGetObjListP (I)
: Die Struktur, die Informationen zu den Objekten oder Teilobjekten enthält, die zurückgeschrieben oder abgerufen werden sollen. Die Struktur verweist auf eine Liste mit Objekt-IDs und - im Fall einer Zurückschreibung oder eines Abrufs von Teilobjekten - auf eine Liste zugeordneter Offsets und Längen. Wenn Ihre Anwendung die Funktion für die Zurückschreibung oder den Abruf von Teilobjekten verwendet, setzen Sie das Feld **dsmGetList.stVersion** auf **dsmGetListPORVersion**. Bei einer Zurückschreibung oder einem Abruf von Teilobjekten können Sie Daten während des Sendevorgangs nicht komprimieren. Um dies durchzusetzen, setzen Sie **ObjAttr.objCompressed** auf *bTrue*.

  Abbildung 1 und Quellendateien für API-Typdefinitionen enthalten weitere Informationen zu dieser Struktur.

  Zurückschreibung oder Abruf von Teilobjekten enthält weitere Informationen zur Zurückschreibung oder zum Abruf von Teilobjekten.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmBeginGetData

Rückkehrcode	Erläuterung
DSM_RC_ABORT_INVALID_OFFSET (33)	Der Offset, der während des Abrufs eines Teilobjekts angegeben wurde, ist größer als die Länge des Objekts.
DSM_RC_ABORT_INVALID_LENGTH (34)	Die Länge, die während des Abrufs eines Teilobjekts angegeben wurde, ist größer als die Länge des Objekts oder der Offset addiert zur Länge liegt hinter dem Ende des Objekts.
DSM_RC_NO_MEMORY (102)	Es ist kein Arbeitsspeicher mehr verfügbar, um die Anforderung auszuführen.
DSM_RC_NUMOBJ_EXCEED (2029)	**dsmGetList.numObjId** ist größer als DSM_MAX_GET_OBJ.
DSM_RC_OBJID_NOTFOUND (2063)	Die Objekt-ID wurde nicht gefunden. Das Objekt wurde nicht zurückgeschrieben.
DSM_RC_WRONG_VERSION_PARM (2065)	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.

dsmBeginQuery

Mit dem Funktionsaufruf dsmBeginQuery wird eine Anforderung zur Abfrage von Informationen zu Daten, Dateibereichen und Verwaltungsklassen an den Server gestartet.

Die Abfrage mit dsmBeginQuery betrifft speziell Folgendes:

- Archivierte Daten
- Gesicherte Daten
- Aktive gesicherte Daten
- Dateibereiche
- Verwaltungsklassen

Die Abfragedaten, die von dem Aufruf zurückgegeben werden, werden von einem oder mehreren Aufrufen dsmGetNextQObj abgerufen. Wenn die Abfrage beendet ist, wird der Aufruf dsmEndQuery gesendet.

Syntax

```
dsInt16_t dsmBeginQuery  (dsUint32_t        dsmHandle,
   dsmQueryType  queryType,
   dsmQueryBuff  *queryBuffer);
```

Parameter

dsUint32_t dsmHandle (I)

Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.

dsmQueryType queryType (I)

Gibt den Abfragetyp an, der ausgeführt werden soll. Weisen Sie eine der folgenden Optionen zu:

qtArchive

Es werden archivierte Objekte abgefragt.

qtBackup

Es werden gesicherte Objekte abgefragt.

qtBackupActive

Es werden nur aktive gesicherte Objekte für den vollständigen von Ihnen übergebenen Dateibereichsnamen abgefragt. Diese Abfrage wird als "Direktaufruf" bezeichnet und ist eine effiziente Möglichkeit, aktive Objekte im Speicher abzufragen. Voraussetzungen: Sie müssen als Rootbenutzer auf einem Betriebssystem UNIX oder Linux angemeldet sein.

qtFilespace

Es werden registrierte Dateibereiche abgefragt.

qtMC

Es werden definierte Verwaltungsklassen abgefragt.

qtBackupGroups

Es werden geschlossene Gruppen abgefragt.

qtOpenGroups

Es werden offene Gruppe abgefragt.

qtProxyNodeAuth

Es werden Knoten abgefragt, an die dieser Knoten Daten weiterleiten kann.

qtProxyNodePeer

Es werden Peerknoten mit demselben Ziel abgefragt.

dsmQueryBuff *queryBuffer (I)

Gibt einen Verweis auf einen Puffer an, der einer bestimmten Datenstruktur zugeordnet ist. Diese Struktur ist dem von Ihnen übergebenen Abfragetyp zugeordnet. Diese Strukturen enthalten die Auswahlkriterien für jeden Abfragetyp. Füllen Sie die Felder in jeder Struktur aus, um den Geltungsbereich der Abfrage anzugeben, die ausgeführt werden soll. In jeder Struktur enthält das Feld `stVersion` die Strukturversionsnummer.

Die Datenstrukturen und ihre zugehörigen Felder umfassen die folgenden Elemente:

qryArchiveData

objName
Der vollständige Objektname. Sie können ein Platzhalterzeichen, wie beispielsweise einen Stern (*) oder ein Fragezeichen (?), verwenden, was sowohl für den übergeordneten als auch den untergeordneten Teil des Namens gilt. Ein Stern entspricht null oder mehr Zeichen; ein Fragezeichen entspricht einem Zeichen. Das Feld objType von objName kann einen der folgenden Werte haben:

- `DSM_OBJ_FILE`
- `DSM_OBJ_DIRECTORY`
- `DSM_OBJ_ANY_TYPE`

Weitere Informationen zu übergeordneten und untergeordneten Namen finden Sie hier: Übergeordnete und untergeordnete Namen.

Eigner

Der Name des Eigners des Objekts.

insDateLowerBound

Die Untergrenze für das Einfügedatum, an dem das Objekt archiviert wurde. Um die standardmäßige Untergrenze abzurufen, setzen Sie die Komponente für das Jahr auf `DATE_MINUS_INFINITE`.

insDateUpperBound

Die Obergrenze für das Einfügedatum, an dem das Objekt archiviert wurde. Um die standardmäßige Obergrenze abzurufen, setzen Sie die Komponente für das Jahr auf `DATE_PLUS_INFINITE`.

expDateLowerBound

Die Untergrenze für das Verfallsdatum. Die Standardwerte für beide Felder für das Verfallsdatum stimmen mit denen für die Felder für das Einfügedatum überein.

expDateUpperBound

Die Obergrenze für das Verfallsdatum.

descr

Die Archivierungsbeschreibung. Geben Sie einen Stern (*) ein, wenn alle Beschreibungen berücksichtigt werden sollen.

qryBackupData

objName
Der vollständige Objektname. Sie können ein Platzhalterzeichen, wie beispielsweise einen Stern (*) oder ein Fragezeichen (?), verwenden, was sowohl für den übergeordneten als auch den untergeordneten Teil des Namens gilt. Ein Stern entspricht null oder mehr Zeichen; ein Fragezeichen entspricht einem Zeichen. Das Feld objType von objName kann einen der folgenden Werte haben:

- `DSM_OBJ_FILE`
- `DSM_OBJ_DIRECTORY`
- `DSM_OBJ_ANY_TYPE`

Weitere Informationen zu übergeordneten und untergeordneten Namen finden Sie hier: Übergeordnete und untergeordnete Namen.

Eigner

Der Name des Eigners des Objekts.

objState

Sie können nach einem der folgenden Objektzustände abfragen:

- DSM_ACTIVE
- DSM_INACTIVE
- DSM_ANY_MATCH

pitDate

Der Zeitpunktwert. Eine Abfrage mit diesem Feld gibt das letzte Objekt zurück, das vor diesem Datum und dieser Uhrzeit gesichert wurde. objState kann 'aktiv' oder 'inaktiv' angeben. Objekte, die vor dem in pitDate angegebenen Zeitpunkt gelöscht wurden, werden nicht zurückgegeben. Beispiel:

```
Mo - ABC(1), DEF, GHI sichern
Di - ABC(2) sichern, DEF löschen
Do - ABC(3) sichern
```

Wenn Sie die Abfrage am Freitag mit einem Zeitpunktwert von Mittwoch 12:00:00 Uhr aufrufen, werden folgende Informationen zurückgegeben:

```
ABC(2) - eine inaktive Kopie
GHI    - eine aktive Kopie
```

Der Aufruf gibt DEF nicht zurück, weil dieses Objekt vor dem Zeitpunktwert gelöscht wurde.

qryABackupData

objName

Der vollständige Objektname. Sie können ein Platzhalterzeichen, wie beispielsweise einen Stern (*) oder ein Fragezeichen (?), verwenden, was sowohl für den übergeordneten als auch den untergeordneten Teil des Namens gilt. Ein Stern entspricht null oder mehr Zeichen; ein Fragezeichen entspricht einem Zeichen. Das Feld objType von objName kann einen der folgenden Werte haben:

- DSM_OBJ_FILE
- DSM_OBJ_DIRECTORY
- DSM_OBJ_ANY_TYPE

Weitere Informationen zu übergeordneten und untergeordneten Namen finden Sie hier: Übergeordnete und untergeordnete Namen.

qryFSData

fsName

Geben Sie in diesem Feld den Namen eines bestimmten Dateibereichs ein oder geben Sie einen Stern (*) ein, um Informationen zu allen registrierten Dateibereichen abzurufen.

qryMCData

mcName

Geben Sie den Namen einer bestimmten Verwaltungsklasse ein oder geben Sie eine leere Zeichenfolge (" ") ein, um Informationen zu allen Verwaltungsklassen abzurufen.
Anmerkung: Sie können keinen Stern (*) verwenden.

mcDetail

Gibt an, ob Informationen zu den Sicherungs- und Archivierungskopiengruppen der Verwaltungsklasse zurückgegeben werden. Die folgenden Werte sind gültig:

- bTrue
- bFalse

qryBackupGroup:

groupType

Der Gruppentyp ist DSM_GROUPTYPE_PEER.

fsName

Der Dateibereichsname.

Eigner

Die Eigner-ID.

groupLeaderObjId

Die Objekt-ID des Gruppenleiters.

objType
Der Objekttyp.

qryProxyNodeAuth:

targetNodeName

Der Zielknotenname.

peerNodeName

Der Peerknotenname.

hlAddress

Die Peeradresse des übergeordneten Namens.

llAddress

Die Peeradresse des untergeordneten Namens.

qryProxyNodePeer:

targetNodeName

Der Zielknotenname.

peerNodeName

Der Peerknotenname.

hlAddress

Die Peeradresse des übergeordneten Namens.

llAddress

Die Peeradresse des untergeordneten Namens.

Rückkehrcodes

In der folgenden Tabelle werden die Rückkehrcodes für den Funktionsaufruf dsmBeginQuery beschrieben.

Tabelle 1. Rückkehrcodes für dsmBeginQuery

Rückkehrcode	Rückkehrcodenummer	Erläuterung
DSM_RC_NO_MEMORY	102	Es ist nicht genug Speicher verfügbar, um die Anforderung auszuführen.
DSM_RC_FILE_SPACE_NOT_FOUND	124	Der angegebene Dateibereich wurde nicht gefunden.
DSM_RC_NO_POLICY_BLK	2007	Die Servermaßnahmeninformationen waren nicht verfügbar.
DSM_RC_INVALID_OBJTYPE	2010	Ungültiger Objekttyp.
DSM_RC_INVALID_OBJOWNER	2019	Ungültiger Objekteignername.
DSM_RC_INVALID_OBJSTATE	2024	Ungültige Objektbedingung.
DSM_RC_WRONG_VERSION_PARM	2065	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.

dsmBeginTxn

Mit dem Funktionsaufruf **dsmBeginTxn** werden eine oder mehrere IBM Spectrum Protect-Transaktionen gestartet, die eine vollständige Aktion starten; entweder werden alle Aktionen erfolgreich ausgeführt oder es wird keine Aktion erfolgreich ausgeführt. Eine Aktion kann entweder ein einzelner Aufruf oder eine Serie von Aufrufen sein. Beispielsweise kann ein Aufruf **dsmSendObj**, auf den eine Reihe von Aufrufen **dsmSendData** folgt, als eine einzige Aktion betrachtet werden. In ähnlicher Weise wird ein Aufruf **dsmSendObj** mit **dataBlkPtr**, der einen Datenbereich angibt, der das zu sichernde Objekt enthält, ebenso als eine einzige Aktion betrachtet.

Versuchen Sie, mehrere Objekte für Datenübertragungsoperationen in einer einzigen Transaktion zusammenzufassen. Das Zusammenfassen von Objekten hat deutliche Leistungsverbesserungen im IBM Spectrum Protect-System zur Folge. Sowohl aus der Perspektive des Clients als auch

aus der Perspektive des Servers bedeutet das Starten und Beenden jeder Transaktion einen gewissen Systemaufwand.

Die Ausführung einer einzigen Transaktion unterliegt bestimmten Einschränkungen. Diese Einschränkungen umfassen:

- Eine maximale Anzahl Objekte, die in einer einzigen Transaktion gesendet oder gelöscht werden können. Dieser Grenzwert ist in den Daten angegeben, die **dsmQuerySessInfo** im Feld *ApiSessInfo.maxObjPerTxn* zurückgibt. Dies entspricht der Serveroption *TxnGroupMax*.
- Alle Objekte, die in einer einzigen Transaktion an den Server gesendet werden (Sicherung oder Archivierung), müssen dasselbe Kopienziel haben, das in der Verwaltungsklassenbindung für das Objekt definiert ist. Dieser Wert ist in den Daten angegeben, die **dsmBindMC** im Feld **mcBindKey.backup_copy_dest** oder **mcBindKey.archive_copy_dest** zurückgibt.

Bei der API kann entweder der Anwendungsclient diese Einschränkungen überwachen und steuern oder die API kann diese Einschränkungen überwachen. Wenn die API Einschränkungen überwacht, wird der Anwendungsclient über entsprechende Rückkehrcodes von den API-Aufrufen benachrichtigt, wenn eine oder mehrere Einschränkungen erfüllt sind.

Geben Sie für einen Aufruf **dsmBeginTxn** auch immer einen Aufruf **dsmEndTxn** an, um die Gruppe von Aktionen in einem Paar aus Aufrufen **dsmBeginTxn** und **dsmEndTxn** zu optimieren.

Syntax

```
dsInt16_t dsmBeginTxn  (dsUint32_t dsmHandle);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmBeginTxn

Rückkehrcode	Erläuterung
DSM_RC_ABORT_NODE_NOT_AUTHORIZED (36)	FROMNODE oder FROMOWNER ist für TXN-Operationen nicht zulässig.

dsmBindMC

Mit den Funktionsaufruf **dsmBindMC** wird eine Verwaltungsklasse dem übergebenen Objekt zugeordnet bzw. an es gebunden. Das Objekt wird über die Einschluss-/Ausschlussliste übergeben, auf die in der Optionsdatei verwiesen wird. Wird in der Einschlussliste keine Übereinstimmung für eine bestimmte Verwaltungsklasse gefunden, wird die Standardverwaltungsklasse zugeordnet. Über die Ausschlussliste können Objekte von einer Sicherung ausgeschlossen werden, aber nicht von einer Archivierung.

Der Anwendungsclient kann mithilfe von Parametern, die in der Struktur `mcBindKey` zurückgegeben werden, bestimmen, ob dieses Objekt gesichert oder archiviert werden soll oder ob wegen unterschiedlicher Kopienziele eine neue Transaktion gestartet werden muss. Weitere Informationen finden Sie unter **dsmBeginTxn**.

Sie müssen **dsmBindMC** aufrufen, bevor Sie **dsmSendObj** aufrufen, da jedem Objekt eine Verwaltungsklasse zugeordnet werden muss. Dieser Aufruf kann innerhalb oder außerhalb einer Transaktion ausgeführt werden. Gibt beispielsweise in einer Transaktion mit mehreren Objekten **dsmBindMC** an, dass das Objekt ein anderes Kopienziel wie das vorherige Objekt hat, muss die Transaktion beendet und eine neue Transaktion gestartet werden. In diesem Fall ist kein weiterer Aufruf **dsmBindMC** erforderlich, da bereits ein derartiger Aufruf für dieses Objekt ausgeführt wurde.

Syntax

```
dsInt16_t dsmBindMC  (dsUint32_t       dsmHandle,
   dsmObjName            *objNameP,
   dsmSendType            sendType,
   mcBindKey   *mcBindKeyP);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

dsmObjName *objNameP (I)
: Ein Verweis auf die Struktur, die den Dateibereichsnamen, den übergeordneten Objektnamen, den untergeordneten Objektnamen und den Objekttyp enthält.

dsmSendType sendType (I)
: Gibt an, ob die Bindung dieser Verwaltungsklasse für Archivierungs- oder Sicherungssendeoperationen gilt. Gültige Werte für diesen Aufruf umfassen:

	Name	Beschreibung
	stBackup	Ein Sicherungsobjekt
	stArchive	Ein Archivierungsobjekt
	stBackupMountWait	Ein Sicherungsobjekt
	stArchiveMountWait	Ein Archivierungsobjekt

Für den Aufruf **dsmBindMC** sind `stBackup` und `stBackupMountWait` sowie `stArchive` und `stArchiveMountWait` funktional entsprechend.

mcBindKey *mcBindKeyP (O)
Dies ist die Adresse einer Struktur `mcBindKey`, in der die Verwaltungsklasseninformationen zurückgegeben werden. Der Anwendungsclient kann mithilfe der zurückgegebenen Informationen bestimmen, ob dieses Objekt für eine Transaktion mit mehreren Objekten geeignet ist oder ob eine Verwaltungsklassenabfrage für die an das Objekt gebundene Verwaltungsklasse ausgeführt werden soll.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmBindMC

Rückkehrcode	Erläuterung
DSM_RC_NO_MEMORY (102)	Es ist kein Arbeitsspeicher mehr verfügbar, um die Anforderung auszuführen.
DSM_RC_INVALID_PARM (109)	Einer der übergebenen Parameter hat einen ungültigen Wert.
DSM_RC_TL_EXCLUDED (185)	Das Sicherungsobjekt wurde ausgeschlossen und kann nicht gesendet werden.
DSM_RC_INVALID_OBJTYPE (2010)	Ungültiger Objekttyp.
DSM_RC_INVALID_SENDTYPE (2022)	Ungültiger Sendetyp.
DSM_RC_WRONG_VERSION_PARM (2065)	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.

dsmChangePW

Mit dem Funktionsaufruf **dsmChangePW** wird ein IBM Spectrum Protect-Kennwort geändert. Bei einem Mehrbenutzerbetriebssystem wie UNIX oder Linux kann dieser Aufruf nur vom Rootbenutzer oder vom berechtigten Benutzer verwendet werden.

Bei den Windows-Betriebssystemen können Sie das Kennwort in der Datei dsm.opt angeben. In diesem Fall wird die Datei dsm.opt nicht durch **dsmChangePW** aktualisiert. Nachdem der Aufruf **dsmChangePW** erfolgt ist, müssen Sie die Datei dsm.opt separat aktualisieren.

Dieser Aufruf muss erfolgreich verarbeitet werden, wenn **dsmInitEx** DSM_RC_VERIFIER_EXPIRED zurückgibt. Die Sitzung wird beendet, wenn der Aufruf **dsmChangePW** in dieser Situation fehlschlägt.

Wird **dsmChangePW** aus einem anderen Grund aufgerufen, bleibt die Sitzung unabhängig vom Rückkehrcode geöffnet.

Syntax

```
dsInt16_t dsmChangePW  (dsUint32_t   dsmHandle,
   char    *oldPW,
   char    *newPW);
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.
char *oldPW (I)
Das alte Kennwort des Aufrufenden. Die maximale Länge ist DSM_MAX_VERIFIER_LENGTH.
char *newPW (I)
Das neue Kennwort des Aufrufenden. Die maximale Länge ist DSM_MAX_VERIFIER_LENGTH.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmChangePW

Rückkehrcode	Erläuterung
DSM_RC_ABORT_BAD_VERIFIER (6)	Es wurde ein falsches Kennwort eingegeben.
DSM_RC_AUTH_FAILURE (137)	Authentifizierungsfehler. Das alte Kennwort ist falsch.
DSM_RC_NEWPW_REQD (2030)	Für das neue Kennwort muss ein Wert eingegeben werden.
DSM_RC_OLDPW_REQD (2031)	Für das alte Kennwort muss ein Wert eingegeben werden.
DSM_RC_PASSWD_TOOLONG (2103)	Das angegebene Kennwort ist zu lang.
DSM_RC_NEED_ROOT (2300)	Der Aufrufende der API muss ein Rootbenutzer oder ein berechtigter Benutzer sein.

dsmCleanUp

Der Funktionsaufruf **dsmCleanUp** wird verwendet, wenn **dsmSetUp** aufgerufen wurde. Der Funktionsaufruf **dsmCleanUp** sollte aufgerufen werden, nachdem **dsmTerminate** aufgerufen wurde. Nachdem **dsmCleanUp** aufgerufen wurde, können keine anderen Aufrufe erfolgen.

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

Syntax

```
dsInt16_t DSMLINKAGE dsmCleanUp
    (dsBool_t        mtFlag);
```

Parameter

dsBool_t mtFlag (I)
Dieser Parameter gibt an, dass die API in einem Einzelthread- oder in einem Multithread-Modus verwendet wurde. Gültige Werte umfassen:

- DSM_SINGLETHREAD
- DSM_MULTITHREAD

dsmDeleteAccess

Mit dem Funktionsaufruf **dsmDeleteAccess** werden aktuelle Berechtigungsregeln für Sicherungsversionen oder archivierte Kopien Ihrer Objekte gelöscht. Wenn Sie eine Berechtigungsregel löschen, entziehen Sie den Zugriff, den ein Benutzer auf alle in der Regel angegebenen Dateien hat.

Bei Verwendung von **dsmDeleteAccess** können Sie jeweils nur eine einzige Regel löschen. Rufen Sie die Regel-ID über den Befehl **dsmQueryAccess** ab.

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

Syntax

```
dsInt16_t DSMLINKAGE dsmDeleteAccess
             (dsUint32_t          dsmHandle,
              dsUint32_t          ruleNum) ;
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.
dsUint32_t ruleNum (I)
Die Regel-ID für die Zugriffsregel, die gelöscht wird. Dieser Wert wird mit einem Funktionsaufruf **dsmQueryAccess** abgerufen.

dsmDeleteFS

Mit dem Funktionsaufruf **dsmDeleteFS** wird ein Dateibereich aus dem Speicher gelöscht. Um einen Dateibereich löschen zu können, muss Ihnen der IBM Spectrum Protect-Administrator die korrekten Berechtigungen erteilen. Rufen Sie **dsmQuerySessInfo** auf, um zu bestimmen, ob Sie über die erforderlichen Berechtigungen verfügen. Dieser Funktionsaufruf gibt eine Datenstruktur des Typs *ApiSessInfo* zurück, die zwei Felder, *archDel* und *backDel*, enthält.

Anmerkung:

- Auf einem Betriebssystem UNIX oder Linux kann nur ein Rootbenutzer oder ein berechtigter Benutzer einen Dateibereich löschen.
- Wenn der Dateibereich, der gelöscht werden muss, Sicherungsversionen enthält, müssen Sie die Berechtigung zum Löschen von Sicherungen (***backDel*** = BACKDEL_YES) haben. Wenn der Dateibereich Archivierungskopien enthält, müssen Sie die Berechtigung zum

Löschen von Archivierungen (*archDel* = ARCHDEL_YES) haben. Wenn der Dateibereich sowohl Sicherungsversionen als auch Archivierungskopien enthält, müssen Sie beide Typen von Löschberechtigung haben.

- Bei der Verwendung eines Archivierungsmanagerservers kann ein Dateibereich nicht wirklich entfernt werden. Dieser Funktionsaufruf gibt selbst dann *rc=0* zurück, wenn der Dateibereich nicht wirklich gelöscht wurde. Die einzige Möglichkeit zur Überprüfung, ob der Dateibereich gelöscht wurde, ist die Ausgabe einer Dateibereichsabfrage an den Server.
- Die IBM Spectrum Protect-Serverfunktion zum Löschen von Dateibereichen ist ein Hintergrundprozess. Wenn außer den Fehlern, die vor der Übergabe eines Rückkehrcodes erkannt wurden, noch weitere Fehler auftreten, werden diese im Protokoll des IBM Spectrum Protect-Servers aufgezeichnet.

Syntax

```
dsInt16_t dsmDeleteFS   (dsUint32_t          dsmHandle,
   char           *fsName,
   unsigned char   repository);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

char *fsName (I)
: Ein Verweis auf den Namen des Dateibereichs, der gelöscht werden soll. Das Platzhalterzeichen ist nicht zulässig.

unsigned char repository (I)
: Gibt an, ob der zu löschende Dateibereich ein Sicherungsrepository und/oder ein Archivrepository ist. Gültige Werte für dieses Feld umfassen:

```
DSM_ARCHIVE_REP     /* Archivrepository     */
DSM_BACKUP_REP      /* Sicherungsrepository */
DSM_REPOS_ALL       /* alle Repository-Typen*/
```

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmDeleteFS

Rückkehrcode	Erläuterung
DSM_RC_ABORT_NOT_AUTHORIZED (27)	Sie haben nicht die erforderliche Berechtigung zum Löschen des Dateibereichs.
DSM_RC_INVALID_REPOS (2015)	Ungültiger Wert für Repository.
DSM_RC_FSNAME_NOTFOUND (2060)	Dateibereichsname nicht gefunden.
DSM_RC_NEED_ROOT (2300)	Der Aufrufende der API muss ein Rootbenutzer sein.

dsmDeleteObj

Mit dem Funktionsaufruf **dsmDeleteObj** werden Sicherungsobjekte inaktiviert oder gelöscht oder Archivierungsobjekte im Speicher gelöscht. Beim Typ **dtBackup** wird nur die momentan aktive Sicherungskopie inaktiviert. Beim Typ **dtBackupID** wird das Objekt mit der jeweils angegebenen Objekt-ID vom Server gelöscht. Rufen Sie diese Funktion innerhalb einer Transaktion auf.

Weitere Informationen finden Sie unter **dsmBeginTxn**.

Bevor Sie den Aufruf **dsmDeleteObj** senden, senden Sie die in IBM Spectrum Protect-System abfragen beschriebene Abfragefolge, um die Informationen für **delInfo** abzurufen. Der Aufruf **dsmGetNextQObj** gibt für Sicherungsabfragen eine Datenstruktur mit dem Namen **qryRespBackupData** und für Archivabfragen eine Datenstruktur mit dem Namen **qryRespArchiveData** zurück. Diese Datenstrukturen enthalten Informationen, die Sie für **delInfo** benötigen.

Der Wert von **maxObjPerTxn** gibt die maximale Anzahl Objekte an, die in einer einzigen Transaktion gelöscht werden können. Rufen Sie **dsmQuerySessInfo** auf, um diesen Wert abzurufen.

Tipp: Ihr Knoten muss die entsprechende, von Ihrem Administrator festgelegte Berechtigung haben. Um Archivierungsobjekte löschen zu können, müssen Sie die Berechtigung zum Löschen von Archivierungen haben. Um ein Sicherungsobjekt inaktivieren zu können, benötigen Sie keine Berechtigung zum Löschen von Sicherungen.

Syntax

```
dsInt16_t dsmDeleteObj  (dsUint32_t      dsmHandle,
   dsmDelType  delType,
   dsmDelInfo  delInfo)
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.
dsmDelType delType (I)
Gibt an, welcher Typ von Objekt (Sicherungs- oder Archivobjekt) gelöscht werden soll. Gültige Werte umfassen:

	Name	Beschreibung
	dtArchive	Das zu löschende Objekt wurde zuvor archiviert.
	dtBackup	Das zu inaktivierende Objekt wurde zuvor gesichert.
	dtBackupID	Das zu löschende Objekt wurde zuvor gesichert. Einschränkung: Wird dieser Löschtyp (**delType**) zusammen mit *objID* verwendet, wird das Sicherungsobjekt vom Server gelöscht. Ein Objekt kann nur von seinem Eigner gelöscht werden. Jede Version (aktiv oder inaktiv) eines Objekts kann gelöscht werden. Der Server gleicht die Versionen ab. Wird eine aktive Version eines Objekts gelöscht, wird die erste inaktive Version aktiv. Wird eine inaktive Version eines Objekts gelöscht, werden alle älteren Versionen vorverlegt. Der Knoten muss mit der Berechtigung **backDel** registriert sein.

dsmDelInfo delInfo (I)
Eine Struktur, deren Felder das Objekt identifizieren. Abhängig davon, ob das Objekt ein Sicherungsobjekt oder ein Archivierungsobjekt ist, sind die Felder unterschiedlich. Die Struktur zum Inaktivieren eines Sicherungsobjekts, `delBack`, enthält den Objektnamen und die Objektkopiengruppe. Die Struktur für ein Archivierungsobjekt, `delArch`, enthält die Objekt-ID.

Die Struktur zum Entfernen eines Sicherungsobjekts, `delBackID`, enthält die Objekt-ID.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmDeleteObj

Rückkehrcode	Erläuterung
DSM_RC_FS_NOT_REGISTERED (2061)	Dateibereichsname ist nicht registriert.
DSM_RC_WRONG_VERSION_PARM (2065)	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.

dsmEndGetData

Mit dem Funktionsaufruf **dsmEndGetData** wird eine **dsmBeginGetData**-Sitzung, mit der Objekte aus Speicher abgerufen werden, beendet.

Der Funktionsaufruf **dsmEndGetData** wird gestartet, nachdem alle Objekte, die zurückgeschrieben werden sollen, verarbeitet wurden, oder er beendet den Abrufprozess vorzeitig. Rufen Sie **dsmEndGetData** auf, um eine **dsmBeginGetData**-Sitzung zu beenden, bevor Sie die weitere Verarbeitung fortsetzen können.

Abhängig davon, wann **dsmEndGetData** aufgerufen wird, muss die API unter Umständen die Verarbeitung eines Teildatenstroms beenden, bevor der Prozess gestoppt werden kann. Der Aufrufende sollte daher keine sofortige Rückkehr von diesem Aufruf erwarten. Verwenden Sie **dsmTerminate**, wenn die Anwendung sofort die Sitzung schließen und die Zurückschreibung beenden muss.

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

Syntax

```
dsInt16_t dsmEndGetData  (dsUint32_t dsmHandle);
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

dsmEndGetDataEx

Mit dem Funktionsaufruf **dsmEndGetDataEx** wird die Gesamtanzahl gesendeter LAN-unabhängiger Byte angegeben. Er ist eine Erweiterung des Funktionsaufrufs **dsmEndGetData**.

Syntax

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

```
dsInt16_t dsmEndGetDataEx (dsmEndGetDataExIn_t * dsmEndGetDataExInP,
                           dsmEndGetDataExOut_t * dsmEndGetDataExOutP);
```

Parameter

dsmEndGetDataExIn_t *dsmEndGetDataExInP (I)
Übergibt den dsmHandle für "'Objekt abrufen' beenden", der die Sitzung identifiziert und nachfolgenden Aufrufen zuordnet.
dsmEndGetDataExOut_t *dsmEndGetDataExOutP (O)
Diese Struktur enthält diesen Eingabeparameter:

totalLFBytesRecv
Die Gesamtanzahl empfangener LAN-unabhängiger Byte.

dsmEndGetObj

Mit dem Funktionsaufruf **dsmEndGetObj** wird eine **dsmGetObj**-Sitzung, mit der Daten für ein bestimmtes Objekt abgerufen werden, beendet.

Starten Sie den Aufruf **dsmEndGetObj**, nachdem ein Datenende für das Objekt empfangen wurde. Dies gibt an, dass alle Daten empfangen wurden oder dass keine weiteren Daten für dieses Objekt empfangen werden. Bevor Sie einen weiteren Aufruf **dsmGetObj** starten können, müssen Sie **dsmEndGetObj** aufrufen.

Abhängig davon, wann **dsmEndGetObj** aufgerufen wird, muss die API unter Umständen die Verarbeitung eines Teildatenstroms beenden, bevor der Prozess gestoppt werden kann. Erwarten Sie keine sofortige Rückkehr von diesem Aufruf.

Syntax

```
dsInt16_t dsmEndGetObj  (dsUint32_t dsmHandle);
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmEndGetObj

Rückkehrcode	Erläuterung
DSM_RC_NO_MEMORY (102)	Es ist kein Arbeitsspeicher mehr verfügbar, um die Anforderung auszuführen.

dsmEndQuery

Mit dem Funktionsaufruf **dsmEndQuery** wird das Ende einer Aktion **dsmBeginQuery** angegeben. Der Anwendungsclient sendet einen Aufruf **dsmEndQuery**, um eine Abfrage abzuschließen. Dieser Aufruf wird entweder gesendet, nachdem alle Abfrageantworten über **dsmGetNextQObj** abgerufen wurden, oder er wird gesendet, um eine Abfrage zu beenden, bevor alle Daten zurückgegeben werden.

Tipp: IBM Spectrum Protect sendet in diesem Fall weiterhin Abfragedaten vom Server an den Client, die API löscht jedoch alle verbleibenden Daten.

Nachdem ein Aufruf **dsmBeginQuery** gesendet wurde, muss ein Aufruf **dsmEndQuery** gesendet werden, bevor irgendeine andere Aktivität gestartet werden kann.

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

Syntax

```
dsInt16_t dsmEndQuery  (dsUint32_t dsmHandle);
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

dsmEndSendObj

Mit dem Funktionsaufruf **dsmEndSendObj** wird das Ende der Daten angegeben, die in den Speicher gesendet werden.

Geben Sie den Funktionsaufruf **dsmEndSendObj** ein, um das Ende der Daten für die Aufrufe **dsmSendObj** und **dsmSendData** anzugeben. Erfolgt dies nicht, ist ein fehlerhaftes Protokoll die Folge. Eine Ausnahme von dieser Regel ist das Aufrufen von **dsmEndTxn** zum Beenden der Transaktion. Damit werden alle Daten, die für die Transaktion gesendet wurden, gelöscht.

Syntax

```
dsInt16_t dsmEndSendObj  (dsUint32_t dsmHandle);
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmEndSendObj

Rückkehrcode	Erläuterung
DSM_RC_NO_MEMORY (102)	Es ist kein Arbeitsspeicher mehr verfügbar, um diese Anforderung auszuführen.

dsmEndSendObjEx

Mit dem Funktionsaufruf **dsmEndSendObjEx** werden zusätzliche Informationen in Bezug auf die Anzahl verarbeiteter Byte bereitgestellt. Die Informationen umfassen: Gesamtanzahl gesendeter Byte, Komprimierungsangaben, LAN-unabhängige Byte und Angaben zur Deduplizierung.

Der Funktionsaufruf dsmEndSendObjEx ist eine Erweiterung des Funktionsaufrufs **dsmEndSendObj**.

Syntax

```
dsInt16_t dsmEndSendObjEx (dsmEndSendObjExIn_t  *dsmEndSendObjExInP,
                           dsmEndSendObjExOut_t *dsmEndSendObjExOutP);
```

Parameter

dsmEndSendObjExIn_t *dsmEndSendObjExInP (I)
Dieser Parameter übergibt den dsmHandle für "'Objekt senden' beenden", der die Sitzung identifiziert und nachfolgenden Aufrufen zuordnet.
dsmEndSendObjExOut_t *dsmEndSendObjExOutP (O)
Dieser Parameter übergibt die Informationen für "'Objekt senden' beenden":

	Name	Beschreibung
	totalBytesSent	Die Gesamtanzahl Byte, die von der Anwendung gelesen wird.
	objCompressed	Ein Flag, das anzeigt, ob das Objekt komprimiert wurde.
	totalCompressedSize	Die Gesamtgröße in Byte nach der Komprimierung.
	totalLFBytesSent	Die Gesamtanzahl gesendeter LAN-unabhängiger Byte.
	objDeduplicated	Ein Flag, das anzeigt, ob das Objekt von der API dedupliziert wurde.
	totalDedupSize	Gesamtanzahl gesendeter Byte nach der Deduplizierung.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmEndSendObjEx

Rückkehrcode	Erläuterung
DSM_RC_NO_MEMORY (102)	Es ist kein Arbeitsspeicher mehr verfügbar, um diese Anforderung auszuführen.

dsmEndTxn

Mit dem Funktionsaufruf dsmEndTxn wird eine IBM Spectrum Protect-Transaktion beendet. Geben Sie den Funktionsaufruf dsmEndTxn zusammen mit dsmBeginTxn an, um den Aufruf oder die Gruppe von Aufrufen, die als eine Transaktion betrachtet werden, zu identifizieren. Der Anwendungsclient kann im Aufruf dsmEndTxn angeben, ob die Transaktion festgeschrieben oder beendet werden muss.

Führen Sie alle folgenden Aufrufe innerhalb der Grenzen einer Transaktion aus:

- **dsmSendObj**
- **dsmSendData**
- **dsmEndSendObj**
- **dsmDeleteObj**

Syntax

```
dsInt16_t dsmEndTxn (dsUint32_t   dsmHandle,
   dsUint8_t    vote,
   dsUint16_t  *reason);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.

dsUint8_t vote (I)
: Gibt an, ob der Anwendungsclient alle Aktionen, die zwischen dem vorherigen Aufruf dsmBeginTxn und diesem Aufruf ausgeführt werden, festschreibt. Die folgenden Werte sind gültig:

```
DSM_VOTE_COMMIT     /* akt. Transaktion festschreiben*/
DSM_VOTE_ABORT      /* akt. Transakt. rückg. machen  */
```

Verwenden Sie `DSM_VOTE_ABORT` nur, wenn Ihre Anwendung einen Grund zum Stoppen der Transaktion findet.

dsUint16_t *reason (O)
: Wenn der Aufruf dsmEndTxn mit einem Fehler beendet wird oder der Wert von `vote` nicht akzeptiert wird, gibt der Ursachencode dieses Parameters an, warum das Votum fehlgeschlagen ist. Der Rückkehrcode für den Aufruf kann null sein, während der Ursachencode ungleich null sein kann. Daher muss der Anwendungsclient immer sowohl den Rückkehrcode als auch den Ursachencode (`if (rc || reason)`) auf Fehler überprüfen, bevor die Ausführung als erfolgreich betrachtet werden kann.

Wenn die Anwendung als Votum `DSM_VOTE_ABORT` angibt, ist der Ursachencode `DSM_RS_ABORT_BY_CLIENT (3)`. Eine Liste der möglichen Ursachencodes finden Sie in Quellendatei mit API-Rückkehrcodes: dsmrc.h. Die Zahlen 1 bis 50 in der Liste der Rückkehrcodes sind für die Ursachencodes reserviert. Wenn der Server die Transaktion beendet, ist der Rückkehrcode `DSM_RC_CHECK_REASON_CODE`. In diesem Fall enthält der Wert des Ursachencodes weitere Informationen zu der Ursache des Abbruchs.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmEndTxn

Rückkehrcode	Erläuterung
`DSM_RC_ABORT_CRC_FAILED (236)`	Das Befehlserkennungszeichen (CRC), das vom Server empfangen wurde, entspricht nicht dem CRC, das vom Client errechnet wurde.
`DSM_RC_INVALID_VOTE (2011)`	Der für `vote` angegebene Wert ist ungültig.
`DSM_RC_CHECK_REASON_CODE (2302)`	Die Transaktion wurde abgebrochen. Überprüfen Sie das Feld für die Ursache.
`DSM_RC_ABORT_STGPOOL_COPY_CONT_NO (241)`	Der Schreibvorgang in einen der Kopienspeicherpools ist fehlgeschlagen und die Option COPYCONTINUE für den IBM Spectrum Protect-Speicherpool ist auf NO gesetzt. Die Transaktion wird beendet.
`DSM_RC_ABORT_RETRY_SINGLE_TXN (242)`	Dieser Abbruchcode gibt an, dass die aktuelle Transaktion aufgrund eines Fehlers während einer Speicheroperation abgebrochen wurde. Der Fehler kann behoben werden, indem jede Datei in einer eigenen Transaktion gesendet wird. Dieser Fehler ist typisch bei folgenden Bedingungen: • Der nächste Speicherpool hat eine andere Kopienspeicherpoolliste. • Die Operation wechselt mitten in einer Transaktion zu diesem Pool. .

dsmEndTxnEx

Mit dem Funktionsaufruf **dsmEndTxnEx** werden Informationen zur Objekt-ID des Gruppenleiters zur Verwendung im Funktionsaufruf **dsmGroupHandler** bereitgestellt. Er ist eine Erweiterung des Funktionsaufrufs **dsmEndTxn**.

Syntax

```
dsInt16_t dsmEndTxnEx (dsmEndTxnExIn_t *dsmEndTxnExInP
                       dsmEndTxnExOut_t *dsmEndTxnExOutP);
```

Parameter

dsmEndTxnExIn_t *dsmEndTxnExInP (I)
Diese Struktur enthält die folgenden Parameter:

dsmHandle
Die Kennung, die die Sitzung identifiziert und nachfolgenden IBM Spectrum Protect-Aufrufen zuordnet.

dsUint8_t vote (I)
Gibt an, ob der Anwendungsclient alle Aktionen, die zwischen dem vorherigen Aufruf dsmBeginTxn und diesem Aufruf ausgeführt werden, festschreibt. Gültige Werte sind:

```
DSM_VOTE_COMMIT     /* akt. Transaktion festschreiben*/
DSM_VOTE_ABORT      /* akt. Transakt. rückg. machen  */
```

Verwenden Sie `DSM_VOTE_ABORT` nur, wenn von Ihrer Anwendung ein Grund zum Stoppen der Transaktion gefunden wurde.

dsmEndTxnExOut_t *dsmEndTxnExOutP (O)
Diese Struktur enthält die folgenden Parameter:

dsUint16_t *reason (O)
Wenn der Aufruf **dsmEndTxnEx** mit einem Fehler beendet wird oder der Wert von *vote* nicht akzeptiert wird, gibt der Ursachencode dieses Parameters an, warum das Votum fehlgeschlagen ist.
Tipp: Der Rückkehrcode für den Aufruf kann null sein, während der Ursachencode ungleich null sein kann. Daher muss der Anwendungsclient immer sowohl den Rückkehrcode als auch den Ursachencode (`if (rc || reason)`) auf Fehler überprüfen, bevor die Ausführung als erfolgreich betrachtet werden kann.

Wenn die Anwendung als Votum DSM_VOTE_ABORT angibt, ist der Ursachencode DSM_RS_ABORT_BY_CLIENT (3). Eine Liste der möglichen Ursachencodes finden Sie in Quellendatei mit API-Rückkehrcodes: dsmrc.h. Die Zahlen 1 bis 50 in der Liste der Rückkehrcodes sind für die Ursachencodes reserviert. Wenn der Server die Transaktion beendet, ist der Rückkehrcode DSM_RC_CHECK_REASON_CODE. In diesem Fall enthält der Wert des Ursachencodes weitere Informationen zu der Ursache des Abbruchs.

groupLeaderObjId
Die Objekt-ID des Gruppenleiters, die zurückgegeben wird, wenn das Flag DSM_ACTION_OPEN mit dem Aufruf **dsmGroupHandler** verwendet wird.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmEndTxnEx

Rückkehrcode	Erläuterung
DSM_RC_INVALID_VOTE (2011)	Der für 'vote' angegebene Wert ist ungültig.
DSM_RC_CHECK_REASON_CODE (2302)	Die Transaktion wurde abgebrochen. Überprüfen Sie das Feld für die Ursache.
DSM_RC_ABORT_STGPOOL_COPY_CONT_NO (241)	Der Schreibvorgang in einen der Kopienspeicherpools ist fehlgeschlagen und die Option COPYCONTINUE für den IBM Spectrum Protect-Speicherpool wurde auf NO gesetzt. Die Transaktion wird beendet.
DSM_RC_ABORT_RETRY_SINGLE_TXN (242)	Während einer Operation für gleichzeitiges Schreiben wird ein Objekt in der Transaktion an ein Ziel mit anderen Kopienspeicherpools gesendet. Beenden Sie die aktuelle Transaktion und senden Sie jedes Objekt erneut in einer eigenen Transaktion.

dsmGetData

Mit dem Funktionsaufruf **dsmGetData** wird ein Bytestrom mit Daten von IBM Spectrum Protect abgerufen und in den Puffer des Aufrufenden gestellt. Der Anwendungsclient ruft **dsmGetData** auf, wenn weitere Daten für den Empfang von einem vorherigen Aufruf **dsmGetObj** oder **dsmGetData** verfügbar sind.

Syntax

```
dsInt16_t dsmGetData  (dsUint32_t   dsmHandle,
   DataBlk *dataBlkPtr);
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.
DataBlk *dataBlkPtr (I/O)
Verweist auf eine Struktur, die sowohl einen Zeiger auf den Puffer für die Daten enthält, die empfangen werden, als auch einen Zeiger auf die Größe des Puffers. Bei der Rückkehr enthält diese Struktur die Anzahl tatsächlich übertragener Byte. Die Typdefinition finden Sie in Quellendateien für API-Typdefinitionen.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmGetData

Rückkehrcode	Erläuterung
DSM_RC_ABORT_INVALID_OFFSET (33)	Der Offset, der während des Abrufs eines Teilobjekts angegeben wurde, ist größer als die Länge des Objekts.
DSM_RC_ABORT_INVALID_LENGTH (34)	Die Länge, die während des Abrufs eines Teilobjekts angegeben wurde, ist größer als die Länge des Objekts oder der Offset addiert zur Länge liegt hinter dem Ende des Objekts.
DSM_RC_FINISHED (121)	Die Verarbeitung wurde beendet. Der letzte Puffer wurde empfangen. Überprüfen Sie `numBytes` auf das Datenvolumen und rufen Sie dann IBM Spectrum ProtectdsmEndGetObj auf.
DSM_RC_NULL_DATABLKPTR (2001)	Datenblockzeiger ist null.
DSM_RC_ZERO_BUFLEN (2008)	Puffergröße für Datenblockzeiger ist null.
DSM_RC_NULL_BUFPTR (2009)	Pufferzeiger für Datenblockzeiger ist null.
DSM_RC_WRONG_VERSION_PARM (2065)	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.
DSM_RC_MORE_DATA (2200)	Es sind keine weiteren Daten zum Abrufen verfügbar.

dsmGetBufferData

Mit dem Funktionsaufruf **dsmGetBufferData** wird ein Bytestrom mit Daten über einen Puffer von IBM Spectrum Protect empfangen. Nach jedem Aufruf muss die Anwendung die Daten kopieren und den Puffer über einen Aufruf **dsmReleaseBuffer** freigeben. Wenn die Anzahl Puffer, die von der Anwendung angehalten wurden, dem im Aufruf **dsmInitEx** für 'numTsmBuffers' angegebenen Wert entspricht, blockt die Funktion **dsmGetBufferData** das Senden von Daten, bis ein Aufruf **dsmReleaseBuffer** gesendet wird.

Syntax

```
dsInt16_t  dsmGetBufferData   (getDatatExIn_t        *dsmGetBufferDataExInP,
                               getDataExOut_t        *dsmGetBufferDataExOutP) ;
```

Parameter

getDataExIn_t * dsmGetBufferDataExInP (I)
Diese Struktur enthält den folgenden Eingabeparameter:

dsUint32_t dsmHandle
Die Kennung, die die Sitzung identifiziert und einem vorherigen Aufruf **dsmInitEx** zuordnet.

getDataExOut_t * dsmGetBufferDataExOutP (0)
Diese Struktur enthält die folgenden Ausgabeparameter:

dsUint8_t tsmBufferHandle(0)
Die Kennung, die den empfangenen Puffer identifiziert.
char *dataPtr(0)
Die Adresse, an die die Daten geschrieben wurden.
dsUint32_t numBytes(0)
Tatsächliche Anzahl Byte, die von IBM Spectrum Protect geschrieben wurde.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmGetBufferData

Rückkehrcode	Erläuterung
DSM_RC_BAD_CALL_SEQUENCE (2041)	Der Aufruf wurde nicht im korrekten Status ausgegeben.
DSM_RC_OBJ_ENCRYPTED (2049)	Diese Funktion kann nicht für verschlüsselte Objekte verwendet werden.
DSM_RC_OBJ_COMPRESSED (2048)	Diese Funktion kann nicht für komprimierte Objekte verwendet werden.
DSM_RC_BUFF_ARRAY_ERROR (2045)	Ein Pufferarrayfehler ist aufgetreten.

dsmGetNextQObj

Mit dem Funktionsaufruf dsmGetNextQObj wird die nächste Abfrageantwort von einem vorherigen Aufruf dsmBeginQuery abgerufen und in den Puffer des Aufrufenden gestellt.

Der Aufruf dsmGetNextQObj wird ein oder mehrmals gesendet. Bei jedem Aufruf der Funktion wird entweder ein einzelner Abfragesatz abgerufen oder ein Fehler oder der Ursachencode `DSM_RC_FINISHED` zurückgegeben. Wird `DSM_RC_FINISHED` zurückgegeben, sind keine weiteren Daten zu verarbeiten. Wenn alle Abfragedaten abgerufen wurden oder keine weiteren Abfragedaten benötigt werden, senden Sie den Aufruf dsmEndQuery, um den Abfrageprozess zu beenden.

Der Parameter dataBlkPtr muss auf einen Puffer verweisen, der mit dem Strukturtyp qryResp*Data definiert ist. Der Kontext, in dem dsmGetNextQObj aufgerufen wird, bestimmt den Strukturtyp für die Abfrageantwort.

Syntax

```
dsInt16_t dsmGetNextQObj (dsUint32_t   dsmHandle,
   DataBlk *dataBlkPtr);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.

DataBlk *dataBlkPtr (I/O)
: Verweist auf eine Struktur, die sowohl einen Zeiger auf den Puffer für die Daten enthält, die empfangen werden sollen, als auch einen Zeiger auf die Größe des Puffers. Dieser Puffer ist die Antwortstruktur des Typs qryResp*Data. Bei der Rückkehr enthält diese Struktur die Anzahl übertragener Byte. Die Struktur, die jedem Typ von Abfrage zugeordnet ist, wird in der folgenden Tabelle beschrieben. Weitere Informationen zur Typdefinition bei DataBlk finden Sie hier: Quellendateien für API-Typdefinitionen.

Tabelle 1. DataBlk-Zeigerstruktur

Abfrage	Antwortstruktur	Felder von besonderem Interesse
qtArchive	qryRespArchiveData	sizeEstimate Enthält den Wert, der in einem vorherigen Aufruf dsmSendObj übergeben wurde. mediaClass Kann den Wert `MEDIA_FIXED` haben, wenn sich das Objekt auf Platte befindet, oder den Wert `MEDIA_LIBRARY`, wenn sich das Objekt auf Band befindet. clientDeduplicated Gibt an, ob dieses Objekt vom Client dedupliziert wird.

Abfrage	Antwortstruktur	Felder von besonderem Interesse
qtBackup	qryRespBackupData	restoreOrderExt Hat den Typ `dsUint16_t`. Sortieren Sie anhand dieses Felds, wenn in einem Aufruf dsmBeginGetData mehrere Objekte zurückgeschrieben werden. Das API-Muster, `dapiqry.c`, enthält ein Beispiel für Sortiercode für diesen Aufruf. Ein Beispiel für das Sortieren finden Sie hier: Abbildung 1. sizeEstimate Enthält den Wert, der in einem vorherigen Aufruf dsmSendObj übergeben wurde. mediaClass Kann den Wert `MEDIA_FIXED` haben, wenn sich das Objekt auf Platte befindet, oder den Wert `MEDIA_LIBRARY`, wenn sich das Objekt auf Band befindet. clientDeduplicated Gibt an, ob dieses Objekt vom Client dedupliziert wird.
qtBackupActive	qryARespBackupData	
qtBackupGroups	qryRespBackupData	dsBool_t isGroupLeader Gibt, wenn wahr, an, dass es sich bei diesem Objekt um einen Gruppenleiter handelt.
qtOpenGroups	qryRespBackupData	dsBool_t isOpenGroup; Gibt, wenn wahr, an, dass diese Gruppe offen und nicht vollständig ist.
qtFilespace	qryRespFSData	backStartDate Enthält die Zeitmarke des Servers, die angibt, wann der Dateibereich mit der Aktion backStartDate aktualisiert wird. backCompleteDate Enthält die Zeitmarke des Servers, die angibt, wann der Dateibereich mit der Aktion backCompleteDate aktualisiert wird. lastReplStartDate Enthält die Zeitmarke für den letzten Start der Replikation auf dem Server. lastReplCmpltDate Enthält die Zeitmarke für die letzte Beendigung der Replikation, auch wenn es einen Fehler gab. lastBackOpDateFromServer Enthält die letzte Speicherungszeitmarke, die auf dem Server gespeichert wurde. lastBackOpDateFromLocal Enthält die letzte Speicherungszeitmarke, die auf dem Client gespeichert wurde.
qtMC	qryRespMCData qryRespMCDetailData	
qtProxyNodeAuth	qryRespProxyNodeData targetNodeName peerNodeName hlAddress llAddress	
qtProxyNodePeer	qryRespProaxyNodeData targetNodeName peerNodeName hlAddress llAddress	

Rückkehrcodes

In der folgenden Tabelle werden die Rückkehrcodes für den Funktionsaufruf dsmGetNextQObj beschrieben.

Tabelle 2. Rückkehrcodes für den Funktionsaufruf dsmGetNextQObj

Rückkehrcode	Rückkehrcodenummer	Beschreibung
DSM_RC_ABORT_NO_MATCH	2	Für die Abfrage wurde keine Übereinstimmung angefordert.
DSM_RC_FINISHED	121	Die Verarbeitung ist beendet (dsmEndQuery starten). Es sind keine weiteren Daten zu verarbeiten.
DSM_RC_UNKNOWN_FORMAT	122	Die Datei, die von IBM Spectrum Protect zurückgeschrieben oder abgerufen werden sollte, hat ein unbekanntes Format.
DSM_RC_COMM_PROTOCOL_ERROR	136	Übertragungsprotokollfehler.
DSM_RC_NULL_DATABLKPTR	2001	Zeiger verweist nicht auf einen Datenblock.
DSM_RC_INVALID_MCNAME	2025	Ungültiger Verwaltungsklassenname.
DSM_RC_BAD_CALL_SEQUENCE	2041	Die Aufruffolge ist ungültig.
DSM_RC_WRONG_VERSION_PARM	2065	Die Version der Anwendungsclient-API stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.
DSM_RC_MORE_DATA	2200	Es sind keine weiteren Daten zum Abrufen verfügbar.
DSM_RC_BUFF_TOO_SMALL	2210	Der Puffer ist zu klein.

dsmGetObj

Mit dem Funktionsaufruf **dsmGetObj** werden die angeforderten Objektdaten aus dem IBM Spectrum Protect-Datenstrom abgerufen und in den Puffer des Aufrufenden gestellt. Der Aufruf **dsmGetObj** verwendet die Objekt-ID, um das nächste Objekt oder das nächste Teilobjekt aus dem Datenstrom abzurufen.

Die Daten für das angegebene Objekt werden in den Puffer gestellt, auf den durch **DataBlk** verwiesen wird. Sind weitere Daten verfügbar, müssen Sie einen oder mehrere Aufrufe **dsmGetData** senden, um die verbleibenden Daten abzurufen, bis der Rückkehrcode DSM_RC_FINISHED zurückgegeben wird. Überprüfen Sie das Feld `numBytes` in **DataBlk**, um festzustellen, ob noch Daten im Puffer verblieben sind.

Die Objekte sollten in der Reihenfolge angefordert werden, in der sie im Aufruf **dsmBeginGetData** im Parameter **dsmGetList** aufgelistet sind. Eine Ausnahme von dieser Regel ist der Fall, wenn der Anwendungsclient ein Objekt in dem Datenstrom überspringen muss, um zu einem Objekt weiter hinten in der Liste zu gelangen. Handelt es sich bei dem Objekt, das durch die Objekt-ID angegeben wird, nicht um das nächste Objekt in dem Datenstrom, wird der Datenstrom verarbeitet, bis das Objekt lokalisiert oder der Datenstrom beendet ist. Diese Funktion sollte mit Bedacht eingesetzt werden, da möglicherweise ein großes Datenvolumen zum Lokalisieren des angeforderten Objekts verarbeitet und gelöscht werden muss.

Voraussetzung: Wenn **dsmGetObj** einen Fehlercode (NOT FINISHED oder MORE_DATA) zurückgibt, muss die Sitzung beendet werden, um die Zurückschreibungsoperation zu stoppen. Dies ist insbesondere dann wichtig, wenn Verschlüsselung verwendet und ein Rückkehrcode RC_ENC_WRONG_KEY empfangen wird. Sie müssen eine neue Sitzung mit dem korrekten Schlüssel starten.

Syntax

```
dsInt16_t dsmGetObj (dsUint32_t dsmHandle,
   ObjID    *objIdP,
   DataBlk  *dataBlkPtr);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

ObjID *objIdP (I)
: Ein Verweis auf die ID des Objekts, das zurückgeschrieben werden soll.

DataBlk *dataBlkPtr (I/O)
: Ein Verweis auf den Puffer, in den die zurückgeschriebenen Daten gestellt werden.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmGetObj

Rückkehrcode	Erläuterung

Rückkehrcode	Erläuterung
DSM_RC_ABORT_INVALID_OFFSET (33)	Der Offset, der während des Abrufs eines Teilobjekts angegeben wird, ist größer als die Länge des Objekts.
DSM_RC_ABORT_INVALID_LENGTH (34)	Die Länge, die während des Abrufs eines Teilobjekts angegeben wird, ist größer als die Länge des Objekts oder der Offset addiert zur Länge liegt hinter dem Ende des Objekts.
DSM_RC_FINISHED (121)	Die Verarbeitung ist beendet (**dsmEndGetObj** starten).
DSM_RC_WRONG_VERSION_PARM (2065)	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.
DSM_RC_MORE_DATA (2200)	Es sind keine weiteren Daten zum Abrufen verfügbar.
RC_ENC_WRONG_KEY (4580)	Der im Aufruf **dsmInitEx** angegebene Schlüssel oder der gespeicherte Schlüssel stimmt nicht mit dem Schlüssel überein, der zum Verschlüsseln dieses Objekts verwendet wurde. Beenden Sie die Sitzung und geben Sie den korrekten Schlüssel an.

dsmGroupHandler

Mit dem Funktionsaufruf **dsmGroupHandler** wird abhängig von der bereitgestellten Eingabe eine Aktion für eine logische Dateigruppe ausgeführt. Der Client fasst eine Reihe einzelner Objekte in einer Gruppe zusammen, um diese auf dem IBM Spectrum Protect-Server als logische Gruppe zu referenzieren und zu verwalten.

Weitere Informationen finden Sie in Dateigruppierung.

Syntax

```
dsInt16_t dsmGroupHandler (dsmGroupHandlerIn_t   *dsmGroupHandlerInP,
                           dsmGroupHandlerOut_t  *dsmGroupHandlerOutP);
```

Parameter

dsmGroupHandlerIn_t *dsmGroupHandlerInP (I)
Übergibt Gruppenattribute an die API.

groupType
Der Typ der Gruppe. Gültige Werte umfassen:

- DSM_GROUPTYPE_PEER - Peergruppe

actionType
Die Aktion, die ausgeführt werden soll. Gültige Werte umfassen:

- DSM_GROUP_ACTION_OPEN - erstellt eine neue Gruppe
- DSM_GROUP_ACTION_CLOSE - schreibt eine offene Gruppe fest und speichert sie
- DSM_GROUP_ACTION_ADD - fügt einer Gruppe ein Mitglied hinzu
- DSM_GROUP_ACTION_ASSIGNTO - ordnet ein Mitglied einer anderen Gruppe zu
- DSM_GROUP_ACTION_REMOVE - entfernt ein Mitglied aus der Gruppe

memberType
Der Gruppentyp des Objekts. Gültige Werte umfassen:

- DSM_MEMBERTYPE_LEADER - Gruppenleiter
- DSM_MEMBERTYPE_MEMBER - Gruppenmitglied

*uniqueGroupTagP
Eine eindeutige Zeichenfolge-ID, die einer Gruppe zugeordnet ist.
leaderObjId
Die Objekt-ID für den Gruppenleiter.
*objNameP
Ein Verweis auf den Objektnamen des Gruppenleiters.
memberObjList
Eine Liste der Objekte, die entfernt oder zugeordnet werden sollen.

dsmGroupHandlerOut_t *dsmGroupHandlerOutP (O)
Übergibt die Adresse der Struktur, die die API ausführt. Die Strukturversionsnummer wird zurückgegeben.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmGroupHandler

Rückkehrcode	Erläuterung
DSM_RC_ABORT_INVALID_GROUP_ACTION (237)	Es wurde versucht, eine ungültige Operation für einen Gruppenleiter oder ein Gruppenmitglied auszuführen.

dsmInit

Mit dem Funktionsaufruf **dsmInit** wird eine API-Sitzung gestartet und der Client mit IBM Spectrum Protect-Speicher verbunden. Für den Anwendungsclient kann jeweils nur eine einzige Sitzung zu einem bestimmten Zeitpunkt aktiv sein. Um eine weitere Sitzung mit anderen Parametern zu öffnen, beenden Sie die aktuelle Sitzung zunächst mit dem Aufruf **dsmTerminate**.

Um die knotenübergreifende Abfrage sowie die Zurückschreibung oder den Abruf zu ermöglichen, verwenden Sie die Zeichenfolgeoptionen -*fromnode* und -*fromowner*. Weitere Informationen finden Sie in Knoten- und eignerübergreifender Zugriff auf Objekte.

Syntax

```
dsInt16_t  dsmInit  (dsUint32_t        *dsmHandle,
   dsmApiVersion *dsmApiVersionP,
   char          *clientNodeNameP,
   char          *clientOwnerNameP,
   char          *clientPasswordP,
   char          *applicationType,
   char          *configfile,
   char          *options);
```

Parameter

dsUint32_t *dsmHandle (O)
: Die Kennung, die diese Initialisierungssitzung identifiziert und nachfolgenden IBM Spectrum Protect-Aufrufen zuordnet.

dsmApiVersion *dsmApiVersionP (I)
: Ein Verweis auf die Datenstruktur, die die Version der API identifiziert, die der Anwendungsclient für diese Sitzung verwendet. Die Struktur enthält die Werte der drei Konstanten DSM_API_VERSION, DSM_API_RELEASE und DSM_API_LEVEL, die in der Datei dsmapitd.h definiert sind. Ein vorheriger Aufruf **dsmQueryApiVersion** muss ausgeführt werden, um sicherzustellen, dass zwischen der API-Version des Anwendungsclients und der Version der API-Bibliothek, die auf der Workstation des Benutzers installiert ist, Kompatibilität besteht.

char *clientNodeNameP (I)
: Dieser Parameter ist ein Verweis auf den Knoten für die IBM Spectrum Protect-Sitzung. Allen Sitzungen muss ein Knotenname zugeordnet sein. Mit der Konstanten DSM_MAX_NODE_LENGTH in der Datei dsmapitd.h wird die maximale Größe festgelegt, die für einen Knotennamen zulässig ist.

  Beim Knotennamen muss die Groß-/Kleinschreibung nicht beachtet werden.

  Wenn dieser Parameter auf NULL und die Option *passwordaccess* auf *prompt* gesetzt wird, versucht die API, den Knotennamen zunächst aus der übergebenen Optionszeichenfolge abzurufen. Ist er dort nicht vorhanden, versucht die API anschließend, den Knotennamen aus der Konfigurationsdatei oder der Optionsdatei abzurufen. Schlagen diese Versuche, den Knotennamen zu finden, fehl, verwendet die UNIX- oder Linux-API den Systemhostnamen, während die APIs unter anderen Betriebssystemen den Code DSM_RC_REJECT_ID_UNKNOWN zurückgeben.

  Dieser Parameter muss NULL sein, wenn die Option *passwordaccess* in der Datei dsm.sys auf *generate* gesetzt ist. Die API verwendet den Systemhostnamen.

char *clientOwnerNameP (I)
: Dieser Parameter ist ein Verweis auf den Eigner der IBM Spectrum Protect-Sitzung. Wenn das Betriebssystem, unter dem die Sitzung gestartet wird, ein Mehrbenutzerbetriebssystem ist, hat der Eignername NULL (der Rootbenutzer) die Berechtigung zum Sichern, Archivieren, Zurückschreiben oder Abrufen von Objekten, die zu der Anwendung gehören, unabhängig vom Eigner des Objekts.

  Beim Eignernamen muss die Groß-/Kleinschreibung beachtet werden.

  Dieser Parameter muss NULL sein, wenn die Option *passwordaccess* in der Datei dsm.sys auf *generate* gesetzt ist. Die API verwendet dann die Anmelde-Benutzer-ID.

  Anmerkung: Wenn bei einem Mehrbenutzerbetriebssystem die Option *passwordaccess* auf *prompt* wird, muss der Eignername nicht mit der ID des aktiven Benutzers der Sitzung übereinstimmen, die die Anwendung ausführt.

char *clientPasswordP (I)
: Dieser Parameter ist ein Verweis auf das Kennwort des Knotens, in dem die IBM Spectrum Protect-Sitzung ausgeführt wird. Mit der Konstanten DSM_MAX_VERIFIER_LENGTH in der Datei dsmapitd.h wird die maximale Größe festgelegt, die für ein Kennwort zulässig ist.

  Beim Kennwort muss die Groß-/Kleinschreibung nicht beachtet werden.

Außer wenn die Kennwortdatei zuerst gestartet wird, wird der Wert dieses Parameters ignoriert, wenn die Option *passwordaccess* auf *generate* gesetzt ist.

char *applicationType (I)
Dieser Parameter identifiziert die Anwendung, die die Sitzung ausführt. Der Wert wird vom Anwendungsclient definiert.

Jedes Mal, wenn ein API-Anwendungsclient eine Sitzung mit dem Server startet, wird der Anwendungstyp (bzw. die Plattform) des Clients auf dem Server aktualisiert. Der Wert für den Anwendungstyp sollte eine Abkürzung für das Betriebssystem enthalten, da dieser Wert in das Feld **platform** auf dem Server eingegeben wird. Die maximale Länge für die Zeichenfolge ist DSM_MAX_PLATFORM_LENGTH.

Der aktuelle Wert für den Anwendungstyp kann mithilfe von **dsmQuerySessInfo** angezeigt werden.

char *configfile (I)
Dieser Parameter verweist auf eine Zeichenfolge, die den vollständig qualifizierten Namen einer API-Konfigurationsdatei enthält. Optionen, die in der API-Konfigurationsdatei angegeben werden, überschreiben die entsprechende Angabe in der Clientoptionsdatei. Optionsdateien werden beim Installieren von IBM Spectrum Protect (Client oder API) installiert.
char *options (I)
Verweist auf eine Zeichenfolge, die Benutzeroptionen wie die folgenden enthalten kann:

- *Compressalways*
- *Servername* (nur UNIX oder Linux)
- *TCPServeraddr*
- *Fromnode*
- *Fromowner*
- *EnableClientEncryptKey*

Der Anwendungsclient kann die Werte für diese Optionen, die in der Konfigurationsdatei definiert sind, mithilfe der Optionsliste überschreiben.

Die Optionen haben das folgende Format:

1. Jede Option, die in der Optionsliste angegeben ist, beginnt mit einem Gedankenstrich (-) gefolgt vom Optionsschlüsselwort.
2. Auf das Schlüsselwort wiederum folgt ein Gleichheitszeichen (=) gefolgt vom Optionsparameter.
3. Wenn der Optionsparameter ein Leerzeichen enthält, schließen Sie den Parameter in Hochkommas oder Anführungszeichen ein.
4. Wenn mehrere Optionen angegeben werden, trennen Sie die einzelnen Optionen jeweils durch ein Leerzeichen voneinander.

Wenn Optionen NULL sind, werden die Werte für alle Optionen aus der Benutzeroptionsdatei oder der API-Konfigurationsdatei übernommen.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmInit

Rückkehrcode	Erläuterung
DSM_RC_ABORT_SYSTEM_ERROR (1)	Der Server hat einen Systemfehler erkannt und die Clients benachrichtigt.
DSM_RC_REJECT_VERIFIER_EXPIRED (52)	Das Kennwort ist abgelaufen und muss aktualisiert werden.
DSM_RC_REJECT_ID_UNKNOWN (53)	Der Knotenname konnte nicht gefunden werden.
DSM_RC_AUTH_FAILURE (137)	Es ist ein Authentifizierungsfehler aufgetreten.
DSM_RC_NO_STARTING_DELIMITER (148)	Das Muster enthält keinen Startbegrenzer.
DSM_RC_NEEDED_DIR_DELIMITER (149)	Direkt vor und hinter der Metazeichenfolge ("...") für den "Verzeichnisabgleich" ist ein Verzeichnisbegrenzer erforderlich, es wurde jedoch keiner gefunden.
DSM_RC_NO_PASS_FILE (168)	Die Kennwortdatei ist nicht verfügbar.
DSM_RC_UNMATCHED_QUOTE (177)	Die Optionszeichenfolge enthält ein Anführungszeichen ohne Entsprechung.
DSM_RC_NLS_CANT_OPEN_TXT (0610)	Die Nachrichtentextdatei kann nicht geöffnet werden.
DSM_RC_INVALID_OPT (400)	Ein Eintrag in der Optionszeichenfolge ist ungültig.
DSM_RC_INVALID_DS_HANDLE (2014)	Ungültige DSM-Kennung.
DSM_RC_NO_OWNER_REQD (2032)	Der Eignerparameter muss NULL sein, wenn die Option *passwordaccess* auf *generate* gesetzt ist.
DSM_RC_NO_NODE_REQD (2033)	Der Knotenparameter muss NULL sein, wenn die Option *passwordaccess* auf *generate* gesetzt ist.
DSM_RC_WRONG_VERSION (2064)	Die API-Version für den Anwendungsclient hat einen höheren Wert als die Version von IBM Spectrum Protect.

Rückkehrcode	Erläuterung
DSM_RC_PASSWD_TOOLONG (2103)	Das angegebene Kennwort ist zu lang.
DSM_RC_NO_OPT_FILE (2220)	Es konnte keine Konfigurationsdatei lokalisiert werden.
DSM_RC_INVALID_KEYWORD (2221)	Ein in einer Optionszeichenfolge angegebenes Schlüsselwort ist ungültig.
DSM_RC_PATTERN_TOO_COMPLEX (2222)	Das Einschluss-/Ausschlussmuster ist zu komplex und kann daher nicht von IBM Spectrum Protect interpretiert werden.
DSM_RC_NO_CLOSING_BRACKET (2223)	Im Muster fehlt die rechte eckige Klammer.
DSM_RC_INVALID_SERVER (2225)	Für eine Mehrplatzsystemumgebung wurde der Server in der Systemkonfigurationsdatei nicht gefunden.
DSM_RC_NO_HOST_ADDR (2226)	Nicht genügend Informationen, um die Verbindung zum Host herzustellen.
DSM_RC_MACHINE_SAME (2227)	Der Knotenname, der in der Optionsdatei definiert ist, darf nicht mit dem Systemhostnamen übereinstimmen.
DSM_RC_NO_API_CONFIGFILE (2228)	Die Konfigurationsdatei kann nicht geöffnet werden.
DSM_RC_NO_INCLEXCL_FILE (2229)	Die Einschluss-/Ausschlussdatei wurde nicht gefunden.
DSM_RC_NO_SYS_OR_INCLEXCL (2230)	Die Datei dsm.sys oder die Einschluss-/Ausschlussdatei wurde nicht gefunden.

Zugehörige Konzepte:
Übersicht über die Clientoptionsdatei
Verarbeitungsoptionen

dsmInitEx

Mit dem Funktionsaufruf dsmInitEx wird eine API-Sitzung gestartet, wobei die zusätzlichen Parameter für die erweiterte Prüfung verwendet werden.

Syntax

```
dsInt16_t  dsmInitEx   (dsUint32_t        *dsmHandleP,
                        dsmInitExIn_t     *dsmInitExInP,
                        dsmInitExOut_t    *dsmInitExOutP) ;
```

Parameter

dsUint32_t *dsmHandleP (O)
Die Kennung, die diese Initialisierungssitzung identifiziert und nachfolgenden IBM Spectrum Protect-Aufrufen zuordnet.

dsmInitExIn_t *dsmInitExInP
Diese Struktur enthält die folgenden Eingabeparameter:

dsmApiVersion *dsmApiVersionP (I)
Dieser Parameter ist ein Verweis auf die Datenstruktur, die die Version der API identifiziert, die der Anwendungsclient für diese Sitzung verwendet. Die Struktur enthält die Werte für die vier Konstanten DSM_API_VERSION, DSM_API_RELEASE, DSM_API_LEVEL und DSM_API_SUBLEVEL, die in der Datei dsmapitd.h definiert werden. Rufen Sie dsmQueryApiVersionEx auf und stellen Sie sicher, dass die API-Version des Anwendungsclients und die Version der API-Bibliothek, die auf der Workstation des Benutzers installiert ist, kompatibel sind.

char *clientNodeNameP (I)
Dieser Parameter ist ein Verweis auf den Knoten für die IBM Spectrum Protect-Sitzung. Alle Sitzungen müssen einem Knotennamen zugeordnet sein. Die Konstante DSM_MAX_NODE_LENGTH in der Datei dsmapitd.h legt die maximale Größe für einen Knotennamen fest.

Beim Knotennamen muss die Groß-/Kleinschreibung nicht beachtet werden.

Wenn dieser Parameter auf NULL und die Option passwordaccess auf prompt gesetzt wird, versucht die API, den Knotennamen zunächst aus der übergebenen Optionszeichenfolge abzurufen. Ist er dort nicht vorhanden, versucht die API anschließend, den Knotennamen aus der Konfigurationsdatei oder der Optionsdatei abzurufen. Schlagen diese Versuche, den Knotennamen zu finden, fehl, verwendet die UNIX- oder Linux-API den Systemhostnamen, während die APIs unter anderen Betriebssystemen `DSM_RC_REJECT_ID_UNKNOWN` zurückgeben.

Dieser Parameter muss NULL sein, wenn die Option passwordaccess in der Datei dsm.sys auf generate gesetzt ist. Die API verwendet dann den Systemhostnamen.

char *clientOwnerNameP (I)
Dieser Parameter ist ein Verweis auf den Eigner der IBM Spectrum Protect-Sitzung. Wenn das Betriebssystem eine Mehrbenutzerplattform ist, hat der Eignername NULL (der Rootbenutzer) die Berechtigung zum Sichern, Archivieren, Zurückschreiben oder Abrufen von Objekten, die zu der Anwendung gehören, unabhängig vom Eigner des Objekts.

Beim Eignernamen muss die Groß-/Kleinschreibung beachtet werden.

Dieser Parameter muss NULL sein, wenn die Option passwordaccess in der Datei dsm.sys auf generate gesetzt ist. Die API verwendet dann die Anmelde-Benutzer-ID.

Tipp: Wenn bei einer Mehrbenutzerplattform die Option passwordaccess auf prompt gesetzt wird, muss der Eignername nicht mit der ID des aktiven Benutzers der Sitzung übereinstimmen, die die Anwendung ausführt.

char *clientPasswordP (I)
Ein Verweis auf das Kennwort des Knotens, in dem die IBM Spectrum Protect-Sitzung ausgeführt wird. Mit der Konstanten DSM_MAX_VERIFIER_LENGTH in der Datei dsmapitd.h wird die maximale Größe festgelegt, die für ein Kennwort zulässig ist.

Beim Kennwort muss die Groß-/Kleinschreibung nicht beachtet werden.

Außer wenn die Kennwortdatei zuerst gestartet wird, wird der Wert dieses Parameters ignoriert, wenn die Option passwordaccess auf generate gesetzt ist.

char *userNameP;
Ein Verweis auf den Namen des Benutzers mit Verwaltungsaufgaben, der über Clientberechtigung für diesen Knoten verfügt.

char *userPasswordP;
Ein Verweis auf das Kennwort für den Parameter userName, sofern ein Wert angegeben ist.

char *applicationType (I)
Identifiziert die Anwendung, die die IBM Spectrum Protect-Sitzung ausführt. Der Anwendungsclient identifiziert den Wert.

Jedes Mal, wenn ein API-Anwendungsclient eine Sitzung mit dem Server startet, wird der Anwendungstyp (bzw. das Betriebssystem) des Clients auf dem Server aktualisiert. Der Wert wird in das Feld platform auf dem Server eingegeben. Ziehen Sie die Verwendung einer Betriebssystem-ID im Wert in Betracht. Die maximale Länge der Zeichenfolge wird in der Konstanten DSM_MAX_PLATFORM_LENGTH definiert.

Der aktuelle Wert für den Anwendungstyp kann mithilfe von dsmQuerySessInfo angezeigt werden.

char *configfile (I)
Verweist auf eine Zeichenfolge, die den vollständig qualifizierten Namen einer API-Konfigurationsdatei enthält. Optionen, die in der API-Konfigurationsdatei angegeben werden, überschreiben die entsprechende Angabe in der Clientoptionsdatei. Optionsdateien werden beim Installieren von IBM Spectrum Protect (Client oder API) installiert.

char *options (I)
Verweist auf eine Zeichenfolge, die Benutzeroptionen wie die folgenden enthalten kann:

- Compressalways
- Servername (nur UNIX- und Linux-Systeme)
- TCPServeraddr (nicht für UNIX-Systeme)
- Fromnode
- Fromowner

Der Anwendungsclient kann die Werte für diese Optionen, die in der Konfigurationsdatei definiert sind, mithilfe der Optionsliste überschreiben.

Optionen weisen das folgende Format auf:

1. Jede Option, die in der Optionsliste angegeben ist, beginnt mit einem Gedankenstrich (-) gefolgt vom Optionsschlüsselwort.
2. Auf das Schlüsselwort folgt ein Gleichheitszeichen (=) und dann der Optionsparameter.
3. Wenn der Optionsparameter ein Leerzeichen enthält, schließen Sie den Parameter in Hochkommas oder Anführungszeichen ein.
4. Wenn mehrere Optionen angegeben werden, trennen Sie die einzelnen Optionen jeweils durch ein Leerzeichen voneinander.

Wenn Optionen NULL sind, werden die Werte für alle Optionen aus der Benutzeroptionsdatei oder der API-Konfigurationsdatei übernommen.

dirDelimiter
Der Verzeichnisbegrenzer, der als Präfix vor Dateibereichsnamen, übergeordneten und untergeordneten Namen angegeben wird. Sie müssen den Parameter dirDelimiter nur angeben, wenn die Anwendung die Systemstandardwerte überschreibt. In einer UNIX- oder Linux-Umgebung bildet der Schrägstrich (/) den Standardwert. In einer Windows-Umgebung bildet der umgekehrte Schrägstrich (\) den Standardwert.

useUnicode
Ein boolesches Flag, das angibt, ob Unicode aktiviert ist. Das Flag useUnicode muss auf false gesetzt sein, um die plattformübergreifende Interoperabilität zwischen UNIX- und Windows-Systemen zu ermöglichen.

bCrossPlatform
Ein boolesches Flag, das gesetzt werden muss (bTrue), um plattformübergreifende Interoperabilität zwischen UNIX- und Windows-Systemen zu ermöglichen. Wenn das Flag bCrossPlatform gesetzt ist, stellt die API sicher, dass für die Dateibereiche nicht Unicode verwendet wird und die Anwendung nicht Unicode verwendet. Eine Windows-Anwendung, die Unicode verwendet, ist nicht mit Anwendungen kompatibel, die Nicht-Unicode-Codierungen verwenden. Das Flag bCrossPlatform darf nicht für eine Windows-Anwendung gesetzt werden, die Unicode verwendet.

UseTsmBuffers

Gibt an, ob die Pufferkopieneliminierung verwendet werden soll.

numTsmBuffers
: Anzahl Puffer, wenn `useTsmBuffers=bTrue` gesetzt ist.

bEncryptKeyEnabled
: Gibt an, ob Verschlüsselung mit anwendungsverwaltetem Schlüssel verwendet wird.

encryptionPasswordP
: Das Verschlüsselungskennwort.
Einschränkung: Wenn `encryptkey=save` gesetzt und ein Verschlüsselungsschlüssel vorhanden ist, wird der in encryptionPasswordP angegebene Wert ignoriert.

dsmAppVersion *appVersionP (I)
: Dieser Parameter ist ein Verweis auf die Datenstruktur, die die Versionsinformationen der Anwendung enthält, die eine API-Sitzung startet. Die Struktur enthält die Werte für die vier Konstanten applicationVersion, applicationRelease, applicationLevel und applicationSubLevel, die in der Datei tsmapitd.h definiert werden.

dsmInitExOut_t *dsmInitExOut P
: Diese Struktur enthält die Ausgabeparameter.

dsUint32_t *dsmHandle (0)
: Die Kennung, die diese Initialisierungssitzung identifiziert und nachfolgenden API-Aufrufen zuordnet.

infoRC
: Zusätzliche Informationen zum Rückkehrcode. Überprüfen Sie sowohl den Funktionsrückkehrcode als auch den Wert von infoRC. Wenn infoRC den Wert DSM_RC_REJECT_LASTSESS_CANCELED (69) hat, gibt IBM Spectrum Protect an, dass der Administrator die letzte Sitzung abgebrochen hat.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmInitEx

Rückkehrcode	Erläuterung
DSM_RC_ABORT_SYSTEM_ERROR (1)	Der IBM Spectrum Protect-Server hat einen Systemfehler erkannt und die Clients benachrichtigt.
DSM_RC_REJECT_VERIFIER_EXPIRED (52)	Das Kennwort ist abgelaufen und muss aktualisiert werden. Der nächste Aufruf muss dsmChangePW sein und in diesem Aufruf muss die Kennung zurückgegeben werden.
DSM_RC_REJECT_ID_UNKNOWN (53)	Der Knotenname wurde nicht gefunden.
DSM_RC_TA_COMM_DOWN (103)	Die Datenübertragungsverbindung ist inaktiv.
DSM_RC_AUTH_FAILURE (137)	Es ist ein Authentifizierungsfehler aufgetreten.
DSM_RC_NO_STARTING_DELIMITER (148)	Das Muster enthält keinen Startbegrenzer.
DSM_RC_NEEDED_DIR_DELIMITER (149)	Direkt vor und hinter der Metazeichenfolge ("...") für den "Verzeichnisabgleich" ist ein Verzeichnisbegrenzer erforderlich, es wurde jedoch keiner gefunden.
DSM_RC_NO_PASS_FILE (168)	Die Kennwortdatei ist nicht verfügbar.
DSM_RC_UNMATCHED_QUOTE (177)	Die Optionszeichenfolge enthält ein Anführungszeichen ohne Entsprechung.
DSM_RC_NLS_CANT_OPEN_TXT (0610)	Die Nachrichtentextdatei kann nicht geöffnet werden.
DSM_RC_INVALID_OPT (2013)	Ein Eintrag in der Optionszeichenfolge ist ungültig.
DSM_RC_INVALID_DS_HANDLE (2014)	Ungültige DSM-Kennung.
DSM_RC_NO_OWNER_REQD (2032)	Der Eignerparameter muss NULL sein, wenn die Option passwordaccess auf generate gesetzt ist.
DSM_RC_NO_NODE_REQD (2033)	Der Knotenparameter muss NULL sein, wenn passwordaccess auf 'generate' gesetzt ist.
DSM_RC_WRONG_VERSION (2064)	Die API-Version des Anwendungsclients hat einen höheren Wert als die Version von IBM Spectrum Protect.
DSM_RC_PASSWD_TOOLONG (2103)	Das angegebene Kennwort ist zu lang.
DSM_RC_NO_OPT_FILE (2220)	Es wurde keine Konfigurationsdatei gefunden.
DSM_RC_INVALID_KEYWORD (2221)	Ein in einer Optionszeichenfolge angegebenes Schlüsselwort ist ungültig.
DSM_RC_PATTERN_TOO_COMPLEX (2222)	Das Einschluss-/Ausschlussmuster ist zu komplex und kann daher nicht von IBM Spectrum Protect interpretiert werden.
DSM_RC_NO_CLOSING_BRACKET (2223)	Im Muster fehlt die rechte eckige Klammer.
DSM_RC_INVALID_SERVER (2225)	Für eine Mehrplatzsystemumgebung wurde der Server in der Systemkonfigurationsdatei nicht gefunden.

Rückkehrcode	Erläuterung
DSM_RC_NO_HOST_ADDR (2226)	Nicht genügend Informationen, um die Verbindung zum Host herzustellen.
DSM_RC_MACHINE_SAME (2227)	Der Knotenname, der in der Optionsdatei definiert ist, darf nicht mit dem Systemhostnamen übereinstimmen.
DSM_RC_NO_API_CONFIGFILE (2228)	Die Konfigurationsdatei kann nicht geöffnet werden.
DSM_RC_NO_INCLEXCL_FILE (2229)	Die Einschluss-/Ausschlussdatei wurde nicht gefunden.
DSM_RC_NO_SYS_OR_INCLEXCL (2230)	Die Datei dsm.sys oder die Einschluss-/Ausschlussdatei wurde nicht gefunden.

Zugehörige Konzepte:
Übersicht über die Clientoptionsdatei
Verarbeitungsoptionen

dsmLogEvent

Mit dem Funktionsaufruf **dsmLogEvent** wird eine Benutzernachricht (ANE4991I) in der Serverprotokolldatei und/oder im lokalen Fehlerprotokoll protokolliert. Eine Struktur des Typs **logInfo** wird in dem Aufruf übergeben. Dieser Aufruf muss während des Zustands **InSession** innerhalb einer Sitzung ausgeführt werden. Er darf nicht in einer Sende-, Abruf- oder Abfrageoperation ausgeführt werden. Um Nachrichten abzurufen, die auf dem Server protokolliert sind, verwenden Sie den Befehl **query actlog** über den Verwaltungsclient.

Siehe das Zusammenfassungszustandsdiagramm, Abbildung 1.

Syntax

```
dsInt16_t dsmLogEvent
     (dsUint32_t    dsmHandle,
     logInfo        *logInfoP);
```

Parameter

dsUint32_t dsmHandle(I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.
logInfo *logInfoP (I)
Übergibt die Nachricht und das Ziel. Der Anwendungsclient ist für das Zuordnen von Speicher für die Struktur zuständig.
Die Struktur **logInfo** enthält folgende Felder:

message
Der Text der Nachricht, die protokolliert werden soll. Dabei muss es sich um eine Zeichenfolge handeln, die auf null endet. Die maximale Länge ist DSM_MAX_RC_MSG_LENGTH.
dsmLogtype
Gibt an, wo die Nachricht protokolliert werden soll. Gültige Werte umfassen: **logServer**, **logLocal**, **logBoth**.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmLogEvent

Rückkehrcode	Erläuterung
DSM_RC_STRING_TOO_LONG (2120)	Die Nachrichtenzeichenfolge ist zu lang.

dsmLogEventEx

Mit dem Funktionsaufruf dsmLogEventEx wird eine Benutzernachricht in der Serverprotokolldatei und/oder im lokalen Fehlerprotokoll protokolliert. Dieser Aufruf muss während des Zustands InSession innerhalb einer Sitzung ausgeführt werden. Der Aufruf kann nicht in einem Sende-, Abruf- oder Abfrageaufruf durchgeführt werden.

Zusammenfassungszustandsdiagramm: Eine Übersicht über die Sitzungsinteraktionen finden Sie im Zusammenfassungszustandsdiagramm hier:

Abbildung 1

Die IBM Spectrum Protect-Nachrichtennummer wird durch die Dringlichkeit bestimmt. Um Nachrichten anzuzeigen, die auf dem Server protokolliert sind, verwenden Sie den Befehl query actlog über den Verwaltungsclient. Verwenden Sie die IBM Spectrum Protect-Clientoption errorlogretention, um die Clientfehlerprotokolldatei zu bereinigen, wenn die Anwendung zahlreiche Clientnachrichten in das Clientprotokoll schreibt (dsmLogType ist entweder logLocal oder logBoth). Weitere Informationen finden Sie in der Dokumentation für den IBM Spectrum Protect-Server.

Syntax

```
extern dsInt16_t DSMLINKAGE  dsmLogEventEx(
       dsUint32_t             dsmHandle,
       dsmLogExIn_t          *dsmLogExInP,
       dsmLogExOut_t         *dsmLogExOutP
);
```

Parameter

dsUint32_t dsmHandle(I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.

dsmLogExIn_t *dsmLogExInP
: Diese Struktur enthält die Eingabeparameter.

  dsmLogSeverity severity;
  : Dieser Parameter gibt die Ereignisdringlichkeit an. Gültige Werte sind:

```
logSevInfo,       /* Information   ANE4990 */
logSevWarning,    /* Warnung       ANE4991 */
logSevError,      /* Fehler        ANE4992 */
logSevSevere      /* schwerwiegend ANE4993 */
```

  char appMsgID[8];
  : Dieser Parameter ist eine Zeichenfolge zum Identifizieren der spezifischen Anwendungsnachricht. Ein geeignetes Format sind drei Zeichen, gefolgt von vier Zahlen, beispielsweise DSM0250.

  dsmLogType logType;
  : Dieser Parameter gibt an, wohin das Ereignis übertragen werden soll. Für diesen Parameter gibt es die folgenden gültigen Werte:

    - logServer
    - logLocal
    - logBoth

  char *message;
  : Dieser Parameter gibt den Text der zu protokollierenden Ereignisnachricht an. Bei dem Text muss es sich um eine Zeichenfolge handeln, die auf null endet. Die maximale Länge ist DSM_MAX_RC_MSG_LENGTH.
  Einschränkung: Nachrichten, die an den Server übertragen werden, müssen in Englisch abgefasst sein. Nachrichten in anderen Sprachen als Englisch werden nicht korrekt angezeigt.

dsmLogExOut_t *dsmLogExOutP
: Diese Struktur enthält die Ausgabeparameter. Momentan sind keine Ausgabeparameter definiert.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmLogEventEx

Rückkehrcode	Erläuterung
DSM_RC_STRING_TOO_LONG (2120)	Die Nachrichtenzeichenfolge ist zu lang.

dsmQueryAccess

Mit dem Funktionsaufruf **dsmQueryAccess** wird der Server nach allen Zugriffsberechtigungsregeln für Sicherungsversionen oder archivierte Kopien Ihrer Objekte abgefragt. Ein Verweis auf ein Array von Zugriffsregeln wird an den Aufruf übergeben und das fertige Array zurückgegeben. Es wird ein Verweis auf die Anzahl Regeln übergeben, um anzugeben, wie viele Regeln das Array enthält.

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

Syntax

```
dsInt16_t DSMLINKAGE dsmQueryAccess
                  (dsUint32_t            dsmHandle),
                   qryRespAccessData     **accessListP,
                   dsUint16_t            *numberOfRules) ;
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

qryRespAccessData **accessListP (O)

Ein Verweis auf einen Array von Elementen `qryRespAccessData`, die die API-Bibliothek zuordnet. Jedes Element entspricht einer Zugriffsregel. Die Anzahl Elemente in dem Array wird im Parameter **numberOfRules** zurückgegeben. Die Informationen, die in jedem Element `qryRespAccessData` zurückgegeben werden, umfassen Folgendes:

	Name	Beschreibung
	ruleNumber	Die ID für die Zugriffsregel. Diese kennzeichnet die Regel zum Löschen.
	AccessType	Der Sicherungs- oder Archivierungstyp.
	Node	Der Knoten, für den Zugriff erteilt wurde.
	Owner	Der Benutzer, dem Zugriff erteilt wurde.
	objName	Die übergeordneten oder untergeordneten Dateibereichsdeskriptoren.

dsUint32_t *numberOfRules (O)
Gibt die Anzahl Regeln in dem Array `accessList` zurück.

dsmQueryApiVersion

Mit dem Funktionsaufruf **dsmQueryApiVersion** wird eine Abfrageanforderung für die API-Bibliotheksversion ausgeführt, auf die der Anwendungsclient zugreift.

Alle Aktualisierungen an der API erfolgen in aufwärtskompatiblem Format. Jeder Anwendungsclient mit einer API-Version oder einem API-Release kleiner-gleich der Version bzw. des Release der API-Bibliothek auf der Workstation des Endbenutzers wird ohne Änderung ausgeführt. Sollte der Aufruf **dsmQueryApiVersion** eine ältere Version oder ein älteres Versionsrelease als die bzw. das des Anwendungsclients zurückgeben, müssen Sie vor dem Fortfahren beachten, dass einige API-Aufrufe möglicherweise auf eine Art und Weise erweitert wurden, die nicht von der älteren API-Version des Endbenutzers unterstützt wird.

Die API-Versionsnummer der Anwendung ist in der Datei dsmapitd.h als die Konstanten DSM_API_VERSION, DSM_API_RELEASE und DSM_API_LEVEL gespeichert.

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

Syntax

```
void dsmQueryApiVersion  (dsmApiVersion *apiVersionP);
```

Parameter

dsmApiVersion *apiVersionP (O)
Dieser Parameter ist ein Verweis auf die Struktur, die die Version, das Release und die Stufe der API-Bibliothek enthält. Wenn die Bibliothek beispielsweise die Version 1.1.0 hat, enthalten die Felder der Struktur nach der Rückkehr des Aufrufs die folgenden Werte:

```
dsmApiVersionP->version  = 1
dsmApiVersionP->release  = 1
dsmApiVersionP->level    = 0
```

dsmQueryApiVersionEx

Mit dem Funktionsaufruf **dsmQueryApiVersionEx** wird eine Abfrageanforderung für die API-Bibliotheksversion ausgeführt, auf die der Anwendungsclient zugreift.

Alle Aktualisierungen an der API erfolgen in aufwärtskompatiblem Format. Jeder Anwendungsclient mit einer API-Version oder einem API-Release kleiner-gleich der Version bzw. des Release der API-Bibliothek auf der Workstation des Endbenutzers wird ohne Änderung ausgeführt. Die Zusammenfassung der Codeänderungen in der Datei README_api_enu gibt Auskunft über die Ausnahmen in Bezug auf die Aufwärtskompatibilität. Wenn der Aufruf **dsmQueryApiVersionEx** eine andere Version oder ein anderes Versionsrelease zurückgibt als die bzw. das des Anwendungsclients, müssen Sie vor dem Fortfahren beachten, dass einige API-Aufrufe möglicherweise auf eine Art und Weise erweitert wurden, die nicht von der älteren API-Version des Endbenutzers unterstützt wird.

Die API-Versionsnummer der Anwendung ist in der Headerdatei dsmapitd.h als die Konstanten DSM_API_VERSION, DSM_API_RELEASE, DSM_API_LEVEL und DSM_API_SUBLEVEL gespeichert.

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

Syntax

```
void dsmQueryApiVersionEx (dsmApiVersionEx *apiVersionP);
```

Parameter

dsmApiVersionEx *apiVersionP (O)
Dieser Parameter ist ein Verweis auf die Struktur, die die Version, das Release, die Stufe und die Unterstufe der API-Bibliothek enthält. Wenn die Bibliothek beispielsweise die Version 5.5.0.0 hat, enthalten die Felder der Struktur nach der Rückkehr des Aufrufs die folgenden Werte:

- `ApiVersionP->version = 5`
- `ApiVersionP->release = 5`
- `ApiVersionP->level = 0`
- `ApiVersionP->subLevel = 0`

dsmQueryCliOptions

Mit dem Funktionsaufruf **dsmQueryCliOptions** werden wichtige Optionswerte in der Benutzeroptionsdatei abgefragt. Eine Struktur des Typs **optStruct** wird in dem Aufruf übergeben und enthält die Informationen. Dieser Aufruf wird ausgeführt, bevor **dsmInitEx** aufgerufen wird; er legt die Konfiguration vor der Sitzung fest.

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

Syntax

```
dsInt16_t dsmQueryCliOptions
    (optStruct     *optstructP);
```

Parameter

optStruct *optstructP (I/O)
Dieser Parameter übergibt die Adresse der Struktur, die die API ausführt. Der Anwendungsclient ist für das Zuordnen von Speicher für die Struktur zuständig. Bei der erfolgreichen Rückkehr enthalten die Felder in der Struktur die entsprechenden Informationen.
Die folgenden Informationen werden in der **optStruct**-Struktur zurückgegeben:

	Name	Beschreibung
	dsmiDir	Der Wert der Umgebungsvariablen DSMI_DIR.
	dsmiConfig	Die in der Umgebungsvariablen DSMI_CONFIG angegebene Clientoptionsdatei.
	serverName	Der Name des IBM Spectrum Protect-Servers.
	commMethod	Die ausgewählte Übertragungsmethode. Siehe #defines für DSM_COMM_* in der Datei dsmapitd.h.
	serverAddress	Die Adresse des Servers auf der Basis der Übertragungsmethode.
	nodeName	Der Name des Clientknotens (Maschine).
	compression	Dieses Feld enthält Informationen, die die Komprimierungsoption betreffen.
	passwordAccess	Gültige Werte sind: *bTrue* für 'generate' und *bFalse* für 'prompt'.

Zugehörige Konzepte:
Verarbeitungsoptionen

dsmQuerySessInfo

Mit dem Funktionsaufruf **dsmQuerySessInfo** wird eine Anforderung zum Abfragen von Informationen an IBM Spectrum Protect gestartet, die sich auf die Operation der angegebenen Sitzung in **dsmHandle** beziehen. Eine Struktur des Typs **ApiSessInfo** wird in dem Aufruf übergeben; sie enthält alle verfügbaren eingegebenen sitzungsbezogenen Informationen. Dieser Aufruf wird nach einem erfolgreichen Aufruf **dsmInitEx** gestartet.

Die Informationen, die in der Struktur des Typs **ApiSessInfo** zurückgegeben werden, umfassen Folgendes:

- Serverinformationen: Portnummer, Datum und Uhrzeit sowie Typ
- Clientstandardwerte: Anwendungstyp, Löschberechtigungen, Begrenzer und Transaktionsgrenzen
- Sitzungsdaten: Anmelde-ID und Eigner
- Maßnahmendaten: Domäne, aktive Maßnahmengruppe und Aufbewahrungszeitraum

Informationen zum Inhalt der übergebenen Struktur und jedes Felds in der Struktur finden Sie in Quellendateien für API-Typdefinitionen.

Syntax

```
dsInt16_t dsmQuerySessInfo  (dsUint32_t         dsmHandle,
   ApiSessInfo   *SessInfoP);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

ApiSessInfo *SessInfoP (I/O)
: Dieser Parameter übergibt die Adresse der Struktur, die die API ausführt. Der Anwendungsclient ist für das Zuordnen von Speicher für die Struktur zuständig und für das Eingeben der Feldeinträge, die die Version der verwendeten Struktur angeben. Bei der erfolgreichen Rückkehr enthalten die Felder in der Struktur die entsprechenden Informationen. Bei adsmServerName handelt es sich um den Namen, der dem IBM Spectrum Protect-Server im Befehl **define server** zugeordnet wird. Ist das Feld 'archiveRetentionProtection' auf wahr gesetzt, ist der Server für den Aufbewahrungsschutz aktiviert.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmQuerySessInfo

Rückkehrcode	Erläuterung
DSM_RC_NO_SESS_BLK (2006)	Keine Serversitzungsblockinformationen.
DSM_RC_NO_POLICY_BLK (2007)	Keine Servermaßnahmeninformationen verfügbar.
DSM_RC_WRONG_VERSION_PARM (2065)	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.

dsmQuerySessOptions

Mit dem Funktionsaufruf dsmQuerySessOptions werden wichtige Optionswerte, die in der in dsmHandle angegebenen Sitzung gültig sind, abgefragt. Eine Struktur des Typs `optStruct` wird in dem Aufruf übergeben und enthält die Informationen.

Dieser Aufruf wird nach einem erfolgreichen Aufruf dsmInitEx gestartet. Die Werte, die zurückgegeben werden, können sich, abhängig von Werten, die an den Aufruf dsmInitEx übergeben werden, von den Werten, die in einem Aufruf dsmQueryCliOptions zurückgegeben werden, unterscheiden; dies betrifft in erste Linie optString und optFile. Informationen zur Vorrangstellung der einzelnen Optionen finden Sie in Erläuterungen zu Konfigurations- und Optionsdateien.

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

Syntax

```
dsInt16_t dsmQuerySessOptions
    (dsUint32_t    dsmHandle,
    optStruct      *optstructP);
```

Parameter

dsUint32_t dsmhandle(I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.

optStruct *optstructP (I/O)
: Dieser Parameter übergibt die Adresse der Struktur, die die API ausführt. Der Anwendungsclient ist für das Zuordnen von Speicher für die Struktur zuständig. Bei der erfolgreichen Rückkehr enthalten die Felder in der Struktur die entsprechenden Informationen.
In der Struktur des Typs 'optStruct' werden die folgenden Informationen zurückgegeben:

	Name	Beschreibung
	dsmiDir	Der Wert der Umgebungsvariablen DSMI_DIR.
	dsmiConfig	Die Datei dsm.opt, die in der Umgebungsvariablen DSMI_CONFIG angegeben ist.
	serverName	Der Name in der IBM Spectrum Protect-Serverzeilengruppe in der Optionsdatei.
	commMethod	Die ausgewählte Übertragungsmethode. Siehe #defines für DSM_COMM_* in der Datei dsmapitd.h.
	serverAddress	Die Adresse des Servers auf der Basis der Übertragungsmethode.
	nodeName	Der Name des Knotens (der Maschine) des Clients.
	compression	Der Wert für die Option 'compression' (bTrue=on und bFalse=off).
	compressAlways	Der Wert für die Option compressalways (bTrue=on und bFalse=off).
	passwordAccess	Wert bTrue für 'generate' und bFalse für 'prompt'.

Zugehörige Konzepte:

dsmRCMsg

Mit dem Funktionsaufruf dsmRCMsg wird der Nachrichtentext abgerufen, der einem API-Rückkehrcode zugeordnet ist.

Der Parameter **msg** zeigt den Nachrichtenpräfixrückkehrcode in runden Klammern ( ) gefolgt vom Nachrichtentext. Ein Aufruf dsmRCMsg könnte beispielsweise Folgendes zurückgeben:

```
ANS0264E (RC2300) Nur der Root
darf dsmChangePW oder
dsmDeleteFS ausführen.
```

Für einige Sprachen, bei denen Zeichen in ANSI- und OEM-Codepages unterschiedlich sind, kann es notwendig sein, Zeichenfolgen von ANSI in OEM zu konvertieren (z. B. Einzelbytezeichensätze für Osteuropa). Nachfolgend ein Beispiel:

```
   dsmRCMsg(dsmHandle, rc, msgBuf);
   #ifdef WIN32
   #ifndef WIN64
   CharToOemBuff(msgBuf, msgBuf, strlen(msgBuf));
   #endif
   #endif
   printf("
```

Syntax

```
dsInt16_t dsmRCMsg  (dsUint32_t       dsmHandle,
   dsInt16_t        dsmRC,
   char         *msg);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.

dsInt16_t dsmRC (I)
: Der API-Rückkehrcode des zugeordneten Nachrichtentextes. Die API-Rückkehrcodes sind in der Datei dsmrc.h aufgelistet. Weitere Informationen finden Sie in Quellendatei mit API-Rückkehrcodes: dsmrc.h.

char *msg (O)
: Dieser Parameter gibt den Nachrichtentext an, der dem Rückkehrcode dsmRC zugeordnet ist. Der Aufrufende ist für das Zuordnen von ausreichend Speicherbereich verantwortlich.

  Die maximale Länge für **msg** ist als DSM_MAX_RC_MSG_LENGTH definiert.

  Auf Plattformen mit Unterstützung in der Landessprache und mehreren länderspezifischen Nachrichtendateien gibt die API eine Nachrichtenzeichenfolge in der Landessprache zurück.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmRCMsg

Rückkehrcode	Erläuterung
DSM_RC_NULL_MSG (2002)	Der Parameter **msg** für den Aufruf dsmRCMsg ist ein NULL-Zeiger.
DSM_RC_INVALID_RETCODE (2021)	Der Rückkehrcode, der an den Aufruf **dsmRCMsg** übergeben wurde, ist ungültig.
DSM_RC_NLS_CANT_OPEN_TXT (0610)	Die Nachrichtentextdatei kann nicht geöffnet werden.

dsmRegisterFS

Mit dem Funktionsaufruf **dsmRegisterFS** wird ein neuer Dateibereich beim IBM Spectrum Protect-Server registriert. Bevor Sie Daten in einem Dateibereich sichern können, müssen Sie diesen zuvor registrieren.

Anwendungsclients dürfen nicht dieselben Dateibereichsnamen wie ein Client für Sichern/Archivieren verwenden.

- Führen Sie unter UNIX oder Linux den Befehl **df** für diese Namen aus.
- Bei Windows handelt es sich bei diesen Namen im Allgemeinen um die Datenträgerkennsätze, die den einzelnen Laufwerken auf Ihrem System zugeordnet sind.

Syntax

```
dsInt16_t dsmRegisterFS  (dsUint32_t         dsmHandle,
   regFSData     *regFilespaceP);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

regFSData *regFilespaceP (I)
: Mit diesem Parameter werden der Name des Dateibereichs und die zugehörigen Informationen, die für die Registrierung beim IBM Spectrum Protect-Server erforderlich sind, übergeben.
Tipp: Das Feld *fstype* umfasst das Präfix, **"API:"**. Diese Zeichenfolge wird für alle Dateibereichsabfragen angezeigt. Übergibt beispielsweise der Benutzer *myfstype* für *fstype* im Aufruf **dsmRegisterFS**, wird als tatsächlicher Wert für die Zeichenfolge auf dem Server bei der Abfrage `API:myfstype` zurückgegeben. Dieses Präfix dient zur Unterscheidung zwischen API-Objekten und Objekten des Clients für Sichern/Archivieren.

: Der verwendbare Bereich für **fsInfo** ist jetzt DSM_MAX_USER_FSINFO_LENGTH.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmRegisterFS

Rückkehrcode	Erläuterung
DSM_RC_INVALID_FSNAME (2016)	Ungültiger Dateibereichsname.
DSM_RC_INVALID_DRIVE_CHAR (2026)	Laufwerkbuchstabe ist kein alphabetischen Zeichen.
DSM_RC_NULL_FSNAME (2027)	Leerer Dateibereichsname.
DSM_RC_FS_ALREADY_REGED (2062)	Dateibereich ist bereits registriert.
DSM_RC_WRONG_VERSION_PARM (2065)	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.
DSM_RC_FSINFO_TOOLONG (2106)	Dateibereichsinformationen sind zu lang.

dsmReleaseBuffer

Mit der Funktion **dsmReleaseBuffer** wird ein Puffer an IBM Spectrum Protect zurückgegeben. **dsmReleaseBuffer** wird von der Anwendung aufgerufen, nachdem ein Aufruf **dsmGetDataEx** erfolgt ist und die Anwendung alle Daten aus dem Puffer übertragen hat und zum Freigeben des Puffers bereit ist. **dsmReleaseBuffer** erfordert den Aufruf **dsmInitEx** unter Angabe von ***btrue*** für *UseTsmBuffers* und einem Wert ungleich null für *numTsmBuffers*. **dsmReleaseBuffer** sollte auch aufgerufen werden, wenn der Aufruf **dsmTerminate** unmittelbar bevorsteht und die Anwendung Datenpuffer noch nicht freigegeben hat.

Syntax

```
dsInt16_t  dsmReleaseBuffer  (releaseBufferIn_t     *dsmReleaseBufferInP,
                              releaseBufferOut_t    *dsmReleaseBufferOutP) ;
```

Parameter

releaseBufferIn_t *dsmReleaseBufferInP (I)
: Diese Struktur enthält die folgenden Eingabeparameter:

  dsUint32_t dsmHandle (I)
  : Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

  dsUint8_t tsmBufferHandle(I)
  : Die Kennung, die diesen Puffer identifiziert.

  char *dataPtr(I)
  : Die Adresse, an die die Anwendung geschrieben wird.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmReleaseBuffer

Rückkehrcode	Erläuterung
DSM_RC_BAD_CALL_SEQUENCE	Der Aufruf wurde nicht im korrekten Status ausgegeben.
DSM_RC_INVALID_TSMBUFFER	Die Kennung oder der Wert von **dataPtr** ist ungültig.

Rückkehrcode	Erläuterung
DSM_RC_BUFF_ARRAY_ERROR	Ein Pufferarrayfehler ist aufgetreten.

dsmRenameObj

Mit dem Funktionsaufruf **dsmRenameObj** wird der übergeordnete oder untergeordnete Objektname umbenannt. Übergeben Sie bei Sicherungsobjekten den aktuellen Objektnamen und Änderungen für über- oder untergeordnete Objektnamen. Übergeben Sie bei Archivierungsobjekten den aktuellen Objektdateibereichsnamen und die Objekt-ID sowie Änderungen für über- oder untergeordnete Objektnamen. Verwenden Sie diesen Funktionsaufruf in Aufrufen **dsmBeginTxn** und **dsmEndTxn**.

Das Mischflag legt fest, ob ein doppelter Sicherungsobjektname mit den vorhandenen Sicherungen gemischt wird. Wenn der neue Name einem vorhandenen Objekt entspricht und der Mischvorgang wahr ist, wird das aktuelle Objekt in den neuen Namen konvertiert und wird zu der aktiven Version des neuen Namens, während das vorhandene aktive Objekt mit diesem Namen zur ersten inaktiven Kopie des Objekts wird. Wenn der neue Name einem vorhandenen Objekt entspricht und der Mischvorgang falsch ist, gibt die Funktion den Rückkehrcode DSM_RC_ABORT_DUPLICATE_OBJECT zurück.

Einschränkungen:

- Ein Objekt kann nur von seinem Eigner umbenannt werden.
- Die Funktion dsmRenameObj wird nicht unterstützt, wenn der Aufbewahrungsschutz für Daten auf dem IBM Spectrum Protect-Server aktiviert ist oder wenn Sie mit dem IBM Spectrum Protect for Data Retention-Server verbunden sind.

Im Funktionsaufruf **dsmRenameObj** wird auf diese Mischbedingungen getestet:

- Das aktuelle Objekt in der Struktur **dsmObjName** und das neue übergeordnete oder untergeordnete Objekt müssen in Bezug auf Eigner, Kopiengruppe und Verwaltungsklasse übereinstimmen.
- Das aktuelle Objekt in der Struktur **dsmObjName** muss nach dem momentan aktiven Objekt mit dem neuen Namen gesichert worden sein.
- Es darf nur eine einzige aktive Kopie des aktuellen Objekts in der Struktur **dsmObjName** und es dürfen keine inaktiven Kopien vorhanden sein.

Syntax

```
dsInt16_t dsmRenameObj   (dsmRenameIn_t     *dsmRenameInP,
                          dsmRenameOut_t    *dsmRenameOutP);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

dsmRenameIn_t *dsmRenameInP
: Diese Struktur enthält die Eingabeparameter.

  dsUint8_t repository (I);
  : Dieser Parameter gibt an, ob der zu löschende Dateibereich im Sicherungsrepository oder im Archivrepository vorhanden ist.

  dsmObjName *objNameP (I);
  : Dieser Parameter ist ein Verweis auf die Struktur, die die aktuellen Werte für den Dateibereichsnamen, den übergeordneten Objektnamen, den untergeordneten Objektnamen und den Objekttyp enthält.

  char newHl [DSM_MAX_HL_LENGTH + 1];
  : Dieser Parameter gibt den neuen übergeordneten Namen an.

  char newLl [DSM_MAX_LL_LENGTH + 1];
  : Dieser Parameter gibt den neuen untergeordneten Namen an.

  dsBool_t merge;
  : Dieser Parameter legt fest, ob ein Sicherungsobjekt mit doppelten benannten Objekten gemischt wird. Gültige Werte sind 'true' und 'false'.

  ObjID;
  : Die Objekt-ID für Archivierungsobjekte.

dsmRenameOut_t *dsmRnameOutP
: Diese Struktur enthält die Ausgabeparameter.
  Anmerkung: Es gibt keine Ausgabeparameter.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmRenameObj

Rückkehrcode	Erläuterung
DSM_RC_ABORT_MERGE_ERROR (45)	Der Server hat einen Mischfehler erkannt.

Rückkehrcode	Erläuterung
DSM_RC_ABORT_DUPLICATE_OBJECT (32)	Das Objekt ist bereits vorhanden und der Mischvorgang ist falsch.
DSM_RC_ABORT_NO_MATCH (2)	Objekt nicht gefunden.
DSM_RC_REJECT_SERVER_DOWNLEVEL (58)	Diese Funktion kann nur auf einem IBM Spectrum Protect-Server der Version 3.7.4.0 oder höher verwendet werden.

dsmRequestBuffer

Mit der Funktion **dsmRequestBuffer** wird ein Puffer an IBM Spectrum Protect zurückgegeben. **dsmRequestBuffer** wird von der Anwendung aufgerufen, nachdem ein Aufruf **dsmGetDataEx** erfolgt ist und die Anwendung alle Daten aus dem Puffer übertragen hat und zum Freigeben des Puffers bereit ist.

dsmReleaseBuffer erfordert den Aufruf **dsmInitEx** unter Angabe von *btrue* für *UseTsmBuffers* und einem Wert ungleich null für *numTsmBuffers*. **dsmReleaseBuffer** sollte auch aufgerufen werden, wenn der Aufruf **dsmTerminate** unmittelbar bevorsteht und die Anwendung IBM Spectrum Protect-Puffer noch nicht freigegeben hat.

Syntax

```
dsInt16_t  dsmRequestBuffer   (getBufferIn_t      *dsmRequestBufferInP,
                               getBufferOut_t     *dsmRequestBufferOutP) ;
```

Parameter

getBufferIn_t * dsmRequestBufferInP (I)
Diese Struktur enthält den folgenden Eingabeparameter:

dsUint32_t dsmHandle
Die Kennung, die die Sitzung identifiziert und einem vorherigen Aufruf **dsmInitEx** zuordnet.

getBufferOut_t *dsmRequestBufferOut P (0)
Diese Struktur enthält die Ausgabeparameter.

dsUint8_t tsmBufferHandle(0)
Die Kennung, die diesen Puffer identifiziert.
char *dataPtr(0)
Die Adresse, an die die Anwendung geschrieben wird.
dsUint32_t *bufferLen(0)
Die maximale Anzahl Byte, die in diesen Puffer geschrieben werden kann.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmRequestBuffer

Rückkehrcode	Erläuterung
DSM_RC_BAD_CALL_SEQUENCE (33)	Der Aufruf wurde nicht im korrekten Status ausgegeben.
DSM_RC_SENDDATA_WITH_ZERO_SIZE (34)	Wenn das gesendete Objekt die Länge 0 hat, sind keine Aufrufe **dsmReleaseBuffer** zulässig.
DSM_RC_BUFF_ARRAY_ERROR (121)	Es konnte kein gültiger Puffer abgerufen werden.

dsmRetentionEvent

Mit dem Funktionsaufruf **dsmRetentionEvent** wird im Rahmen einer Aufbewahrungsereignisoperation, die für die in der Liste angegebenen Objekte ausgeführt werden soll, eine Liste mit Objekt-IDs an den IBM Spectrum Protect-Server gesendet. Verwenden Sie diesen Funktionsaufruf in Aufrufen **dsmBeginTxn** und **dsmEndTxn**.

Anmerkung: Diese Funktion kann nur auf einem Server der Version 5.2.2.0 oder höher verwendet werden.

Die maximale Anzahl Objekte in einem Aufruf ist auf den Wert im Feld *maxObjPerTxn* begrenzt, das in der Struktur des Typs *ApisessInfo* von einem Aufruf **dsmQuerySessInfo** zurückgegeben wird.

Ein Ereignis für ein Objekt kann nur vom Eigner dieses Objekts gesendet werden.

Gültige Ereignisse sind:

eventRetentionActivate
: Kann nur für Objekte ausgegeben werden, die an eine ereignisgesteuerte Verwaltungsklasse gebunden sind. Durch das Senden dieses Ereignisses wird das Ereignis für dieses Objekt aktiviert und der Status für die Aufbewahrungsdauer für dieses Objekt ändert sich von DSM_ARCH_RETINIT_PENDING in DSM_ARCH_RETINIT_STARTED.

eventHoldObj
: Dieses Ereignis gibt eine temporäre Sperre in Bezug auf die Aufbewahrungsdauer oder das Löschen für ein Objekt aus, sodass das Objekt erst verfallen oder gelöscht werden kann, nachdem eine Freigabe erfolgt ist.

eventReleaseObj
: Dieses Ereignis kann nur für ein Objekt ausgegeben werden, für das das Feld *objectHeld* den Wert DSM_ARCH_HELD_TRUE enthält; mit diesem Ereignis wird die temporäre Sperre für das Objekt entfernt und die ursprüngliche Maßnahme für Aufbewahrungsdauer wieder aufgenommen.

Bevor Sie den Aufruf *dsmRetentionEvent* senden, senden Sie die in IBM Spectrum Protect-System abfragen beschriebene Abfragefolge, um die Informationen für das Objekt abzurufen. Der Aufruf **dsmGetNextQObj** gibt für Archivabfragen eine Datenstruktur mit dem Namen **qryRespArchiveData** zurück. Diese Datenstruktur enthält die Informationen, die für **dsmRetentionEvent** benötigt werden.

Syntax

```
extern dsInt16_t DSMLINKAGE dsmRetentionEvent(
  dsmRetentionEventIn_t          *ddsmRetentionEventInP,
  dsmRetentionEventOut_t         *dsmRetentionEventOutP
   );
```

Parameter

dsmRetentionEventIn_t *dsmRetentionEventP
: Diese Struktur enthält die folgenden Eingabeparameter:

  dsUint16_t stVersion;
  : Dieser Parameter gibt die Strukturversion an.

  dsUint32_t dsmHandle (I)
  : Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.

  dsmEventType_t evenType (I);
  : Dieser Parameter gibt den Ereignistyp an. Die Bedeutung der gültigen Werte (**eventRetentionActivate**, **eventHoldObj** und **eventReleaseObj**) finden Sie am Anfang dieses Abschnitts.

  dsmObjList_t objList;
  : Dieser Parameter gibt eine Liste der als Signal zu sendenden Objekt-IDs an.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmRetentionEvent

Rückkehrcode	Erläuterung
DSM_RC_ABORT_NODE_NOT_AUTHORIZED (36)	Der Knoten oder Benutzer hat nicht die korrekte Berechtigung.
DSM_RC_ABORT_TXN_LIMIT_EXCEEDED (249)	Zu viele Objekte in der Transaktion.
DSM_RC_ABORT_OBJECT_ALREADY_HELD (250)	Das Objekt ist bereits gesperrt, daher kann keine weitere temporäre Sperre ausgegeben werden.
DSM_RC_REJECT_SERVER_DOWNLEVEL (58)	Diese Funktion kann nur auf einem Server der Version 5.2.2.0 oder höher verwendet werden.

dsmSendBufferData

Mit dem Funktionsaufruf **dsmSendBufferData** wird ein Bytestrom mit Daten über einen in einem vorherigen Aufruf **dsmReleaseBuffer** bereitgestellten Puffer an IBM Spectrum Protect gesendet. Der Anwendungsclient kann jeden Typ von Daten zum Speichern auf dem Server übergeben. In der Regel (aber nicht ausschließlich) handelt es sich bei diesen Daten um Dateidaten. Sie können **dsmSendBufferData** mehrmals aufrufen, wenn der Bytestrom mit Daten, den Sie senden, groß ist. Der Puffer wird unabhängig davon, ob der Aufruf erfolgreich ausgeführt wird oder fehlschlägt, freigegeben.

Einschränkung: Bei Verwendung der Option *useTsmBuffers* wird das Objekt nicht komprimiert, selbst wenn es für die Komprimierung eingeschlossen ist.

Syntax

```
dsInt16_t  dsmSendBufferData   (sendBufferDataIn_t        *dsmSendBufferDataExInP,
                                sendBufferDataOut_t       *dsmSendBufferDataOutP) ;
```

Parameter

sendBufferDataIn_t * dsmSendBufferDataInP (I)
Diese Struktur enthält die folgenden Eingabeparameter:

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.
dsUint8_t tsmBufferHandle(I)
Die Kennung, die den zu sendenden Puffer identifiziert.
char *dataPtr(I)
Die Adresse, an die Anwendungsdaten geschrieben wurden.
dsUint32_t numBytes(I)
Die tatsächliche Anzahl Byte, die von der Anwendung geschrieben wurde (dieser Wert sollte immer kleiner als der in **dsmReleaseBuffer** angegebene Wert sein).

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmSendBufferData

Rückkehrcode	Erläuterung
DSM_RC_BAD_CALL_SEQUENCE (2041)	Der Aufruf wurde nicht im korrekten Status ausgegeben.
DSM_RC_INVALID_TSMBUFFER (2042)	Die Kennung oder der Wert von **dataPtr** ist ungültig.
DSM_RC_BUFF_ARRAY_ERROR (2045)	Ein Pufferarrayfehler ist aufgetreten.
DSM_RC_TOO_MANY_BYTES (2043)	Der Wert von *numBytes* ist größer als der im Aufruf **dsmReleaseBuffer** bereitgestellte Puffer.

dsmSendData

Mit dem Funktionsaufruf **dsmSendData** wird ein Bytestrom mit Daten über einen Puffer an IBM Spectrum Protect gesendet. Der Anwendungsclient kann jeden Typ von Daten zum Speichern auf dem Server übergeben. In der Regel (aber nicht ausschließlich) handelt es sich bei diesen Daten um Dateidaten. Sie können **dsmSendData** mehrmals aufrufen, wenn der Bytestrom mit Daten, der gesendet werden soll, groß ist.

Einschränkung: Der Anwendungsclient kann den Puffer, der in **dsmSendData** angegeben ist, erst nach der Rückkehr des Aufrufs **dsmSendData** wiederverwenden.
Tipp: Wenn IBM Spectrum Protect den Code 157 (DSM_RC_WILL_ABORT) zurückgibt, starten Sie einen Aufruf **dsmEndSendObj** und dann einen Aufruf **dsmEndTxn** mit dem Votum DSM_VOTE_COMMIT. Die Anwendung empfängt dann den Rückkehrcode 2302 (DSM_RC_CHECK_REASON_CODE) und übergibt den Ursachencode zurück an den Anwendungsbenutzer. Damit wird dem Benutzer mitgeteilt, warum der Server die Transaktion beendet.

Syntax

```
dsInt16_t dsmSendData  (dsUint32_t   dsmHandle,
   DataBlk *dataBlkPtr);
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.
DataBlk *dataBlkPtr (I/O)
Dieser Parameter verweist auf eine Struktur, die sowohl einen Zeiger auf den Puffer enthält, aus dem die Daten gesendet werden sollen, als auch einen Zeiger auf die Größe des Puffers. Bei der Rückkehr enthält diese Struktur die Anzahl tatsächlich übertragener Byte. Die Typdefinition finden Sie in Quellendateien für API-Typdefinitionen.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmSendData

Rückkehrcode	Erläuterung
DSM_RC_NO_COMPRESS_MEMORY (154)	Es ist nicht genügend Speicher zum Ausführen der Datenkomprimierung oder -erweiterung verfügbar.

Rückkehrcode	Erläuterung
DSM_RC_COMPRESS_GREW (155)	Während der Komprimierung nahm die Größe der komprimierten Daten im Vergleich zu den ursprünglichen Daten zu.
DSM_RC_WILL_ABORT (157)	Ein unbekannter und unerwarteter Fehler ist aufgetreten, der das Anhalten der Transaktion zur Folge hatte.
DSM_RC_WRONG_VERSION_PARM (2065)	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.
DSM_RC_NEEDTO_ENDTXN (2070)	Die Transaktion muss beendet werden.
DSM_RC_OBJ_EXCLUDED (2080)	Das Objekt wird von der Einschluss-/Ausschlussliste ausgeschlossen.
DSM_RC_OBJ_NOBCG (2081)	Das Objekt hat keine Sicherungskopiengruppe und wird nicht an den Server gesendet.
DSM_RC_OBJ_NOACG (2082)	Das Objekt hat keine Archivierungskopiengruppe und wird nicht an den Server gesendet.
DSM_RC_SENDDATA_WITH_ZERO_SIZE (2107)	Ein Objekt kann keine Daten mit einer Größenschätzung (*sizeEstimate*) von null Byte senden.

dsmSendObj

Mit dem Funktionsaufruf **dsmSendObj** wird eine Anforderung zum Senden eines einzelnen Objekts in Speicher gestartet. Aufgrund von Leistungsaspekten können mehrere Aufrufe **dsmSendObj** und zugehörige Aufrufe **dsmSendData** innerhalb der Grenzen einer Transaktion ausgeführt werden.

Mit dem Aufruf **dsmSendObj** werden die Daten für das Objekt als Bytestrom verarbeitet, der in Hauptspeicherpuffer übergeben wurde. Der Parameter **dataBlkPtr** im Aufruf **dsmSendObj** ermöglicht dem Anwendungsclient eine der folgenden Aktionen:

- Übergabe der Daten und der Attribute (die Attribute werden über **objAttrPtr** übergeben) des Objekts in einem einzigen Aufruf.
- Angabe eines Teils der Objektdaten über den Aufruf **dsmSendObj** und Angabe der verbleibenden Daten über einen oder mehrere Aufrufe **dsmSendData**.

Alternativ kann der Anwendungsclient auch nur die Attribute über den Aufruf **dsmSendObj** angeben und die Objektdaten über einen oder mehrere Aufrufe **dsmSendData** angeben. Bei diesem Verfahren müssen Sie **dataBlkPtr** im Aufruf **dsmSendObj** auf NULL setzen.
Tipp: Bei bestimmten Objekttypen werden Bytestromdaten möglicherweise nicht den Daten zugeordnet, beispielsweise ein Verzeichniseintrag ohne erweiterte Attribute.

Bevor **dsmSendObj** aufgerufen wird, muss ein vorhergehender Aufruf **dsmBindMC** ausgeführt werden, um eine Verwaltungsklasse korrekt an das Objekt zu binden, das gesichert oder archiviert werden soll. Die API behält diese Bindung bei, sodass sie dem Objekt, wenn es an den Server gesendet wird, die korrekte Verwaltungsklasse zuordnen kann. Wenn die Verwaltungsklasse, die in einem Aufruf **dsmSendObj** gebunden wird, standardmäßig den Objekttyp 'Verzeichnis' (DSM_OBJ_DIRECTORY) annehmen kann, entspricht der Standardwert möglicherweise nicht der Standardverwaltungsklasse. Stattdessen wird die Verwaltungsklasse mit dem längsten Aufbewahrungszeitraum verwendet. Sind mehrere Verwaltungsklassen mit diesem Aufbewahrungszeitraum vorhanden, wird die erste gefundene Verwaltungsklasse verwendet.

Führen Sie für alle Objektdaten, die in Speicher gesendet werden, anschließend einen Aufruf **dsmEndSendObj** aus. Sind keine Objektdaten zum Senden an den Server vorhanden oder waren alle Daten in dem Aufruf **dsmSendObj** enthalten, müssen Sie einen Aufruf **dsmEndSendObj** starten, bevor Sie einen weiteren Aufruf **dsmSendObj** starten können. Waren mehrere Operationen für das Senden von Daten über den Aufruf **dsmSendData** erforderlich, folgt der Aufruf **dsmEndSendObj** auf die letzte Sendeoperation, um die Statusänderung anzugeben.

Tipp: Wenn IBM Spectrum Protect den Code 157 (DSM_RC_WILL_ABORT) zurückgibt, starten Sie einen Aufruf **dsmEndTxn** mit dem Votum DSM_VOTE_COMMIT. Die Anwendung empfängt den Rückkehrcode 2302 (DSM_RC_CHECK_REASON_CODE) und übergibt den Ursachencode zurück an den Anwendungsbenutzer. Damit wird dem Benutzer mitgeteilt, warum der Server die Transaktion beendet.

Lautet der Ursachencode 11 (DSM_RS_ABORT_NO_REPOSIT_SPACE), ist es möglich, dass die Größenschätzung (*sizeEstimate*) für das tatsächliche Datenvolumen zu klein ist. Die Anwendung muss eine genauere Größenschätzung (*sizeEstimate*) durchführen und die Daten erneut senden.

Syntax

```
dsInt16_t dsmSendObj   (dsUint32_t       dsmHandle,
   dsmSendType             sendType,
   void        *sendBuff,
   dsmObjName              *objNameP,
   ObjAttr     *objAttrPtr,
   DataBlk     *dataBlkPtr);
```

Parameter

dsUint32_t dsmHandle (I)

Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

dsmSendType sendType (I)

Dieser Parameter gibt den Sendetyp an, der ausgeführt wird. Gültige Werte umfassen:

	Name	Beschreibung
	stBackup	Ein Sicherungsobjekt, das an den Server gesendet wird.
	stArchive	Ein Archivierungsobjekt, das an den Server gesendet wird.
	stBackupMountWait	Ein Sicherungsobjekt, für das der Server warten soll, bis die erforderliche Einheit bereitgestellt wird , z. B. ein Band geladen wird.
	stArchiveMountWait	Ein Archivierungsobjekt, für das der Server warten soll, bis die erforderliche Einheit bereitgestellt wird, z. B. ein Band geladen wird.

Anmerkung: Verwenden Sie die **MountWait**-Typen, wenn die Möglichkeit besteht, dass Ihr Anwendungsbenutzer unter Umständen Daten an ein Band sendet.

void *sendBuff (I)

Dieser Parameter ist ein Verweis auf eine Struktur, die andere Informationen enthält, die für den Sendetyp (**sendType**) in dem Aufruf spezifisch sind. Derzeit ist nur für einen Sendetyp (**sendType**) mit dem Wert **stArchive** eine Struktur zugeordnet. Diese Struktur hat den Namen **sndArchiveData** und enthält die Archivierungsbeschreibung.

dsmObjName *objNameP (I)

Dieser Parameter ist ein Verweis auf die Struktur, die den Dateibereichsnamen, den übergeordneten Objektnamen, den untergeordneten Objektnamen und den Objekttyp enthält. Weitere Informationen finden Sie in Objektnamen und -IDs.

ObjAttr *objAttrPtr (I)

Dieser Parameter übergibt Objektattribute, die für die Anwendung von Interesse sind. Die Typdefinition finden Sie in Quellendateien für API-Typdefinitionen.

Die Attribute sind:

- **owner** bezieht sich auf den Eigner des Objekts. Wenn das Objekt wieder aus dem IBM Spectrum Protect-Speicher abgerufen wird, ist es wichtig festzustellen, ob der Eigner als spezifischer Name oder als leere Zeichenfolge deklariert ist. Weitere Informationen finden Sie in Zugriff auf Objekte als Sitzungseigner.
- **sizeEstimate** ist die bestmögliche Schätzung der Gesamtgröße des Datenobjekts, das an den Server gesendet werden soll. Diese Größe sollte so genau wie möglich geschätzt werden, da der Server dieses Attribut für die effiziente Bereichszuordnung und Objektpositionierung in seinen Speicherressourcen verwendet.
  Ist die von Ihnen angegebene Größenschätzung erheblich geringer als die tatsächliche Anzahl Byte, die gesendet wird, hat der Server möglicherweise Schwierigkeiten, ausreichend Speicherbereich zuzuordnen, und beendet die Transaktion mit dem Ursachencode 11 (DSM_RS_ABORT_NO_REPOSIT_SPACE).
  Anmerkung: Die Größenschätzung gilt für die Gesamtgröße des Datenobjekts und wird in Byte angegeben.

  Objekte mit einer geringeren Größe als DSM_MIN_COMPRESS_SIZE werden nicht komprimiert.

  Wenn Ihr Objekt keine Bitdaten (sondern nur Attributinformationen dieses Aufrufs) enthält, sollte der Wert für **sizeEstimate** null sein.
  Anmerkung: Ab Version 5.1.0 wird das Kopienziel innerhalb einer Transaktion für Objekte mit der Länge null nicht auf Konsistenz geprüft.
- **objCompressed** ist ein boolescher Wert, der angibt, ob die Objektdaten bereits komprimiert wurden oder nicht.

  Wenn das Objekt komprimiert ist (*compressed=bTrue*), versucht IBM Spectrum Protect nicht, das Objekt erneut zu komprimieren. Wenn das Objekt nicht komprimiert ist, entscheidet IBM Spectrum Protect, ob das Objekt komprimiert werden soll. Diese Entscheidung ist von den Werten für die Option compression abhängig, die vom Administrator und in den API-Konfigurationsquellen festgelegt wurden.

  Soll Ihre Anwendung eine Zurückschreibung oder einen Abruf von Teilobjekten ausführen, können die Daten während des Sendevorgangs nicht komprimiert werden. Um dies durchzusetzen, setzen Sie *ObjAttr.objCompressed* auf *bTrue*.

- Mit **objInfo** werden Informationen zu dem spezifischen Objekt gespeichert.
  Einschränkung: Die Informationen werden nicht automatisch gespeichert. Wenn dieses Attribut verwendet wird, müssen Sie das Attribut *objInfoLength* definieren, um die Länge für *objInfo* anzugeben.
- **mcNameP** enthält den Namen einer Verwaltungsklasse, die die mit **dsmBindMC** abgerufene Verwaltungsklasse überschreibt.
- **disableDeduplication** ist ein boolescher Wert. Wird er auf wahr gesetzt, wird das Objekt nicht vom Client dedupliziert.

DataBlk *dataBlkPtr (I/O)

Dieser Parameter verweist auf eine Struktur, die sowohl einen Zeiger auf den Puffer für die Daten enthält, die gesichert oder archiviert werden sollen, als auch einen Zeiger auf die Größe des Puffers. Dieser Parameter gilt nur für **dsmSendObj**. Wenn Sie den Sendevorgang für Daten in einem nachfolgenden Aufruf **dsmSendData** statt im Aufruf **dsmSendObj** starten möchten, setzen Sie den Pufferzeiger in der DataBlk-Struktur auf NULL. Bei der Rückkehr enthält diese Struktur die Anzahl tatsächlich übertragener Byte. Die Typdefinition finden Sie in Quellendateien für API-Typdefinitionen.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmSendObj

Rückkehrcode	Erläuterung
DSM_RC_NO_COMPRESS_MEMORY (154)	Es ist nicht genügend Speicher zum Ausführen der Datenkomprimierung oder -erweiterung verfügbar.
DSM_RC_COMPRESS_GREW (155)	Während der Komprimierung nahm die Größe der komprimierten Daten im Vergleich zu den ursprünglichen Daten zu.
DSM_RC_WILL_ABORT (157)	Ein unbekannter und unerwarteter Fehler ist aufgetreten, der das Anhalten der Transaktion zur Folge hatte.
DSM_RC_TL_NOACG (186)	Die Verwaltungsklasse für diese Datei hat keine gültige Kopiengruppe für den Sendetyp.
DSM_RC_NULL_OBJNAME (2000)	Objektname ist null.
DSM_RC_NULL_OBJATTRPTR (2004)	Objektattributzeiger ist null.
DSM_RC_INVALID_OBJTYPE (2010)	Ungültiger Objekttyp.
DSM_RC_INVALID_OBJOWNER (2019)	Ungültiger Objekteigner.
DSM_RC_INVALID_SENDTYPE (2022)	Ungültiger Sendetyp.
DSM_RC_WILDCHAR_NOTALLOWED (2050)	Platzhalterzeichen nicht zulässig.
DSM_RC_FS_NOT_REGISTERED (2061)	Dateibereich nicht registriert.
DSM_RC_WRONG_VERSION_PARM (2065)	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.
DSM_RC_NEEDTO_ENDTXN (2070)	Die Transaktion muss beendet werden.
DSM_RC_OBJ_EXCLUDED (2080)	Das Objekt wurde von der Einschluss-/Ausschlussliste ausgeschlossen.
DSM_RC_OBJ_NOBCG (2081)	Das Objekt hat keine Sicherungskopiengruppe und wird nicht an den Server gesendet.
DSM_RC_OBJ_NOACG (2082)	Das Objekt hat keine Archivierungskopiengruppe und wird nicht an den Server gesendet.
DSM_RC_DESC_TOOLONG (2100)	Die Beschreibung ist zu lang.
DSM_RC_OBJINFO_TOOLONG (2101)	Die Objektinformationen sind zu lang.
DSM_RC_HL_TOOLONG (2102)	Das übergeordnete Qualifikationsmerkmal ist zu lang.
DSM_RC_FILESPACE_TOOLONG (2104)	Der Dateibereichsname ist zu lang.
DSM_RC_LL_TOOLONG (2105)	Das untergeordnete Qualifikationsmerkmal ist zu lang.
DSM_RC_NEEDTO_CALL_BINDMC (2301)	**dsmBindMC** muss zuerst aufgerufen werden.

dsmSetAccess

Mit dem Funktionsaufruf **dsmSetAccess** wird anderen Benutzern oder Knoten Zugriff auf Sicherungsversionen oder archivierte Kopien Ihrer Objekte, Zugriff auf alle Ihre Objekte oder Zugriff auf eine ausgewählte Gruppe von Objekten erteilt. Wenn Sie einem anderen Benutzer Zugriff erteilen, kann dieser Benutzer Ihre Dateien abfragen, zurückschreiben oder abrufen. Dieser Befehl unterstützt Platzhalterzeichen für die folgenden Felder: *fs*, *hl*, *ll*, *node*, *owner*.

Anmerkung: Es ist nicht möglich, in einem einzigen Befehl sowohl Zugriff auf Sicherungsversionen als auch Zugriff auf Archivierungskopien zu erteilen. Sie müssen entweder Sicherung oder Archivierung angeben.

Syntax

```
dsInt16_t DSMLINKAGE dsmSetAccess
        (dsUint32_t          dsmHandle,
         dsmSetAccessType    accessType,
         dsmObjName          *objNameP,
         char                *node,
         char                *owner);
```

Parameter

dsUint32_t dsmHandle (I)

Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

dsmAccessType accessType (I)

Dieser Parameter gibt den Typ von Objekten an, für die Zugriff erteilt werden soll. Gültige Werte umfassen:

	Name	Beschreibung
	atBackup	Gibt an, dass der Zugriff für Sicherungsobjekte erteilt wird.

	Name	Beschreibung
	atArchive	Gibt an, dass der Zugriff für Archivierungsobjekte erteilt wird.

dsmObjName *objNameP (I)
Dieser Parameter ist ein Verweis auf die Struktur, die den Dateibereichsnamen, den übergeordneten Objektnamen und den untergeordneten Objektnamen enthält.
Anmerkung: Um alle Dateibereiche anzugeben, verwenden Sie einen Stern (*) für den Dateibereichsnamen.

char *node (I)
Dieser Parameter ist ein Verweis auf den Knotennamen, für den Zugriff erteilt wird. Geben Sie für alle Knoten einen Stern (*) an.

char *owner (I)
Dieser Parameter ist ein Verweis auf den Benutzernamen in dem Knoten, für den Zugriff erteilt wurde. Geben Sie für alle Benutzer einen Stern (*) an.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmSetAccess

Rückkehrcode	Erläuterung
DSM_RC_INVALID_ACCESS_TYPE (2110)	Ungültiger Zugriffstyp angegeben.
DSM_RC_FILE_SPACE_NOT_FOUND (124)	Der angegebene Dateibereich wurde auf dem Server nicht gefunden.
DSM_RC_QUERY_COMM_FAILURE (2111)	Kommunikationsfehler während der Serverabfrage.
DSM_RC_NO_FILES_BACKUP (2112)	Für diesen Dateibereich wurden keine Dateien gesichert.
DSM_RC_NO_FILES_ARCHIVE (2113)	Für diesen Dateibereich wurden keine Dateien archiviert.
DSM_RC_INVALID_SETACCESS (2114)	Ungültige Formulierung beim Erteilen des Zugriffs.

dsmSetUp

Mit dem Funktionsaufruf **dsmSetUp** werden Umgebungsvariablenwerte überschrieben. Rufen Sie **dsmSetUp** auf, bevor Sie **dsmInitEx** aufrufen. Die Werte, die in der Struktur **envSetUp** übergeben wurden, überschreiben alle vorhandenen Umgebungsvariablen oder Standardwerte. Wenn Sie NULL für ein Feld angeben, werden die Werte aus der Umgebung übernommen. Wenn Sie keinen Wert definieren, werden die Werte aus den Standardwerden übernommen.

Voraussetzungen:

1. Wenn Sie **dsmSetUp** verwenden, rufen Sie immer **dsmTerminate** auf, bevor Sie **dsmCleanUp** aufrufen.
2. Die API-Instrumentierung kann nur aktiviert werden, wenn die API 'testflag INSTRUMENT:' in der Konfigurationsdatei definiert ist und die Aufrufe **dsmSetUp** oder **dsmCleanUp** in der Anwendung verwendet werden.

Syntax

```
dsInt16_t DSMLINKAGE dsmSetUp
        (dsBool_t    mtFlag,
         envSetUp    *envSetUpP);
```

Parameter

dsBool_t mtFlag (I)
Dieser Parameter gibt an, ob die API in einem Einzelthread- oder in einem Multithread-Modus verwendet wird. Gültige Werte umfassen:

```
DSM_SINGLETHREAD
DSM_MULTITHREAD
```

Voraussetzung: Das Flag für Multithread muss aktiviert sein, damit eine LAN-unabhängige Datenübertragung erfolgen kann.

envSetUp *envSetUpP(I)
Dieser Parameter ist ein Verweis auf die Struktur, die die Überschreibungswerte enthält. Geben Sie NULL an, wenn vorhandene Umgebungsvariablen nicht überschrieben werden sollen. Die Struktur **envSetUp** enthält folgende Felder:

	Name	Beschreibung
	dsmiDir	Ein vollständig qualifizierter Verzeichnispfad, der unter UNIX oder Linux eine Nachrichtendatei enthält. Dieses Feld gibt außerdem die Verzeichnisse für dsm.sys an.
	dsmiConfig	Der vollständig qualifizierte Name der Clientoptionsdatei.

	Name	Beschreibung
	dsmiLog	Der vollständig qualifizierte Pfad des Fehlerprotokollverzeichnisses.
	argv	Übergeben Sie den argv[0]-Namen des aufrufenden Programms, wenn die Anwendung mit der Berechtigung eines berechtigten Benutzers ausgeführt werden muss. Weitere Informationen finden Sie in Zugriff auf Kennwortdateien steuern.
	logName	Der Dateiname für ein Fehlerprotokoll, sofern die Anwendung nicht dsierror.log verwendet.
	inclExclCaseSensitive	Gibt an, ob bei Einschluss-/Ausschlussregeln die Groß-/Kleinschreibung beachtet werden muss oder nicht. Dieser Parameter kann nur unter Windows verwendet werden; für andere Betriebssysteme wird er ignoriert.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmSetUp

Rückkehrcode	Erläuterung
DSM_RC_ACCESS_DENIED (106)	Der Zugriff auf die angegebene Datei oder das angegebene Verzeichnis wird verweigert.
DSM_RC_INVALID_OPT (0400)	Es wurde eine ungültige Option gefunden.
DSM_RC_NO_HOST_ADDR (0405)	TCPSERVERADDRESS für diesen Server ist in der Zeilengruppe für den Servernamen in der Systemoptionsdatei nicht definiert.
DSM_RC_NO_OPT_FILE (0406)	Die über den Dateinamen angegebene Optionsdatei kann nicht gefunden werden.
DSM_RC_MACHINE_SAME (0408)	Der in der Optionsdatei definierte Knotenname (NODENAME) darf nicht mit dem Hostnamen (*HostName*) des Systems übereinstimmen.
DSM_RC_INVALID_SERVER (0409)	Die Systemoptionsdatei enthält nicht die Option SERVERNAME.
DSM_RC_INVALID_KEYWORD (0410)	In der Konfigurationsdatei, der Optionszeichenfolge, der Datei dsm.sys oder der Datei dsm.opt wurde für **dsmInitEx** ein ungültiges Optionsschlüsselwort gefunden.
DSM_RC_PATTERN_TOO_COMPLEX (0411)	Das ausgegebene Einschluss- oder Ausschlussmuster ist zu komplex und kann daher von IBM Spectrum Protect nicht korrekt interpretiert werden.
DSM_RC_NO_CLOSING_BRACKET (0412)	Das Einschluss- oder Ausschlussmuster wurde nicht korrekt erstellt. Die rechte eckige Klammer fehlt.
DSM_RC_NLS_CANT_OPEN_TXT (0610)	Das System kann die Nachrichtentextdatei nicht öffnen.
DSM_RC_NLS_INVALID_CNTL_REC (0612)	Das System kann die Nachrichtentextdatei nicht verwenden.
DSM_RC_NOT_ADSM_AUTHORIZED (0927)	Sie müssen der berechtigte Benutzer sein, um Multithreading und '*passwordaccess* generate' verwenden zu können.
DSM_RC_NO_INCLEXCL_FILE (2229)	Die Einschluss-/Ausschlussdatei wurde nicht gefunden.
DSM_RC_NO_SYS_OR_INCLEXCL (2230)	Die Datei dsm.sys oder die Einschluss-/Ausschlussdatei wurde nicht gefunden.

dsmTerminate

Mit dem Funktionsaufruf **dsmTerminate** wird eine Sitzung mit dem IBM Spectrum Protect-Server beendet und die IBM Spectrum Protect-Umgebung bereinigt.

Syntax

Es gibt keine spezifischen Rückkehrcodes für diesen Aufruf.

```
dsInt16_t dsmTerminate (dsUint32_t dsmHandle);
```

Parameter

dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.

dsmUpdateFS

Mit dem Funktionsaufruf dsmUpdateFS wird ein Dateibereich im IBM Spectrum Protect-Speicher aktualisiert. Diese Aktualisierung stellt sicher, das der Administrator über einen aktuellen Satz Ihres Dateibereichs verfügt.

Syntax

```
dsInt16_t dsmUpdateFS  (dsUint32_t      dsmHandle,
   char         *fs,
   dsmFSUpd     *fsUpdP,
   dsUint32_t    fsUpdAct);
```

Parameter

dsUint32_t dsmHandle (I)
: Die Kennung, die diesen Aufruf einem vorherigen Aufruf dsmInitEx zuordnet.

char *fs (I)
: Dieser Parameter ist ein Verweis auf den Dateibereichsnamen.

dsmFSUpd *fsUpdP (I)
: Dieser Parameter ist ein Verweis auf die Struktur mit den richtigen Feldern für die gewünschte Aktualisierung. Geben Sie nur Werte für die Felder an, die aktualisiert werden müssen.

dsUint32_t fsUpdAct (I)
: Eine 2-Byte-Bitzuordnung, die angibt, welche Felder aktualisiert werden müssen. Die Bitmasken haben die folgenden Werte:

  - `DSM_FSUPD_FSTYPE`
  - `DSM_FSUPD_FSINFO`
    Tipp: Bei Windows-Betriebssystemen wird auch der Wert für den Laufwerkbuchstaben in dsmDOSAttrib aktualisiert, wenn FSINFO ausgewählt wird.
  - `DSM_FSUPD_OCCUPANCY`
  - `DSM_FSUPD_CAPACITY`
  - `DSM_FSUPD_BACKSTARTDATE`
  - `DSM_FSUPD_BACKCOMPLETEDATE`

  Eine Beschreibung dieser Bitmasken finden Sie in den `DSM_FSUPD`-Definitionen hier: Quellendateien für API-Typdefinitionen.

Rückkehrcodes

In der folgenden Tabelle werden Rückkehrcodes für den Funktionsaufruf dsmUpdateFS aufgelistet.

Tabelle 1. Rückkehrcodes für dsmUpdateFS

Rückkehrcode	Rückkehrcodenummer	Beschreibung
`DSM_RC_FS_NOT_REGISTERED`	2061	Dateibereichsname ist nicht registriert.
`DSM_RC_WRONG_VERSION_PARM`	2065	Die API-Version des Anwendungsclients stimmt nicht mit der Version der IBM Spectrum Protect-Bibliothek überein.
`DSM_RC_FSINFO_TOOLONG`	2106	Dateibereichsinformationen sind zu lang.

dsmUpdateObj

Mit dem Funktionsaufruf **dsmUpdateObj** werden die Metainformationen aktualisiert, die einem aktiven Sicherungs- oder Archivierungsobjekt zugeordnet sind, das sich bereits auf dem Server befindet. Der Aufruf hat keine Auswirkungen auf die Anwendungsbitdaten. Um ein Objekt aktualisieren zu können, müssen Sie einen bestimmten Namen ohne Platzhalterzeichen angeben. Um ein archiviertes Objekt zu aktualisieren, setzen Sie **dsmSendType** auf **stArchive**. Es wird nur das letzte benannte Archivierungsobjekt aktualisiert.

Sie können den Aufruf **dsmUpdateObj** nur im Sitzungsstatus starten; er kann nicht innerhalb einer Transaktion aufgerufen werden, da er seine eigene Transaktion ausführt. Außerdem können Sie jeweils nur ein einziges Objekt aktualisieren.

Einschränkung: Auf einem Betriebssystem UNIX oder Linux können Sie, wenn Sie das Feld für den Eigner ändern, das Objekt nur dann abfragen oder zurückschreiben, wenn Sie der Rootbenutzer sind.

Syntax

```
dsInt16_t  dsmUpdateObj
   (dsUint32_t      dsmHandle,
    dsmSendType     sendType,
    void           *sendBuff,
    dsmObjName     *objNameP,
```

```
    ObjAttr        *objAttrPtr,  /* objInfo */
    dsUint16_t      objUpdAct);  /* Aktionsbitvektor */
```

Parameter

Die Feldbeschreibungen sind mit denen von **dsmSendObj** bis auf die folgenden Ausnahmen identisch:

dsmObjName *objNameP (I)
: Sie können kein Platzhalterzeichen verwenden.

ObjAttr *objAttrPtr (I)
: Das Feld **objCompressed** wird für diesen Aufruf ignoriert.

  Weitere Unterschiede sind:

  - **owner**. Wenn Sie ein neues Feld **owner** angeben, ändert sich der Eigner.
  - **sizeEstimate**. Wenn Sie einen Wert ungleich null angeben, muss das tatsächlich gesendete Datenvolumen in Byte angegeben werden. Der Wert wird für die zukünftige Verwendung in den IBM Spectrum Protect-Metadaten gespeichert.
  - **objInfo**. Dieses Attribut enthält die neuen Informationen, die in das Feld **objInfo** gestellt werden sollen. Setzen Sie **objInfoLength** auf die Länge für die neuen Objektinformationen (**objInfo**).

dsUint16_t objUpdAct
: Die Bitmasken und gültigen Aktionen für **objUpdAct** sind wie folgt:

  DSM_BACKUPD_MC
  : Aktualisiert die Verwaltungsklasse für das Objekt.

  DSM_BACKUPD_OBJINFO
  : Aktualisiert **objInfo**, **objInfoLength** und **sizeEstimate**.

  DSM_BACKUPD_OWNER
  : Aktualisiert den Eigner des Objekts.

  DSM_ARCHUPD_DESCR
  : Aktualisiert das Feld **Description**. Geben Sie den Wert für die neue Beschreibung über den Parameter **SendBuff** ein. Siehe das Musterprogramm zur korrekten Verwendung.

  DSM_ARCHUPD_OBJINFO
  : Aktualisiert **objInfo**, **objInfoLength** und **sizeEstimate**.

  DSM_ARCHUPD_OWNER
  : Aktualisiert den Eigner des Objekts.

Rückkehrcodes

Die Rückkehrcodenummern sind in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmUpdateObj

Rückkehrcode	Erläuterung
DSM_RC_INVALID_ACTION (2232)	Ungültige Aktion.
DSM_RC_FS_NOT_REGISTERED (2061)	Dateibereich nicht registriert.
DSM_RC_BAD_CALL_SEQUENCE (2041)	Aufruffolge ist ungültig.
DSM_RC_WILDCHAR_NOTALLOWED (2050)	Es sind keine Platzhalterzeichen zulässig.
DSM_RC_ABORT_NO_MATCH (2)	Vorherige Abfrage stimmt nicht überein.

dsmUpdateObjEx

Mit dem Funktionsaufruf **dsmUpdateObjEx** werden die Metainformationen aktualisiert, die einem aktiven Sicherungs- oder Archivierungsobjekt zugeordnet sind, das sich auf dem Server befindet. Der Aufruf hat keine Auswirkungen auf die Anwendungsbitdaten. Um ein Objekt aktualisieren zu können, müssen Sie einen Namen ohne Platzhalterzeichen angeben; Sie können auch die Objekt-ID angeben, um ein bestimmtes archiviertes Objekt zu aktualisieren. Bei der Angabe des Namens können Sie keine Platzhalterzeichen verwenden. Um ein Sicherungsobjekt zu aktualisieren, setzen Sie den Parameter **dsmSendType** auf **stBackup**. Um ein archiviertes Objekt zu aktualisieren, setzen Sie den Parameter **dsmSendType** auf **stArchive**.

Sie können den Aufruf **dsmUpdateObjEx** nur im Sitzungsstatus starten; er kann nicht innerhalb einer Transaktion aufgerufen werden, da er seine eigene Transaktion ausführt. Sie können jeweils nur ein einziges Objekt aktualisieren.

Einschränkung: Auf einem Betriebssystem UNIX oder Linux können Sie, wenn Sie das Feld für den Eigner ändern, das Objekt nur dann abfragen oder zurückschreiben, wenn Sie der Rootbenutzer sind. Es kann nur die momentan aktive Version eines Sicherungsobjekts aktualisiert werden.

Syntax

```
dsInt16_t  dsmUpdateObjEx
   (dsmUpdateObjExIn_t   *dsmUpdateObjExInP,
    dsmUpdateObjExOut_t  *dsmUpdateObjExOutP);
```

Parameter

dsmUpdateObjExIn_t *dsmUpdateObjExInP
Diese Struktur enthält die folgenden Eingabeparameter:

dsUint16_t stVersion (I)
Die aktuelle Version der Struktur, die verwendet wird.
dsUint32_t dsmHandle (I)
Die Kennung, die diesen Aufruf einem vorherigen Aufruf **dsmInitEx** zuordnet.
dsmSendType sendType (I)
Der Sendetyp, der ausgeführt wird. Gültige Werte sind:

stBackup
Ein Sicherungsobjekt, das an den Server gesendet wird.
stArchive
Ein Archivierungsobjekt, das an den Server gesendet wird.

dsmObjName *objNameP (I)
Ein Verweis auf die Struktur, die den Dateibereichsnamen, den übergeordneten Objektnamen, den untergeordneten Objektnamen und den Objekttyp enthält. Sie können kein Platzhalterzeichen verwenden.
ObjAttr *objAttrPtr (I)
Übergibt Objektattribute an die Anwendung. Welche Werte aktualisiert werden, ist von den Flags im Feld **objUpdAct** abhängig. Das Attribut **objCompressed** wird für diesen Aufruf ignoriert.

Die Attribute sind:

- **owner**; wenn ein neuer Name eingegeben wird, ändert sich der Eigner.
- **sizeEstimate** ist das tatsächlich gesendete Datenvolumen in Byte. Der Wert wird für die zukünftige Verwendung in den IBM Spectrum Protect-Metadaten gespeichert.
- **objCompressed** ist ein boolescher Wert, der angibt, ob die Objektdaten bereits komprimiert wurden oder nicht.
- **objInfo** ist ein Attribut, das die neuen Informationen enthält, die in das Feld **objInfo** gestellt werden sollen. Setzen Sie **objInfoLength** auf die Länge für die neuen Objektinformationen (**objInfo**).
- **mcNameP** enthält den Namen einer Verwaltungsklasse, die die mit **dsmBindMC** abgerufene Verwaltungsklasse überschreibt.

dsUint32_t objUpdAct
Gibt die Bitmasken und Aktionen für **objUpdAct** an:

DSM_BACKUPD_MC
Aktualisiert die Verwaltungsklasse für das Objekt.
DSM_BACKUPD_OBJINFO
Aktualisiert die Objektinformationen (**objInfo**), die Länge der Objektinformationen (**objInfoLength**) und das gesendete Datenvolumen (**sizeEstimate**) für das Sicherungsobjekt.
DSM_BACKUPD_OWNER
Aktualisiert den Eigner des Sicherungsobjekts.
DSM_ARCHUPD_DESCR
Aktualisiert das Feld **Description** für das Archivierungsobjekt. Geben Sie den Wert für die neue Beschreibung über den Parameter **sendBuff** ein.
DSM_ARCHUPD_OBJINFO
Aktualisiert die Objektinformationen (**objInfo**), die Länge der Objektinformationen (**objInfoLength**) und das gesendete Datenvolumen (**sizeEstimate**) für das Archivierungsobjekt.
DSM_ARCHUPD_OWNER
Aktualisiert den Eigner des Archivierungsobjekts.

ObjID archObjId
Gibt die eindeutige Objekt-ID für ein bestimmtes Archivierungsobjekt an. Da mehrere Archivierungsobjekte denselben Namen haben können, kann über diesen Parameter ein bestimmtes Archivierungsobjekt identifiziert werden. Sie können die Objekt-ID mithilfe eines Abfragearchivaufrufs abrufen.

dsmUpdateObjExOut_t *dsmUpdateObjExOutP
Diese Struktur enthält den Ausgabeparameter:

dsUint16_t stVersion (I)
Die aktuelle Version der Struktur, die verwendet wird.

Rückkehrcodes

Die Rückkehrcodenummern sind in der folgenden Tabelle in runden Klammern ( ) angegeben.

Tabelle 1. Rückkehrcodes für dsmUpdateObjEx

Rückkehrcode	Erläuterung
DSM_RC_INVALID_ACTION (2012)	Ungültige Aktion.
DSM_RC_FS_NOT_REGISTERED (2061)	Dateibereich nicht registriert.
DSM_RC_BAD_CALL_SEQUENCE (2041)	Aufruffolge ist ungültig.
DSM_RC_WILDCHAR_NOTALLOWED (2050)	Es sind keine Platzhalterzeichen zulässig.
DSM_RC_ABORT_NO_MATCH (2)	Vorherige Abfrage stimmt nicht überein.

Quellendatei mit API-Rückkehrcodes: dsmrc.h

Die Headerdatei dsmrc.h enthält alle Rückkehrcodes, die die API an eine Anwendung zurückgeben kann.

Die hier bereitgestellten Informationen enthalten eine Zeitpunktkopie der Datei dsmrc.h, die mit der API verteilt wird. Die neueste Version können Sie der Datei im API-Verteilerpaket entnehmen.

```
/*************************************************************************
* Tivoli Storage Manager                                                 *
* API-Clientkomponente                                                   *
*                                                                        *
* (C) Copyright IBM Corporation 1993, 2010                               *
*************************************************************************/

/*************************************************************************/
/* Headerdateiname:     dsmrc.h                                          */
/*                                                                       */
/* Beschreibender Name: Rückkehrcodes von Tivoli Storage Manager-APIs */
/*************************************************************************/
#ifndef _H_DSMRC
#define _H_DSMRC


#ifndef DSMAPILIB

#ifndef _H_ANSMACH
typedef int RetCode ;
#endif

#endif


#define DSM_RC_SUCCESSFUL               0 /* erfolgreiche Ausführung */
#define DSM_RC_OK                       0 /* erfolgreiche Ausführung */

#define DSM_RC_UNSUCCESSFUL            -1 /* nicht erfolgr. Ausführ. */

/* dsmEndTxn Ursachencode */
#define DSM_RS_ABORT_SYSTEM_ERROR           1
#define DSM_RS_ABORT_NO_MATCH               2
#define DSM_RS_ABORT_BY_CLIENT              3
#define DSM_RS_ABORT_ACTIVE_NOT_FOUND       4
#define DSM_RS_ABORT_NO_DATA                5
#define DSM_RS_ABORT_BAD_VERIFIER           6
#define DSM_RS_ABORT_NODE_IN_USE            7
#define DSM_RS_ABORT_EXPDATE_TOO_LOW        8
#define DSM_RS_ABORT_DATA_OFFLINE           9
#define DSM_RS_ABORT_EXCLUDED_BY_SIZE       10
#define DSM_RS_ABORT_NO_STO_SPACE_SKIP      11
#define DSM_RS_ABORT_NO_REPOSIT_SPACE       DSM_RS_ABORT_NO_STO_SPACE_SKIP
#define DSM_RS_ABORT_MOUNT_NOT_POSSIBLE     12
#define DSM_RS_ABORT_SIZESTIMATE_EXCEED     13
#define DSM_RS_ABORT_DATA_UNAVAILABLE       14
#define DSM_RS_ABORT_RETRY                  15
#define DSM_RS_ABORT_NO_LOG_SPACE           16
#define DSM_RS_ABORT_NO_DB_SPACE            17
#define DSM_RS_ABORT_NO_MEMORY              18

#define DSM_RS_ABORT_FS_NOT_DEFINED         20
#define DSM_RS_ABORT_NODE_ALREADY_DEFED     21
#define DSM_RS_ABORT_NO_DEFAULT_DOMAIN      22
#define DSM_RS_ABORT_INVALID_NODENAME       23
#define DSM_RS_ABORT_INVALID_POL_BIND       24
#define DSM_RS_ABORT_DEST_NOT_DEFINED       25
#define DSM_RS_ABORT_WAIT_FOR_SPACE         26
```

```
#define DSM_RS_ABORT_NOT_AUTHORIZED          27
#define DSM_RS_ABORT_RULE_ALREADY_DEFED      28
#define DSM_RS_ABORT_NO_STOR_SPACE_STOP      29

#define DSM_RS_ABORT_LICENSE_VIOLATION       30
#define DSM_RS_ABORT_EXTOBJID_ALREADY_EXISTS 31
#define DSM_RS_ABORT_DUPLICATE_OBJECT        32

#define DSM_RS_ABORT_INVALID_OFFSET          33    /* Teilobjektabruf         */
#define DSM_RS_ABORT_INVALID_LENGTH          34    /* Teilobjektabruf         */
#define DSM_RS_ABORT_STRING_ERROR            35
#define DSM_RS_ABORT_NODE_NOT_AUTHORIZED     36
#define DSM_RS_ABORT_RESTART_NOT_POSSIBLE    37
#define DSM_RS_ABORT_RESTORE_IN_PROGRESS     38
#define DSM_RS_ABORT_SYNTAX_ERROR            39

#define DSM_RS_ABORT_DATA_SKIPPED            40
#define DSM_RS_ABORT_EXCEED_MAX_MP           41
#define DSM_RS_ABORT_NO_OBJSET_MATCH         42
#define DSM_RS_ABORT_PVR_ERROR               43
#define DSM_RS_ABORT_BAD_RECOGTOKEN          44
#define DSM_RS_ABORT_MERGE_ERROR             45
#define DSM_RS_ABORT_FSRENAME_ERROR          46
#define DSM_RS_ABORT_INVALID_OPERATION       47
#define DSM_RS_ABORT_STGPOOL_UNDEFINED       48
#define DSM_RS_ABORT_INVALID_DATA_FORMAT     49
#define DSM_RS_ABORT_DATAMOVER_UNDEFINED     50

#define DSM_RS_ABORT_INVALID_MOVER_TYPE      231
#define DSM_RS_ABORT_ITEM_IN_USE             232
#define DSM_RS_ABORT_LOCK_CONFLICT           233
#define DSM_RS_ABORT_SRV_PLUGIN_COMM_ERROR   234
#define DSM_RS_ABORT_SRV_PLUGIN_OS_ERROR     235
#define DSM_RS_ABORT_CRC_FAILED              236
#define DSM_RS_ABORT_INVALID_GROUP_ACTION    237
#define DSM_RS_ABORT_DISK_UNDEFINED          238
#define DSM_RS_ABORT_BAD_DESTINATION         239
#define DSM_RS_ABORT_DATAMOVER_NOT_AVAILABLE 240
#define DSM_RS_ABORT_STGPOOL_COPY_CONT_NO    241
#define DSM_RS_ABORT_RETRY_SINGLE_TXN        242
#define DSM_RS_ABORT_TOC_CREATION_FAIL       243
#define DSM_RS_ABORT_TOC_LOAD_FAIL           244
#define DSM_RS_ABORT_PATH_RESTRICTED         245
#define DSM_RS_ABORT_NO_LANFREE_SCRATCH      246
#define DSM_RS_ABORT_INSERT_NOT_ALLOWED      247
#define DSM_RS_ABORT_DELETE_NOT_ALLOWED      248
#define DSM_RS_ABORT_TXN_LIMIT_EXCEEDED      249
#define DSM_RS_ABORT_OBJECT_ALREADY_HELD     250
#define DSM_RS_ABORT_INVALID_CHUNK_REFERENCE 254
#define DSM_RS_ABORT_DESTINATION_NOT_DEDUP   255
#define DSM_RS_ABORT_DESTINATION_POOL_CHANGED 257
#define DSM_RS_ABORT_NOT_ROOT                258


/* RÜCKKEHRCODE */

#define DSM_RC_ABORT_SYSTEM_ERROR            DSM_RS_ABORT_SYSTEM_ERROR
#define DSM_RC_ABORT_NO_MATCH                DSM_RS_ABORT_NO_MATCH
#define DSM_RC_ABORT_BY_CLIENT               DSM_RS_ABORT_BY_CLIENT
#define DSM_RC_ABORT_ACTIVE_NOT_FOUND        DSM_RS_ABORT_ACTIVE_NOT_FOUND
#define DSM_RC_ABORT_NO_DATA                 DSM_RS_ABORT_NO_DATA
#define DSM_RC_ABORT_BAD_VERIFIER            DSM_RS_ABORT_BAD_VERIFIER
#define DSM_RC_ABORT_NODE_IN_USE             DSM_RS_ABORT_NODE_IN_USE
#define DSM_RC_ABORT_EXPDATE_TOO_LOW         DSM_RS_ABORT_EXPDATE_TOO_LOW
#define DSM_RC_ABORT_DATA_OFFLINE            DSM_RS_ABORT_DATA_OFFLINE
#define DSM_RC_ABORT_EXCLUDED_BY_SIZE        DSM_RS_ABORT_EXCLUDED_BY_SIZE

#define DSM_RC_ABORT_NO_REPOSIT_SPACE        DSM_RS_ABORT_NO_STO_SPACE_SKIP
#define DSM_RC_ABORT_NO_STO_SPACE_SKIP       DSM_RS_ABORT_NO_STO_SPACE_SKIP

#define DSM_RC_ABORT_MOUNT_NOT_POSSIBLE      DSM_RS_ABORT_MOUNT_NOT_POSSIBLE
#define DSM_RC_ABORT_SIZESTIMATE_EXCEED      DSM_RS_ABORT_SIZESTIMATE_EXCEED
#define DSM_RC_ABORT_DATA_UNAVAILABLE        DSM_RS_ABORT_DATA_UNAVAILABLE
#define DSM_RC_ABORT_RETRY                   DSM_RS_ABORT_RETRY
#define DSM_RC_ABORT_NO_LOG_SPACE            DSM_RS_ABORT_NO_LOG_SPACE
#define DSM_RC_ABORT_NO_DB_SPACE             DSM_RS_ABORT_NO_DB_SPACE
#define DSM_RC_ABORT_NO_MEMORY               DSM_RS_ABORT_NO_MEMORY

#define DSM_RC_ABORT_FS_NOT_DEFINED          DSM_RS_ABORT_FS_NOT_DEFINED
#define DSM_RC_ABORT_NODE_ALREADY_DEFED      DSM_RS_ABORT_NODE_ALREADY_DEFED
#define DSM_RC_ABORT_NO_DEFAULT_DOMAIN       DSM_RS_ABORT_NO_DEFAULT_DOMAIN
#define DSM_RC_ABORT_INVALID_NODENAME        DSM_RS_ABORT_INVALID_NODENAME
```

```
#define DSM_RC_ABORT_INVALID_POL_BIND        DSM_RS_ABORT_INVALID_POL_BIND
#define DSM_RC_ABORT_DEST_NOT_DEFINED        DSM_RS_ABORT_DEST_NOT_DEFINED
#define DSM_RC_ABORT_WAIT_FOR_SPACE          DSM_RS_ABORT_WAIT_FOR_SPACE
#define DSM_RC_ABORT_NOT_AUTHORIZED          DSM_RS_ABORT_NOT_AUTHORIZED
#define DSM_RC_ABORT_RULE_ALREADY_DEFED      DSM_RS_ABORT_RULE_ALREADY_DEFED
#define DSM_RC_ABORT_NO_STOR_SPACE_STOP      DSM_RS_ABORT_NO_STOR_SPACE_STOP

#define DSM_RC_ABORT_LICENSE_VIOLATION       DSM_RS_ABORT_LICENSE_VIOLATION
#define DSM_RC_ABORT_EXTOBJID_ALREADY_EXISTS DSM_RS_ABORT_EXTOBJID_ALREADY_EXISTS
#define DSM_RC_ABORT_DUPLICATE_OBJECT        DSM_RS_ABORT_DUPLICATE_OBJECT

#define DSM_RC_ABORT_INVALID_OFFSET          DSM_RS_ABORT_INVALID_OFFSET
#define DSM_RC_ABORT_INVALID_LENGTH          DSM_RS_ABORT_INVALID_LENGTH

#define DSM_RC_ABORT_STRING_ERROR            DSM_RS_ABORT_STRING_ERROR
#define DSM_RC_ABORT_NODE_NOT_AUTHORIZED     DSM_RS_ABORT_NODE_NOT_AUTHORIZED
#define DSM_RC_ABORT_RESTART_NOT_POSSIBLE    DSM_RS_ABORT_RESTART_NOT_POSSIBLE
#define DSM_RC_ABORT_RESTORE_IN_PROGRESS     DSM_RS_ABORT_RESTORE_IN_PROGRESS
#define DSM_RC_ABORT_SYNTAX_ERROR            DSM_RS_ABORT_SYNTAX_ERROR

#define DSM_RC_ABORT_DATA_SKIPPED            DSM_RS_ABORT_DATA_SKIPPED
#define DSM_RC_ABORT_EXCEED_MAX_MP           DSM_RS_ABORT_EXCEED_MAX_MP
#define DSM_RC_ABORT_NO_OBJSET_MATCH         DSM_RS_ABORT_NO_OBJSET_MATCH
#define DSM_RC_ABORT_PVR_ERROR               DSM_RS_ABORT_PVR_ERROR
#define DSM_RC_ABORT_BAD_RECOGTOKEN          DSM_RS_ABORT_BAD_RECOGTOKEN
#define DSM_RC_ABORT_MERGE_ERROR             DSM_RS_ABORT_MERGE_ERROR
#define DSM_RC_ABORT_FSRENAME_ERROR          DSM_RS_ABORT_FSRENAME_ERROR
#define DSM_RC_ABORT_INVALID_OPERATION       DSM_RS_ABORT_INVALID_OPERATION
#define DSM_RC_ABORT_STGPOOL_UNDEFINED       DSM_RS_ABORT_STGPOOL_UNDEFINED
#define DSM_RC_ABORT_INVALID_DATA_FORMAT     DSM_RS_ABORT_INVALID_DATA_FORMAT
#define DSM_RC_ABORT_DATAMOVER_UNDEFINED     DSM_RS_ABORT_DATAMOVER_UNDEFINED

#define DSM_RC_ABORT_INVALID_MOVER_TYPE      DSM_RS_ABORT_INVALID_MOVER_TYPE
#define DSM_RC_ABORT_ITEM_IN_USE             DSM_RS_ABORT_ITEM_IN_USE
#define DSM_RC_ABORT_LOCK_CONFLICT           DSM_RS_ABORT_LOCK_CONFLICT
#define DSM_RC_ABORT_SRV_PLUGIN_COMM_ERROR   DSM_RS_ABORT_SRV_PLUGIN_COMM_ERROR
#define DSM_RC_ABORT_SRV_PLUGIN_OS_ERROR     DSM_RS_ABORT_SRV_PLUGIN_OS_ERROR
#define DSM_RC_ABORT_CRC_FAILED              DSM_RS_ABORT_CRC_FAILED
#define DSM_RC_ABORT_INVALID_GROUP_ACTION    DSM_RS_ABORT_INVALID_GROUP_ACTION
#define DSM_RC_ABORT_DISK_UNDEFINED          DSM_RS_ABORT_DISK_UNDEFINED
#define DSM_RC_ABORT_BAD_DESTINATION         DSM_RS_ABORT_BAD_DESTINATION
#define DSM_RC_ABORT_DATAMOVER_NOT_AVAILABLE DSM_RS_ABORT_DATAMOVER_NOT_AVAILABLE
#define DSM_RC_ABORT_STGPOOL_COPY_CONT_NO    DSM_RS_ABORT_STGPOOL_COPY_CONT_NO
#define DSM_RC_ABORT_RETRY_SINGLE_TXN        DSM_RS_ABORT_RETRY_SINGLE_TXN
#define DSM_RC_ABORT_TOC_CREATION_FAIL       DSM_RS_ABORT_TOC_CREATION_FAIL
#define DSM_RC_ABORT_TOC_LOAD_FAIL           DSM_RS_ABORT_TOC_LOAD_FAIL
#define DSM_RC_ABORT_PATH_RESTRICTED         DSM_RS_ABORT_PATH_RESTRICTED
#define DSM_RC_ABORT_NO_LANFREE_SCRATCH      DSM_RS_ABORT_NO_LANFREE_SCRATCH
#define DSM_RC_ABORT_INSERT_NOT_ALLOWED      DSM_RS_ABORT_INSERT_NOT_ALLOWED
#define DSM_RC_ABORT_DELETE_NOT_ALLOWED      DSM_RS_ABORT_DELETE_NOT_ALLOWED
#define DSM_RC_ABORT_TXN_LIMIT_EXCEEDED      DSM_RS_ABORT_TXN_LIMIT_EXCEEDED
#define DSM_RC_ABORT_OBJECT_ALREADY_HELD     DSM_RS_ABORT_OBJECT_ALREADY_HELD
#define DSM_RC_ABORT_INVALID_CHUNK_REFERENCE DSM_RS_ABORT_INVALID_CHUNK_REFERENCE
#define DSM_RC_ABORT_DESTINATION_NOT_DEDUP   DSM_RS_ABORT_DESTINATION_NOT_DEDUP
#define DSM_RC_ABORT_DESTINATION_POOL_CHANGED DSM_RS_ABORT_DESTINATION_POOL_CHANGED
#define DSM_RC_ABORT_NOT_ROOT                DSM_RS_ABORT_NOT_ROOT

#define DSM_RC_ABORT_CERTIFICATE_NOT_FOUND   DSM_RS_ABORT_CERTIFICATE_NOT_FOUND

/* Definitionen für Codes für Zurückweisung der Serveranmeldung        */
/* Diese Fehlercodes liegen zwischen 51 und 99 einschließlich.         */
#define DSM_RC_REJECT_NO_RESOURCES           51
#define DSM_RC_REJECT_VERIFIER_EXPIRED       52
#define DSM_RC_REJECT_ID_UNKNOWN             53
#define DSM_RC_REJECT_DUPLICATE_ID           54
#define DSM_RC_REJECT_SERVER_DISABLED        55
#define DSM_RC_REJECT_CLOSED_REGISTER        56
#define DSM_RC_REJECT_CLIENT_DOWNLEVEL       57
#define DSM_RC_REJECT_SERVER_DOWNLEVEL       58
#define DSM_RC_REJECT_ID_IN_USE              59
#define DSM_RC_REJECT_ID_LOCKED              61
#define DSM_RC_SIGNONREJECT_LICENSE_MAX      62
#define DSM_RC_REJECT_NO_MEMORY              63
#define DSM_RC_REJECT_NO_DB_SPACE            64
#define DSM_RC_REJECT_NO_LOG_SPACE           65
#define DSM_RC_REJECT_INTERNAL_ERROR         66
#define DSM_RC_SIGNONREJECT_INVALID_CLI      67 /* Clienttyp nicht lizenz.  */
#define DSM_RC_CLIENT_NOT_ARCHRETPROT        68
#define DSM_RC_REJECT_LASTSESS_CANCELED      69
#define DSM_RC_REJECT_UNICODE_NOT_ALLOWED    70
#define DSM_RC_REJECT_NOT_AUTHORIZED         71
#define DSM_RC_REJECT_TOKEN_TIMEOUT          72
```

```
#define DSM_RC_REJECT_INVALID_NODE_TYPE      73
#define DSM_RC_REJECT_INVALID_SESSIONINIT    74
#define DSM_RC_REJECT_WRONG_PORT             75
#define DSM_RC_CLIENT_NOT_SPMRETPROT         79



#define DSM_RC_USER_ABORT          101 /* Verarbeitung vom Ben. abgebrochen */
#define DSM_RC_NO_MEMORY           102 /* kein RAM für Anforderungsausführ. */
#define DSM_RC_TA_COMM_DOWN       2021 /* nicht mehr verwendet              */
#define DSM_RC_FILE_NOT_FOUND      104 /* angegebene Datei nicht gefunden   */
#define DSM_RC_PATH_NOT_FOUND      105 /* angegebener Pfad nicht vorhanden  */
#define DSM_RC_ACCESS_DENIED       106 /* wg. falscher Berecht. zurückgew.  */
#define DSM_RC_NO_HANDLES          107 /* keine Dateikennungen mehr verfügb.*/
#define DSM_RC_FILE_EXISTS         108 /* Datei ist bereits vorhanden       */
#define DSM_RC_INVALID_PARM        109 /* ungült. Param. übergeben. KRITISCH*/
#define DSM_RC_INVALID_HANDLE      110 /* ungültige Dateikennung übergeben  */
#define DSM_RC_DISK_FULL           111 /* kein Plattenspeicherplatz verfügb.*/
#define DSM_RC_PROTOCOL_VIOLATION  113 /* fehlerh. Protokollaufruf. KRITISCH*/
#define DSM_RC_UNKNOWN_ERROR       114 /* unbekannter Systemfehler. KRITISCH*/
#define DSM_RC_UNEXPECTED_ERROR    115 /* unerwarteter Fehler. KRITISCH     */
#define DSM_RC_FILE_BEING_EXECUTED 116 /* Schreiben nicht zulässig          */
#define DSM_RC_DIR_NO_SPACE        117 /* Verz. kann nicht erweitert werden */
#define DSM_RC_LOOPED_SYM_LINK     118 /* zu viele symbolische Verbindungen
                                          beim Umsetzen des Pfads gefunden  */
#define DSM_RC_FILE_NAME_TOO_LONG  119 /* Dateiname zu lang                 */
#define DSM_RC_FILE_SPACE_LOCKED   120 /* Dateibereich vom System gesperrt  */
#define DSM_RC_FINISHED            121 /* Verarbeitung beendet              */
#define DSM_RC_UNKNOWN_FORMAT      122 /* unbekanntes Format                */
#define DSM_RC_NO_AUTHORIZATION    123 /* Serverantwort, wenn Client keine
                                          Berechtigung zum Lesen der Daten
                                          des Eigners eines anderen Hosts
                                          für Sichern/Archivieren hat       */
#define DSM_RC_FILE_SPACE_NOT_FOUND 124/* angeg. Dateibereich nicht gefunden*/
#define DSM_RC_TXN_ABORTED         125 /* Transaktion abgebrochen           */
#define DSM_RC_SUBDIR_AS_FILE      126 /* Unterverzeichnisname als Datei
                                          vorhanden                         */
#define DSM_RC_PROCESS_NO_SPACE    127 /* kein weiterer Plattenspeicherplatz
                                          für Prozess vorhanden             */
#define DSM_RC_PATH_TOO_LONG       128 /* ein erstellter Verzeichnispfad ist
                                          zu lang                           */
#define DSM_RC_NOT_COMPRESSED      129 /* Datei, die komprimiert sein sollte,
                                          ist nicht komprimiert             */
#define DSM_RC_TOO_MANY_BITS       130 /* Datei mit mehr Bit komprimiert,
                                          als Expander handhaben            */
#define DSM_RC_SYSTEM_ERROR        131 /* interner Systemfehler             */
#define DSM_RC_NO_SERVER_RESOURCES 132 /* keine Ressourcen für Server verf. */
#define DSM_RC_FS_NOT_KNOWN        133 /* Dateibereich ist dem Server nicht
                                          bekannt                           */
#define DSM_RC_NO_LEADING_DIRSEP   134 /* kein führendes Verzeichnistrennz. */
#define DSM_RC_WILDCARD_DIR        135 /* Platzhalterzeichen in Verzeichnis-
                                          pfad an unzulässiger Stelle       */
#define DSM_RC_COMM_PROTOCOL_ERROR 136 /* Übertragungsprotokollfehler       */
#define DSM_RC_AUTH_FAILURE        137 /* Authentifizierungsfehler          */
#define DSM_RC_TA_NOT_VALID        138 /* TA kein Root und/od. SUID-Programm*/
#define DSM_RC_KILLED              139 /* Prozess abgebrochen               */

#define DSM_RC_RETRY               143 /* dieselbe Operation wiederholen    */

#define DSM_RC_WOULD_BLOCK         145 /* Operation hätte das Blockieren des
                                          Systems zur Folge, um auf Eingabe
                                          zu warten.                        */
#define DSM_RC_TOO_SMALL           146 /* Bereich f. kompil. Muster zu klein*/
#define DSM_RC_UNCLOSED            147 /* keine rechte eckige Klammer in
                                          Muster                            */
#define DSM_RC_NO_STARTING_DELIMITER 148 /* Muster muss mit Verzeichnis-
                                            begrenzer beginnen              */
#define DSM_RC_NEEDED_DIR_DELIMITER 149 /* direkt vor und hinter der Meta-
                                           zeichenfolge ("...") für den
                                           Verzeichnisabgleich ist ein Ver-
                                           zeichnisbegrenzer erforderlich,
                                           es wurde jedoch keiner gefunden   */
#define DSM_RC_UNKNOWN_FILE_DATA_TYPE 150 /* strukturierter Dateidatentyp
                                             ist unbekannt                  */
#define DSM_RC_BUFFER_OVERFLOW     151 /* Datenpufferüberlauf               */


#define DSM_RC_NO_COMPRESS_MEMORY  154 /* kein Speicher für Erweitern/Kompr.*/
#define DSM_RC_COMPRESS_GREW       155 /* Komprimierung gewachsen           */
#define DSM_RC_INV_COMM_METHOD     156 /* Ungültige Übertragungsmethode ang.*/
#define DSM_RC_WILL_ABORT          157 /* Transaktion wird abgebrochen      */
#define DSM_RC_FS_WRITE_LOCKED     158 /* Schreibsperre für Dateibereich    */
```

```
#define DSM_RC_SKIPPED_BY_USER     159 /* Benutzeranforderung, Datei bei
                                           ABORT_DATA_OFFLINE zu überspringen*/
#define DSM_RC_TA_NOT_FOUND        160 /* TA in Verzeichnis nicht gefunden  */
#define DSM_RC_TA_ACCESS_DENIED    161 /* Zugriff auf TA verweigert         */
#define DSM_RC_FS_NOT_READY        162 /* Dateibereich nicht bereit         */
#define DSM_RC_FS_IS_BAD           163 /* Dateibereich ungültig             */
#define DSM_RC_FIO_ERROR           164 /* Dateiein-/ausgabefehler           */
#define DSM_RC_WRITE_FAILURE       165 /* Fehler beim Schreiben in Datei    */
#define DSM_RC_OVER_FILE_SIZE_LIMIT 166 /* Datei über System-/Benutzer-
                                           Grenzwert                         */
#define DSM_RC_CANNOT_MAKE         167 /* Datei/Verzeichnis konnte wegen
                                           eines ungültigen Namens nicht
                                           erstellt werden                   */
#define DSM_RC_NO_PASS_FILE        168 /* Kennwortdatei erforderlich und
                                           Benutzer ist nicht Rootbenutzer   */
#define DSM_RC_VERFILE_OLD         169 /* lokal gespeichertes Kennwort stimmt
                                           nicht mit dem auf Host überein    */
#define DSM_RC_INPUT_ERROR         173 /* Tastatureingabe kann nicht gelesen
                                           werden                            */
#define DSM_RC_REJECT_PLATFORM_MISMATCH 174 /* Plattformname stimmt nicht mit
                                              der Angabe überein, die laut
                                              Server die Plattform für den
                                              Client ist                     */
#define DSM_RC_TL_NOT_FILE_OWNER   175 /* Benutzer, der versucht, Datei zu
                                           sichern, ist nicht Dateieigner.   */
#define DSM_RC_COMPRESSED_DATA_CORRUPTED 176 /* komprim. Daten beschädigt   */
#define DSM_RC_UNMATCHED_QUOTE     177 /* fehlendes Anführungszeichen am
                                           Anfang oder Ende                  */

#define DSM_RC_SIGNON_FAILOVER_MODE 178 /* Übernahme auf Replikationsserver,
                                           aktiv im Übernahmemodus     */
#define DSM_RC_FAILOVER_MODE_FUNC_BLOCKED 179 /* Funktion blockiert, weil
                                           Sitzung im Übernahmemodus  */

/*-----------------------------------------------------------------------*/
/* Rückkehrcodes 180-199 sind für Handhabung von Maßnahmengruppen reserviert */
/*-----------------------------------------------------------------------*/
#define DSM_RC_PS_MULTBCG          181 /* Mehrere Sicherungskopiengruppen in
                                           1 Verwaltungsklasse               */
#define DSM_RC_PS_MULTACG          182 /* Mehrere Archivierungskopiengruppen
                                           in 1 Verwaltungsklasse            */
#define DSM_RC_PS_NODFLTMC         183 /* Standardverwaltungsklassenname
                                           nicht in Maßnahmengruppe          */
#define DSM_RC_TL_NOBCG            184 /* Sicherung erforderlich; keine
                                           Sicherungskopiengruppe            */
#define DSM_RC_TL_EXCLUDED         185 /* Sicherung erforderlich; von Ein-/
                                           Ausschlussfilter ausgeschlossen   */
#define DSM_RC_TL_NOACG            186 /* Archivierung erforderlich; keine
                                           Archivierungskopiengruppe         */
#define DSM_RC_PS_INVALID_ARCHMC   187 /* Ungültiger Verwaltungsklassenname
                                           in Archivierungsüberschreibung    */
#define DSM_RC_NO_PS_DATA          188 /* Keine Maßnahmengruppendaten auf dem
                                           Server                            */
#define DSM_RC_PS_INVALID_DIRMC    189 /* Ungültiges Verzeichnis MC in
                                           Optionsdatei angegeben            */
#define DSM_RC_PS_NO_CG_IN_DIR_MC  190 /* Keine Sicherungskopiengruppe in
                                           Verzeichnis MC. Verwaltungsklasse
                                           muss mit Option DirMC ang. werden. */

#define DSM_RC_WIN32_UNSUPPORTED_FILE_TYPE 280 /* Datei hat nicht Win32-Typ
                                             FILE_TYPE_DISK            */

/*-----------------------------------------------------------------------*/
/* Rückkehrcodes für Trusted Communication Agent                         */
/*-----------------------------------------------------------------------*/
#define DSM_RC_TCA_NOT_ROOT        161 /* Zugriff auf TA verweigert         */
#define DSM_RC_TCA_ATTACH_SHR_MEM_ERR  200 /* Fehler beim Zuordnen von
                                           gemeinsam genutztem Speicher   */
#define DSM_RC_TCA_SHR_MEM_BLOCK_ERR   200 /* Fehler bei Shared-Memory-Block */
#define DSM_RC_TCA_SHR_MEM_IN_USE      200 /* Fehler bei Shared-Memory-Block */
#define DSM_RC_TCA_SHARED_MEMORY_ERROR 200 /* Fehler bei Shared-Memory-Block */
#define DSM_RC_TCA_SEGMENT_MISMATCH    200 /* Fehler bei Shared-Memory-Block */
#define DSM_RC_TCA_FORK_FAILED     292 /* Fehler beim Abzweigen v. TA-Prozess*/
#define DSM_RC_TCA_DIED            294 /* TCA unerwartet inaktiviert        */
#define DSM_RC_TCA_INVALID_REQUEST 295 /* Ungültige Anford. an TCA gesendet  */
#define DSM_RC_TCA_SEMGET_ERROR    297 /* Fehler beim Abrufen von Semaphors  */
#define DSM_RC_TCA_SEM_OP_ERROR    298 /* Fehler bei Semaphorgruppe oder
                                           Warten                            */
#define DSM_RC_TCA_NOT_ALLOWED     299 /* TCA nicht zulässig (Multithread)   */

/*-----------------------------------------------------------------------*/
/* 400-430  für Optionen                                                 */
```

```
/*------------------------------------------------------------------------*/
#define DSM_RC_INVALID_OPT           400 /* ungültige Option                */
#define DSM_RC_NO_HOST_ADDR          405 /* Nicht genügend Informationen, um
                                            Verbindung zu Server herzustellen*/
#define DSM_RC_NO_OPT_FILE           406 /* Keine Standardbenutzerkonf.-Datei*/
#define DSM_RC_MACHINE_SAME          408 /* -MACHINENAME = realer Name       */
#define DSM_RC_INVALID_SERVER        409 /* ungültiger Servername von Client */
#define DSM_RC_INVALID_KEYWORD       410 /* ungültiges Optionsschlüsselwort  */
#define DSM_RC_PATTERN_TOO_COMPLEX   411 /* Einschluss-/Ausschluss kann nicht
                                            abgeglichen werden               */
#define DSM_RC_NO_CLOSING_BRACKET    412 /* Fehlende rechte eckige Klammer
                                            für Einschluss/Ausschluss        */
#define DSM_RC_OPT_CLIENT_NOT_ACCEPTING 417/* Client akzeptiert diese Option
                                            nicht vom Server                 */
#define DSM_RC_OPT_CLIENT_DOES_NOT_WANT 418/* Client will diesen Wert
                                            nicht vom Server                 */
#define DSM_RC_OPT_NO_INCLEXCL_FILE  419   /* Einschluss-/Ausschlussdatei
                                            nicht gefunden                   */
#define DSM_RC_OPT_OPEN_FAILURE      420   /* Datei kann nicht geöffnet
                                            werden                           */
#define DSM_RC_OPT_INV_NODENAME      421   /* für Windows, wenn nodename=lokale
                                            Maschine, wenn CLUSTERNODE=YES */
#define DSM_RC_OPT_NODENAME_INVALID  423   /* ungült. generischer Knotenname */
#define DSM_RC_OPT_ERRORLOG_CONFLICT 424   /* logmax & Aufbewahrungsdauer
                                            angegeben                        */
#define DSM_RC_OPT_SCHEDLOG_CONFLICT 425   /* logmax & Aufbewahrungsdauer
                                            angegeben                        */
#define DSM_RC_CANNOT_OPEN_TRACEFILE 426   /* Tracedatei kann nicht geöffnet
                                            werden                           */
#define DSM_RC_CANNOT_OPEN_LOGFILE   427   /* Fehlerprotokolldatei kann nicht
                                            geöffnet werden                  */
#define DSM_RC_OPT_SESSINIT_LF_CONFLICT 428/* sessioninit=server und

enablelanfree=yes angegeben    */
#define DSM_RC_OPT_OPTION_IGNORE     429   /* Option wird ignoriert           */
#define DSM_RC_OPT_DEDUP_CONFLICT    430   /* Fehlerprotokolldatei kann nicht
                                            geöffnet werden                  */
#define DSM_RC_OPT_HSMLOG_CONFLICT 431/* logmax & Aufbewahrungsdauer angegeben */


/*------------------------------------------------------------------------*/
/* 600 bis 610 für Datenträgerkennsatzcodes                               */
/*------------------------------------------------------------------------*/
#define DSM_RC_DUP_LABEL           600 /* doppelten Datenträgerkennsatz
                                          gefunden                         */
#define DSM_RC_NO_LABEL            601 /* Laufwerk hat keinen Kennsatz     */

/*------------------------------------------------------------------------*/
/* Rückkehrcodes für Nachrichtendateiverarbeitung                         */
/*------------------------------------------------------------------------*/
#define DSM_RC_NLS_CANT_OPEN_TXT   610 /* Fehler beim Öffnen der Nachrichten-
                                          textdatei                        */
#define DSM_RC_NLS_CANT_READ_HDR   611 /* Fehler beim Lesen von Header     */
#define DSM_RC_NLS_INVALID_CNTL_REC 612 /* ungültiger Steuersatz           */
#define DSM_RC_NLS_INVALID_DATE_FMT 613 /* ungültiges Standarddatumsformat */
#define DSM_RC_NLS_INVALID_TIME_FMT 614 /* ungültiges Standardzeitformat   */
#define DSM_RC_NLS_INVALID_NUM_FMT 615 /* ungültiges Standardzahlenformat  */

/*------------------------------------------------------------------------*/
/* Rückkehrcodes 620-630 für Rückkehrcodes f. Protokollnachrichten reserviert*/
/*------------------------------------------------------------------------*/
#define DSM_RC_LOG_CANT_BE_OPENED  620     /* Fehler beim Öffnen des
                                              Fehlerprotokolls               */
#define DSM_RC_LOG_ERROR_WRITING_TO_LOG 621 /* Fehler beim Schreiben in
                                              Protokolldatei                 */
#define DSM_RC_LOG_NOT_SPECIFIED   622     /* keine Fehlerprotokolldatei
                                              angegeben                      */


/*------------------------------------------------------------------------*/
/* Rückkehrcode  900-999 NUR TSM-CLIENT                                   */
/*------------------------------------------------------------------------*/
#define DSM_RC_NOT_ADSM_AUTHORIZED  927  /* Muss für ADSM berechtigt sein, um
                                            Aktion ausführen zu können: Root
                                            oder Kennwortberechtigung      */
#define DSM_RC_REJECT_USERID_UNKNOWN 940 /* Benutzer-ID auf Server unbekannt */
#define DSM_RC_FILE_IS_SYMLINK      959  /* Fehlerprotokoll oder Trace ist
                                            eine symbolische Verbindung    */

#define DSM_RC_DIRECT_STORAGE_AGENT_UNSUPPORTED 961 /* Direktverbindung zu
                                                       Speicheragent nicht
                                                       unterstützt         */
```

```
#define DSM_RC_FS_NAMESPACE_DOWNLEVEL 963 /* Langer Namensbereich wurde aus
                                             Netware-Datenträger entfernt    */
#define DSM_RC_CONTINUE_NEW_CONSUMER   972 /* Verarbeitung mit neuem
                                             Konsumenten fortsetzen          */
#define DSM_RC_CONTINUE_NEW_CONSUMER_NODEDUP   973 /* Verarbeitung mit neuem
                                                     Konsumenten fortsetzen;
                                                     keine Deduplizierung   */
#define DSM_RC_CONTINUE_NEW_CONSUMER_NOCOMPRESS 976 /* Verarbeitung mit neuem
                                                      Konsumenten fortsetzen;
                                                      keine Komprimierung   */


#define DSM_RC_SERVER_SUPPORTS_FUNC    994 /* Server unterstützt diese Funktion  */
#define DSM_RC_SERVER_AND_SA_SUPPORT_FUNC 995 /* Server und Speicheragent
                                                 unterstützen die Funktion       */
#define DSM_RC_SERVER_DOWNLEVEL_FUNC   996 /* Serverversion ist für Funktion
                                             veraltet                        */
#define DSM_RC_STORAGEAGENT_DOWNLEVEL  997 /* Speicheragentenversion ist veraltet*/
#define DSM_RC_SERVER_AND_SA_DOWNLEVEL 998 /* Server- und Speicheragentenversion
                                             sind veraltet                   */


/* TCP/IP-Fehlercodes */
#define DSM_RC_TCPIP_FAILURE       -50 /* TCP/IP-Übertragungsfehler          */
#define DSM_RC_CONN_TIMEDOUT       -51 /* Zeitlimitüberschreitung bei
                                          TCP/IP-Verbindung                  */
#define DSM_RC_CONN_REFUSED        -52 /* TCP/IP-Verbindung von Host
                                          zurückgewiesen                     */
#define DSM_RC_BAD_HOST_NAME       -53 /* Ungültiger TCP/IP-Hostname angeg.  */
#define DSM_RC_NETWORK_UNREACHABLE -54 /* TCP/IP-Hostname nicht erreichbar   */
#define DSM_RC_WINSOCK_MISSING     -55 /* TCP/IP-Datei WINSOCK.DLL fehlt     */
#define DSM_RC_TCPIP_DLL_LOADFAILURE -56 /* Fehler von LoadLibrary           */
#define DSM_RC_TCPIP_LOADFAILURE   -57 /* Fehler von GetProcAddress          */
#define DSM_RC_TCPIP_USER_ABORT    -58 /* Abbruch durch Benutzer in
                                          TCP/IP-Schicht                     */

/*---------------------------------------------------------------------------*/
/* Rückkehrcodes (-71)-(-90) sind für CommTSM-Fehlercodes reserviert         */
/*---------------------------------------------------------------------------*/
#define DSM_RC_TSM_FAILURE         -71 /* TSM-Kommunikationsfehler           */
#define DSM_RC_TSM_ABORT           -72 /* Sitzung abnormal abgebrochen       */

/*comm3270-Fehlercodes - nicht mehr verwendet*/
#define DSM_RC_COMM_TIMEOUT       2021   /* nicht mehr verwendet              */
#define DSM_RC_EMULATOR_INACTIVE  2021   /* nicht mehr verwendet              */
#define DSM_RC_BAD_HOST_ID        2021   /* nicht mehr verwendet              */
#define DSM_RC_HOST_SESS_BUSY     2021   /* nicht mehr verwendet              */
#define DSM_RC_3270_CONNECT_FAILURE 2021 /* nicht mehr verwendet              */
#define DSM_RC_NO_ACS3ELKE_DLL    2021   /* nicht mehr verwendet              */
#define DSM_RC_EMULATOR_ERROR     2021   /* nicht mehr verwendet              */
#define DSM_RC_EMULATOR_BACKLEVEL 2021   /* nicht mehr verwendet              */
#define DSM_RC_CKSUM_FAILURE      2021   /* nicht mehr verwendet              */


/* Die folgenden Rückkehrcode gelten für EHLLAPI für Windows                 */
#define DSM_RC_3270COMMError_DLL        2021   /* nicht mehr verwendet       */
#define DSM_RC_3270COMMError_GetProc    2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_DLL         2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_GetProc     2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_HostConnect 2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_AllocBuff   2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_SendKey     2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_PacketChk   2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_ChkSum      2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_HostTimeOut 2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_Send        2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_Recv        2021   /* nicht mehr verwendet       */
#define DSM_RC_EHLLAPIError_General     2021   /* nicht mehr verwendet       */
#define DSM_RC_PC3270_MISSING_DLL       2021   /* nicht mehr verwendet       */
#define DSM_RC_3270COMM_MISSING_DLL     2021   /* nicht mehr verwendet       */


/* NETBIOS-Fehlercodes */
#define DSM_RC_NETB_ERROR         -151 /* Knoten konnte LAN nicht hinzugefügt
                                          werden                             */
#define DSM_RC_NETB_NO_DLL        -152 /* ACSNETB.DLL konnte nicht geladen
                                          werden                             */
#define DSM_RC_NETB_LAN_ERR       -155 /* LAN-Fehler erkannt                 */
#define DSM_RC_NETB_NAME_ERR      -158 /* NetBIOS-Fehler im Hinzufügenamen   */
#define DSM_RC_NETB_TIMEOUT       -159 /* Zeitlimitüberschreitung in
                                          NetBIOS-Sendeoperation             */
#define DSM_RC_NETB_NOTINST       -160 /* NetBIOS nicht installiert - DOS    */
```

```
#define DSM_RC_NETB_REBOOT        -161 /* NetBIOS-Konfigurationsfehler -
                                          Warmstart für DOS durchführen      */

/* Fehlercodes für benannte Pipe */
#define DSM_RC_NP_ERROR                        -190

/* CPIC-Fehlercodes */
#define DSM_RC_CPIC_ALLOCATE_FAILURE           2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_TYPE_MISMATCH              2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_PIP_NOT_SPECIFY_ERR        2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_SECURITY_NOT_VALID         2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_SYNC_LVL_NO_SUPPORT        2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_TPN_NOT_RECOGNIZED         2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_TP_ERROR                   2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_PARAMETER_ERROR            2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_PROD_SPECIFIC_ERR          2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_PROGRAM_ERROR              2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_RESOURCE_ERROR             2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_DEALLOCATE_ERROR           2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_SVC_ERROR                  2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_PROGRAM_STATE_CHECK        2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_PROGRAM_PARAM_CHECK        2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_UNSUCCESSFUL               2021 /* nicht mehr verwendet*/
#define DSM_RC_UNKNOWN_CPIC_PROBLEM            2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_MISSING_LU                 2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_MISSING_TP                 2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_SNA6000_LOAD_FAIL          2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_STARTUP_FAILURE            2021 /* nicht mehr verwendet*/

/*-----------------------------------------------------------------------------*/
/* Rückkehrcodes -300 bis -307 sind für die IPX/SPX-Kommunikation reserviert */
/*-----------------------------------------------------------------------------*/
#define DSM_RC_TLI_ERROR                       2021 /* nicht mehr verwendet*/
#define DSM_RC_IPXSPX_FAILURE                  2021 /* nicht mehr verwendet*/
#define DSM_RC_TLI_DLL_MISSING                 2021 /* nicht mehr verwendet*/
#define DSM_RC_DLL_LOADFAILURE                 2021 /* nicht mehr verwendet*/
#define DSM_RC_DLL_FUNCTION_LOADFAILURE        2021 /* nicht mehr verwendet*/
#define DSM_RC_IPXCONN_REFUSED                 2021 /* nicht mehr verwendet*/
#define DSM_RC_IPXCONN_TIMEDOUT                2021 /* nicht mehr verwendet*/
#define DSM_RC_IPXADDR_UNREACHABLE             2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_MISSING_DLL                2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_DLL_LOADFAILURE            2021 /* nicht mehr verwendet*/
#define DSM_RC_CPIC_FUNC_LOADFAILURE           2021 /* nicht mehr verwendet*/

/*=== Fehlercodes für Shared-Memory-Protokoll ===*/
#define DSM_RC_SHM_TCPIP_FAILURE               -450
#define DSM_RC_SHM_FAILURE                     -451
#define DSM_RC_SHM_NOTAUTH                     -452

#define DSM_RC_NULL_OBJNAME        2000 /* Objektnamenverweis ist NULL      */
#define DSM_RC_NULL_DATABLKPTR     2001 /* dataBlkPtr ist NULL              */
#define DSM_RC_NULL_MSG            2002 /* Nachrichtenparameter in dsmRCMsg
                                           ist NULL                         */

#define DSM_RC_NULL_OBJATTRPTR     2004 /* Objektattributverweis ist NULL   */

#define DSM_RC_NO_SESS_BLK         2006 /* keine Serversitzungsinformationen*/
#define DSM_RC_NO_POLICY_BLK       2007 /* keine Maßnahmenheaderinformat.   */
#define DSM_RC_ZERO_BUFLEN         2008 /* bufferLen für dataBlkPtr ist null*/
#define DSM_RC_NULL_BUFPTR         2009 /* bufferPtr für dataBlkPtr ist NULL*/

#define DSM_RC_INVALID_OBJTYPE     2010 /* ungültiger Objekttyp             */
#define DSM_RC_INVALID_VOTE        2011 /* ungültiges Votum                 */
#define DSM_RC_INVALID_ACTION      2012 /* ungültige Aktion                 */
#define DSM_RC_INVALID_DS_HANDLE   2014 /* ungültige ADSM-Kennung           */
#define DSM_RC_INVALID_REPOS       2015 /* ungültiger Wert für Repository   */
#define DSM_RC_INVALID_FSNAME      2016 /* Dateibereichsname muss mit
                                           Verzeichnisbegrenzer beginnen    */
#define DSM_RC_INVALID_OBJNAME     2017 /* ungültiger vollständiger Pfadname*/
#define DSM_RC_INVALID_LLNAME      2018 /* untergeordneter Name muss mit
                                           Verzeichnisbegrenzer beginnen    */
#define DSM_RC_INVALID_OBJOWNER    2019 /* ungültiger Objekteignername      */
#define DSM_RC_INVALID_ACTYPE      2020 /* ungültiger Aktionstyp            */
#define DSM_RC_INVALID_RETCODE     2021 /* dsmRC in dsmRCMsg ist ungültig   */
#define DSM_RC_INVALID_SENDTYPE    2022 /* ungültiger Sendetyp              */
#define DSM_RC_INVALID_PARAMETER   2023 /* ungültiger Parameter             */
#define DSM_RC_INVALID_OBJSTATE    2024 /* aktiv, inaktiv oder beliebige
                                           Übereinstimmung?                 */
#define DSM_RC_INVALID_MCNAME      2025 /* Verwaltungsklassenname nicht gef.*/
#define DSM_RC_INVALID_DRIVE_CHAR  2026 /* Laufwerkbuchstabe ist kein
                                           alphabetisches Zeichen           */
#define DSM_RC_NULL_FSNAME         2027 /* Dateibereichsname ist NULL       */
```

```
#define DSM_RC_INVALID_HLNAME      2028 /* untergeordneter Name muss mit
                                           Verzeichnisbegrenzer beginnen    */

#define DSM_RC_NUMOBJ_EXCEED       2029 /* Anzahl Objekte für BeginGetData
                                           überschritten                    */

#define DSM_RC_NEWPW_REQD          2030 /* neues Kennwort ist erforderlich  */
#define DSM_RC_OLDPW_REQD          2031 /* altes Kennwort ist erforderlich  */
#define DSM_RC_NO_OWNER_REQD       2032 /* Eigner nicht zulässig. Standard-
                                           wert zulassen                    */
#define DSM_RC_NO_NODE_REQD        2033 /* Knoten ohne password=generate
                                           nicht zulässig                   */
#define DSM_RC_KEY_MISSING         2034 /* Schlüsseldatei nicht gefunden    */
#define DSM_RC_KEY_BAD             2035 /* Inhalt d. Schlüsseldatei ungültig*/

#define DSM_RC_BAD_CALL_SEQUENCE   2041 /* Folge von DSM-Aufrufen nicht zulässig */
#define DSM_RC_INVALID_TSMBUFFER   2042 /* ungültiger Wert für tsmbuffhandle oder dataPtr */
#define DSM_RC_TOO_MANY_BYTES      2043 /* zu viele Byte in Puffer kopiert  */
#define DSM_RC_MUST_RELEASE_BUFFER 2044 /* Anwendung, die Puffer freigeben muss, kann nicht
                                           verlassen werden */
#define DSM_RC_BUFF_ARRAY_ERROR    2045 /* interner Pufferarrayfehler */
#define DSM_RC_INVALID_DATABLK     2046 /* bei Verwendung von TsmBuffers muss DataBlk null sein */
#define DSM_RC_ENCR_NOT_ALLOWED    2047 /* bei Verwendung von TsmBuffers keine Verschlüsselung
                                           zulässig */
#define DSM_RC_OBJ_COMPRESSED      2048 /* Keine Zurückschreibung möglich bei Verwendung von
                                           TsmBuffers für komprimiertes Objekt */
#define DSM_RC_OBJ_ENCRYPTED       2049 /* Keine Zurückschreibung möglich bei Verwendung von
                                           TsmBuffers für verschlüsseltes Objekt */
#define DSM_RC_WILDCHAR_NOTALLOWED 2050 /* Platzhalter für über-/untergeordneten Namen
                                           nicht zulässig */
#define DSM_RC_POR_NOT_ALLOWED     2051 /* Keine Zurückschreibung von Teilobjekten
                                           mit TsmBuffers möglich */
#define DSM_RC_NO_ENCRYPTION_KEY   2052 /* Verschlüsselungsschlüssel nicht gefunden */
#define DSM_RC_ENCR_CONFLICT       2053 /* sich gegenseitig ausschließende Optionen */

#define DSM_RC_FSNAME_NOTFOUND     2060 /* Dateibereichsname nicht gefunden      */
#define DSM_RC_FS_NOT_REGISTERED   2061 /* Dateibereichsname nicht registriert   */
#define DSM_RC_FS_ALREADY_REGED    2062 /* Dateibereich bereits registriert      */
#define DSM_RC_OBJID_NOTFOUND      2063 /* Keine Objekt-ID zum Zurückschreiben   */
#define DSM_RC_WRONG_VERSION       2064 /* Falsche Codeversion                   */
#define DSM_RC_WRONG_VERSION_PARM  2065 /* Falsche Parameterstrukturversion      */

#define DSM_RC_NEEDTO_ENDTXN       2070 /* Aufruf von dsmEndTxn erforderlich     */

#define DSM_RC_OBJ_EXCLUDED        2080 /* Objekt wird von Verwaltungsklasse
                                           ausgeschlossen                   */
#define DSM_RC_OBJ_NOBCG           2081 /* Objekt hat keine Sich.-Kopiengruppe   */
#define DSM_RC_OBJ_NOACG           2082 /* Objekt hat keine Arch.-Kopiengruppe   */

#define DSM_RC_APISYSTEM_ERROR     2090 /* interner API-Fehler                   */

#define DSM_RC_DESC_TOOLONG             2100 /* Beschreibung ist zu lang         */
#define DSM_RC_OBJINFO_TOOLONG          2101 /* Objektattribut objInfo zu lang   */
#define DSM_RC_HL_TOOLONG               2102 /* übergeordnetes Qualifikations-
                                                merkmal zu lang                 */
#define DSM_RC_PASSWD_TOOLONG           2103 /* Kennwort ist zu lang             */
#define DSM_RC_FILESPACE_TOOLONG        2104 /* Dateibereichsname ist zu lang    */
#define DSM_RC_LL_TOOLONG               2105 /* untergeordnetes Qualifikations-
                                                merkmal zu lang                 */
#define DSM_RC_FSINFO_TOOLONG           2106 /* Dateibereichslänge ist zu groß   */
#define DSM_RC_SENDDATA_WITH_ZERO_SIZE  2107 /* Daten mit Größenschätzung 'null'
                                                senden                          */

/*=== neue Rückkehrcodes für dsmaccess ===*/
#define DSM_RC_INVALID_ACCESS_TYPE 2110 /* ungültiger Zugriffstyp               */
#define DSM_RC_QUERY_COMM_FAILURE  2111 /* Kommunikationsfehler während Abfrage  */
#define DSM_RC_NO_FILES_BACKUP     2112 /* Keine gesicherten Dateien für diesen
                                           Dateibereich                     */
#define DSM_RC_NO_FILES_ARCHIVE    2113 /* Keine archivierten Dateien für diesen
                                           Dateibereich                     */
#define DSM_RC_INVALID_SETACCESS   2114 /* ungültiges SetAccess-Format          */

/*=== neue Rückkehrcodes für dsmaccess ===*/
#define DSM_RC_STRING_TOO_LONG     2120 /* Zeichenfolgeparameter zu lang        */

#define DSM_RC_MORE_DATA           2200 /* Weitere Daten zum Zurückschreiben vorh.*/

#define DSM_RC_BUFF_TOO_SMALL      2210 /* DataBlk-Puffer für Abfrage zu klein    */

#define DSM_RC_NO_API_CONFIGFILE   2228 /* angegebene API-Konfigurationsdatei
                                           nicht gefunden                    */
#define DSM_RC_NO_INCLEXCL_FILE    2229 /* angegebene Ein-/Ausschlussdatei nicht
```

```
                                        gefunden                          */
#define DSM_RC_NO_SYS_OR_INCLEXCL  2230 /* entweder wurde dsm.sys oder die in
                                        dsm.sys angegebene Ein-/Ausschlussdatei
                                        nicht gefunden                    */
#define DSM_RC_REJECT_NO_POR_SUPPORT 2231 /* keine POR-Unterstützung für Server   */

#define DSM_RC_NEED_ROOT           2300 /* Aufrufender der API muss Root sein     */
#define DSM_RC_NEEDTO_CALL_BINDMC  2301 /* dsmBindMC muss zuerst aufgerufen werden*/
#define DSM_RC_CHECK_REASON_CODE   2302 /* Ursachencode aus dsmEndTxn prüfen      */
#define DSM_RC_NEEDTO_ENDTXN_DEDUP_SIZE_EXCEEDED 2303 /* maximale Anzahl Byte bei
                                                         Dedupl. überschritten    */

/*=== Rückkehrcodes 2400-2410 von Lizenzdatei verwendet; siehe agentrc.h ===*/

/*=== Rückkehrcodes 2410-2430 von Orcale-Agent verwendet; siehe agentrc.h ===*/

#define DSM_RC_ENC_WRONG_KEY       4580 /* angegebener Schlüssel ist falsch */
#define DSM_RC_ENC_NOT_AUTHORIZED  4582 /* Benutzer darf nicht entschlüsseln*/
#define DSM_RC_ENC_TYPE_UNKNOWN    4584 /* unbekannter Verschlüsselungstyp  */

/*============================================================================
   Rückkehrcodes 4600-4624 sind für Clustering reserviert
============================================================================*/
#define DSM_RC_CLUSTER_INFO_LIBRARY_NOT_LOADED        4600
#define DSM_RC_CLUSTER_LIBRARY_INVALID                4601
#define DSM_RC_CLUSTER_LIBRARY_NOT_LOADED             4602
#define DSM_RC_CLUSTER_NOT_MEMBER_OF_CLUSTER          4603
#define DSM_RC_CLUSTER_NOT_ENABLED                    4604
#define DSM_RC_CLUSTER_NOT_SUPPORTED                  4605
#define DSM_RC_CLUSTER_UNKNOWN_ERROR                  4606

/*============================================================================
   Rückkehrcodes 5200-5600 sind für neue Abbruchcodes des Servers reserviert (dsmcomm.h)
============================================================================*/
#define DSM_RS_ABORT_CERTIFICATE_NOT_FOUND   5200

/*============================================================================
   Rückkehrcodes 5701-5749 sind für Proxy reserviert
============================================================================*/
#define DSM_RC_PROXY_REJECT_NO_RESOURCES              5702
#define DSM_RC_PROXY_REJECT_DUPLICATE_ID              5705
#define DSM_RC_PROXY_REJECT_ID_IN_USE                 5710
#define DSM_RC_PROXY_REJECT_INTERNAL_ERROR            5717
#define DSM_RC_PROXY_REJECT_NOT_AUTHORIZED            5722
#define DSM_RC_PROXY_INVALID_FROMNODE                 5746
#define DSM_RC_PROXY_INVALID_SERVERFREE               5747
#define DSM_RC_PROXY_INVALID_CLUSTER                  5748
#define DSM_RC_PROXY_INVALID_FUNCTION                 5749

/*============================================================================
   Rückkehrcodes 5801-5849 sind für Verschlüsselung/Sicherheit reserviert
============================================================================*/

#define DSM_RC_CRYPTO_ICC_ERROR                       5801
#define DSM_RC_CRYPTO_ICC_CANNOT_LOAD                 5802
#define DSM_RC_SSL_NOT_SUPPORTED                      5803
#define DSM_RC_SSL_INIT_FAILED                        5804
#define DSM_RC_SSL_KEYFILE_OPEN_FAILED                5805
#define DSM_RC_SSL_KEYFILE_BAD_PASSWORD               5806
#define DSM_RC_SSL_BAD_CERTIFICATE                    5807

/*============================================================================
   Rückkehrcodes 6300-6399 sind für clientseitige Deduplizierung reserviert
============================================================================*/
#define DSM_RC_DIGEST_VALIDATION_ERROR                6300  /* Fehler bei Überprüfung der
                                                               End-to-End-Digest-Verarbeitung   */
#define DSM_RC_DATA_FINGERPRINT_ERROR                 6301 /* Fehler bei Rabin-Fingerabdruck    */
#define DSM_RC_DATA_DEDUP_ERROR                       6302 /* Fehler beim Konvertieren von
                                                              Daten in Chunks                   */


#endif /* _H_DSMRC */
```

Zugehörige Verweise:
API-Rückkehrcodes

Quellendateien für API-Typdefinitionen

Dieser Anhang enthält Strukturdefinitionen, Typdefinitionen und Konstanten für die API. Die ersten Headerdateien, dsmapitd.h und tsmapitd.h, enthalten die Definitionen, die für alle Betriebssysteme einheitlich sind.

Die zweite Headerdatei, dsmapips.h, stellt ein Beispiel mit Definitionen bereit, die speziell für ein bestimmtes Betriebssystem gelten, im vorliegenden Beispiel für die Windows-Plattform.

Die dritte Headerdatei, release.h, enthält die Versions- und Releaseinformationen.

Die hier bereitgestellten Informationen enthalten eine Zeitpunktkopie der Dateien, die mit der API verteilt werden. Die neueste Version können Sie den Dateien im API-Verteilerpaket entnehmen.

```
/********************************************************************
* Tivoli Storage Manager                                            *
* API-Clientkomponente                                              *
*                                                                   *
* (C) Copyright IBM Corporation 1993, 2010                          *
********************************************************************/

/***********************************************************************
* Headerdateiname: dsmapitd.h
*
* Umgebung:        ***********************************************
*                  ** Dies ist eine plattformunabhängige        **
*                  ** Quellendatei                              **
*
*                  ***********************************************
*
* Anm. zum Entwurf: Diese Datei enthält Basisdatentypen und Konstanten, die in
*                   allen Clientquellendateien verwendet werden können. Die Konstanten
*                   in dieser Datei müssen für die spezielle Maschine bzw. für das
*                   spezielle Betriebssystem, auf dem die Clientsoftware ausgeführt
*                   werden soll, ordnungsgemäß gesetzt werden.
*
*                   dsmapips.h enthält plattformspezifische Definitionen
*
* Beschreib. Name:  Definitionen für Konstanten der Tivoli Storage
*                   Manager-API
*-----------------------------------------------------------------------*/

#ifndef _H_DSMAPITD
#define _H_DSMAPITD


#include "dsmapips.h"      /* Plattformspezif. Definitionen*/
#include "release.h"

/*=== Strukturausrichtung zum Packen der Strukturen definieren ===*/
#if (_OPSYS_TYPE == DS_WINNT) && !defined(_WIN64)
#pragma pack(1)
#endif

#ifdef _MAC
/*========================================================================
  Auswahlmöglichkeiten:
http://developer.apple.com/documentation/DeveloperTools/Conceptual/PowerPCRuntime/Data/chapter_2_section_3.html

#pragma option align=<mode>
Dabei ist <mode> power, mac68k, natural oder packed.
========================================================================*/
#pragma options align=packed
#endif

typedef char osChar_t;

/*<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>*/
/*                    D E F I N I T I O N E N                        */
/*<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>*/
/*-----------------------------------------------------------------------+
|  API-Version, -Release und -Stufe für Verwendung in dsmApiVersion      |
|  in dsmInit()                                                          |
+-----------------------------------------------------------------------*/
#define DSM_API_VERSION     COMMON_VERSION
#define DSM_API_RELEASE     COMMON_RELEASE
#define DSM_API_LEVEL       COMMON_LEVEL
#define DSM_API_SUBLEVEL    COMMON_SUBLEVEL

/*-----------------------------------------------------------------------+
| Maximale Feldlängen                                                    |
+-----------------------------------------------------------------------*/
#define DSM_MAX_CG_DEST_LENGTH        30       /* Ziel für Kopiengruppe  */
#define DSM_MAX_CG_NAME_LENGTH        30       /* Kopiengruppenname      */
#define DSM_MAX_DESCR_LENGTH          255      /* Archivierungsbeschr.   */
#define DSM_MAX_DOMAIN_LENGTH         30       /* Richtliniendomänenname */
#define DSM_MAX_FSINFO_LENGTH         500      /* Dateibereichsinformat. */
#define DSM_MAX_USER_FSINFO_LENGTH    480      /* Dateibereichsinformat. zu
```

```
                                              max. Anz. Benutzer     */
#define DSM_MAX_FSNAME_LENGTH         1024      /* Dateibereichsname      */
#define DSM_MAX_FSTYPE_LENGTH         32        /* Dateibereichstyp       */
#define DSM_MAX_HL_LENGTH             1024      /* übergeord. Objektname  */
#define DSM_MAX_ID_LENGTH             64        /* Sitzungsknotenname     */
#define DSM_MAX_LL_LENGTH             256       /* untergeord. Objektname */
#define DSM_MAX_MC_NAME_LENGTH        30        /* Verwaltungsklassenname */
#define DSM_MAX_OBJINFO_LENGTH        255       /* Objektinformationen    */
#define DSM_MAX_EXT_OBJINFO_LENGTH    1500      /* Erweiterte Objektinfo. */
#define DSM_MAX_OWNER_LENGTH          64        /* Objekteignername       */
#define DSM_MAX_PLATFORM_LENGTH       16        /* Anwendungstyp          */
#define DSM_MAX_PS_NAME_LENGTH        30        /* Richtliniengruppename  */
#define DSM_MAX_SERVERTYPE_LENGTH     32        /* Serverplattformtyp     */
#define DSM_MAX_VERIFIER_LENGTH       64        /* Kennwort               */
#define DSM_PATH_MAX                  1024      /* API-Konfig.-Datei: Pfad*/
#define DSM_NAME_MAX                  255       /* API-Konfig.-Datei: Name*/
#define DSM_MAX_NODE_LENGTH           64        /* Knoten-/Maschinenname  */
#define DSM_MAX_RC_MSG_LENGTH         1024      /* Nachr.-PRM f. dsmRCMsg */
#define DSM_MAX_SERVER_ADDRESS        1024      /* Serveradresse          */

#define DSM_MAX_MC_DESCR_LENGTH       DSM_MAX_DESCR_LENGTH /* Verw.-Klasse*/
#define DSM_MAX_SERVERNAME_LENGTH     DSM_MAX_ID_LENGTH /* Servername     */
#define DSM_MAX_GET_OBJ               4080    /* max. Obj. in BeginGetData*/
#define DSM_MAX_PARTIAL_GET_OBJ       1300 /*max. Teilobj. in BeginGetData*/
#define DSM_MAX_COMPRESSTYPE_LENGTH   32       /* max. Komprimierungsalgorithmusname */

/*-----------------------------------------------------------------------+
| Mindestfeldlängen                                                      |
+-----------------------------------------------------------------------*/
#define DSM_MIN_COMPRESS_SIZE  2048 /* Mindestanzahl Byte, die ein Objekt */
                                    /* benötigt, bevor Komprimierung      */
                                    /* zulässig ist                       */

/*-----------------------------------------------------------------------+
|  Werte für mtFlag im Aufruf dsmSetup                                   |
+-----------------------------------------------------------------------*/
#define DSM_MULTITHREAD      bTrue
#define DSM_SINGLETHREAD     bFalse

/*-----------------------------------------------------------------------+
|  Werte für Objekttyp in Struktur dsmObjName                            |
|  Anm.: Diese Werte müssen mit dsmcomm.h synchronisiert werden          |
+-----------------------------------------------------------------------*/
#define DSM_OBJ_FILE                  0x01 /*Obj. hat Attr.-Inf. & -Daten */
#define DSM_OBJ_DIRECTORY             0x02 /*Objekt hat nur Attributinf.  */
#define DSM_OBJ_RESERVED1             0x04 /* für zukünftige Verwendung   */
#define DSM_OBJ_RESERVED2             0x05 /* für zukünftige Verwendung   */
#define DSM_OBJ_RESERVED3             0x06 /* für zukünftige Verwendung   */
#define DSM_OBJ_WILDCARD              0xFE /* beliebiger Objekttyp        */
#define DSM_OBJ_ANY_TYPE              0xFF /* für zukünftige Verwendung   */

/*-----------------------------------------------------------------------+
| Typdefinition für compressedState in QryResp                           |
+-----------------------------------------------------------------------*/
#define DSM_OBJ_COMPRESSED_UNKNOWN    0
#define DSM_OBJ_COMPRESSED_YES        1
#define DSM_OBJ_COMPRESSED_NO         2

/*-----------------------------------------------------------------------+
| Definitionen für Feld "Gruppentyp" in tsmGrouphandlerIn_t              |
+-----------------------------------------------------------------------*/

#define  DSM_GROUPTYPE_NONE         0x00   /* Kein Gruppenmitglied    */
#define  DSM_GROUPTYPE_RESERVED1    0x01   /* für zukünftige Verwend. */
#define  DSM_GROUPTYPE_PEER         0x02   /* Peergruppe              */
#define  DSM_GROUPTYPE_RESERVED2    0x03   /* für zukünftige Verwend. */

/*-----------------------------------------------------------------------+
| Definitionen für Feld "Mitgliedstyp" in tsmGrouphandlerIn_t            |
+-----------------------------------------------------------------------*/

#define  DSM_MEMBERTYPE_LEADER      0x01   /* Gruppenleiter           */
#define  DSM_MEMBERTYPE_MEMBER      0x02   /* Gruppenmitglied         */

/*-----------------------------------------------------------------------+
| Definitionen für Feld "Operationstyp" in tsmGrouphandlerIn_t           |
+-----------------------------------------------------------------------*/
#define DSM_GROUP_ACTION_BEGIN         0x01
#define DSM_GROUP_ACTION_OPEN          0x02 /* neue Gruppe erstellen  */
#define DSM_GROUP_ACTION_CLOSE         0x03 /* offene Gruppe fest-    */
                                            /* schreiben und speichern*/
#define DSM_GROUP_ACTION_ADD           0x04 /* an Gruppe anhängen     */
```

```
#define DSM_GROUP_ACTION_ASSIGNTO      0x05 /* anderer Gruppe zuordnen*/
#define DSM_GROUP_ACTION_REMOVE        0x06 /* Mitgl. aus Gruppe entf.*/

/*-----------------------------------------------------------------------+
| Werte für copySer in Strukturen DetailCG für Antwort der               |
| Abfrageverwerwaltungsklasse                                            |
+-----------------------------------------------------------------------*/
#define Copy_Serial_Static          1   /*Kopiennummer.:Statisch          */
#define Copy_Serial_Shared_Static   2   /*Kopiennummer.:Gemeinsam statisch*/
#define Copy_Serial_Shared_Dynamic  3   /*Kopiennummer.:Gem. dynamisch    */
#define Copy_Serial_Dynamic         4   /*Kopiennummer.:Dynamisch         */

/*-----------------------------------------------------------------------+
| Werte für copyMode in Strukturen DetailCG für Antwort der              |
| Abfrageverwerwaltungsklasse                                            |
+-----------------------------------------------------------------------*/
#define Copy_Mode_Modified          1   /* Kopiermodus: Geändert          */
#define Copy_Mode_Absolute          2   /* Kopiermodus: Absolut           */

/*-----------------------------------------------------------------------+
|  Werte für objState in Struktur qryBackupData                          |
+-----------------------------------------------------------------------*/
#define DSM_ACTIVE            0x01      /* nur aktive Objekte abfragen    */
#define DSM_INACTIVE          0x02      /* nur inaktive Objekte abfragen  */
#define DSM_ANY_MATCH         0xFF      /* alle Sicherungsobjekte abfragen*/

/*-----------------------------------------------------------------------+
| Grenzwerte für Feld dsmDate.year in Struktur qryArchiveData            |
+-----------------------------------------------------------------------*/
#define DATE_MINUS_INFINITE         0x0000   /* niedrigster Grenzwert     */
#define DATE_PLUS_INFINITE          0xFFFF   /* höchster oberer Grenzwert */

/*-----------------------------------------------------------------------+
| Bitmasken für Parameter für Aktualisierungsaktion in dsmUpdateFS()     |
+-----------------------------------------------------------------------*/
#define DSM_FSUPD_FSTYPE              ((unsigned) 0x00000002)
#define DSM_FSUPD_FSINFO              ((unsigned) 0x00000004)
#define DSM_FSUPD_BACKSTARTDATE       ((unsigned) 0x00000008)
#define DSM_FSUPD_BACKCOMPLETEDATE    ((unsigned) 0x00000010)
#define DSM_FSUPD_OCCUPANCY           ((unsigned) 0x00000020)
#define DSM_FSUPD_CAPACITY            ((unsigned) 0x00000040)
#define DSM_FSUPD_RESERVED1           ((unsigned) 0x00000100)

/*-----------------------------------------------------------------------+
| Bitmasken für Parameter für Sicherungsaktual.-Aktion in dsmUpdateObj()  |
+-----------------------------------------------------------------------*/
#define DSM_BACKUPD_OWNER              ((unsigned) 0x00000001)
#define DSM_BACKUPD_OBJINFO            ((unsigned) 0x00000002)
#define DSM_BACKUPD_MC                 ((unsigned) 0x00000004)

#define DSM_ARCHUPD_OWNER              ((unsigned) 0x00000001)
#define DSM_ARCHUPD_OBJINFO            ((unsigned) 0x00000002)
#define DSM_ARCHUPD_DESCR              ((unsigned) 0x00000004)

/*-----------------------------------------------------------------------+
|  Werte für Repositoryparameter in dsmDeleteFS()                        |
+-----------------------------------------------------------------------*/
#define DSM_ARCHIVE_REP       0x0A      /* Archivrepository               */
#define DSM_BACKUP_REP        0x0B      /* Sicherungsrepository           */
#define DSM_REPOS_ALL         0x01      /* alle Respositorytypen          */

/*-----------------------------------------------------------------------+
|  Werte für Votumparameter in dsmEndTxn()                               |
+-----------------------------------------------------------------------*/
#define DSM_VOTE_COMMIT  1             /* akt. Transaktion festschreiben  */
#define DSM_VOTE_ABORT   2             /* akt. Transakt. rückgängig machen*/

/*-----------------------------------------------------------------------+
|  Werte für verschiedene in Struktur ApiSessInfo zurückgegebene Flags   |
+-----------------------------------------------------------------------*/
/* Codes für Feld für Clientkomprimierung */
#define COMPRESS_YES    1    /* Client muss Daten komprimieren            */
#define COMPRESS_NO     2    /* Client darf Daten NICHT komprimieren      */
#define COMPRESS_CD     3    /* vom Client bestimmt                       */

/* Berechtigungscodes zum Löschen der Archivierung */
#define ARCHDEL_YES     1    /* Löschen der Archivierung zulässig         */
#define ARCHDEL_NO      2    /* Löschen der Archivierung NICHT zulässig   */

/* Berechtigungscode zum Löschen der Sicherung */
#define BACKDEL_YES     1    /* Löschen der Sicherung zulässig            */
#define BACKDEL_NO      2    /* Löschen der Sicherung NICHT zulässig      */
```

```
/*--------------------------------------------------------------------------+
  Werte für verschiedene in Struktur optStruct zurückgegebene Flags        |
--------------------------------------------------------------------------*/
#define DSM_PASSWD_GENERATE  1
#define DSM_PASSWD_PROMPT    0

#define DSM_COMM_TCP        1    /* TCP/IP         */
#define DSM_COMM_NAMEDPIPE  2    /* Benannte Pipes */
#define DSM_COMM_SHM        3    /* Shared Memory  */

/* veraltete Übertragungsmethoden */
#define DSM_COMM_PVM_IUCV   12
#define DSM_COMM_3270       12
#define DSM_COMM_IUCV       12
#define DSM_COMM_PWSCS      12
#define DSM_COMM_SNA_LU6_2  12
#define DSM_COMM_IPXSPX     12    /* Für IPX/SPX-Unterstützung */
#define DSM_COMM_NETBIOS    12    /* NETBIOS */
#define DSM_COMM_400COMM    12
#define DSM_COMM_CLIO       12    /* CLIO/S */
/*--------------------------------------------------------------------------+
|  Werte für userNameAuthorities in dsmInitEx für zukünftige Verwendung    |
+--------------------------------------------------------------------------*/
#define DSM_USERAUTH_NONE     ((dsInt16_t)0x0000)
#define DSM_USERAUTH_ACCESS   ((dsInt16_t)0x0001)
#define DSM_USERAUTH_OWNER    ((dsInt16_t)0x0002)
#define DSM_USERAUTH_POLICY   ((dsInt16_t)0x0004)
#define DSM_USERAUTH_SYSTEM   ((dsInt16_t)0x0008)

/*--------------------------------------------------------------------------+
|  Werte für encryptionType in dsmEndSendObjEx, queryResp                  |
+--------------------------------------------------------------------------*/
#define DSM_ENCRYPT_NO              ((dsUint8_t)0x00)
#define DSM_ENCRYPT_USER            ((dsUint8_t)0x01)
#define DSM_ENCRYPT_CLIENTENCRKEY   ((dsUint8_t)0x02)
#define DSM_ENCRYPT_DES_56BIT       ((dsUint8_t)0x04)
#define DSM_ENCRYPT_AES_128BIT      ((dsUint8_t)0x08)
#define DSM_ENCRYPT_AES_256BIT      ((dsUint8_t)0x10)

/*--------------------------------------------------------------------------+
| Definitionen für Feld "Datenträgerklasse" (mediaClass)                   |
+--------------------------------------------------------------------------*/
/*
 *  Die folgenden Konstanten definieren eine Hierarchie von
 *  Datenträgerzugriffsklassen.
 *  Je niedriger die Zahl, desto schneller kann der Zugriff auf Daten
 *  von dem Datenträger bereitgestellt werden.
 */

/* Fixed: Gibt die Klasse der online verfügbaren fest installierten
          Datenträger (wie z. B. Festplatten) an. */
#define  MEDIA_FIXED         0x10

/* Library: Gibt die Klasse mountfähiger Datenträger an, auf die
            über eine mechanische Ladeeinheit zugegriffen werden
            kann. */
#define  MEDIA_LIBRARY       0x20

/* zukünftige Verwendung */
#define  MEDIA_NETWORK       0x30

/* zukünftige Verwendung */
#define  MEDIA_SHELF         0x40

/* zukünftige Verwendung */
#define  MEDIA_OFFSITE       0x50

/* zukünftige Verwendung */
#define  MEDIA_UNAVAILABLE   0xF0


/*--------------------------------------------------------------------------+
| Typdefinition für partielle Objektdaten für dsmBeginGetData()            |
+--------------------------------------------------------------------------*/
typedef struct
{
    dsUint16_t   stVersion;               /* Strukturversion                  */
    dsStruct64_t   partialObjOffset;   /* Abweichung in Objekt für Lesebeginn   */
    dsStruct64_t   partialObjLength;   /* Zu lesende Objektmenge                */
} PartialObjData ;                     /* partielle Objektdaten                 */
```

```
#define PartialObjDataVersion 1  /*                                          */

/*---------------------------------------------------------------------------+
|  Typdefinition für Datumsstruktur                                          |
+---------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t    year;                 /* Jahr, 16-Bit-Integer (z. B. 1990) */
   dsUint8_t     month;                /* Monat, 8-Bit-Integer (1 - 12)     */
   dsUint8_t     day;                  /* Tag, 8-Bit-Integer (1 - 31)       */
   dsUint8_t     hour;                 /* Stunde, 8-Bit-Integer (0 - 23)    */
   dsUint8_t     minute;               /* Minute, 8-Bit-Integer (0 - 59)    */
   dsUint8_t     second;               /* Sekunde, 8-Bit-Integer (0 - 59)   */
}dsmDate ;

/*---------------------------------------------------------------------------+
|  Typdefinition für Objekt-ID in dsmGetObj() und in Struktur dsmGetList     |
+---------------------------------------------------------------------------*/
typedef dsStruct64_t  ObjID ;

/*---------------------------------------------------------------------------+
| Typdefinition für dsmQueryBuff in dsmBeginQuery()                          |
+---------------------------------------------------------------------------*/
typedef void dsmQueryBuff ;

/*---------------------------------------------------------------------------+
| Typdefinition für Parameter dsmGetType in dsmBeginGetData()                |
+---------------------------------------------------------------------------*/
typedef enum
{
        gtBackup = 0x00,                    /* Sicherungsverarbeitungstyp*/
        gtArchive                           /* Archivier.verarbeitungstyp*/
} dsmGetType ;

/*---------------------------------------------------------------------------+
|  Typdefinition für Parameter dsmQueryType in dsmBeginQuery()               |
+---------------------------------------------------------------------------*/
typedef enum
{
   qtArchive = 0x00,                 /* Archivabfragetyp                   */
   qtBackup,                         /* Sicherungsabfragetyp               */
   qtBackupActive,                   /* Schnellabfr. f. aktive Sich.dateien*/
   qtFilespace,                      /* Dateibereichsabfragetyp            */
   qtMC,                             /* Verwaltungsklassenabfragetyp       */
   qtReserved1,                      /* zukünftige Verwendung              */
   qtReserved2,                      /* zukünftige Verwendung              */
   qtReserved3,                      /* zukünftige Verwendung              */
   qtReserved4,                      /* zukünftige Verwendung              */
   qtBackupGroups,                   /* Gruppenleiter in speziell. Dateisy.*/
   qtOpenGroups,                     /* Offene Gruppen i.speziell.Dateisys.*/
   qtReserved5,                      /* zukünftige Verwendung              */
   qtProxyNodeAuth,                  /* Knoten, an die Knoten weiterl. kann*/
   qtProxyNodePeer,                  /* Peerknoten mit demselben Ziel      */
   qtReserved6,                      /* zukünftige Verwendung              */
   qtReserved7,                      /* zukünftige Verwendung              */
   qtReserved8                       /* zukünftige Verwendung              */
}dsmQueryType ;

/*---------------------------------------------------------------------------+
|  Typdefinition für Parameter sendType in dsmBindMC() und dsmSendObj()      |
+---------------------------------------------------------------------------*/
typedef enum
{
   stBackup = 0x00,                    /* Sicherungsverarbeitungstyp    */
   stArchive,                          /* Archivierungsverarbeitungstyp */
   stBackupMountWait,           /* Sicherungsverarbeitung; 'Auf Ladevorgang warten' ist aktiviert*/
   stArchiveMountWait           /* Archivierungsverarbeitung; 'Auf Ladevorgang warten' ist aktiviert*/
}dsmSendType ;

/*---------------------------------------------------------------------------+
|  Typdefinition für Parameter delType in dsmDeleteObj()                     |
+---------------------------------------------------------------------------*/
typedef enum
{
   dtArchive = 0x00,                  /* Typ 'Archivierung löschen' */
   dtBackup,                          /* Typ 'Sicherung löschen (inaktivieren)' */
   dtBackupID                         /* Typ 'Sicherung löschen (entfernen)' */
}dsmDelType ;

/*---------------------------------------------------------------------------+
|  Typdefinition für Parameter sendType in dsmSetAccess()                    |
```

```
+------------------------------------------------------------------------*/
typedef enum
{
   atBackup = 0x00,                       /* Sicherungsverarbeitungstyp   */
   atArchive                              /* Archivierungsverarbeitungstyp*/
}dsmAccessType;

/*------------------------------------------------------------------------+
|  Typdefinition für API-Version in dsmInit() und dsmQueryApiVersion()    |
+------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t version;       /* API-Version                    */
   dsUint16_t release;       /* API-Release                    */
   dsUint16_t level;         /* API-Stand                      */
}dsmApiVersion;

/*------------------------------------------------------------------------+
|  Typdefinition für API-Version in dsmInit() und dsmQueryApiVersion()    |
+------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t     stVersion;             /* Strukturversion             */
   dsUint16_t version;       /* API-Version                    */
   dsUint16_t release;       /* API-Release                    */
   dsUint16_t level;         /* API-Stand                      */
   dsUint16_t subLevel;      /* API-Unterstufe                 */
   dsmBool_t  unicode;       /* API-Unicode? */
}dsmApiVersionEx;


#define apiVersionExVer       2

/*------------------------------------------------------------------------+
|  Typdefinition für Anwendungsversion in dsmInit()                       |
+------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t   stVersion;               /* Strukturversion                  */
   dsUint16_t   applicationVersion;      /* Anwendungsversionsnummer         */
   dsUint16_t   applicationRelease;      /* Anwendungsreleasenummer          */
   dsUint16_t   applicationLevel;        /* Anwendungsebenennummer           */
   dsUint16_t   applicationSubLevel;     /* Anwendungsunterstufennummer      */
} dsmAppVersion;

#define appVersionVer      1

/*------------------------------------------------------------------------+
|  Typdefinition für in BindMC, Send, Delete, Query verwendeten Objektnamen|
+------------------------------------------------------------------------*/
typedef struct S_dsmObjName
{
   char       fs[DSM_MAX_FSNAME_LENGTH + 1] ;             /* Dateibereichsname */
   char       hl[DSM_MAX_HL_LENGTH + 1] ;                 /* Übergeordneter Name */
   char       ll[DSM_MAX_LL_LENGTH + 1] ;                 /* Untergeordneter Name */
   dsUint8_t  objType;              /* Definitionen für Objekttypwerte siehe oben */
}dsmObjName;


/*------------------------------------------------------------------------+
|  Typdefinition f. Informationen zu 'Sicherung löschen' in dsmDeleteObj() |
+------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmObjName       *objNameP ;                   /* Objektname             */
   dsUint32_t       copyGroup ;                   /* Kopiengruppe           */
}delBack ;

#define  delBackVersion    1

/*------------------------------------------------------------------------+
|  Typdefinition für Infos zu 'Archivierung löschen' in dsmDeleteObj()    |
+------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsStruct64_t     objId ;                       /* Objekt-ID              */
}delArch ;

#define  delArchVersion  1
```

```
/*-------------------------------------------------------------------------+
|  Typdefinition für Infos zu 'Sicherungs-ID löschen' in dsmDeleteObj()    |
+-------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsStruct64_t     objId ;                       /* Objekt-ID             */
}delBackID;

#define  delBackIDVersion  1

/*-------------------------------------------------------------------------+
|  Typdefinition für Löschinformationen in dsmDeleteObj()                  |
+-------------------------------------------------------------------------*/
typedef union
{
   delBack   backInfo ;
   delArch   archInfo ;
   delBackID backIDInfo ;
}dsmDelInfo ;

/*-------------------------------------------------------------------------+
|  Typdefinition für Parameter Object Attribute in dsmSendObj()            |
+-------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t   stVersion;                      /* Strukturversion   */
   char         owner[DSM_MAX_OWNER_LENGTH + 1]; /* Objekteigner      */
   dsStruct64_t sizeEstimate;                   /* Größenschätzung des Objekts in Byte */
   dsmBool_t    objCompressed;                  /* Ist Objekt bereits komprimiert? */
   dsUint16_t   objInfoLength;                  /* Länge der objektabhängigen Information */
   char         *objInfo;                       /* objektabhängige Information */
   char         *mcNameP;                       /* Verwaltungsklassenname für Überschreibung */
   dsmBool_t    disableDeduplication;     /* 'Keine Deduplizierung' für dieses Objekt erzwingen */
   dsmBool_t    useExtObjInfo;                  /* Erw. Objektinfo. bis zu 1536 verwenden */
}ObjAttr;

#define ObjAttrVersion  4



/*-------------------------------------------------------------------------+
| Typdefinition für zurückgegebenen mcBindKey in dsmBindMC()               |
+-------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char        mcName[DSM_MAX_MC_NAME_LENGTH + 1];
                                     /* Name der an das Objekt gebundenen Verwaltungsklasse. */
   dsmBool_t   backup_cg_exists;                    /* Wahr/Falsch */
   dsmBool_t   archive_cg_exists;                   /* Wahr/Falsch */
   char        backup_copy_dest[DSM_MAX_CG_DEST_LENGTH + 1];
                                          /* Zielname für Sicherungskopie */
   char        archive_copy_dest[DSM_MAX_CG_DEST_LENGTH + 1];
                                             /* Zielname für Archivierungskopie */
}mcBindKey;

#define mcBindKeyVersion  1


/*-------------------------------------------------------------------------+
| Typdefinition für Objektliste in dsmBeginGetData()                       |
+-------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t       numObjId ;          /* Anzahl Objekt-IDs in Liste   */
   ObjID           *objId ;             /* Liste der zurückzuschreibenden Objekt-IDs */
   PartialObjData  *partialObjData;     /* Liste partieller Objektdateninformationen */
}dsmGetList ;

#define dsmGetListVersion     2  /* Standard, bei Nichtverwendung partieller Objektdaten */
#define dsmGetListPORVersion  3  /* Version, bei Verwendung partieller Objektdaten */

/*-------------------------------------------------------------------------+
|  Typdefinition für DataBlk zum Abrufen oder Senden von Daten             |
+-------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t      stVersion;            /* Strukturversion     */
   dsUint32_t bufferLen;                 /* Länge des unten übergebenen Puffers */
   dsUint32_t numBytes;                  /* Anzahl der aktuell aus dem Puffer gelesenen */
```

```
                                        /* oder in den Puffer geschriebenen Byte */
   char       *bufferPtr;               /* Datenpuffer */
   dsUint32_t numBytesCompressed;       /* beim Senden tatsächlich komprimierte Byte */
   dsUint16_t reserved;                 /* für zukünftige Verwendung      */
}DataBlk;

#define DataBlkVersion  3


/*--------------------------------------------------------------------------+
|  Typdefinition für queryBuffer für Verwaltungsklasse in dsmBeginQuery()  |
+--------------------------------------------------------------------------*/
typedef struct S_qryMCData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char         *mcName;                        /* Verwaltungsklassenname */
                        /* einzelner Name für 1 Klasse oder leere Zeichenfolge, um alle abzurufen */
   dsmBool_t    mcDetail;                           /* Details erwünscht oder nicht? */
}qryMCData;

#define qryMCDataVersion  1

/*=== Werte für RETINIT ===*/
#define ARCH_RETINIT_CREATE 0
#define ARCH_RETINIT_EVENT  1

/*--------------------------------------------------------------------------+
|  Typdefinition f. Archivierungskopiengruppendetails in Antwort auf Verwaltungsklassenabfrage|
+--------------------------------------------------------------------------*/
typedef struct S_archDetailCG
{
   char         cgName[DSM_MAX_CG_NAME_LENGTH + 1];       /* Kopiengruppenname */
   dsUint16_t   frequency;                        /* Häufigkeit von Kopien (Archivierungen) */
   dsUint16_t   retainVers;                          /* Version aufbewahren */
   dsUint8_t    copySer;       /* Hinweise zur Kopiennummerierung siehe Definitionen */
   dsUint8_t    copyMode;         /* Hinweise zu Kopiermoduswerten siehe Definitionen oben */
   char         destName[DSM_MAX_CG_DEST_LENGTH + 1];      /* Zielname für Kopie */
   dsmBool_t    bLanFreeDest;            /* Ziel hat LAN-unabhängigen Pfad?    */
   dsmBool_t    reserved;                /* Derzeit nicht verwendet          */
   dsUint8_t    retainInit;              /* Mögliche Werte siehe oben        */
   dsUint16_t   retainMin;               /* wenn retInit auf EVENT gesetzt: Anzahl Tage */
   dsmBool_t    bDeduplicate;            /* Am Ziel ist Deduplizierung aktiviert    */
}archDetailCG;

/*--------------------------------------------------------------------------+
|  Typdefinition f. Sicherungskopiengruppendetails in Antwort auf Verwaltungsklassenabfrage   |
+--------------------------------------------------------------------------*/
typedef struct S_backupDetailCG
{
   char         cgName[DSM_MAX_CG_NAME_LENGTH + 1];       /* Kopiengruppenname */
   dsUint16_t   frequency;                           /* Häufigkeit der Sicherung */
   dsUint16_t   verDataExst;                        /* Versionen bestehender Daten */
   dsUint16_t   verDataDltd;                       /* Versionen gelöschter Daten */
   dsUint16_t   retXtraVers;                       /* Extraversionen aufbewahren */
   dsUint16_t   retOnlyVers;                       /* Einzige Version aufbewahren */
   dsUint8_t    copySer;       /* Hinweise zur Kopiennummerierung siehe Definitionen */
   dsUint8_t    copyMode;         /* Hinweise zu Kopiermoduswerten siehe Definitionen oben */
   char         destName[DSM_MAX_CG_DEST_LENGTH + 1];      /* Zielname für Kopie */
   dsmBool_t    bLanFreeDest;            /* Ziel hat LAN-unabhängigen Pfad?    */
   dsmBool_t    reserved;                /* Derzeit nicht verwendet          */
   dsmBool_t    bDeduplicate;            /* Am Ziel ist Deduplizierung aktiviert    */
}backupDetailCG;


/*--------------------------------------------------------------------------+
|  Typdefinition für Detailantwort zu Verwaltungsklassenabfrage in dsmGetNextQObj()           |
+--------------------------------------------------------------------------*/
typedef struct S_qryRespMCDetailData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char            mcName[DSM_MAX_MC_NAME_LENGTH + 1];        /* Verwaltungsklassenname */
   char            mcDesc[DSM_MAX_MC_DESCR_LENGTH + 1]; /* Verwaltungsklassenbeschreibung */
   archDetailCG    archDet;                /* Archivierungskopiengruppendetail */
   backupDetailCG  backupDet;               /* Sicherungskopiengruppendetail */
}qryRespMCDetailData;

#define qryRespMCDetailDataVersion  4

/*--------------------------------------------------------------------------+
| Typdefinition f. Antwort mit Zusammenfass. zur Verwaltungsklassenabfrage in dsmGetNextQObj()|
+--------------------------------------------------------------------------*/
typedef struct S_qryRespMCData
```

```
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char            mcName[DSM_MAX_MC_NAME_LENGTH + 1];        /* Verwaltungsklassenname */
   char            mcDesc[DSM_MAX_MC_DESCR_LENGTH + 1]; /* Verwaltungsklassenbeschreibung */
}qryRespMCData;

#define qryRespMCDataVersion  1



/*------------------------------------------------------------------------+
|  Typdefinition für queryBuffer für Archivierung in dsmBeginQuery()      |
+------------------------------------------------------------------------*/
typedef struct S_qryArchiveData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmObjName   *objName;                    /* Vollständiger DSM-Name des Objekts */
   char         *owner;                                 /* Eignername */
                 /* Hinweise zu maximalen Datumsgrenzen siehe Definitionen oben */
   dsmDate      insDateLowerBound;      /* unterer Grenzwert für Archivierungseinfügedatum */
   dsmDate      insDateUpperBound;      /* oberer Grenzwert für Archivierungseinfügedatum */
   dsmDate      expDateLowerBound;      /* unterer Grenzwert für Verfallsdatum */
   dsmDate      expDateUpperBound;      /* oberer Grenzwert für Verfallsdatum */
   char         *descr;               /* Archivierungsbeschreibung */
} qryArchiveData;

#define qryArchiveDataVersion  1



/*=== Werte für Feld retentionInitiated ===*/
#define DSM_ARCH_RETINIT_UNKNOWN 0 /* Aufbewahrungseinleitung ist unbekannt (Server mit älterer Version) */
#define DSM_ARCH_RETINIT_STARTED 1 /* Uhr für Aufbewahrungsdauer wird gestartet */
#define DSM_ARCH_RETINIT_PENDING 2 /* Uhr für Aufbewahrungsdauer wird nicht gestartet */


/*=== Werte für objHeld ===*/
#define DSM_ARCH_HELD_UNKNOWN 0    /* unbekannter Haltestatus (Server mit älterer Version) */
#define DSM_ARCH_HELD_FALSE   1    /* Objekt ist NICHT in einem Rückstellungsstatus für 'Löschen' */
#define DSM_ARCH_HELD_TRUE    2    /* Objekt ist in einem Rückstellungsstatus für 'Löschen' */

/*------------------------------------------------------------------------+
| Typdefinition für Antwort auf Archivierungsabfrage in dsmGetNextQObj()  |
+------------------------------------------------------------------------*/
typedef struct S_qryRespArchiveData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmObjName      objName;                          /* Qualifikationsmerkmal für Dateibereichsname */
   dsUint32_t      copyGroup;                        /* Kopiengruppenzahl */
   char            mcName[DSM_MAX_MC_NAME_LENGTH + 1];        /* Verwaltungsklassenname */
   char        owner[DSM_MAX_OWNER_LENGTH + 1];           /* Eignername */
   dsStruct64_t    objId;                            /* Eindeutige Kopien-ID */
   dsStruct64_t    reserved;                      /* Abwärtskompatibilität */
   dsUint8_t       mediaClass;                       /* Datenträgerzugriffsklasse */
   dsmDate         insDate;                          /* Archivierungseinfügedatum */
   dsmDate         expDate;                     /* Verfallsdatum für Objekt */
   char            descr[DSM_MAX_DESCR_LENGTH + 1];     /* Archivierungsbeschreibung */
   dsUint16_t  objInfolen;                        /* Länge der objektabhängigen Informationen */
   char            reservedObjInfo[DSM_MAX_OBJINFO_LENGTH];  /* objektabhängige Informationen */
   dsUint160_t     restoreOrderExt;                  /* Zurückschreibungsreihenfolge */
   dsStruct64_t    sizeEstimate;              /* vom Benutzer gespeicherte Größenschätzung */
   dsUint8_t       compressType;                       /* Komprimierungsflag */
   dsUint8_t       retentionInitiated;               /* Objekt wartet bei Aufbewahrungsereignis */
   dsUint8_t       objHeld;  /* Objekt befindet sich im Aufbewahrungshaltestatus, siehe Werte oben */
   dsUint8_t       encryptionType;          /* Verschlüsselungstyp */
   dsmBool_t       clientDeduplicated;      /* Objekt wird von API dedupliziert */
   char            objInfo[DSM_MAX_EXT_OBJINFO_LENGTH];  /* objektabhängige Informationen */
   char            compressAlg[DSM_MAX_COMPRESSTYPE_LENGTH + 1];  /* Komprimierungsalgorithmusname */
}qryRespArchiveData;

#define qryRespArchiveDataVersion  7

/*------------------------------------------------------------------------+
|  Typdefinition für Archivierungsparameter sendBuff in dsmSendObj()      |
+------------------------------------------------------------------------*/
typedef struct S_sndArchiveData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char         *descr;                      /* Archivierungsbeschreibung */
}sndArchiveData;

#define sndArchiveDataVersion  1
```

```
/*------------------------------------------------------------------------+
|  Typdefinition für queryBuffer für Sicherung in dsmBeginQuery()         |
+------------------------------------------------------------------------*/
typedef struct S_qryBackupData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmObjName  *objName;          /* Vollständiger DSM-Name des Objekts */
   char        *owner;            /* Eignername */
   dsUint8_t   objState;          /* Objektstatusselektor */
   dsmDate     pitDate;           /* Datumswert für zeitpunktgesteuerte Zurückschreibung */
                                  /* Hinweise zu möglichen Werten siehe Definitionen oben */
}qryBackupData;

#define qryBackupDataVersion  2

typedef struct
{
  dsUint8_t    reserved1;
  dsStruct64_t reserved2;
} reservedInfo_t;                 /* für zukünftige Verwendung */

/*------------------------------------------------------------------------+
| Typdefinition für Antwort auf Sicherungsabfrage in dsmGetNextQObj()     |
+------------------------------------------------------------------------*/
typedef struct S_qryRespBackupData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmObjName      objName;                      /* Vollständiger DSM-Name des Objekts */
   dsUint32_t      copyGroup;                          /* Kopiengruppenzahl */
   char            mcName[DSM_MAX_MC_NAME_LENGTH + 1];        /* Verwaltungsklassenname */
   char        owner[DSM_MAX_OWNER_LENGTH + 1];           /* Eignername */
   dsStruct64_t    objId;                              /* Eindeutige Objekt-ID */
   dsStruct64_t    reserved;                        /* Abwärtskompatibilität */
   dsUint8_t       mediaClass;                         /* Datenträgerzugriffsklasse */
   dsUint8_t       objState;                            /* Objektstatus, aktiv usw. */
   dsmDate     insDate;                           /* Sicherungseinfügedatum */
   dsmDate         expDate;                    /* Verfallsdatum für Objekt */
   dsUint16_t  objInfolen;                          /* Länge der objektabhängigen Informationen */
   char            reservedObjInfo[DSM_MAX_OBJINFO_LENGTH];  /* objektabhängige Informationen */
   dsUint160_t     restoreOrderExt;                    /* Zurückschreibungsreihenfolge */
   dsStruct64_t    sizeEstimate;                       /* vom Benutzer gespeicherte Größenschätzung */
   dsStruct64_t    baseObjId;
   dsUint16_t      baseObjInfolen;                     /* Länge der basisobjektabhängigen Informationen */
   dsUint8_t       baseObjInfo[DSM_MAX_OBJINFO_LENGTH]; /* basisobjektabhängige Informationen */
   dsUint160_t     baseRestoreOrder;                   /* Zurückschreibungsreihenfolge */
   dsUint32_t      fsID;
   dsUint8_t       compressType;
   dsmBool_t       isGroupLeader;
   dsmBool_t       isOpenGroup;
   dsUint8_t       reserved1;              /* für zukünftige Verwendung */
   dsmBool_t       reserved2;              /* für zukünftige Verwendung */
   dsUint16_t      reserved3;              /* für zukünftige Verwendung */
   reservedInfo_t  *reserved4;             /* für zukünftige Verwendung */
   dsUint8_t       encryptionType;         /* Verschlüsselungstyp */
   dsmBool_t       clientDeduplicated;     /* Objekt wird von API dedupliziert */
   char            objInfo[DSM_MAX_EXT_OBJINFO_LENGTH];  /* objektabhängige Informationen */
   char            compressAlg[DSM_MAX_COMPRESSTYPE_LENGTH + 1];  /* Komprimierungsalgorithmusname */
}qryRespBackupData;

#define qryRespBackupDataVersion  8

/*------------------------------------------------------------------------+
|  Typdefinition für queryBuffer für aktive Sicherung in dsmBeginQuery()  |
|                                                                         |
|  Hinweise: Für die Abfrage der aktiven Sicherung müssen nur die Felder  |
|            fs (Dateibereich) und objType gesetzt werden. objType kann nur|
|            auf DSM_OBJ_FILE oder DSM_OBJ_DIRECTORY gesetzt werden.     |
|            Für DSM_OBJ_ANY_TYPE wird keine Übereinstimmung in der Abfrage|
|            gefunden.                                                    |
+------------------------------------------------------------------------*/
typedef struct S_qryABackupData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmObjName      *objName;                    /* Nur fs und objType werden verwendet */
}qryABackupData;

#define qryABackupDataVersion  1

/*------------------------------------------------------------------------+
| Typdefinition für Antwort auf Abfrage der aktiven Sicherung in dsmGetNextQObj()          |
+------------------------------------------------------------------------*/
```

```
typedef struct S_qryARespBackupData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmObjName  objName;                      /* Vollständiger DSM-Name des Objekts */
   dsUint32_t  copyGroup;                       /* Kopiengruppenzahl */
   char        mcName[DSM_MAX_MC_NAME_LENGTH + 1];/* Verwaltungsklassenname */
   char        owner[DSM_MAX_OWNER_LENGTH + 1];           /* Eignername */
   dsmDate     insDate;                        /* Sicherungseinfügedatum */
   dsUint16_t  objInfolen;                     /* Länge der objektabhängigen Informationen */
   char           reservedObjInfo[DSM_MAX_OBJINFO_LENGTH];  /* objektabhängige Informationen */
   char           objInfo[DSM_MAX_EXT_OBJINFO_LENGTH];  /* objektabhängige Informationen */
}qryARespBackupData;

#define qryARespBackupDataVersion  2

/*------------------------------------------------------------------------+
|  Typdefinition für queryBuffer für Sicherung in dsmBeginQuery()         |
+------------------------------------------------------------------------*/
typedef struct qryBackupGroups
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint8_t    groupType;
   char         *fsName;
   char         *owner;
   dsStruct64_t groupLeaderObjId;
   dsUint8_t    objType;
   dsmBool_t    noRestoreOrder;
   dsmBool_t    noGroupInfo;
   char         *hl;
}qryBackupGroups;

#define qryBackupGroupsVersion 3


/*------------------------------------------------------------------------+
|  Typdefinition für queryBuffer für Proxy-Knoten in dsmBeginQuery()      |
+------------------------------------------------------------------------*/
typedef struct qryProxyNodeData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char        *targetNodeName;            /* Zielknotenname  */
}qryProxyNodeData;

#define qryProxyNodeDataVersion  1

/*------------------------------------------------------------------------+
| Typdefinition für den in dsmGetNextQObj() verwendeten Parameter qryRespProxyNodeData       |
+------------------------------------------------------------------------*/

typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char           targetNodeName[DSM_MAX_ID_LENGTH+1]; /* Zielknotenname  */
   char           peerNodeName[DSM_MAX_ID_LENGTH+1];   /* Peerknotenname  */
   char           hlAddress[DSM_MAX_ID_LENGTH+1];      /* übergeordnete Peeradresse */
   char           llAddress[DSM_MAX_ID_LENGTH+1];      /* untergeordnete Peeradresse */
}qryRespProxyNodeData;

#define qryRespProxyNodeDataVersion  1


/*------------------------------------------------------------------------+
|  Typdefinition für WINNT- und OS/2-Dateibereichsattribute               |
+------------------------------------------------------------------------*/
typedef struct
{
   char         driveLetter ;          /* Laufwerkbuchstabe für Dateibereich */
   dsUint16_t   fsInfoLength;          /* für Dateibereichsinformationen verwendete Länge */
   char         fsInfo[DSM_MAX_FSINFO_LENGTH];/* vom Aufrufenden bestimmte Daten */
}dsmDosFSAttrib ;

/*------------------------------------------------------------------------+
|  Typdefinition für UNIX-Dateibereichsattribute                          |
+------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t   fsInfoLength;          /* für Dateibereichsinformationen verwendete Länge */
   char         fsInfo[DSM_MAX_FSINFO_LENGTH];/* vom Aufrufenden bestimmte Daten */
}dsmUnixFSAttrib ;

/*------------------------------------------------------------------------+
|  Typdefinition für NetWare-Dateibereichsattribute                       |
```

```
+--------------------------------------------------------------------------*/
typedef dsmUnixFSAttrib dsmNetwareFSAttrib;

/*--------------------------------------------------------------------------+
|  Typdefinition für Dateibereichsattribute in allen Dateibereichsaufrufen |
+--------------------------------------------------------------------------*/
typedef union
{
   dsmNetwareFSAttrib  netwareFSAttr;
   dsmUnixFSAttrib     unixFSAttr ;
   dsmDosFSAttrib      dosFSAttr ;
}dsmFSAttr ;

/*--------------------------------------------------------------------------+
|  Typdefinition für Parameter fsUpd in dsmUpdateFS()                       |
+--------------------------------------------------------------------------*/
typedef struct S_dsmFSUpd
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char            *fsType ;              /* Dateibereichstyp              */
   dsStruct64_t    occupancy ;            /* Belegungsschätzung            */
   dsStruct64_t    capacity  ;            /* Kapazitätsschätzung           */
   dsmFSAttr       fsAttr ;               /* plattformspezifische Attribute */
}dsmFSUpd ;

#define dsmFSUpdVersion  1

/*--------------------------------------------------------------------------+
|  Typdefinition für queryBuffer für Dateibereich in dsmBeginQuery()        |
+--------------------------------------------------------------------------*/
typedef struct S_qryFSData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char        *fsName;                  /* Dateibereichsname */
}qryFSData;

#define qryFSDataVersion  1

/*--------------------------------------------------------------------------+
| Typdefinition für Antwort auf Dateibereichsabfrage in dsmGetNextQObj()    |
+--------------------------------------------------------------------------*/
typedef struct S_qryRespFSData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char           fsName[DSM_MAX_FSNAME_LENGTH + 1];         /* Dateibereichsname */
   char           fsType[DSM_MAX_FSTYPE_LENGTH + 1] ;        /* Dateibereichstyp  */
   dsStruct64_t   occupancy;                        /* Belegungsschätzung in Byte */
   dsStruct64_t   capacity;                         /* Kapazitätsschätzung in Byte */
   dsmFSAttr      fsAttr ;                         /* plattformspezifische Attribute */
   dsmDate        backStartDate;                   /* Datum für Sicherungsbeginn */
   dsmDate        backCompleteDate;                /* Datum für Sicherungsende   */
   dsmDate        reserved1;                       /* Für zukünftige Verwendung  */
   dsmDate        lastReplStartDate;        /* Startzeitpunkt der letzten Replikation     */
   dsmDate        lastReplCmpltDate;        /* Endzeitpunkt der letzten Replikation       */
                                            /*   (eventuell trat ein Fehler auf,          */
                                            /*    aber sie wurde dennoch beendet)         */
   dsmDate        lastBackOpDateFromServer; /* Die letzte Speicherungszeitmarke, die der  */
                                            /* Client auf dem Server gespeichert hat      */
   dsmDate        lastArchOpDateFromServer; /* Die letzte Speicherungszeitmarke, die der  */
                                            /* Client auf dem Server gespeichert hat      */
   dsmDate        lastSpMgOpDateFromServer; /* Die letzte Speicherungszeitmarke, die der  */
                                            /* Client auf dem Server gespeichert hat      */
   dsmDate        lastBackOpDateFromLocal;  /* Die letzte Speicherungszeitmarke, die der  */
                                            /*    Client lokal gespeichert hat            */
   dsmDate        lastArchOpDateFromLocal;  /* Die letzte Speicherungszeitmarke, die der  */
                                            /*    Client lokal gespeichert hat            */
   dsmDate        lastSpMgOpDateFromLocal;  /* Die letzte Speicherungszeitmarke, die der  */
                                            /*    Client lokal gespeichert hat            */
   dsInt32_t      failOverWriteDelay;       /* Minuten, die der Client vor dem Speichern  */
                                            /* auf diesem Rpl.server warten muss; Sonder- */
                                            /* codes: NO_ACCESS(-1), ACCESS_RDONLY (-2)   */
}qryRespFSData;

#define qryRespFSDataVersion 4

/*--------------------------------------------------------------------------+
|  Typdefinition für Parameter regFilespace in dsmRegisterFS()              |
+--------------------------------------------------------------------------*/
typedef struct S_regFSData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char            *fsName;                    /* Dateibereichsname */
```

```
   char           *fsType;                      /* Dateibereichstype */
   dsStruct64_t    occupancy;                   /* Belegungsschätzung in Byte */
   dsStruct64_t   capacity;                      /* Kapazitätsschätzung in Byte */
   dsmFSAttr       fsAttr ;                     /* plattformspezifische Attribute */
}regFSData;

#define regFSDataVersion  1

/*------------------------------------------------------------------------+
| Typdefinition für den in apisessInfo verwendeten dedupType              |
+------------------------------------------------------------------------*/
typedef enum
{
   dedupServerOnly= 0x00,            /* Deduplizierung erfolgt nur auf dem Server */
   dedupClientOrServer               /* Deduplizierung kann auf dem Client oder Server erfolgen */
}dsmDedupType ;

/*------------------------------------------------------------------------+
 | Typdefinition für Übernahmekonfiguration und -status
 ------------------------------------------------------------------------*/
typedef enum
{
   failOvrNotConfigured = 0x00,
   failOvrConfigured,
   failOvrConnectedToReplServer
}dsmFailOvrCfgType ;

/*------------------------------------------------------------------------+
|  Typdefinition für Antwort mit Sitzungsdaten in dsmQuerySessionInfo()    |
+------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t   stVersion;               /* Strukturversion                 */
      /*-------------------------------------------------------------------*/
      /*           Serverinformationen                                     */
      /*-------------------------------------------------------------------*/
   char           serverHost[DSM_MAX_SERVERNAME_LENGTH+1];
                                         /* Netzhostname des DSM-Servers */
   dsUint16_t     serverPort;            /* Serverkommunikationsport auf Host */
   dsmDate        serverDate;            /* Datum/Zeit des Servers */
   char           serverType[DSM_MAX_SERVERTYPE_LENGTH+1];
                                         /* Ausführungsplattform des Servers */
   dsUint16_t     serverVer;             /* Versionsnummer des Servers       */
   dsUint16_t     serverRel;             /* Releasenummer des Servers        */
   dsUint16_t     serverLev;             /* Stufennummer des Servers         */
   dsUint16_t         serverSubLev;  /* Unterstufennummer des Servers    */
      /*-------------------------------------------------------------------*/
      /*           Clientstandardwerte                                     */
n
      /*-------------------------------------------------------------------*/
   char           nodeType[DSM_MAX_PLATFORM_LENGTH+1]; /* Knoten-/Anwendungstyp */
   char           fsdelim;               /* Dateibereichsbegrenzer             */
   char           hldelim;               /* Begrenzer zwischen oberer u. unterer Ebene */
   dsUint8_t      compression;           /* Komprimierungsflag */
   dsUint8_t      archDel;               /* Berechtigung zum Löschen des Archivs */
   dsUint8_t      backDel;               /* Berechtigung zum Löschen der Sicherung */
   dsUint32_t     maxBytesPerTxn;        /* für zukünftige Verwendung */
   dsUint16_t     maxObjPerTxn;          /* Max. Anzahl Objekte in einer Transaktion */
      /*-------------------------------------------------------------------*/
      /*           Sitzungsdaten                                           */
      /*-------------------------------------------------------------------*/
   char       id[DSM_MAX_ID_LENGTH+1];    /* Knotenname der Anmelde-ID    */
   char       owner[DSM_MAX_OWNER_LENGTH+1]; /* Anmeldeeigner             */
                                 /*   (für Mehrbenutzerplattformen   */
   char       confFile[DSM_PATH_MAX + DSM_NAME_MAX +1];
                                /* Länge ist plattformabhängig       */
                                /* dsInit-Name der Anwend.-Konfig.-Datei */
   dsUint8_t  opNoTrace;             /* Option dsInit - NoTrace = 1      */
      /*-------------------------------------------------------------------*/
      /*           Maßnahmendaten                                          */
      /*-------------------------------------------------------------------*/
   char           domainName[DSM_MAX_DOMAIN_LENGTH+1]; /* Domänenname         */
   char           policySetName[DSM_MAX_PS_NAME_LENGTH+1];
                                 /* Name der aktiven Maßnahmengruppe */
   dsmDate        polActDate;         /* Aktivierungsdatum der Maßnahmengruppe */
   char           dfltMCName[DSM_MAX_MC_NAME_LENGTH+1];/* Standardverwaltungsklasse */
   dsUint16_t     gpBackRetn;            /* Karenzzeit f. Aufbewahrungszeitraum f. Sicherung */
   dsUint16_t     gpArchRetn;            /* Karenzzeit f. Aufbewahrungszeitraum f. Archivierung */
   char           adsmServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* ADSM-Servername */
   dsmBool_t      archiveRetentionProtection; /* Aufbewahrungsschutz durch Server ist aktiviert*/
   dsStruct64_t   maxBytesPerTxn_64;         /* für zukünftige Verwendung      */
   dsmBool_t      lanFreeEnabled;            /* Option 'LAN-unabhängig' ist gesetzt */
```

```
   dsmDedupType   dedupType;                /* server oder clientOrServer       */
   char           accessNode[DSM_MAX_ID_LENGTH+1];    /* als Knotenname          */

   /*-------------------------------------------------------------------*/
   /*          Replikations- und Übernahmeinformationen                 */
   /*-------------------------------------------------------------------*/
   dsmFailOvrCfgType failOverCfgType; /* Status der Übernahme */
   char           replServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* Replikationsservername            */
   char           homeServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* Home-Servername                   */
   char           replServerHost[DSM_MAX_SERVERNAME_LENGTH+1]; /* Netzhostname des DSM-Servers      */
   dsInt32_t      replServerPort;                              /* Serverkommunikationsport auf Host */

}ApiSessInfo;

#define ApiSessInfoVersion  6



/*-------------------------------------------------------------------------+
| Typdefinition für Antwort auf Abfrageoptionen in dsmQueryCliOptions()    |
|      und dsmQuerySessOptions()                                           |
+-------------------------------------------------------------------------*/

typedef struct
{
   char        dsmiDir[DSM_PATH_MAX + DSM_NAME_MAX +1];
   char        dsmiConfig[DSM_PATH_MAX + DSM_NAME_MAX +1];
   char        serverName[DSM_MAX_SERVERNAME_LENGTH+1];
   dsInt16_t   commMethod;
   char        serverAddress[DSM_MAX_SERVER_ADDRESS];
   char        nodeName[DSM_MAX_NODE_LENGTH+1];
   dsmBool_t   compression;
   dsmBool_t   compressalways;
   dsmBool_t   passwordAccess;
}optStruct ;

/*-------------------------------------------------------------------------+
| Typdefinition für in logInfo verwendeten LogType                         |
+-------------------------------------------------------------------------*/
typedef enum
{
   logServer = 0x00,            /* Protokollnachricht nur an Server */
   logLocal,                    /* Protokollnachricht nur an lokales Fehlerprotokoll */
   logBoth,                     /* Protokollnachricht an Server und lokales Fehlerprotokoll */
   logNone
}dsmLogType ;

/*-------------------------------------------------------------------------+
| Typdefinition für in dsmLogEvent() verwendeten Parameter logInfo         |
+-------------------------------------------------------------------------*/

typedef struct
{
   char        *message;   /* Text der zu protokollierenden Nachricht */
   dsmLogType  logType;    /* Protokolltyp: lokal, Server oder beides */
}logInfo;

/*-------------------------------------------------------------------------+
| Typdefinition für den in dsmQueryAccess() verwendeten Parameter qryRespAccessData           |
+-------------------------------------------------------------------------*/

typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char              node[DSM_MAX_ID_LENGTH+1];     /* Knotenname             */
   char              owner[DSM_MAX_OWNER_LENGTH+1]; /* Eigner                 */
   dsmObjName        objName ;                      /* Objektname             */
   dsmAccessType     accessType;                    /* Archiv. oder Sicherung */
   dsUint32_t        ruleNumber ;                   /* Zugriffsregel-ID       */
}qryRespAccessData;

#define qryRespAccessDataVersion  1

/*-------------------------------------------------------------------------+
|  Typdefinition für Parameter envSetUp in dsmSetUp()                      |
+-------------------------------------------------------------------------*/
typedef struct S_envSetUp
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   char            dsmiDir[DSM_PATH_MAX + DSM_NAME_MAX +1];
   char            dsmiConfig[DSM_PATH_MAX + DSM_NAME_MAX +1];
   char            dsmiLog[DSM_PATH_MAX + DSM_NAME_MAX +1];
```

```
   char          **argv;  /* für Name von ausführbaren Dateien (argv[0]) */
   char            logName[DSM_NAME_MAX +1];
   dsmBool_t       reserved1;         /* für zukünftige Verwendung */
   dsmBool_t       reserved2;              /* für zukünftige Verwendung */
}envSetUp;

#define envSetUpVersion  4

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmInitExIn_t                                         |
+-------------------------------------------------------------------------*/
typedef struct dsmInitExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmApiVersionEx    *apiVersionExP;
   char               *clientNodeNameP;
   char               *clientOwnerNameP;
   char               *clientPasswordP;
   char               *userNameP;
   char               *userPasswordP;
   char               *applicationTypeP;
   char               *configfile;
   char               *options;
   char               dirDelimiter;
   dsmBool_t          useUnicode;
   dsmBool_t          bCrossPlatform;
   dsmBool_t          bService;
   dsmBool_t          bEncryptKeyEnabled;
   char               *encryptionPasswordP;
   dsmBool_t          useTsmBuffers;
   dsUint8_t          numTsmBuffers;
   dsmAppVersion      *appVersionP;
}dsmInitExIn_t;

#define dsmInitExInVersion 5

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmInitExOut_t                                        |
+-------------------------------------------------------------------------*/
typedef struct dsmInitExOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsInt16_t          userNameAuthorities;
   dsInt16_t          infoRC;        /* Fehlercode, falls festgestellt */
   char               adsmServerName[DSM_MAX_SERVERNAME_LENGTH+1];
   dsUint16_t     serverVer;              /* Versionsnummer des Servers       */
   dsUint16_t         serverRel;     /* Releasenummer des Servers        */
   dsUint16_t     serverLev;              /* Stufennummer des Servers         */
   dsUint16_t         serverSubLev;  /* Unterstufennummer des Servers    */

   dsmBool_t          bIsFailOverMode; /* wahr im Fall einer Übernahme   */
   char               replServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* Replikationsservername */
   char               homeServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* Home-Servername        */

}dsmInitExOut_t;

#define dsmInitExOutVersion 3

/*-------------------------------------------------------------------------+
| Typdefinition für in logInfo verwendeten LogType                         |
+-------------------------------------------------------------------------*/
typedef enum
{
   logSevInfo = 0x00,       /* Information ANE4991 */
   logSevWarning,           /* Warnung     ANE4992 */
   logSevError,             /* Fehler      ANE4993 */
   logSevSevere,            /* schwerwiegend  ANE4994 */
   logSevLicense,           /* Lizenz      ANE4995 */
   logSevTryBuy             /* Probelizenz ANE4996 */
}dsmLogSeverity ;


/*-------------------------------------------------------------------------+
|  Typdefinition für dsmLogExIn_t                                          |
+-------------------------------------------------------------------------*/
typedef struct dsmLogExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmLogSeverity     severity;
   char               appMsgID[8];
   dsmLogType         logType;    /* Protokolltyp: lokal, Server oder beides */
   char               *message;   /* Text der zu protokollierenden Nachricht */
```

```
   char               appName[DSM_MAX_PLATFORM_LENGTH];
   char               osPlatform[DSM_MAX_PLATFORM_LENGTH];
   char               appVersion[DSM_MAX_PLATFORM_LENGTH];
}dsmLogExIn_t;

#define dsmLogExInVersion 2

/*------------------------------------------------------------------------+
|  Typdefinition für dsmlogExOut_t                                        |
+------------------------------------------------------------------------*/
typedef struct dsmLogExOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
}dsmLogExOut_t;

#define dsmLogExOutVersion 1

/*------------------------------------------------------------------------+
|  Typdefinition für dsmRenameIn_t                                        |
+------------------------------------------------------------------------*/
typedef struct dsmRenameIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t      dsmHandle;        /* Sitzungskennung */
   dsUint8_t        repository;                  /* Sicherung oder Archivierung */
   dsmObjName       *objNameP ;                  /* Objektname             */
   char             newHl[DSM_MAX_HL_LENGTH + 1];  /* neuer übergeordneter Name */
   char             newLl[DSM_MAX_LL_LENGTH + 1];  /* neuer untergeordneter Name */
   dsmBool_t        merge;                     /* mit vorhandenem Namen zusammenfassen */
   ObjID            objId;                     /* Objekt-ID für Archivierung */
}dsmRenameIn_t;

#define dsmRenameInVersion 1

/*------------------------------------------------------------------------+
|  Typdefinition für dsmRenameOut_t                                       |
+------------------------------------------------------------------------*/
typedef struct dsmRenameOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
}dsmRenameOut_t;

#define dsmRenameOutVersion 1

/*------------------------------------------------------------------------+
|  Typdefinition für dsmEndSendObjExIn_t                                  |
+------------------------------------------------------------------------*/
typedef struct dsmEndSendObjExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t      dsmHandle;        /* Sitzungskennung */
}dsmEndSendObjExIn_t;

#define dsmEndSendObjExInVersion 1

/*------------------------------------------------------------------------+
|  Typdefinition für dsmEndSendObjExOut_t                                 |
+------------------------------------------------------------------------*/
typedef struct dsmEndSendObjExOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsStruct64_t       totalBytesSent;      /* Gesamtsumme aus Anwendung gelesener Byte */
   dsmBool_t          objCompressed;       /* mit Objektkomprimierung */
   dsStruct64_t       totalCompressSize;   /* Gesamtgröße nach Komprimierung */
   dsStruct64_t       totalLFBytesSent;    /* Gesamtanzahl LAN-unabhängig gesendeter Byte */
   dsUint8_t          encryptionType;      /* verwendeter Verschlüsselungstyp */
   dsmBool_t          objDeduplicated;     /* Objektverarbeitung für verteilte Deduplizierung */
   dsStruct64_t       totalDedupSize;      /* Gesamtgröße nach Deduplizierung */
}dsmEndSendObjExOut_t;

#define dsmEndSendObjExOutVersion 3
/*------------------------------------------------------------------------+
|  Typdefinition für dsmGroupHandlerIn_t                                  |
+------------------------------------------------------------------------*/
typedef struct dsmGroupHandlerIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t      dsmHandle;        /* Sitzungskennung */
   dsUint8_t       groupType;        /* Gruppentyp         */
   dsUint8_t       actionType;       /* Gruppenoperationstyp */
   dsUint8_t       memberType;       /* Mitgliedstyp: Leiter oder Mitglied */
   dsStruct64_t    leaderObjId;      /* OBJID des Gruppenleiters beim Bearbeiten eines Mitglieds */
```

```
   char            *uniqueGroupTagP; /* Eindeutige Gruppen-ID */
   dsmObjName      *objNameP ;       /* Objektname des Gruppenleiters */
   dsmGetList      memberObjList;    /* Liste der zu enfernenden bzw. zuzuordnenden Objekte */
}dsmGroupHandlerIn_t;

#define dsmGroupHandlerInVersion 1

/*------------------------------------------------------------------------+
|  Typdefinition für dsmGroupHandlerExOut_t                               |
+------------------------------------------------------------------------*/
typedef struct dsmGroupHandlerOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
}dsmGroupHandlerOut_t;

#define dsmGroupHandlerOutVersion 1

/*------------------------------------------------------------------------+
|  Typdefinition für dsmEndTxnExIn_t                                      |
+------------------------------------------------------------------------*/
typedef struct dsmEndTxnExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t      dsmHandle;        /* Sitzungskennung */
   dsUint8_t        vote;
}dsmEndTxnExIn_t;

#define dsmEndTxnExInVersion 1

/*------------------------------------------------------------------------+
|  Typdefinition für dsmEndTxnExOut_t                                     |
+------------------------------------------------------------------------*/
typedef struct dsmEndTxnExOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint16_t         reason;                 /* Ursachencode                  */
   dsStruct64_t       groupLeaderObjId;       /* Gruppenleiterobjekt-ID (für   */
                                              /* DSM_ACTION_OPEN zurückgegeben) */
   dsUint8_t          reserved1;              /* für zukünftige Verwendung     */
   dsUint16_t         reserved2;              /* für zukünftige Verwendung     */
}dsmEndTxnExOut_t;

#define dsmEndTxnExOutVersion 1

/*------------------------------------------------------------------------+
|  Typdefinition für dsmEndGetDataExIn_t                                  |
+------------------------------------------------------------------------*/
typedef struct dsmEndGetDataExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t     dsmHandle;     /* Sitzungskennung */
}dsmEndGetDataExIn_t;

#define dsmEndGetDataExInVersion 1

/*------------------------------------------------------------------------+
|  Typdefinition für dsmEndGetDataExOut_t                                 |
+------------------------------------------------------------------------*/
typedef struct dsmEndGetDataExOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint16_t         reason;                 /* Ursachencode                  */
   dsStruct64_t   totalLFBytesRecv;  /* Gesamtzahl LAN-unabhängig empfangener Byte */
}dsmEndGetDataExOut_t;

#define dsmEndGetDataExOutVersion 1

/*------------------------------------------------------------------------+
| Typdefinition für Objektliste in dsmRetentionEvent()                    |
+------------------------------------------------------------------------*/
typedef struct dsmObjList
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t       numObjId ;         /* Anzahl Objekt-IDs in Liste       */
   ObjID            *objId;            /* Liste der als Signal zu sendenden Objekt-IDs */
}dsmObjList_t ;

#define dsmObjlistVersion 1

/*------------------------------------------------------------------------+
| Typdefinition für den in dsmRetentionEvent verwendeten eventType        |
+------------------------------------------------------------------------*/
```

```
typedef enum
{
   eventRetentionActivate = 0x00,   /* dem Server signalisieren, dass das Ereignis stattgefunden hat */
   eventHoldObj,                    /* Löschen/Verfall des Objekts aussetzen */
   eventReleaseObj                  /* normale Lösch-/Verfallsverarbeitung wiederaufnehmen */
}dsmEventType_t;

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmRetentionEvent()                                   |
+-------------------------------------------------------------------------*/
typedef struct dsmRetentionEventIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t         dsmHandle;                   /* Sitzungskennung    */
   dsmEventType_t     eventType;                   /* Ereignistyp      */
   dsmObjList_t       objList;                     /* Objekt-ID        */
}dsmRetentionEventIn_t;

#define dsmRetentionEventInVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmRetentionEvent()                                   |
+-------------------------------------------------------------------------*/
typedef struct dsmRetentionEventOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
}dsmRetentionEventOut_t;

#define dsmRetentionEventOutVersion 1


/*-------------------------------------------------------------------------+
|  Typdefinition für dsmRequestBuffer()                                    |
+-------------------------------------------------------------------------*/
typedef struct requestBufferIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t         dsmHandle;                   /* Sitzungskennung    */
}requestBufferIn_t;

#define requestBufferInVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmRequestBuffer()                                    |
+-------------------------------------------------------------------------*/
typedef struct requestBufferOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint8_t        tsmBufferHandle;          /* Kennung zu TSM-Datenpuffer */
   char             *dataPtr;                 /* Adresse, in die Daten geschrieben werden */
   dsUint32_t       bufferLen;                /* Maximale Länge der zu schreibenden Daten */
}requestBufferOut_t;

#define requestBufferOutVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmReleaseBuffer()                                    |
+-------------------------------------------------------------------------*/
typedef struct releaseBufferIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t         dsmHandle;                   /* Sitzungskennung    */
   dsUint8_t        tsmBufferHandle;       /* Kennung zu TSM-Datenpuffer */
   char               *dataPtr;                  /* Adresse, in die Daten geschrieben werden */
}releaseBufferIn_t;

#define releaseBufferInVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmReleaseBuffer()                                    |
+-------------------------------------------------------------------------*/
typedef struct releaseBufferOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
}releaseBufferOut_t;

#define releaseBufferOutVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmGetBufferData()                                    |
+-------------------------------------------------------------------------*/
typedef struct getBufferDataIn_t
```

```
{
   dsUint16_t         stVersion;               /* Strukturversion               */
   dsUint32_t         dsmHandle;                    /* Sitzungskennung    */
}getBufferDataIn_t;

#define getBufferDataInVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmGetBufferData()                                    |
+-------------------------------------------------------------------------*/
typedef struct getBufferDataOut_t
{
   dsUint16_t         stVersion;               /* Strukturversion               */
   dsUint8_t        tsmBufferHandle;       /* Kennung zu TSM-Datenpuffer */
   char             *dataPtr;              /* Adresse der aktuell zu lesenden Daten */
   dsUint32_t       numBytes;              /* Aktuell aus dataPtr zu lesende Anzahl Byte */
}getBufferDataOut_t;

#define getBufferDataOutVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmSendBufferData()                                   |
+-------------------------------------------------------------------------*/
typedef struct sendBufferDataIn_t
{
   dsUint16_t         stVersion;               /* Strukturversion               */
   dsUint32_t         dsmHandle;             /* Sitzungskennung    */
   dsUint8_t          tsmBufferHandle;       /* Kennung zu TSM-Datenpuffer */
   char               *dataPtr;              /* Adresse der aktuell zu sendenden Daten */
   dsUint32_t         numBytes;              /* Anzahl der aktuell aus dataPtr zu sendenden Byte */
}sendBufferDataIn_t;

#define sendBufferDataInVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmSendBufferData()                                   |
+-------------------------------------------------------------------------*/
typedef struct sendBufferDataOut_t
{
   dsUint16_t         stVersion;               /* Strukturversion               */
}sendBufferDataOut_t;

#define sendBufferDataOutVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmUpdateObjExIn_t                                    |
+-------------------------------------------------------------------------*/
typedef struct dsmUpdateObjExIn_t
{
   dsUint16_t         stVersion;               /* Strukturversion               */
   dsUint32_t      dsmHandle;            /* Sitzungskennung     */
   dsmSendType     sendType;             /* Sendetyp (Sich./Archiv.) */
   char            *descrP;              /* Archivierungsbeschreibung */
   dsmObjName      *objNameP;            /* Objektname          */
   ObjAttr         *objAttrPtr;          /* Attribut            */
   dsUint32_t      objUpdAct;            /* Aktualisierungsaktion */
   ObjID           archObjId;            /* Objekt-ID für Archivierung */
}dsmUpdateObjExIn_t;

#define dsmUpdateObjExInVersion 1

/*-------------------------------------------------------------------------+
|  Typdefinition für dsmUpdateObjExOut_t                                   |
+-------------------------------------------------------------------------*/
typedef struct dsmUpdateObjExOut_t
{
    dsUint16_t         stVersion;               /* Strukturversion               */
}dsmUpdateObjExOut_t;

#define dsmUpdateObjExOutVersion 1

#if (_OPSYS_TYPE == DS_WINNT) && !defined(_WIN64)
#pragma pack()
#endif


#ifdef _MAC
#pragma options align=reset
#endif
#endif /* _H_DSMAPITD */
```

```
/*****************************************************************
 * Tivoli Storage Manager                                        *
 * API-Clientkomponente                                          *
 *                                                               *
 * (C) Copyright IBM Corporation 1993, 2010                      *
 *****************************************************************/

/*****************************************************************
 * Headerdateiname: tsmapitd.h
 *
 * Umgebung:        ***********************************************
 *                  ** Dies ist eine plattformunabhängige         **
*                  ** Quellendatei                               **
 *
 *                  ***********************************************
 *
 * Anm. zum Entwurf: Diese Datei enthält Basisdatentypen und Konstanten, die in
 *                   allen Clientquellendateien verwendet werden können. Die Konstanten
 *                   in dieser Datei müssen für die spezielle Maschine bzw. für das
 *                   spezielle Betriebssystem, auf dem die Clientsoftware ausgeführt
 *                   werden soll, ordnungsgemäß gesetzt werden.
 *
 *                   dsmapips.h enthält plattformspezifische Definitionen
 *
 * Beschreib. Name:  Definitionen für Konstanten der Tivoli Storage
*                  Manager-API
 *-----------------------------------------------------------------*/

#ifndef _H_TSMAPITD
#define _H_TSMAPITD


/*=== Strukturausrichtung zum Packen der Strukturen definieren ===*/
#if _OPSYS_TYPE == DS_WINNT
#ifdef _WIN64
#pragma pack(8)
#else
#pragma pack(1)
#endif
#endif

#ifdef _MAC
#pragma options align = packed
#endif

/*============================================================
 Win32-Anwendungen, die die TSM-Schnittstelle verwenden,
 müssen während der Kompilierung das Flag -DUNICODE verwenden.
 ============================================================*/
#if _OPSYS_TYPE == DS_WINNT && !defined(DSMAPILIB)
#ifndef UNICODE
#error "Win32-Anwendungen, die die TSM-Schnittstelle verwenden, MÜSSEN mit dem Flag -DUNICODE kompiliert
werden"
#endif
#endif

/*============================================================
 Mac OS X-Anwendungen, die die TSM-Schnittstelle verwenden,
 müssen während der Kompilierung das Flag -DUNICODE verwenden.
 ============================================================*/
#if _OPSYS_TYPE == DS_MACOS && !defined(DSMAPILIB)
#ifndef UNICODE
#error "Mac OS X-Anwendungen, die die TSM-Schnittstelle verwenden, MÜSSEN mit dem Flag -DUNICODE kompiliert
werden"
#endif
#endif

/*-----------------------------------------------------------------------+
 | Typdefinition für Parameter dsmGetType in tsmBeginGetData()           |
 +-----------------------------------------------------------------------*/
typedef enum
{
   gtTsmBackup = 0x00,                    /* Sicherungsverarbeitungstyp    */
   gtTsmArchive                           /* Archivierungsverarbeitungstyp */
} tsmGetType ;

/*-----------------------------------------------------------------------+
 |  Typdefinition für Parameter dsmQueryType in tsmBeginQuery()          |
 +-----------------------------------------------------------------------*/
typedef enum
{
   qtTsmArchive = 0x00,                    /* Archivabfragetyp          */
```

```
   qtTsmBackup,                          /* Sicherungsabfragetyp      */
   qtTsmBackupActive,                   /* Schnellabfr. f. aktive Sich.dateien*/
   qtTsmFilespace,                       /* Dateibereichsabfragetyp   */
   qtTsmMC,                              /* Verwaltungsklassenabfragetyp */
    qtTsmReserved1,                       /* zukünftige Verwendung     */
    qtTsmReserved2,                       /* zukünftige Verwendung     */
    qtTsmReserved3,                       /* zukünftige Verwendung     */
    qtTsmReserved4,                       /* zukünftige Verwendung     */
   qtTsmBackupGroups,                    /* Alle Gruppenleiter in einem bestimmten Dateibereich */
   qtTsmOpenGroups,                      /* Alle einem Leiter zugeordneten Gruppenmitglieder */
    qtTsmReserved5,                       /* zukünftige Verwendung     */
   qtTsmProxyNodeAuth,                   /* Knoten, an die dieser Knoten weiterleiten kann*/
    qtTsmProxyNodePeer,                   /* Peerknoten unter diesem Zielknoten */
    qtTsmReserved6,                      /* zukünftige Verwendung     */
    qtTsmReserved7,                      /* zukünftige Verwendung     */
    qtTsmReserved8                       /*  zukünftige Verwendung    */
} tsmQueryType ;

/*-------------------------------------------------------------------------+
 |  Typdefinition für Parameter sendType in tsmBindMC() und tsmSendObj()    |
 +-------------------------------------------------------------------------*/
typedef enum
{
   stTsmBackup = 0x00,                      /* Sicherungsverarbeitungstyp */
   stTsmArchive,                            /* Archivierungsverarbeitungstyp */
   stTsmBackupMountWait,           /* Sicherungsverarbeitung; 'Auf Ladevorgang warten' ist aktiviert*/
   stTsmArchiveMountWait           /* Archivierungsverarbeitung; 'Auf Ladevorgang warten' ist aktiviert*/
} tsmSendType ;

/*-------------------------------------------------------------------------+
 |  Typdefinition für Parameter delType in tsmDeleteObj()                   |
 +-------------------------------------------------------------------------*/
typedef enum
{
   dtTsmArchive = 0x00,                 /* Typ 'Archivierung löschen' */
   dtTsmBackup,                         /* Typ 'Sicherung löschen (inaktivieren)' */
   dtTsmBackupID                        /* Typ 'Sicherung löschen' (entfernen)' */
} tsmDelType ;

/*-------------------------------------------------------------------------+
 |  Typdefinition für Parameter sendType in tsmSetAccess()                  |
 +-------------------------------------------------------------------------*/
typedef enum
{
   atTsmBackup = 0x00,                   /* Sicherungsverarbeitungstyp */
   atTsmArchive                          /* Archivierungsverarbeitungstyp */
}tsmAccessType;

/*-------------------------------------------------------------------------+
 |  Typdefinition für Parameter Overwrite in tsmSendObj()                   |
 +-------------------------------------------------------------------------*/
typedef enum
{
   owIGNORE = 0x00,
   owYES,
   owNO
}tsmOwType;


/*-------------------------------------------------------------------------+
 |  Typdefinition für API-Version in tsmInit() und tsmQueryApiVersion()     |
 +-------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t     stVersion;             /* Strukturversion             */
   dsUint16_t version;       /* API-Version                       */
   dsUint16_t release;       /* API-Release                       */
   dsUint16_t level;         /* API-Stand                         */
   dsUint16_t subLevel;      /* API-Unterstufe                    */
   dsBool_t  unicode;        /* API-Unicode? */
} tsmApiVersionEx;

#define tsmApiVersionExVer       2

/*-------------------------------------------------------------------------+
|  Typdefinition für Anwendungsversion in tsmInit()                         |
+-------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t   stVersion;               /* Strukturversion                  */
   dsUint16_t   applicationVersion;      /* Anwendungsversionsnummer         */
   dsUint16_t   applicationRelease;      /* Anwendungsreleasenummer          */
```

```
   dsUint16_t   applicationLevel;         /* Anwendungsebenennummer            */
   dsUint16_t   applicationSubLevel;      /* Anwendungsunterstufennummer       */
} tsmAppVersion;

#define tsmAppVersionVer      1


/*-------------------------------------------------------------------------+
 |  Typdefinition für in BindMC, Send, Delete, Query verwendeten Objektnamen|
 +-------------------------------------------------------------------------*/

typedef struct tsmObjName
{
   dsChar_t   fs[DSM_MAX_FSNAME_LENGTH + 1] ;              /* Dateibereichsname */
   dsChar_t   hl[DSM_MAX_HL_LENGTH + 1] ;                  /* Übergeordneter Name */
   dsChar_t   ll[DSM_MAX_LL_LENGTH + 1] ;                  /* Untergeordneter Name */
   dsUint8_t  objType;               /* Definitionen für Objekttypwerte siehe oben */
   dsChar_t   dirDelimiter;
} tsmObjName;

/*-------------------------------------------------------------------------+
 |  Typdefinition f. Informationen zu 'Sicherung löschen' in dsmDeleteObj() |
 +-------------------------------------------------------------------------*/
typedef struct tsmDelBack
{
   dsUint16_t         stVersion;              /* Strukturversion                */
   tsmObjName       *objNameP ;                   /* Objektname             */
   dsUint32_t       copyGroup ;                   /* Kopiengruppe           */
} tsmDelBack ;

#define  tsmDelBackVersion    1

/*-------------------------------------------------------------------------+
 |  Typdefinition für Infos zu 'Archivierung löschen' in dsmDeleteObj()     |
 +-------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion                */
   dsStruct64_t     objId ;                       /* Objekt-ID              */
} tsmDelArch ;

#define  tsmDelArchVersion  1

/*-------------------------------------------------------------------------+
 |  Typdefinition für Infos zu 'Sicherungs-ID löschen' in dsmDeleteObj()    |
 +-------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion                */
   dsStruct64_t     objId ;                       /* Objekt-ID              */
} tsmDelBackID;

#define  tsmDelBackIDVersion  1


/*-------------------------------------------------------------------------+
 |  Typdefinition für Löschinformationen in dsmDeleteObj()                  |
 +-------------------------------------------------------------------------*/
typedef union
{
   tsmDelBack   backInfo ;
   tsmDelArch   archInfo ;
   tsmDelBackID backIDInfo;
} tsmDelInfo ;

/*-------------------------------------------------------------------------+
 |  Typdefinition für Parameter Object Attribute in dsmSendObj()            |
 +-------------------------------------------------------------------------*/
typedef struct tsmObjAttr
{
   dsUint16_t   stVersion;               /* Strukturversion                   */
   dsChar_t     owner[DSM_MAX_OWNER_LENGTH + 1];      /* Objekteigner         */
   dsStruct64_t sizeEstimate;            /* Größenschätzung des Objekts in Byte */
   dsmBool_t    objCompressed;           /* Ist Objekt bereits komprimiert? */
   dsUint16_t   objInfoLength;           /* Länge der objektabhängigen Information */
   char         *objInfo;                /* Bytepuffer für objektabhängige Informationen */
   dsChar_t     *mcNameP;                /* Verwaltungsklassenname für Überschreibung */
   tsmOwType    reserved1;               /* für zukünftige Verwendung         */
   tsmOwType    reserved2;               /* für zukünftige Verwendung         */
   dsmBool_t    disableDeduplication;    /* 'Keine Deduplizierung' für dieses Objekt erzwingen */
   dsmBool_t    useExtObjInfo;                /* Erw. Objektinfo. bis zu 1536 verwenden */
} tsmObjAttr;
```

```
#define tsmObjAttrVersion 5

/*-------------------------------------------------------------------------+
 | Typdefinition für zurückgegebenen mcBindKey in dsmBindMC()               |
 +-------------------------------------------------------------------------*/
typedef struct tsmMcBindKey
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t    mcName[DSM_MAX_MC_NAME_LENGTH + 1];
   /* Name der an das Objekt gebundenen Verwaltungsklasse. */
   dsmBool_t   backup_cg_exists;                          /* Wahr/Falsch */
   dsmBool_t   archive_cg_exists;                         /* Wahr/Falsch */
   dsChar_t    backup_copy_dest[DSM_MAX_CG_DEST_LENGTH + 1];
   /* Zielname für Sicherungskopie */
   dsChar_t    archive_copy_dest[DSM_MAX_CG_DEST_LENGTH + 1];
   /* Zielname für Archivierungskopie */
} tsmMcBindKey;

#define tsmMcBindKeyVersion  1


/*-------------------------------------------------------------------------+
 |  Typdefinition für queryBuffer für Verwaltungsklasse in dsmBeginQuery()  |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryMCData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t     *mcName;                        /* Verwaltungsklassenname */
   /* einzelner Name für 1 Klasse oder leere Zeichenfolge, um alle abzurufen */
   dsmBool_t    mcDetail;                       /* Details erwünscht oder nicht? */
} tsmQryMCData;

#define tsmQryMCDataVersion  1


/*-------------------------------------------------------------------------+
 |  Typdefinition f. Archivierungskopiengruppendetails in Antwort auf Verwaltungsklassenabfrage|
 +-------------------------------------------------------------------------*/
typedef struct tsmArchDetailCG
{
   dsChar_t     cgName[DSM_MAX_CG_NAME_LENGTH + 1];     /* Kopiengruppenname */
   dsUint16_t   frequency;                      /* Häufigkeit von Kopien (Archivierungen) */
   dsUint16_t   retainVers;                                /* Version aufbewahren */
   dsUint8_t    copySer;       /* Hinweise zur Kopiennummerierung siehe Definitionen */
   dsUint8_t    copyMode;         /* Hinweise zu Kopiermoduswerten siehe Definitionen oben */
   dsChar_t     destName[DSM_MAX_CG_DEST_LENGTH + 1];    /* Zielname für Kopie */
   dsmBool_t    bLanFreeDest;            /* Ziel hat LAN-unabhängigen Pfad?    */
   dsmBool_t    reserved;                /* Derzeit nicht verwendet          */
   dsUint8_t    retainInit;              /* Mögliche Werte siehe dsmapitd.h  */
   dsUint16_t   retainMin;               /* wenn retInit auf EVENT gesetzt: Anzahl Tage */
   dsmBool_t    bDeduplicate;            /* Am Ziel ist Deduplizierung aktiviert    */
}tsmArchDetailCG;

/*-------------------------------------------------------------------------+
 |  Typdefinition f. Sicherungskopiengruppendetails in Antwort auf Verwaltungsklassenabfrage   |
 +-------------------------------------------------------------------------*/
typedef struct tsmBackupDetailCG
{
   dsChar_t     cgName[DSM_MAX_CG_NAME_LENGTH + 1];     /* Kopiengruppenname */
   dsUint16_t   frequency;                              /* Häufigkeit der Sicherung */
   dsUint16_t   verDataExst;                         /* Versionen bestehender Daten */
   dsUint16_t   verDataDltd;                        /* Versionen gelöschter Daten */
   dsUint16_t   retXtraVers;                        /* Extraversionen aufbewahren */
   dsUint16_t   retOnlyVers;                        /* Einzige Version aufbewahren */
   dsUint8_t    copySer;       /* Hinweise zur Kopiennummerierung siehe Definitionen */
   dsUint8_t    copyMode;         /* Hinweise zu Kopiermoduswerten siehe Definitionen oben */
   dsChar_t     destName[DSM_MAX_CG_DEST_LENGTH + 1];    /* Zielname für Kopie */
   dsmBool_t    bLanFreeDest;            /* Ziel hat LAN-unabhängigen Pfad?    */
   dsmBool_t    reserved;                /* Derzeit nicht verwendet          */
   dsmBool_t    bDeduplicate;            /* Am Ziel ist Deduplizierung aktiviert    */
}tsmBackupDetailCG;


/*-------------------------------------------------------------------------+
 |  Typdefinition für Detailantwort zu Verwaltungsklassenabfrage in dsmGetNextQObj()           |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryRespMCDetailData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t        mcName[DSM_MAX_MC_NAME_LENGTH + 1];        /* Verwaltungsklassenname */
   dsChar_t        mcDesc[DSM_MAX_MC_DESCR_LENGTH + 1]; /* Verwaltungsklassenbeschreibung */
```

```
   archDetailCG    archDet;                /* Archivierungskopiengruppendetail */
   backupDetailCG  backupDet;               /* Sicherungskopiengruppendetail */
} tsmQryRespMCDetailData;

#define tsmQryRespMCDetailDataVersion  4

/*-------------------------------------------------------------------------+
 | Typdefinition f. Antwort mit Zusammenfass. zur Verwaltungsklassenabfrage in dsmGetNextQObj()|
 +-------------------------------------------------------------------------*/
typedef struct tsmQryRespMCData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t        mcName[DSM_MAX_MC_NAME_LENGTH + 1];        /* Verwaltungsklassenname */
   dsChar_t     mcDesc[DSM_MAX_MC_DESCR_LENGTH + 1];    /* Verwaltungsklassenbeschreibung */
}tsmQryRespMCData;

#define tsmQryRespMCDataVersion  1

/*-------------------------------------------------------------------------+
 |  Typdefinition für queryBuffer für Archivierung in tsmBeginQuery()       |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryArchiveData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   tsmObjName   *objName;                    /* Vollständiger DSM-Name des Objekts */
   dsChar_t     *owner;                                 /* Eignername */
   /* Hinweise zu maximalen Datumsgrenzen siehe Definitionen oben */
   dsmDate      insDateLowerBound;      /* unterer Grenzwert für Archivierungseinfügedatum */
   dsmDate      insDateUpperBound;      /* oberer Grenzwert für Archivierungseinfügedatum */
   dsmDate      expDateLowerBound;      /* unterer Grenzwert für Verfallsdatum */
   dsmDate      expDateUpperBound;      /* oberer Grenzwert für Verfallsdatum */
   dsChar_t     *descr;                 /* Archivierungsbeschreibung */
} tsmQryArchiveData;

#define tsmQryArchiveDataVersion  1

/*-------------------------------------------------------------------------+
| Typdefinition für Antwort auf Archivierungsabfrage in dsmGetNextQObj()   |
+-------------------------------------------------------------------------*/
typedef struct tsmQryRespArchiveData
{
    dsUint16_t         stVersion;              /* Strukturversion               */
    tsmObjName      objName;                            /* Qualifikationsmerkmal für Dateibereichsname */
    dsUint32_t      copyGroup;                          /* Kopiengruppenzahl */
    dsChar_t        mcName[DSM_MAX_MC_NAME_LENGTH + 1];  /* Verwaltungsklassenname */
    dsChar_t        owner[DSM_MAX_OWNER_LENGTH + 1];     /* Eignername */
    dsStruct64_t    objId;                              /* Eindeutige Kopien-ID */
    dsStruct64_t    reserved;                       /* Abwärtskompatibilität */
    dsUint8_t       mediaClass;                         /* Datenträgerzugriffsklasse */
    dsmDate         insDate;                            /* Archivierungseinfügedatum */
    dsmDate         expDate;                       /* Verfallsdatum für Objekt */
    dsChar_t        descr[DSM_MAX_DESCR_LENGTH + 1];     /* Archivierungsbeschreibung */
    dsUint16_t  objInfolen;                           /* Länge der objektabhängigen Informationen */
    dsUint8_t       reservedObjInfo[DSM_MAX_OBJINFO_LENGTH];  /* objektabhängige Informationen */
    dsUint160_t     restoreOrderExt;                    /* Zurückschreibungsreihenfolge */
    dsStruct64_t    sizeEstimate;              /* vom Benutzer gespeicherte Größenschätzung */
    dsUint8_t       compressType;                       /* Komprimierungsflag */
    dsUint8_t       retentionInitiated;                 /* Objekt wartet bei Aufbewahrungsereignis */
    dsUint8_t       objHeld;                            /* Objekt angehalten; Werte siehe dsmapitd.h */
    dsUint8_t       encryptionType;          /* Verschlüsselungstyp */
    dsmBool_t       clientDeduplicated;      /* Objekt wird von API dedupliziert */
    dsUint8_t       objInfo[DSM_MAX_EXT_OBJINFO_LENGTH];  /* objektabhängige Informationen */
    dsChar_t        compressAlg[DSM_MAX_COMPRESSTYPE_LENGTH + 1];  /* Komprimierungsalgorithmusname */
} tsmQryRespArchiveData;

#define tsmQryRespArchiveDataVersion  7

/*-------------------------------------------------------------------------+
 |  Typdefinition für Archivierungsparameter sendBuff in dsmSendObj()       |
 +-------------------------------------------------------------------------*/
typedef struct tsmSndArchiveData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t     *descr;                   /* Archivierungsbeschreibung */
} tsmSndArchiveData;

#define tsmSndArchiveDataVersion  1

/*-------------------------------------------------------------------------+
 |  Typdefinition für queryBuffer für Sicherung in dsmBeginQuery()          |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryBackupData
```

```
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   tsmObjName  *objName;          /* Vollständiger DSM-Name des Objekts */
   dsChar_t    *owner;            /* Eignername */
   dsUint8_t   objState;          /* Objektstatusselektor */
   dsmDate     pitDate;           /* Datumswert für zeitpunktgesteuerte Zurückschreibung */
   /* Hinweise zu möglichen Werten siehe Definitionen oben */
    dsUint32_t  reserved1;
    dsUint32_t  reserved2;
} tsmQryBackupData;

#define tsmQryBackupDataVersion  3

/*-------------------------------------------------------------------------+
 | Typdefinition für Antwort auf Sicherungsabfrage in dsmGetNextQObj()     |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryRespBackupData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   tsmObjName      objName;                      /* Vollständiger DSM-Name des Objekts */
   dsUint32_t      copyGroup;                         /* Kopiengruppenzahl */
   dsChar_t        mcName[DSM_MAX_MC_NAME_LENGTH + 1];  /* Verwaltungsklassenname */
   dsChar_t        owner[DSM_MAX_OWNER_LENGTH + 1];     /* Eignername */
   dsStruct64_t    objId;                             /* Eindeutige Objekt-ID */
   dsStruct64_t    reserved;                       /* Abwärtskompatibilität */
   dsUint8_t       mediaClass;                        /* Datenträgerzugriffsklasse */
   dsUint8_t       objState;                           /* Objektstatus, aktiv usw. */
   dsmDate     insDate;                          /* Sicherungseinfügedatum */
   dsmDate         expDate;                    /* Verfallsdatum für Objekt */
   dsUint16_t  objInfolen;                        /* Länge der objektabhängigen Informationen */
   dsUint8_t       reservedObjInfo[DSM_MAX_OBJINFO_LENGTH];  /* objektabhängige Informationen */
   dsUint160_t     restoreOrderExt;                   /* Zurückschreibungsreihenfolge */
   dsStruct64_t    sizeEstimate;                      /* vom Benutzer gespeicherte Größenschätzung */
   dsStruct64_t    baseObjId;
   dsUint16_t      baseObjInfolen;                    /* Länge der basisobjektabhängigen Informationen */
   dsUint8_t       baseObjInfo[DSM_MAX_OBJINFO_LENGTH]; /* basisobjektabhängige Informationen */
   dsUint160_t     baseRestoreOrder;                  /* Zurückschreibungsreihenfolge */
   dsUint32_t      fsID;
   dsUint8_t       compressType;
   dsmBool_t       isGroupLeader;
   dsmBool_t       isOpenGroup;
   dsUint8_t       reserved1;              /* für zukünftige Verwendung */
   dsmBool_t       reserved2;              /* für zukünftige Verwendung */
   dsUint16_t      reserved3;              /* für zukünftige Verwendung */
   reservedInfo_t  *reserved4;             /* für zukünftige Verwendung */
   dsUint8_t       encryptionType;         /* Verschlüsselungstyp */
   dsmBool_t       clientDeduplicated;     /* Objekt wird von API dedupliziert */
   dsUint8_t       objInfo[DSM_MAX_EXT_OBJINFO_LENGTH];  /* objektabhängige Informationen */
   dsChar_t        compressAlg[DSM_MAX_COMPRESSTYPE_LENGTH + 1];  /* Komprimierungsalgorithmusname */
} tsmQryRespBackupData;

#define tsmQryRespBackupDataVersion  8
/*-------------------------------------------------------------------------+
 |  Typdefinition für queryBuffer für aktive Sicherung in dsmBeginQuery()  |
 |
 |  Hinweise: Für die Abfrage der aktiven Sicherung müssen nur die Felder  |
 |            fs (Dateibereich) und objType gesetzt werden. objType kann nur|
 |            auf DSM_OBJ_FILE oder DSM_OBJ_DIRECTORY gesetzt werden.      |
 |            Für DSM_OBJ_ANY_TYPE wird keine Übereinstimmung in der Abfrage|
 |            gefunden.                                                    |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryABackupData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   tsmObjName      *objName;                    /* Nur fs und objType werden verwendet */
} tsmQryABackupData;

#define tsmQryABackupDataVersion  1

/*-------------------------------------------------------------------------+
 | Typdefinition für Antwort auf Abfrage der aktiven Sicherung in dsmGetNextQObj()          |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryARespBackupData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   tsmObjName  objName;                      /* Vollständiger DSM-Name des Objekts */
   dsUint32_t  copyGroup;                         /* Kopiengruppenzahl */
   dsChar_t    mcName[DSM_MAX_MC_NAME_LENGTH + 1];  /* Verwaltungsklassenname */
   dsChar_t        owner[DSM_MAX_OWNER_LENGTH + 1];     /* Eignername */
   dsmDate     insDate;                          /* Sicherungseinfügedatum */
   dsUint16_t  objInfolen;                        /* Länge der objektabhängigen Informationen */
   dsUint8_t       reservedObjInfo[DSM_MAX_OBJINFO_LENGTH];  /* objektabhängige Informationen */
```

```
   dsUint8_t       objInfo[DSM_MAX_EXT_OBJINFO_LENGTH];  /* objektabhängige Informationen */
} tsmQryARespBackupData;

#define tsmQryARespBackupDataVersion  2

/*-------------------------------------------------------------------------+
 |  Typdefinition für queryBuffer für Sicherung in dsmBeginQuery()         |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryBackupGroups
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint8_t    groupType;
   dsChar_t     *fsName;
   dsChar_t     *owner;
   dsStruct64_t groupLeaderObjId;
   dsUint8_t    objType;
   dsUint32_t   reserved1;
   dsUint32_t   reserverd2;
   dsmBool_t    noRestoreOrder;
   dsmBool_t    noGroupInfo;
   dsChar_t     *hl;
} tsmQryBackupGroups;

#define tsmQryBackupGroupsVersion 4

/*-------------------------------------------------------------------------+
 |  Typdefinition für queryBuffer für Proxy-Knoten in tsmBeginQuery()      |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryProxyNodeData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t    *targetNodeName;            /* Zielknotenname  */
}tsmQryProxyNodeData;

#define tsmQryProxyNodeDataVersion  1

/*-------------------------------------------------------------------------+
 | Typdefinition für den in tsmGetNextQObj() verwendeten Parameter qryRespProxyNodeData       |
 +-------------------------------------------------------------------------*/

typedef struct tsmQryRespProxyNodeData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t          targetNodeName[DSM_MAX_ID_LENGTH+1];  /* Zielknotenname  */
   dsChar_t          peerNodeName[DSM_MAX_ID_LENGTH+1];    /* Peerknotenname  */
   dsChar_t          hlAddress[DSM_MAX_ID_LENGTH+1];       /* übergeordnete Peeradresse */
   dsChar_t          llAddress[DSM_MAX_ID_LENGTH+1];       /* untergeordnete Peeradresse */
}tsmQryRespProxyNodeData;

#define tsmQryRespProxyNodeDataVersion  1

/*-------------------------------------------------------------------------+
 |  Typdefinition für WINNT- und OS/2-Dateibereichsattribute               |
 +-------------------------------------------------------------------------*/
typedef struct tsmDosFSAttrib
{
   osChar_t     driveLetter ;          /* Laufwerkbuchstabe für Dateibereich */
   dsUint16_t   fsInfoLength;          /* für Dateibereichsinformationen verwendete Länge */
   osChar_t     fsInfo[DSM_MAX_FSINFO_LENGTH]; /* vom Aufrufenden bestimmte Daten */
} tsmDosFSAttrib ;

/*-------------------------------------------------------------------------+
 |  Typdefinition für UNIX-Dateibereichsattribute                          |
 +-------------------------------------------------------------------------*/
typedef struct tsmUnixFSAttrib
{
   dsUint16_t   fsInfoLength;          /* für Dateibereichsinformationen verwendete Länge */
   osChar_t     fsInfo[DSM_MAX_FSINFO_LENGTH]; /* vom Aufrufenden bestimmte Daten */
} tsmUnixFSAttrib ;

/*-------------------------------------------------------------------------+
 |  Typdefinition für NetWare-Dateibereichsattribute                       |
 +-------------------------------------------------------------------------*/
typedef tsmUnixFSAttrib tsmNetwareFSAttrib;

/*-------------------------------------------------------------------------+
 |  Typdefinition für Dateibereichsattribute in allen Dateibereichsaufrufen |
 +-------------------------------------------------------------------------*/
typedef union
{
   tsmNetwareFSAttrib  netwareFSAttr;
   tsmUnixFSAttrib     unixFSAttr ;
```

```
   tsmDosFSAttrib      dosFSAttr ;
} tsmFSAttr ;

/*-------------------------------------------------------------------------+
 |  Typdefinition für Parameter fsUpd in dsmUpdateFS()                     |
 +-------------------------------------------------------------------------*/
typedef struct   tsmFSUpd
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t        *fsType ;              /* Dateibereichstyp              */
   dsStruct64_t    occupancy ;            /* Belegungsschätzung            */
   dsStruct64_t    capacity  ;            /* Kapazitätsschätzung           */
   tsmFSAttr       fsAttr ;                    /* plattformspezifische Attribute */
} tsmFSUpd ;

#define tsmFSUpdVersion  1

/*-------------------------------------------------------------------------+
 |  Typdefinition für queryBuffer für Dateibereich in dsmBeginQuery()      |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryFSData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t    *fsName;                  /* Dateibereichsname */
} tsmQryFSData;

#define tsmQryFSDataVersion  1

/*-------------------------------------------------------------------------+
 | Typdefinition für Antwort auf Dateibereichsabfrage in dsmGetNextQObj()  |
 +-------------------------------------------------------------------------*/
typedef struct tsmQryRespFSData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t       fsName[DSM_MAX_FSNAME_LENGTH + 1];     /* Dateibereichsname */
   dsChar_t       fsType[DSM_MAX_FSTYPE_LENGTH + 1] ;    /* Dateibereichstyp  */
   dsStruct64_t    occupancy;                      /* Belegungsschätzung in Byte */
   dsStruct64_t   capacity;                        /* Kapazitätsschätzung in Byte */
   tsmFSAttr       fsAttr ;                       /* plattformspezifische Attribute */
   dsmDate        backStartDate;                  /* Datum für Sicherungsbeginn */
   dsmDate        backCompleteDate;        /* Datum für Sicherungsende   */
    dsmDate        reserved1;                      /* Für zukünftige Verwendung  */
   dsmBool_t      bIsUnicode;
   dsUint32_t     fsID;
   dsmDate        lastReplStartDate;        /* Startzeitpunkt der letzten Replikation     */
   dsmDate        lastReplCmpltDate;        /* Endzeitpunkt der letzten Replikation       */
                                            /*   (eventuell trat ein Fehler auf,          */
                                            /*    aber sie wurde dennoch beendet)         */
   dsmDate        lastBackOpDateFromServer; /* Die letzte Speicherungszeitmarke, die der  */
                                            /* Client auf dem Server gespeichert hat      */
   dsmDate        lastArchOpDateFromServer; /* Die letzte Speicherungszeitmarke, die der  */
                                            /* Client auf dem Server gespeichert hat      */
   dsmDate        lastSpMgOpDateFromServer; /* Die letzte Speicherungszeitmarke, die der  */
                                            /* Client auf dem Server gespeichert hat      */
   dsmDate        lastBackOpDateFromLocal;  /* Die letzte Speicherungszeitmarke, die der  */
                                            /*    Client lokal gespeichert hat            */
   dsmDate        lastArchOpDateFromLocal;  /* Die letzte Speicherungszeitmarke, die der  */
                                            /*    Client lokal gespeichert hat            */
   dsmDate        lastSpMgOpDateFromLocal;  /* Die letzte Speicherungszeitmarke, die der  */
                                            /*    Client lokal gespeichert hat            */
   dsInt32_t      failOverWriteDelay;       /* Minuten, die der Client vor dem Speichern  */
                                            /* auf diesem Rpl.server warten muss; Sonder- */
                                            /* codes: NO_ACCESS(-1), ACCESS_RDONLY (-2)   */
} tsmQryRespFSData;

#define tsmQryRespFSDataVersion 5

/*-------------------------------------------------------------------------+
 |  Typdefinition für Parameter regFilespace in dsmRegisterFS()            |
 +-------------------------------------------------------------------------*/
typedef struct tsmRegFSData
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t        *fsName;                       /* Dateibereichsname */
   dsChar_t        *fsType;                       /* Dateibereichstyp */
   dsStruct64_t    occupancy;                     /* Belegungsschätzung in Byte */
   dsStruct64_t    capacity;                      /* Kapazitätsschätzung in Byte */
   tsmFSAttr       fsAttr ;                       /* plattformspezifische Attribute */
} tsmRegFSData;

#define tsmRegFSDataVersion  1
```

```
/*------------------------------------------------------------------------+
 |  Typdefinition für Antwort mit Sitzungsdaten in dsmQuerySessionInfo()    |
 +------------------------------------------------------------------------*/
typedef struct
{
   dsUint16_t   stVersion;               /* Strukturversion                  */
   /*---------------------------------------------------------------------*/
   /*           Serverinformationen                                       */
   /*---------------------------------------------------------------------*/
   dsChar_t       serverHost[DSM_MAX_SERVERNAME_LENGTH+1];
       /* Netzhostname des DSM-Servers */
   dsUint16_t     serverPort;            /* Serverkommunikationsport auf Host */
   dsmDate        serverDate;            /* Datum/Zeit des Servers */
   dsChar_t       serverType[DSM_MAX_SERVERTYPE_LENGTH+1];
        /* Ausführungsplattform des Servers */
   dsUint16_t     serverVer;             /* Versionsnummer des Servers       */
   dsUint16_t     serverRel;             /* Releasenummer des Servers        */
   dsUint16_t     serverLev;             /* Stufennummer des Servers         */
   dsUint16_t         serverSubLev;  /* Unterstufennummer des Servers    */
   /*---------------------------------------------------------------------*/
   /*           Clientstandardwerte                                       */
n
   /*---------------------------------------------------------------------*/
   dsChar_t       nodeType[DSM_MAX_PLATFORM_LENGTH+1]; /* Knoten-/Anwendungstyp */
   dsChar_t       fsdelim;               /* Dateibereichsbegrenzer             */
   dsChar_t       hldelim;               /* Begrenzer zwischen oberer u. unterere Ebene */
   dsUint8_t      compression;           /* Komprimierungsflag */
   dsUint8_t      archDel;               /* Berechtigung zum Löschen des Archivs */
   dsUint8_t      backDel;               /* Berechtigung zum Löschen der Sicherung */
   dsUint32_t     maxBytesPerTxn;        /* für zukünftige Verwendung */
   dsUint16_t     maxObjPerTxn;          /* Max. Anzahl Objekte in einer Transaktion */
   /*---------------------------------------------------------------------*/
   /*           Sitzungsdaten                                             */
   /*---------------------------------------------------------------------*/
   dsChar_t       id[DSM_MAX_ID_LENGTH+1];    /* Knotenname der Anmelde-ID */
   dsChar_t       owner[DSM_MAX_OWNER_LENGTH+1]; /* Anmeldeeigner */
   /*   (für Mehrbenutzerplattformen   */
   dsChar_t       confFile[DSM_PATH_MAX + DSM_NAME_MAX +1];
   /* Länge ist plattformabhängig       */
   /* dsInit-Name der Anwend.-Konfig.-Datei */
   dsUint8_t  opNoTrace;             /* Option dsInit - NoTrace = 1      */
   /*---------------------------------------------------------------------*/
   /*           Maßnahmendaten                                            */
   /*---------------------------------------------------------------------*/
   dsChar_t       domainName[DSM_MAX_DOMAIN_LENGTH+1]; /* Domänenname */
   dsChar_t       policySetName[DSM_MAX_PS_NAME_LENGTH+1];
   /* Name der aktiven Maßnahmengruppe */
   dsmDate        polActDate;         /* Aktivierungsdatum der Maßnahmengruppe */
   dsChar_t       dfltMCName[DSM_MAX_MC_NAME_LENGTH+1]; /* Standardverwaltungsklasse */
   dsUint16_t     gpBackRetn;            /* Karenzzeit f. Aufbewahrungszeitraum f. Sicherung */
   dsUint16_t     gpArchRetn;            /* Karenzzeit f. Aufbewahrungszeitraum f. Archivierung */
   dsChar_t       adsmServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* ADSM-Servername */
  dsmBool_t      archiveRetentionProtection; /* Aufbewahrungsschutz durch Server ist aktiviert*/
   dsUint64_t     maxBytesPerTxn_64;          /* für zukünftige Verwendung     */
   dsmBool_t      lanFreeEnabled;           /* Option 'LAN-unabhängig' ist gesetzt */
   dsmDedupType   dedupType;                /* server oder clientOrServer       */
   dsChar_t       accessNode[DSM_MAX_ID_LENGTH+1];    /* als Knotenname    */

   /*---------------------------------------------------------------------*/
   /*           Replikations- und Übernahmeinformationen                  */
   /*---------------------------------------------------------------------*/
   dsmFailOvrCfgType failOverCfgType; /* Status der Übernahme */
   dsChar_t           replServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* Replikationsservername           */
   dsChar_t           homeServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* Home-Servername                  */
   dsChar_t        replServerHost[DSM_MAX_SERVERNAME_LENGTH+1]; /* Netzhostname des DSM-Servers      */
   dsInt32_t      replServerPort;                          /* Serverkommunikationsport auf Host */

} tsmApiSessInfo;

#define tsmApiSessInfoVersion  6

/*------------------------------------------------------------------------+
 | Typdefinition für Antwort auf Abfrageoptionen in dsmQueryCliOptions()    |
 |      und dsmQuerySessOptions()                                           |
 +------------------------------------------------------------------------*/

typedef struct
{
   dsUint16_t  stVersion;
   dsChar_t    dsmiDir[DSM_PATH_MAX + DSM_NAME_MAX +1];
   dsChar_t        dsmiConfig[DSM_PATH_MAX + DSM_NAME_MAX +1];
   dsChar_t    serverName[DSM_MAX_SERVERNAME_LENGTH+1];
```

```
   dsInt16_t   commMethod;
   dsChar_t    serverAddress[DSM_MAX_SERVER_ADDRESS];
   dsChar_t    nodeName[DSM_MAX_NODE_LENGTH+1];
   dsmBool_t   compression;
   dsmBool_t   compressalways;
   dsmBool_t   passwordAccess;
}tsmOptStruct ;

#define tsmOptStructVersion  1

/*------------------------------------------------------------------------+
 | Typdefinition für den in dsmQueryAccess() verwendeten Parameter qryRespAccessData           |
 +------------------------------------------------------------------------*/

typedef struct
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t          node[DSM_MAX_ID_LENGTH+1];     /* Knotenname             */
   dsChar_t          owner[DSM_MAX_OWNER_LENGTH+1]; /* Eigner                 */
   tsmObjName        objName ;                      /* Objektname             */
   dsmAccessType     accessType;                    /* Archiv. oder Sicherung */
   dsUint32_t        ruleNumber ;                   /* Zugriffsregel-ID       */

}tsmQryRespAccessData;

#define tsmQryRespAccessDataVersion  1

/*------------------------------------------------------------------------+
 |  Typdefinition für Parameter envSetUp in dsmSetUp()                     |
 +------------------------------------------------------------------------*/
typedef struct tsmEnvSetUp
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsChar_t    dsmiDir[DSM_PATH_MAX + DSM_NAME_MAX +1];
   dsChar_t        dsmiConfig[DSM_PATH_MAX + DSM_NAME_MAX +1];
   dsChar_t        dsmiLog[DSM_PATH_MAX + DSM_NAME_MAX +1];
   char            **argv;  /* für Name von ausführbaren Dateien (argv[0]) */
   dsChar_t        logName[DSM_NAME_MAX +1];
   dsmBool_t       reserved1;         /* für zukünftige Verwendung */
   dsmBool_t       reserved2;               /* für zukünftige Verwendung */
} tsmEnvSetUp;

#define tsmEnvSetUpVersion  4

/*------------------------------------------------------------------------+
 |  Typdefinition für dsmInitExIn_t                                        |
 +------------------------------------------------------------------------*/
typedef struct tsmInitExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   tsmApiVersionEx    *apiVersionExP;
   dsChar_t           *clientNodeNameP;
   dsChar_t           *clientOwnerNameP;
   dsChar_t           *clientPasswordP;
   dsChar_t           *userNameP;
   dsChar_t           *userPasswordP;
   dsChar_t           *applicationTypeP;
   dsChar_t           *configfile;
   dsChar_t           *options;
   dsChar_t           dirDelimiter;
   dsmBool_t          useUnicode;
   dsmBool_t          bCrossPlatform;
   dsmBool_t          bService;
   dsmBool_t          bEncryptKeyEnabled;
   dsChar_t           *encryptionPasswordP;
   dsmBool_t          useTsmBuffers;
   dsUint8_t          numTsmBuffers;
   tsmAppVersion      appVersionP;
} tsmInitExIn_t;

#define tsmInitExInVersion 5

/*------------------------------------------------------------------------+
 |  Typdefinition für dsmInitExOut_t                                       |
 +------------------------------------------------------------------------*/
typedef struct tsmInitExOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsInt16_t          userNameAuthorities;
   dsInt16_t          infoRC;        /* Fehlercode, falls festgestellt */
   /* ADSM-Servername               */
   dsChar_t           adsmServerName[DSM_MAX_SERVERNAME_LENGTH+1];
```

```
   dsUint16_t     serverVer;              /* Versionsnummer des Servers       */
   dsUint16_t         serverRel;     /* Releasenummer des Servers        */
   dsUint16_t     serverLev;              /* Stufennummer des Servers         */
   dsUint16_t         serverSubLev;  /* Unterstufennummer des Servers    */
   dsmBool_t          bIsFailOverMode; /* wahr im Fall einer Übernahme   */
   dsChar_t           replServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* Replikationsservername            */
   dsChar_t           homeServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* Home-Servername                   */
} tsmInitExOut_t;

#define tsmInitExOutVersion 3

/*------------------------------------------------------------------------+
 |  Typdefinition für dsmLogExIn_t                                        |
 +------------------------------------------------------------------------*/
typedef struct tsmLogExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsmLogSeverity     severity;
   dsChar_t           appMsgID[8];
   dsmLogType         logType;    /* Protokolltyp: lokal, Server oder beides */
   dsChar_t           *message;   /* Text der zu protokollierenden Nachricht */
   dsChar_t           appName[DSM_MAX_PLATFORM_LENGTH];
   dsChar_t           osPlatform[DSM_MAX_PLATFORM_LENGTH];
   dsChar_t           appVersion[DSM_MAX_PLATFORM_LENGTH];

} tsmLogExIn_t;

#define tsmLogExInVersion 2

/*------------------------------------------------------------------------+
 |  Typdefinition für dsmlogExOut_t                                       |
 +------------------------------------------------------------------------*/
typedef struct tsmLogExOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
} tsmLogExOut_t;

#define tsmLogExOutVersion 1

/*------------------------------------------------------------------------+
 |  Typdefinition für dsmRenameIn_t                                       |
 +------------------------------------------------------------------------*/
typedef struct tsmRenameIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t       tsmHandle;                  /* Sitzungskennung */
   dsUint8_t        repository;                 /* Sicherung oder Archivierung */
   tsmObjName       *objNameP ;                 /* Objektname             */
   dsChar_t         newHl[DSM_MAX_HL_LENGTH + 1];  /* neuer übergeordneter Name */
   dsChar_t         newLl[DSM_MAX_LL_LENGTH + 1];  /* neuer untergeordneter Name */
   dsmBool_t        merge;                     /* mit vorhandenem Namen zusammenfassen */
   ObjID            objId;                     /* Objekt-ID für Archivierung */
} tsmRenameIn_t;

#define tsmRenameInVersion 1

/*------------------------------------------------------------------------+
 |  Typdefinition für dsmRenameOut_t                                      |
 +------------------------------------------------------------------------*/
typedef struct tsmRenameOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
} tsmRenameOut_t;

#define tsmRenameOutVersion 1

/*------------------------------------------------------------------------+
 |  Typdefinition für tsmEndSendObjExIn_t                                 |
 +------------------------------------------------------------------------*/
typedef struct tsmEndSendObjExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t       tsmHandle;                  /* Sitzungskennung */
} tsmEndSendObjExIn_t;

#define tsmEndSendObjExInVersion 1

/*------------------------------------------------------------------------+
 |  Typdefinition für dsmEndSendObjExOut_t                                |
 +------------------------------------------------------------------------*/
typedef struct tsmEndSendObjExOut_t
{
```

```
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsStruct64_t       totalBytesSent;      /* Gesamtsumme aus Anwendung gelesener Byte */
   dsmBool_t          objCompressed;       /* mit Objektkomprimierung */
   dsStruct64_t       totalCompressSize;   /* Gesamtgröße nach Komprimierung */
   dsStruct64_t       totalLFBytesSent;    /* Gesamtanzahl LAN-unabhängig gesendeter Byte */
   dsUint8_t          encryptionType;      /* verwendeter Verschlüsselungstyp */
   dsmBool_t          objDeduplicated;     /* Objektverarbeitung für verteilte Deduplizierung */
   dsStruct64_t       totalDedupSize;      /* Gesamtgröße nach Deduplizierung */
}tsmEndSendObjExOut_t;

#define tsmEndSendObjExOutVersion 3

/*------------------------------------------------------------------------+
 |  Typdefinition für tsmGroupHandlerIn_t                                 |
 +------------------------------------------------------------------------*/
typedef struct tsmGroupHandlerIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t       tsmHandle;                    /* Sitzungskennung */
   dsUint8_t       groupType;        /* Gruppentyp         */
   dsUint8_t        actionType;       /* Gruppenoperationstyp                  */
   dsUint8_t       memberType;       /* Mitgliedstyp: Leiter oder Mitglied */
   dsStruct64_t     leaderObjId;      /* OBJID des Gruppenleiters              */
   dsChar_t         *uniqueGroupTagP; /* Eindeutige Gruppen-ID                 */
   tsmObjName       *objNameP ;       /* Objektname des Gruppenleiters         */
   dsmGetList      memberObjList;    /* Liste der zu enfernenden bzw. zuzuordnenden Objekte */
} tsmGroupHandlerIn_t;

#define tsmGroupHandlerInVersion 1

/*------------------------------------------------------------------------+
 |  Typdefinition für tsmGroupHandlerExOut_t                              |
 +------------------------------------------------------------------------*/
typedef struct tsmGroupHandlerOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
} tsmGroupHandlerOut_t;

#define tsmGroupHandlerOutVersion 1

/*------------------------------------------------------------------------+
 |  Typdefinition für tsmEndTxnExIn_t                                     |
 +------------------------------------------------------------------------*/
typedef struct tsmEndTxnExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t       tsmHandle;                    /* Sitzungskennung */
   dsUint8_t        vote;
} tsmEndTxnExIn_t;

#define tsmEndTxnExInVersion 1

/*------------------------------------------------------------------------+
 |  Typdefinition für tsmEndTxnExOut_t                                    |
 +------------------------------------------------------------------------*/
typedef struct tsmEndTxnExOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint16_t         reason;                 /* Ursachencode                  */
   dsStruct64_t       groupLeaderObjId;       /* Gruppenleiterobjekt-ID (für    */
   /* DSM_ACTION_OPEN zurückgegeben) */
    dsUint8_t          reserved1;             /* für zukünftige Verwendung      */
    dsUint16_t         reserved2;             /* für zukünftige Verwendung      */
} tsmEndTxnExOut_t;

#define tsmEndTxnExOutVersion 1

/*------------------------------------------------------------------------+
 |  Typdefinition für tsmEndGetDataExIn_t                                 |
 +------------------------------------------------------------------------*/
typedef struct tsmEndGetDataExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t       tsmHandle;                    /* Sitzungskennung */
}tsmEndGetDataExIn_t;

#define tsmEndGetDataExInVersion 1

/*------------------------------------------------------------------------+
 |  Typdefinition für tsmEndGetDataExOut_t                                |
 +------------------------------------------------------------------------*/
typedef struct tsmEndGetDataExOut_t
```

```
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint16_t         reason;                 /* Ursachencode                  */
   dsStruct64_t   totalLFBytesRecv;  /* Gesamtzahl LAN-unabhängig empfangener Byte */
}tsmEndGetDataExOut_t;

#define tsmEndGetDataExOutVersion 1

/*-------------------------------------------------------------------------+
 |  Typdefinition für tsmRetentionEvent()                                  |
 +-------------------------------------------------------------------------*/
typedef struct tsmRetentionEventIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t         tsmHandle;                   /* Sitzungskennung  */
   dsmEventType_t     eventType;                   /* Ereignistyp      */
   dsmObjList_t       objList;                     /* Objekt-ID        */
}tsmRetentionEventIn_t;

#define tsmRetentionEventInVersion 1

/*-------------------------------------------------------------------------+
 |  Typdefinition für tsmRetentionEvent()                                  |
 +-------------------------------------------------------------------------*/
typedef struct tsmRetentionEventOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
}tsmRetentionEventOut_t;

#define tsmRetentionEventOutVersion 1

/*-------------------------------------------------------------------------+
 |  Typdefinition für tsmUpdateObjExIn_t                                   |
 +-------------------------------------------------------------------------*/
typedef struct tsmUpdateObjExIn_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
   dsUint32_t         tsmHandle;                   /* Sitzungskennung  */
   tsmSendType     sendType;            /* Sendetyp(Sich./Archiv.) */
   dsChar_t        *descrP;             /* Archivierungsbeschreibung */
   tsmObjName      *objNameP;           /* Objektname          */
   tsmObjAttr      *objAttrPtr;         /* Attribut            */
   dsUint32_t      objUpdAct;           /* Aktualisierungsaktion */
   ObjID           archObjId;           /* Objekt-ID für Archivierung */
}tsmUpdateObjExIn_t;

#define tsmUpdateObjExInVersion 1

/*-------------------------------------------------------------------------+
 |  Typdefinition für tsmUpdateObjExOut_t                                  |
 +-------------------------------------------------------------------------*/
typedef struct tsmUpdateObjExOut_t
{
   dsUint16_t         stVersion;              /* Strukturversion               */
}tsmUpdateObjExOut_t;

#define tsmUpdateObjExOutVersion 1

#if _OPSYS_TYPE == DS_WINNT
#pragma pack()
#endif


#ifdef _MAC
#pragma options align = reset
#endif
#endif /* _H_TSMAPITD */


/*************************************************************************
* Tivoli Storage Manager                                                 *
* API-Clientkomponente                                                   *
*                                                                        *
* (C) Copyright IBM Corporation 1993, 2010                               *
*************************************************************************/

/*************************************************************************
* Header File Name: dsmapips.h
*
* Umgebung:         ******************************************
*                   ** Dies ist eine plattformspezifische      **
*                   ** Quellendatei für Windows NT             **
```

```
*
*                    ********************************************
*
* Anm. zum Entwurf: Diese Datei enthält plattformabhängige Definitionen
*
* Beschreib. Name:  Definitionen für Tivoli Storage Manager-Typdefinitionen
*                   und LINKAGE
*-----------------------------------------------------------------------*/

#ifndef _H_DSMAPIPS
#define _H_DSMAPIPS


#ifndef _WIN64
#pragma pack(1)
#endif

/*<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>*/
/*                     T Y P D E F I N I T I O N E N                    */
/*<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>*/

/* Neue Datei typedef für Version 3   */


#if !defined(DSMAPILIB) || defined (XOPEN_BUILD)

/* Unterstützung für Linkage */
#include <windows.h>
#define DSMLINKAGE WINAPI


#define DS_WINNT    22
#define _OPSYS_TYPE DS_WINNT

   typedef signed   char  dsInt8_t;
   typedef unsigned char  dsUint8_t;
   typedef signed   short dsInt16_t;
   typedef unsigned short dsUint16_t;
   typedef signed   long  dsInt32_t;
   typedef unsigned long  dsUint32_t;

/*=== Zeichen- und Zeichenfolgedatentypen ===*/
#ifdef UNICODE
  typedef wchar_t dsChar_t;
  #define dsTEXT(x)       L##x
#else
  typedef char dsChar_t;
  #define dsTEXT(x)       x
#endif  /* !UNICODE */

/*=== Aus dsChar_t abgeleitete einheitliche Typdefinitionen und Definitionen ===*/
typedef dsChar_t            *dsString_t;

  /* für erweiterte Zurückschreibungsreihenfolge hinzugefügt */
   typedef struct
   {
     dsUint32_t top;
     dsUint32_t hi_hi;
     dsUint32_t hi_lo;
     dsUint32_t lo_hi;
     dsUint32_t lo_lo;
   } dsUint160_t ;

#if defined(_LONG_LONG)
   typedef __int64              dsInt64_t;
   typedef unsigned __int64     dsUint64_t;
   /*=== Eine "true" 64-Bit-Ganzzahl ohne Vorzeichen ===*/
   typedef __int64              dsLongLong_t;
#else
typedef struct tagUINT64_t
   {
      dsUint32_t hi;        /* Höchstwertige 32 Bit. */
      dsUint32_t lo;        /* Niedrigstwertige 32 Bit. */
   } dsUint64_t;
#endif

/*-----------------------------------------------------------------------+
| Typdefinition für bool_t                                               |
+-----------------------------------------------------------------------*/
/*
 *  Es musste ein boolescher Typ erstellt werden, der mit keiner anderen vordefinierten
 *  Version in einem Betriebssystem oder einer Fenstertechnik kollidierte.
```

```
 */
typedef enum
{
   dsmFalse = 0x00,
   dsmTrue  = 0x01
}dsmBool_t ;


/*===  für Abwärtskompatibilität ===*/
#define uint8    dsUint8_t
#define int8     dsInt8_t
#define uint16   dsUint16_t
#define int16    dsInt16_t
#define uint32   dsUint32_t
#define int32    dsInt32_t
#define uint64   dsStruct64_t
#define bool_t   dsBool_t
#define dsBool_t dsmBool_t
#define bTrue    dsmTrue
#define bFalse   dsmFalse

typedef struct
{
   dsUint32_t hi;        /* Höchstwertige 32 Bit. */
   dsUint32_t lo;        /* Niedrigstwertige 32 Bit. */
}dsStruct64_t ;

#endif /* DSMAPILIB */



#ifndef _WIN64
#pragma pack()
#endif
#endif  /* _H_DSMAPIPS */

/*****************************************************************************
* IBM Spectrum Protect                                                      *
* Allgemeine Quellenkomponente                                                *
*                                                                             *
* (C) Copyright IBM Corporation 1993,2016                                     *
*****************************************************************************/

/*****************************************************************************
* Headerdateiname: release.h
*
* Umgebung:        ***********************************************
*                  ** Dies ist eine plattformunabhängige         **
*                  ** Quellendatei                               **
*                  ***********************************************
*
* Anm. zum Entwurf: Diese Datei enthält allgemeine Informationen zur
*                   aktuellen Version samt Release.Stufe.Unterstufe
*
Beschreib. Name:    Definitionen für Tivoli Storage Manager-Version
*
* Hinweis: Diese Datei sollte keine LOG- oder CMVC-Informationen
*          enthalten. Sie wird mit dem API-Code geliefert.
*
*----------------------------------------------------------------------------*/

#ifndef _H_RELEASE
#define _H_RELEASE

#define COMMON_VERSION         8
#define COMMON_RELEASE         1
#define COMMON_LEVEL           2
#define COMMON_SUBLEVEL        0
#define COMMON_DRIVER          dsTEXT("")

#define COMMON_VERSIONTXT "8.1.2.0"

#define SHIPYEARTXT  "2017"
#define SHIPYEARTXTW dsTEXT("2017")
#define TSMPRODTXT  "IBM Spectrum Protect"

/*===========================================================================
   Die folgenden Zeichenfolgendefinitionen werden für die Versions-
   information verwendet und sollten nicht in dsTEXT oder osTEXT konver-
   tiert werden. Sie werden nur zum Zeitpunkt der Verbindung verwendet.

   Sie werden auch beim Erstellen der JAR-Datei unter UNIX verwendet.
```

```
   Siehe Perl-Script tools/unx/mzbuild/createReleaseJava.
=============================================================================*/
#define COMMON_VERSION_STR    "8"
#define COMMON_RELEASE_STR    "1"
#define COMMON_LEVEL_STR      "2"
#define COMMON_SUBLEVEL_STR   "0"
#define COMMON_DRIVER_STR     ""

/*=== Produktnamendefinitionen ===*/
#define COMMON_NAME_DFDSM      1
#define COMMON_NAME_ADSM       2
#define COMMON_NAME_TSM        3
#define COMMON_NAME_ITSM       4
#define COMMON_NAME            COMMON_NAME_ITSM

/*=============================================================================
   Interne Version mit Release und Stufenversion (Build). Sie sollte für
   Version+Release+PTF eines Produkts immer eindeutig sein.
   Diese Informationen werden in den Dateiattributen und im Datenstrom
   zu Diagnosezwecken aufgezeichnet.
   HINWEIS: MODIFIZIEREN SIE DIESE WERTE NICHT. SIE KÖNNEN LEDIGLICH
            NEUE EINTRÄGE HINZUFÜGEN!
=============================================================================*/
#define COMMON_BUILD_TSM_510   1
#define COMMON_BUILD_TSM_511   2
#define COMMON_BUILD_TSM_515   3
#define COMMON_BUILD_TSM_516   4
#define COMMON_BUILD_TSM_520   5
#define COMMON_BUILD_TSM_522   6
#define COMMON_BUILD_TSM_517   7
#define COMMON_BUILD_TSM_523   8
#define COMMON_BUILD_TSM_530   9
#define COMMON_BUILD_TSM_524   10
#define COMMON_BUILD_TSM_532   11
#define COMMON_BUILD_TSM_533   12
#define COMMON_BUILD_TSM_525   13
#define COMMON_BUILD_TSM_534   14
#define COMMON_BUILD_TSM_540   15
#define COMMON_BUILD_TSM_535   16
#define COMMON_BUILD_TSM_541   17
#define COMMON_BUILD_TSM_550   18
#define COMMON_BUILD_TSM_542   19
#define COMMON_BUILD_TSM_551   20
#define COMMON_BUILD_TSM_610   21
#define COMMON_BUILD_TSM_552   22
#define COMMON_BUILD_TSM_611   23
#define COMMON_BUILD_TSM_543   24
#define COMMON_BUILD_TSM_620   25
#define COMMON_BUILD_TSM_612   26
#define COMMON_BUILD_TSM_553   27
#define COMMON_BUILD_TSM_613   28
#define COMMON_BUILD_TSM_621   29
#define COMMON_BUILD_TSM_622   30
#define COMMON_BUILD_TSM_614   31
#define COMMON_BUILD_TSM_623   32
#define COMMON_BUILD_TSM_630   33
#define COMMON_BUILD_TSM_615   34
#define COMMON_BUILD_TSM_624   35
#define COMMON_BUILD_TSM_631   36
#define COMMON_BUILD_TSM_640   37
#define COMMON_BUILD_TSM_710   38
#define COMMON_BUILD_TSM_625   39
#define COMMON_BUILD_TSM_641   40
#define COMMON_BUILD_TSM_711   41
#define COMMON_BUILD_TSM_712   42
#define COMMON_BUILD_TSM_713   43
#define COMMON_BUILD_TSM_714   44
#define COMMON_BUILD_TSM_720   45
#define COMMON_BUILD_TSM_721   46
#define COMMON_BUILD_TSM_642   47
#define COMMON_BUILD_TSM_643   48
#define COMMON_BUILD_TSM_715   49
#define COMMON_BUILD_TSM_716   50
#define COMMON_BUILD_TSM_810   51
#define COMMON_BUILD_TSM_811   52
#define COMMON_BUILD_TSM_812   53
#define COMMON_BUILD           COMMON_BUILD_TSM_812

/*=== define VRL as an Int for bitmap version compares ====*/
static const  int  VRL_712 = 712;
static const  int  VRL_713 = 713;
static const  int  VRL_714 = 714;
```

```
static const  int  VRL_715 = 715;
static const  int  VRL_716 = 716;
static const  int  VRL_810 = 810;
static const  int  VRL_811 = 811;
static const  int  VRL_812 = 812;


#define   TDP4VE_PLATFORM_STRING_MBCS     "TDP VMware"
#define   TDP4VE_PLATFORM_STRING          dsTEXT("TDP VMware")

#define   TDP4HYPERV_PLATFORM_STRING_MBCS "TDP HyperV"
#define   TDP4HYPERV_PLATFORM_STRING      dsTEXT("TDP HyperV")

#endif /* _H_RELEASE */
```

Quellendatei mit den API-Funktionsdefinitionen

Dieser Anhang enthält die Headerdatei dsmapifp.h mit den Funktionsdefinitionen für die API.

Anmerkung: DSMLINKAGE ist für jedes Betriebssystem unterschiedlich definiert. Lesen Sie die Definitionen in der Datei dsmapips.h für Ihr Betriebssystem.

Die hier bereitgestellten Informationen enthalten eine Zeitpunktkopie der Dateien, die mit der API verteilt werden. Die neueste Version können Sie den Dateien im API-Verteilerpaket entnehmen.

```
/*****************************************************************************
* Tivoli Storage Manager                                                     *
* API-Clientkomponente                                                       *
*                                                                            *
* (C) Copyright IBM Corporation 1993,2002                                    *
*****************************************************************************/

/*****************************************************************************/
/* Headerdateiname:     dsmapifp.h                                           */
/*                                                                           */
/* Beschreibender Name: Tivoli Storage Manager API-Funktionsprototypen    */
/*****************************************************************************/
#ifndef _H_DSMAPIFP
#define _H_DSMAPIFP

#if defined(__cplusplus)
extern "C" {
#endif

#ifdef DYNALOAD_DSMAPI

/* Funktion wird dynamisch geladen     */
#include "dsmapidl.h"

#else

/* Funktionen werden implizit aus Bibliothek geladen*/

/*===========================================================================*/
/*               A L L G E M E I N E   F U N K T I O N E N                   */
/*===========================================================================*/


extern dsInt16_t DSMLINKAGE  dsmBeginGetData(
       dsUint32_t             dsmHandle,
       dsBool_t              mountWait,
       dsmGetType            getType,
       dsmGetList            *dsmGetObjListP
);

extern dsInt16_t DSMLINKAGE  dsmBeginQuery(
       dsUint32_t             dsmHandle,
       dsmQueryType          queryType,
       dsmQueryBuff          *queryBuffer
);

extern dsInt16_t DSMLINKAGE  dsmBeginTxn(
       dsUint32_t            dsmHandle
);

extern dsInt16_t DSMLINKAGE  dsmBindMC(
       dsUint32_t             dsmHandle,
       dsmObjName            *objNameP,
       dsmSendType           sendType,
       mcBindKey             *mcBindKeyP
```

```
);

extern dsInt16_t DSMLINKAGE  dsmChangePW(
       dsUint32_t             dsmHandle,
       char                  *oldPW,
       char                  *newPW
);

extern dsInt16_t DSMLINKAGE dsmCleanUp(
       dsBool_t              mtFlag
);


extern dsInt16_t DSMLINKAGE  dsmDeleteAccess(
       dsUint32_t             dsmHandle,
       dsUint32_t            ruleNum
);

extern dsInt16_t DSMLINKAGE  dsmDeleteObj(
       dsUint32_t             dsmHandle,
       dsmDelType            delType,
       dsmDelInfo            delInfo
);

extern dsInt16_t DSMLINKAGE  dsmDeleteFS(
       dsUint32_t             dsmHandle,
       char                  *fsName,
       dsUint8_t             repository
);

extern dsInt16_t DSMLINKAGE  dsmEndGetData(
       dsUint32_t            dsmHandle
);

extern dsInt16_t DSMLINKAGE  dsmEndGetDataEx(
       dsmEndGetDataExIn_t  *dsmEndGetDataExInP,
       dsmEndGetDataExOut_t *dsmEndGetDataExOutP
);

extern dsInt16_t DSMLINKAGE  dsmEndGetObj(
       dsUint32_t            dsmHandle
);

extern dsInt16_t DSMLINKAGE  dsmEndQuery(
       dsUint32_t            dsmHandle
);

extern dsInt16_t DSMLINKAGE  dsmEndSendObj(
       dsUint32_t            dsmHandle
);

extern dsInt16_t DSMLINKAGE  dsmEndSendObjEx(
       dsmEndSendObjExIn_t   *dsmEndSendObjExInP,
       dsmEndSendObjExOut_t  *dsmEndSendObjExOutP
);

extern dsInt16_t DSMLINKAGE  dsmEndTxnEx(
       dsmEndTxnExIn_t      *dsmEndTxnExInP,
       dsmEndTxnExOut_t     *dsmEndTxnExOutP
);

extern dsInt16_t DSMLINKAGE  dsmEndTxn(
       dsUint32_t             dsmHandle,
       dsUint8_t             vote,
       dsUint16_t            *reason
);

extern dsInt16_t DSMLINKAGE  dsmGetData(
       dsUint32_t             dsmHandle,
       DataBlk               *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE  dsmGetBufferData(
       getBufferDataIn_t     *dsmGetBufferDataInP,
       getBufferDataOut_t    *dsmGetBufferDataOutP
);

extern dsInt16_t DSMLINKAGE  dsmGetNextQObj(
       dsUint32_t             dsmHandle,
       DataBlk               *dataBlkPtr
) ;
```

```
extern dsInt16_t DSMLINKAGE  dsmGetObj(
       dsUint32_t             dsmHandle,
       ObjID                 *objIdP,
       DataBlk               *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE  dsmGroupHandler(
       dsmGroupHandlerIn_t   *dsmGroupHandlerInP,
       dsmGroupHandlerOut_t  *dsmGroupHandlerOutP
);

extern dsInt16_t DSMLINKAGE  dsmInit(
       dsUint32_t            *dsmHandle,
       dsmApiVersion         *dsmApiVersionP,
       char                  *clientNodeNameP,
       char                  *clientOwnerNameP,
       char                  *clientPasswordP,
       char                  *applicationType,
       char                  *configfile,
       char                  *options
);

extern dsInt16_t DSMLINKAGE  dsmInitEx(
       dsUint32_t            *dsmHandleP,
       dsmInitExIn_t         *dsmInitExInP,
       dsmInitExOut_t        *dsmInitExOutP
);


extern dsInt16_t DSMLINKAGE  dsmLogEvent(
       dsUint32_t             dsmHandle,
       logInfo               *lopInfoP
);

extern dsInt16_t DSMLINKAGE  dsmLogEventEx(
       dsUint32_t             dsmHandle,
       dsmLogExIn_t          *dsmLogExInP,
       dsmLogExOut_t         *dsmLogExOutP
);

extern dsInt16_t DSMLINKAGE  dsmQueryAccess(
       dsUint32_t             dsmHandle,
       qryRespAccessData     **accessListP,
       dsUint16_t            *numberOfRules
);

extern void DSMLINKAGE       dsmQueryApiVersion(
       dsmApiVersion         *apiVersionP
);

extern void DSMLINKAGE       dsmQueryApiVersionEx(
       dsmApiVersionEx       *apiVersionP
);

extern dsInt16_t DSMLINKAGE  dsmQueryCliOptions(
       optStruct             *optstructP
);

extern dsInt16_t DSMLINKAGE  dsmQuerySessInfo(
       dsUint32_t             dsmHandle,
       ApiSessInfo           *SessInfoP
);

extern dsInt16_t DSMLINKAGE  dsmQuerySessOptions(
       dsUint32_t             dsmHandle,
       optStruct             *optstructP
);

extern dsInt16_t DSMLINKAGE  dsmRCMsg(
       dsUint32_t             dsmHandle,
       dsInt16_t             dsmRC,
       char                  *msg
);

extern dsInt16_t DSMLINKAGE  dsmRegisterFS(
       dsUint32_t             dsmHandle,
       regFSData             *regFilespaceP
);

extern dsInt16_t DSMLINKAGE   dsmReleaseBuffer(
       releaseBufferIn_t      *dsmReleaseBufferInP,
       releaseBufferOut_t     *dsmReleaseBufferOutP
```

```
);

extern dsInt16_t DSMLINKAGE   dsmRenameObj(
       dsmRenameIn_t          *dsmRenameInP,
       dsmRenameOut_t         *dsmRenameOutP
);

extern dsInt16_t DSMLINKAGE  dsmRequestBuffer(
       requestBufferIn_t     *dsmRequestBufferInP,
       requestBufferOut_t    *dsmRequestBufferOutP
);

extern dsInt16_t DSMLINKAGE   dsmRetentionEvent(
       dsmRetentionEventIn_t  *dsmRetentionEventInP,
       dsmRetentionEventOut_t *dsmRetentionEventOutP
);

extern dsInt16_t DSMLINKAGE   dsmSendBufferData(
       sendBufferDataIn_t     *dsmSendBufferDataInP,
       sendBufferDataOut_t    *dsmSendBufferDataOutP
);

extern dsInt16_t DSMLINKAGE   dsmSendData(
       dsUint32_t             dsmHandle,
       DataBlk                *dataBlkPtr
) ;

extern dsInt16_t DSMLINKAGE   dsmSendObj(
       dsUint32_t             dsmHandle,
       dsmSendType            sendType,
       void                   *sendBuff,
       dsmObjName            *objNameP,
       ObjAttr                *objAttrPtr,
       DataBlk                *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE   dsmSetAccess(
       dsUint32_t             dsmHandle,
       dsmAccessType          accessType,
       dsmObjName            *objNameP,
       char                   *node,
       char                   *owner
);

extern dsInt16_t DSMLINKAGE   dsmSetUp(
       dsBool_t               mtFlag,
       envSetUp               *envSetUpP
);

extern dsInt16_t DSMLINKAGE   dsmTerminate(
       dsUint32_t             dsmHandle
);

extern dsInt16_t DSMLINKAGE   dsmUpdateFS(
       dsUint32_t             dsmHandle,
       char                   *fs,
       dsmFSUpd               *fsUpdP,
       dsUint32_t             fsUpdAct
);

extern dsInt16_t DSMLINKAGE   dsmUpdateObj(
       dsUint32_t             dsmHandle,
       dsmSendType            sendType,
       void                   *sendBuff,
       dsmObjName            *objNameP,
       ObjAttr                *objAttrPtr,
       dsUint32_t             objUpdAct

);

extern dsInt16_t DSMLINKAGE   dsmUpdateObjEx(
       dsmUpdateObjExIn_t     *dsmUpdateObjExInP,
       dsmUpdateObjExOut_t    *dsmUpdateObjExOutP
);


#endif /* ifdef DYNALOAD */

#if defined(__cplusplus)
   }
#endif
```

```
#endif /* _H_DSMAPIFP */
```

Dieser Abschnitt enthält die Funktionsdefinition für die API. Es handelt sich um eine Kopie der Headerdatei tsmapifp.h.
Anmerkung: DSMLINKAGE ist für jedes Betriebssystem unterschiedlich definiert. Lesen Sie die Definitionen in der Datei tsmapips.h für Ihr Betriebssystem.

```
/*****************************************************************
* Tivoli Storage Manager                                         *
* API-Clientkomponente                                           *
*                                                                *
* (C) Copyright IBM Corporation 1993,2002                        *
*****************************************************************/

/*****************************************************************************/
/* Headerdateiname:     tsmapifp.h                                           */
/*                                                                 */
/* Beschreibender Name: Tivoli Storage Manager API-Funktionsprototypen    */
/*****************************************************************************/
#ifndef _H_TSMAPIFP
#define _H_TSMAPIFP

#if defined(__cplusplus)
extern "C" {
#endif

#ifdef DYNALOAD_DSMAPI

/* Funktion wird dynamisch geladen     */
#include "dsmapidl.h"

#else

/* Funktionen werden implizit aus Bibliothek geladen*/

/*===========================================================================*/
/*               A L L G E M E I N E   F U N K T I O N E N                   */
/*===========================================================================*/


typedef void tsmQueryBuff;

extern dsInt16_t DSMLINKAGE  tsmBeginGetData(
       dsUint32_t            tsmHandle,
       dsBool_t              mountWait,
       tsmGetType            getType,
       dsmGetList            *dsmGetObjListP
);

extern dsInt16_t DSMLINKAGE  tsmBeginQuery(
       dsUint32_t            tsmHandle,
       tsmQueryType          queryType,
       tsmQueryBuff          *queryBuffer
);

extern dsInt16_t DSMLINKAGE  tsmBeginTxn(
       dsUint32_t            tsmHandle
);

extern dsInt16_t DSMLINKAGE  tsmBindMC(
       dsUint32_t            tsmHandle,
       tsmObjName            *objNameP,
       tsmSendType           sendType,
       tsmMcBindKey          *mcBindKeyP
);

extern dsInt16_t DSMLINKAGE  tsmChangePW(
       dsUint32_t            tsmHandle,
       dsChar_t              *oldPW,
       dsChar_t              *newPW
);

extern dsInt16_t DSMLINKAGE tsmCleanUp(
       dsBool_t              mtFlag
);


extern dsInt16_t DSMLINKAGE  tsmDeleteAccess(
       dsUint32_t            tsmHandle,
       dsUint32_t            ruleNum
);
```

```
extern dsInt16_t DSMLINKAGE  tsmDeleteObj(
       dsUint32_t            tsmHandle,
       tsmDelType            delType,
       tsmDelInfo            delInfo
);

extern dsInt16_t DSMLINKAGE  tsmDeleteFS(
       dsUint32_t            tsmHandle,
       dsChar_t              *fsName,
       dsUint8_t             repository
);

extern dsInt16_t DSMLINKAGE  tsmEndGetData(
       dsUint32_t            tsmHandle
);

extern dsInt16_t DSMLINKAGE  tsmEndGetDataEx(
       tsmEndGetDataExIn_t      *tsmEndGetDataExInP,
       tsmEndGetDataExOut_t     *tsmEndGetDataExOutP
);

extern dsInt16_t DSMLINKAGE  tsmEndGetObj(
       dsUint32_t            tsmHandle
);

extern dsInt16_t DSMLINKAGE  tsmEndQuery(
       dsUint32_t            tsmHandle
);

extern dsInt16_t DSMLINKAGE  tsmEndSendObj(
       dsUint32_t            tsmHandle
);

extern dsInt16_t DSMLINKAGE  tsmEndSendObjEx(
       tsmEndSendObjExIn_t      *tsmEndSendObjExInP,
       tsmEndSendObjExOut_t     *tsmEndSendObjExOutP
);

extern dsInt16_t DSMLINKAGE  tsmEndTxn(
       dsUint32_t            tsmHandle,
       dsUint8_t             vote,
       dsUint16_t            *reason
);

extern dsInt16_t DSMLINKAGE  tsmEndTxnEx(
       tsmEndTxnExIn_t      *tsmEndTxnExInP,
       tsmEndTxnExOut_t     *tsmEndTxnExOutP
);

extern dsInt16_t DSMLINKAGE  tsmGetData(
       dsUint32_t            tsmHandle,
       DataBlk*dataBlkPtr
);

extern dsInt16_t DSMLINKAGE  tsmGetBufferData(
       getBufferDataIn_t     *tsmGetBufferDataInP,
       getBufferDataOut_t    *tsmGetBufferDataOutP
);

extern dsInt16_t DSMLINKAGE  tsmGetNextQObj(
       dsUint32_t            tsmHandle,
       DataBlk*dataBlkPtr
) ;

extern dsInt16_t DSMLINKAGE  tsmGetObj(
       dsUint32_t            tsmHandle,
       ObjID                 *objIdP,
       DataBlk               *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE  tsmGroupHandler(
       tsmGroupHandlerIn_t   *tsmGroupHandlerInP,
       tsmGroupHandlerOut_t  *tsmGroupHandlerOutP
);

extern dsInt16_t DSMLINKAGE  tsmInitEx(
       dsUint32_t            *tsmHandleP,
       tsmInitExIn_t         *tsmInitExInP,
       tsmInitExOut_t        *tsmInitExOutP
);
```

```
extern dsInt16_t DSMLINKAGE  tsmLogEventEx(
       dsUint32_t            tsmHandle,
       tsmLogExIn_t          *tsmLogExInP,
       tsmLogExOut_t         *tsmLogExOutP
);

extern dsInt16_t DSMLINKAGE  tsmQueryAccess(
       dsUint32_t            tsmHandle,
       tsmQryRespAccessData  **accessListP,
       dsUint16_t            *numberOfRules
);


extern void DSMLINKAGE       tsmQueryApiVersionEx(
       tsmApiVersionEx       *apiVersionP
);

extern dsInt16_t DSMLINKAGE  tsmQueryCliOptions(
       tsmOptStruct          *optstructP
);

extern dsInt16_t DSMLINKAGE  tsmQuerySessInfo(
       dsUint32_t            tsmHandle,
       tsmApiSessInfo        *SessInfoP
);

extern dsInt16_t DSMLINKAGE  tsmQuerySessOptions(
       dsUint32_t            tsmHandle,
       tsmOptStruct          *optstructP
);

extern dsInt16_t DSMLINKAGE  tsmRCMsg(
       dsUint32_t            tsmHandle,
       dsInt16_t             tsmRC,
       dsChar_t              *msg
);

extern dsInt16_t DSMLINKAGE  tsmRegisterFS(
       dsUint32_t            tsmHandle,
       tsmRegFSData          *regFilespaceP
);

extern dsInt16_t DSMLINKAGE  tsmReleaseBuffer(
       releaseBufferIn_t     *tsmReleaseBufferInP,
       releaseBufferOut_t    *tsmReleaseBufferOutP
);

extern dsInt16_t DSMLINKAGE  tsmRenameObj(
       tsmRenameIn_t         *tsmRenameInP,
       tsmRenameOut_t        *tsmRenameOutP
);

extern dsInt16_t DSMLINKAGE  tsmRequestBuffer(
       requestBufferIn_t     *tsmRequestBufferInP,
       requestBufferOut_t    *tsmRequestBufferOutP
);

extern dsInt16_t DSMLINKAGE   tsmRetentionEvent(
       tsmRetentionEventIn_t  *tsmRetentionEventInP,
       tsmRetentionEventOut_t *tsmRetentionEventOutP
);

extern dsInt16_t DSMLINKAGE   tsmSendBufferData(
       sendBufferDataIn_t     *tsmSendBufferDataInP,
       sendBufferDataOut_t    *tsmSendBufferDataOutP
);

extern dsInt16_t DSMLINKAGE  tsmSendData(
       dsUint32_t            tsmHandle,
       DataBlk               *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE  tsmSendObj(
       dsUint32_t            tsmHandle,
       tsmSendType           sendType,
       void           *sendBuff,
       tsmObjName            *objNameP,
       tsmObjAttr            *objAttrPtr,
       DataBlk               *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE  tsmSetAccess(
```

```
        dsUint32_t            tsmHandle,
        tsmAccessType         accessType,
        tsmObjName            *objNameP,
        dsChar_t              *node,
        dsChar_t              *owner
);

extern dsInt16_t DSMLINKAGE tsmSetUp(
        dsBool_t             mtFlag,
        tsmEnvSetUp          *envSetUpP
);

extern dsInt16_t DSMLINKAGE  tsmTerminate(
        dsUint32_t            tsmHandle
);

extern dsInt16_t DSMLINKAGE  tsmUpdateFS(
        dsUint32_t            tsmHandle,
        dsChar_t              *fs,
        tsmFSUpd              *fsUpdP,
        dsUint32_t            fsUpdAct
);

extern dsInt16_t DSMLINKAGE  tsmUpdateObj(
        dsUint32_t            tsmHandle,
        tsmSendType           sendType,
        void           *sendBuff,
        tsmObjName            *objNameP,
        tsmObjAttr            *objAttrPtr,
        dsUint32_t            objUpdAct

);

extern dsInt16_t DSMLINKAGE tsmUpdateObjEx(
        tsmUpdateObjExIn_t         *tsmUpdateObjExInP,
        tsmUpdateObjExOut_t        *tsmUpdateObjExOutP
);


#endif /* ifdef DYNALOAD */

#if defined(__cplusplus)
   }
#endif

#endif /* _H_TSMAPIFP */
```

Dokumentation für die Anwendungsprogrammierschnittstelle in PDF-Dateien

Die Informationen zur IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API), die im IBM Knowledge Center verfügbar sind, sind auch in PDF-Dateien verfügbar.

- Verwendung der Anwendungsprogrammierschnittstelle
- Clientnachrichten und API-Rückkehrcodes

Zugehörige Informationen:
Lösungen mit der Anwendungsprogrammierschnittstelle entwickeln

Leistung

Viele Faktoren beeinflussen die Leistung des Servers und der Clients, einschließlich Betriebssysteme, Systemhardware, Netzkonfigurationen, Speichereinheitentypen sowie Größe und Anzahl der Clientdateien. Die Interaktionen zwischen diesen Faktoren können eine komplexe Leistungsoptimierung zur Folge haben.

Dieses Release enthält keine aktualisierte Version der Leistungskomponente. Die Leistungsdokumentation finden Sie unter Version 8.1.0.

Fehlerbehebung

Fehlerbehebungsprozeduren für die Problemdiagnose und Problemlösung sind verfügbar.

Dieses Release enthält keine aktualisierte Version der Fehlerbehebungskomponente. Die Dokumentation für die Fehlerbehebung finden Sie unter Version 8.1.0.

Nachrichten, Rückkehrcodes und Fehlercodes

Erläuterungen und vorgeschlagene Aktionen sind für Nachrichten verfügbar, die von IBM Spectrum Protect-Komponenten ausgegeben werden.

- Einführung in Nachrichten
- Rückkehrcodes für IBM Global Security Kit
  Der Server und Client verwenden das IBM Global Security Kit (GSKit) für die SSL-Verarbeitung (SSL - Secure Sockets Layer) zwischen dem Server und dem Client für Sichern/Archivieren. Einige Nachrichten, die für die SSL-Verarbeitung ausgegeben werden, enthalten GSKit-Rückkehrcodes.
- ANE: Auf dem Server protokollierte Clientereignisse
- ANR: Allgemeine und plattformspezifische Servernachrichten
- ANS: Clientnachrichten
- API-Rückkehrcodes
- E/A-Fehlercodebeschreibungen in Servernachrichten
- Einheitenfehlercodes im AIX-Systemfehlerprotokoll
- Fehlerbehebung (Version 8.1.0 ist die neueste Veröffentlichung)

Einführung in Nachrichten

Nachrichten, Fehlercodes und Rückkehrcodes werden von den IBM Spectrum Protect-Servern und -Clients ausgegeben.

Nachrichten und Codes können an der Serverkonsole, im Verwaltungsclient, an der Datenstation des Bedieners, in der grafischen Benutzerschnittstelle des Verwaltungsclients, im Client für Sichern/Archivieren oder im Client für hierarchische Speicherverwaltung (HSM-Client) angezeigt werden.

IBM Spectrum Protect stellt ein Aktivitätenprotokoll zur Verfügung, das dem Administrator helfen soll, Serveraktivitäten zu verfolgen und das System zu überwachen. Das Aktivitätenprotokoll enthält Nachrichten, die vom Server generiert wurden, und ist in der Datenbank gespeichert. Der Server löscht automatisch Nachrichten aus dem Aktivitätenprotokoll, die die angegebene Aufbewahrungszeit überschritten haben. Alle Nachrichten, die an die Serverkonsole gesendet wurden, werden im Aktivitätenprotokoll gespeichert. Beispiele für die Arten von Nachrichten, die im Aktivitätenprotokoll gespeichert werden, sind:

- Start oder Ende von Clientsitzungen
- Start oder Ende von Umlagerungen
- Verfall gesicherter Dateien im Serverspeicher
- Alle Ausgaben, die von Hintergrundprozessen generiert werden

Einige Nachrichten haben keine Erläuterungen und werden nicht veröffentlicht. Der Client kann Statistiken an den Server senden, um Informationen zu einer Sicherungs- oder Zurückschreibungsoperation zur Verfügung zu stellen. Diese Statistiken sind Informationsnachrichten, die für die verschiedenen Ereignisprotokollempfänger aktiviert oder inaktiviert werden können. Diese Nachrichten werden nicht veröffentlicht.

- Format der IBM Spectrum Protect-Server- und -Clientnachrichten
- Rückkehrcodenachrichten interpretieren

Zugehörige Tasks:
Aktivitätenprotokoll verwenden (Version 7.1.1)

Format der IBM Spectrum Protect-Server- und -Clientnachrichten

IBM Spectrum Protect-Server- und -Clientnachrichten bestehen aus den folgenden Elementen:

- Einem Präfix mit drei Buchstaben. Nachrichten haben verschiedene Präfixe, mit denen Sie die IBM Spectrum Protect-Komponente identifizieren können, die die Nachricht ausgibt. Alle Nachrichten für eine Komponente haben normalerweise dasselbe Präfix. Manchmal gibt eine Komponente Nachrichten mit zwei oder drei verschiedenen Präfixen aus.

  Beispielsweise geben Clients für Sichern/Archivieren Nachrichten mit dem Präfix ANS aus. Ereignisse des Clients für Sichern/Archivieren, die auf dem Server protokolliert werden, haben das Präfix ANE. Allgemeine und plattformspezifische Nachrichten des Servers haben das Präfix ANR.

- Einer numerischen Nachricht-ID.
- Einem Bewertungscode mit einem Buchstaben. Die folgenden Codes geben die Bewertung der Aktion an, die die Nachricht generiert hat:

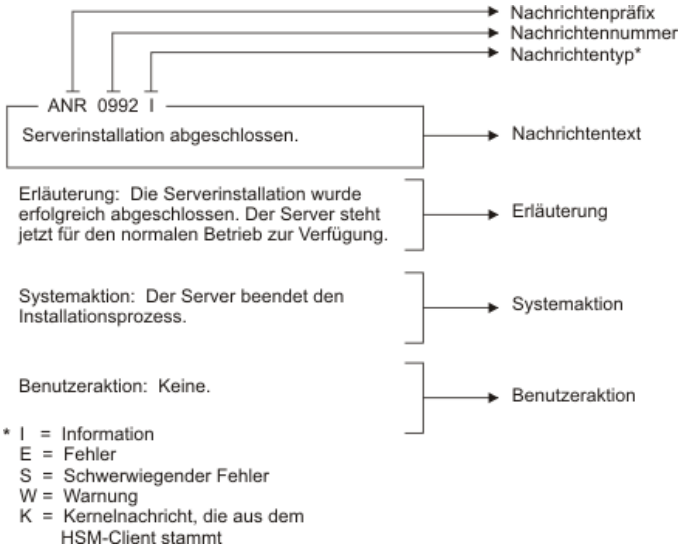
Code	Bewertung	Bedeutung
S	Schwerwiegend	Das Produkt oder eine Produktfunktion kann nicht fortgesetzt werden. Eine Benutzeraktion ist erforderlich.
E	Fehler	Bei der Verarbeitung ist ein Fehler aufgetreten. Die Verarbeitung wird möglicherweise gestoppt. Eine Benutzeraktion kann erforderlich sein.
W	Warnung	Die Verarbeitung wird fortgesetzt, aber es können zu einem späteren Zeitpunkt aufgrund der Warnung Probleme auftreten.
I	Information	Die Verarbeitung wird fortgesetzt. Es ist keine Benutzeraktion erforderlich.

- Nachrichtentext, der angezeigt und in Nachrichtenprotokolle geschrieben wird.

- Erläuterung, Systemaktion und Benutzeraktion. In diesen Texten wird der Nachrichtentext näher erläutert. Die Texte sind in den Nachrichtenhandbüchern des Produkts und in der Befehlszeilenhilfe verfügbar.

Die folgende Abbildung zeigt eine typische IBM Spectrum Protect-Servernachricht.

Die Beschriftungen geben jedes Element der Nachricht an.



Nachrichtenvariablen im Nachrichtentext werden kursiv angezeigt.

Rückkehrcodenachrichten interpretieren

Viele verschiedene Befehle können denselben *Rückkehrcode* generieren. Die folgenden Beispiele zeigen zwei verschiedene Befehle, die ausgegeben wurden und denselben Rückkehrcode zur Folge haben; daher muss die *beschreibende Nachricht* für den Befehl gelesen werden.

In diesen Beispielen haben zwei verschiedene Befehle denselben Rückkehrcode zur Folge, aber sie geben auch beschreibende Nachrichten zurück, die für jeden Befehl eindeutig sind. Die beiden Befehle sind `q event standard dddd` und `def vol cstg05 primary`. Beide haben eine generische Nachricht mit diesem Rückkehrcode zur Folge:

```
ANS5102I: Rückkehrcode 11.
```

Der erste Befehl gibt jedoch auch eine beschreibende Nachricht zurück:

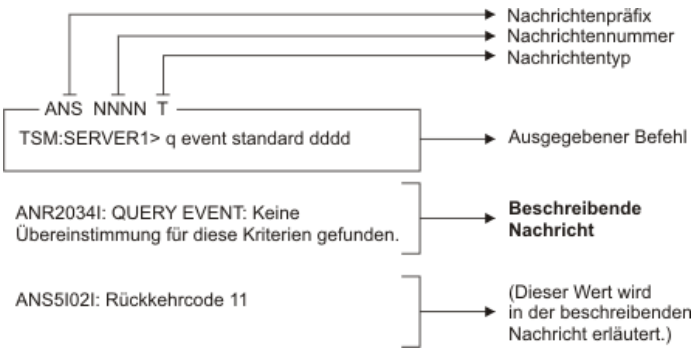
```
ANR2034I: QUERY EVENT: Keine Übereinstimmung für diese
Abfrage gefunden.
```

Der zweite Befehl gibt ebenfalls eine eindeutige beschreibende Nachricht zurück:

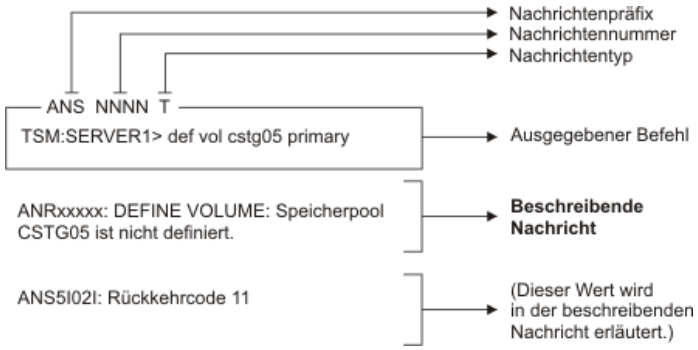
```
ANRxxxx: DEFINE VOLUME: Speicherpool CSTG05 ist nicht definiert.
```

- Erstes Beispiel für den Befehl QUERY EVENT
- Zweites Beispiel für den Befehl DEFINE VOLUME

Erstes Beispiel für den Befehl QUERY EVENT



Zweites Beispiel für den Befehl DEFINE VOLUME



ANE-Nachrichten

ANE-Nachrichten werden vom Server ausgegeben. Alle Nachrichten mit dem Präfix ANE sind Clientereignisse, die auf dem Server protokolliert werden.

- Liste der ANE-Nachrichten

ANR-Nachrichten

ANR-Nachrichten werden vom Server ausgegeben. Einige ANR-Nachrichten gelten für alle Betriebssysteme, andere gelten nur für ein einzelnes Betriebssystem.

- Liste der ANR-Nachrichten

ANS-Nachrichten 0000-9999

ANS-Nachrichten mit Nachrichtennummern im Bereich von 0000 bis 9999 werden von den folgenden IBM Spectrum Protect-Clients ausgegeben:

- Verwaltungsclients
- API-Clients
- Clients für Sichern/Archivieren
- IBM Spectrum Protect for Space Management-Clients (HSM-Clients)

Eine Liste der Nachrichten, die seit der vorherigen Produktmodifikationsstufe hinzugefügt und geändert wurden, ist in der Datei client_message.chg im Produktinstallationsverzeichnis verfügbar. Die Listen der neuen und geänderten Clientnachrichten für Version 8.1.2 und höher sind auch im IBM developerWorks-Wiki verfügbar.

- Liste der ANS-Nachrichten

API-Rückkehrcodes

Die Rückkehrcodes der IBM Spectrum Protect-API Version 8.1.2 werden aufgelistet. Das Format der Rückkehrcodes wird beschrieben.

Außerdem enthalten einige Nachrichten, die für die SSL-Verarbeitung ausgegeben werden, GSKit-Rückkehrcodes. Ausführliche Informationen finden Sie in Rückkehrcodes für IBM Global Security Kit.

- Format der API-Rückkehrcodes
- API-Rückkehrcodes

Format der API-Rückkehrcodes

In diesem Abschnitt wird das Format der API-Rückkehrcodes (API - Application Programming Interface) erläutert. Für jeden Rückkehrcode werden die folgenden Informationen bereitgestellt:

- Die Rückkehrcodenummer. Diese Nummer entspricht der Nummer in der Header-Datei **dsmrc.h**.
- Der Bewertungscode. Dieser Buchstabe gibt die Wertigkeit an, die den Rückkehrcode generiert hat. Die Bewertungscodes haben folgende Bedeutung:

S	Schwerwiegender Fehler	Die Verarbeitung kann nicht fortgesetzt werden.
E	Fehler	Die Verarbeitung kann nicht fortgesetzt werden.
W	Warnung	Die Verarbeitung kann zwar fortgesetzt werden, es können jedoch zu einem späteren Zeitpunkt Probleme auftreten. Sie sollten vorsichtig sein.
I	Information	Die Verarbeitung wird fortgesetzt. Es ist keine Benutzeraktion erforderlich.

- Der symbolische Name. Dieser Name entspricht der Definition in der Header-Datei **dsmrc.h**. *Verwenden Sie in Ihrer Anwendung statt der Rückkehrcodenummer immer den symbolischen Namen für einen Rückkehrcode.*
- Die Erläuterung. Dieses Feld erläutert, unter welchen Umständen dieser Rückkehrcode generiert werden kann.
- Die Systemaktion. Dieses Feld beschreibt, welche Aktion IBM Spectrum Protect als Antwort auf den Rückkehrcode ausführen wird.
- Die Benutzeraktion. Dieses Feld erläutert, wie Sie auf die Systemaktion reagieren sollten.

Viele der Rückkehrcodes beschreiben Fehler, die das Stoppen der Verarbeitung bewirken. Sie können eine Nachricht an den Endbenutzer senden, die den Fehler beschreibt und einen Vorschlag zur Fehlerbehebung enthält. Um unterschiedliche Nachrichten zu kennzeichnen, verwenden Sie diese Rückkehrcodewerte oder entwickeln Sie ein eigenes Nummerierungssystem.

API-Rückkehrcodes

Die Rückkehrcodes der IBM Spectrum Protect-API Version 8.1.2 sind in aufsteigender numerischer Reihenfolge aufgelistet. Es wird der vollständige Rückkehrcode angegeben.

- -452 E
  DSM_RC_SHM_NOTAUTH Unzureichende Berechtigung für Verbindung mit Shared Memory-Region
- -451 E
  DSM_RC_SHM_FAILURE Fehler bei Verwendung des Shared-Memory-Protokolls
- -450 E
  DSM_RC_SHM_TCPIP_FAILURE Sitzung zurückgewiesen: TCP/IP-Verbindungsfehler für Shared Memory
- -190 E
  DSM_RC_NP_ERROR Sitzung zurückgewiesen: Verbindungsfehler mit benannten Pipes.
- -057 E
  DSM_RC_TCPIP_LOADFAILURE Die TCP/IP-Ladefunktion ist fehlgeschlagen.
- -056 E
  DSM_RC_TCPIP_DLL_LOADFAILURE Fehler beim Laden einer Bibliothek aufgetreten.
- -055 E
  DSM_RC_WINSOCK_MISSING Die TCP/IP-Datei WINSOCK.DLL kann nicht gefunden werden.
- -054 E
  DSM_RC_NETWORK_UNREACHABLE Der angegebene TCP/IP-Host-Name ist nicht erreichbar
- -053 E
  DSM_RC_BAD_HOST_NAME Es wurde eine ungültige TCP/IP-Adresse angegeben.
- -052 E
  DSM_RC_CONN_REFUSED Versuch, eine TCP/IP-Verbindung herzustellen, vom Host zurückgewiesen
- -051 E
  DSM_RC_CONN_TIMEDOUT Beim Versuch, eine TCP/IP-Verbindung aufzubauen, wurde das zulässige Zeitlimit überschritten, bevor die Verbindung zustande kam.
- -050 E
  DSM_RC_TCPIP_FAILURE Sitzung zurückgewiesen: TCP/IP-Verbindungsfehler.
- 0000 I
  DSM_RC_OK Erfolgreich beendet.
- 0001 E
  DSM_RC_ABORT_SYSTEM_ERROR Diese Operation kann aufgrund eines Fehlers auf dem IBM Spectrum Protect-Server nicht fortgesetzt werden. Bitten Sie Ihren IBM Spectrum Protect-Serveradministrator um Unterstützung.
- 0002 E
  DSM_RC_ABORT_NO_MATCH Keine Objekte auf dem Server stimmen mit der Abfrage überein
- 0003 E
  DSM_RC_ABORT_BY_CLIENT Client hat Transaktion beendet
- 0004 W
  DSM_RC_ABORT_ACTIVE_NOT_FOUND Es konnte keine aktive Sicherungsversion gefunden werden.
- 0005 E
  DSM_RC_ABORT_NO_DATA Der IBM Spectrum Protect-Server hat keine Daten für das Objekt.
- 0006 E
  DSM_RC_ABORT_BAD_VERIFIER Sie haben ein falsches Kennwort eingegeben.
- 0007 E
  DSM_RC_ABORT_NODE_IN_USE Knoten bereits im Gebrauch
- 0008 E
  DSM_RC_ABORT_EXPDATE_TOO_LOW Verfallsdatum muß später als das heutige Datum sein
- 0009 W
  DSM_RC_ABORT_DATA_OFFLINE Die angeforderten Daten sind offline.
- 0010 E
  DSM_RC_ABORT_EXCLUDED_BY_SIZE Objekt für Server-Begrenzungen zu groß
- 0011 E
  DSM_RC_ABORT_NO_REPOSIT_SPACE Server hat keinen Datenspeicherbereich mehr
- 0012 E
  DSM_RC_ABORT_MOUNT_NOT_POSSIBLE Laden von Serverdatenträgern nicht möglich

- 0013 E
  DSM_RC_ABORT_SIZESTIMATE_EXCEED Größenschätzung überschritten
- 0014 E
  DSM_RC_ABORT_DATA_UNAVAILABLE Dateidaten derzeit auf dem Server nicht verfügbar
- 0015 E
  DSM_RC_ABORT_RETRY Unerwartete Wiederholungsanforderung. Der IBM Spectrum Protect-Server hat beim Schreiben der Daten einen Fehler gefunden.
- 0016 E
  DSM_RC_ABORT_NO_LOG_SPACE Der Server hat nicht genug Speicherbereich für das Wiederherstellungsprotokoll, um die aktuelle Operation fortzusetzen.
- 0017 E
  DSM_RC_ABORT_NO_DB_SPACE Der Server hat nicht genug Speicher für den Datenbankbereich, um die aktuelle Operation fortzusetzen.
- 0018 E
  DSM_RC_ABORT_NO_MEMORY Der Server hat nicht genug Speicher, um die aktuelle Operation fortzusetzen.
- 0020 E
  DSM_RC_ABORT_FS_NOT_DEFINED Der angegebene Dateibereich ist auf dem Server nicht vorhanden. Der Dateibereich wurde möglicherweise von einem anderen Client oder einem Administrator gelöscht.
- 0021 S
  DSM_RC_ABORT_NODE_ALREADY_DEFED Offene Registrierung fehlgeschlagen, da der angegebene Knotenname im Server definiert ist
- 0022 S
  DSM_RC_ABORT_NO_DEFAULT_DOMAIN Offene Registrierung fehlgeschlagen, da keine Standarddomäne vorhanden ist.
- 0023 S
  DSM_RC_ABORT_INVALID_NODENAME Offene Registrierung fehlgeschlagen, da angegebener Knotenname ungültig ist
- 0024 S
  DSM_RC_ABORT_INVALID_POL_BIND Auf dem IBM Spectrum Protect-Server ist ein Maßnahmenverwaltungsfehler aufgetreten.
- 0024 E
  DSM_RC_ABORT_NO_INVALID_POL_BIND Ein Objekt in der Transaktion wurde an eine ungültige Verwaltungsklasse gebunden.
- 0025 E
  DSM_RC_ABORT_DEST_NOT_DEFINED Serverfehler: Zielort nicht definiert.
- 0026 S
  DSM_RC_ABORT_WAIT_FOR_SPACE Der IBM Spectrum Protect-Server hat für diese Datei momentan keinen Speicher im Speicherpool. Dies ist möglicherweise ein temporärer Zustand.
- 0027 E
  DSM_RC_ABORT_NOT_AUTHORIZEDDer Dateibereich kann nicht gelöscht werden, da dieser Knoten keine Berechtigung zum Löschen archivierter oder gesicherter Daten hat.
- 0028 E
  DSM_RS_ABORT_RULE_ALREADY_DEFED Zugriffsregel 'Zugriffsregel' für Knoten 'Knoten' bereits definiert. Alte Regel muss gelöscht werden, bevor neue definiert werden kann.
- 0029 S
  DSM_RC_ABORT_NO_STOR_SPACE_STOP Server hat keinen Datenspeicherbereich mehr
- 0030 E
  DSM_RC_ABORT_LICENSE_VIOLATION Die Operation ist auf Grund von Serverlizenzwerten nicht gestattet.
- 0032 E
  DSM_RC_ABORT_DUPLICATE_OBJECT Ein doppeltes Objekt wurde gefunden, Operation kann nicht beendet werden.
- 0033 E
  DSM_RC_ABORT_INVALID_OFFSET Wert für 'partialObjOffset' für Abrufen von partiellen Objekten ist ungültig.
- 0034 E
  DSM_RC_ABORT_INVALID_LENGTH Wert für 'partialObjLength' für Abrufen von partiellen Objekten ist ungültig.
- 0036 E
  DSM_RC_END_NODE_NOT_AUTHORIZED Der Knoten oder Benutzer hat nicht die korrekte Berechtigung zum Ausführen dieser Operation.
- 0041 E
  DSM_RC_ABORT_EXCEED_MAX_MP Dieser Knoten hat die maximale Anzahl Mountpunkte überschritten.
- 0045 E
  DSM_RC_ABORT_MERGE_ERROR Die angegebenen Objekte sind beim Mischtest fehlgeschlagen.
- 0047 E
  DSM_RC_ABORT_INVALID_OPERATIONUngültige Operation für Knoten versucht
- 0048 E
  DSM_RC_ABORT_STGPOOL_UNDEFINEDDer angegebene Zielspeicherpool ist nicht definiert.
- 0049 E
  DSM_RC_ABORT_INVALID_DATA_FORMATEin Zielspeicherpool verfügt nicht über das korrekte Datenformat für die angegebene Knotenart.
- 0050 E
  DSM_RC_ABORT_DATAMOVER_UNDEFINEDKeine zugeordnete Einheit zum Versetzen von Daten ist für den angegebenen Knoten definiert.
- 0051 E
  DSM_RC_REJECT_NO_RESOURCES Sitzung zurückgewiesen: Alle Serversitzungen sind derzeit im Gebrauch
- 0052 E
  DSM_RC_REJECT_VERIFIER_EXPIRED Die Sitzung wird zurückgewiesen. Ihr Kennwort ist abgelaufen.

- 0053 E
  DSM_RC_REJECT_ID_UNKNOWN Sitzung zurückgewiesen: Die Benutzer-ID ist falsch, hat keine Administratorberechtigung oder ist dem Server nicht bekannt.
- 0054 E
  DSM_RC_REJECT_DUPLICATE_ID Sitzung zurückgewiesen: Doppelte ID eingegeben
- 0055 E
  DSM_RC_REJECT_SERVER_DISABLED Sitzung zurückgewiesen: Server inaktiv.
- 0056 E
  DSM_RC_REJECT_CLOSED_REGISTER Der Server ist nicht für offene Registrierung konfiguriert
- 0057 S
  DSM_RC_REJECT_CLIENT_DOWNLEVEL Sitzung zurückgewiesen: Codeversion des Clients ist älter
- 0058 S
  DSM_RC_REJECT_SERVER_DOWNLEVEL Sitzung zurückgewiesen: Codeversion des Servers ist älter
- 0059 E
  DSM_RC_REJECT_ID_IN_USE Sitzung zurückgewiesen: Angegebener Knotenname derzeit im Gebrauch
- 0061 E
  DSM_RC_REJECT_ID_LOCKED Sitzung zurückgewiesen: Der angegebene Knotenname ist derzeit gesperrt.
- 0062 S
  DSM_RC_SIGNONREJECT_LICENSE_MAX SLM LICENSE EXCEEDED: Die Clientlizenzen für IBM Spectrum Protect sind überschritten. Verständigen Sie Ihren Systemadministrator.
- 0063 E
  DSM_RC_REJECT_NO_MEMORY Sitzung zurückgewiesen: Der Server hat nicht genug Speicher, um das Herstellen einer Verbindung zuzulassen.
- 0064 E
  DSM_RC_REJECT_NO_DB_SPACE Sitzung zurückgewiesen: Der Server hat nicht genug Datenbankbereich, um das Herstellen einer Verbindung zuzulassen.
- 0065 E
  DSM_RC_REJECT_NO_LOG_SPACE Sitzung zurückgewiesen: Der Server hat nicht genug Speicherbereich für das Wiederherstellungsprotokoll, um das Herstellen einer Verbindung zuzulassen.
- 0066 E
  DSM_RC_REJECT_INTERNAL_ERROR Die Sitzung wird zurückgewiesen. Beim IBM Spectrum Protect-Server ist ein interner Fehler aufgetreten.
- 0067 S
  DSM_RC_SIGNONREJECT_INVALID_CLI Sitzung zurückgewiesen: Der Server ist nicht für diesen Plattformtyp lizenziert. Verständigen Sie Ihren Systemadministrator.
- 0068 E
  DSM_RC_CLIENT_NOT_ARCHRETPROT Die Sitzung wird zurückgewiesen. Der Server erlaubt nicht das Anmelden eines Clients, dessen Aufbewahrungsschutz für Archivierung nicht aktiviert ist.
- 0069 E
  DSM_RC_SESSION_CANCELED Sitzung zurückgewiesen: Die Sitzung wurde vom Server-Administrator abgebrochen.
- 0073 E
  DSM_RC_REJECT_INVALID_NODE_TYPE Zwischen dem Clientknoten und dem auf dem IBM Spectrum Protect-Server registrierten Knoten wurde eine Inkonsistenz festgestellt.
- 0074 E
  DSM_RC_REJECT_INVALID_SESSIONINIT Der Server lässt keine vom Client eingeleiteten Verbindungen für diesen Knoten zu.
- 0075 E
  DSM_RC_REJECT_WRONG_PORT Falscher Serveranschluss.
- 0079 E
  DSM_RC_CLIENT_NOT_SPMRETPROT Die Sitzung wird zurückgewiesen. Der Server erlaubt nicht das Anmelden eines Clients, dessen Aufbewahrungsschutz für Speicherverwaltung nicht aktiviert ist.
- 0101 W
  DSM_RC_USER_ABORT Die Operation wurde vom Benutzer gestoppt.
- 0102 E
  DSM_RC_NO_MEMORY Dateiname(Zeilennummer) Das Betriebssystem hat eine IBM Spectrum Protect-Anforderung für Speicherzuordnung zurückgewiesen.
- 0104 E
  DSM_RC_FILE_NOT_FOUND Datei bei Sicherungs-, Archivierungs- oder Umlagerungsverarbeitung nicht gefunden
- 0105 E
  DSM_RC_PATH_NOT_FOUND Der angegebene Verzeichnispfad 'Pfadname' konnte nicht gefunden werden.
- 0106 E
  DSM_RC_ACCESS_DENIED Zugriff auf angegebene Datei oder Verzeichnis verweigert
- 0106 E
  DSM_RC_ACCESS_DENIED Die angegebene Datei wird von einem anderen Prozeß verwendet
- 0107 E
  DSM_RC_NO_HANDLES Keine Dateikennungen verfügbar
- 0108 E
  DSM_RC_FILE_EXISTS Die Datei ist vorhanden und kann nicht überschrieben werden.

- 0109 E
  DSM_RC_INVALID_PARM Ungültiger Parameter gefunden.
- 0110 E
  DSM_RC_INVALID_HANDLE Es wurde eine ungültige Dateikennung übergeben; Systemfehler.
- 0111 E
  DSM_RC_DISK_FULL Verarbeitung gestoppt; Bedingung 'Platte voll'.
- 0113 E
  DSM_RC_PROTOCOL_VIOLATION Fehlerhaftes Protokoll
- 0114 E
  DSM_RC_UNKNOWN_ERROR Es ist ein unbekannter Systemfehler aufgetreten, aufgrund dessen IBM Spectrum Protect nicht wiederhergestellt werden kann.
- 0115 E
  DSM_RC_UNEXPECTED_ERROR Es ist ein unerwarteter Fehler aufgetreten.
- 0116 E
  DSM_RC_FILE_BEING_EXECUTED Datei wird gerade ausgeführt; Schreibzugriff verweigert.
- 0117 E
  DSM_RC_DIR_NO_SPACE Es können keine weiteren Dateien zurückgeschrieben oder abgerufen werden, da das Zielverzeichnis voll ist.
- 0118 E
  DSM_RC_LOOPED_SYM_LINK Beim Auflösen des Namens zu viele symbolische Verbindungen festgestellt
- 0119 E
  DSM_RC_FILE_NAME_TOO_LONG Der Dateiname ist zu lang und kann von IBM Spectrum Protect nicht verarbeitet werden.
- 0120 E
  DSM_RC_FILE_SPACE_LOCKED Dateisystem vom System gesperrt
- 0121 I
  DSM_RC_FINISHED Die Operation ist beendet.
- 0122 E
  DSM_RC_UNKNOWN_FORMAT Die Datei hat ein unbekanntes Format.
- 0123 E
  DSM_RC_NO_AUTHORIZATION Keine Berechtigung zum Zurückschreiben von Daten des anderen Knotens.
- 0124 E
  DSM_RC_FILE_SPACE_NOT_FOUND Dateibereich 'Dateibereichsname' nicht vorhanden
- 0125 E
  DSM_RC_TXN_ABORTED Transaktion abgebrochen
- 0126 E
  DSM_RC_SUBDIR_AS_FILE IBM Spectrum Protect kann keinen Verzeichnispfad erstellen, weil eine Datei mit demselben Namen wie das Verzeichnis vorhanden ist.
- 0127 E
  DSM_RC_PROCESS_NO_SPACE Plattenspeicherplatzbegrenzung für diesen Prozeß erreicht
- 0128 E
  DSM_RC_PATH_TOO_LONG Pfadlänge des Zielverzeichnisses überschreitet Systemmaximum
- 0129 E
  DSM_RC_NOT_COMPRESSED Datei ist nicht komprimiert. Systemfehler.
- 0130 E
  DSM_RC_TOO_MANY_BITS Datei auf einer anderen Client-Maschine mit mehr Speicher komprimiert
- 0131 E
  DSM_RC_COMPRESSED_DATA_CORRUPTED Die komprimierte Datei ist beschädigt und kann nicht ordnungsgemäß erweitert werden.
- 0131 S
  DSM_RC_SYSTEM_ERROR Ein interner Programmfehler ist aufgetreten.
- 0132 E
  DSM_RC_NO_SERVER_RESOURCES Der IBM Spectrum Protect-Server hat keine Ressourcen mehr.
- 0133 E
  DSM_RC_FS_NOT_KNOWN Der Dateibereich für die Domäne 'Domänenname' wurde auf dem IBM Spectrum Protect-Server nicht gefunden.
- 0134 E
  DSM_RC_NO_LEADING_DIRSEP Das Feld 'objName' hat keinen führenden Verzeichnisseparator.
- 0135 E
  DSM_RC_WILDCARD_DIR Platzhalterzeichen sind im objName-Verzeichnispfad nicht zulässig.
- 0136 E
  DSM_RC_COMM_PROTOCOL_ERROR Die Sitzung wird zurückgewiesen: Es gab einen Fehler im Übertragungsprotokoll.
- 0137 E
  DSM_RC_AUTH_FAILURE Sitzung zurückgewiesen: Fehler bei Authentifizierung
- 0138 E
  DSM_RC_TA_NOT_VALID Die Ausführungs-/Eignerberechtigungen für 'dsmtca' sind ungültig.
- 0139 S
  DSM_RC_KILLED Prozeß abgebrochen.
- 0145 S
  DSM_RC_WOULD_BLOCK Das Modul 'dsmtca' würde die Operation blockieren.

- 0146 S
  DSM_RC_TOO_SMALL Der Bereich für das Einschluß-/Ausschlußmuster ist zu klein.
- 0147 S
  DSM_RC_UNCLOSED Das Muster enthält keine rechte eckige Klammer.
- 0148 S
  DSM_RC_NO_STARTING_DELIMITER Das Einschluss-/Ausschlussmuster muss mit einem Verzeichnisbegrenzer beginnen
- 0149 S
  DSM_RC_NEEDED_DIR_DELIMITER Ein führender oder abschließender Verzeichnisbegrenzer fehlt im Einschluss-/Ausschlussmuster.
- 0151 S
  DSM_RC_BUFFER_OVERFLOW Der Datenpuffer ist voll.
- 0154 E
  DSM_RC_NO_COMPRESS_MEMORY Nicht genügend Speicher für Dateikomprimierung/-erweiterung
- 0155 T
  DSM_RC_COMPRESS_GREW Komprimierte Daten angewachsen
- 0156 E
  DSM_RC_INV_COMM_METHOD Es wurde eine nicht unterstützte Übertragungsmethode angegeben.
- 0157 S
  DSM_RC_WILL_ABORT Die Transaktion wird abgebrochen.
- 0158 E
  DSM_RC_FS_WRITE_LOCKED Zieldatei oder Verzeichnis ist schreibgeschützt
- 0159 I
  DSM_RC_SKIPPED_BY_USER Eine Datei wurde bei einer Zurückschreibungsoperation übersprungen, da die Datei inaktiv war und von der Anwendung ausgewählt wurde, nicht auf das Laden eines Bands zu warten.
- 0160 E
  DSM_RC_TA_NOT_FOUND Das Modul 'dsmtca' wurde nicht gefunden.
- 0162 E
  DSM_RC_FS_NOT_READY Dateisystem/Laufwerk nicht bereit
- 0164 E
  DSM_RC_FIO_ERROR Dateiein-/-ausgabefehler
- 0165 E
  DSM_RC_WRITE_FAILURE Fehler beim Schreiben in Datei
- 0166 E
  DSM_RC_OVER_FILE_SIZE_LIMIT Datei überschreitet System-/Benutzerdateibegrenzungen
- 0167 E
  DSM_RC_CANNOT_MAKE Datei/Verzeichnis kann nicht erstellt werden
- 0168 E
  DSM_RC_NO_PASS_FILE Kennwortdatei ist nicht verfügbar.
- 0169 E
  DSM_RC_VERFILE_OLD PASSWORDACCESS ist GENERATE, aber für den Server 'Servername' wird ein Kennwort benötigt. Entweder ist das Kennwort nicht lokal gespeichert oder es wurde auf dem Server geändert.
- 0173 E
  DSM_RC_INPUT_ERROR Der Prozess wird in einem nicht interaktiven Modus ausgeführt, erfordert aber Benutzereingaben.
- 0174 E
  DSM_RC_REJECT_PLATFORM_MISMATCH Sitzung zurückgewiesen: Abweichung bei Knotenart
- 0175 E
  DSM_RC_TL_NOT_FILE_OWNER Nicht der Dateieigner
- 0177 S
  DSM_RC_UNMATCHED_QUOTE Anführungszeichen stimmen nicht überein
- 0184 E
  DSM_RC_TL_NOBCG Die Verwaltungsklasse für diese Datei hat keine gültige Sicherungskopiengruppe. Diese Datei wird nicht gesichert.
- 0185 W
  DSM_RC_TL_EXCLUDED Datei 'DateinameDateinameDateiname' durch Einschluss-/Ausschlussliste ausgeschlossen
- 0186 E
  DSM_RC_TL_NOACG Die Verwaltungsklasse für diese Datei hat keine gültige Archivierungskopiengruppe. Diese Datei wird nicht archiviert.
- 0187 E
  DSM_RC_PS_INVALID_ARCHMC Ungültige Verwaltungsklasse eingegeben
- 0188 S
  DSM_RC_NO_PS_DATA Entweder ist der Knoten auf dem Server nicht vorhanden oder es gibt keine aktive Maßnahmengruppe für den Knoten.
- 0189 S
  DSM_RC_PS_INVALID_DIRMC Die den Verzeichnissen zugeordnete Verwaltungsklasse ist nicht vorhanden.
- 0190 S
  DSM_RC_PS_NO_CG_IN_DIR_MC Es gibt keine Sicherungskopiengruppe in der für Verzeichnisse verwendeten Verwaltungsklasse.
- 0231 E
  DSM_RC_ABORT_MOVER_TYPEUnbekannte Art der fernen Versetzungseinheit
- 0232 E
  DSM_RC_ABORT_ITEM_IN_USEEine Operation für den angeforderten Knoten und Dateibereich wird bereits ausgeführt.

- 0233 E
  DSM_RC_ABORT_LOCK_CONFLICTSystemressource wird verwendet
- 0234 E
  DSM_RC_ABORT_SRV_PLUGIN_COMM_ERRORServer-Plug-in-Kommunikationsfehler
- 0235 E
  DSM_RC_ABORT_SRV_PLUGIN_OS_ERRORServer-Plug-in hat nicht unterstütztes Betriebssystem für NAS-Dateieinheit erkannt.
- 0236E
  DSM_RC_ABORT_CRC_FAILED Der vom Server empfangene CRC stimmt nicht mit dem vom Client berechneten CRC überein.
- 0237E
  DSM_RC_ABORT_INVALID_GROUP_ACTION Ungültige Operation für einen Gruppenleiter oder ein Gruppenmitglied.
- 0238E
  DSM_RC_ABORT_DISK_UNDEFINED Ferne Platte nicht definiert.
- 0239E
  DSM_RC_ABORT_BAD_DESTINATION Eingabezielort entspricht nicht dem erwarteten Zielort.
- 0240E
  DSM_RC_ABORT_DATAMOVER_NOT_AVAILABLE Einheit zum Versetzen von Daten ist nicht verfügbar.
- 0241E
  DSM_RC_ABORT_STGPOOL_COPY_CONT_NO Operation fehlgeschlagen, da die Option zum Fortsetzen des Kopierens auf NO gesetzt war.
- 0242E
  DSM_RC_ABORT_RETRY_SINGLE_TXN Transaktion aufgrund eines Fehlers während einer Speicheroperation fehlgeschlagen.
- 0245 E
  DSM_RC_ABORT_PATH_RESTRICTED Die aktuelle Clientkonfiguration ist nicht konform mit dem Wert der Serveroption DATAWRITEPATH oder DATAREADPATH für diesen Knoten.
- 0247 E
  DSM_RC_ABORT_INSERT_NOT_ALLOWED Dieser Server unterstützt keine Sicherungsoperationen.
- 0248 E
  DSM_RC_ABORT_DELETE_NOT_ALLOWED Das Löschen des Objekts: "fshlll" ist nicht zulässig.
- 0249 E
  DSM_RC_ABORT_TXN_LIMIT_EXCEEDED Die Anzahl der Objekte in dieser Transaktion überschreitet die Werte für TXNGROUPMAX.
- 0250 E
  DSM_RC_ABORT_OBJECT_ALREADY_HELD fshlll ist bereits auf Halten gesetzt.
- 0292 E
  DSM_RC_TCA_FORK_FAILED Fehler beim Starten des Prozesses dsmtca oder dsmenc.
- 0295 E
  DSM_RC_TCA_INVALID_REQUEST Der IBM Spectrum Protect-Prozess 'dsmtca' hat eine ungültige Anforderung empfangen.
- 0296 E
  DSM_RC_TCA_NOT_ROOT Diese Aktion erfordert IBM Spectrum Protect-Administratorberechtigung auf diesem System.
- 0297 E
  DSM_RC_TCA_SEMGET_ERROR Fehler beim Zuordnen von Semaphors.
- 0298 E
  DSM_RC_TCA_SEM_OP_ERROR Fehler beim Definieren des Semaphorwerts oder beim Warten auf Semaphor.
- 0400 E
  DSM_RC_INVALID_OPT Bei der Syntaxanalyse wurde eine ungültige Option gefunden.
- 0405 E
  DSM_RC_NO_HOST_ADDR TCPSERVERADDRESS für diesen Server in der Systemoptionsdatei nicht definiert
- 0406 S
  DSM_RC_NO_OPT_FILE Optionsdatei 'Dateiname' konnte nicht gefunden werden oder kann nicht gelesen werden.
- 0408 E
  DSM_RC_MACHINE_SAME Ein virtueller Knotenname darf nicht gleich einem Knotennamen oder dem Systemhostnamen sein.
- 0409 E
  DSM_RC_INVALID_SERVER Servername in Systemoptionsdatei nicht gefunden
- 0410 E
  DSM_RC_INVALID_KEYWORD Bei der Syntaxanalyse wurde ein ungültiges Optionsschlüsselwort gefunden.
- 0411 S
  DSM_RC_PATTERN_TOO_COMPLEX Das Einschluss- oder Ausschlussmuster kann nicht syntaktisch analysiert werden.
- 0412 S
  DSM_RC_NO_CLOSING_BRACKET Im Einschluss-/Ausschlussmuster fehlt eine rechte eckige Klammer
- 0426 E
  DSM_RC_CANNOT_OPEN_TRACEFILE Die Initialisierungsfunktionen können die angegebene Ablaufverfolgungsdatei nicht öffnen.
- 0427 E
  DSM_RC_CANNOT_OPEN_LOGFILE Die Initialisierungsfunktionen können die angegebene Fehlerprotokolldatei nicht öffnen.
- 0600 E
  DSM_RC_DUP_LABEL Doppelter Datenträgerkennsatz vorhanden. Die Operation kann nicht fortgesetzt werden.
- 0601 E
  DSM_RC_NO_LABEL Das Laufwerk hat keinen Kennsatz. Die Operation kann nicht fortgesetzt werden.
- 0610 E
  DSM_RC_NLS_CANT_OPEN_TXT Nachrichtentextdatei kann nicht geöffnet werden.

- 0611 E
  DSM_RC_NLS_CANT_READ_HDR Nachrichtentextdatei kann nicht verwendet werden.
- 0612 E
  DSM_RC_NLS_INVALID_CNTL_REC Nachrichtentextdatei kann nicht verwendet werden.
- 0613 E
  DSM_RC_NLS_INVALID_DATE_FMT Ungültigen Wert für DATEFORMAT angegeben.
- 0614 E
  DSM_RC_NLS_INVALID_TIME_FMT Ungültigen Wert für TIMEFORMAT angegeben.
- 0615 E
  DSM_RC_NLS_INVALID_NUM_FMT Ungültigen Wert für NUMBERFORMAT angegeben.
- 0620 E
  DSM_RC_LOG_CANT_BE_OPENED Fehlerprotokolldatei kann nicht geöffnet werden.
- 0621 E
  DSM_RC_LOG_ERROR_WRITING_TO_LOG In die Protokolldatei kann nicht geschrieben werden.
- 0622 E
  DSM_RC_LOG_NOT_SPECIFIED Der Name der Protokolldatei wurde nicht angegeben.
- 0927 E
  DSM_RC_NOT_ADSM_AUTHORIZED Nur ein berechtigter IBM Spectrum Protect-Benutzer kann diese Aktion ausführen.
- 961 E
  DSM_RC_DIRECT_STORAGE_AGENT_UNSUPPORTED Direktverbindung zum Speicheragenten ist nicht zulässig.
- 963 E
  DSM_RC_FS_NAMESPACE_DOWNLEVEL Der lange Namensbereich wurde aus dem lokalen Dateibereich entfernt. Wenn Sie die Operation zum Sichern/Archivieren fortsetzen wollen, müssen Sie Ihren Dateibereich auf dem Server umbenennen.
- 0996 E
  DSM_RC_SERVER_DOWNLEVEL_FUNC Der IBM Spectrum Protect-Server ist nicht auf dem neuesten Stand und unterstützt die angeforderte Funktion nicht. Das Fehlerprotokoll enthält die Versionsnummer.
- 0997 E
  DSM_RC_STORAGEAGENT_DOWNLEVEL Der IBM Spectrum Protect-Speicheragent ist nicht auf dem neuesten Stand und unterstützt die angeforderte Funktion nicht. Das Fehlerprotokoll enthält die Versionsnummer.
- 0998 E
  DSM_RC_SERVER_AND_SA_DOWNLEVEL Der IBM Spectrum Protect-Server und der IBM Spectrum Protect-Speicheragent sind nicht auf dem neuesten Stand und unterstützen nicht die angeforderte Funktion. Das Fehlerprotokoll enthält die Versionsnummer.
- 1376 E
  DSM_RC_DIGEST_VALIDATION_ERROR Fehler bei der Verarbeitung von 'DateibereichsnamePfadnameDateiname'; End-to-End-Digestprüfung ist fehlgeschlagen.
- 2000 E
  DSM_RC_NULL_OBJNAME Der Objektnamenzeiger ist NULL.
- 2001 E
  DSM_RC_NULL_DATABLKPTR Der Datenblockzeiger ist NULL.
- 2002 E
  DSM_RC_NULL_MSG Nachrichtenparameter für 'dsmRCMsg' ist ein Nullzeiger.
- 2004 E
  DSM_RC_NULL_OBJATTRPTR Der Objektattributzeiger ist NULL.
- 2006 E
  DSM_RC_NO_SESS_BLK Keine Informationen für Server-Sitzung vorhanden.
- 2007 E
  DSM_RC_NO_POLICY_BLK Keine Server-Maßnahmeninformationen vorhanden.
- 2008 E
  DSM_RC_ZERO_BUFLEN Der Wert für 'dataBlk bufferLen' ist Null.
- 2009 E
  DSM_RC_NULL_BUFPTR Der Wert für 'dataBlk bufferPtr' ist NULL.
- 2010 E
  DSM_RC_INVALID_OBJTYPE Der Wert für 'objType' ist ungültig.
- 2011 E
  DSM_RC_INVALID_VOTE Der Wert für 'dsmEndTxn' ist ungültig.
- 2012 E
  DSM_RC_INVALID_ACTION Die Aktualisierungsaktion ist ungültig.
- 2014 E
  DSM_RC_INVALID_DS_HANDLE Es ist ein Fehler in den internen IBM Spectrum Protect-API-Prozeduren aufgetreten.
- 2015 E
  DSM_RC_INVALID_REPOS Die Repository-Art ist ungültig.
- 2016 E
  DSM_RC_INVALID_FSNAME Dateibereichsname muß mit dem Verzeichnisbegrenzer beginnen.
- 2017 E
  DSM_RC_INVALID_OBJNAME Objektname ist entweder leer oder hat keinen führenden Begrenzer.
- 2018 E
  DSM_RC_INVALID_LLNAME Untergeordnetes Qualifikationsmerkmal des Objektnamens muß mit dem Verzeichnisbegrenzer beginnen.

- 2019 E
  DSM_RC_INVALID_OBJOWNER Der Objekteigner ist ungültig.
- 2020 E
  DSM_RC_INVALID_ACTYPE Der Wert für 'dsmBindMC sendType' ist ungültig.
- 2021 E
  DSM_RC_INVALID_RETCODE Kein Text für diesen Rückkehrcode verfügbar.
- 2022 E
  DSM_RC_INVALID_SENDTYPE Der Wert für 'dsmSendObj sendType' ist ungültig.
- 2023 E
  DSM_RC_INVALID_PARAMETER Der Wert für 'dsmDeleteObj delType' ist ungültig.
- 2024 E
  DSM_RC_INVALID_OBJSTATE Der Wert für 'qryBackupData objState' ist ungültig.
- 2025 E
  DSM_RC_INVALID_MCNAME Der Name der Verwaltungsklasse wurde nicht gefunden.
- 2026 E
  DSM_RC_INVALID_DRIVE_CHAR Der Laufwerkbuchstabe ist kein alphabetisches Zeichen.
- 2027 E
  DSM_RC_NULL_FSNAME Der Wert für 'Dateibereichsname registrieren' ist NULL.
- 2028 E
  DSM_RC_INVALID_HLNAME Übergeordnetes Qualifikationsmerkmal des Objektnamens muß mit dem Verzeichnisbegrenzer beginnen.
- 2029 E
  DSM_RC_NUMOBJ_EXCEED Die Anzahl Objekte in 'dsmBeginGetData' überschreitet DSM_MAX_GET_OBJ | DSM_MAX_PARTIAL_GET_OBJ.
- 2030 E
  DSM_RC_NEWPW_REQD Der Wert für das neue Kennwort ist NULL oder leer.
- 2031 E
  DSM_RC_OLDPW_REQD Der Wert für das alte Kennwort ist NULL oder leer.
- 2032 E
  DSM_RC_NO_OWNER_REQD In dsmInit darf der Eigner bei PASSWORDACCESS=generate keine Sitzung aufbauen.
- 2033 E
  DSM_RC_NO_NODE_REQD In 'dsmInit' ist die Angabe des Knotens nicht zulässig, wenn PASSWORDACCESS=generate.
- 2034 E
  DSM_RC_KEY_MISSING Die Schlüsseldatei fehlt.
- 2035 E
  DSM_RC_KEY_BAD Der Inhalt der Schlüsseldatei ist ungültig.
- 2041 E
  DSM_RC_BAD_CALL_SEQUENCE Die Reihenfolge der Aufrufe ist ungültig.
- 2042 E
  DSM_RC_INVALID_TSMBUFFER tsmBuffHandle ist ungültig oder der Wert von dataPtr ist ungültig.
- 2043 E
  DSM_RC_TOO_MANY_BYTES Die Anzahl Byte, die in den tsmBuffer kopiert wurden, ist größer als der zulässige Wert.
- 2044 E
  DSM_RC_MUST_RELEASE_BUFFER dsmTerminate kann nicht beendet werden, da die Anwendung an 1 oder mehreren tsmBuffers festhält.
- 2045 E
  DSM_RC_BUFF_ARRAY_ERROR Interner Fehler im tsmBuffer-Bereich.
- 2046 E
  DSM_RC_INVALID_DATABLK Bei Verwendung von useTsmBuffers muss dataBlk in Aufrufen von dsmSendObj und dsmGetObj NULL sein.
- 2047 E
  DSM_RC_ENCR_NOT_ALLOWED Verschlüsselung ist bei Verwendung von useTsmBuffers nicht zulässig.
- 2048 E
  DSM_RC_OBJ_COMPRESSED Dieses Objekt kann nicht mit useTsmBuffers zurückgeschrieben/abgerufen werden, da es komprimiert ist.
- 2049 E
  DSM_RC_OBJ_ENCRYPTED Dieses Objekt kann nicht mit useTsmBuffers zurückgeschrieben/abgerufen werden, da es verschlüsselt ist.
- 2050 E
  DSM_RC_WILDCHAR_NOTALLOWED In 'dsmSendObj' sind für 'objName' keine Platzhalterzeichen zulässig.
- 2051 E
  DSM_RC_POR_NOT_ALLOWED Bei Verwendung von useTsmBuffers ist ein Zurückschreiben/Abrufen mit Teilobjektzurückschreibung nicht zulässig.
- 2052 E
  DSM_RC_NO_ENCRYPTION_KEY Kein Chiffrierschlüssel gefunden. Bei Verwendung von -encryptkey=prompt müssen Sie sicherstellen, dass das Feld encryptionPasswordP einen Wert aufweist und dass bEncryptKeyEnabled auf wahr gesetzt ist.
- 2053 E
  DSM_RC_ENCR_CONFLICT Es wurden unverträgliche Chiffrierschlüsseloptionen angegeben.
- 2060 E
  DSM_RC_FSNAME_NOTFOUND Der Dateibereich, der gelöscht/dessen Zugriff definiert werden soll, kann nicht gefunden werden.
- 2061 E
  DSM_RC_FS_NOT_REGISTERED In 'dsmSendObj', 'dsmDeleteObj' oder 'dsmUpdateFS' ist der Dateibereich nicht registriert.

- 2062 W
  DSM_RC_FS_ALREADY_REGED In 'dsmRegisterFS' ist der Dateibereich bereits registriert.
- 2063 E
  DSM_RC_OBJID_NOTFOUND In 'dsmBeginGetData' ist die 'objID' NULL.
- 2064 E
  DSM_RC_WRONG_VERSION In 'dsmInit' weicht die API-Version des aufrufenden Programms von der IBM Spectrum Protect-Bibliotheksversion ab.
- 2065 E
  DSM_RC_WRONG_VERSION_PARM Die Strukturversion des aufrufenden Programms weicht von der IBM Spectrum Protect-Bibliotheksversion ab.
- 2070 E
  DSM_RC_NEEDTO_ENDTXN 'dsmEndTxn' ausgeben und dann eine neue Transaktionssitzung beginnen.
- 2080 E
  DSM_RC_OBJ_EXCLUDED Das Sicherungs- oder Archivierungsobjekt ist von der Verarbeitung ausgeschlossen.
- 2081 E
  DSM_RC_OBJ_NOBCG Das Sicherungsobjekt hat keine Kopiengruppe.
- 2082 E
  DSM_RC_OBJ_NOACG Das Archivierungsobjekt hat keine Kopiengruppe.
- 2090 E
  DSM_RC_APISYSTEM_ERROR Der von der IBM Spectrum Protect-API verwendete Speicher wurde beschädigt.
- 2100 E
  DSM_RC_DESC_TOOLONG Die 'sendObj'-Archivierungsbeschreibung ist zu lang.
- 2101 E
  DSM_RC_OBJINFO_TOOLONG 'sendObj ObjAttr.objInfo' ist zu lang.
- 2102 E
  DSM_RC_HL_TOOLONG 'sendObj dsmObjName.hl' ist zu lang.
- 2103 E
  DSM_RC_PASSWD_TOOLONG Das Kennwort oder die Zeichenfolge für encryptionPassword ist zu lang.
- 2104 E
  DSM_RC_FILESPACE_TOOLONG 'sendObj dsmObjName.fs' ist zu lang.
- 2105 E
  DSM_RC_LL_TOOLONG 'sendObj dsmObjName.ll' ist zu lang.
- 2106 E
  DSM_RC_FSINFO_TOOLONG In 'RegisterFS' oder 'UpdateFS' ist 'fsInfo' der Dateisystemattribute zu lang.
- 2107 E
  DSM_RC_SENDDATA_WITH_ZERO_SIZE Daten mit einer Größenschätzung von Null Byte können nicht gesendet werden.
- 2110 E
  DSM_RC_INVALID_ACCESS_TYPE Die Zugriffsart dsmSetAccess ist ungültig.
- 2111 E
  DSM_RC_QUERY_COMM_FAILURE Übertragungsfehler mit Server bei Objektabfrage
- 2112 E
  DSM_RC_NO_FILES_BACKUP Für diesen Dateinamen/Dateibereich wurden noch keine Dateien gesichert.
- 2113 E
  DSM_RC_NO_FILES_ARCHIVE Für diesen Dateinamen/Dateibereich wurden noch keine Dateien archiviert.
- 2114 E
  DSM_RC_INVALID_SETACCESS Ungültiges Format für Befehl SET ACCESS.
- 2120 E
  DSM_RC_STRING_TOO_LONG Die folgende Nachricht war für die Protokollierung auf dem Server zu lang: 'Gekürzte Nachricht mit Nachrichtennummer'
- 2200 I
  DSM_RC_MORE_DATA In 'dsmGetNextQObj' oder 'dsmGetData' sind weitere Daten verfügbar.
- 2210 E
  DSM_RC_BUFF_TOO_SMALL Der 'dataBlk'-Puffer ist für die Abfrageantwort zu klein.
- 2228 E
  DSM_RC_NO_API_CONFIGFILE Die in 'dsmInit' angegebene Konfigurationsdatei kann nicht geöffnet werden.
- 2229 E
  DSM_RC_NO_INCLEXCL_FILE Die Datei mit Einschluß-/Ausschlußdefinitionen wurde nicht gefunden.
- 2230 E
  DSM_RC_NO_SYS_OR_INCLEXCL Entweder wurde die Datei dsm.sys nicht gefunden oder die in dsm.sys angegebene Einschluß-/Ausschlußdatei wurde nicht gefunden.
- 2231 E
  DSM_RC_REJECT_NO_POR_SUPPORT Abrufen partieller Objekte wird auf diesem Server nicht unterstützt.
- 2300 E
  DSM_RC_NEED_ROOT Nur ein UNIX-Root darf 'dsmChangePW' oder 'dsmDeleteFS' ausführen.
- 2301 E
  DSM_RC_NEEDTO_CALL_BINDMC 'dsmBindMC' muß vor 'dsmSendObj' ausgegeben werden.
- 2302 I
  DSM_RC_CHECK_REASON_CODE Der Wert für 'dsmEndTxn' lautet ABORT; das Feld für den Grund überprüfen.

- 2400 E
  DSM_RC_ALMGR_OPEN_FAIL Lizenzdatei konnte nicht geöffnet werden.
- 2401 E
  DSM_RC_ALMGR_READ_FAIL Lesefehler bei Lizenzdatei.
- 2402 E
  DSM_RC_ALMGR_WRITE_FAIL Schreibfehler bei Lizenzdatei.
- 2403 E
  DSM_RC__ALMGR_DATA_FMT Daten in der Lizenzdatei haben ungültiges Format.
- 2404 E
  DSM_RC_ALMGR_CKSUM_BAD Die Kontrollsumme in der Lizenzdatei stimmt nicht mit der Zeichenfolge der Lizenzregistrierung überein.
- 2405 E
  DSM_RC_ALMGR_TRIAL_EXPRD Abgelaufene Testlizenz.
- 4580 E
  DSM_RC_ENC_WRONG_KEY Fehler bei der Verarbeitung von 'DateibereichsnamePfadnameDateiname'; ungültiger Verschlüsselungsschlüssel.
- 4582 E
  DSM_RC_ENC_NOT_AUTHORIZED Benutzer ist zum Verschlüsseln von DateibereichsnameVerzeichnispfadDateiname nicht berechtigt.
- 4584 E
  DSM_RC_ENC_TYPE_UNKOWN Fehler bei der Verarbeitung von 'DateibereichsnamePfadnameDateiname': Verschlüsselungstyp nicht unterstützt.
- 4600 E
  DSM_RC_CLUSTER_INFO_LIBRARY_NOT_LOADED CLUSTERNODE ist auf YES gesetzt, aber der Clusterinformationsdämon wurde nicht gestartet.
- 4601 E
  DSM_RC_CLUSTER_LIBRARY_INVALID CLUSTERNODE ist auf YES gesetzt, aber die Clusterladebibliothek ist ungültig.
- 4602 E
  DSM_RC_CLUSTER_LIBRARY_NOT_LOADED CLUSTERNODE ist auf YES gesetzt, aber die Cluster-Software ist auf diesem System nicht verfügbar.
- 4603 E
  DSM_RC_CLUSTER_NOT_MEMBER_OF_CLUSTER CLUSTERNODE ist auf YES gesetzt, aber diese Maschine ist nicht Teil eines Clusters.
- 4604 E
  DSM_RC_CLUSTER_NOT_ENABLED CLUSTERNODE ist auf YES gesetzt, aber der Cluster-Service ist auf diesem System nicht aktiviert.
- 4605 E
  DSM_RC_CLUSTER_NOT_SUPPORTED Die Option CLUSTERNODE wird auf diesem System nicht unterstützt.
- 4606 E
  DSM_RC_CLUSTER_UNKNOWN_ERROR Unerwarteter Fehler (Rückkehrcode) beim Versuch des Programms, den Clusternamen vom System abzurufen.
- 5200 E
  DSM_RC_ABORT_CERTIFICATE_NOT_FOUND Der ferne Knoten ist auf dem IBM Spectrum Protect-Server nicht korrekt konfiguriert.
- 5702 E
  DSM_RC_PROXY_REJECT_NO_RESOURCES Proxy zurückgewiesen: Der IBM Spectrum Protect-Server verfügt nicht mehr über genügend Speicher.
- 5705 E
  DSM_RC_PROXY_REJECT_DUPLICATE_ID Proxy zurückgewiesen: Die Optionen ASNODENAME und NODENAME haben denselben Wert.
- 5710 E
  DSM_RC_PROXY_REJECT_ID_IN_USE Proxy zurückgewiesen: Der Knotenname, den Sie in der Option ASNODENAME angegeben haben, ist gesperrt.
- 5717 E
  DSM_RC_PROXY_REJECT_INTERNAL_ERROR Proxy zurückgewiesen: Der Server hat einen internen Fehler.
- 5722 E
  DSM_RC_PROXY_REJECT_NOT_AUTHORIZED Proxy zurückgewiesen: Diesem Knoten wurde keine Proxy-Berechtigung erteilt.
- 5746 E
  DSM_RC_PROXY_INVALID_FROMNODE Die Option ASNODENAME ist mit der Option FROMNODE nicht gültig.
- 5748 E
  DSM_RC_PROXY_INVALID_CLUSTER Die Option ASNODENAME kann nicht mit der Option CLUSTERNODE verwendet werden.
- 5749 E
  DSM_RC_PROXY_INVALID_FUNCTION Die versuchte Operation kann mit der Option ASNODENAME nicht aufgerufen werden.
- 5801 E
  DSM_RC_CRYPTO_ICC_ERROR Unerwarteter Fehler in der Kryptografiebibliothek.

-452 E DSM_RC_SHM_NOTAUTH Unzureichende Berechtigung für Verbindung mit Shared Memory-Region

Erläuterung

Der Benutzer, der den Befehl ausgibt, ist nicht berechtigt, eine Verbindung zum Shared Memory-Segment herzustellen. Wenn das Shared Memory-Segment vom Server erstellt wird, ist dessen Eigner die gültige Benutzer-ID des Server-Prozesses (dsmserv). Nur Prozesse, die unter dieser Benutzer-ID oder dem Root ausgeführt werden, können eine Verbindung zu dem Segment (und folglich zu dem Server) herstellen.

Systemaktion

Die Sitzung wird zurückgewiesen und die Verarbeitung gestoppt.

Benutzeraktion

Falls möglich, den Befehl unter der Benutzer-ID des Prozesses ausführen, der dsmserv ausführt. Andernfalls für weitergehende Hilfe den Systemadministrator verständigen.

-451 E DSM_RC_SHM_FAILURE Fehler bei Verwendung des Shared-Memory-Protokolls

Erläuterung

Beim Lesen oder Schreiben von Daten unter Verwendung des Shared-Memory-Übertragungsprotokolls ist ein Fehler aufgetreten.

Systemaktion

IBM Spectrum Protect kann die angeforderte Operation nicht ausführen.

Benutzeraktion

Das Ablaufverfolgungsprotokoll auf zusätzliche Informationen überprüfen und die Operation wiederholen. Bleibt der Fehler bestehen, für weitergehende Hilfe den Systemadministrator verständigen.

-450 E DSM_RC_SHM_TCPIP_FAILURE Sitzung zurückgewiesen: TCP/IP-Verbindungsfehler für Shared Memory

Erläuterung

Der Versuch, mit Hilfe des Shared Memory-Protokolls eine Verbindung zum lokalen Server herzustellen, ist während der anfänglichen TCP/IP-Übertragung fehlgeschlagen. Dieser Fehler kann auftreten, wenn der Server an dem korrekten Anschluß nicht empfangsbereit ist oder der Server nicht aktiv ist.

Systemaktion

Die Sitzung wurde zurückgewiesen. Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation oder warten Sie, bis der Server wieder aktiv ist, und wiederholen Sie dann die Operation. Bleibt der Fehler bestehen, für weitergehende Hilfe den Systemadministrator verständigen.

-190 E DSM_RC_NP_ERROR Sitzung zurückgewiesen: Verbindungsfehler mit benannten Pipes.

Erläuterung

Der Versuch, mit Hilfe der Übertragung durch benannte Pipes eine Verbindung zum Server herzustellen, ist fehlgeschlagen. Dieser Fehler kann auftreten, wenn in den Optionsdateien ein falscher Name für benannte Pipes (NAMEDPIPENAME) angegeben wurde oder wenn der Systemadministrator eine Sicherungsoperation abgebrochen hat.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation oder warten Sie, bis der Server wieder aktiv ist, und wiederholen Sie dann die Operation. Sicherstellen, daß der in der Option NAMEDPIPENAME angegebene Wert derselbe ist wie der, der vom Server verwendet wird. Bleibt der Fehler bestehen, für weitergehende Hilfe den Systemadministrator verständigen.

-057 E DSM_RC_TCPIP_LOADFAILURE Die TCP/IP-Ladefunktion ist fehlgeschlagen.

Erläuterung

Beim Lokalisieren einer Funktion ist ein Fehler aufgetreten. Die TCP/IP-Ladefunktion ist fehlgeschlagen.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Die TCP/IP-Installation überprüfen.

-056 E DSM_RC_TCPIP_DLL_LOADFAILURE Fehler beim Laden einer Bibliothek aufgetreten.

Erläuterung

Beim Laden einer Bibliothek ist ein Fehler aufgetreten. Das Laden der TCP/IP-DLL ist fehlgeschlagen.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Die TCP/IP-Installation überprüfen.

-055 E DSM_RC_WINSOCK_MISSING Die TCP/IP-Datei WINSOCK.DLL kann nicht gefunden werden.

Erläuterung

Die TCP/IP-Datei WINSOCK.DLL kann nicht gefunden werden.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Die TCP/IP-Installation überprüfen.

-054 E DSM_RC_NETWORK_UNREACHABLE Der angegebene TCP/IP-Host-Name ist nicht erreichbar

Erläuterung

Der in der Anweisung TCPSERVERADDRESS angegebene Host-Name ist nicht erreichbar.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Prüfen, ob die Optionsdatei die korrekte Anweisung TCPSERVERADDRESS enthält. Den Administrator nach dem korrekten Namen des Servers fragen.

-053 E DSM_RC_BAD_HOST_NAME Es wurde eine ungültige TCP/IP-Adresse angegeben.

Erläuterung

Die durch die Einstellung TCPSERVERADDRESS des IBM Spectrum Protect-Clients angegebene TCP/IP-Adresse wurde im Netz nicht gefunden. Allgemeine Ursachen für diesen Fehler sind:

- Die Clientoption TCPSERVERADDRESS gibt die falsche TCP/IP-Adresse für den IBM Spectrum Protect-Server an.
- Die Maschine, die als Host für den IBM Spectrum Protect-Server dient, befindet sich nicht im Netz.
- Ein Netzproblem verhindert, dass der IBM Spectrum Protect-Client die Maschine erreicht, die als Host für den IBM Spectrum Protect-Server dient.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Prüfen Sie, ob die Einstellungen für TCPSERVERADDRESS und TCPPORT die korrekten Werte für Ihren IBM Spectrum Protect-Server aufweisen. Verwenden Sie das Pingsignal oder ein ähnliches Dienstprogramm Ihres Betriebssystems, um sicherzustellen, dass Ihre Maschine die Maschine, die als Host für den IBM Spectrum Protect-Server dient, im Netz finden kann. Wiederholen Sie die Operation. Bleibt der Fehler bestehen, bitten Sie Ihren IBM Spectrum Protect-Administrator um weitere Unterstützung.

-052 E DSM_RC_CONN_REFUSED Versuch, eine TCP/IP-Verbindung herzustellen, vom Host zurückgewiesen

Erläuterung

Der Versuch, eine TCP/IP-Verbindung herzustellen, wurde vom Server zurückgewiesen.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Der Server war nicht vollständig initialisiert, ist gerade nicht aktiv, war nicht für TCP/IP-Übertragung aktiviert, oder es wurde eine falsche TCP/IP-Anschlußnummer angegeben. Bleibt der Fehler bestehen, den Systemadministrator verständigen.

-051 E DSM_RC_CONN_TIMEDOUT Beim Versuch, eine TCP/IP-Verbindung aufzubauen, wurde das zulässige Zeitlimit überschritten, bevor die Verbindung zustande kam.

Erläuterung

Das Objekt des Verbindungsversuchs hat nicht innerhalb der zulässigen Wartezeit geantwortet. Beim Client für Sichern/Archivieren geht dieser Nachricht in der Datei dsmerror.log die Nachricht ANS5216E voran, die Details zu der Verbindung enthält, die fehlgeschlagen ist. Die Bedingung kann eine temporäre Bedingung sein.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

- Starten Sie den IBM Spectrum Protect-Client erneut und wiederholen Sie die Operation.
- Überprüfen Sie die Clientoptionsdatei und prüfen Sie, ob TCPSERVERADDRESS und TCPPORT die korrekte TCP/IP-Adresse und Anschlussnummer für Ihren IBM Spectrum Protect-Server angeben.
- Prüfen Sie, ob Netzkonnektivität zwischen der IBM Spectrum Protect-Clientmaschine und der IBM Spectrum Protect-Servermaschine besteht.
- Bleibt der Fehler bestehen, bitten Sie Ihren IBM Spectrum Protect-Administrator um weitere Unterstützung.

-050 E DSM_RC_TCPIP_FAILURE Sitzung zurückgewiesen: TCP/IP-Verbindungsfehler.

Erläuterung

Der Versuch, eine Verbindung zum Server unter Verwendung der TCP/IP-Übertragung herzustellen, ist fehlgeschlagen. Dies kann ein Ergebnis falscher TCP/IP-Optionseinstellungen in Ihrer Clientoptionsdatei sein. Dieser Fehler kann auch auftreten, wenn die LAN-Verbindung unterbrochen wurde oder Ihr Systemadministrator eine Sicherungsoperation abgebrochen hat.

Systemaktion

Die Sitzung wurde zurückgewiesen. Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation oder warten Sie, bis der Server wieder aktiv ist, und wiederholen Sie dann die Operation. Bleibt der Fehler bestehen, für weitergehende Hilfe den Systemadministrator verständigen.

0000 I DSM_RC_OK Erfolgreich beendet.

Erläuterung

Die Operation wurde erfolgreich ausgeführt.

Systemaktion

Keine.

Benutzeraktion

Keine.

0001 E DSM_RC_ABORT_SYSTEM_ERROR Diese Operation kann aufgrund eines Fehlers auf dem IBM Spectrum Protect-Server nicht fortgesetzt werden. Bitten Sie Ihren IBM Spectrum Protect-Serveradministrator um Unterstützung.

Erläuterung

Der IBM Spectrum Protect-Server hat eine Fehlerbedingung festgestellt, die die Fortsetzung der IBM Spectrum Protect-Clientoperation verhindert. Ihr IBM Spectrum Protect-Serveradministrator kann das IBM Spectrum Protect-Serveraktivitätenprotokoll auf weitere Details zu dem Fehler überprüfen.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Bitten Sie Ihren IBM Spectrum Protect-Serveradministrator um Unterstützung. Der Administrator kann das IBM Spectrum Protect-Serveraktivitätenprotokoll auf weitere Informationen zu den Bedingungen überprüfen, die zu diesem Fehler geführt haben.

0002 E DSM_RC_ABORT_NO_MATCH Keine Objekte auf dem Server stimmen mit der Abfrage überein

Erläuterung

Keine Objekte auf dem Server stimmen mit der ausgeführten Abfrageoperation überein. Wenn dieses Objekt Teil eines auf einem Knoten generierten Sicherungssatzes ist und der Knotenname auf dem Server geändert wird, stimmen keine Sicherungssatzobjekte, die vor der Namensänderung generiert wurden, mit dem neuen Knotennamen überein.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Sicherstellen, dass die Namen richtig eingegeben wurden. Wenn das Objekt Teil eines Sicherungssatzes ist, der vor einer Knotennamensänderung generiert wurde, müssen Sie sicherstellen, dass der Knotenname derselbe ist wie für den Knoten, für den der Sicherungssatz generiert wurde.

0003 E DSM_RC_ABORT_BY_CLIENT Client hat Transaktion beendet

Erläuterung

Das Clientsystem hat die Operation mit dem Server sowie die aktuelle Transaktion beendet.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Die Sitzung erneut starten.

0004 W DSM_RC_ABORT_ACTIVE_NOT_FOUND Es konnte keine aktive Sicherungsversion gefunden werden.

Erläuterung

Es wurde versucht, ein Objekt als verfallen zu markieren, aber der IBM Spectrum Protect-Server konnte keine aktive Sicherungsversion des Objekts finden. Dieser Nachricht geht die Nachricht ANS1228E voraus, die den Objektnamen angibt.

Diese Nachricht könnte beispielsweise ausgegeben werden, wenn zwei separate Clientprozesse gleichzeitig dasselbe Dateisystem sichern. Wenn einer der beiden Prozesse eine Datei als verfallen markiert, versetzt der IBM Spectrum Protect-Server diese Datei in den inaktiven Status. Wenn der zweite Prozess nachfolgend versucht, dieselbe Datei als verfallen zu markieren, wird der IBM Spectrum Protect-Server keine aktive Version der Datei finden, sodass der zweite Prozess diese Nachricht für diese Datei ausgibt.

Systemaktion

Das Objekt wird nicht als verfallen markiert. Die Verarbeitung wird mit dem nächsten Objekt fortgesetzt.

Benutzeraktion

- Prüfen Sie die Konsolausgabe, das Planungsprotokoll oder das Fehlerprotokoll und suchen Sie die Nachricht ANS1228E, die dieser Nachricht unmittelbar vorangeht. ANS1228E identifiziert das Objekt, das nicht als verfallen markiert werden konnte.
- Untersuchen Sie die Umstände, unter denen der Fehler aufgetreten ist, und bewerten Sie, ob diese Umstände das Vorkommen dieser Nachricht erklären. Beispiel: Diese Nachricht könnte angezeigt werden, wenn mehrere Instanzen des Clients versuchen würden, das

Dateisystem gleichzeitig zu sichern.

- Falls die Ursache für das Auftreten dieser Nachricht nicht bestimmt werden kann und die Nachricht auftritt, wenn die Operation wiederholt wird, bitten Sie den IBM Support um Unterstützung. Versuchen Sie außerdem, für diese Nachrichtennummer unter http://www.ibm.com nach möglichen Lösungen zu suchen.

0005 E DSM_RC_ABORT_NO_DATA Der IBM Spectrum Protect-Server hat keine Daten für das Objekt.

Erläuterung

IBM Spectrum Protect hat versucht, eine Zurückschreibung oder einen Abruf für ein Objekt durchzuführen, dem keine Daten zugeordnet sind. Falls eine Fehlerberichtigung möglich ist, liegt sie beim IBM Spectrum Protect-Server.

Systemaktion

IBM Spectrum Protect beendet die aktuelle Operation.

Benutzeraktion

Bitten Sie den IBM Spectrum Protect-Administrator, das IBM Spectrum Protect-Aktivitätenprotokoll auf alle für diesen Fehler relevanten Nachrichten zu überprüfen, die zur Ermittlung des Problems beitragen könnten.

0006 E DSM_RC_ABORT_BAD_VERIFIER Sie haben ein falsches Kennwort eingegeben.

Erläuterung

Sie haben ein falsches aktuelles Kennwort eingegeben oder Sie haben ein neues Kennwort eingegeben, das nicht die auf dem Server definierten Kennwortlängenvoraussetzungen erfüllt.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Wiederholen Sie die Sitzung mit dem korrekten Kennwort. Falls dies fehlschlägt oder Sie Ihr Kennwort vergessen haben, bitten Sie den IBM Spectrum Protect-Administrator, ein neues Kennwort zuzuordnen.

0007 E DSM_RC_ABORT_NODE_IN_USE Knoten bereits im Gebrauch

Erläuterung

Der Knoten, auf dem das System läuft, ist bereits durch eine andere Operation auf dem Server im Gebrauch. Dies kann durch einen anderen Client oder durch Aktivitäten auf dem Server verursacht werden.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Die Operation später wiederholen oder den Systemadministrator verständigen, um zu erfahren, welche anderen Operationen für den Benutzerknoten ausgeführt werden.

0008 E DSM_RC_ABORT_EXPDATE_TOO_LOW Verfallsdatum muß später als das heutige Datum sein

Erläuterung

Das Verfallsdatum für Archivierung muss nach dem heutigen Datum liegen.

Systemaktion

IBM Spectrum Protect hat die aktuelle Operation abgebrochen.

Benutzeraktion

Die Archivierung der Datei mit einem Verfallsdatum, das nach dem heutigen Datum liegt, wiederholen.

0009 W DSM_RC_ABORT_DATA_OFFLINE Die angeforderten Daten sind offline.

Erläuterung

Für die Zurückschreibungs- oder Abrufoperation müssen eine bzw. mehrere der angeforderten Dateien von Offline-Speicherdatenträgern (im allgemeinen Bänder) zurückgerufen werden. Die Wartezeit hängt von den Offline-Speicherverwaltungsmaßnahmen am Standort ab.

Systemaktion

IBM Spectrum Protect wartet, bis Offlinespeichermedien verfügbar werden, und setzt danach die Verarbeitung fort.

Benutzeraktion

Keine.

0010 E DSM_RC_ABORT_EXCLUDED_BY_SIZE Objekt für Server-Begrenzungen zu groß

Erläuterung

Das Objekt ist zu groß. Die Server-Konfiguration verfügt über keinen Datenspeicherbereich, der das Objekt akzeptiert.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Den Systemadministrator verständigen, um die maximale Dateigröße (Objektgröße) zu bestimmen, für die der Server an diesem Standort konfiguriert ist.

0011 E DSM_RC_ABORT_NO_REPOSIT_SPACE Server hat keinen Datenspeicherbereich mehr

Erläuterung

Der Server hat keinen Speicherbereich mehr verfügbar, um das Objekt zu speichern.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Sie können eine der folgenden Aktionen durchführen:

- Bitten Sie den Systemadministrator, dem Speicherpool Speicherbereich hinzuzufügen.

- Setzen Sie für den IBM Spectrum Protect-Client COMPRESSALWAYS=NO und COMPRESSIon=YES in der Optionsdatei (DSM.OPT), dann wird die Datei in dekomprimiertem Zustand erneut gesendet, wenn sie während der Komprimierung anwächst.
- Bei API-Anwendungen sollten Sie in der Dokumentation der Anwendung nachschlagen, um Empfehlungen in Bezug auf Komprimierung zu erhalten.
- Das Platten-Caching im Plattenspeicherpool ausschalten und bei jedem Plattenpooldatenträger den Befehl MOVE DATA eingeben, um die Cache-Bitdateien zu löschen.

0012 E DSM_RC_ABORT_MOUNT_NOT_POSSIBLE Laden von Serverdatenträgern nicht möglich

Erläuterung

Das Laden von Serverdatenträgern ist nicht möglich. Beim Warten auf das Laden eines Offline-Datenträgers ist es beim Server zu einer Zeitlimitüberschreitung gekommen.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Operation später wiederholen, wenn die Serverdatenträger geladen werden können. Stellen Sie sicher, dass der Parameter MAXNUMMP (maximale Anzahl Mount-Punkte), der auf dem Server für diesen Knoten definiert ist, größer als 0 ist.

0013 E DSM_RC_ABORT_SIZESTIMATE_EXCEED Größenschätzung überschritten

Erläuterung

Die Gesamtmenge der Daten für eine Sicherungs- oder Archivierungsoperation überschreitet die geschätzte Menge, die ursprünglich an den Server zwecks Zuordnung von Datenspeicherbereich gesendet wurde. Dies geschieht, wenn viele Dateien übermäßig anwachsen, während die Sicherungs- oder Archivierungsoperation ausgeführt wird.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, überprüfen, welche anderen Prozesse auf der Client-Maschine laufen, die große Datenmengen generieren. Diese Operationen inaktivieren, während die Sicherungs- oder Archivierungsoperation ausgeführt wird.

0014 E DSM_RC_ABORT_DATA_UNAVAILABLE Dateidaten derzeit auf dem Server nicht verfügbar

Erläuterung

Die Dateidaten sind derzeit auf dem Server nicht verfügbar. Es wurde versucht, eine Zurückschreibungs- oder Abrufoperation auszuführen. Mögliche Ursachen sind:

- Die Daten wurden auf dem Server beschädigt
- Der Server hat einen Lesefehler gefunden
- Die Datei ist vorübergehend von einer Zurückforderungsoperation auf dem Server betroffen
- Der Server forderte einen Banddatenträger an, der als nicht verfügbar markiert ist

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator verständigen, damit er den Fehler mit Hilfe der Server-Konsole oder des Aktivitätenprotokolls bestimmt. Überprüfen, ob ein Banddatenträger angefordert wurde, der nicht verfügbar ist. Ein Banddatenträger wurde möglicherweise als nicht verfügbar markiert, wenn früher Lesefehler aufgetreten sind oder der Datenträger dem Bandarchiv entnommen wurde.

0015 E DSM_RC_ABORT_RETRY Unerwartete Wiederholungsanforderung. Der IBM Spectrum Protect-Server hat beim Schreiben der Daten einen Fehler gefunden.

Erläuterung

Keine.

Systemaktion

Wenn die aktuelle Operation eine weitere Wiederholung unterstützt, unternimmt der Client einen erneuten Versuch, die Operation auszuführen. Andernfalls wird die Verarbeitung gestoppt.

Benutzeraktion

Keine.

0016 E DSM_RC_ABORT_NO_LOG_SPACE Der Server hat nicht genug Speicherbereich für das Wiederherstellungsprotokoll, um die aktuelle Operation fortzusetzen.

Erläuterung

Der Server hat keinen Speicherbereich mehr für das Wiederherstellungsprotokoll.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Dies ist ein temporärer Fehler. Die Operation später wiederholen oder den Systemadministrator verständigen.

0017 E DSM_RC_ABORT_NO_DB_SPACE Der Server hat nicht genug Speicher für den Datenbankbereich, um die aktuelle Operation fortzusetzen.

Erläuterung

Der Server hat keinen Speicher mehr für den Datenbankbereich.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0018 E DSM_RC_ABORT_NO_MEMORY Der Server hat nicht genug Speicher, um die aktuelle Operation fortzusetzen.

Erläuterung

Der Server hat keinen Speicher mehr.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Dies ist ein temporärer Fehler. Die Operation später wiederholen oder den Systemadministrator verständigen.

0020 E DSM_RC_ABORT_FS_NOT_DEFINED Der angegebene Dateibereich ist auf dem Server nicht vorhanden. Der Dateibereich wurde möglicherweise von einem anderen Client oder einem Administrator gelöscht.

Erläuterung

Der angegebene Dateibereich ist auf dem Server nicht vorhanden. Der Systemadministrator hat den Dateibereich bereits gelöscht, oder der Dateibereich wurde von einem anderen Client unter Verwendung des Knotennamens Ihres Clients gelöscht.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Den Dateibereichsnamen auf Korrektheit überprüfen und die Operation wiederholen.

0021 S DSM_RC_ABORT_NODE_ALREADY_DEFED Offene Registrierung fehlgeschlagen, da der angegebene Knotenname im Server definiert ist

Erläuterung

Die offene Registrierung ist fehlgeschlagen, da auf dem Server ein Knoten mit demselben Namen definiert ist.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Die Operation mit einem anderen Knotennamen wiederholen.

0022 S DSM_RC_ABORT_NO_DEFAULT_DOMAIN Offene Registrierung fehlgeschlagen, da keine Standarddomäne vorhanden ist.

Erläuterung

Die offene Registrierung ist fehlgeschlagen, da es keine Standardmaßnahmendomäne gibt, in die der Benutzer seinen Knoten stellen könnte.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0023 S DSM_RC_ABORT_INVALID_NODENAME Offene Registrierung fehlgeschlagen, da angegebener Knotenname ungültig ist

Erläuterung

Die offene Registrierung ist fehlgeschlagen, da der angegebene Knotenname ungültige Zeichen aufweist.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Die Operation mit einem anderen Knotennamen, der keine ungültigen Zeichen hat, wiederholen.

0024 S DSM_RC_ABORT_INVALID_POL_BIND Auf dem IBM Spectrum Protect-Server ist ein Maßnahmenverwaltungsfehler aufgetreten.

Erläuterung

Das Clientfehlerprotokoll und das Aktivitätenprotokoll des IBM Spectrum Protect-Servers enthalten möglicherweise weitere Informationen zu diesem Fehler.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, untersuchen Sie das Clientfehlerprotokoll und das Aktivitätenprotokoll des IBM Spectrum Protect-Servers auf weitere Informationen zu diesem Fehler. Kann der Fehler nicht behoben werden, fordern Sie einen SERVICE-Trace an, der den Fehler aufzeichnet, und bitten Sie die technische Unterstützung von IBM um Hilfe. Ihr IBM Spectrum Protect-Administrator kann Sie beim Konfigurieren des Trace unterstützen.

0024 E DSM_RC_ABORT_NO_INVALID_POL_BIND Ein Objekt in der Transaktion wurde an eine ungültige Verwaltungsklasse gebunden.

Erläuterung

Eines der Objekte in der Transaktion ist an eine Verwaltungsklasse gebunden, die nicht Teil der Maßnahme dieses Knotens ist, oder der Verwaltungsklassentyp wird für diese Version des Clients nicht unterstützt.

Systemaktion

Die aktuelle Operation wird beendet.

Benutzeraktion

Stellen Sie sicher, dass alle Objekte an eine gültige Verwaltungsklasse gebunden sind, oder aktualisieren Sie den Client auf die korrekte Versionsstufe.

0025 E DSM_RC_ABORT_DEST_NOT_DEFINED Serverfehler: Zielort nicht definiert.

Erläuterung

Serverfehler: Zielort nicht definiert.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Das Fehlerprotokoll vom Kundendienst überprüfen lassen.

0026 S DSM_RC_ABORT_WAIT_FOR_SPACE Der IBM Spectrum Protect-Server hat für diese Datei momentan keinen Speicher im Speicherpool. Dies ist möglicherweise ein temporärer Zustand.

Erläuterung

Diese Nachricht wird normalerweise ausgegeben, wenn der Speicherpool, in den die Daten gestellt werden, nicht über ausreichende Kapazität zum Speichern der Daten verfügt, der Speicher aber bald verfügbar sein wird. So kann z. B. eine Speicherpoolumlagerung ausreichend Kapazität zum Speichern der Daten freigeben.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Wiederholen Sie die Operation zu einem späteren Zeitpunkt. Schlägt dies fehl, verständigen Sie den IBM Spectrum Protect-Administrator und fordern Sie mehr Speicherpoolspeicherbereich an.

0027 E DSM_RC_ABORT_NOT_AUTHORIZEDDer Dateibereich kann nicht gelöscht werden, da dieser Knoten keine Berechtigung zum Löschen archivierter oder gesicherter Daten hat.

Erläuterung

Sie können die Dateibereichsdaten erst dann löschen, wenn Ihr IBM Spectrum Protect-Administrator Ihren Knoten dafür berechtigt hat. Die Berechtigung erlaubt Ihnen, Sicherungsdaten, Archivierungsdaten oder beide zu löschen.

Systemaktion

Die Operation zum Löschen schlägt fehl.

Benutzeraktion

Überprüfen Sie Ihre Berechtigung mit Hilfe des Befehls DSMC QUERY SESSION. Bitten Sie Ihren IBM Spectrum Protect-Administrator, die erforderliche Berechtigung zur Verfügung zu stellen oder den Dateibereich für Sie zu löschen.

0028 E DSM_RS_ABORT_RULE_ALREADY_DEFED Zugriffsregel '*Zugriffsregel*' für Knoten '*Knoten*' bereits definiert.
Alte Regel muss gelöscht werden, bevor neue definiert werden kann.

Erläuterung

Es wird versucht, eine Berechtigung für den angegebenen Knoten zu definieren, für den eine Berechtigung bereits definiert wurde.

Systemaktion

IBM Spectrum Protect hat die Berechtigung für den angegebenen Knoten nicht erneut definiert.

Benutzeraktion

Die Berechtigung aktualisieren, die alte Regel löschen und eine neue definieren oder die aktuelle Berechtigung verwenden.

0029 S DSM_RC_ABORT_NO_STOR_SPACE_STOP Server hat keinen Datenspeicherbereich mehr

Erläuterung

Der Server hat keinen Speicherbereich mehr verfügbar, um das Objekt zu speichern.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Dem Systemadministrator melden, dass ein Speicherpool auf dem Server voll ist.

0030 E DSM_RC_ABORT_LICENSE_VIOLATION Die Operation ist auf Grund von Serverlizenzwerten nicht gestattet.

Erläuterung

Der Knoten oder Benutzer versucht, eine Operation auszuführen, die entweder die Lizenzwerte überschreitet oder nicht lizenziert ist.

Systemaktion

Die Sitzung wird zurückgewiesen oder die Transaktion wird abgebrochen, wodurch die aktuelle Operation beendet wird.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0032 E DSM_RC_ABORT_DUPLICATE_OBJECT Ein doppeltes Objekt wurde gefunden, Operation kann nicht beendet werden.

Erläuterung

Ein doppeltes Objekt wurde gefunden, die Operation kann nicht beendet werden.

Systemaktion

Die angeforderte Operation ist fehlgeschlagen.

Benutzeraktion

Die Operation mit einer anderen Dateispezifikation wiederholen.

0033 E DSM_RC_ABORT_INVALID_OFFSET Wert für 'partialObjOffset' für Abrufen von partiellen Objekten ist ungültig.

Erläuterung

Der Wert für 'partialObjOffset' für das Abrufen von partiellen Objekten ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Einen gültigen Wert angeben.

0034 E DSM_RC_ABORT_INVALID_LENGTH Wert für 'partialObjLength' für Abrufen von partiellen Objekten ist ungültig.

Erläuterung

Der Wert für 'partialObjLength' für das Abrufen von partiellen Objekten ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Einen gültigen Wert angeben.

0036 E DSM_RC_END_NODE_NOT_AUTHORIZED Der Knoten oder Benutzer hat nicht die korrekte Berechtigung zum Ausführen dieser Operation.

Erläuterung

Der Knoten oder Benutzer hat nicht die korrekte Berechtigung zum Ausführen dieser Operation.

Systemaktion

Die Transaktion wird beendet.

Benutzeraktion

Überprüfen Sie die Berechtigung für das angegebene Objekt.

0041 E DSM_RC_ABORT_EXCEED_MAX_MP Dieser Knoten hat die maximale Anzahl Mountpunkte überschritten.

Erläuterung

Entweder sind für diese Operation keine Band- oder sequenzielle Plattenmountpunkte erlaubt oder die maximale Anzahl zulässiger Mountpunkte ist bereits im Gebrauch. Die Operation kann nicht ausgeführt werden. Der IBM Spectrum Protect-Administrator definiert die maximale Anzahl Mountpunkte mit der Eigenschaft MAXNUMMP Ihrer Knotendefinition.

Systemaktion

Das Objekt wird übersprungen.

Benutzeraktion

Wenn Sie weitere Operationen ausführen, die eventuell Mountpunkte verwenden, warten Sie, bis diese Operationen beendet sind, und wiederholen Sie dann die fehlgeschlagene Operation. Andernfalls bitten Sie Ihren IBM Spectrum Protect-Administrator um Unterstützung.

0045 E DSM_RC_ABORT_MERGE_ERROR Die angegebenen Objekte sind beim Mischtest fehlgeschlagen.

Erläuterung

Die angegebenen Objekte sind beim Mischtest fehlgeschlagen, die Operation kann nicht beendet werden.

Systemaktion

Die angeforderte Operation ist fehlgeschlagen.

Benutzeraktion

Die Dokumentation enthält Informationen über die Parameter für den Mischtest.

0047 E DSM_RC_ABORT_INVALID_OPERATIONUngültige Operation für Knoten versucht

Erläuterung

Die Operation ist nicht gültig.

Systemaktion

Die aktuelle Operation wurde beendet.

Benutzeraktion

Ihr Systemadministrator erteilt weitere Informationen.

0048 E DSM_RC_ABORT_STGPOOL_UNDEFINEDDer angegebene Zielspeicherpool ist nicht definiert.

Erläuterung

Der Speicherpool ist nicht definiert.

Systemaktion

Die aktuelle Operation wurde beendet.

Benutzeraktion

Ihr Systemadministrator erteilt weitere Informationen.

0049 E DSM_RC_ABORT_INVALID_DATA_FORMATEin Zielspeicherpool verfügt nicht über das korrekte Datenformat für die angegebene Knotenart.

Erläuterung

Keine.

Systemaktion

Die aktuelle Operation wurde beendet.

Benutzeraktion

Ihr Systemadministrator erteilt weitere Informationen.

0050 E DSM_RC_ABORT_DATAMOVER_UNDEFINEDKeine zugeordnete Einheit zum Versetzen von Daten ist für den angegebenen Knoten definiert.

Erläuterung

Keine.

Systemaktion

Die aktuelle Operation wurde beendet.

Benutzeraktion

Ihr Systemadministrator erteilt weitere Informationen.

0051 E DSM_RC_REJECT_NO_RESOURCES Sitzung zurückgewiesen: Alle Serversitzungen sind derzeit im Gebrauch

Erläuterung

IBM Spectrum Protect verwendet alle verfügbaren Sitzungen und kann momentan keine neue Sitzung akzeptieren.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator verständigen, damit er die Anzahl der gleichzeitig ablaufenden aktiven Sitzungen auf dem Server erhöht.

0052 E DSM_RC_REJECT_VERIFIER_EXPIRED Die Sitzung wird zurückgewiesen. Ihr Kennwort ist abgelaufen.

Erläuterung

Das Kennwort für die IBM Spectrum Protect-Benutzer-ID ist abgelaufen. Es kann sich um das Kennwort des IBM Spectrum Protect-Knotennamens und/oder um das Kennwort der Benutzer-ID mit Administratorberechtigung handeln.

Systemaktion

Die aktuelle Operation wurde abgebrochen. Sie dürfen erst dann eine Verbindung zum Server herstellen, wenn das Kennwort aktualisiert ist.

Benutzeraktion

Aktualisieren Sie Ihr Kennwort. Dazu müssen unter Umständen das Kennwort des Knotennamens und/oder das Kennwort der Administrator-ID aktualisiert werden. Sie können den Befehl SET PASSWORD verwenden oder Ihren Knoten oder Ihre Administrator-ID vom IBM Spectrum Protect-Administrator aktualisieren lassen.

0053 E DSM_RC_REJECT_ID_UNKNOWN Sitzung zurückgewiesen: Die Benutzer-ID ist falsch, hat keine Administratorberechtigung oder ist dem Server nicht bekannt.

Erläuterung

Die Benutzer-ID, bei der es sich um den IBM Spectrum Protect-Knotennamen oder die Benutzer-ID mit Administratorberechtigung handelt, ist dem Server nicht bekannt. Mögliche Ursachen sind:

- Ihr Knotenname ist auf dem IBM Spectrum Protect-Server nicht registriert
- Der Knotenname ist korrekt, verfügt jedoch nicht über eine entsprechende Administrator-ID mit demselben Namen und derselben Clienteignerberechtigung
- Sie versuchen, auf eine Datei zuzugreifen, die auf einen anderen Knoten umgelagert wurde

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Führen Sie die folgenden Überprüfungen aus:

- Stellen Sie sicher, dass Ihre IBM Spectrum Protect-Benutzer-ID korrekt eingegeben wird.
- Überprüfen Sie die Administrator-ID, die Ihrem IBM Spectrum Protect-Knoten zugeordnet ist, und ob der IBM Spectrum Protect-Knotenname über eine übereinstimmende Administrator-ID mit Clienteignerberechtigung für den Knoten verfügt. Ist dies nicht der Fall, muss Ihr IBM Spectrum Protect-Administrator diese erstellen.
- Stellen Sie sicher, dass der Server die geschlossene Registrierung verwendet und der Knotenname beim Server registriert ist.
- Wird versucht, auf eine umgelagerte Datei zuzugreifen, muss der Knotenname mit dem Knoten übereinstimmen, der die Datei umgelagert hat.

0054 E DSM_RC_REJECT_DUPLICATE_ID Sitzung zurückgewiesen: Doppelte ID eingegeben

Erläuterung

Ein anderer Prozess, der diesen Knotennamen verwendet, ist mit dem Server bereits aktiv.

Systemaktion

IBM Spectrum Protect kann keine Verbindung zum Server herstellen. Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Wenn Sie ein UNIX-basiertes System ausführen, müssen Sie sicherstellen, dass kein anderer Prozess unter demselben Namen in IBM Spectrum Protect aktiv ist. Stellen Sie außerdem sicher, dass der Knotenname für den Server eindeutig ist, damit er nicht von einer anderen Person verwendet werden kann. Den Systemadministrator fragen, wer der Eigner dieses Knotennamens ist.

0055 E DSM_RC_REJECT_SERVER_DISABLED Sitzung zurückgewiesen: Server inaktiv.

Erläuterung

Der Server befindet sich im inaktiven Status und ist für normale Aktivitäten nicht zugänglich.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Führen Sie auf dem IBM Spectrum Protect-Server den Verwaltungsbefehl ENABLE SESSIONS aus. Wiederholen Sie die Operation, wenn der Server in den aktiven Status zurückkehrt. Bleibt der Fehler bestehen, den Systemadministrator verständigen.

0056 E DSM_RC_REJECT_CLOSED_REGISTER Der Server ist nicht für offene Registrierung konfiguriert

Erläuterung

Keine Berechtigung. Registrierung durch den Systemadministrator erforderlich. Der Server ist nicht für offene Registrierung konfiguriert.

Systemaktion

Die Sitzung wurde nicht gestartet.

Benutzeraktion

Sie müssen einen IBM Spectrum Protect-Knoten und ein Kennwort von Ihrem Systemadministrator anfordern.

0057 S DSM_RC_REJECT_CLIENT_DOWNLEVEL Sitzung zurückgewiesen: Codeversion des Clients ist älter

Erläuterung

Die Serverversion und die Clientversion stimmen nicht überein. Der Client-Code befindet sich auf einer niedrigeren Stufe.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Den Systemadministrator fragen, welche Version von IBM Spectrum Protect an Ihrem Standort ausgeführt werden muss.

0058 S DSM_RC_REJECT_SERVER_DOWNLEVEL Sitzung zurückgewiesen: Codeversion des Servers ist älter

Erläuterung

Die Serverversion und die Clientversion stimmen nicht überein. Der Server-Code befindet sich auf einer niedrigeren Stufe.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Den Systemadministrator fragen, welche Version von IBM Spectrum Protect an Ihrem Standort ausgeführt werden muss.

0059 E DSM_RC_REJECT_ID_IN_USE Sitzung zurückgewiesen: Angegebener Knotenname derzeit im Gebrauch

Erläuterung

Der angegebene Knotenname ist auf dem Server im Gebrauch.

Systemaktion

Die Sitzung wurde nicht gestartet.

Benutzeraktion

Der Server führt wahrscheinlich eine Task aus, die verhindert, daß der Knoten eine Sitzung aufbaut. Die Operation später wiederholen oder den Systemadministrator zu Rate ziehen.

0061 E DSM_RC_REJECT_ID_LOCKED Sitzung zurückgewiesen: Der angegebene Knotenname ist derzeit gesperrt.

Erläuterung

Der angegebene Knotenname ist auf dem Server derzeit gesperrt.

Systemaktion

Die Sitzung wurde nicht gestartet.

Benutzeraktion

Den Systemadministrator fragen, weshalb der Knotenname gesperrt ist.

0062 S DSM_RC_SIGNONREJECT_LICENSE_MAX SLM LICENSE EXCEEDED: Die Clientlizenzen für IBM Spectrum Protect sind überschritten. Verständigen Sie Ihren Systemadministrator.

Erläuterung

Durch das Hinzufügen einer neuen Registrierung wird die Anzahl der Produktlizenzen für IBM Spectrum Protect überschritten.

Systemaktion

Die Ausführung der Client-Registrierung oder Verbindungsanforderung wird beendet.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0063 E DSM_RC_REJECT_NO_MEMORY Sitzung zurückgewiesen: Der Server hat nicht genug Speicher, um das Herstellen einer Verbindung zuzulassen.

Erläuterung

Der Server hat nicht genug Speicher, um zuzulassen, daß der Client eine Verbindung mit dem Server herstellt.

Systemaktion

Die Sitzung wurde nicht gestartet.

Benutzeraktion

Die Operation später wiederholen oder den Systemadministrator verständigen.

0064 E DSM_RC_REJECT_NO_DB_SPACE Sitzung zurückgewiesen: Der Server hat nicht genug Datenbankbereich, um das Herstellen einer Verbindung zuzulassen.

Erläuterung

Der Server hat keinen Speicher mehr für den Datenbankbereich.

Systemaktion

Die Sitzung wurde nicht gestartet.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0065 E DSM_RC_REJECT_NO_LOG_SPACE Sitzung zurückgewiesen: Der Server hat nicht genug Speicherbereich für das Wiederherstellungsprotokoll, um das Herstellen einer Verbindung zuzulassen.

Erläuterung

Der Server hat keinen Speicherbereich mehr für das Wiederherstellungsprotokoll.

Systemaktion

Die Sitzung wurde nicht gestartet.

Benutzeraktion

Dies ist ein temporärer Fehler. Die Operation später wiederholen oder den Systemadministrator verständigen.

0066 E DSM_RC_REJECT_INTERNAL_ERROR Die Sitzung wird zurückgewiesen. Beim IBM Spectrum Protect-Server ist ein interner Fehler aufgetreten.

Erläuterung

Der Client kann wegen eines internen Serverfehlers keine Verbindung zum IBM Spectrum Protect-Server herstellen.

Systemaktion

Die Sitzung wurde nicht gestartet.

Benutzeraktion

Melden Sie diesen Fehler Ihrem IBM Spectrum Protect-Administrator.

0067 S DSM_RC_SIGNONREJECT_INVALID_CLI Sitzung zurückgewiesen: Der Server ist nicht für diesen Plattformtyp lizenziert. Verständigen Sie Ihren Systemadministrator.

Erläuterung

Der Server ist für den anfordernden Clienttyp nicht lizenziert.

Systemaktion

Die Ausführung der Client-Registrierung oder Verbindungsanforderung wird beendet.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0068 E DSM_RC_CLIENT_NOT_ARCHRETPROT Die Sitzung wird zurückgewiesen. Der Server erlaubt nicht das Anmelden eines Clients, dessen Aufbewahrungsschutz für Archivierung nicht aktiviert ist.

Erläuterung

Der Client kann keine Verbindung zum Server herstellen, da der Server im Gegensatz zum Client für den Aufbewahrungsschutz für Archivierung aktiviert ist.

Systemaktion

Die Sitzung wird nicht gestartet.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0069 E DSM_RC_SESSION_CANCELED Sitzung zurückgewiesen: Die Sitzung wurde vom Server-Administrator abgebrochen.

Erläuterung

Der Serveradministrator hat die aktuelle Clientsitzung abgebrochen.

Systemaktion

Die Ausführung der Clientverbindungsanforderung wird beendet.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0073 E DSM_RC_REJECT_INVALID_NODE_TYPE Zwischen dem Clientknoten und dem auf dem IBM Spectrum Protect-Server registrierten Knoten wurde eine Inkonsistenz festgestellt.

Erläuterung

Der Benutzer hat wahrscheinlich die Knotenoption falsch codiert. So könnte der beim IBM Spectrum Protect-Server als NAS-Knoten registrierte Knoten in Wirklichkeit ein Nicht-NAS-Client sein.

Systemaktion

Die Operation wird beendet.

Benutzeraktion

Stellen Sie sicher, dass der Knotenname in der Clientoptionsdatei korrekt ist. Stellen Sie sicher, dass Sie einen Knoten der Art NAS nur zusammen mit der Option nasnodename verwenden.

0074 E DSM_RC_REJECT_INVALID_SESSIONINIT Der Server lässt keine vom Client eingeleiteten Verbindungen für diesen Knoten zu.

Erläuterung

Auf Grund der Konfigurationsparameter für diesen Knoten auf dem Server darf der Knoten keine Verbindungen einleiten. Der Server kann Verbindungen zum Client-Scheduler einleiten, wenn dieser im Modus mit Bedienerführung ausgeführt wird.

Systemaktion

Die IBM Spectrum Protect-Operation wird beendet.

Benutzeraktion

Wenden Sie sich an Ihren Systemadministrator, damit er vom Client eingeleitete Sitzungen für Ihren Knoten aktiviert, oder aktualisieren Sie die Option SESSIONINITIATION und führen Sie den Client-Scheduler aus.

0075 E DSM_RC_REJECT_WRONG_PORT Falscher Serveranschluss.

Erläuterung

Sie haben versucht, eine Sitzung des Clients für Sichern/Archivieren auf dem Serveranschluss zu öffnen, der nur für Verwaltungssitzungen definiert ist.

Systemaktion

Die IBM Spectrum Protect-Operation wird beendet.

Benutzeraktion

Wenden Sie sich an Ihren Systemadministrator und/oder verwenden Sie die korrekten Werte für den TCP-Anschluss und den TCP-Verwaltungsanschluss.

0079 E DSM_RC_CLIENT_NOT_SPMRETPROT Die Sitzung wird zurückgewiesen. Der Server erlaubt nicht das Anmelden eines Clients, dessen Aufbewahrungsschutz für Speicherverwaltung nicht aktiviert ist.

Erläuterung

Der Client kann keine Verbindung zum Server herstellen, da der Server im Gegensatz zum Client für den Aufbewahrungsschutz für Speicherverwaltung aktiviert ist.

Systemaktion

Die Sitzung wird nicht gestartet.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0101 W DSM_RC_USER_ABORT Die Operation wurde vom Benutzer gestoppt.

Erläuterung

Die Operation wurde auf Anforderung des Benutzers gestoppt. Dies geschieht normalerweise, wenn die Taste 'Q' zweimal gedrückt wird.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Keine.

0102 E DSM_RC_NO_MEMORY *Dateiname*(*Zeilennummer*) Das Betriebssystem hat eine IBM Spectrum Protect-Anforderung für Speicherzuordnung zurückgewiesen.

Erläuterung

IBM Spectrum Protect erfordert mit fortschreitender Verarbeitung den Zugriff auf Speicher, um Informationen zu speichern. In diesem Fall wurde mehr Speicher angefordert als das Betriebssystem zuordnen würde. Mögliche Ursachen sind:

- Das System hat nur noch wenig Hauptspeicher.
- Der Prozess, in dem das Programm ausgeführt wird, hat den maximalen zugeordneten Speicher überschritten.
- Es ist eine andere Fehlerbedingung aufgetreten. Es ist kein Speicher verfügbar.

Systemaktion

IBM Spectrum Protect kann die angeforderte Operation nicht ausführen.

Benutzeraktion

Schließen Sie alle nicht benötigten Anwendungen und wiederholen Sie die Operation. Wenn die Operation dennoch fehlschlägt, versuchen Sie, die Task in mehrere kleinere Einheiten aufzuteilen. Wenn beispielsweise eine Dateispezifikation mehrere Verzeichnisse höherer Ebene enthält, führen Sie die IBM Spectrum Protect-Task nacheinander für jedes Verzeichnis aus. Wenn die IBM Spectrum Protect-Task eine Teilsicherung ist, verwenden Sie die Option "-memoryefficientbackup=yes".

Bei UNIX-Systemen, die Ressourcengrenzen unterstützen, können Sie überprüfen, ob die Speicherressourcengrenze zu niedrig ist, indem Sie folgenden Befehl eingeben: `ulimit -a`

Abhängig von den daraus resultierenden Daten können Sie den Rootbenutzer des UNIX-Systems bitten, den Ressourcengrenzwert zu erhöhen, damit er über dem aktuellen Standardgrenzwert liegt. Der Rootbenutzer des UNIX-Systems hat die Berechtigung, Ressourcengrenzen zu erhöhen.

0104 E DSM_RC_FILE_NOT_FOUND Datei bei Sicherungs-, Archivierungs- oder Umlagerungsverarbeitung nicht gefunden

Erläuterung

Die Datei, die zur Sicherung, Archivierung oder Umlagerung verarbeitet wird, ist auf dem Client nicht mehr vorhanden. Ein anderer Prozess hat die Datei gelöscht, bevor sie von IBM Spectrum Protect gesichert, archiviert oder umgelagert werden konnte.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Keine.

0105 E DSM_RC_PATH_NOT_FOUND Der angegebene Verzeichnispfad '*Pfadname*' konnte nicht gefunden werden.

Erläuterung

Es wurde ein ungültiger oder unerreichbarer Verzeichnispfad angegeben.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation mit einem gültigen Verzeichnispfad.

0106 E DSM_RC_ACCESS_DENIED Zugriff auf angegebene Datei oder Verzeichnis verweigert

Erläuterung

Zugriff auf angegebene Datei oder Verzeichnis verweigert. Sie haben versucht, aus einer Datei zu lesen oder in eine Datei zu schreiben, und Sie haben keine Zugriffsberechtigung für die Datei oder das Verzeichnis.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Stellen Sie sicher, dass Sie den korrekten Datei- oder Verzeichnisnamen angegeben haben, korrigieren Sie die Berechtigungen oder geben Sie einen neuen Standort an.

0106 E DSM_RC_ACCESS_DENIED Die angegebene Datei wird von einem anderen Prozeß verwendet

Erläuterung

Die angegebene Datei wird von einem anderen Prozess verwendet. Sie haben versucht, aus einer Datei zu lesen oder in eine Datei zu schreiben, die derzeit von einem anderen Prozess verwendet wird.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Stellen Sie sicher, dass Sie den korrekten Datei- oder Verzeichnisnamen angegeben haben, korrigieren Sie die Berechtigungen oder geben Sie einen neuen Standort an.

0107 E DSM_RC_NO_HANDLES Keine Dateikennungen verfügbar

Erläuterung

Alle Dateikennungen für das System sind derzeit im Gebrauch. Weitere sind nicht verfügbar.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Entweder einige Dateikennungen durch das Beenden anderer Prozesse freigeben oder die Systemkonfiguration so ändern, daß mehr Dateien gleichzeitig geöffnet sein können.

0108 E DSM_RC_FILE_EXISTS Die Datei ist vorhanden und kann nicht überschrieben werden.

Erläuterung

Die Datei, die zurückgeschrieben oder abgerufen wird, ist vorhanden und kann wegen fehlender Berechtigung oder wegen fehlenden Zugriffsberechtigungen nicht überschrieben werden.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Prüfen Sie, ob Sie über ausreichende Zugriffsberechtigungen zum Überschreiben der Datei verfügen und wiederholen Sie anschließend die Operation. Bleibt der Fehler bestehen, verständigen Sie zwecks weiterer Unterstützung Ihren Systemadministrator oder IBM Spectrum Protect-Administrator.

0109 E DSM_RC_INVALID_PARM Ungültiger Parameter gefunden.

Erläuterung

Das System hat aufgrund eines ungültigen Parameters einen internen Programmfehler festgestellt.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Fehlerprotokoll vom Kundendienst überprüfen lassen.

0110 E DSM_RC_INVALID_HANDLE Es wurde eine ungültige Dateikennung übergeben; Systemfehler.

Erläuterung

Es ist ein interner Systemfehler aufgetreten: Eine Dateioperation ist wegen einer ungültigen Dateikennung fehlgeschlagen.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, fordern Sie einen Service-Trace an, der den Fehler aufzeichnet, und bitten Sie die technische Unterstützung von IBM um Hilfe. Ihr IBM Spectrum Protect-Administrator kann Sie beim Konfigurieren des Trace unterstützen.

0111 E DSM_RC_DISK_FULL Verarbeitung gestoppt; Bedingung 'Platte voll'.

Erläuterung

Es können keine Dateien mehr zurückgeschrieben oder abgerufen werden, da die Zielplatte voll ist.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Plattenspeicherplatz freigeben oder die Datei auf einer anderen Platte zurückschreiben oder abrufen.

0113 E DSM_RC_PROTOCOL_VIOLATION Fehlerhaftes Protokoll

Erläuterung

Ein Übertragungsprotokollfehler ist aufgetreten. Das DFV-Subsystem ist nicht richtig definiert oder ist fehlerhaft.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Prüfen, ob die Übertragungsprozesse richtig funktionieren, und anschließend die Operation wiederholen.

0114 E DSM_RC_UNKNOWN_ERROR Es ist ein unbekannter Systemfehler aufgetreten, aufgrund dessen IBM Spectrum Protect nicht wiederhergestellt werden kann.

Erläuterung

Es ist ein unbekannter Fehler aufgetreten. Es könnte sich um einen Low-Level-System- oder -Kommunikationsfehler handeln, aufgrund dessen IBM Spectrum Protect nicht wiederhergestellt werden kann.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, prüfen Sie das IBM Spectrum Protect-Fehlerprotokoll auf zugehörige Nachrichten. Fordern Sie einen Service-Trace an, der den Fehler aufzeichnet, und bitten Sie die technische Unterstützung von IBM um Hilfe. Ihr IBM Spectrum Protect-Administrator kann Sie beim Konfigurieren des Trace unterstützen.

0115 E DSM_RC_UNEXPECTED_ERROR Es ist ein unerwarteter Fehler aufgetreten.

Erläuterung

Normalerweise wird dies von einem Low-Level-System- oder -Kommunikationsfehler verursacht, aufgrund dessen IBM Spectrum Protect nicht wiederhergestellt werden kann.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Untersuchen Sie das Clientfehlerprotokoll auf zusätzliche Nachrichten in Bezug auf dieses Problem. Wiederholen Sie die Operation. Bleibt der Fehler bestehen, bitten Sie die technische Unterstützung von IBM Spectrum Protect um Hilfe.

0116 E DSM_RC_FILE_BEING_EXECUTED Datei wird gerade ausgeführt; Schreibzugriff verweigert.

Erläuterung

Die aktuelle Datei kann nicht zum Schreiben geöffnet werden, da sie derzeit von einer anderen Operation ausgeführt wird.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Die Operation, die die Datei ausführt, stoppen und die Operation wiederholen, oder die Datei unter einem anderen Namen oder in einem anderen Verzeichnis zurückschreiben oder abrufen.

0117 E DSM_RC_DIR_NO_SPACE Es können keine weiteren Dateien zurückgeschrieben oder abgerufen werden, da das Zielverzeichnis voll ist.

Erläuterung

Es können keine weiteren Dateien zurückgeschrieben oder abgerufen werden, da das Zielverzeichnis voll ist.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Plattenspeicherplatz freigeben oder die Datei auf einer anderen Platte zurückschreiben oder abrufen.

0118 E DSM_RC_LOOPED_SYM_LINK Beim Auflösen des Namens zu viele symbolische Verbindungen festgestellt

Erläuterung

Beim Versuch, den Dateinamen aufzulösen, wurden zu viele symbolische Verbindungen gefunden.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Sicherstellen, daß für die Datei keine symbolische Verbindung in einer Schleife vorliegt.

0119 E DSM_RC_FILE_NAME_TOO_LONG Der Dateiname ist zu lang und kann von IBM Spectrum Protect nicht verarbeitet werden.

Erläuterung

Die Größenbegrenzung für Dateinamen kann abhängig vom Betriebssystem variieren. Der am häufigsten verwendete Grenzwert beträgt 256 Zeichen. Der Dateiname, der gerade verarbeitet wird, überschreitet den Grenzwert, der von IBM Spectrum Protect auf diesem System unterstützt wird.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Geben Sie HELP FILE SPEC ein oder lesen Sie die Informationen im Clienthandbuch für das Betriebssystem, auf dem Sie diesen Fehler empfangen. Im Handbuch sind im Abschnitt über die Syntax für Dateispezifikationen die von IBM Spectrum Protect unterstützten Dateinamenlängen angegeben.

0120 E DSM_RC_FILE_SPACE_LOCKED Dateisystem vom System gesperrt

Erläuterung

Auf das Dateisystem kann nicht zugegriffen werden, da es vom System gesperrt ist.

Systemaktion

Die Operation kann nicht ausgeführt werden.

Benutzeraktion

Verständigen Sie Ihren Systemadministrator.

0121 I DSM_RC_FINISHED Die Operation ist beendet.

Erläuterung

Die Operation ist beendet.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Mit dem nächsten Funktionsaufruf fortfahren.

0122 E DSM_RC_UNKNOWN_FORMAT Die Datei hat ein unbekanntes Format.

Erläuterung

Der Prozess hat versucht, eine Datei zurückzuschreiben oder abzurufen, aber sie hatte ein unbekanntes Format.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Die Datei wurde entweder von einer anderen Anwendung gesichert oder die Daten sind ungültig. Falls die Datei zu diesem System gehört, wiederholen Sie die Operation. Bleibt der Fehler bestehen, bitten Sie die technische Unterstützung von IBM um Hilfe.

0123 E DSM_RC_NO_AUTHORIZATION Keine Berechtigung zum Zurückschreiben von Daten des anderen Knotens.

Erläuterung

Der Client ist nicht berechtigt, die Daten des anderen Knotens zurückzuschreiben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Berechtigung vom anderen Knoten anfordern.

0124 E DSM_RC_FILE_SPACE_NOT_FOUND Dateibereich '*Dateibereichsname*' nicht vorhanden

Erläuterung

Der angegebene Dateibereichsname (Domäne) ist falsch oder nicht auf der Maschine vorhanden.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Die Operation wiederholen und dabei eine bestehende Domäne (Laufwerkbuchstaben oder Dateisystemnamen) angeben.

0125 E DSM_RC_TXN_ABORTED Transaktion abgebrochen

Erläuterung

Die laufende Transaktion zwischen dem Server und dem Client wurde gestoppt. Ein Server-, Client- oder Übertragungsfehler konnte nicht behoben werden.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator verständigen, damit er den Fehler bestimmt.

0126 E DSM_RC_SUBDIR_AS_FILE IBM Spectrum Protect kann keinen Verzeichnispfad erstellen, weil eine Datei mit demselben Namen wie das Verzeichnis vorhanden ist.

Erläuterung

Keine.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Entfernen Sie die Datei, die den gleichen Namen wie das Verzeichnis hat, oder benennen Sie sie um. Alternativ dazu können Sie das Verzeichnis an einen anderen Standort zurückschreiben.

0127 E DSM_RC_PROCESS_NO_SPACE Plattenspeicherplatzbegrenzung für diesen Prozeß erreicht

Erläuterung

Der dem Clienteigner zugeordnete Plattenspeicherplatz ist belegt.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Plattenspeicherplatz freigeben und die Zurückschreibungs- oder Abrufoperation wiederholen.

0128 E DSM_RC_PATH_TOO_LONG Pfadlänge des Zielverzeichnisses überschreitet Systemmaximum

Erläuterung

Der angegebene Pfadname plus der Pfadname im zurückgeschriebenen Dateinamen ergeben zusammen einen Namen, dessen Länge das vom System zugelassene Maximum überschreitet.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Einen Zielpfad angeben, der, wenn er kombiniert wird, kleiner als das vom System zugelassene Maximum ist.

0129 E DSM_RC_NOT_COMPRESSED Datei ist nicht komprimiert. Systemfehler.

Erläuterung

Eine Datei, die als komprimiert markiert war, war nicht komprimiert, und es kam zu einem Systemfehler.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Dem Systemadministrator diesen Fehler mitteilen. Dieser Fehler ist ein Systemfehler.

0130 E DSM_RC_TOO_MANY_BITS Datei auf einer anderen Client-Maschine mit mehr Speicher komprimiert

Erläuterung

Es wurde versucht, eine Datei zurückzuschreiben, die auf einer anderen Client-Datenstation mit mehr Speicher gesichert und komprimiert wurde. Diese Datei kann nicht zurückgeschrieben werden. Beim Zurückschreiben wird die Datei erweitert. Die Datenstation hat dafür nicht genügend Speicher.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Die Operation auf einer Maschine mit mehr Speicher wiederholen.

0131 E DSM_RC_COMPRESSED_DATA_CORRUPTED Die komprimierte Datei ist beschädigt und kann nicht ordnungsgemäß erweitert werden.

Erläuterung

Die komprimierte Datei konnte auf Grund einer der folgenden Ursachen nicht ordnungsgemäß erweitert werden:

- Es liegt ein Fehler auf dem Band vor.
- Es liegt ein Kommunikationsfehler vor.
- Die komprimierte Datei wurde auf dem IBM Spectrum Protect-Server beschädigt.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

1) Die komprimierte Datei ist beschädigt, weil ein Fehler auf dem Band vorliegt. Um festzustellen, ob dies das Problem ist, geben Sie bitte den folgenden Befehl auf dem IBM Spectrum Protect-Server ein: audit volume <Datenträgername> fix=no Falls ein Fehler gemeldet wird, könnten Sie die Daten von diesem Datenträger auf einen neuen Datenträger versetzen (siehe Befehl MOVE DATA) und die Zurückschreibung wiederholen. 2) Es liegen Kommunikationsfehler zwischen dem IBM Spectrum Protect-Server und dem IBM Spectrum Protect-Client vor und dies führt dazu, dass die Datei während der Übertragung beschädigt wird. Wenn Sie einen Gigabit Ethernet-Adapter auf dem Server verwenden, aktualisieren Sie bitte den Kartentreiber (AIX-Plattform) oder fügen Sie die bereitgestellten, von SUN vorgeschlagenen Änderungen zu einigen Systemnetzoptionen hinzu, die dieses Problem gelöst haben (SUN-Plattform). 3) Bitte prüfen Sie mit Ihrer Netzunterstützung, ob es während der Zurückschreibung zu Fehlern zwischen dem IBM Spectrum Protect-Client/Server kommt, von dem die Dateibeschädigung ausgeht.

0131 S DSM_RC_SYSTEM_ERROR Ein interner Programmfehler ist aufgetreten.

Erläuterung

Eine nicht erwartete Bedingung ist aufgetreten und die Operation kann nicht fortgesetzt werden. Dies könnte ein Programmierfehler sein.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, verständigen Sie zwecks weiterer Unterstützung Ihren IBM Spectrum Protect-Administrator oder die technische Unterstützung von IBM.

0132 E DSM_RC_NO_SERVER_RESOURCES Der IBM Spectrum Protect-Server hat keine Ressourcen mehr.

Erläuterung

Das Fehlen einer Speicherressource oder ein Maximalwertzustand erlaubt keine neuen Aktivitäten.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Wiederholen Sie die Operation zu einem späteren Zeitpunkt. Bleibt der Fehler bestehen, verständigen Sie Ihren IBM Spectrum Protect-Administrator, um die nicht verfügbare Ressource einzugrenzen. Der IBM Spectrum Protect-Administrator kann das Aktivitätenprotokoll des IBM Spectrum Protect-Servers auf Nachrichten überprüfen, die den Fehler unter Umständen erklären.

0133 E DSM_RC_FS_NOT_KNOWN Der Dateibereich für die Domäne '*Domänenname*' wurde auf dem IBM Spectrum Protect-Server nicht gefunden.

Erläuterung

Es wurde erwartet, dass der angegebene Dateibereich auf dem Server gefunden wurde, aber er existiert nicht mehr. Es ist möglich, dass ein Befehl abgesetzt wurde, den Dateibereich aus dem Server zu löschen, während die aktuelle Operation ausgeführt wurde.

Systemaktion

Die IBM Spectrum Protect-Verarbeitung wird gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Wenn das Problem erneut auftritt, überprüfen Sie das Fehlerprotokoll auf alle anderen Nachrichten, die eine Ursache für den Fehler anzeigen könnten. Versuchen Sie, alle angezeigten Fehler zu korrigieren, und wiederholen Sie anschließend die Operation. Bleibt der Fehler bestehen, bitten Sie die technische Unterstützung von IBM um Hilfe.

0134 E DSM_RC_NO_LEADING_DIRSEP Das Feld 'objName' hat keinen führenden Verzeichnisseparator.

Erläuterung

Das Feld 'objName' hat keinen führenden Verzeichnisseparator.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Wert für das Feld 'objName' korrigieren.

0135 E DSM_RC_WILDCARD_DIR Platzhalterzeichen sind im objName-Verzeichnispfad nicht zulässig.

Erläuterung

Platzhalterzeichen sind im objName-Verzeichnispfad nicht zulässig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Wert für das Feld 'objName' korrigieren.

0136 E DSM_RC_COMM_PROTOCOL_ERROR Die Sitzung wird zurückgewiesen: Es gab einen Fehler im Übertragungsprotokoll.

Erläuterung

Es wurde eine unerwartete Netznachricht vom Client empfangen. Dies könnte durch Netzprobleme oder einen Programmierfehler verursacht worden sein.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Prüfen Sie, ob Ihr Übertragungsweg richtig funktioniert und wiederholen Sie die Operation. Bleibt der Fehler bestehen, bitten Sie Ihren IBM Spectrum Protect-Administrator um weitere Unterstützung.

0137 E DSM_RC_AUTH_FAILURE Sitzung zurückgewiesen: Fehler bei Authentifizierung

Erläuterung

Fehler bei Authentifizierung. Sie haben eine falsche Benutzer-ID oder ein falsches Kennwort eingegeben.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Geben Sie die korrekte Benutzer-ID und das korrekte Kennwort ein. Wenn Sie sich nicht an die korrekte Benutzer-ID oder das korrekte Kennwort erinnern können, wenden Sie sich an Ihren Systemadministrator, damit Ihrem Knotennamen neue Berechtigungsnachweise zugeordnet werden.

0138 E DSM_RC_TA_NOT_VALID Die Ausführungs-/Eignerberechtigungen für 'dsmtca' sind ungültig.

Erläuterung

Die Ausführungs-/Eignerberechtigungen für 'dsmtca' sind ungültig.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Lassen Sie die Installationsanweisungen für den Client von Ihrem Systemadministrator überprüfen, um sicherzustellen, dass die Berechtigungen für 'dsmtca' korrekt definiert sind.

0139 S DSM_RC_KILLED Prozeß abgebrochen.

Erläuterung

Die Verarbeitung wurde gestoppt. Dies ist ein Programmierfehler und das Clientprogramm wird beendet.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator verständigen.

0145 S DSM_RC_WOULD_BLOCK Das Modul 'dsmtca' würde die Operation blockieren.

Erläuterung

Das Modul 'dsmtca' blockiert die Operation. Dies ist ein Programmierfehler und das Clientprogramm wird beendet.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator verständigen.

0146 S DSM_RC_TOO_SMALL Der Bereich für das Einschluß-/Ausschlußmuster ist zu klein.

Erläuterung

Der Bereich für das Einschluß-/Ausschlußmuster ist zu klein. Dies ist ein Programmierfehler und das Clientprogramm wird beendet.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator verständigen.

0147 S DSM_RC_UNCLOSED Das Muster enthält keine rechte eckige Klammer.

Erläuterung

Das Muster enthält keine rechte eckige Klammer. Dies ist ein Programmierfehler und das Clientprogramm wird beendet.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator verständigen.

0148 S DSM_RC_NO_STARTING_DELIMITER Das Einschluss-/Ausschlussmuster muss mit einem Verzeichnisbegrenzer beginnen

Erläuterung

Das Einschluss-/Ausschlussmuster muss mit einem Verzeichnisbegrenzer beginnen.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Korrigieren Sie die Syntax für das Muster.

0149 S DSM_RC_NEEDED_DIR_DELIMITER Ein führender oder abschließender Verzeichnisbegrenzer fehlt im Einschluss-/Ausschlussmuster.

Erläuterung

1. Das Einschluss-/Ausschlussmuster hat '...' ohne Verzeichnisbegrenzer am Anfang und Ende.
2. Für Windows folgt auf das Laufwerktrennzeichen nicht unmittelbar ein Verzeichnisbegrenzer.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Korrigieren Sie die Syntax für das Muster.

0151 S DSM_RC_BUFFER_OVERFLOW Der Datenpuffer ist voll.

Erläuterung

Der Datenpuffer ist voll. Dies ist ein Programmierfehler und das Clientprogramm wird beendet.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator verständigen.

0154 E DSM_RC_NO_COMPRESS_MEMORY Nicht genügend Speicher für Dateikomprimierung/-erweiterung

Erläuterung

Zum Komprimieren und Erweitern von Daten ist nicht genügend Speicher verfügbar. Beim Zurückschreiben oder Abrufen kann die Datei erst dann vom Server zurückgerufen werden, wenn mehr Speicher zur Verfügung gestellt wird. Beim Sichern oder Archivieren versuchen, die Operation ohne Komprimierung auszuführen, wenn kein Speicher zur Verfügung gestellt werden kann.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Zusätzlichen Speicher freigeben, damit die Operation fortgesetzt werden kann, oder den Sicherungs- oder Archivierungsprozeß ohne aktivierte Komprimierung ausführen.

0155 T DSM_RC_COMPRESS_GREW Komprimierte Daten angewachsen

Erläuterung

Die Datei ist nach der Komprimierung größer als vor der Komprimierung.

Systemaktion

Obwohl die Größe der Datei zugenommen hat, wird die Datei komprimiert.

Benutzeraktion

Keine.

0156 E DSM_RC_INV_COMM_METHOD Es wurde eine nicht unterstützte Übertragungsmethode angegeben.

Erläuterung

Keine.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Geben Sie eine DFV-Schnittstelle an, die vom IBM Spectrum Protect-Client auf Ihrem Betriebssystem unterstützt wird. Das Handbuch zum IBM Spectrum Protect-Client für Ihr Betriebssystem enthält weitere Informationen zum Konfigurieren der IBM Spectrum Protect-Clientkommunikation.

0157 S DSM_RC_WILL_ABORT Die Transaktion wird abgebrochen.

Erläuterung

Der Server hat einen Fehler festgestellt und wird die Transaktion abbrechen.

Systemaktion

Die Transaktion wird abgebrochen. Der Ursachencode wird in dem Aufruf 'dsmEndTxn' übergeben.

Benutzeraktion

'dsmEndTxn' mit dem Wert DSM_VOTE_COMMIT ausgeben und den Ursachencode überprüfen.

0158 E DSM_RC_FS_WRITE_LOCKED Zieldatei oder Verzeichnis ist schreibgeschützt

Erläuterung

In die Datei oder in das Verzeichnis, die/das vom Server zurückgeschrieben oder abgerufen wird, kann nicht geschrieben werden, da der Zielort schreibgeschützt ist. Möglicherweise wurde die Datei von einer anderen Operation geöffnet, die nicht zuläßt, daß die Datei aktualisiert wird.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Entweder feststellen, durch welche Operation die Schreibsperre für die Datei aktiviert wurde, oder die Datei unter einem anderen Namen oder an einem anderen Standort zurückschreiben.

0159 I DSM_RC_SKIPPED_BY_USER Eine Datei wurde bei einer Zurückschreibungsoperation übersprungen, da die Datei inaktiv war und von der Anwendung ausgewählt wurde, nicht auf das Laden eines Bands zu warten.

Erläuterung

Eine Datei wurde bei einer Zurückschreibungsoperation übersprungen, da die Datei inaktiv war und von der Anwendung ausgewählt wurde, nicht auf das Laden eines Bands zu warten.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Sicherstellen, daß die Anwendung den Wert für 'mountWait' in 'dsmBeginGetData' korrekt setzt.

0160 E DSM_RC_TA_NOT_FOUND Das Modul 'dsmtca' wurde nicht gefunden.

Erläuterung

IBM Spectrum Protect konnte das Modul 'dsmtca' in dem angegebenen Verzeichnis nicht finden.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Stellen Sie sicher, dass das Modul 'dsmtca' sich in dem Verzeichnis befindet, das durch DSMI_DIR angegeben ist.

0162 E DSM_RC_FS_NOT_READY Dateisystem/Laufwerk nicht bereit

Erläuterung

Das Dateisystem/Laufwerk ist für den Zugriff nicht bereit.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Stellen Sie sicher, dass das Laufwerk verfügbar ist, und wiederholen Sie dann die Operation.

0164 E DSM_RC_FIO_ERROR Dateiein-/-ausgabefehler

Erläuterung

Beim Lesen oder Schreiben in einer Datei wurde ein Fehler gefunden.

Systemaktion

Die Datei oder das Dateisystem wurde übersprungen.

Benutzeraktion

Das System überprüfen, um sicherzustellen, daß es richtig arbeitet. Ist OS/2 installiert, CHKDSK /F für das fehlerhafte Laufwerk ausführen, das in dsmerror.log angegeben ist.

0165 E DSM_RC_WRITE_FAILURE Fehler beim Schreiben in Datei

Erläuterung

Beim Schreiben in die Datei wurde ein Fehler gefunden.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Überprüfen Sie Ihr System, um sicherzustellen, dass es ordnungsgemäß funktioniert.

0166 E DSM_RC_OVER_FILE_SIZE_LIMIT Datei überschreitet System-/Benutzerdateibegrenzungen

Erläuterung

Eine Datei, die zurückgeschrieben oder abgerufen wird, überschreitet die vom System festgelegten Begrenzungen für diesen Benutzer.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Sicherstellen, daß die Systembegrenzungen korrekt festgelegt sind.

0167 E DSM_RC_CANNOT_MAKE Datei/Verzeichnis kann nicht erstellt werden

Erläuterung

Der Verzeichnispfad für Dateien, die zurückgeschrieben oder abgerufen werden, kann nicht erstellt werden.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Sicherstellen, daß die richtige Berechtigung vorliegt, um das Verzeichnis für Dateien zu erstellen, die zurückgeschrieben oder abgerufen werden sollen. Es muß Schreibzugriff vorhanden sein.

0168 E DSM_RC_NO_PASS_FILE Kennwortdatei ist nicht verfügbar.

Erläuterung

Die Datei, die das gespeicherte Kennwort für den angegebenen Server *Servername* enthält, ist nicht verfügbar.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Der Root muss ein neues Kennwort festlegen und speichern.

0169 E DSM_RC_VERFILE_OLD PASSWORDACCESS ist GENERATE, aber für den Server '*Servername*' wird ein Kennwort benötigt. Entweder ist das Kennwort nicht lokal gespeichert oder es wurde auf dem Server geändert.

Erläuterung

Entweder ist das Kennwort nicht lokal gespeichert oder es wurde auf dem Server geändert.

Systemaktion

IBM Spectrum Protect fordert das Kennwort an, wenn IBM Spectrum Protect im Vordergrund läuft.

Benutzeraktion

Wurde IBM Spectrum Protect als Hintergrundprozess ausgeführt, geben Sie alle IBM Spectrum Protect-Befehle im Vordergrund aus. Das Kennwort als Antwort auf die Eingabeaufforderung eingeben. Führen Sie dann den IBM Spectrum Protect-Hintergrundbefehl erneut aus.

0173 E DSM_RC_INPUT_ERROR Der Prozess wird in einem nicht interaktiven Modus ausgeführt, erfordert aber Benutzereingaben.

Erläuterung

Dieser Prozess erfordert Tastatureingaben, aber nicht interaktive Prozesse können keine Eingaben von der Tastatur lesen.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Führen Sie folgende Aktionen aus, um diesen Fehler zu beheben:

- Führen Sie das Produkt im Dialogmodus aus.
- Stellen Sie sicher, dass Ihr Kennwort richtig definiert ist.

0174 E DSM_RC_REJECT_PLATFORM_MISMATCH Sitzung zurückgewiesen: Abweichung bei Knotenart

Erläuterung

Ihr Knotenname ist einem anderen Betriebssystemtyp zugeordnet und kann auf diesem System nicht verwendet werden.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Wird ein neuer Knotenname benötigt, den Systemadministrator verständigen, damit er einen neuen Knotennamen zuordnet. Im allgemeinen gibt es für jedes Paar Maschine/Betriebssystem, das auf den Server zugreifen muß, einen eindeutigen Knotennamen.

0175 E DSM_RC_TL_NOT_FILE_OWNER Nicht der Dateieigner

Erläuterung

Die Datei kann nicht gesichert werden, da der Client nicht der Dateieigner ist.

Systemaktion

Die Datei wird übersprungen.

Benutzeraktion

Keine.

0177 S DSM_RC_UNMATCHED_QUOTE Anführungszeichen stimmen nicht überein

Erläuterung

Die im Muster angegebenen Anführungszeichen sind nicht identisch und ergeben kein Paar.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Das Muster unter Verwendung übereinstimmender Anführungszeichen in der Syntax korrigieren.

0184 E DSM_RC_TL_NOBCG Die Verwaltungsklasse für diese Datei hat keine gültige Sicherungskopiengruppe. Diese Datei wird nicht gesichert.

Erläuterung

Für die Verwaltungsklasse dieser Datei wurde keine Sicherungskopiengruppe angegeben. Diese Datei wird nicht gesichert.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Fügen Sie der Verwaltungsklasse eine gültige Sicherungskopiengruppe hinzu und wiederholen Sie dann die Operation.

0185 W DSM_RC_TL_EXCLUDED Datei '*DateinameDateinameDateiname*' durch Einschluss-/Ausschlussliste ausgeschlossen

Erläuterung

Sie können keine Dateien, die ausgeschlossen sind, sichern, archivieren oder umlagern.

Systemaktion

Die Datei kann nicht verarbeitet werden.

Benutzeraktion

Wird die Datei absichtlich ausgeschlossen, kann diese Nachricht ignoriert werden. Andernfalls müssen Sie die Einschluss-/Ausschlussliste ändern, den Client erneut starten und die Operation wiederholen. Verständigen Sie zwecks weiterer Unterstützung Ihren IBM Spectrum Protect-Administrator.

0186 E DSM_RC_TL_NOACG Die Verwaltungsklasse für diese Datei hat keine gültige Archivierungskopiengruppe. Diese Datei wird nicht archiviert.

Erläuterung

Für die Verwaltungsklasse dieser Datei wurde keine Archivierungskopiengruppe angegeben. Diese Datei wird nicht archiviert.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Eine gültige Archivierungskopiengruppe der Verwaltungsklasse hinzufügen und dann die Operation wiederholen.

0187 E DSM_RC_PS_INVALID_ARCHMC Ungültige Verwaltungsklasse eingegeben

Erläuterung

Es wurde eine ungültige Verwaltungsklasse eingegeben.

Systemaktion

Die angeforderte Operation ist nicht möglich.

Benutzeraktion

Die Operation unter Verwendung einer gültigen Verwaltungsklasse wiederholen.

0188 S DSM_RC_NO_PS_DATA Entweder ist der Knoten auf dem Server nicht vorhanden oder es gibt keine aktive Maßnahmengruppe für den Knoten.

Erläuterung

Dieser Fehler tritt auf, wenn Sie versuchen, auf die Daten eines anderen Knotens zuzugreifen. Entweder ist der Knoten beim IBM Spectrum Protect-Server nicht registriert oder es gibt keine aktive Maßnahmengruppe für den Knoten.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Prüfen Sie, ob der Knoten, auf dessen Daten Sie zugreifen möchten, beim IBM Spectrum Protect-Server registriert ist. Haben Sie mehrere IBM Spectrum Protect-Server, stellen Sie sicher, dass Sie die Verbindung zum korrekten Server herstellen, und wiederholen Sie anschließend die Operation. Bleibt der Fehler bestehen, bitten Sie Ihren IBM Spectrum Protect-Administrator um weitere Unterstützung.

0189 S DSM_RC_PS_INVALID_DIRMC Die den Verzeichnissen zugeordnete Verwaltungsklasse ist nicht vorhanden.

Erläuterung

Die in der Option DIRMC benannte Verwaltungsklasse ist in Ihrer zugeordneten Maßnahmengruppe auf dem Server nicht vorhanden. Das Fehlerprotokoll enthält einen Eintrag, der den ungültigen Namen der Verwaltungsklasse anzeigt.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Entfernen Sie die aktuelle Option DIRMC aus der Clientoptionsdatei und führen Sie anschließend DSMC QUERY MGMTCLASS -DETAIL aus, um Informationen über verfügbare Verwaltungsklassen anzuzeigen. Stellen Sie sicher, dass die von Ihnen ausgewählte Verwaltungsklasse eine Sicherungskopiengruppe besitzt. Haben Sie mehrere IBM Spectrum Protect-Server, stellen Sie sicher, dass Sie die Verbindung zum korrekten Server herstellen. Wenn Sie keine passende Verwaltungsklasse finden können, bitten Sie Ihren IBM Spectrum Protect-Administrator um Unterstützung.

0190 S DSM_RC_PS_NO_CG_IN_DIR_MC Es gibt keine Sicherungskopiengruppe in der für Verzeichnisse verwendeten Verwaltungsklasse.

Erläuterung

Die Option DIRMC benennt eine Verwaltungsklasse, die keine Sicherungskopiengruppe enthält.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Entfernen Sie die aktuelle Option DIRMC aus der Clientoptionsdatei und führen Sie anschließend DSMC QUERY MGMTCLASS -DETAIL aus, um Informationen über verfügbare Verwaltungsklassen anzuzeigen. Stellen Sie sicher, dass die von Ihnen ausgewählte Verwaltungsklasse eine Sicherungskopiengruppe besitzt. Haben Sie mehrere IBM Spectrum Protect-Server, stellen Sie sicher, dass Sie die Verbindung zum korrekten Server herstellen. Wenn Sie keine passende Verwaltungsklasse finden können, bitten Sie Ihren IBM Spectrum Protect-Administrator um Unterstützung.

0231 E DSM_RC_ABORT_MOVER_TYPEUnbekannte Art der fernen Versetzungseinheit

Erläuterung

Die angegebene Art der fernen Versetzungseinheit ist unbekannt.

Systemaktion

Die aktuelle Operation wurde beendet.

Benutzeraktion

Ihr Systemadministrator erteilt weitere Informationen.

0232 E DSM_RC_ABORT_ITEM_IN_USEEine Operation für den angeforderten Knoten und Dateibereich wird bereits ausgeführt.

Erläuterung

Es wurde angefordert, mithilfe der Einheit zum Versetzen von Daten eine Operation für den angegebenen Knoten und Dateibereich auszuführen. Da eine Operation für diesen Knoten und Dateibereich bereits ausgeführt wird, kann die neue Operation nicht ausgeführt werden.

Systemaktion

Die aktuelle Operation wurde beendet.

Benutzeraktion

Wiederholen Sie die Operation zu einem späteren Zeitpunkt.

0233 E DSM_RC_ABORT_LOCK_CONFLICTSystemressource wird verwendet

Erläuterung

Eine erforderliche Ressource wird von einem anderen Befehl oder Prozess verwendet.

Systemaktion

Die aktuelle Operation wurde beendet.

Benutzeraktion

Wiederholen Sie die Operation zu einem späteren Zeitpunkt.

0234 E DSM_RC_ABORT_SRV_PLUGIN_COMM_ERRORServer-Plug-in-Kommunikationsfehler

Erläuterung

Die Kommunikation zwischen einem Server-Plug-in und einer NAS-Dateieinheit ist fehlgeschlagen.

Systemaktion

Die aktuelle Operation wurde beendet.

Benutzeraktion

Ihr Systemadministrator erteilt weitere Informationen.

0235 E DSM_RC_ABORT_SRV_PLUGIN_OS_ERRORServer-Plug-in hat nicht unterstütztes Betriebssystem für NAS-Dateieinheit erkannt.

Erläuterung

Ein Plug-in-Modul hat festgestellt, dass eine NAS-Dateieinheit ein nicht unterstütztes Betriebssystem oder eine nicht unterstützte Betriebssystemstufe ausführt.

Systemaktion

Die aktuelle Operation wurde beendet.

Benutzeraktion

Ihr Systemadministrator erteilt weitere Informationen.

0236E DSM_RC_ABORT_CRC_FAILED Der vom Server empfangene CRC stimmt nicht mit dem vom Client berechneten CRC überein.

Erläuterung

Der Server hat einen CRC für einen Puffer gesendet. Der Client hat einen CRC für denselben Puffer berechnet. Die beiden stimmen nicht überein. Die Abweichung zeigt einen Kommunikationsfehler an.

Systemaktion

In einigen Fällen kann der Client dem Server den Fehler anzeigen und die Operation wiederholen.

Benutzeraktion

Das Ablaufverfolgungsprotokoll auf zusätzliche Informationen überprüfen und die Operation wiederholen. Bleibt der Fehler bestehen, den Systemadministrator verständigen.

0237E DSM_RC_ABORT_INVALID_GROUP_ACTION Ungültige Operation für einen Gruppenleiter oder ein Gruppenmitglied.

Erläuterung

Es wurde eine ungültige Operation für eine logische Gruppe versucht.

Systemaktion

Die aktuelle Operation wird gestoppt.

Benutzeraktion

Wiederholen Sie den Vorgang mit einer gültigen Operation.

0238E DSM_RC_ABORT_DISK_UNDEFINED Ferne Platte nicht definiert.

Erläuterung

Es sollte eine Operation für eine ferne Platte ausgeführt werden, die nicht definiert ist.

Systemaktion

Die aktuelle Operation wird gestoppt.

Benutzeraktion

Definieren Sie die korrekte ferne Platte.

0239E DSM_RC_ABORT_BAD_DESTINATION Eingabezielort entspricht nicht dem erwarteten Zielort.

Erläuterung

Eingabezielort entspricht nicht dem erwarteten Zielort.

Systemaktion

Die aktuelle Operation wird gestoppt.

Benutzeraktion

Wiederholen Sie die Operation mit dem korrekten Zielort.

0240E DSM_RC_ABORT_DATAMOVER_NOT_AVAILABLE Einheit zum Versetzen von Daten ist nicht verfügbar.

Erläuterung

Einheit zum Versetzen von Daten ist nicht verfügbar.

Systemaktion

Die aktuelle Operation wird gestoppt.

Benutzeraktion

Wiederholen Sie die Operation mit einer korrekten Einheit zum Versetzen von Daten.

0241E DSM_RC_ABORT_STGPOOL_COPY_CONT_NO Operation fehlgeschlagen, da die Option zum Fortsetzen des Kopierens auf NO gesetzt war.

Erläuterung

Die Operation ist fehlgeschlagen, da die Option zum Fortsetzen des Kopierens auf NO gesetzt war.

Systemaktion

Die aktuelle Operation wird gestoppt.

Benutzeraktion

Dieser Abbruchcode gibt an, dass eine Speicheroperation, wie beispielsweise Sichern oder Archivieren, fehlgeschlagen ist, da die Option zum Fortsetzen des Kopierens auf NO gesetzt war. Der Systemadministrator muss den Fehler auf der Serverseite beheben.

0242E DSM_RC_ABORT_RETRY_SINGLE_TXN Transaktion aufgrund eines Fehlers während einer Speicheroperation fehlgeschlagen.

Erläuterung

Die Transaktion ist aufgrund eines Fehlers während einer Speicheroperation fehlgeschlagen. Dieser Fehler tritt normalerweise auf, wenn der nächste Speicherpool über eine andere Kopienspeicherpoolliste verfügt und während einer Transaktion zu diesem Pool gewechselt wird.

Systemaktion

Die Transaktion wird abgebrochen.

Benutzeraktion

Senden Sie die Objekte in separaten Transaktionen erneut.

0245 E DSM_RC_ABORT_PATH_RESTRICTED Die aktuelle Clientkonfiguration ist nicht konform mit dem Wert der Serveroption DATAWRITEPATH oder DATAREADPATH für diesen Knoten.

Erläuterung

Die Werte der Serveroptionen DATAWRITEPATH und DATAREADPATH geben an, wohin der Client Daten senden darf und woher Daten gelesen werden. Die Werte für den angegebenen Knotennamen sollten der Clientkonfiguration entsprechen. Sie erhalten beispielsweise diese Fehlernachricht, wenn DATAWRITEPATH einen LAN-Wert enthält und der Client für die Verwendung des LAN-freien Protokolls konfiguriert ist, oder wenn der umgekehrte Fall eintritt.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Überprüfen Sie die Protokolle von Client, Server und Speicheragent, um festzustellen, warum der Client Daten nicht LAN-frei senden konnte. Stellen Sie sicher, dass die Clientkonfiguration und die Serveroptionen kompatibel sind.

0247 E DSM_RC_ABORT_INSERT_NOT_ALLOWED Dieser Server unterstützt keine Sicherungsoperationen.

Erläuterung

Dieser Server unterstützt nur Archivierungsoperationen, Sichern ist nicht zulässig.

Systemaktion

Die aktuelle Operation wird beendet.

Benutzeraktion

Verwenden Sie mit diesem Server nur Archivierungsoperationen.

0248 E DSM_RC_ABORT_DELETE_NOT_ALLOWED Das Löschen des Objekts: "*fshlll*" ist nicht zulässig.

Erläuterung

Das Objekt hat entweder den Status "Löschen unzulässig" und kann nicht gelöscht werden, oder das Objekt befindet sich auf einem Server, auf dem der Aufbewahrungsschutz aktiviert ist, und das Objekt ist nicht verfallen.

Systemaktion

Das Objekt wird übersprungen und die Verarbeitung wird fortgesetzt.

Benutzeraktion

Überprüfen Sie den Status des Objekts durch eine Abfrage, um festzustellen, ob es auf Halten gesetzt ist oder wann es verfällt.

0249 E DSM_RC_ABORT_TXN_LIMIT_EXCEEDED Die Anzahl der Objekte in dieser Transaktion überschreitet die Werte für TXNGROUPMAX.

Erläuterung

Es sind zu viele Objekte in dieser Transaktion.

Systemaktion

Die aktuelle Operation wird beendet.

Benutzeraktion

Wiederholen Sie die Operation mit weniger Objekten in der Transaktion oder erhöhen Sie den Wert für TXNGROUPMAX auf dem Server.

0250 E DSM_RC_ABORT_OBJECT_ALREADY_HELD *fshlll* ist bereits auf Halten gesetzt.

Erläuterung

Eines der Objekte in der Transaktion Das angegebene Objekt ist bereits auf Halten gesetzt und kann nicht erneut auf Halten gesetzt werden.

Systemaktion

Die aktuelle Operation wird beendet. Dieses Objekt wird übersprungen und die Verarbeitung wird fortgesetzt.

Benutzeraktion

Geben Sie eine Abfrage ein, um den Status der Objekte festzustellen, und wiederholen Sie die Operation ohne das Objekt, das bereits auf Halten gesetzt ist.

0292 E DSM_RC_TCA_FORK_FAILED Fehler beim Starten des Prozesses dsmtca oder dsmenc.

Erläuterung

Beim Starten des Prozesses dsmtca oder dsmenc ist ein Fehler aufgetreten; speziell die Funktion `fork()` ist fehlgeschlagen.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Wahrscheinlich ein Systemfehler. Bleibt der Fehler bestehen, einen Neustart der Datenstation ausführen.

0295 E DSM_RC_TCA_INVALID_REQUEST Der IBM Spectrum Protect-Prozess 'dsmtca' hat eine ungültige Anforderung empfangen.

Erläuterung

Der Prozess dsmtca oder dsmenc wurde vom Client für Sichern/Archivieren aufgerufen und hat in dem Aufruf ein unbekanntes Anforderungsargument empfangen.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Es ist möglich, dass der Prozess dsmtca oder dsmenc fälschlicherweise von einem anderen Prozess als dem Client für Sichern/Archivieren aufgerufen wurde. Ist dies der Fall, handelt es sich hier um einen internen Fehler. Wenden Sie sich an Ihren IBM-Servicemitarbeiter, falls das Problem erneut auftritt.

0296 E DSM_RC_TCA_NOT_ROOT Diese Aktion erfordert IBM Spectrum Protect-Administratorberechtigung auf diesem System.

Erläuterung

Es wurde versucht, eine Aktion auszuführen, die vom IBM Spectrum Protect-Administrator ausgeführt werden muss (z. B. offene Registrierung, Löschen eines Dateibereichs oder Kennwortaktualisierung).

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Ist die Aktion erforderlich, muß sie vom Administrator ausgeführt werden.

0297 E DSM_RC_TCA_SEMGET_ERROR Fehler beim Zuordnen von Semaphors.

Erläuterung

Es ist ein Fehler aufgetreten, weil die Semaphors, die Sie zuordnen wollen, nicht mehr ausreichen.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Bitten Sie Ihren Systemadministrator um Hilfe und vergrößern Sie möglicherweise die Zahl der Semaphors in Ihrem System.

0298 E DSM_RC_TCA_SEM_OP_ERROR Fehler beim Definieren des Semaphorwerts oder beim Warten auf Semaphor.

Erläuterung

Beim Versuch, ein Semaphor zu definieren oder auf ein Semaphor zu warten, ist ein Fehler aufgetreten.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Wahrscheinlich ein Systemfehler. Bleibt der Fehler bestehen, einen Neustart der Datenstation ausführen.

0400 E DSM_RC_INVALID_OPT Bei der Syntaxanalyse wurde eine ungültige Option gefunden.

Erläuterung

Eine ungültige Option wurde gefunden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Optionen in dsm.opt und dsm.sys und die Optionszeichenfolge überprüfen. Das Fehlerprotokoll auf weitere Informationen über den Fehler überprüfen. Auf der AS/400-Plattform die Optionen in *LIB/QOPTIBM Spectrum Protect(APIOPT) überprüfen.

0405 E DSM_RC_NO_HOST_ADDR TCPSERVERADDRESS für diesen Server in der Systemoptionsdatei nicht definiert

Erläuterung

Die Option TCPSERVERADDRESS ist für diesen Server in der Server-Namenzeilengruppe der Systemoptionsdatei nicht definiert.

Systemaktion

Die IBM Spectrum Protect-Initialisierung schlägt fehl und das Programm wird beendet.

Benutzeraktion

Verständigen Sie den IBM Spectrum Protect-Administrator und stellen Sie sicher, dass für den Server, zu dem eine Verbindung hergestellt werden soll, eine gültige Option TCPSERVERADDRESS in der Systemoptionsdatei definiert ist.

0406 S DSM_RC_NO_OPT_FILE Optionsdatei '*Dateiname*' konnte nicht gefunden werden oder kann nicht gelesen werden.

Erläuterung

Allgemeine Ursachen für diesen Fehler sind:

- Die Standardoptionsdatei ist nicht vorhanden.
- Sie haben die Option -OPTFILE beim Starten des IBM Spectrum Protect-Clients angegeben, aber die von Ihnen zur Verfügung gestellte Optionsdatei ist nicht vorhanden.
- Die Umgebungsvariable DSM_CONFIG (oder DSMI_CONFIG, wenn Sie die IBM Spectrum Protect-API verwenden) gibt eine Optionsdatei an, die nicht vorhanden ist.
- Sie haben die Option -OPTFILE beim Starten des IBM Spectrum Protect-Clients angegeben, aber die von Ihnen zur Verfügung gestellte Optionsdatei liegt nicht in der Standarddateicodierung des Systems vor. Unter Windows beispielsweise wird als Dateicodierung ANSI erwartet.
- Sie haben die Option -OPTFILE beim Starten des IBM Spectrum Protect-Clients angegeben, aber die von Ihnen zur Verfügung gestellte Optionsdatei verfügt nicht über die entsprechenden Leseberechtigungen für den Benutzer, der die Operation ausführt.

Systemaktion

Die IBM Spectrum Protect-Clientverarbeitung wird gestoppt.

Benutzeraktion

Stellen Sie sicher, dass die Optionsdatei, die verwendet werden soll, vorhanden ist, dass sie über die Leseberechtigungen verfügt, die für den Benutzer, der die Operation ausführt, definiert sind, und dass die Datei in der Standarddateicodierung des Systems vorliegt. Unter Windows beispielsweise wird als Dateicodierung ANSI erwartet. Lesen Sie die Konfigurationsinformationen im IBM Spectrum Protect-Clienthandbuch für Ihr Betriebssystem. Bleibt der Fehler bestehen, bitten Sie Ihren IBM Spectrum Protect-Administrator um weitere Unterstützung.

0408 E DSM_RC_MACHINE_SAME Ein virtueller Knotenname darf nicht gleich einem Knotennamen oder dem Systemhostnamen sein.

Erläuterung

Die Option VIRTUALNODENAME wurde mit einem Namen eingegeben, der entweder einem Namen in der Option NODENAME oder dem Systemhostnamen entsprach.

Systemaktion

Die Initialisierung schlägt fehl und das Programm wird beendet.

Benutzeraktion

Wenn der eingegebene virtuelle Knotenname mit dem Hostnamen identisch war, müssen Sie die Option für den virtuellen Knotennamen entfernen. War der Name mit demjenigen in der Option für den Knotennamen identisch, können Sie, abhängig von der beabsichtigten Verwendung, einen der beiden entfernen. Der Knotenname wird verwendet, um Ihrem System einen Alternativnamen zuzuordnen. Der virtuelle Knotenname wird verwendet, um auf die Serverdaten eines anderen Systems zuzugreifen.

0409 E DSM_RC_INVALID_SERVER Servername in Systemoptionsdatei nicht gefunden

Erläuterung

Die Systemoptionsdatei enthält nicht die Option SERVERNAME.

Systemaktion

Die IBM Spectrum Protect-Initialisierung schlägt fehl und das Programm wird beendet.

Benutzeraktion

Verständigen Sie den IBM Spectrum Protect-Administrator für Ihr System und stellen Sie sicher, dass die Systemoptionsdatei den Servernamen enthält.

0410 E DSM_RC_INVALID_KEYWORD Bei der Syntaxanalyse wurde ein ungültiges Optionsschlüsselwort gefunden.

Erläuterung

In der 'dsmInit'-Konfigurationsdatei, in der Optionszeichenfolge, in dsm.sys oder dsm.opt wurde ein ungültiges Optionsschlüsselwort gefunden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Schreibweise der Optionsschlüsselwörter korrigieren. Sicherstellen, daß die 'dsmInit'-Konfigurationsdatei nur eine Untermenge der Optionen in dsm.sys enthält. Das Fehlerprotokoll auf weitere Informationen über den Fehler überprüfen.

0411 S DSM_RC_PATTERN_TOO_COMPLEX Das Einschluss- oder Ausschlussmuster kann nicht syntaktisch analysiert werden.

Erläuterung

Das Muster ist falsch formatiert oder zu komplex und kann nicht interpretiert werden.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Stellen Sie sicher, dass das Einschluss- oder Ausschlussmuster korrekt angegeben ist. Ist das Muster korrekt, bitten Sie die technische Unterstützung von IBM um Hilfe.

0412 S DSM_RC_NO_CLOSING_BRACKET Im Einschluss-/Ausschlussmuster fehlt eine rechte eckige Klammer

Erläuterung

Das Einschluss- oder Ausschlussmuster wurde falsch erstellt. Die rechte eckige Klammer fehlt.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Korrigieren Sie die Syntax für das Muster.

0426 E DSM_RC_CANNOT_OPEN_TRACEFILE Die Initialisierungsfunktionen können die angegebene Ablaufverfolgungsdatei nicht öffnen.

Erläuterung

Die Datei konnte während der Initialisierung nicht geöffnet werden. Der angegebene Pfad ist möglicherweise falsch. Es ist außerdem möglich, dass der aktuelle Benutzer nicht die Berechtigung hat, in die Ablaufverfolgungsdatei im angegebenen Verzeichnis zu schreiben. Es ist ebenfalls möglich, dass am Standort der Ablaufverfolgungsdatei kein Speicherbereich verfügbar ist.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Stellen Sie sicher, dass die Option TRACEFILE auf einen gültigen Pfad zeigt und dass der Benutzer über ordnungsgemäße Berechtigungen verfügt, um in die angegebene Datei zu schreiben.

0427 E DSM_RC_CANNOT_OPEN_LOGFILE Die Initialisierungsfunktionen können die angegebene Fehlerprotokolldatei nicht öffnen.

Erläuterung

Die Fehlerprotokolldatei konnte während der Initialisierung nicht geöffnet werden. Der angegebene Pfad ist möglicherweise falsch. Es ist außerdem möglich, dass der aktuelle Benutzer nicht die Berechtigung hat, in die Protokolldatei im angegebenen Verzeichnis zu schreiben. Es ist ebenfalls möglich, dass am angegebenen Standort der Protokolldatei kein Speicherbereich verfügbar ist.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Stellen Sie sicher, dass die Option LOGFILE auf einen gültigen Pfad zeigt und dass der Benutzer über ordnungsgemäße Berechtigungen verfügt, um in die angegebene Datei zu schreiben.

0600 E DSM_RC_DUP_LABEL Doppelter Datenträgerkennsatz vorhanden. Die Operation kann nicht fortgesetzt werden.

Erläuterung

Für austauschbare Datenträger verwendet IBM Spectrum Protect den Datenträgerkennsatz als Dateibereichsnamen. Um zu verhindern, dass Daten von verschiedenen Datenträgern in demselben Dateibereich auf dem IBM Spectrum Protect-Server gespeichert werden, ist das Sichern oder Archivieren von austauschbaren Datenträgern mit doppelten Datenträgerkennsätzen nicht zulässig.

Systemaktion

Die angeforderte Operation wird nicht ausgeführt.

Benutzeraktion

Ändern Sie die Datenträgerkennsätze auf den austauschbaren Datenträgern, sodass es keine doppelten Kennsätze gibt. Starten Sie dann IBM Spectrum Protect erneut und wiederholen Sie die Operation.

0601 E DSM_RC_NO_LABEL Das Laufwerk hat keinen Kennsatz. Die Operation kann nicht fortgesetzt werden.

Erläuterung

Das Sichern oder Archivieren von austauschbaren Datenträgern erfordert, dass die Datenträger einen Datenträgerkennsatz haben. Es wurde versucht, Daten auf einem austauschbaren Datenträger, der keinen Kennsatz hat, zu sichern oder zu archivieren.

Systemaktion

Die angeforderte Operation wird nicht ausgeführt.

Benutzeraktion

Erstellen Sie einen Datenträgerkennsatz auf dem austauschbaren Datenträger und wiederholen Sie die Operation.

0610 E DSM_RC_NLS_CANT_OPEN_TXT Nachrichtentextdatei kann nicht geöffnet werden.

Erläuterung

Das System kann die Nachrichtentextdatei (dscdeu.txt oder dsmclientV3.cat für AIX) nicht öffnen. Auf der AS/400-Plattform hat diese Datei den Namen QANSAPI/QAANSENU(TXT).

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Prüfen Sie, ob die Datei dscdeu.txt in dem Verzeichnis steht, auf das DSMI_DIR zeigt. Für AIX ist sicherzustellen, dass die Datei dsmclientV3.cat über eine symbolische Verbindung zu /usr/lib/nls/msg/<locale>/dsmclientV3.cat verfügt.

0611 E DSM_RC_NLS_CANT_READ_HDR Nachrichtentextdatei kann nicht verwendet werden.

Erläuterung

Das System kann die Nachrichtentextdatei (dscdeu.text oder dsmclientV3.cat für AIX) auf Grund eines ungültigen Kennsatzes nicht verwenden. Auf der AS/400-Plattform hat diese Datei den Namen QANSAPI/QAANSENU(TXT).

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Nachrichtentextdatei erneut installieren.

0612 E DSM_RC_NLS_INVALID_CNTL_REC Nachrichtentextdatei kann nicht verwendet werden.

Erläuterung

Das System kann die Nachrichtentextdatei (dscdeu.txt oder dsmclientV3.cat für AIX) auf Grund eines ungültigen Steuersatzes nicht verwenden. Auf der AS/400-Plattform hat diese Datei den Namen QANSAPI/QAANSENU(TXT).

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Nachrichtentextdatei erneut installieren.

0613 E DSM_RC_NLS_INVALID_DATE_FMT Ungültigen Wert für DATEFORMAT angegeben.

Erläuterung

Für DATEFORMAT ist ein ungültiger Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Einen gültigen Wert angeben.

0614 E DSM_RC_NLS_INVALID_TIME_FMT Ungültigen Wert für TIMEFORMAT angegeben.

Erläuterung

Für TIMEFORMAT ist ein ungültiger Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Einen gültigen Wert angeben.

0615 E DSM_RC_NLS_INVALID_NUM_FMT Ungültigen Wert für NUMBERFORMAT angegeben.

Erläuterung

Für NUMBERFORMAT ist ein ungültiger Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Einen gültigen Wert angeben.

0620 E DSM_RC_LOG_CANT_BE_OPENED Fehlerprotokolldatei kann nicht geöffnet werden.

Erläuterung

Das System kann die Fehlerprotokolldatei nicht öffnen.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Wert für DSMI_LOG und die Zugriffsberechtigung überprüfen. Auf der AS/400-Plattform den Wert überprüfen, der für ERRORLOGNAME in der API-Optionsdatei angegeben wurde.

0621 E DSM_RC_LOG_ERROR_WRITING_TO_LOG In die Protokolldatei kann nicht geschrieben werden.

Erläuterung

Beim Schreiben in die Protokolldatei ist ein Fehler aufgetreten.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Wert für DSMI_LOG und die Zugriffsberechtigung überprüfen. Auf der AS/400-Plattform den Wert überprüfen, der für ERRORLOGNAME in der API-Optionsdatei angegeben wurde.

0622 E DSM_RC_LOG_NOT_SPECIFIED Der Name der Protokolldatei wurde nicht angegeben.

Erläuterung

Das System kann die Fehlerprotokolldatei nicht öffnen.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Wert für DSMI_LOG und die Zugriffsberechtigung überprüfen. Auf der AS/400-Plattform den Wert überprüfen, der für ERRORLOGNAME in der API-Optionsdatei angegeben wurde.

0927 E DSM_RC_NOT_ADSM_AUTHORIZED Nur ein berechtigter IBM Spectrum Protect-Benutzer kann diese Aktion ausführen.

Erläuterung

Zum Ausführen dieser Aktion muss der Benutzer ein berechtigter IBM Spectrum Protect-Benutzer sein. Benutzer ist nicht kennwortberechtigt, und für diese Aktion ist eine Berechtigung erforderlich.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Der Benutzer muß der Root oder der Eigner der ausführbaren Datei sein, und das Bit zum Definieren der aktuellen Benutzer-ID ('s' Bit) muß auf 'On' gesetzt sein.

961 E DSM_RC_DIRECT_STORAGE_AGENT_UNSUPPORTED Direktverbindung zum Speicheragenten ist nicht zulässig.

Erläuterung

Sie können keine direkte Verbindung zum Speicheragenten herstellen.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Zum Ausführen LAN-freier Operationen mit Hilfe des Speicheragenten müssen Sie die Option ENABLELANFREE in Ihrer Optionsdatei angeben und die Verarbeitung erneut starten.

963 E DSM_RC_FS_NAMESPACE_DOWNLEVEL Der lange Namensbereich wurde aus dem lokalen Dateibereich entfernt. Wenn Sie die Operation zum Sichern/Archivieren fortsetzen wollen, müssen Sie Ihren Dateibereich auf dem Server umbenennen.

Erläuterung

Der Prozess hat festgestellt, dass der Servernamensbereich NTW:LONG lautet, aber der lokale Datenträger unterstützt keine Langnamen. Wenn Sie den Datenträger mit Kurznamen sichern wollen, müssen Sie den Dateibereich auf dem Server umbenennen. Wenn Sie mit Langnamen sichern wollen, müssen Sie dem fraglichen Datenträger die Unterstützung langer Namensbereiche hinzufügen.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Fügen Sie dem Datenträger die Unterstützung langer Namensbereiche hinzu oder benennen Sie den entsprechenden Serverdateibereich um (bzw. entfernen Sie ihn).

0996 E DSM_RC_SERVER_DOWNLEVEL_FUNC Der IBM Spectrum Protect-Server ist nicht auf dem neuesten Stand und unterstützt die angeforderte Funktion

nicht. Das Fehlerprotokoll enthält die Versionsnummer.

Erläuterung

Die Funktion, die verwendet werden soll, erfordert einen aktuelleren IBM Spectrum Protect-Server.

Systemaktion

Die Operation schlägt fehl.

Benutzeraktion

Führen Sie für Ihren IBM Spectrum Protect-Server ein Upgrade auf eine Version durch, die diese Funktion unterstützt. Das Fehlerprotokoll enthält die Versionsnummer.

0997 E DSM_RC_STORAGEAGENT_DOWNLEVEL Der IBM Spectrum Protect-Speicheragent ist nicht auf dem neuesten Stand und unterstützt die angeforderte Funktion nicht. Das Fehlerprotokoll enthält die Versionsnummer.

Erläuterung

Die Funktion, die verwendet werden soll, erfordert einen aktuelleren IBM Spectrum Protect-Speicheragenten.

Systemaktion

Die Operation schlägt fehl.

Benutzeraktion

Führen Sie für Ihren IBM Spectrum Protect-Speicheragenten ein Upgrade auf eine Version durch, die diese Funktion unterstützt. Das Fehlerprotokoll enthält die Versionsnummer.

0998 E DSM_RC_SERVER_AND_SA_DOWNLEVEL Der IBM Spectrum Protect-Server und der IBM Spectrum Protect-Speicheragent sind nicht auf dem neuesten Stand und unterstützen nicht die angeforderte Funktion. Das Fehlerprotokoll enthält die Versionsnummer.

Erläuterung

Die Funktion, die verwendet werden soll, erfordert einen aktuelleren IBM Spectrum Protect-Server und IBM Spectrum Protect-Speicheragenten.

Systemaktion

Die Operation schlägt fehl.

Benutzeraktion

Führen Sie für Ihren IBM Spectrum Protect-Server und IBM Spectrum Protect-Speicheragenten ein Upgrade auf eine Version durch, die diese Funktion unterstützt. Das Fehlerprotokoll enthält die Versionsnummer.

1376 E DSM_RC_DIGEST_VALIDATION_ERROR Fehler bei der Verarbeitung von '*DateibereichsnamePfadnameDateiname*'; End-to-End-Digestprüfung ist fehlgeschlagen.

Erläuterung

Das verschlüsselte Digest der zurückgeschriebenen oder abgerufenen Daten stimmte nicht mit dem während der Sicherungs- oder Archivierungsoperation generierten Digest überein. Mögliche Ursachen sind ein Übertragungsfehler, ein Datenverlust oder eine Hashkollision.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Wiederholen Sie die Zurückschreibungsoperation. Bleibt der Fehler bestehen, bitten Sie die technische Unterstützung von IBM um Hilfe.

2000 E DSM_RC_NULL_OBJNAME Der Objektnamenzeiger ist NULL.

Erläuterung

Für den Objektnamenzeiger ist kein Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Für die Struktur 'dsmObjName' eine Adresse zur Verfügung stellen.

2001 E DSM_RC_NULL_DATABLKPTR Der Datenblockzeiger ist NULL.

Erläuterung

Für den Datenblockzeiger ist kein Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Für die Struktur 'DataBlk' eine Adresse zur Verfügung stellen.

2002 E DSM_RC_NULL_MSG Nachrichtenparameter für 'dsmRCMsg' ist ein Nullzeiger.

Erläuterung

Der Nachrichtenparameter für 'dsmRCMsg' ist ein Nullzeiger.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Für den Nachrichtenparameter genügend Speicherbereich zuordnen.

2004 E DSM_RC_NULL_OBJATTRPTR Der Objektattributzeiger ist NULL.

Erläuterung

Für den Objektattributzeiger ist kein Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Für die Struktur 'ObjAttr' eine Adresse zur Verfügung stellen.

2006 E DSM_RC_NO_SESS_BLK Keine Informationen für Server-Sitzung vorhanden.

Erläuterung

Der Server hat nicht mit den Sitzungsinformationen geantwortet.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Server-Status überprüfen.

2007 E DSM_RC_NO_POLICY_BLK Keine Server-Maßnahmeninformationen vorhanden.

Erläuterung

Der Server hat nicht mit den Maßnahmeninformationen geantwortet.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Server-Maßnahmendefinitionen überprüfen.

2008 E DSM_RC_ZERO_BUFLEN Der Wert für 'dataBlk bufferLen' ist Null.

Erläuterung

Der Wert für 'dataBlk bufferLen' ist Null.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Einen Wert ungleich Null für 'bufferLen' angeben.

2009 E DSM_RC_NULL_BUFPTR Der Wert für 'dataBlk bufferPtr' ist NULL.

Erläuterung

Für 'dataBlk bufferPtr' ist kein Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Für 'bufferPtr' eine Adresse zur Verfügung stellen.

2010 E DSM_RC_INVALID_OBJTYPE Der Wert für 'objType' ist ungültig.

Erläuterung

Der Wert für 'objType' ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Wert für 'dsmObjName.objType' muss lauten:

- DSM_OBJ_FILE oder DSM_OBJ_DIRECTORY für Sichern
- DSM_OBJ_FILE für Archivieren

2011 E DSM_RC_INVALID_VOTE Der Wert für 'dsmEndTxn' ist ungültig.

Erläuterung

Der Wert für 'dsmEndTxn' ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Wert muß DSM_VOTE_COMMIT oder DSM_VOTE_ABORT lauten.

2012 E DSM_RC_INVALID_ACTION Die Aktualisierungsaktion ist ungültig.

Erläuterung

Die Aktion 'dsmUpdateFS' oder 'dsmUpdateObj' ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Aktionswert korrigieren. Gültige Werte sind in dsmapitd.h definiert und in dem Handbuch zur Verwendung der API dokumentiert.

2014 E DSM_RC_INVALID_DS_HANDLE Es ist ein Fehler in den internen IBM Spectrum Protect-API-Prozeduren aufgetreten.

Erläuterung

Das System hat einen Fehler in den internen API-Prozeduren festgestellt.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Prozeß beenden und die Operation wiederholen. Sicherstellen, daß alle vorherigen dsmInit-Aufrufe bereinigt und durch einen dsmTerminate-Aufruf beendet wurden. Bleibt der Fehler bestehen, den Systemadministrator oder Kundendienst verständigen.

2015 E DSM_RC_INVALID_REPOS Die Repository-Art ist ungültig.

Erläuterung

Die Repository-Art ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Für 'dsmDeleteFS' muss das Repository wie folgt lauten:

- DSM_ARCHIVE_REP
- DSM_BACKUP_REP
- DSM_REPOS_ALL.

2016 E DSM_RC_INVALID_FSNAME Dateibereichsname muß mit dem Verzeichnisbegrenzer beginnen.

Erläuterung

Der Dateibereichsname ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Dateibereichsname muss mit dem Verzeichnisbegrenzer beginnen.

2017 E DSM_RC_INVALID_OBJNAME Objektname ist entweder leer oder hat keinen führenden Begrenzer.

Erläuterung

Der Objektname ist ungültig, da er eine leere Zeichenfolge ist oder keinen führenden Begrenzer aufweist.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Format des vollständigen Pfads für 'dsmObjName' überprüfen.

2018 E DSM_RC_INVALID_LLNAME Untergeordnetes Qualifikationsmerkmal des Objektnamens muß mit dem Verzeichnisbegrenzer beginnen.

Erläuterung

Das untergeordnete Qualifikationsmerkmal des Objektnamens ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das untergeordnete Qualifikationsmerkmal des Objektnamens mit dem Verzeichnisbegrenzer beginnen.

2019 E DSM_RC_INVALID_OBJOWNER Der Objekteigner ist ungültig.

Erläuterung

Der Objekteigner muß entweder der Root sein oder der Objekteigner muß mit dem Sitzungseigner übereinstimmen.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Sitzungseigner und Objekteigner überprüfen.

2020 E DSM_RC_INVALID_ACTYPE Der Wert für 'dsmBindMC sendType' ist ungültig.

Erläuterung

Der Wert für 'dsmBindMC sendType' ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Wert für 'sendType' muss wie folgt lauten:

- stBackup
- stArchive
- stBackupMountWait
- stArchiveMountWait

2021 E DSM_RC_INVALID_RETCODE Kein Text für diesen Rückkehrcode verfügbar.

Erläuterung

Der Parameter 'dsmRC' für 'dsmRCMsg' ist ein nicht unterstützter Rückkehrcode.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Einen gültigen Wert angeben.

2022 E DSM_RC_INVALID_SENDTYPE Der Wert für 'dsmSendObj sendType' ist ungültig.

Erläuterung

Der Wert für 'dsmSendObj sendType' ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Wert für 'sendType' muss wie folgt lauten:

- stBackup
- stArchive
- stBackupMountWait
- stArchiveMountWait

2023 E DSM_RC_INVALID_PARAMETER Der Wert für 'dsmDeleteObj delType' ist ungültig.

Erläuterung

Der Wert für 'dsmDeleteObj delType' ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Wert für 'delType' muss 'dtBackup' oder 'dtArchive' lauten.

2024 E DSM_RC_INVALID_OBJSTATE Der Wert für 'qryBackupData objState' ist ungültig.

Erläuterung

Der Wert für 'qryBackupData objState' ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Wert für 'qryBackupData.objState' muss wie folgt lauten:

- DSM_ACTIVE
- DSM_INACTIVE
- DSM_ANY_MATCH

2025 E DSM_RC_INVALID_MCNAME Der Name der Verwaltungsklasse wurde nicht gefunden.

Erläuterung

Bei einer Abfrage- oder Sendeoperation konnte der Name der Verwaltungsklasse nicht gefunden werden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Namen der Verwaltungsklasse überprüfen.

2026 E DSM_RC_INVALID_DRIVE_CHAR Der Laufwerkbuchstabe ist kein alphabetisches Zeichen.

Erläuterung

Der Laufwerkbuchstabe ist kein alphabetisches Zeichen. Dieser Rückkehrcode ist nur für Microsoft Windows gültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Sicherstellen, dass die Laufwerkbezeichnung ein alphabetisches Zeichen ist. Das Feld, auf das verwiesen wird, ist 'dsmDosFSAttrib.driveLetter'.

2027 E DSM_RC_NULL_FSNAME Der Wert für 'Dateibereichsname registrieren' ist NULL.

Erläuterung

Für das Registrieren des Dateibereichsnamens ist kein Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Einen Dateibereichsnamen in 'dsmRegisterFS' angeben.

2028 E DSM_RC_INVALID_HLNAME Übergeordnetes Qualifikationsmerkmal des Objektnamens muß mit dem Verzeichnisbegrenzer beginnen.

Erläuterung

Das übergeordnete Qualifikationsmerkmal des Objektnamens ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das übergeordnete Qualifikationsmerkmal des Objektnamens muss mit dem Verzeichnisbegrenzer beginnen.

2029 E DSM_RC_NUMOBJ_EXCEED Die Anzahl Objekte in 'dsmBeginGetData' überschreitet DSM_MAX_GET_OBJ | DSM_MAX_PARTIAL_GET_OBJ.

Erläuterung

Die Anzahl der Objekte (numObjId), die in dem Aufruf 'dsmBeginGetData' angegeben wurde, überschreitet DSM_MAX_GET_OBJ | DSM_MAX_PARTIAL_GET_OBJ.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Anzahl der Objekte überprüfen, bevor 'dsmBeginGetData' aufgerufen wird. Ist die Anzahl größer als DSM_MAX_GET_OBJ | DSM_MAX_PARTIAL_GET_OBJ, mehrere Get-Aufrufe ausgeben.

2030 E DSM_RC_NEWPW_REQD Der Wert für das neue Kennwort ist NULL oder leer.

Erläuterung

Für das neue Kennwort ist kein Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Ein neues Kennwort in 'dsmChangePW' angeben.

2031 E DSM_RC_OLDPW_REQD Der Wert für das alte Kennwort ist NULL oder leer.

Erläuterung

Für das alte Kennwort ist kein Wert angegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Ein altes Kennwort in 'dsmChangePW' angeben.

2032 E DSM_RC_NO_OWNER_REQD In dsmInit darf der Eigner bei PASSWORDACCESS=generate keine Sitzung aufbauen.

Erläuterung

PASSWORDACCESS=GENERATE baut eine Sitzung mit dem aktuellen Anmeldebenutzer als Eigner auf. Die Anwendung sollte clientOwnerNameP auf NULL setzen, wenn PASSWORDACCESS=GENERATE aktiv ist.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.Ob die Anwendung die Verarbeitung fortsetzen kann, hängt davon ab, wie die Anwendung den Fehler handhabt.

Benutzeraktion

Diese Nachricht gilt für Anwendungen, die die IBM Spectrum Protect-API verwenden, und ist primär für den Anbieter der Anwendung bestimmt, für die die Nachricht ausgegeben wird. Abhängig von der Anwendung könnte dies ein Konfigurationsproblem sein.

Schlagen Sie in der Dokumentation für die Anwendung nach und prüfen Sie, ob die Anwendung korrekt konfiguriert ist. Bleibt der Fehler bestehen, verständigen Sie zwecks weiterer Unterstützung den Lieferanten der Anwendung.

2033 E DSM_RC_NO_NODE_REQD In 'dsmInit' ist die Angabe des Knotens nicht zulässig, wenn PASSWORDACCESS=generate.

Erläuterung

Bei PASSWORDACCESS=generate wird eine Sitzung mit dem aktuellen Hostnamen als Knoten aufgebaut.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Wird PASSWORDACCESS=generate verwendet, clientNodeNameP auf NULL setzen.

2034 E DSM_RC_KEY_MISSING Die Schlüsseldatei fehlt.

Erläuterung

Die Schlüsseldatei für Data Protection for Oracle wurde nicht gefunden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Stellen Sie sicher, dass Sie Data Protection for Oracle bestellt haben, und installieren Sie die Schlüsseldatei.

2035 E DSM_RC_KEY_BAD Der Inhalt der Schlüsseldatei ist ungültig.

Erläuterung

Der Inhalt der Schlüsseldatei für Data Protection for Oracle ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Stellen Sie sicher, dass Sie Data Protection for Oracle bestellt haben, und installieren Sie die Schlüsseldatei.

2041 E DSM_RC_BAD_CALL_SEQUENCE Die Reihenfolge der Aufrufe ist ungültig.

Erläuterung

Für die Anwendungsprogrammierschnittstelle (API) müssen Funktionsaufrufe in einer bestimmten Reihenfolge erfolgen. Die Funktionsaufrufe wurden nicht in der erwarteten Reihenfolge ausgeführt. Der Fehler kann durch folgende Probleme ausgelöst werden:

- Netzfehler
- Fehler in der IBM Spectrum Protect-API.
- Fehler im IBM Spectrum Protect-Server.
- Fehler in der Anwendung (IBM oder anderer Anbieter), von der die IBM Spectrum Protect-API verwendet wird.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Mögliche Aktionen des Endbenutzers:

- Überprüfen Sie das Netz auf Fehler.
- Suchen Sie nach Hinweisen in der Aktivitätenprotokolldatei des IBM Spectrum Protect-Servers, in der Protokolldatei 'dsierror.log' auf der Clientseite und in den Protokolldateien der betroffenen fehlerhaften Anwendung.
- Suchen Sie auf den IBM-Unterstützungsseiten nach APARs, in denen das Problem behandelt wird. Die Unterstützungssite befindet sich unter IBM Spectrum Protect Support Portal.
- Wurde die API-Anwendung von einem anderen Anbieter (nicht IBM) entwickelt, suchen Sie auf den Unterstützungsseiten des anderen Anbieters nach bekannten Problemen, die Ihrem Problem entsprechen.

Lässt sich das Problem durch keine der genannten Maßnahmen lösen, wenden Sie sich an den Anbieter der Anwendung, von der die IBM Spectrum Protect-API verwendet wird, um das Problem zu melden.

Ein Entwickler einer Anwendung, die die IBM Spectrum Protect-API verwendet, muss die Fehlerursache untersuchen. Hierzu gehört auch die Überprüfung des Zustandsdiagramms der IBM Spectrum Protect-API. Das IBM Spectrum Protect-API-Zustandsdiagramm befindet sich in der Produktdokumentation bei Produktdokumentation für IBM Spectrum Protect.

2042 E DSM_RC_INVALID_TSMBUFFER tsmBuffHandle ist ungültig oder der Wert von dataPtr ist ungültig.

Erläuterung

Ein ungültiger Wert für eine interne Kennung oder einen dataPtr wurde an die API übergeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Es gibt ein Problem mit der aufrufenden Anwendung. Prüfen Sie die an die API übergebenen Werte von tsmBuffHandle und dataptr.

2043 E DSM_RC_TOO_MANY_BYTES Die Anzahl Byte, die in den tsmBuffer kopiert wurden, ist größer als der zulässige Wert.

Erläuterung

Es wurde eine ungültige Anzahl Byte in einen tsmBuffer kopiert.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Es gibt ein Problem mit der aufrufenden Anwendung. Prüfen Sie die Anzahl Byte, die in den tsmBuffer kopiert wurden.

2044 E DSM_RC_MUST_RELEASE_BUFFER dsmTerminate kann nicht beendet werden, da die Anwendung an 1 oder mehreren tsmBuffers festhält.

Erläuterung

Eine Anwendung versucht, eine Sitzung zu beenden, aber sie hält immer noch an einigen tsmBuffers fest.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Anwendung muss alle Puffer für diese Sitzung durch Aufruf von tsmReleaseBuffer zurückgeben und anschließend dsmTerminate absetzen.

2045 E DSM_RC_BUFF_ARRAY_ERROR Interner Fehler im tsmBuffer-Bereich.

Erläuterung

Es ist ein interner Fehler im API-Pufferbereich aufgetreten.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator oder Kundendienst verständigen.

2046 E DSM_RC_INVALID_DATABLK Bei Verwendung von useTsmBuffers muss dataBlk in Aufrufen von dsmSendObj und dsmGetObj NULL sein.

Erläuterung

Der Wert für dataBlk muss NULL sein, wenn useTsmBuffers verwendet wird.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Es gibt ein Problem mit der aufrufenden Anwendung. Verständigen Sie Ihren Anwendungslieferanten.

2047 E DSM_RC_ENCR_NOT_ALLOWED Verschlüsselung ist bei Verwendung von useTsmBuffers nicht zulässig.

Erläuterung

useTsmBuffers unterstützt keine Verschlüsselung.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Wiederholen Sie die Operation ohne Verwendung von useTsmBuffers, oder inaktivieren Sie die Verschlüsselung für diese Operation.

2048 E DSM_RC_OBJ_COMPRESSED Dieses Objekt kann nicht mit useTsmBuffers zurückgeschrieben/abgerufen werden, da es komprimiert ist.

Erläuterung

useTsmBuffers unterstützt keine Komprimierung.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Wiederholen Sie die Operation ohne Verwendung von useTsmBuffers.

2049 E DSM_RC_OBJ_ENCRYPTED Dieses Objekt kann nicht mit useTsmBuffers zurückgeschrieben/abgerufen werden, da es verschlüsselt ist.

Erläuterung

useTsmBuffers unterstützt keine Verschlüsselung.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Wiederholen Sie die Operation ohne Verwendung von useTsmBuffers.

2050 E DSM_RC_WILDCHAR_NOTALLOWED In 'dsmSendObj' sind für 'objName' keine Platzhalterzeichen zulässig.

Erläuterung

In 'dsmSendObj' sind für 'objName' keine Platzhalterzeichen zulässig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

'fs', 'hl' und 'll' für 'dsmObjName' angeben.

2051 E DSM_RC_POR_NOT_ALLOWED Bei Verwendung von useTsmBuffers ist ein Zurückschreiben/Abrufen mit Teilobjektzurückschreibung nicht zulässig.

Erläuterung

useTsmBuffers unterstützt keine Teilobjektzurückschreibung.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Stellen Sie sicher, dass die aufrufende Anwendung entweder Teilobjektzurückschreibung oder useTsmBuffers verwendet.

2052 E DSM_RC_NO_ENCRYPTION_KEY Kein Chiffrierschlüssel gefunden. Bei Verwendung von -encryptkey=prompt müssen Sie sicherstellen, dass das Feld encryptionPasswordP einen Wert aufweist und dass bEncryptKeyEnabled auf wahr gesetzt ist.

Erläuterung

Es wurde kein Chiffrierschlüssel in der Kennwortdatei gefunden, oder es wurde von der Anwendung kein Schlüssel zur Verfügung gestellt.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Bei Verwendung von -encryptkey=prompt müssen Sie sicherstellen, dass encryptionPasswordP einen Wert aufweist und dass bEncryptKeyEnabled auf wahr gesetzt ist.

2053 E DSM_RC_ENCR_CONFLICT Es wurden unverträgliche Chiffrierschlüsseloptionen angegeben.

Erläuterung

Bei Verwendung der Option ENABLEENCRYPTKEY darf der Parameter bEncryptKeyEnabled für die IBM Spectrum Protect-API-Strukturen 'dsmInitExIn_t' und 'tsmInitExIn_t' nicht auf 'bTrue' gesetzt werden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Entfernen Sie die Option ENABLEENCRYPTKEY aus der Optionsdatei oder setzen Sie den Parameter 'bEncryptKeyEnabled' mit Hilfe der IBM Spectrum Protect-API im Programm auf 'bFalse'.

2060 E DSM_RC_FSNAME_NOTFOUND Der Dateibereich, der gelöscht/dessen Zugriff definiert werden soll, kann nicht gefunden werden.

Erläuterung

Der zu löschende Dateibereich kann nicht gefunden werden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Dateibereichsnamen überprüfen.

2061 E DSM_RC_FS_NOT_REGISTERED In 'dsmSendObj', 'dsmDeleteObj' oder 'dsmUpdateFS' ist der Dateibereich nicht registriert.

Erläuterung

In 'dsmSendObj', 'dsmDeleteObj' oder 'dsmUpdateFS' ist der Dateibereich nicht registriert.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Dateibereichsnamen überprüfen.

2062 W DSM_RC_FS_ALREADY_REGED In 'dsmRegisterFS' ist der Dateibereich bereits registriert.

Erläuterung

In 'dsmRegisterFS' ist der Dateibereich bereits registriert.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Dateibereichsnamen überprüfen.

2063 E DSM_RC_OBJID_NOTFOUND In 'dsmBeginGetData' ist die 'objID' NULL.

Erläuterung

In 'dsmBeginGetData' ist die 'objID' NULL.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Stellen Sie Folgendes sicher:

- 'dsmGetList' ist nicht NULL.
- Jede 'objID' ist nicht NULL.
- 'dsmGetList numObjId' ist nicht Null.

2064 E DSM_RC_WRONG_VERSION In 'dsmInit' weicht die API-Version des aufrufenden Programms von der IBM Spectrum Protect-Bibliotheksversion ab.

Erläuterung

In 'dsmInit' ist die API-Version des aufrufenden Programms höher als die IBM Spectrum Protect-Bibliotheksversion.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Installieren Sie die neueste IBM Spectrum Protect-API-Bibliothek.

2065 E DSM_RC_WRONG_VERSION_PARM Die Strukturversion des aufrufenden Programms weicht von der IBM Spectrum Protect-Bibliotheksversion ab.

Erläuterung

Die Strukturversion des aufrufenden Programms weicht von der IBM Spectrum Protect-Bibliotheksversion ab.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Sicherstellen, daß das Feld 'stVersion' mit dem Wert in der Kopfdatei definiert wird. Die Anwendung mit den neuesten Kopfdateien erneut kompilieren.

2070 E DSM_RC_NEEDTO_ENDTXN 'dsmEndTxn' ausgeben und dann eine neue Transaktionssitzung beginnen.

Erläuterung

Aus einem der folgenden Gründe muß diese Transaktion beendet und eine neue Transaktion gestartet werden:

- Der Zielort hat sich geändert.
- Die Bytegrenze wurde überschritten.
- Die maximale Anzahl Objekte wurde überschritten.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

'dsmEndTxn' ausgeben und eine neue Transaktionssitzung starten.

2080 E DSM_RC_OBJ_EXCLUDED Das Sicherungs- oder Archivierungsobjekt ist von der Verarbeitung ausgeschlossen.

Erläuterung

Das Sicherungs- oder Archivierungsobjekt ist von der Verarbeitung ausgeschlossen.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

'objName' und die Ausschlußlisten überprüfen.

2081 E DSM_RC_OBJ_NOBCG Das Sicherungsobjekt hat keine Kopiengruppe.

Erläuterung

Das Sicherungsobjekt hat keine Kopiengruppe.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Server-Maßnahmendefinitionen überprüfen.

2082 E DSM_RC_OBJ_NOACG Das Archivierungsobjekt hat keine Kopiengruppe.

Erläuterung

Das Archivierungsobjekt hat keine Kopiengruppe.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Server-Maßnahmendefinitionen überprüfen.

2090 E DSM_RC_APISYSTEM_ERROR Der von der IBM Spectrum Protect-API verwendete Speicher wurde beschädigt.

Erläuterung

Der von der IBM Spectrum Protect-API verwendete Speicher wurde beschädigt.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, den Systemadministrator oder Kundendienst verständigen.

2100 E DSM_RC_DESC_TOOLONG Die 'sendObj'-Archivierungsbeschreibung ist zu lang.

Erläuterung

Die 'sendObj'-Archivierungsbeschreibung ist zu lang.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Zeichenfolge für 'sndArchiveData.descr' muß kleiner-gleich DSM_MAX_DESCR_LENGTH sein.

2101 E DSM_RC_OBJINFO_TOOLONG 'sendObj ObjAttr.objInfo' ist zu lang.

Erläuterung

'sendObj ObjAttr.objInfo' ist zu lang.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Feld 'objInfo' muß kleiner-gleich DSM_MAX_OBJINFO_LENGTH sein.

2102 E DSM_RC_HL_TOOLONG 'sendObj dsmObjName.hl' ist zu lang.

Erläuterung

'sendObj dsmObjName.hl' ist zu lang.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Feld 'hl' muss kleiner-gleich DSM_MAX_HL_LENGTH sein.

2103 E DSM_RC_PASSWD_TOOLONG Das Kennwort oder die Zeichenfolge für encryptionPassword ist zu lang.

Erläuterung

Der für password oder encryptionPassword zur Verfügung gestellte Wert ist zu lang.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Feld Kennwort oder Verschlüsselungskennwort (password oder encryptionPassword) muss kleiner sein als DSM_MAX_VERIFIER_LENGTH.

2104 E DSM_RC_FILESPACE_TOOLONG 'sendObj dsmObjName.fs' ist zu lang.

Erläuterung

'sendObj dsmObjName.fs' ist zu lang.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Feld 'fs' muss kleiner-gleich DSM_MAX_FS_LENGTH sein.

2105 E DSM_RC_LL_TOOLONG 'sendObj dsmObjName.ll' ist zu lang.

Erläuterung

'sendObj dsmObjName.ll' ist zu lang.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Feld 'll' muss kleiner-gleich DSM_MAX_LL_LENGTH sein.

2106 E DSM_RC_FSINFO_TOOLONG In 'RegisterFS' oder 'UpdateFS' ist 'fsInfo' der Dateisystemattribute zu lang.

Erläuterung

In 'RegisterFS' oder 'UpdateFS' ist 'fsInfo' der Dateisystemattribute zu lang.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Feld 'fsInfo' muss kleiner-gleich DSM_MAX_FSINFO_LENGTH sein.

2107 E DSM_RC_SENDDATA_WITH_ZERO_SIZE Daten mit einer Größenschätzung von Null Byte können nicht gesendet werden.

Erläuterung

Sie können keine Daten für ein Objekt mit einer Größenschätzung = 0 senden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Definieren Sie die Größenschätzung in dsmSendObj größer als 0.

2110 E DSM_RC_INVALID_ACCESS_TYPE Die Zugriffsart dsmSetAccess ist ungültig.

Erläuterung

Die Zugriffsart dsmSetAccess ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Zulässige Werte für die Zugriffsart:

- atBackup
- atArchive

2111 E DSM_RC_QUERY_COMM_FAILURE Übertragungsfehler mit Server bei Objektabfrage

Erläuterung

Während einer Objektabfrage auf dem Server ist ein unerwarteter Übertragungsfehler aufgetreten.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Prüfen, ob die Übertragung zwischen dem Client und den Server-Maschinen aktiv ist. Ausfälle des Servers, des Prozessors und der DFV-Steuereinheit können diesen Fehler verursachen.

2112 E DSM_RC_NO_FILES_BACKUP Für diesen Dateinamen/Dateibereich wurden noch keine Dateien gesichert.

Erläuterung

Es wurde versucht, den Zugriff auf Dateien festzulegen. Es wurden jedoch zuvor keine Dateien für den angegebenen Dateinamen, das angegebene Laufwerk oder das angegebene Dateisystem gesichert.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Sicherstellen, daß das korrekte Laufwerk oder Dateisystem angegeben wurde und Dateien zum Festlegen des Zugriffs gesichert wurden.

2113 E DSM_RC_NO_FILES_ARCHIVE Für diesen Dateinamen/Dateibereich wurden noch keine Dateien archiviert.

Erläuterung

Es wurde versucht, den Zugriff auf Dateien festzulegen. Es wurden jedoch zuvor keine Dateien für den angegebenen Dateinamen, das angegebene Laufwerk oder das angegebene Dateisystem archiviert.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Sicherstellen, daß das korrekte Laufwerk oder Dateisystem angegeben wurde und Dateien zum Festlegen des Zugriffs archiviert wurden.

2114 E DSM_RC_INVALID_SETACCESS Ungültiges Format für Befehl SET ACCESS.

Erläuterung

Der Befehl SET ACCESS muss mindestens drei Operanden aufweisen, von denen der erste Operand entweder BACKUP oder ARCHIVE sein muss. Darauf muss eine Dateispezifikation mit einem gültigen Format folgen.

Systemaktion

Die Verarbeitung wird gestoppt. Der Befehl wird nicht ausgeführt.

Benutzeraktion

Verwenden Sie den Befehl HELP SET ACCESS, um ausführliche Informationen zur Syntax aufzurufen. Geben Sie dann den Befehl SET ACCESS mit der korrekten Syntax ein.

2120 E DSM_RC_STRING_TOO_LONG Die folgende Nachricht war für die Protokollierung auf dem Server zu lang: '*Gekürzte Nachricht mit Nachrichtennummer*'

Erläuterung

Der Nachrichtentext und die Einfügungen sind zu lang, um sie im verfügbaren internen Puffer an den Server senden zu können.

Systemaktion

Die Nachricht *Nachrichtennummer* wird in das lokale Clientfehlerprotokoll geschrieben, anschließend gekürzt und dann als Teil dieser Nachricht an den Server gesendet. Die Nachricht wird gekürzt, indem '...' in der Mitte der Originalnachricht eingesetzt wird.

Benutzeraktion

Die Nachricht, auf die Bezug genommen wird, wurde gekürzt, beschreibt aber den Fehler, der aufgetreten ist. Die Dokumentation für diese Nachricht enthält weitere Informationen.

2200 I DSM_RC_MORE_DATA In 'dsmGetNextQObj' oder 'dsmGetData' sind weitere Daten verfügbar.

Erläuterung

In 'dsmGetNextQObj' oder 'dsmGetData' sind weitere Daten verfügbar.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Funktion erneut aufrufen.

2210 E DSM_RC_BUFF_TOO_SMALL Der 'dataBlk'-Puffer ist für die Abfrageantwort zu klein.

Erläuterung

Der 'dataBlk'-Puffer ist für die Abfrageantwort zu klein.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

In 'dsmGetNextQObj' sicherstellen, dass der 'dataBlk'-Puffer mindestens so groß wie die Abfrageantwortstruktur ist.

2228 E DSM_RC_NO_API_CONFIGFILE Die in 'dsmInit' angegebene Konfigurationsdatei kann nicht geöffnet werden.

Erläuterung

Die in 'dsmInit' angegebene Konfigurationsdatei kann nicht geöffnet werden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Dateinamen überprüfen.

2229 E DSM_RC_NO_INCLEXCL_FILE Die Datei mit Einschluß-/Ausschlußdefinitionen wurde nicht gefunden.

Erläuterung

Die Datei mit Einschluß-/Ausschlußdefinitionen wurde nicht gefunden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Den Dateinamen in der Option 'Inclexcl' überprüfen.

2230 E DSM_RC_NO_SYS_OR_INCLEXCL Entweder wurde die Datei dsm.sys nicht gefunden oder die in dsm.sys angegebene Einschluß-/Ausschlußdatei wurde nicht gefunden.

Erläuterung

Entweder wurde die Datei dsm.sys nicht gefunden oder die in dsm.sys angegebene Einschluß-/Ausschlußdatei wurde nicht gefunden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Die Datei dsm.sys muß sich in dem Verzeichnis befinden, auf das durch die Umgebungsvariable DSMI_DIR verwiesen wird. Den Dateinamen in der Option 'Inclexcl' in der Datei dsm.sys überprüfen.

2231 E DSM_RC_REJECT_NO_POR_SUPPORT Abrufen partieller Objekte wird auf diesem Server nicht unterstützt.

Erläuterung

Der vom Benutzer angegebene IBM Spectrum Protect-Server unterstützt nicht den Abruf eines Teilobjekts.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Einen IBM Spectrum Protect-Server angeben, der das Abrufen partieller Objekte unterstützt.

2300 E DSM_RC_NEED_ROOT Nur ein UNIX-Root darf 'dsmChangePW' oder 'dsmDeleteFS' ausführen.

Erläuterung

Nur ein UNIX-Root kann 'dsmChangePW' oder 'dsmDeleteFS' ausführen.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Dieses Programm als Root ausführen.

2301 E DSM_RC_NEEDTO_CALL_BINDMC 'dsmBindMC' muß vor 'dsmSendObj' ausgegeben werden.

Erläuterung

'dsmBindMC' muß vor 'dsmSendObj' ausgegeben werden.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Programm ändern.

2302 I DSM_RC_CHECK_REASON_CODE Der Wert für 'dsmEndTxn' lautet ABORT; das Feld für den Grund überprüfen.

Erläuterung

Nach einem Aufruf 'dsmEndTxn' wird die Transaktion durch den Server oder den Client mit DSM_VOTE_ABORT abgebrochen und der Grund wird zurückgegeben.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Das Feld für den Grund auf den Code überprüfen, mit dem angegeben wird, warum die Transaktion abgebrochen wurde.

2400 E DSM_RC_ALMGR_OPEN_FAIL Lizenzdatei konnte nicht geöffnet werden.

Erläuterung

Die Lizenzdatei wurde nicht gefunden oder konnte aufgrund von Berechtigungen nicht geöffnet werden, oder die Datei ist beschädigt.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Überprüfen Sie die Berechtigungen für die Datei. Überprüfen Sie, ob sich die Lizenzdatei an der korrekten Position befindet.

2401 E DSM_RC_ALMGR_READ_FAIL Lesefehler bei Lizenzdatei.

Erläuterung

Die Lizenzdatei wurde nicht gefunden, die Datei konnte aufgrund der Berechtigungen nicht geöffnet werden oder die Datei ist beschädigt.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Überprüfen Sie die Berechtigungen für die Datei. Überprüfen Sie, ob sich die Lizenzdatei an der korrekten Position befindet.

2402 E DSM_RC_ALMGR_WRITE_FAIL Schreibfehler bei Lizenzdatei.

Erläuterung

Die Lizenzdatei wurde nicht gefunden oder konnte aufgrund von Berechtigungen nicht geöffnet werden, oder die Datei ist beschädigt.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Überprüfen Sie die Berechtigungen für die Datei. Prüfen, ob sich die Lizenzdatei an der korrekten Position befindet.

2403 E DSM_RC__ALMGR_DATA_FMT Daten in der Lizenzdatei haben ungültiges Format.

Erläuterung

Die Lizenzdatei ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Benutzer muß eine neue Lizenz anfordern.

2404 E DSM_RC_ALMGR_CKSUM_BAD Die Kontrollsumme in der Lizenzdatei stimmt nicht mit der Zeichenfolge der Lizenzregistrierung überein.

Erläuterung

Die Registrierungszeichenfolge ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Benutzer muß eine neue Lizenz anfordern.

2405 E DSM_RC_ALMGR_TRIAL_EXPRD Abgelaufene Testlizenz.

Erläuterung

Die Registrierungszeichenfolge ist ungültig.

Systemaktion

Das System kehrt zur aufrufenden Prozedur zurück.

Benutzeraktion

Der Benutzer muß eine neue Lizenz anfordern.

4580 E DSM_RC_ENC_WRONG_KEY Fehler bei der Verarbeitung von '*DateibereichsnamePfadnameDateiname*'; ungültiger Verschlüsselungsschlüssel.

Erläuterung

Der Schlüssel, den Sie eingegeben haben, stimmt nicht mit dem Schlüssel überein, der beim Sichern für das Verschlüsseln der Datei verwendet wurde. Die Datei kann erst dann zurückgeschrieben werden, wenn der übereinstimmende Schlüssel eingegeben wird.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Wiederholen Sie die Zurückschreibungsoperation und stellen Sie den korrekten Schlüssel zur Verfügung.

4582 E DSM_RC_ENC_NOT_AUTHORIZED Benutzer ist zum Verschlüsseln von *DateibereichsnameVerzeichnispfadDateiname* nicht berechtigt.

Erläuterung

Der Benutzer ist nicht berechtigt, die Datei zu verschlüsseln. Normalerweise kann nur ein für IBM Spectrum Protect berechtigter Benutzer oder ein Root die IBM Spectrum Protect-Verschlüsselung verwenden. Eine bestimmte Kombination aus den Optionen PASSWORDACCESS und ENCRYPTKEY ermöglicht jedoch gegebenenfalls Verschlüsselungsoperationen durch einen nicht berechtigten Benutzer.

Systemaktion

Die Datei wird nicht gesichert oder zurückgeschrieben.

Benutzeraktion

Melden Sie sich als Root oder als berechtigter IBM Spectrum Protect-Benutzer an und wiederholen Sie die Operation. Im IBM Spectrum Protect Clients für Sichern/Archivieren Installations- und Benutzerhandbuch wird die korrekte Verwendung der Option ENCRYPTKEY beschrieben.

4584 E DSM_RC_ENC_TYPE_UNKOWN Fehler bei der Verarbeitung von '*DateibereichsnamePfadnameDateiname*': Verschlüsselungstyp nicht unterstützt.

Erläuterung

Die Dateien, die Sie zurückzuschreiben oder abzurufen versuchen, wurden von einer neueren Version des IBM Spectrum Protect-Clients gesichert oder archiviert. Das Dateiverschlüsselungsverfahren wird vom aktuellen Client nicht unterstützt.

Systemaktion

Das Objekt wird übersprungen.

Benutzeraktion

Sie müssen die Datei mit der neuesten Version des IBM Spectrum Protect-Clients zurückschreiben oder abrufen.

4600 E DSM_RC_CLUSTER_INFO_LIBRARY_NOT_LOADED CLUSTERNODE ist auf YES gesetzt, aber der Clusterinformationsdämon wurde nicht gestartet.

Erläuterung

Der HACMP-Clusterinformationsdämon muss gestartet sein, damit die Option CLUSTERNODE angegeben werden kann.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Starten Sie den HACMP-Clusterinformationsdämon.

4601 E DSM_RC_CLUSTER_LIBRARY_INVALID CLUSTERNODE ist auf YES gesetzt, aber die Clusterladebibliothek ist ungültig.

Erläuterung

Die Ladebibliothek, die das Betriebssystem zur Verfügung stellt, um den Clusternamen zu erhalten, ist nicht gültig. Mögliche Ursache ist eine veraltete Ladebibliothek, die nicht die richtigen Routinen enthält, die dieses Produkt erwartet.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Stellen Sie sicher, dass die neueste Cluster-Software auf dem System installiert ist.

4602 E DSM_RC_CLUSTER_LIBRARY_NOT_LOADED CLUSTERNODE ist auf YES gesetzt, aber die Cluster-Software ist auf diesem System nicht verfügbar.

Erläuterung

Die Ladebibliothek, die das Betriebssystem zur Verfügung stellt, um den Clusternamen zu erhalten, ist auf diesem System nicht verfügbar.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Stellen Sie sicher, dass die Cluster-Software auf dem System installiert ist.

4603 E DSM_RC_CLUSTER_NOT_MEMBER_OF_CLUSTER CLUSTERNODE ist auf YES gesetzt, aber diese Maschine ist nicht Teil eines Clusters.

Erläuterung

Diese Maschine ist nicht Teil eines Clusterknotens. Mögliche Ursachen sind, dass der Cluster-Service nicht korrekt konfiguriert ist oder dass der Cluster im Initialisierungsprozess steht.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Stellen Sie sicher, dass die Cluster-Software ordnungsgemäß konfiguriert ist. Wenn der Cluster im Initialisierungsprozess ist, die Operation zu einem späteren Zeitpunkt wiederholen.

4604 E DSM_RC_CLUSTER_NOT_ENABLED CLUSTERNODE ist auf YES gesetzt, aber der Cluster-Service ist auf diesem System nicht aktiviert.

Erläuterung

Der Cluster-Service wurde auf diesem System nicht aktiviert.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Aktivieren Sie den Cluster-Service auf dem System.

4605 E DSM_RC_CLUSTER_NOT_SUPPORTED Die Option CLUSTERNODE wird auf diesem System nicht unterstützt.

Erläuterung

Diese Option wird auf diesem System nicht unterstützt.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Inaktivieren Sie die Option CLUSTERNODE in der lokalen Optionsdatei.

4606 E DSM_RC_CLUSTER_UNKNOWN_ERROR Unerwarteter Fehler (*Rückkehrcode*) beim Versuch des Programms, den Clusternamen vom System abzurufen.

Erläuterung

Beim Versuch des Programms, den Clusternamen aus dem Cluster-Service abzurufen, ist ein unbekannter Fehler aufgetreten. Der Fehlercode ist der Ursachencode, der direkt von dem in dieser Betriebssystemumgebung verwendeten Cluster-Service zur Verfügung gestellt wird.

Systemaktion

Die Verarbeitung wird beendet.

Benutzeraktion

Schlagen Sie in der Dokumentation zu Ihrer Clustering-Software eine Erläuterung des Ursachencodes nach. Stellen Sie sicher, dass Ihr Clustering-Service betriebsbereit ist und wiederholen Sie anschließend die IBM Spectrum Protect-Operation.

5200 E DSM_RC_ABORT_CERTIFICATE_NOT_FOUND Der ferne Knoten ist auf dem IBM Spectrum Protect-Server nicht korrekt konfiguriert.

Erläuterung

Der ferne Knoten ist auf dem IBM Spectrum Protect-Server nicht korrekt konfiguriert.

Systemaktion

Die Verarbeitung wurde gestoppt.

Benutzeraktion

Stellen Sie sicher, dass der ferne Knoten korrekt konfiguriert und unter Verwendung von TLS mit dem IBM Spectrum Protect-Server verbunden ist. Damit wird die Konfiguration des fernen Knotens validiert und sichergestellt, dass die mit dem fernen Knoten verbundenen Informationen an den Server gesendet werden.

5702 E DSM_RC_PROXY_REJECT_NO_RESOURCES Proxy zurückgewiesen: Der IBM Spectrum Protect-Server verfügt nicht mehr über genügend Speicher.

Erläuterung

Es ist nicht genug Speicher verfügbar, um diese Operation fortzusetzen.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Wiederholen Sie die Operation. Bleibt der Fehler bestehen, verständigen Sie Ihren Systemadministrator, damit er die Speicherkapazität auf dem Server erhöht.

5705 E DSM_RC_PROXY_REJECT_DUPLICATE_ID Proxy zurückgewiesen: Die Optionen ASNODENAME und NODENAME haben denselben Wert.

Erläuterung

Die Optionen ASNODENAME und NODENAME dürfen nicht denselben Wert haben.

Systemaktion

Die aktuelle Operation wird abgebrochen.

Benutzeraktion

Verwenden Sie die Option ASNODENAME nur für den Zugriff auf einen anderen Knoten. Es ist nicht notwendig, die Option ASNODENAME für den Zugriff auf Ihren eigenen Knoten zu definieren. Entfernen Sie die Option ASNODENAME aus Ihrer Optionsdatei; es sei denn, Sie versuchen tatsächlich, auf einen Knoten zuzugreifen, für den Ihnen mit dem Verwaltungsbefehl "`Grant Proxynode`" die Zugriffsberechtigung erteilt wurde.

5710 E DSM_RC_PROXY_REJECT_ID_IN_USE Proxy zurückgewiesen: Der Knotenname, den Sie in der Option ASNODENAME angegeben haben, ist gesperrt.

Erläuterung

Der IBM Spectrum Protect-Administrator hat den Knoten, den Sie in der Option ASNODENAME angegeben haben, gesperrt.

Systemaktion

Die IBM Spectrum Protect-Operation wird beendet.

Benutzeraktion

Der IBM Spectrum Protect-Serveradministrator muss den Knoten entsperren, bevor Sie auf ihn zugreifen können. Wiederholen Sie die Operation zu einem späteren Zeitpunkt oder verständigen Sie Ihren IBM Spectrum Protect-Administrator.

5717 E DSM_RC_PROXY_REJECT_INTERNAL_ERROR Proxy zurückgewiesen: Der Server hat einen internen Fehler.

Erläuterung

Der Client kann wegen eines internen Serverfehlers nicht an den Knoten weiterleiten, der durch die Option ASNODENAME angegeben ist.

Systemaktion

Die aktuelle Operation wurde abgebrochen.

Benutzeraktion

Sofort den Systemadministrator verständigen.

5722 E DSM_RC_PROXY_REJECT_NOT_AUTHORIZED Proxy zurückgewiesen: Diesem Knoten wurde keine Proxy-Berechtigung erteilt.

Erläuterung

Dem Knoten wurde keine Proxy-Berechtigung erteilt, um auf den Knoten zuzugreifen, der durch die Option ASNODENAME benannt ist. Der IBM Spectrum Protect-Administrator muss zuerst die Proxy-Berechtigung erteilen.

Systemaktion

Die IBM Spectrum Protect-Operation wird beendet.

Benutzeraktion

Der IBM Spectrum Protect-Serveradministrator muss die Proxy-Berechtigung für diesen Knoten erteilen. Siehe den Administratorbefehl "Grant Proxynode".

5746 E DSM_RC_PROXY_INVALID_FROMNODE Die Option ASNODENAME ist mit der Option FROMNODE nicht gültig.

Erläuterung

Keine.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Entfernen Sie die Option ASNODENAME aus der Optionsdatei oder verwenden Sie nicht die Option FROMNODE.

5748 E DSM_RC_PROXY_INVALID_CLUSTER Die Option ASNODENAME kann nicht mit der Option CLUSTERNODE verwendet werden.

Erläuterung

Keine.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Entfernen Sie die Option ASNODENAME und wiederholen Sie die Operation.

5749 E DSM_RC_PROXY_INVALID_FUNCTION Die versuchte Operation kann mit der Option ASNODENAME nicht aufgerufen werden.

Erläuterung

Keine.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Entfernen Sie die Option ASNODENAME und wiederholen Sie die Operation.

5801 E DSM_RC_CRYPTO_ICC_ERROR Unerwarteter Fehler in der Kryptografiebibliothek.

Erläuterung

In der Kryptografiebibliothek ist ein unerwarteter Fehler aufgetreten. Das Fehlerprotokoll enthält weitere Informationen.

Systemaktion

Die Verarbeitung wird gestoppt.

Benutzeraktion

Überprüfen Sie das Fehlerprotokoll für ANS1467E, um die Fehlerursache festzustellen. Prüfen Sie, ob Ihr IBM Spectrum Protect-Client ordnungsgemäß installiert ist. Falls notwendig, installieren Sie den Client und/oder die API erneut. Bleibt der Fehler bestehen, wenden Sie sich an die technische Unterstützung für IBM Spectrum Protect.

Beschreibungen der E/A-Codes in Servernachrichten

IBM Spectrum Protect-Nachrichten können Ein-/Ausgabecodes (E/A-Codes) enthalten. Die Codes können Operationscodes, Beendigungscodes, ASC-Codes (ASC = Additional Sense Codes) und ASCQ-Codes (ASCQ = Additional Sense Code Qualifier) sein.

Codebeschreibungen für E/A-Fehlernachrichten des IBM Spectrum Protect-Servers werden für alle unterstützten Betriebssysteme bereitgestellt.

Code

Beschreibung

OP

Fehlgeschlagene E/A-Operation. Diese Werte können angezeigt werden:

- READ
- WRITE
- FSR (Speicherbereichssatz weiterleiten)
- RSR (Speicherbereichssatz zurücknehmen)
- FSF (Speicherbereichsdatei weiterleiten)
- RSF (Speicherbereichsdatei zurücknehmen)
- WEOF (Dateiendemarkierung schreiben)
- OFFL (Band zurückspulen und entnehmen)
- FLUSH (Flushoperation ausführen)
- GET_MEDIUM_INFO (Datenträgerinformationen abrufen)
- LOCATE (lokalisieren)
- QRYLBP (Schutz logischer Blöcke abfragen)
- RDBLKID (Block-ID lesen)
- SETLBP (Schutz logischer Blöcke definieren)
- SETMODE (Modus definieren)
- REW (zurückspulen)
- SPACEEOD (Datenende des Speicherbereichs)
- TESTREADY (Testlaufwerk bereit)

CC

E/A-Beendigungscode. Dieser Wert wird von dem Einheitentreiber an den Server zurückgegeben, wenn ein Fehler auftritt. Eine Liste der Beendigungscodes finden Sie in Übersicht über die Werte der Beendigungscodes und Operationscodes. Informationen zu Bandarchivsystemaufrufen und Fehlerbeschreibungen für die Speicherarchiv-E/A-Steuerungsanforderungen finden Sie in Technote S7002972.

KEY

Byte 2 der Prüfbyte des Fehlers. Nachfolgend sind einige Definitionen aufgelistet:

0 = keine weiteren Prüfbyte verfügbar
1 = behobener Fehler
2 = nicht bereit
3 = Datenträgerfehler
4 = Hardwarefehler
5 = falsche Anforderung
6 = Einheitenabruf (zum Beispiel Zurücksetzen eines SCSI-Busses)
7 = Datenschutz
8 = Leerprüfung
9 = lieferantenspezifisch
A = Kopieroperation abgebrochen
B = abgebrochener Befehl
C = veraltet
D = Datenträgerüberlauf
E = fehlende Übereinstimmung
F = reserviert

ASC/ASCQ

ASC- und ASCQ-Codes sind die Byte 12 und 13 der Prüfbyte. Das mit der Einheit zur Verfügung gestellte Referenzhandbuch zum Laufwerk oder Kassettenarchiv enthält Tabellen, die die Werte der Felder KEY, ASC und ASCQ erläutern. Der Abschnitt Beschreibungen der ASC- und ASCQ-Standardcodes stellt weitere Informationen zu den Standardwerten der ASC- und ASCQ-Codes bereit.

Fehlercodes des Betriebssystems

Wenn ein Befehl fehlschlägt, gibt das Betriebssystem eine Fehlernummer zurück. Um die Bedeutung der Fehlercodes zu bestimmen, führen Sie die folgende Aktion aus:

- Rufen Sie auf den Plattformen AIX, HP-UX und Solaris die Datei errno.h im Verzeichnis /usr/include/sys auf. Diese Datei stellt Definitionen der Fehlercodes bereit.
- Rufen Sie auf Linux-Plattformen die Dateien errno-base.h und errno.h im Verzeichnis /usr/include/asm-generic auf. Diese Dateien stellen Definitionen für Codes bereit.
- Wenden Sie sich auf Windows-Plattformen zwecks Unterstützung bei den Fehlernachrichten an den Microsoft Support.

- Übersicht über die Werte der Beendigungscodes und Operationscodes
  IBM Spectrum Protect-Nachrichten können Beendigungscodes von den Einheitentreibern enthalten.
- Beschreibungen der ASC- und ASCQ-Standardcodes
  ASC- und ASCQ-Standardcodes werden beschrieben.

Übersicht über die Werte der Beendigungscodes und Operationscodes

IBM Spectrum Protect-Nachrichten können Beendigungscodes von den Einheitentreibern enthalten.

- Beendigungscodes für Einheitentreiber: Allgemeine Codes
  IBM Spectrum Protect-Einheitentreiber stellen Beendigungscodes bereit, die für alle Einheitenklassen gelten.
- Beendigungscodes für Einheitentreiber: Datenträgerwechsler
  IBM Spectrum Protect-Einheitentreiber stellen Beendigungscodes bereit, die für bestimmte Datenträgerwechseleinheiten gelten.
- Beendigungscodes für Einheitentreiber: Bandlaufwerke
  IBM Spectrum Protect-Einheitentreiber stellen Beendigungscodes bereit, die für bestimmte Bandlaufwerke gelten.

Beendigungscodes für Einheitentreiber: Allgemeine Codes

IBM Spectrum Protect-Einheitentreiber stellen Beendigungscodes bereit, die für alle Einheitenklassen gelten.

Die folgende Tabelle enthält allgemeine Beendigungscodewerte für IBM Spectrum Protect-Einheitentreiber. Jeder Eintrag stellt eine Beschreibung für die E/A-Fehlernachricht und die empfohlene Aktion zur Verfügung. Wiederholen Sie nach der Ausführung der empfohlenen Aktion die fehlgeschlagene Operation.

Tabelle 1. Beendigungscodewerte, die auf alle Einheitenklassen zutreffen

Dezimal	Hexadezimal	Beschreibung	Empfohlene Aktion
200	X'C8'	Die Einheit hat eine Fehlerbedingung angezeigt, Prüfdaten waren jedoch nicht verfügbar.	Die fehlgeschlagene Operation wiederholen.
201	X'C9'	Der Einheitentreiber ist fehlgeschlagen.	Den IBM Spectrum Protect Support verständigen.
202	X'CA'	Die Einheit EEPROM ist fehlgeschlagen.	Die Einheit testen. Bei Bedarf die Einheit warten.
203	X'CB'	Manueller Eingriff ist erforderlich.	Den Fehler an der Einheit beheben. Bei dem Problem kann es sich um ein steckengebliebenes Band, verschmutzte Plattenköpfe oder einen eingeklemmten Plattenzugriffsarm handeln.
204	X'CC'	Das System wurde nach einem E/A-Fehler wiederhergestellt; nur zu Informationszwecken.	Keine Aktion erforderlich.
205	X'CD'	Der SCSI-Adapter ist fehlgeschlagen.	Auf lose Kabel, verbogene Kontaktstifte, falsche Kabel, falsche SCSI-Adapter, nicht ordnungsgemäße Abschlüsse oder falsche Abschlussstecker überprüfen.
206	X'CE'	Ein allgemeiner SCSI-Fehler ist aufgetreten.	Auf lose Kabel, verbogene Kontaktstifte, falsche Kabel, falsche SCSI-Adapter, nicht ordnungsgemäße Abschlüsse oder falsche Abschlussstecker überprüfen.
207	X'CF'	Die Einheit kann die angeforderte Aktion nicht ausführen.	Sicherstellen, dass die Einheit eingeschaltet und bereit ist. Stellen Sie sicher, dass das Laufwerk mit dem Befehl DEFINE DRIVE korrekt definiert wurde. Stellen Sie sicher, dass die Einheitenklasse mit dem Befehl DEFINE DEVCLASS korrekt definiert wurde.
208	X'D0'	Der Befehl wurde gestoppt.	Den IBM Spectrum Protect Support verständigen.
209	X'D1'	Im Mikrocode der Einheit wurde ein Fehler gefunden.	Die Mikrocodeversion des Laufwerks überprüfen. Den Hersteller des Laufwerks benachrichtigen und die neueste Version anfordern.
210	X'D2'	Die Einheit wurde aufgrund des Einschaltens, der SCSI-Buszurücksetzung oder des manuellen Ladens/Entladens von Bändern zurückgesetzt.	Die fehlgeschlagene Operation wiederholen.
211	X'D3'	Der SCSI-Bus ist aktiv.	Sicherstellen, dass die SCSI-IDs der korrekten Einheit richtig zugeordnet wurden und auf die Einheit nicht durch einen anderen Prozess zugegriffen wird.

Dezimal	Hexadezimal	Beschreibung	Empfohlene Aktion
212	X'D4'	Persistente Reservierung wird auf dieser Einheit nicht unterstützt.	Keine Aktion erforderlich.
213	X'D5'	Eine Operation für persistente Reservierung ist fehlgeschlagen.	Die Einheit zurücksetzen und die Operation wiederholen. Bleibt der Fehler bestehen, den IBM Spectrum Protect Support verständigen.

Beendigungscodes für Einheitentreiber: Datenträgerwechsler

IBM Spectrum Protect-Einheitentreiber stellen Beendigungscodes bereit, die für bestimmte Datenträgerwechseleinheiten gelten.

Die folgende Tabelle enthält Beendigungscodewerte für IBM Spectrum Protect-Einheitentreiber für Datenträgerwechsler. Jeder Eintrag stellt eine Beschreibung für die E/A-Fehlernachricht und die empfohlene Aktion zur Verfügung. Wiederholen Sie nach der Ausführung der empfohlenen Aktion die fehlgeschlagene Operation.

Tabelle 1. Beendigungscodewerte für Datenträgerwechsler

Dezimal	Hexadezimal	Beschreibung	Empfohlene Aktion
300	X'12C'	Kassetten-Eingangs/Ausgangsfehler	Den Eingang/Ausgang auf einen eingeklemmten Datenträger überprüfen.
301	X'12D'	Kassettenladefehler	Das Laufwerk auf eingeklemmte Datenträger überprüfen. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.
302	X'12E'	Kassette in fehlerhaftem Laufwerk	Das Laufwerk auf eingeklemmte Datenträger überprüfen. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.
303	X'12F'	Karussell nicht geladen	Sicherstellen, dass das Karussell korrekt positioniert und die Tür geschlossen ist.
304	X'130'	Wechslerfehler	Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.
305	X'131'	Laufwerkfehler	Sicherstellen, dass die Köpfe sauber sind. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.
306	X'132'	Laufwerk- oder Datenträgerfehler	Sicherstellen, dass die Köpfe sauber sind. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.
307	X'133'	Eingangs-/Ausgangsfehler	Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen.
308	X'134'	Eingangs-/Ausgangsanschluss nicht vorhanden	Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen.
309	X'135'	Kassettenarchivprüffehler	Sicherstellen, dass keine Datenträger eingeklemmt sind. Es ist möglich, dass die Kassettenarchivprüfung aufgrund von Hardwarefehlern fehlschlägt. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.
310	X'136'	Kassettenarchiv voll	Auf eingeklemmte Datenträger überprüfen. Sicherstellen, dass die Datenträger nicht neu angeordnet werden. Ist das Kassettenarchiv nicht voll, den Befehl AUDIT LIBRARY starten.
311	X'137'	Datenträgerexport	Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen.
312	jX'138'	Schachtfehler	Sicherstellen, dass in dem Schacht nichts eingeklemmt ist.

Dezimal	Hexadezimal	Beschreibung	Empfohlene Aktion
313	X'139'	Schacht- oder Datenträgerfehler	Sicherstellen, dass der Datenträger in dem Schacht nicht eingeklemmt ist und die Datenträger nicht neu angeordnet werden. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.
314	X'13A'	Quellenschacht oder -laufwerk waren bei Versuch leer, Datenträger zu versetzen	Sicherstellen, dass die Datenträger nicht neu angeordnet werden. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.
315	X'13B'	Zielschacht oder -laufwerk waren bei Versuch leer, Datenträger zu versetzen	Sicherstellen, dass die Datenträger nicht neu angeordnet werden und dass kein Datenträger in dem Laufwerk eingeklemmt ist. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.
316	X'13C'	Reinigungskassette installiert	Den IBM Spectrum Protect Support verständigen.
317	X'13D'	Datenträger nicht ausgegeben	Sicherstellen, dass die Datenträger nicht neu angeordnet werden und dass kein Datenträger in dem Laufwerk eingeklemmt ist. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.
318	X'13E'	E/A-Anschluss nicht konfiguriert	Den IBM Spectrum Protect Support verständigen.
319	X'13F'	Erster Zielort ist leer	Sicherstellen, dass die Datenträger nicht neu angeordnet werden. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.
320	X'140'	Keine Informationen zum Datenträgerbestand	Den Befehl AUDIT LIBRARY starten.
321	X'141'	Abweichung beim Lesen des Elementstatus	Stellen Sie sicher, dass die Hostbusadaptertreiber und die Firmware über aktuelle Versionen verfügen. Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen.
322	X'142'	Bereichsinitialisierung fehlgeschlagen	Die Bandarchivschnittstelle auf Hardwarefehler überprüfen. Sind keine Fehler vorhanden, den IBM Spectrum Protect Support verständigen.

Beendigungscodes für Einheitentreiber: Bandlaufwerke

IBM Spectrum Protect-Einheitentreiber stellen Beendigungscodes bereit, die für bestimmte Bandlaufwerke gelten.

Die folgende Tabelle enthält Beendigungscodewerte für IBM Spectrum Protect-Einheitentreiber für Bandlaufwerke. Jeder Eintrag stellt eine Beschreibung für die E/A-Fehlernachricht und die empfohlene Aktion zur Verfügung. Wiederholen Sie nach der Ausführung der empfohlenen Aktion die fehlgeschlagene Operation.

Tabelle 1. Beendigungscodewerte für Bandlaufwerke

Dezimal	Hexadezimal	Beschreibung	Empfohlene Aktion
400	X'190'	Physisches Ende des Datenträgers erkannt	Sicherstellen, dass die Köpfe im Laufwerk sauber sind.
401	X'191'	Datenende erkannt	Den IBM Spectrum Protect Support verständigen.
402	X'192'	Datenträger beschädigt	Sicherstellen, dass die Köpfe sauber sind. Stellen Sie sicher, dass der Datenträger nicht physisch beschädigt ist und nicht das Ende des Lebenszyklus erreicht hat, das vom Hersteller des Datenträgers angegeben wurde.
403	X'193'	Datenträgerfehler	Sicherstellen, dass die Köpfe sauber sind. Stellen Sie sicher, dass der Datenträger nicht physisch beschädigt ist und nicht das Ende des Lebenszyklus erreicht hat, das vom Hersteller des Datenträgers angegeben wurde.
404	X'194'	Datenträgerinkompatibilität	Sicherstellen, dass die korrekte Länge und der korrekte Typ des Datenträgers verwendet wird.

Dezimal	Hexadezimal	Beschreibung	Empfohlene Aktion
406	X'196'	Angeforderter Sektor ist ungültig	Interner Serverfehler. Den IBM Spectrum Protect Support verständigen.
407	X'197'	Schreibgeschützt	Sicherstellen, dass der Datenträger nicht schreibgeschützt ist.
408	X'198'	Datenträger und Laufwerk reinigen	Die Laufwerkköpfe mit einer Reinigungskassette reinigen.
409	X'199'	Datenträgerfehler	Sicherstellen, dass die Köpfe sauber sind. Stellen Sie sicher, dass der Datenträger nicht physisch beschädigt ist und nicht das Ende des Lebenszyklus erreicht hat, das vom Hersteller des Datenträgers angegeben wurde.
410	X'19A'	Reinigung beendet	Die fehlgeschlagene Operation wiederholen.
411	X'19B'	Logisches Datenträgerende festgestellt	Den IBM Spectrum Protect Support verständigen.
412	X'19C'	Datenträger in Laufwerk nicht vorhanden	Sicherstellen, dass der Datenträger im Laufwerk korrekt positioniert ist. Bleibt der Fehler bestehen, den Befehl AUDIT LIBRARY starten.
413	X'19D'	Anfang des Datenträgers festgestellt	Den IBM Spectrum Protect Support verständigen.
414	X'19E'	Fehler beim Löschen	Die Laufwerkköpfe reinigen.
415	X'19F'	Versuch, beschriebenen WORM-Datenträger zu überschreiben	Interner Serverfehler. Den IBM Spectrum Protect Support verständigen.
416	X'1A0'	Block mit falscher Länge gelesen.	Sicherstellen, dass die Köpfe sauber sind. Unter AIX den errpt zum Überprüfen auf Hardwarefehler anzeigen.
417	X'1A1'	Nur zum Lesen öffnen	Den IBM Spectrum Protect Support verständigen.
418	X'1A2'	Nur zum Schreiben öffnen	Den IBM Spectrum Protect Support verständigen.
419	X'1A2'	Durchsuchen des Datenträgers fehlgeschlagen	Das Laufwerk und den Datenträger reinigen.
420	X'1A4'	Kein logischer Schreibzugriff	Sicherstellen, dass die Köpfe sauber sind. Die Fehlerprotokolle des Betriebssystems auf Hardwarefehler überprüfen. Sicherstellen, dass der Schreibschutzschalter auf 'Off' gesetzt ist. Die SAN-Bandbeschleunigung inaktivieren oder CHECKTAPEPOS auf OFF oder TSMonly setzen.
422	X'1A6'	Reinigung ist erforderlich	Das Bandlaufwerk reinigen.
423	X'1A7'	Datenträgerfehler	Die Fehlerprotokolle des Betriebssystems auf Hardwarefehler überprüfen. Überprüfen, ob fehlerhafte Datenträger vorhanden sind.
424	X'1A8'	Mit der Verschlüsselung zusammenhängender Fehler ist aufgetreten	Überprüfen Sie Ihre Verschlüsselungseinstellung für Ihre Einheitenklasse und Ihr Bandlaufwerk.
425	X'1A9'	Mit der Entschlüsselung zusammenhängender Fehler ist aufgetreten	Überprüfen Sie Ihre Verschlüsselungseinstellung für Ihre Einheitenklasse und Ihr Bandlaufwerk.
425	X'1AA'	Ein externer mit der Verschlüsselung zusammenhängender Fehler ist aufgetreten	Überprüfen Sie die Verschlüsselungseinstellung für Ihre Einheitenklasse und Ihr Bandlaufwerk.
426	X'1AB'	Eine CRC-Abweichung ist aufgetreten	Stellen Sie sicher, dass der Datenträger nicht das Ende des Lebenszyklus erreicht hat, das vom Hersteller des Datenträgers angegeben wurde. Wiederholen Sie die Operation.

Beschreibungen der ASC- und ASCQ-Standardcodes

ASC- und ASCQ-Standardcodes werden beschrieben.

Die ASC- und ASCQ-Codes sind die Byte 12 und 13 für SCSI-2-Einheiten. Auf Windows-Systemen werden diese Codes im Windows-Ereignisprotokoll angezeigt, aber die Informationen zeigen andere Byte.

Die Servernachricht ANR8300E oder ANR8302E gibt die empfohlene Aktion an.

Die folgende Tabelle enthält Standardbeschreibungen für einige ASC- und ASCQ-Codes. Jeder Wert hat das Präfix 0x, das angibt, dass es sich um eine Hexadezimalkonstante handelt. Beachten Sie, dass die Beschreibungen unter Einheiten variieren. Eine genaue Beschreibung der ASC- und ASCQ-Codes für eine bestimmte Einheit enthält die mit der Einheit bereitgestellte Dokumentation.

Tabelle 1. Beschreibungen der ASC- und ASCQ-Standardcodes

ASC	ASCQ	Beschreibung
0x00	0x00	Keine weiteren Prüfcodes
0x00	0x01	Dateimarkierung erkannt
0x00	0x02	Datenträgerende erkannt
0x00	0x03	Gruppenmarkierung erkannt
0x00	0x04	Datenträgeranfang
0x00	0x05	Datenende
0x00	0x06	E/A-Prozeß beendet
0x02	0x00	Kein Suchvorgang abgeschlossen
0x03	0x00	Einheitenschreibfehler
0x03	0x01	Kein aktueller Schreibvorgang
0x03	0x02	Zu viele Schreibfehler
0x04	0x00	Logische Einheit nicht bereit
0x04	0x01	Wird in Bereitschaft gesetzt
0x04	0x02	Nicht bereit, Initialisierung des Befehls erforderlich
0x04	0x03	Nicht bereit, manueller Eingriff erforderlich
0x04	0x04	Nicht bereit, Formatierung läuft
0x05	0x00	Keine auszuwählende Antwort
0x06	0x00	Keine Referenzposition gefunden
0x07	0x00	Mehrere Einheiten ausgewählt
0x08	0x00	Übertragungsfehler
0x08	0x01	Zeitlimitüberschreitung bei Übertragung
0x08	0x02	Übertragungsparitätsfehler
0x09	0x00	Fehlerverfolgung
0x0A	0x00	Fehlerprotokollüberlauf
0x0C	0x00	Schreibfehler
0x11	0x00	Nicht behobener Lesefehler
0x11	0x01	Wiederholungslimit für Lesen erreicht
0x11	0x02	Fehler zum Korrigieren zu lang
0x11	0x03	Mehrere Lesefehler
0x11	0x08	Unvollständiges Lesen des Blocks
0x11	0x09	Kein Abstand gefunden
0x11	0x0A	Falsch korrigierter Fehler
0x14	0x00	Aufgezeichnete Entität nicht gefunden
0x14	0x01	Satz nicht gefunden
0x14	0x02	Dateimarkierung/Gruppenmarkierung nicht gefunden
0x14	0x03	Datenende nicht gefunden
0x14	0x04	Blockfolgefehler
0x15	0x00	Fehler bei wahlfreier Positionierung
0x15	0x01	Mechanischer Positionierungsfehler
0x15	0x02	Lesepositionierungsfehler
0x17	0x00	Keine Fehlerkorrektur angewendet

ASC	ASCQ	Beschreibung
0x17	0x01	Mit Wiederholungen wiederhergestellt
0x17	0x02	Mit positiver Kopfkorrektur wiederhergestellt
0x17	0x03	Mit negativer Kopfkorrektur wiederhergestellt
0x18	0x00	ECC angewendet
0x1A	0x00	Längenfehler bei Parameterliste
0x1B	0x00	Fehler bei synchroner Datenübertragung
0x20	0x00	Ungültiger Operationscode
0x21	0x00	Block außerhalb des Bereichs
0x21	0x01	Ungültige Elementadresse
0x24	0x00	Ungültiges Feld in CDB
0x25	0x00	LUN nicht unterstützt
0x26	00	Ungültiges Feld in Parameterliste
0x26	0x01	Parameter nicht unterstützt
0x26	0x02	Parameterwert ungültig
0x26	0x03	Schwellenparameter nicht unterstützt
0x27	0x00	Schreibgeschützt
0x28	0x00	Nicht bereit zu bereit
0x28	0x01	Zugriff auf Import-/Exportelement
0x29	0x00	Einschalten, zurücksetzen, Bus zurücksetzen
0x2A	0x00	Parameter geändert
0x2A	0x01	Modusparameter geändert
0x2A	0x02	Protokollparameter geändert
0x2B	0x00	Kopiervorgang kann nicht ausgeführt werden
0x2C	0x00	Befehlsfolgefehler
0x2D	0x00	Überschreibungsfehler bei Aktualisierung
0x2F	0x00	Befehl vom Initiator gelöscht
0x30	0x00	Inkompatible Datenträger
0x30	0x01	Unbekanntes Format für Datenträger
0x30	0x02	Inkompatibles Format für Datenträger
0x30	0x03	Reinigungskassette installiert
0x31	0x00	Datenträgerformat beschädigt
0x33	0x00	Bandlängenfehler
0x37	0x00	Gerundeter Parameter
0x39	0x00	Sichern von Parametern nicht unterstützt
0x3A	0x00	Datenträger nicht vorhanden
0x3B	0x00	Fehler bei sequentieller Positionierung
0x3B	0x01	Positionierungsfehler bei BOT
0x3B	0x02	Positionierungsfehler bei EOT
0x3B	0x08	Neupositionierungsfehler
0x3B	0x0D	Datenträgerzielelement voll
0x3B	0x0E	Datenträgerquellenelement leer
0x3D	0x00	Ungültige Bits in Nachricht
0x3E	0x00	LUN nicht selbstkonfiguriert
0x3F	0x00	Betriebsbedingungen geändert

ASC	ASCQ	Beschreibung
0x3F	0x01	Mikrocode geändert
0x3F	0x02	Geänderte Betriebsdefinition
0x3F	0x03	Abfragedaten geändert
0x3F	0x0E	Zurückgemeldete LUN-Daten geändert
0x43	0x00	Nachrichtenfehler
0x44	0x00	Fehler bei internem Ziel
0x45	0x00	Fehler beim Auswählen/Erneuten Auswählen
0x46	0x00	Nicht erfolgreicher Warmstart
0x47	0x00	SCSI-Paritätsfehler
0x48	0x00	Initiator hat empfangene Nachricht erkannt
0x49	0x00	Ungültige Nachricht
0x4A	0x00	Befehlsphasenfehler
0x4B	0x00	Datenphasenfehler
0x4C	0x00	Fehlgeschlagene Selbstkonfiguration bei LUN
0x4E	0x00	Überlappte Befehle
0x50	0x00	Anfügefehler beim Schreiben
0x50	0x01	Anfügepositionsfehler beim Schreiben
0x50	0x02	Positionsfehler (Ablaufsteuerung)
0x51	0x00	Fehler beim Löschen
0x52	0x00	Kassettenfehler
0x53	0x00	Laden/Entnehmen des Datenträgers fehlgeschlagen
0x53	0x01	Fehler beim Entnehmen des Bandes
0x53	0x02	Datenträgerentnahme verhindert
0x5A	0x00	Operatorstatus geändert
0x5A	0x01	Datenträgerentnahme durch Operator
0x5A	0x02	Operator - kein Schreibzugriff
0x5A	0x03	Operator - Schreibzugriff
0x5B	0x00	Protokollausnahme
0x5B	0x01	Schwellenbedingung erfüllt
0x5B	0x02	Protokollzähler auf Maximum
0x5B	0x03	Protokollistencodes erschöpft

- ASC- und ASCQ-Codes im Windows-Ereignisprotokoll
  ASC- und ASCQ-Codes werden im Windows-Ereignisprotokoll angezeigt.

Einheitenfehlercodes im AIX-Systemfehlerprotokoll

Einige Einheitenfehlercodes werden im AIX-Systemfehlerprotokoll protokolliert.

ADSM_DD_LOG1 (0xAC3AB953)
DEVICE DRIVER SOFTWARE ERROR

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, wenn in der IBM Spectrum Protect-Einheitentreibersoftware ein Fehler vermutet wird. Gibt der IBM Spectrum Protect-Einheitentreiber einen SCSI-E/A-Befehl mit einem ungültigen Operationscode aus, schlägt der Befehl fehl und der Fehler wird mit dieser Kennung protokolliert. Melden Sie diesen Fehler sofort der IBM Spectrum Protect-Unterstützung.

Detaildaten: Prüfdaten

Die Prüfdaten enthalten Informationen, die die Fehlerursache bestimmen können. Melden Sie alle Daten in dem Fehlereintrag der IBM Spectrum Protect-Unterstützung.

ADSM_DD_LOG2 (0x5680E405)
HARDWARE/COMMAND-ABORTED ERROR

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, wenn die Einheit einen Hardwarefehler oder Fehler beim Stoppen des Befehls als Antwort auf einen SCSI-E/A-Befehl meldet.

Detaildaten: Prüfdaten

Die Prüfdaten enthalten Informationen, mit denen die fehlerhafte Hardwarekomponente und die Fehlerursache bestimmt werden können. Ziehen Sie das SCSI-Spezifikationshandbuch der Einheit zu Rate, um die Prüfdaten für eine bestimmte Einheit zu interpretieren.

ADSM_DD_LOG3 (0x461B41DE)
MEDIA ERROR

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, wenn ein SCSI-E/A-Befehl fehlschlägt, weil Datenträger beschädigt oder inkompatibel sind oder ein Laufwerk gereinigt werden muss.

Detaildaten: Prüfdaten

Die Prüfdaten enthalten Informationen, die die Fehlerursache bestimmen können. Ziehen Sie das SCSI-Spezifikationshandbuch der Einheit zu Rate, um die Prüfdaten für eine bestimmte Einheit zu interpretieren.

ADSM_DD_LOG4 (0x4225DB66)
TARGET DEVICE GOT UNIT ATTENTION

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, nachdem bestimmte UNIT ATTENTION-Hinweise von einer Einheit empfangen wurden. UNIT ATTENTION-Hinweise dienen zur Information und geben normalerweise an, dass sich ein bestimmter Zustand der Einheit geändert hat. Dieser Fehler würde beispielsweise protokolliert, wenn die Tür einer Kassettenarchiveinheit geöffnet und dann geschlossen wurde. Durch Protokollieren dieses Ereignisses wird angegeben, dass die Aktivität stattgefunden hat und der Bestand im Kassettenarchiv möglicherweise geändert wurde.

Detaildaten: Prüfdaten

Die Prüfdaten enthalten Informationen, die die Ursache für die UNIT ATTENTION beschreiben. Ziehen Sie das SCSI-Spezifikationshandbuch der Einheit zu Rate, um die Prüfdaten für eine bestimmte Einheit zu interpretieren.

ADSM_DD_LOG5 (0xDAC55CE5)
PERMANENT UNKNOWN ERROR

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, nachdem ein unbekannter Fehler von einer Einheit als Antwort auf einen SCSI-E/A-Befehl empfangen wurde. Bleibt der Fehler bestehen, müssen Sie die Mitarbeiter der IBM Spectrum Protect-Unterstützung benachrichtigen.

Detaildaten: Prüfdaten

Die Prüfdaten bestehen aus Informationen, die die Fehlerursache bestimmen können. Melden Sie alle Daten in dem Fehlereintrag der IBM Spectrum Protect-Unterstützung.

ADSM_DD_LOG6 (0xBC539B26)
WARNING OR INFORMATIONAL MESSAGE FOR TARGET DEVICE

Dieser Fehler wird vom IBM Spectrum Protect-Einheitentreiber protokolliert, nachdem eine Warnung oder eine Informationsnachricht von einer Einheit als Antwort auf einen SCSI-E/A-Befehl empfangen wurde. Diese Informationsnachrichten müssen nicht notwendigerweise auf ein Problem hinweisen. Wird die Nachricht weiterhin angezeigt, müssen Sie die IBM Spectrum Protect-Unterstützung benachrichtigen.

Detaildaten: Prüfdaten

Die Prüfdaten bestehen aus Informationen, die die Ursache für die Nachricht angeben können. Melden Sie alle Daten in dem Eintrag der IBM Spectrum Protect-Unterstützung.

Rückkehrcodes für IBM Global Security Kit

Der Server und Client verwenden das IBM Global Security Kit (GSKit) für die SSL-Verarbeitung (SSL - Secure Sockets Layer) zwischen dem Server und dem Client für Sichern/Archivieren. Einige Nachrichten, die für die SSL-Verarbeitung ausgegeben werden, enthalten GSKit-Rückkehrcodes.

GSKit wird während der IBM Spectrum Protect-Installation automatisch installiert oder aktualisiert und stellt die folgenden Bibliotheken bereit:

- GSKit SSL
- GSKit Key Management API
- IBM Crypto for C (ICC)

Mit dem Dienstprogramm 'tsmdiag' wird die auf Ihrem System installierte GSKit-Version zurückgemeldet. Sie können auch eine der folgenden Methoden verwenden:

- Geben Sie für Windows die folgenden Befehle aus:

  ```
  regedit /e gskitinfo.txt "HKEY_LOCAL_MACHINE\software\ibm\gsk8\"
  notepad gskitinfo.txt
  ```

  Vorsicht:
  Sie können das Systemregistry beschädigen, wenn Sie 'regedit' nicht ordnungsgemäß verwenden.
- Geben Sie für den AIX-Server (64-Bit) den folgenden Befehl in der Befehlszeile aus: `gsk8ver_64`

Tabelle 1 enthält die GSKit SSL-Rückkehrcodes.

Der Server verwendet die GSKit Key Management API, um die Schlüsselmanagementdatenbank und die privaten und öffentlichen Schlüssel des Servers automatisch zu erstellen. Einige Nachrichten, die für diese Verarbeitung ausgegeben werden, können GSKit Key Management-Rückkehrcodes einschließen. Tabelle 2 enthält die Key Management-Rückkehrcodes.

Tabelle 1. Allgemeine Rückkehrcodes für IBM Global Security Kit SSL

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000000	0	GSK_OK	Die Task wurde erfolgreich ausgeführt. Wird von jedem Funktionsaufruf ausgegeben, der erfolgreich ausgeführt wird.
0x00000001	1	GSK_INVALID_HANDLE	Die Umgebungskennung oder SSL-Kennung ist nicht gültig. Die angegebene Kennung war nicht das Ergebnis eines erfolgreichen Funktionsaufrufs `open()`.
0x00000002	2	GSK_API_NOT_AVAILABLE	Die DLL-Datei wurde entladen und ist nicht verfügbar (tritt nur auf Microsoft Windows-Systemen auf).
0x00000003	3	GSK_INTERNAL_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	Für die Ausführung der Operation ist nicht genügend Speicher verfügbar.
0x00000005	5	GSK_INVALID_STATE	Die Kennung hat keinen gültigen Status für die Operation, z. B. bei zweimaliger Ausführung einer Operation `init()` für eine Kennung.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	Der angegebene Schlüsselkennsatz wurde nicht in der Schlüsseldatei gefunden.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	Zertifikat nicht vom Partner empfangen.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Fehler bei der Zertifikatsvalidierung.
0x00000009	9	GSK_ERROR_CRYPTO	Fehler bei der Verarbeitung der Verschlüsselung.
0x0000000a	10	GSK_ERROR_ASN	Fehler bei der Validierung von ASN-Feldern im Zertifikat.
0x0000000b	11	GSK_ERROR_LDAP	Fehler beim Herstellen der Verbindung zur Benutzerregistry.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x0000000d	13	GSK_INVALID_PARAMETER	Ungültiger Parameter.
0x0000000e	14	GSK_ERROR_UNEXPECTED_INT_EXCEPTION	Ungültiger Parameter. Melden Sie diesen Fehler dem IBM Software Support.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x00000066	102	GSK_KEYFILE_IO_ERROR	E/A-Fehler beim Lesen der Schlüsseldatei.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	Die Schlüsseldatei hat kein gültiges internes Format. Erstellen Sie die Schlüsseldatei erneut.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	Die Schlüsseldatei hat zwei Einträge mit demselben Schlüssel.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	Die Schlüsseldatei hat zwei Einträge mit demselben Kennsatz.

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	Das Kennwort für die Schlüsseldatei wird als Integritätsprüfung verwendet. Entweder ist die Schlüsseldatei beschädigt oder die Kennwort-ID ist falsch.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	Der Standardschlüssel in der Schlüsseldatei hat ein abgelaufenes Zertifikat.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Beim Laden einer der GSK DLL-Dateien ist ein Fehler aufgetreten. Überprüfen Sie, ob GSK korrekt installiert wurde.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Gibt an, dass eine Verbindung in einer GSK-Umgebung hergestellt werden soll, nachdem GSK_ENVIRONMENT_CLOSE_OPTIONS auf GSK_DELAYED_ ENVIRONMENT_CLOSE gesetzt und die Funktion gsk_environment_close() aufgerufen wurde.
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	Weder das Kennwort noch der Name der Stashdatei wurde angegeben. Die Schlüsseldatei wurde nicht initialisiert.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	Die Schlüsseldatei kann nicht geöffnet werden. Entweder wurde der Pfad nicht korrekt angegeben oder die Dateiberechtigungen erlauben nicht das Öffnen der Datei.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	Temporäres Schlüsselpaar kann nicht generiert werden. Melden Sie diesen Fehler dem IBM Software Support.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Das angegebene Benutzernamenobjekt wurde nicht gefunden.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	Ein Kennwort, das für eine LDAP-Abfrage (LDAP = Lightweight Directory Access Protocol) verwendet wird, ist nicht korrekt.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Ein Index in der Übernahmeliste der LDAP-Server war nicht korrekt.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Diese Installation von GSKit unterstützt nicht die FIPS-Betriebsart.
0x0000012d	301	GSK_CLOSE_FAILED	Gibt an, dass die Anforderung zum Schließen der GSK-Umgebung nicht korrekt ausgeführt wurde. Die Ursache ist wahrscheinlich ein Befehl gsk_secure_socket*(), der nach einem Aufruf gsk_close_environment() ausgeführt werden sollte.
0x00000191	401	GSK_ERROR_BAD_DATE	Das Systemdatum wurde nicht auf einen gültigen Wert gesetzt.
0x00000192	402	GSK_ERROR_NO_CIPHERS	SSLv2 und SSLv3 sind nicht aktiviert.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	Das erforderliche Zertifikat wurde nicht vom Partner empfangen.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	Das empfangene Zertifikat war nicht korrekt formatiert.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	Der empfangene Zertifikatstyp wurde nicht unterstützt.
0x00000196	406	GSK_ERROR_IO	Ein E/A-Fehler ist bei einer Datenlese- oder -schreiboperation aufgetreten.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	Der angegebene Schlüsseldateikennsatz wurde nicht gefunden.

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	Das angegebene Kennwort für die Schlüsseldatei ist falsch. Die Schlüsseldatei kann nicht verwendet werden. Die Schlüsseldatei kann auch beschädigt sein.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	In einer eingeschränkten Verschlüsselungsumgebung wird die Schlüsselgröße nicht unterstützt.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Eine falsch formatierte SSL-Nachricht wurde vom Partner empfangen.
0x0000019b	411	GSK_ERROR_BAD_MAC	Der Nachrichtenauthentifizierungscode wurde nicht erfolgreich überprüft.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Nicht unterstütztes SSL-Protokoll oder nicht unterstützter Zertifikatstyp.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	Das empfangene Zertifikat enthielt eine falsche Signatur.
0x0000019e	414	GSK_ERROR_BAD_CERT	Falsch formatiertes Zertifikat vom Partner empfangen.
0x0000019f	415	GSK_ERROR_BAD_PEER	Kein gültiges SSL-Protokoll vom Partner empfangen.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	Das selbst signierte Zertifikat ist nicht gültig.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	`read()` ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	`write()` ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	Der Partner hat das Socket geschlossen, bevor das Protokoll beendet war.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	Die angegebene V2-Verschlüsselung ist nicht gültig.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	Die angegebene V3-Verschlüsselung ist nicht gültig.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	Die Kennung kann nicht erstellt werden. Melden Sie diesen Fehler dem IBM Software Support.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	Initialisierung ist fehlgeschlagen. Melden Sie diesen internen Fehler dem Service.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	Bei der Überprüfung eines Zertifikats kann nicht auf die angegebene Benutzerregistry zugegriffen werden.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	Der angegebene Schlüssel enthielt keinen privaten Schlüssel.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	Der Versuch, die angegebene gemeinsam genutzte PKCS11-Bibliothek zu laden, ist fehlgeschlagen.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	Der PKCS #11-Treiber konnte das vom aufrufenden Programm angegebene Token nicht finden.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	Ein PKCS #11-Token ist in dem Bereich nicht vorhanden.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	Das Kennwort/die PIN für den Zugriff auf das PKCS #11-Token ist nicht gültig.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	Der empfangene SSL-Header war kein korrekt formatierter SSLv2-Header.

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x000001b2	434	GSK_CSP_OPEN_ERROR	Der hardwarebasierte Verschlüsselungsserviceanbieter (Cryptographic Service Provider = CSP) kann nicht geöffnet werden. Entweder ist der CSP-Name nicht korrekt angegeben oder ein Versuch, auf den angegebenen CSP-Zertifikatsspeicher zuzugreifen, ist fehlgeschlagen.
0x000001b3	435	GSK_CONFLICTING_ATTRIBUTE_SETTING	Konflikt bei der Attributeinstellung zwischen PKCS11, der CMS-Schlüsseldatenbank und der Microsoft Krypto-API.
0x000001b4	436	GSK_UNSUPPORTED_PLATFORM	Die angeforderte Funktion wird auf der Plattform, die von der Anwendung ausgeführt wird, nicht unterstützt. Die Microsoft Krypto-API wird beispielsweise nur auf der Plattform Windows 2000 unterstützt.
0x000001b6	438	GSK_ERROR_INCORRECT_SESSION_TYPE	Ein falscher Wert wird von der Callback-Funktion zum Zurücksetzen des Sitzungstyps zurückgegeben. Nur GSKit `gsk_sever_session`, `gsk_sever_session_with_cl_auth` oder `gsk_sever_session_with_cl_auth_crit` ist zulässig.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	Die Puffergröße ist negativ oder Null.
0x000001f6	502	GSK_WOULD_BLOCK	Wird mit nicht geblockter Ein-/Ausgabe verwendet. Siehe den Abschnitt zur nicht geblockten Ein-/Ausgabe.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 ist für `reset_cipher()` erforderlich, und die Verbindung verwendet SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	Es wurde keine gültige ID für den Funktionsaufruf `gsk_secure_soc_misc()` angegeben.
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	Der Funktionsaufruf hat keine gültige ID. Dieses Problem kann auch durch die Angabe einer Umgebungskennung verursacht werden, wenn stattdessen eine Kennung für eine SSL-Verbindung verwendet werden müsste.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	Das Attribut hat eine negative Länge, die nicht gültig ist.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	Der Aufzählungswert ist für den angegebenen Aufzählungstyp nicht gültig.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Eine Parameterliste, die zum Ersetzen der SID-Cacheroutinen nicht gültig ist.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	Beim Definieren eines numerischen Attributs ist der angegebene Wert für das spezielle Attribut, das definiert wird, nicht gültig.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Für die zusätzliche Zertifikatsvalidierung wurden sich widersprechende Parameter definiert.
0x000002c3	707	GSK_AES_UNSUPPORTED	Der AES-Verschlüsselungsalgorithmus wird nicht unterstützt.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	Die PEERID hat nicht die korrekte Länge.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	Der betreffende Chiffrierwert ist nicht zulässig, wenn die FIPS-Betriebsart auf OFF gesetzt ist.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	In der FIPS-Betriebsart sind keine genehmigten FIPS-Chiffrierwerte ausgewählt.
0x00000641	1601	GSK_TRACE_STARTED	Der Trace wurde erfolgreich gestartet.
0x00000642	1602	GSK_TRACE_STOPPED	Der Trace wurde erfolgreich gestoppt.
0x00000643	1603	GSK_TRACE_NOT_STARTED	Es wurde zuvor keine Tracedatei gestartet. Daher kann sie nicht gestoppt werden.

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	Die Tracedatei wurde bereits gestartet. Daher kann sie nicht erneut gestartet werden.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	Die Tracedatei kann nicht geöffnet werden. Der erste Parameter von gsk_start_trace() muss ein gültiger vollständiger Pfaddateiname sein.

Tabelle 2. IBM Global Security Kit Key Management-Rückkehrcodes

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000000	0	GSK_OK	Die Task wurde erfolgreich ausgeführt. Diese Nachricht wird von jedem Funktionsaufruf ausgegeben, der erfolgreich ausgeführt wird.
0x00000001	1	GSK_INVALID_HANDLE	Die Umgebungskennung oder SSL-Kennung ist nicht gültig. Die angegebene Kennung war nicht das Ergebnis eines erfolgreichen Funktionsaufrufs open().
0x00000002	2	GSK_API_NOT_AVAILABLE	Die DLL-Datei (DLL = Dynamic Link Library) wurde entladen und ist nicht verfügbar (tritt nur auf Microsoft Windows-Systemen auf).
0x00000003	3	GSK_INTERNAL_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	Für die Ausführung der Operation ist nicht genügend Speicher verfügbar.
0x00000005	5	GSK_INVALID_STATE	Die Kennung hat einen falschen Status für die Operation, z. B. bei zweimaliger Ausführung einer Operation init() für eine Kennung.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	Der angegebene Schlüsselkennsatz wurde nicht in der Schlüsseldatei gefunden.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	Zertifikat nicht vom Partner empfangen.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Fehler bei der Zertifikatsvalidierung.
0x00000009	9	GSK_ERROR_CRYPTO	Fehler bei der Verarbeitung der Verschlüsselung.
0x0000000a	10	GSK_ERROR_ASN	Fehler bei der Validierung von ASN-Feldern im Zertifikat.
0x0000000b	11	GSK_ERROR_LDAP	Fehler beim Herstellen der Verbindung zur Benutzerregistry.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Interner Fehler. Melden Sie diesen Fehler dem IBM Software Support.
0x00000066	102	GSK_KEYFILE_IO_ERROR	E/A-Fehler beim Lesen der Schlüsseldatei.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	Die Schlüsseldatei hat ein internes Format, das nicht gültig ist. Die Schlüsseldatei erneut erstellen.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	Die Schlüsseldatei hat zwei Einträge mit demselben Schlüssel.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	Die Schlüsseldatei hat zwei Einträge mit demselben Kennsatz.

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_ PASSWORD	Das Kennwort für die Schlüsseldatei wird als Integritätsprüfung verwendet. Entweder ist die Schlüsseldatei beschädigt oder die Kennwort-ID ist falsch.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	Der Standardschlüssel in der Schlüsseldatei hat ein abgelaufenes Zertifikat.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Beim Laden einer der GSK DLL-Dateien ist ein Fehler aufgetreten. Überprüfen Sie, ob GSK korrekt installiert wurde.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Diese Nachricht gibt an, dass eine Verbindung in einer GSK-Umgebung hergestellt werden soll, nachdem GSK_ENVIRONMENT_CLOSE_OPTIONS auf GSK_DELAYED_ ENVIRONMENT_CLOSE gesetzt und die Funktion gsk_environment_close() aufgerufen wurde.
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	Es wurde weder das Kennwort noch der Stashdateiname angegeben, daher konnte die Schlüsseldatei nicht initialisiert werden.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	Die Schlüsseldatei kann nicht geöffnet werden. Entweder wurde der Pfad nicht korrekt angegeben oder die Dateiberechtigungen erlauben nicht das Öffnen der Datei.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	Temporäres Schlüsselpaar kann nicht generiert werden. Melden Sie diesen Fehler dem IBM Software Support.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Das angegebene Benutzernamenobjekt wurde nicht gefunden.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_ CREDENTIALS	Ein Kennwort, das für eine LDAP-Abfrage verwendet wird, ist nicht korrekt.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Ein Index in der Übernahmeliste der LDAP-Server war nicht korrekt.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Diese Installation von GSKit unterstützt nicht die FIPS-Betriebsart.
0x0000012d	301	GSK_CLOSE_FAILED	Gibt an, dass die Anforderung zum Schließen der GSK-Umgebung nicht korrekt ausgeführt wurde. Die Ursache ist wahrscheinlich ein Befehl gsk_secure_socket*(), der nach einem Aufruf gsk_close_environment() ausgeführt werden sollte.
0x00000191	401	GSK_ERROR_BAD_DATE	Das Systemdatum wurde auf einen Wert gesetzt, der nicht gültig ist.
0x00000192	402	GSK_ERROR_NO_CIPHERS	SSLv2 und SSLv3 sind nicht aktiviert.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	Das erforderliche Zertifikat wurde nicht vom Partner empfangen.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	Das empfangene Zertifikat war nicht korrekt formatiert.
0x00000195	405	GSK_ERROR_UNSUPPORTED_ CERTIFICATE_TYPE	Der empfangene Zertifikatstyp wurde nicht unterstützt.

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x00000196	406	GSK_ERROR_IO	Ein E/A-Fehler ist bei einer Datenlese- oder -schreiboperation aufgetreten.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	Der angegebene Schlüsseldateikennsatz wurde nicht gefunden.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	Das angegebene Kennwort für die Schlüsseldatei ist falsch. Die Schlüsseldatei kann nicht verwendet werden. Die Schlüsseldatei könnte auch beschädigt sein.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_ FOR_EXPORT	In einer eingeschränkten Verschlüsselungsumgebung wird die Schlüsselgröße nicht unterstützt.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Eine falsch formatierte SSL-Nachricht wurde vom Partner empfangen.
0x0000019b	411	GSK_ERROR_BAD_MAC	Der Nachrichtenauthentifizierungscode wurde nicht erfolgreich verifiziert.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Nicht unterstütztes SSL-Protokoll oder nicht unterstützter Zertifikatstyp.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	Das empfangene Zertifikat enthielt eine falsche Signatur.
0x0000019e	414	GSK_ERROR_BAD_CERT	Falsch formatiertes Zertifikat vom Partner empfangen.
0x0000019f	415	GSK_ERROR_BAD_PEER	Ein ungültiges SSL-Protokoll wurde vom Partner empfangen.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	Das selbst signierte Zertifikat ist nicht gültig.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	read() ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	write() ist fehlgeschlagen. Melden Sie diesen Fehler dem IBM Software Support.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	Der Partner hat das Socket geschlossen, bevor das Protokoll beendet war.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	Die angegebene V2-Verschlüsselung ist nicht gültig.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	Die angegebene V3-Verschlüsselung ist nicht gültig.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_ COMBINATION	Melden Sie diesen Fehler dem IBM Software Support.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_ FAILED	Die Kennung wurde nicht erstellt. Melden Sie diesen Fehler dem IBM Software Support.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	Initialisierung ist fehlgeschlagen. Melden Sie diesen internen Fehler dem Service.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	Bei der Überprüfung eines Zertifikats kann nicht auf die angegebene Benutzerregistry zugegriffen werden.

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	Der angegebene Schlüssel enthielt keinen privaten Schlüssel.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_ NOTLOADED	Der Versuch, die angegebene gemeinsam genutzte PKCS11-Bibliothek zu laden, ist fehlgeschlagen.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_ LABELMISMATH	Der PKCS #11-Treiber konnte das vom aufrufenden Programm angegebene Token nicht finden.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_ NOTPRESENT	Ein PKCS #11-Token ist in dem Bereich nicht vorhanden.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_ BADPASSWORD	Das Kennwort/die PIN für den Zugriff auf das PKCS #11-Token ist falsch.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	Der empfangene SSL-Header war kein korrekt formatierter SSLv2-Header.
0x000001b2	434	GSK_CSP_OPEN_ERROR	Der hardwarebasierte Verschlüsselungsserviceanbieter (Cryptographic Service Provider = CSP) konnte nicht geöffnet werden. Entweder ist der CSP-Name nicht korrekt angegeben oder ein Versuch, auf den angegebenen CSP-Zertifikatsspeicher zuzugreifen, ist fehlgeschlagen.
0x000001b3	435	GSK_CSP_OPEN_ERROR	Einige sich widersprechende Attribute für die SSL-Operation wurden definiert.
0x000001b4	436	GSK_CSP_OPEN_ERROR	Die Microsoft Crypto API wird nur unter Microsoft Windows 2000 mit Service-Pack 2 unterstützt.
0x000001b5	437	GSK_CSP_OPEN_ERROR	System wird im IPv6-Modus ausgeführt, ohne dass eine PEERID definiert ist.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	Die Puffergröße ist negativ oder Null.
0x000001f6	502	GSK_WOULD_BLOCK	Wird mit nicht geblockter Ein-/Ausgabe verwendet. Siehe den Abschnitt zur nicht geblockten Ein-/Ausgabe.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 ist für reset_cipher() erforderlich, und die Verbindung verwendet SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	Eine ungültige ID wurde für den Funktionsaufruf gsk_secure_soc_misc() angegeben.
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	Der Funktionsaufruf hat eine ID, die nicht gültig ist. Dieses Problem kann auch durch die Angabe einer Umgebungskennung verursacht werden, wenn stattdessen eine Kennung für eine SSL-Verbindung verwendet werden müsste.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	Das Attribut hat eine negative Länge, die nicht gültig ist.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ ENUMERATION	Der Aufzählungswert ist für den angegebenen Aufzählungstyp nicht gültig.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Eine Parameterliste, die zum Ersetzen der SID-Cacheroutinen nicht gültig ist.

Rückkehrcode (hex)	Rückkehrcode (dezimal)	Konstante	Erläuterung
0x000002c1	705	GSK_ATTRIBUTE_INVALID_ NUMERIC_VALUE	Beim Definieren eines numerischen Attributs ist der angegebene Wert für das spezielle Attribut, das definiert wird, nicht gültig.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_ SETTING	Für die zusätzliche Zertifikatsvalidierung wurden sich widersprechende Parameter definiert.
0x000002c3	707	GSK_AES_UNSUPPORTED	Der AES-Verschlüsselungsalgorithmus wird nicht unterstützt.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	Die PEERID hat nicht die korrekte Länge.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	Der betreffende Chiffrierwert ist nicht zulässig, wenn die FIPS-Betriebsart auf OFF gesetzt ist.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	In der FIPS-Betriebsart sind keine genehmigten FIPS-Chiffrierwerte ausgewählt.
0x00000641	1601	GSK_TRACE_STARTED	Der Trace wurde erfolgreich gestartet.
0x00000642	1602	GSK_TRACE_STOPPED	Der Trace wurde erfolgreich gestoppt.
0x00000643	1603	GSK_TRACE_NOT_STARTED	Es wurde zuvor keine Tracedatei gestartet. Daher kann sie nicht gestoppt werden.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	Die Tracedatei wurde bereits gestartet. Daher kann sie nicht erneut gestartet werden.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	Die Tracedatei kann nicht geöffnet werden. Der erste Parameter von gsk_start_trace() muss ein gültiger vollständiger Pfaddateiname sein.

Glossar

Dieses Glossar stellt Begriffe und Definitionen für IBM Spectrum Protect, IBM Spectrum Protect Snapshot und zugehörige Produkte bereit.

Die folgenden Querverweise werden in diesem Glossar verwendet:

- Mit *Siehe* wird von einem Begriff, der nicht bevorzugt verwendet wird, auf den bevorzugten Begriff oder von einer Abkürzung auf die vollständige Form verwiesen.
- Mit *Siehe auch* wird auf einen zugehörigen oder gegensätzlichen Begriff verwiesen.

Andere Begriffe und Definitionen finden Sie auf der IBM® Terminology-Website.

A B C D E F G H I J K L M N O P Q R S T U V W Z

A

Abruf
: Archivierte Informationen aus dem Speicherpool auf die Workstation kopieren, um sie zu verwenden. Die Abrufoperation hat keine Auswirkungen auf die archivierte Version im Speicherpool. Siehe auch Archivierung.

Absoluter Modus
: Bei der Speicherverwaltung ein Modus der Sicherungskopiengruppe, der angibt, dass eine Datei oder ein Verzeichnis bei der Teilsicherung zu berücksichtigen ist, auch wenn sich die Datei oder das Verzeichnis seit der letzten Sicherung nicht geändert hat. Siehe auch Modus, Geänderter Modus.

Abstimmung
: Der Prozess, bei dem die Konsistenz zwischen dem ursprünglichen Datenrepository und dem größeren System, auf dem die Daten für die Sicherung gespeichert werden, sichergestellt wird. Beispiele für größere Systeme, auf denen die Daten für die Sicherung gespeichert werden, sind Speicherserver oder andere Speichersysteme. Während des Abstimmungsprozesses werden Daten, die nicht mehr benötigt werden, entfernt.

ACK
: Siehe Empfangsbestätigung.

ACL

Siehe Zugriffssteuerungsliste (ACL).

Adaptive Subdateisicherung
: Ein Sicherungstyp, bei dem nur geänderte Teile einer Datei an den Server gesendet werden und nicht die gesamte Datei. Mit der adaptiven Subdateisicherung wird der Datenaustausch im Netz reduziert und die Sicherungsgeschwindigkeit wird erhöht.

Administrator
: Eine Person, die für Verwaltungstasks wie z. B. Zugriffsberechtigungen und Content-Management verantwortlich ist. Administratoren können Benutzern auch Berechtigungsstufen zuordnen.

Agentenknoten
: Ein Clientknoten, dem Proxyberechtigung erteilt wurde, um Operationen für einen anderen Clientknoten auszuführen, der der Zielknoten ist.

Aggregat
: Ein Objekt, das in einem oder mehreren Speicherpools gespeichert ist und das aus einer Gruppe von logischen Dateien besteht, die zusammengefasst sind. Siehe auch Logische Datei, Physische Datei.

Aktive Maßnahmengruppe
: Die aktivierte Maßnahmengruppe. Diese Maßnahmengruppe enthält die Maßnahmenregeln, die alle der Maßnahmendomäne zugeordneten Clientknoten derzeit verwenden. Siehe auch Maßnahmendomäne, Maßnahmengruppe.

Aktives Dateisystem
: Ein Dateisystem, dem die Speicherverwaltung hinzugefügt wurde. Mit der Speicherverwaltung werden folgende Tasks für ein aktives Dateisystem ausgeführt: automatische Umlagerung, Abstimmung, selektive Umlagerung und Rückruf. Siehe auch Inaktives Dateisystem.

Aktive Version
: Die neueste Sicherungskopie einer gespeicherten Datei. Die aktive Version einer Datei kann erst dann gelöscht werden, wenn ein Sicherungsprozess erkennt, dass der Benutzer die Datei entweder durch eine neuere Version ersetzt oder vom Dateiserver bzw. von der Workstation gelöscht hat. Siehe auch Sicherungsversion, Inaktive Version.

Aktivieren
: Den Inhalt einer Maßnahmengruppe überprüfen und die Maßnahmengruppe dann zur aktiven Maßnahmengruppe machen.

Aktivitätenprotokoll
: Ein Protokoll, in dem die Nachrichten für normale Aktivitäten aufgezeichnet werden, die der Server generiert. Diese Nachrichten enthalten Informationen zu Server- und Clientoperationen, wie die Startzeit der Sitzungen oder E/A-Fehler von Einheiten.

Anwendungsclient
: Ein Programm, das auf einem System installiert ist, um eine Anwendung zu schützen. Der Server stellt Sicherungsservices für einen Anwendungsclient zur Verfügung.

Arbeitsdatenträger
: Ein Datenträger mit Kennsatz, der keine Daten oder keine gültigen Daten enthält, der nicht definiert ist und der für die Verwendung zur Verfügung steht. Siehe auch Datenträger.

Archivierung
: Programme, Daten oder Dateien auf andere Speichermedien kopieren, normalerweise für die Langzeitspeicherung oder zur Absicherung. Siehe auch Abruf.

Archivierungskopie
: Eine Datei oder Dateigruppe, die im Serverspeicher archiviert wurde.

Archivierungskopiengruppe
: Ein Maßnahmenobjekt mit Attributen, die die Generierung, den Zielort und das Verfallsdatum von archivierten Dateien steuern. Siehe auch Kopiengruppe.

Aufbewahrungsdauer
: Die Zeit in Tagen, in denen inaktive gesicherte oder archivierte Dateien im Speicherpool aufbewahrt werden, bevor sie gelöscht werden. Kopiengruppenattribute und Standardaufbewahrungszeiträume für die Domäne definieren die Aufbewahrungszeit.

Aufbewahrungszeitraum für Archivierung
: Die Anzahl der Tage, die der Speichermanager eine archivierte Datei aufbewahrt, wenn der Server die Datei nicht erneut an eine entsprechende Verwaltungsklasse binden kann. Siehe auch Binden.

Aufbewahrungszeitraum für Sicherung
: Die Anzahl der Tage, die der Speichermanager eine Sicherungsversion aufbewahrt, nachdem der Server die Datei nicht erneut an eine entsprechende Verwaltungsklasse binden kann.

Ausgelagerte VSS-Sicherung
: Eine Sicherungsoperation, bei der ein (auf einem anderen System installierter) Microsoft-VSS-Hardwareprovider (VSS - Volume Shadow Copy Service) verwendet wird, um Daten auf den Server zu versetzen. Bei diesem Typ der Sicherungsoperation wird die Arbeitslast der Sicherung vom Produktionssystem auf ein anderes System verlagert.

Ausschließen
: Der Prozess der Angabe von Dateien in einer Einschluss-/Ausschlussliste. Dieser Prozess verhindert, dass Dateien gesichert oder umgelagert werden, wenn ein Benutzer oder ein Zeitplan eine Teilsicherungsoperation oder selektive Sicherungsoperation startet. Eine Datei kann von der Sicherung und/oder der Speicherverwaltung ausgeschlossen werden.

Ausschluss-/Einschlussliste
: Siehe Einschluss-/Ausschlussliste.

Authentifizierungsregel
: Eine Spezifikation, die ein anderer Benutzer verwenden kann, um Dateien aus dem Speicher zurückzuschreiben oder abzurufen.

AutoFS
: Siehe Auto-Mount-Dateisystem.

Automatische Erkennung
: Eine Funktion, die die Seriennummer eines Laufwerks oder eines Kassettenarchivs in der Datenbank feststellt, auflistet und aktualisiert, wenn der Pfad vom lokalen Server definiert ist.

Automatische Umlagerung
: Der Prozess, mit dem Dateien automatisch von einem lokalen Dateisystem in den Speicher versetzt werden. Dieser Prozess basiert auf Optionen und Einstellungen, die ein Root auf einer Workstation auswählt. Siehe auch Bedarfsumlagerung, Schwellenumlagerung.

Auto-Mount-Dateisystem (AutoFS)
: Ein Dateisystem, das von einem Automount-Dämon verwaltet wird. Der Automount-Dämon überwacht einen bestimmten Verzeichnispfad und hängt das Dateisystem automatisch an, um auf Daten zuzugreifen.

B

Bandarchiv
: Eine Gruppe von Geräten und Funktionen, die die Bandumgebung einer Installation unterstützen. Das Bandarchiv kann Racks für Bandkassetten, Mechanismen für das automatische Einlegen von Bändern, eine Reihe von Bandlaufwerken und eine Gruppe von zugehörigen Banddatenträgern umfassen, die in diese Laufwerke eingelegt sind.

Bedarfsumlagerung
: Der Prozess, mit dem in einem Dateisystem, für das die hierarchische Speicherverwaltung (Hierarchical Storage Management - HSM) aktiv ist, auf eine Bedingung 'Zu wenig Speicherbereich' reagiert wird. Dateien werden in den Serverspeicher umgelagert, bis die Speicherbereichsbelegung die untere Schwelle erreicht, die für das Dateisystem definiert wurde. Sind die obere Schwelle und die untere Schwelle identisch, wird eine einzige Datei umgelagert. Siehe auch Automatische Umlagerung, Selektive Umlagerung, Schwellenumlagerung.

Bedienerberechtigungsklasse
: Eine Berechtigungsklasse, die einem Administrator die Berechtigung für folgende Tasks erteilt: Server inaktivieren oder stoppen, Server aktivieren, Serverprozesse abbrechen und austauschbare Datenträger verwalten. Siehe auch Berechtigungsklasse.

Benannte Pipe
: Eine Art der Interprozesskommunikation, bei der Nachrichtendatenströme zwischen Peer-Prozessen, wie z. B. einem Client und einem Server, fließen können.

Berechtigter Benutzer
: Ein Benutzer mit Administratorberechtigung für den Client auf einer Workstation. Dieser Benutzer ändert Kennwörter, führt offene Registrierungen durch und löscht Dateibereiche.

Berechtigung
: Das Recht, auf Objekte, Ressourcen oder Funktionen zuzugreifen. Siehe auch Berechtigungsklasse.

Berechtigungsklasse
: Eine Berechtigungsstufe, die einem Administrator erteilt wird. Die Berechtigungsklasse bestimmt, welche Verwaltungstasks vom Administrator ausgeführt werden können. Siehe auch Berechtigung, Knotenberechtigungsklasse, Bedienerberechtigungsklasse, Maßnahmenberechtigungsklasse, Speicherberechtigungsklasse, Systemberechtigungsklasse.

Berechtigungsregel
: Eine Spezifikation, die es einem anderen Benutzer ermöglicht, die Dateien eines Benutzers aus dem Speicher zurückzuschreiben oder abzurufen.

Beschädigte Datei
: Eine physische Datei, in der Lesefehler erkannt wurden.

Binden
: Einer Datei einen Verwaltungsklassennamen zuordnen. Siehe auch Aufbewahrungszeitraum für Archivierung, Verwaltungsklasse, Erneut binden.

Bucket
: Cloudspeichercontainer, der von Amazon Simple Storage Service (Amazon S3) verwendet wird.

C

Cache
: Eine Duplikatkopie einer Datei auf ein Speichermedium mit wahlfreiem Zugriff stellen, wenn der Server eine Datei in einen anderen Speicherpool in der Hierarchie umlagert.

Cachedatei
: Eine Momentaufnahme eines logischen Datenträgers, die vom Logical Volume Snapshot Agent erstellt wurde. Werden Blöcke während der Imagesicherung geändert, werden sie unmittelbar vor der Änderung gesichert und ihre logischen Bereiche werden in den Cachedateien gesichert.

CAD
: Siehe Clientakzeptordämon.

Client
: Ein Softwareprogramm oder ein Computer, das bzw. der Services von einem Server anfordert. Siehe auch Server.

Clientakzeptor
: Ein Service, der Web-Browsern das Java™-Applet für den Web-Client bereitstellt. Auf Windows-Systemen wird der Clientakzeptor so installiert, dass er als Dienst ausgeführt wird. Auf AIX-, UNIX- und Linux-Systemen wird der Clientakzeptor als Dämon ausgeführt.

Clientakzeptordämon (CAD)
: Siehe Clientakzeptor.

Clientbenutzeroptionsdatei
: Eine Datei, die die Gruppe von Verarbeitungsoptionen enthält, die die Clients auf dem System verwenden. Die Gruppe kann Optionen umfassen, die den Server angeben, den der Client kontaktiert, sowie Optionen, die sich auf Sicherungsoperationen, Archivierungsoperationen, Operationen für hierarchische Speicherverwaltung und geplante Operationen auswirken. Diese Datei wird auch

als Datei dsm.opt bezeichnet. Für AIX-, UNIX- oder Linux-Systeme siehe auch 'Clientsystemoptionsdatei'. Siehe auch Clientsystemoptionsdatei, Optionsdatei.

Clientdomäne
: Die Gruppe von Laufwerken, Dateisystemen oder Datenträgern, die der Benutzer für das Sichern oder Archivieren von Daten mit dem Client für Sichern/Archivieren auswählt.

Client für hierarchische Speicherverwaltung (HSM-Client)
: Ein Clientprogramm, das zusammen mit dem Server hierarchische Speicherverwaltung (HSM - Hierarchical Storage Management) für ein System bereitstellt. Siehe auch Hierarchische Speicherverwaltung, Verwaltungsklasse.

Client für Sichern/Archivieren
: Ein Programm, das auf einer Workstation oder einem Dateiserver ausgeführt wird und Benutzern ein Mittel zum Sichern, Archivieren, Zurückschreiben und Abrufen von Dateien bietet. Siehe auch Verwaltungsclient.

Clientknoten
: Ein Dateiserver oder eine Workstation, auf dem bzw. der das Clientprogramm für Sichern/Archivieren installiert und beim Server registriert wurde.

Clientknotensitzung
: Eine Sitzung, in der ein Clientknoten mit einem Server kommuniziert, um Sicherungs-, Zurückschreibungs-, Archivierungs-, Abruf-, Umlagerungs- oder Rückrufanforderungen auszuführen. Siehe auch Verwaltungssitzung.

Clientoptionsdatei
: Eine editierbare Datei, in der der Server und die Übertragungsmethode angegeben sind und die die Konfiguration für die Sicherung, Archivierung, hierarchische Speicherverwaltung und Zeitplanung bereitstellt.

Clientoptionsgruppe
: Eine Gruppe von Optionen, die auf dem Server definiert sind und auf Clientknoten in Verbindung mit der Clientoptionsdatei verwendet werden.

Client/Server
: Bezieht sich auf das Interaktionsmodell bei der verteilten Datenverarbeitung, bei dem ein Programm auf einem Computer eine Anforderung an ein Programm auf einem anderen Computer sendet und auf eine Antwort wartet. Das anfordernde Programm wird als Client bezeichnet, das antwortende Programm als Server.

Clientsystemoptionsdatei
: Eine Datei, die auf Clients mit AIX-, UNIX- oder Linux-Systemen verwendet wird. Diese Datei enthält eine Gruppe von Verarbeitungsoptionen, die die Server angeben, die für Services kontaktiert werden sollen. Diese Datei gibt auch die Übertragungsmethoden und Optionen für Sicherung, Archivierung, hierarchische Speicherverwaltung und Zeitplanung an. Siehe auch Clientbenutzeroptionsdatei, Optionsdatei.

Clientzeitplan
: Ein Datenbanksatz, der die geplante Verarbeitung einer Clientoperation während einer bestimmten Zeitspanne beschreibt. Bei der Clientoperation kann es sich um eine Sicherungs-, Archivierungs-, Zurückschreibungs- oder Abrufoperation, einen Clientbetriebssystembefehl oder ein Makro handeln. Siehe auch Zeitplan für Verwaltungsbefehle, Zentrale Zeitplanung, Zeitplan.

Cloud-Containerspeicherpool
: Ein Speicherpool, der von einem Server verwendet wird, um Daten im Cloudspeicher zu speichern. Der Cloudspeicher kann sich vor Ort (on premises) oder außerhalb des Unternehmens (off premises) befinden. Siehe auch Containerspeicherpool, Verzeichniscontainerspeicherpool, Speicherpool.

Container
: Eine Datenspeicherposition, z. B. eine Datei, ein Verzeichnis oder eine Einheit. Siehe auch Containerspeicherpool.

Containerkopienspeicherpool
: Ein Speicherpool, der von einem Server verwendet wird, um Kopien von Bereichen aus Verzeichniscontainerspeicherpools zu speichern. Die Kopien werden verwendet, um Beschädigungen in einem Verzeichniscontainerspeicherpool zu reparieren. Containerkopienspeicherpools verwenden sequenzielle Datenträger wie z. B. Band. Siehe auch Verzeichniscontainerspeicherpool.

Containerspeicherpool
: Ein primärer Speicherpool, der von einem Server zum Speichern von Daten verwendet wird. Daten werden in Containern in Dateisystemverzeichnissen oder im Cloudspeicher gespeichert. Falls erforderlich, werden Daten dedupliziert, wenn der Server die Daten in den Speicherpool schreibt. Siehe auch Cloud-Containerspeicherpool, Container, Verzeichniscontainerspeicherpool.

D

Dämon
: Ein unbeaufsichtigtes Programm, das kontinuierliche oder regelmäßige Funktionen wie Netzsteuerung ausführt.

Data Storage-Management Application-Programming Interface (DSMAPI)
: Eine Funktions- und Semantikgruppe, die Ereignisse für Dateien überwachen und die Daten in einer Datei verwalten und pflegen kann. In einer HSM-Umgebung verwendet eine DSMAPI Ereignisse, um Datenverwaltungsanwendungen über Operationen mit Dateien zu informieren. Zudem speichert eine DSMAPI beliebige Attributinformationen mit einer Datei; sie unterstützt verwaltete Regionen in einer Datei und verwendet DSMAPI-Zugriffsberechtigungen, um den Zugriff auf ein Dateiobjekt zu steuern.

Dateialter
: Bei der Festlegung der Umlagerungspriorität die Anzahl Tage seit dem letzten Zugriff auf eine Datei.

Dateibereich
: Ein logischer Speicherbereich im Serverspeicher, der eine Gruppe von Dateien enthält, die von einem Clientknoten aus einer einzelnen logischen Partition, einem einzelnen Dateisystem oder einem einzelnen virtuellen Mountpunkt gesichert oder archiviert wurden. Clientknoten können ihre Dateibereiche im Serverspeicher zurückschreiben, abzurufen oder löschen. Im Serverspeicher werden Dateien, die zu einem einzigen Dateibereich gehören, nicht notwendigerweise zusammen gespeichert.

Dateibereichs-ID (FSID)

Eine eindeutige numerische Kennung, die der Server einem Dateibereich zuordnet, wenn er in einem Serverspeicher gespeichert wird.

Dateiindex
: Die interne Struktur, die einzelne Dateien auf AIX-, UNIX- oder Linux-Systemen beschreibt. Ein Dateiindex enthält den Knoten, den Typ, den Eigner und die Position einer Datei.

Dateiindexnummer
: Eine Nummer, die eine bestimmte Dateiindexdatei im Dateisystem angibt.

Datei mit freien Bereichen
: Eine Datei, die mit einer Länge erstellt wird, die größer als die darin enthaltenen Daten ist. Somit sind leere Speicherbereiche für die zukünftige Hinzufügung von Daten vorhanden.

Dateiserver
: Ein dedizierter Computer mit seinen peripheren Speichereinheiten, die an ein lokales Netz angeschlossen sind. Der Computer speichert Programme und Dateien, die von Benutzern in dem Netz gemeinsam genutzt werden.

Dateistatus
: Der Speicherverwaltungsmodus einer Datei, die in einem Dateisystem gespeichert ist, dem die Speicherverwaltung hinzugefügt wurde. Eine Datei kann sich in einem der drei folgenden Status befinden: resident, vorumgelagert oder umgelagert. Siehe auch Umgelagerte Datei, Vorumgelagerte Datei, Residente Datei.

Dateisystemstatus
: Der Speicherverwaltungsmodus eines Dateisystems, das sich auf einer Workstation befindet, auf der der HSM-Client (HSM = Hierarchical Storage Management = Hierarchische Speicherverwaltung) installiert ist. Ein Dateisystem kann sich in einem der folgenden Status befinden: nativ, aktiv, inaktiv oder global inaktiv.

Dateizugriffszeit
: Auf AIX-, UNIX- oder Linux-Systemen die Zeit, zu der der letzte Zugriff auf die Datei erfolgte.

Datenbank für vorumgelagerte Dateien
: Eine Datenbank, die Informationen zu allen in den Serverspeicher vorumgelagerten Dateien enthält.

Datenbankmomentaufnahme
: Eine vollständige Sicherung der gesamten Datenbank auf Medien, die an einen anderen Standort gebracht werden können. Wenn eine Momentaufnahme der Datenbank erstellt wird, wird die momentane Datenbanksicherungsserie nicht unterbrochen. Eine Datenbankmomentaufnahme kann keine Datenbankteilsicherungen enthalten. Siehe auch Datenbanksicherungsserie, Gesamtsicherung.

Datenbanksicherungsserie
: Eine Gesamtsicherung der Datenbank, plus bis zu 32 Teilsicherungen, die seit der Gesamtsicherung erstellt wurden. Jede Gesamtsicherung, die ausgeführt wird, startet eine neue Datenbanksicherungsserie. Eine Zahl identifiziert jede Sicherungsserie. Siehe auch Datenbankmomentaufnahme, Gesamtsicherung.

Datencenter
: In einer virtualisierten Umgebung ein Container, der Hosts, Cluster, Netze und Datenspeicher enthält.

Datendeduplizierung
: Eine Methode zum Reduzieren des Speicherbedarfs, indem redundante Daten entfernt werden. Nur eine Instanz der Daten wird auf Speicherdatenträgern aufbewahrt. Andere Instanzen derselben Daten werden durch einen Zeiger auf die aufbewahrte Instanz ersetzt. Siehe auch Inline-Datendeduplizierung, Nachgeordnete Datendeduplizierung.

Datenmanagerserver
: Ein Server, der Metadateninformationen für den Clientdatenträgerbestand sammelt und für den Speicheragenten Transaktionen über das LAN verwaltet. Der Datenmanagerserver informiert den Speicheragenten über die jeweiligen Kassettenarchivattribute und die Kennung des Zieldatenträgers.

Datenspeicher
: In einer virtualisierten Umgebung die Position, an der Daten der virtuellen Maschine gespeichert werden.

Datenträger
: Ein diskreter Speicherbereich auf Platte, Band oder einem anderen Medium zur Datenaufzeichnung, das eine Kennung und eine Parameterliste unterstützt, z. B. einen Datenträgerkennsatz oder Ein-/Ausgabesteuerung. Siehe auch Arbeitsdatenträger, Serverspeicher, Speicherpool, Speicherpooldatenträger.

Datenträgerhistorydatei
: Eine Datei, die Informationen zu Datenträgern enthält, die vom Server für Datenbanksicherungen und für den Export von Administrator-, Knoten-, Maßnahmen- oder Serverdaten verwendet wurde. Die Datei umfasst außerdem Informationen zu Datenträgern in Speicherpools mit sequenziellem Zugriff, die hinzugefügt, erneut verwendet oder gelöscht wurden. Die Informationen sind eine Kopie der Datenträgerinformationen in der Serverdatenbank.

Datenübertragungsgeschwindigkeit im Netz
: Eine Geschwindigkeit, die durch Dividieren der Gesamtzahl der übertragenen Byte durch die Datenübertragungszeit berechnet wird. Bei dieser Geschwindigkeit kann es sich beispielsweise um die Zeit handeln, die für die Übertragung von Daten über ein Netz erforderlich ist.

Deduplizierung
: Siehe Datendeduplizierung.

Dialog
: Eine Verbindung zwischen zwei Programmen über eine Sitzung, über die diese während der Verarbeitung einer Transaktion kommunizieren können.

Disaster Recovery Manager (DRM)
: Eine Funktion, die Benutzer bei der Vorbereitung und Verwendung einer Plandatei zur Wiederherstellung nach einem Katastrophenfall für den Server unterstützt.

Domäne
: Eine Gruppierung von Clientknoten mit einer oder mehreren Maßnahmengruppen, die für die Clientknoten Daten oder Speicherressourcen verwalten. Siehe auch Maßnahmendomäne.

DRM

Siehe Disaster Recovery Manager.

DSMAPI
: Siehe Data Storage-Management Application-Programming Interface.

Durchnummerierung
: Der Prozess, bei dem Dateien verarbeitet werden, die während der Sicherungs- oder Archivierungsverarbeitung geändert wurden. Siehe auch Gemeinsam dynamisch (Durchnummerierung), Gemeinsam statisch (Durchnummerierung), Statisch (Durchnummerierung).

Durchsatz
: Bei der Speicherverwaltung die Gesamtsumme der Byte im Verarbeitungsprozess (mit Ausnahme des Systemaufwands), die gesichert oder zurückgeschrieben werden, dividiert durch die abgelaufene Zeit.

Dynamisch (Durchnummerierung)
: Die Kopiennummerierung, bei der eine Datei oder ein Ordner beim ersten Versuch gesichert oder archiviert wird, unabhängig davon, ob sie bzw. er sich bei der Sicherung oder Archivierung ändert. Siehe auch Gemeinsam dynamisch (Durchnummerierung), Gemeinsam statisch (Durchnummerierung), Statisch (Durchnummerierung).

E

EA
: Siehe Erweitertes Attribut.

EB
: Siehe Exabyte.

EFS
: Siehe Verschlüsseltes Dateisystem.

EFS (Encrypted File System - Verschlüsseltes Dateisystem)
: Ein Dateisystem, das Verschlüsselung auf Dateisystemebene verwendet.

Einheitenklasse
: Eine benannte Reihe von Merkmalen, die auf eine Gruppe von Speichereinheiten angewendet wird. Jede Einheitenklasse verfügt über einen eindeutigen Namen und stellt den Einheitentyp Platte, Datei, optische Platte oder Band dar.

Einheitenkonfigurationsdatei

1. Für einen Server eine Datei, die Informationen zu definierten Einheitenklassen und auf einigen Servern auch zu definierten Kassettenarchiven und Laufwerken enthält. Die Informationen sind eine Kopie der Einheitenkonfigurationsdaten in der Datenbank.
2. Für einen Speicheragenten eine Datei, die den Namen und das Kennwort des Speicheragenten sowie Informationen zu dem Server enthält, der die an ein SAN angeschlossenen Kassettenarchive und Laufwerke verwaltet, die der Speicheragent verwendet.

Einheitentyp FILE
: Ein Einheitentyp, bei dem Dateien mit sequenziellem Zugriff auf Plattenspeicher als Datenträger verwendet werden.

Einheit zum Versetzen von Daten
: Eine Einheit, die für den Server Daten versetzt. Ein NAS-Dateiserver (NAS - Network-Attached Storage) ist eine Einheit zum Versetzen von Daten.

Einschluss-/Ausschlussdatei
: Eine Datei, die Anweisungen enthält, mit denen die zu sichernden Dateien und die zugeordneten Verwaltungsklassen bestimmt werden, die zum Sichern oder Archivieren verwendet werden sollen. Siehe auch Einschluss-/Ausschlussliste.

Einschluss-/Ausschlussliste
: Eine Liste mit Optionen, die bestimmte Dateien für die Sicherung einschließen oder ausschließen. Eine Exclude-Option gibt Dateien an, die nicht gesichert werden sollen. Eine Include-Option gibt Dateien an, die von den Ausschlussregeln ausgeschlossen sind, oder ordnet einer Datei oder einer Dateigruppe eine Verwaltungsklasse für Sicherungs- oder Archivierungsservices zu. Siehe auch Einschluss-/Ausschlussdatei.

Empfänger
: Ein Server-Repository, das ein Protokoll der Server- und Clientnachrichten als Ereignisse enthält. Ein Empfänger kann beispielsweise ein Dateiexit, Benutzerexit oder die Serverkonsole und das Aktivitätenprotokoll sein. Siehe auch Ereignis.

Empfangsbestätigung (Acknowledgment = ACK)
: Das Senden von Empfangsbestätigungszeichen als positive Antwort auf eine Datenübertragung.

Ereignis
: Ein Vorkommen mit Signifikanz für eine Task oder ein System. Ereignisse können die Beendigung oder das Fehlschlagen einer Operation, eine Benutzeraktion oder die Änderung des Status eines Prozesses einschließen. Siehe auch Unternehmensprotokollierung, Empfänger.

Ereignissatz
: Ein Datenbanksatz, der den tatsächlichen Status und die Ergebnisse für Ereignisse beschreibt.

Ereignisserver
: Ein Server, an den andere Server Ereignisse zum Protokollieren senden können. Der Ereignisserver leitet die Ereignisse an alle Empfänger weiter, die für die Ereignisse des sendenden Servers aktiviert sind.

Erneut binden
: Allen gesicherten Versionen einer Datei einen neuen Verwaltungsklassennamen zuordnen. Beispielsweise wird eine Datei, die über eine aktive Sicherungsversion verfügt, erneut gebunden, wenn eine spätere Version der Datei mit einer anderen Verwaltungsklassenzuordnung gesichert wird. Siehe auch Binden, Verwaltungsklasse.

Erweitern
: Den Teil des verfügbaren Speicherbereichs vergrößern, der zum Speichern von Datenbank- oder Wiederherstellungsprotokolldaten verwendet wird.

Erweitertes Attribut (EA)

Namen oder Wertepaare, die Dateien oder Verzeichnissen zugeordnet sind. Es gibt drei Klassen von erweiterten Attributen: Benutzerattribute, Systemattribute und Vertrauensattribute.

Exabyte (EB)
: Für den Hauptspeicher, die realen und virtuellen Speicherkapazitäten und die Kanalkapazität 2 hoch 60 oder 1 152 921 504 606 846 976 Byte. Für die Plattenspeicher- und Übertragungskapazität 1 000 000 000 000 000 000 Byte.

Externes Kassettenarchiv
: Eine Gruppe von Laufwerken, die von einem anderen Datenträgerverwaltungssystem als dem Speicherverwaltungsserver verwaltet wird.

F

Fehlerprotokoll
: Ein Datensatz oder eine Datei, der bzw. die zum Aufzeichnen von Fehlerinformationen zu einem Produkt oder System verwendet wird.

Fern
: Bei Produkten für die hierarchische Speicherverwaltung bezieht sich der Begriff auf den Ursprung von umgelagerten Dateien, die versetzt werden. Siehe auch Lokal.

Festschreibungspunkt
: Ein Zeitpunkt, zu dem Daten als konsistent angesehen werden.

File System Migrator (FSM)
: Eine Kernelerweiterung, die alle Dateisystemoperationen abfängt und die erforderliche Speicherverwaltungsunterstützung bereitstellt. Ist keine Speicherverwaltungsunterstützung erforderlich, wird die Operation an das Betriebssystem weitergeleitet, das seine normalen Funktionen ausführt. Der File System Migrator wird über das Dateisystem angehängt, wenn dem Dateisystem die Speicherverwaltung hinzugefügt wird.

FSID
: Siehe Dateibereichs-ID.

FSM
: Siehe File System Migrator.

G

GB
: Siehe Gigabyte.

Geänderter Modus
: Bei der Speicherverwaltung ein Modus der Sicherungskopiengruppe, der angibt, dass eine Datei oder ein Verzeichnis bei der Teilsicherung nur zu berücksichtigen ist, wenn sie bzw. es sich seit der letzten Sicherung geändert hat. Eine Datei oder ein Verzeichnis wird als geändert betrachtet, wenn sich das Datum, die Größe, der Eigner oder die Berechtigung geändert hat. Siehe auch Absoluter Modus, Modus.

Gemeinsam dynamisch (Durchnummerierung)
: Ein Wert für die Durchnummerierung, der angibt, dass eine Datei nicht gesichert oder archiviert werden darf, wenn sie während der Operation gerade geändert wird. Der Client für Sichern/Archivieren versucht mehrmals, die Sicherungs- oder Archivierungsoperation zu wiederholen. Wenn die Datei bei jedem Versuch gerade geändert wird, sichert oder archiviert der Client für Sichern/Archivieren die Datei beim letzten Versuch. Siehe auch Dynamisch (Durchnummerierung), Durchnummerierung, Gemeinsam statisch (Durchnummerierung), Statisch (Durchnummerierung).

Gemeinsam genutztes Kassettenarchiv
: Eine Kassettenarchiveinheit, die von mehreren Speicherverwaltungsservern verwendet wird.

Gemeinsam statisch (Durchnummerierung)
: Ein Durchnummerierungswert für die Kopiengruppe, der angibt, dass eine Datei während einer Sicherungs- oder Archivierungsoperation nicht geändert werden darf. Der Client versucht mehrmals, die Operation zu wiederholen. Ist die Datei bei jedem Versuch im Gebrauch, wird sie nicht gesichert oder archiviert. Siehe auch Dynamisch (Durchnummerierung), Durchnummerierung, Gemeinsam dynamisch (Durchnummerierung), Statisch (Durchnummerierung).

General Parallel File System (GPFS)
: Ein leistungsfähiges Dateisystem für gemeinsam genutzte Platten, das den Knoten in einer Clustersystemumgebung Datenzugriff bereitstellen kann. Siehe auch Information Lifecycle Management.

Gesamtsicherung
: Der Prozess, bei dem die gesamte Serverdatenbank gesichert wird. Eine Gesamtsicherung beginnt eine neue Datenbanksicherungsserie. Siehe auch Datenbanksicherungsserie, Datenbankmomentaufnahme, Teilsicherung.

Gesamtübertragungsrate
: Eine Leistungsstatistik, die die durchschnittliche Anzahl der Byte angibt, die während der Verarbeitung einer bestimmten Operation pro Sekunde übertragen wurden.

Geschätzte Kapazität
: Der verfügbare Speicherbereich eines Speicherpools in Megabyte.

Geschlossene Registrierung
: Ein Registrierungsprozess, bei dem nur ein Administrator Workstations als Clientknoten beim Server registrieren kann. Siehe auch Offene Registrierung.

Geschützter Standort
: Siehe Primärer Standort.

Gigabyte (GB)
: Für den Hauptspeicher, den realen und virtuellen Speicher und die Kanalkapazität zwei hoch 30 oder 1.073.741.824 Byte. Für die Plattenspeicher- und Übertragungskapazität 1.000.000.000 Byte.

Global eindeutige ID (GUID)

Eine über einen Algorithmus ermittelte Nummer, die eine Entität innerhalb eines Systems eindeutig identifiziert. Siehe auch Universally Unique Identifier.

Global inaktiver Status
: Der Status aller Dateisysteme, denen die Speicherverwaltung hinzugefügt wurde, wenn die Speicherverwaltung für einen Clientknoten global inaktiviert wird.

GPFS
: Siehe General Parallel File System.

GPFS-Knotengruppe
: Eine angehängte, definierte Gruppe von GPFS-Dateisystemen.

Grenzwert für Ladeanforderung
: Die maximale Anzahl Datenträger, auf die von derselben Einheitenklasse gleichzeitig zugegriffen werden kann. Der Grenzwert für Ladeanforderungen legt die maximale Anzahl von Mountpunkten fest. Siehe auch Mountpunkt.

Größe der Stubdatei
: Die Größe einer Datei, durch die eine Originaldatei in einem lokalen Dateisystem ersetzt wird, wenn sie in den Serverspeicher umgelagert wird. Die für Stubdateien angegebene Größe legt fest, wie viele Vorspanndaten in der Stubdatei gespeichert werden können. Der Standardwert für die Größe der Stubdatei ist die für ein Dateisystem definierte Blockgröße minus 1 Byte.

Gruppensicherung
: Die Sicherung einer Gruppe, die eine Liste von Dateien aus einem oder mehreren Dateibereichen enthält.

GUID
: Siehe Global eindeutige ID.

H

Häufigkeit
: Ein Kopiengruppenattribut, das das Mindestintervall zwischen Teilsicherungen in Tagen angibt.

Hierarchische Speicherverwaltung (HSM - Hierarchical Storage Management)
: Eine Funktion, die Daten auf Platte, Band oder beidem automatisch verteilt und verwaltet. Dabei werden die Einheiten dieses Typs und potenzieller anderer Typen als Ebenen in einer Speicherhierarchie betrachtet, die von schnellen, kostenintensiven Einheiten bis hin zu langsameren, kostengünstigeren Einheiten und möglicherweise austauschbaren Einheiten reicht. Diese Funktion soll die Zugriffszeit auf Daten minimieren und die verfügbare Datenträgerkapazität maximieren. Siehe auch Client für hierarchische Speicherverwaltung, Rückruf, Speicherhierarchie.

HSM
: Siehe Hierarchische Speicherverwaltung.

HSM-Client
: Siehe Client für hierarchische Speicherverwaltung.

I

IBM Spectrum Protect-Befehlsscript
: Eine Folge von IBM Spectrum Protect-Verwaltungsbefehlen, die in der Datenbank des IBM Spectrum Protect-Servers gespeichert sind. Das Script kann von jeder Serverschnittstelle aus ausgeführt werden. Das Script kann Ersetzungen für Befehlsparameter und bedingte Logik enthalten. Siehe auch Makrodatei, Script.

ILM
: Siehe Information Lifecycle Management.

Image
: Ein Dateisystem oder ein unformatierter logischer Datenträger, der als ein einziges Objekt gesichert wird.

Imagesicherung
: Die Sicherung eines gesamten Dateisystems oder eines unformatierten logischen Datenträgers als einzelnes Objekt.

Inaktives Dateisystem
: Ein Dateisystem, für das die Speicherverwaltung inaktiviert wurde. Siehe auch Aktives Dateisystem.

Inaktive Version
: Eine Sicherungsversion einer Datei, bei der es sich entweder nicht um die neueste Sicherungsversion handelt oder bei der es sich um eine Sicherungsversion einer Datei handelt, die nicht mehr im Clientsystem vorhanden ist. Inaktive Sicherungsversionen können entsprechend der Verwaltungsklasse, die der Datei zugeordnet wurde, für die Verfallsverarbeitung ausgewählt werden. Siehe auch Aktive Version, Sicherungsversion.

Information Lifecycle Management (ILM, Verwaltung von Daten über ihre gesamte Lebensdauer)
: Ein auf Maßnahmen basierendes Dateiverwaltungssystem für Speicherpools und Dateigruppen. Siehe auch General Parallel File System.

Inline-Datendeduplizierung
: Eine Methode zum Reduzieren des Speicherbedarfs, indem redundante Daten entfernt werden. Die Daten werden dedupliziert, während sie in einen Containerspeicherpool geschrieben werden. Siehe auch Datendeduplizierung, Nachgeordnete Datendeduplizierung.

Inline-Komprimierung
: Eine Methode zum Reduzieren des Speicherbereichs. Sich wiederholende Zeichen, Leerzeichen, Zeichenfolgen oder Binärdaten werden entfernt, während Daten in einen Containerspeicherpool geschrieben werden. Siehe auch Komprimierung.

IP-Adresse
: Eine eindeutige Adresse für eine Einheit oder eine logische Einheit in einem Netz, die den IP-Standard (Internet Protocol) verwendet.

J

Jobdatei
: Eine generierte Datei, die Konfigurationsdaten für einen Umlagerungsjob enthält. Die Datei weist das XML-Format auf und sie kann in der grafischen Benutzerschnittstelle des HSM for Windows-Clients (HSM = Hierarchical Storage Management = Hierarchische Speicherverwaltung) erstellt und editiert werden. Siehe auch Umlagerungsjob.

Journaldämon
: Auf AIX-, UNIX- oder Linux-Systemen ein Programm, das die Änderungsaktivität für Dateien verfolgt, die in Dateisystemen gespeichert sind.

Journalgestützte Sicherung
: Eine Methode zum Sichern von Windows-Clients und AIX-Clients, die den Mechanismus einer Datei für Änderungsbenachrichtigung nutzt. Dadurch wird die Leistung bei der Teilsicherung erhöht, da nicht das gesamte Dateisystem durchsucht werden muss.

Journalservice
: Unter Microsoft Windows ein Programm, das die Änderungsaktivität für Dateien verfolgt, die in Dateisystemen gespeichert sind.

K

Kassettenarchiv

1. Ein Repository für beschriebene Speichermedien, die abgehängt werden können, wie Magnetplatten und Magnetbänder.
2. Eine Sammlung aus einem oder mehreren Laufwerken und eventuell ferngesteuerten Einheiten (je nach dem Typ des Kassettenarchivs), die für den Zugriff auf Speicherdatenträger verwendet werden kann.

Kassettenarchivclient
: Ein Server, der Server-zu-Server-Übertragung verwendet, um auf ein Kassettenarchiv zuzugreifen, das von einem anderen Speicherverwaltungsserver verwaltet wird. Siehe auch Kassettenarchivmanager.

Kassettenarchivmanager
: Ein Server, der Einheitenoperationen steuert, wenn mehrere Speicherverwaltungsserver eine Speichereinheit gemeinsam nutzen. Siehe auch Kassettenarchivclient.

KB
: Siehe Kilobyte.

Kennwortgenerierung
: Ein Prozess, der ein neues Kennwort erstellt und in einer verschlüsselten Kennwortdatei speichert, wenn das alte Kennwort abgelaufen ist. Die automatische Generierung eines Kennworts verhindert die Aufforderung zur Kennworteingabe.

Kilobyte (KB)
: Für den Hauptspeicher, den realen und virtuellen Speicher und die Kanalkapazität 2 hoch 10 oder 1.024 Byte. Für die Plattenspeicher- und Übertragungskapazität 1.000 Byte.

Knoten
: Ein Dateiserver oder eine Workstation, auf dem bzw. der das Clientprogramm für Sichern/Archivieren installiert und beim Server registriert wurde.

Knotenberechtigungsklasse
: Eine Berechtigungsklasse, die einem Administrator die Berechtigung für den Fernzugriff auf Clients für Sichern/Archivieren für einen bestimmten Clientknoten oder für alle Clients in einer Maßnahmendomäne erteilt. Siehe auch Berechtigungsklasse.

Knotenname
: Ein eindeutiger Name, mit dem eine Workstation, ein Dateiserver oder ein PC für den Server identifiziert wird.

Kollokation
: Der Prozess, alle Daten, die zu einem einzelnen Clientdateibereich, einem einzelnen Clientknoten oder einer Gruppe von Clientknoten gehören, auf einer minimalen Anzahl Datenträger mit sequenziellem Zugriff innerhalb eines Speicherpools aufzubewahren. Die Kollokation kann die Anzahl der Datenträger reduzieren, auf die beim Zurückschreiben einer großen Datenmenge zugegriffen werden muss.

Kollokationsgruppe
: Eine benutzerdefinierte Gruppe von Clientknoten, deren Daten über den Kollokationsprozess auf einer minimalen Anzahl von Datenträgern gespeichert werden.

Komprimierung
: Eine Funktion, die sich wiederholende Zeichen, Leerzeichen, Zeichenfolgen oder Binärdaten in den Daten, die verarbeitet werden, entfernt und Zeichen durch Steuerzeichen ersetzt. Durch Komprimierung wird der Speicherbereich reduziert, der für Daten erforderlich ist. Siehe auch Inline-Komprimierung.

Konfigurationsmanager
: Ein Server, der an verwaltete Server Konfigurationsdaten wie Maßnahmen und Zeitpläne entsprechend den Profilen der Server verteilt. Konfigurationsdaten können Maßnahmen und Zeitpläne umfassen. Siehe auch Unternehmenskonfiguration, Verwalteter Server, Profil.

Kopie mit grober Übereinstimmung
: Eine Sicherungsversion oder Archivierungskopie einer Datei, die möglicherweise nicht genau dem Originalinhalt der Datei entspricht, da die Datei während der Sicherung oder Archivierung geändert wurde.

Kopiengruppe
: Ein Maßnahmenobjekt, das Attribute enthält, die Folgendes steuern: wie Sicherungsversionen oder Archivierungskopien generiert werden, an welcher Position Sicherungsversionen oder Archivierungskopien sich ursprünglich befinden und wann Sicherungsversionen oder Archivierungskopien verfallen. Eine Kopiengruppe gehört zu einer Verwaltungsklasse. Siehe auch Archivierungskopiengruppe, Sicherungskopiengruppe, Sicherungsversion, Verwaltungsklasse.

Kopiensicherung
: Eine vollständige Sicherung, bei der die Transaktionsprotokolldateien nicht gelöscht werden, um Auswirkungen auf Sicherungsprozeduren mit Teilsicherungen oder Differenzsicherungen zu vermeiden.

Kopienspeicherpool

Eine benannte Gruppe von Datenträgern, die Kopien von Dateien enthalten, die sich in primären Speicherpools befinden. Kopienspeicherpools werden ausschließlich verwendet, um die Daten zu sichern, die in primären Speicherpools gespeichert sind. Ein Kopienspeicherpool kann kein Zielort für eine Sicherungskopiengruppe, eine Archivierungskopiengruppe oder eine Verwaltungsklasse (für speicherverwaltete Dateien) sein. Siehe auch Ziel, Primärer Speicherpool, Serverspeicher, Speicherpool, Speicherpooldatenträger.

L

Ladedauer
: Die maximale Anzahl Minuten, die ein Server einen angehängten Datenträger mit sequenziellem Zugriff, der nicht verwendet wird, aufbewahrt, bevor der Datenträger mit sequenziellem Zugriff abgehängt wird.

LAN
: Siehe Lokales Netz.

LAN-unabhängige Datenübertragung
: Siehe LAN-unabhängige Datenversetzung.

LAN-unabhängige Datenversetzung
: Die Versetzung von Clientdaten zwischen einem Clientsystem und einer Speichereinheit in einem Speicherbereichsnetz (Storage Area Network - SAN) unter Umgehung des lokalen Netzes.

LOFS
: Siehe Loopback Virtual File System.

Logical Volume Snapshot Agent (LVSA)
: Software, die als Momentaufnahme-Provider fungieren kann, um während einer Online-Imagesicherung eine Momentaufnahme eines logischen Datenträgers zu erstellen.

Logische Belegung
: Der Speicherbereich, der in einem Speicherpool durch logische Dateien belegt ist. Dieser Speicherbereich umfasst nicht den freien Speicherplatz, der entsteht, wenn logische Dateien aus Aggregatdateien gelöscht werden. Daher kann die logische Belegung geringer als die physische Belegung sein. Siehe auch Physische Belegung.

Logische Datei
: Eine Datei, die entweder alleine oder als Teil eines Aggregats in einem oder mehreren Serverspeicherpools gespeichert ist. Siehe auch Aggregat, Physische Datei, Physische Belegung.

Logischer Datenträger
: Ein Teil eines physischen Datenträgers, der ein Dateisystem enthält.

Lokal
: 1. Bezieht sich auf eine Einheit, eine Datei oder ein System, auf das von einem Benutzersystem aus direkt, ohne DFV-Leitung, zugegriffen wird.
  2. Bei Produkten für die hierarchische Speicherverwaltung bezieht sich der Begriff auf das Ziel von umgelagerten Dateien, die versetzt werden. Siehe auch Fern.

Lokaler Spiegeldatenträger
: Daten, die auf Spiegeldatenträgern gespeichert werden, die zu einem Plattenspeichersubsystem gehören.

Lokales Netz (LAN)
: Ein Netz, das mehrere Einheiten in einem begrenzten Gebiet (z. B. in einem einzigen Gebäude oder in mehreren benachbarten Gebäuden) verbindet und das mit einem größeren Netz verbunden werden kann.

Loopback Virtual File System (LOFS)
: Ein Dateisystem, das durch Anhängen eines Verzeichnisses über ein anderes lokales Verzeichnis erstellt wird; auch als "Mount-Over-Mount" bezeichnet. Ein LOFS kann auch mit Hilfe eines automatischen Mountprogramms generiert werden.

LUN
: Siehe Nummer der logischen Einheit.

LVSA
: Siehe Logical Volume Snapshot Agent.

M

Mailboxzurückschreibung
: Eine Funktion, die Microsoft Exchange Server-Daten (aus IBM Data Protection for Microsoft Exchange-Sicherungen) auf der Mailboxebene oder auf der Mailboxelementebene zurückschreibt.

Makrodatei
: Eine Datei, die einen oder mehrere IBM Spectrum Protect-Verwaltungsbefehle enthält und die nur auf einem Verwaltungsclient mit dem Befehl MACRO ausgeführt werden kann. Siehe auch IBM Spectrum Protect-Befehlsscript.

Maßnahmenberechtigungsklasse
: Eine Berechtigungsklasse, die einem Administrator die Berechtigung für folgende Tasks erteilt: Maßnahmenobjekte verwalten, Clientknoten registrieren und Clientoperationen für Clientknoten planen. Die Berechtigung kann auf bestimmte Maßnahmendomänen beschränkt sein. Siehe auch Berechtigungsklasse.

Maßnahmendomäne
: Eine Gruppierung von Maßnahmenbenutzern mit einer oder mit mehreren Maßnahmengruppen, die Daten oder Speicherressourcen für die Benutzer verwalten. Die Benutzer sind Clientknoten, die der Maßnahmendomäne zugeordnet sind. Siehe auch Aktive Maßnahmengruppe, Domäne.

Maßnahmengruppe

Eine Gruppe von Regeln in einer Maßnahmendomäne. Die Regeln geben an, wie Daten oder Speicherressourcen für Clientknoten in der Maßnahmendomäne automatisch verwaltet werden. Regeln können in Verwaltungsklassen enthalten sein. Siehe auch Aktive Maßnahmengruppe, Verwaltungsklasse.

Maximale Übertragungseinheit (MTU)
: Der größte Block, der auf einem bestimmten physischen Medium in einem einzigen Frame gesendet werden kann. Beispielsweise beträgt die maximale Übertragungseinheit für Ethernet 1500 Byte.

MB
: Siehe Megabyte.

Media-Server
: In einer z/OS-Umgebung ein Programm, das Zugriff auf z/OS-Platten- und -Bandeinheitenspeicher für IBM Spectrum Protect-Server bereitstellt, die auf anderen Betriebssystemen als z/OS ausgeführt werden.

Megabyte (MB)
: Für den Hauptspeicher, den realen und virtuellen Speicher und die Kanalkapazität 2 hoch 20 oder 1.048.576 Byte. Für die Plattenspeicher- und Übertragungskapazität 1.000.000 Byte.

Metadaten
: Daten, die die Merkmale von Daten beschreiben; beschreibende Daten.

Modus
: Ein Kopiengruppenattribut, das angibt, ob eine Datei gesichert werden soll, die seit der letzten Sicherung nicht mehr geändert wurde. Siehe auch Absoluter Modus, Geänderter Modus.

Momentaufnahme
: Ein Imagesicherungstyp, der aus einer zeitpunktgesteuerten Sicht eines Datenträgers besteht.

Mountpunkt
: Ein logisches Laufwerk, über das auf Datenträger in einer Einheitenklasse für den sequenziellen Zugriff zugegriffen wird. Für Einheitentypen für austauschbare Datenträger wie z. B. ein Band ist der Mountpunkt ein logisches Laufwerk, das einem physischen Laufwerk zugeordnet ist. Für den Einheitentyp FILE ist ein Mountpunkt ein logisches Laufwerk, das einem Ein-/Ausgabedatenstrom zugeordnet ist. Siehe auch Grenzwert für Ladeanforderung.

MTU
: Siehe Maximale Übertragungseinheit.

N

Nachgeordnete Datendeduplizierung
: Eine Methode zum Reduzieren des Speicherbedarfs, indem redundante Daten entfernt werden. Die Daten werden zuerst in den Speicherpool geschrieben, die doppelten Daten werden identifiziert und dann wird der Speicherbereich im Speicherpool konsolidiert. Siehe auch Datendeduplizierung, Inline-Datendeduplizierung.

Nagle-Algorithmus
: Ein Algorithmus, der Engpässe in TCP/IP-Netzen reduziert, indem er kleinere Pakete zusammenfasst und gemeinsam sendet.

NAS-Dateiserver
: Siehe Network Attached Storage-Dateiserver.

NAS-Dateiserverknoten
: Siehe NAS-Knoten.

NAS-Knoten
: Ein Clientknoten, der ein NAS-Dateiserver ist. Die Daten für den NAS-Knoten werden von einem NAS-Dateiserver übertragen, der vom Protokoll NDMP (Network Data Management Protocol) gesteuert wird. Ein NAS-Knoten wird auch als NAS-Dateiserverknoten bezeichnet.

Natives Dateisystem
: Ein Dateisystem, das dem Dateiserver lokal und nicht für die Speicherverwaltung hinzugefügt wird. Der HSM-Client (Hierarchical Storage Manager - hierarchische Speicherverwaltung) stellt keine Speicherverwaltungsservices für das Dateisystem bereit.

Natives Format
: Ein Datenformat, das vom Server direkt in einen Speicherpool geschrieben wird. Siehe auch Nicht natives Datenformat.

NDMP
: Siehe Network Data Management Protocol.

NetBIOS (Network Basic Input/Output System)
: Eine Standardschnittstelle für Netze und Personal Computer, die in lokalen Netzen verwendet wird, um Funktionen für Nachrichten, Druckserver und Dateiserver bereitzustellen. Anwendungsprogramme, die NetBIOS verwenden, müssen sich nicht mit den Details von Protokollen für die LAN-Datenübertragungssteuerung (Data Link Control - DLC) beschäftigen.

Network Attached Storage-Dateiserver (NAS-Dateiserver)
: Eine dedizierte Speichereinheit mit einem Betriebssystem, das für Dateiserverfunktionen optimiert ist. Ein NAS-Dateiserver kann sowohl die Merkmale eines Knotens als auch die Merkmale einer Einheit zum Versetzen von Daten aufweisen.

Network Basic Input/Output System
: Siehe NetBIOS.

Network Data Management Protocol (NDMP)
: Ein Protokoll, mit dem eine Netzspeicherverwaltungsanwendung die Sicherung und Wiederherstellung eines NDMP-kompatiblen Dateiservers steuern kann, ohne dass eine spezielle Software auf diesem Dateiserver installiert werden muss.

Nicht natives Datenformat
: Ein in den Speicherpool geschriebenes Datenformat, das sich von dem Format unterscheidet, das der Server für Operationen verwendet. Siehe auch Natives Format.

Nummer der logischen Einheit (Logical Unit Number - LUN)

Im SCSI-Standard (Small Computer System Interface) eine eindeutige Kennung, die für die Unterscheidung von Einheiten verwendet wird. Jede dieser Einheiten ist eine logische Einheit (Logical Unit - LU).

O

Offene Registrierung
: Ein Registrierungsprozess, bei dem Benutzer ihre Workstations als Clientknoten beim Server registrieren können. Siehe auch Geschlossene Registrierung.

Offlinedatenträgersicherung
: Eine Sicherung, bei der der Datenträger gesperrt ist, so dass andere Systemanwendungen während der Sicherungsoperation nicht auf ihn zugreifen können.

Onlinedatenträgersicherung
: Eine Sicherung, bei der der Datenträger während der Sicherungsoperation für andere Systemanwendungen verfügbar ist.

Optionsdatei
: Eine Datei, die Verarbeitungsoptionen enthält. Siehe auch Clientsystemoptionsdatei, Clientbenutzeroptionsdatei.

P

Paket
: Bei der Datenübertragung eine Folge von Binärziffern einschließlich Daten und Steuersignalen, die als Einheit übertragen und weitergeleitet werden.

Partieller Dateirückruf (Rückrufmodus)
: Ein Rückrufmodus, bei dem die Funktion für hierarchische Speicherverwaltung (HSM-Funktion) nur denjenigen Teil einer umgelagerten Datei aus dem Speicher liest, den die auf die Datei zugreifende Anwendung anfordert.

Pfad
: Ein Objekt, das eine Eins-zu-eins-Beziehung zwischen einer Quelle und einem Ziel definiert. Die Quelle greift unter Verwendung des Pfads auf das Ziel zu. Daten können von der Quelle zum Ziel und zurück fließen. Ein Beispiel für eine Quelle ist eine Einheit zum Versetzen von Daten (wie ein NAS-Dateiserver) und ein Beispiel für ein Ziel ist ein Bandlaufwerk.

Physische Belegung
: Der Speicherbereich, der in einem Speicherpool durch physische Dateien belegt ist. Dieser Speicherbereich umfasst den freien Speicherplatz, der entsteht, wenn logische Dateien aus Aggregaten gelöscht werden. Siehe auch Logische Datei, Logische Belegung, Physische Datei.

Physische Datei
: Eine Datei, die in einem oder mehreren Speicherpools gespeichert ist und entweder aus einer einzigen logischen Datei oder aus einer Gruppe von logischen Dateien besteht, die in einem Aggregat zusammengefasst sind. Siehe auch Aggregat, Logische Datei, Physische Belegung.

Planungsmodus
: Der Typ der Planungsoperation für Server und Clientknoten. Zwei Planungsmodi werden unterstützt: Clientsendeaufruf und Serversystemanfrage.

Platzhalterzeichen
: Ein Sonderzeichen wie ein Stern (*) oder ein Fragezeichen (?), das verwendet werden kann, um ein oder mehrere Zeichen darzustellen. Das Platzhalterzeichen kann durch ein beliebiges Zeichen oder eine Gruppe von beliebigen Zeichen ersetzt werden.

Plug-in
: Ein separat installierbares Softwaremodul, das einem vorhandenen Programm, einer Anwendung oder einer Schnittstelle Funktionen hinzufügt.

Pool für aktive Daten
: Eine benannte Gruppe von Speicherpooldatenträgern, die nur aktive Versionen von Clientsicherungsdaten enthält. Siehe auch Serverspeicher, Speicherpool, Speicherpooldatenträger.

Präfix für Banddatenträger
: Das übergeordnete Qualifikationsmerkmal des Namens der Datei oder des Datensatzes im Standardbandkennsatz.

Primärer Speicherpool
: Eine benannte Gruppe von Datenträgern oder Containern, die der Server verwendet, um Sicherungsversionen und Archivierungskopien von Dateien sowie von Clientknoten umgelagerte Dateien zu speichern. Siehe auch Kopienspeicherpool, Serverspeicher, Speicherpool, Speicherpooldatenträger.

Primärer Standort
: Ein physischer oder virtueller Standort, der aus Hardware-, Netz- und Speicherressourcen besteht. Normalerweise werden Produktionsoperationen am primären Standort ausgeführt. Daten können für die Wiederherstellung nach einem Katastrophenfall und Übernahmeoperationen auf einen sekundären Standort repliziert werden. Siehe auch Sekundärer Standort.

Profil
: Eine benannte Gruppe aus Konfigurationsdaten, die von einem Konfigurationsmanager verteilt werden kann, wenn ein verwalteter Server eine Subskription vornimmt. Die Konfigurationsdaten können registrierte Administrator-IDs, Maßnahmen, Clientzeitpläne, Clientoptionsgruppen, Verwaltungszeitpläne, Befehlsprozeduren des Speichermanagers, Serverdefinitionen und Servergruppendefinitionen umfassen. Siehe auch Konfigurationsmanager, Unternehmenskonfiguration, Verwalteter Server.

Profilzuordnung
: Auf einem Konfigurationsmanager die definierte Beziehung zwischen einem Profil und einem Objekt wie einer Maßnahmendomäne. Profilzuordnungen definieren die Konfigurationsdaten, die einem verwalteten Server zugeteilt werden, wenn er das Profil subskribiert.

Prüfen

Die Maßnahmengruppe auf Bedingungen hin prüfen, die unter Umständen Probleme verursachen könnten, wenn die betreffende Maßnahmengruppe zur aktiven Maßnahmengruppe gemacht würde. Bei der Prüfung wird beispielsweise geprüft, ob die Maßnahmengruppe eine Standardverwaltungsklasse enthält.

Prüfung
: Die Suche nach logischen Inkonsistenzen zwischen Informationen auf dem Server und den tatsächlich auf dem System vorliegenden Gegebenheiten. Der Speichermanager kann Informationen zu Elementen wie Datenträgern, Kassettenarchiven und Lizenzen prüfen. Wenn ein Speichermanager beispielsweise einen Datenträger prüft, stellt der Server Inkonsistenzen zwischen den in der Datenbank gespeicherten Informationen zu gesicherten oder archivierten Dateien und den tatsächlichen Daten fest, die jeder Sicherungsversion oder Archivierungskopie im Serverspeicher zugeordnet sind.

Q

Quote

1. Für HSM auf AIX-, UNIX- oder Linux-Systemen der Grenzwert (in Megabyte) für das Datenvolumen, das von einem Dateisystem in den Serverspeicher umgelagert oder vorumgelagert werden kann.
2. Für HSM auf Windows-Systemen ein benutzerdefinierter Grenzwert für den Speicherbereich, der von zurückgerufenen Dateien belegt wird.

R

Registrieren
: Einen Clientknoten oder eine Administrator-ID definieren, der bzw. die auf den Server zugreifen kann.

Registry
: Ein Repository, das Zugriffs- und Konfigurationsdaten für Benutzer, Systeme und Software enthält.

Residente Datei
: Auf einem Windows-System eine vollständige Datei in einem lokalen Dateisystem, bei der es sich auch um eine umgelagerte Datei handeln könnte, da eine umgelagerte Kopie im Serverspeicher vorhanden sein kann. Auf einem UNIX- oder Linux-System eine vollständige Datei in einem lokalen Dateisystem, die nicht umgelagert oder vorumgelagert wurde oder die aus dem Serverspeicher zurückgerufen und geändert wurde.

Ressourcennutzung in Sitzung
: Die Wartezeit, die Prozessorzeit und der Speicherbereich, die während einer Clientsitzung verwendet oder abgerufen werden.

Root
: Ein Systembenutzer, dessen Berechtigungen keinen Einschränkungen unterliegen. Ein Root verfügt über besondere Rechte und Berechtigungen, die für die Ausführung von Verwaltungstasks erforderlich sind.

Rückruf
: Das Zurückkopieren einer umgelagerten Datei aus dem Serverspeicher in das ursprüngliche Dateisystem mit Hilfe des Clients für hierarchische Speicherverwaltung. Siehe auch Selektiver Rückruf.

S

SAN
: Siehe Speicherbereichsnetz.

Schwellenumlagerung
: Der Prozess, bei dem Dateien aus einem lokalen Dateisystem in den Serverspeicher versetzt werden, basierend auf den Werten für die obere und untere Schwelle, die für das Dateisystem definiert wurden. Siehe auch Automatische Umlagerung, Bedarfsumlagerung, Umlagerungsjob, Selektive Umlagerung.

Script
: Eine Serie von Befehlen, die in einer Datei enthalten sind und die eine bestimmte Funktion ausführen, wenn die Datei ausgeführt wird. Scripts werden bei ihrer Ausführung interpretiert. Siehe auch IBM Spectrum Protect-Befehlsscript.

Secure Sockets Layer (SSL)
: Ein Sicherheitsprotokoll, das Daten bei der Übertragung schützt. Mit SSL können Client/Server-Anwendungen miteinander kommunizieren, ohne dass die Daten ausspioniert oder manipuliert und Nachrichten gefälscht werden können.

Seite
: Eine definierte Einheit des Speicherbereichs in einem Speichermedium oder innerhalb eines Datenbankdatenträgers.

Sekundärer Standort
: Ein physischer oder virtueller Standort, der aus den Hardware-, Netz- und Speicherressourcen besteht, die die Wiederherstellungsanforderungen des primären Standorts unterstützen. Wenn ein Fehler an dem primären Standort auftritt, können Operationen am sekundären Standort fortgesetzt werden. Siehe auch Primärer Standort.

Selektiver Rückruf
: Der Prozess, bei dem vom Benutzer ausgewählte Dateien aus dem Serverspeicher in ein lokales Dateisystem kopiert werden. Siehe auch Rückruf, Transparenter Rückruf.

Selektive Sicherung
: Der Prozess der Sicherung bestimmter Dateien oder Verzeichnisse in einer Clientdomäne. Gesichert werden dabei die Dateien, die in der Einschluss-/Ausschlussliste nicht ausgeschlossen sind. Die Dateien müssen den Anforderungen bezüglich der Durchnummerierung in der Sicherungskopiengruppe der Verwaltungsklasse entsprechen, die jeder Datei zugeordnet ist. Siehe auch Teilsicherung.

Selektive Umlagerung

Der Prozess, bei dem vom Benutzer ausgewählte Dateien aus einem lokalen Dateisystem in den Serverspeicher kopiert und die Dateien in dem lokalen Dateisystem durch Stubdateien ersetzt werden. Siehe auch Bedarfsumlagerung, Schwellenumlagerung.

Server
: Ein Softwareprogramm oder ein Computer, das bzw. der Services für andere Softwareprogramme oder Computer zur Verfügung stellt. Siehe auch Client.

Serveroptionsdatei
: Eine Datei mit Einstellungen, die verschiedene Serveroperationen steuern. Diese Einstellungen betreffen Aspekte wie Datenübertragung, Einheiten und Leistung.

Serverspeicher
: Die primären Speicherpools, Kopienspeicherpools und Speicherpools für aktive Daten, die der Server verwendet, um Benutzerdateien wie Sicherungsversionen, Archivierungskopien und von Clientknoten für hierarchische Speicherverwaltung umgelagerte Dateien (speicherverwaltete Dateien) zu speichern. Siehe auch Pool für aktive Daten, Containerspeicherpool, Kopienspeicherpool, Primärer Speicherpool, Speicherpooldatenträger, Datenträger.

Sicherung logischer Datenträger
: Die Sicherung eines Dateisystems oder logischen Datenträgers als einzelnes Objekt.

Sicherung mit grober Übereinstimmung
: Eine Sicherungsversion einer Datei, die möglicherweise nicht genau dem Stand der aktuellen Datei entspricht, da die Datei während der Sicherung geändert wurde.

Sicherungsgruppe
: Eine übertragbare, konsolidierte Gruppe von aktiven Versionen von Sicherungsdateien, die für einen Client für Sichern/Archivieren generiert werden.

Sicherungsgruppensammlung
: Eine Gruppe von Sicherungsgruppen, die zu demselben Zeitpunkt generiert werden und die über dieselben Sicherungsgruppennamen, Datenträgernamen, Beschreibungen und Einheitenklassen verfügen. Der Server identifiziert jede Sicherungsgruppe in der Sammlung über seinen Knotennamen, Sicherungsgruppennamen und Dateityp.

Sicherungskopiengruppe
: Ein Maßnahmenobjekt mit Attributen, die die Generierung, den Zielort und den Verfallstermin von Sicherungsversionen von Dateien steuern. Eine Sicherungskopiengruppe gehört zu einer Verwaltungsklasse. Siehe auch Kopiengruppe.

Sicherungsversion
: Eine Datei oder ein Verzeichnis, die bzw. das ein Clientknoten im Speicher gesichert hat. Es können mehrere Sicherungsversionen im Speicher vorhanden sein, aber nur eine Sicherungsversion ist die aktive Version. Siehe auch Aktive Version, Kopiengruppe, Inaktive Version.

Sitzung
: Eine logische oder virtuelle Verbindung zwischen zwei Stationen, Softwareprogrammen oder Einheiten in einem Netz, über die die beiden Elemente für die Dauer der Sitzung miteinander kommunizieren und Daten austauschen können. Siehe auch Verwaltungssitzung.

Speicheragent
: Ein Programm, das die direkte Sicherung von Clientdaten in Speichereinheiten und die direkte Wiederherstellung von Clientdaten aus Speichereinheiten ermöglicht, die mit einem Speicherbereichsnetz (SAN - Storage Area Network) verbunden sind.

Speicherberechtigungsklasse
: Eine Berechtigungsklasse, die einem Administrator die Berechtigung erteilt, die Zuordnung und Verwendung der Speicherressourcen für den Server zu steuern. Siehe auch Berechtigungsklasse.

Speicherbereich
: Der Teil einer Datei, der während des Datendeduplizierungsprozesses erstellt wird. Speicherbereiche werden mit anderen Dateibereichen verglichen, um doppelte Daten zu identifizieren.

Speicherbereichsnetz (SAN)
: Ein dediziertes Speichernetz, das an eine bestimmte Umgebung angepasst ist und das Server, Systeme, Speicherprodukte, Netzprodukte, Software und Services kombiniert.

Speicherhierarchie
: Eine logische Reihenfolge von primären Speicherpools, die von einem Administrator definiert wurde. Die Reihenfolge basiert normalerweise auf der Geschwindigkeit und der Kapazität der Einheiten, die die Speicherpools verwenden. Die Speicherhierarchie wird durch Angabe des nächsten Speicherpools in einer Speicherpooldefinition definiert. Siehe auch Speicherpool.

Speichermonitordämon
: Ein Dämon, der die Speicherbereichsbelegung in allen Dateisystemen überprüft, für die die Speicherverwaltung aktiv ist, und der die Schwellenumlagerung automatisch startet, wenn die Speicherbereichsbelegung in einem Dateisystem die obere Schwelle erreicht oder überschreitet.

Speicherpool
: Eine Gruppe von Speicherdatenträgern oder Containern, die der Zielort für das Speichern von Clientdaten sind. Siehe auch Pool für aktive Daten, Cloud-Containerspeicherpool, Kopienspeicherpool, Verzeichniscontainerspeicherpool, Primärer Speicherpool, Speicherhierarchie.

Speicherpooldatenträger
: Ein Datenträger, der einem Speicherpool zugeordnet wurde. Siehe auch Pool für aktive Daten, Kopienspeicherpool, Primärer Speicherpool, Serverspeicher, Datenträger.

Speicherverwaltete Datei
: Eine Datei, die der HSM-Client (HSM = Hierarchical Storage Management = Hierarchische Speicherverwaltung) von einem Clientknoten umlagert. Der HSM-Client ruft die Datei bei Bedarf in den Clientknoten zurück.

Speicherverwaltung
: Siehe Hierarchische Speicherverwaltung.

Spezielle Datei

Auf AIX-, UNIX- oder Linux-Systemen eine Datei, die Einheiten für das System definiert, oder temporäre Dateien, die von Prozessen erstellt werden. Man unterscheidet drei Grundtypen von speziellen Dateien: First In/First Out (FIFO), Block und Zeichen.

Spiegeldatenträger
: Die Daten, die aus einer Momentaufnahme eines Datenträgers gespeichert wurden. Die Momentaufnahme kann erstellt werden, während Anwendungen auf dem System weiterhin Daten auf die Datenträger schreiben.

Spiegelkopie
: Eine Momentaufnahme eines Datenträgers. Die Momentaufnahme kann erstellt werden, während Anwendungen auf dem System weiterhin Daten auf die Datenträger schreiben.

Spiegeln
: Der Prozess, bei dem dieselben Daten gleichzeitig auf mehrere Platten geschrieben werden. Die Spiegelung von Daten bietet Schutz vor Datenverlust in der Datenbank oder im Wiederherstellungsprotokoll.

SSL
: Siehe Secure Sockets Layer.

Stabilisierter Dateibereich
: Ein Dateibereich, der auf dem Server, jedoch nicht auf dem Client vorhanden ist.

Standardverwaltungsklasse
: Eine Verwaltungsklasse, die einer Maßnahmengruppe zugeordnet ist. Diese Klasse wird zum Verwalten von gesicherten oder archivierten Dateien verwendet, wenn eine Datei nicht explizit über die Einschluss-/Ausschlussliste einer bestimmten Verwaltungsklasse zugeordnet ist.

Startfenster
: Eine Zeitspanne, während der ein Zeitplan eingeleitet werden muss.

Statisch (Durchnummerierung)
: Ein Durchnummerierungswert für die Kopiengruppe, der angibt, dass eine Datei während einer Sicherungs- oder Archivierungsoperation nicht geändert werden darf. Ist die Datei beim ersten Versuch im Gebrauch, kann der Client für Sichern/Archivieren die Datei nicht sichern oder archivieren. Siehe auch Dynamisch (Durchnummerierung), Durchnummerierung, Gemeinsam dynamisch (Durchnummerierung), Gemeinsam statisch (Durchnummerierung).

Stub
: Eine Verknüpfung im Windows-Dateisystem, die vom HSM-Client (HSM = Hierarchical Storage Management = Hierarchische Speicherverwaltung) für eine umgelagerte Datei generiert wird. Diese Verknüpfung ermöglicht den transparenten Benutzerzugriff. Ein Stub ist die Darstellung einer umgelagerten Datei als Datei mit freien Bereichen, der ein Analysepunkt zugeordnet ist.

Stubdatei
: Eine Datei, die die Originaldatei in einem lokalen Dateisystem ersetzt, wenn die Datei in den Speicher umgelagert wird. Eine Stubdatei enthält die Informationen, die erforderlich sind, um eine umgelagerte Datei aus dem Serverspeicher zurückzurufen. Sie enthält darüber hinaus weitere Informationen, die möglicherweise verwendet werden können, anstatt die umgelagerte Datei zurückzurufen. Siehe auch Umgelagerte Datei, Residente Datei.

Stubdatei ohne Verbindung
: Eine Datei, für die keine umgelagerte Datei auf dem Server gefunden wird, von dem der Clientknoten Speicherverwaltungsservices anfordert. Eine Stubdatei kann beispielsweise zu einer Stubdatei ohne Verbindung werden, wenn die Optionsdatei des Clientsystems so geändert wird, dass ein anderer Server kontaktiert wird als der Server, auf den die Datei umgelagert wurde.

Subskription
: In einer Speicherumgebung der Prozess der Identifizierung der Subskribenten, an die die Profile verteilt werden. Siehe auch Unternehmenskonfiguration, Verwalteter Server.

Systemberechtigungsklasse
: Eine Berechtigungsklasse, die einem Administrator die Berechtigung für das Ausgeben aller Serverbefehle erteilt. Siehe auch Berechtigungsklasse.

T

TCA
: Siehe Trusted Communications Agent.

TCP/IP
: Siehe Transmission Control Protocol/Internet Protocol.

Teilsicherung
: Der Prozess, bei dem Dateien oder Verzeichnisse gesichert oder Seiten in die Datenbank kopiert werden, die seit der letzten Gesamt- oder Teilsicherung hinzugefügt oder geändert wurden. Siehe auch Selektive Sicherung.

Tombstoneobjekt
: Eine kleine Untergruppe von Attributen eines gelöschten Objekts. Das Tombstoneobjekt wird für einen angegebenen Zeitraum aufbewahrt und am Ende des angegebenen Zeitraums permanent gelöscht.

Transmission Control Protocol/Internet Protocol (TCP/IP)
: Eine standardisierte, nicht proprietäre Gruppe von Übertragungsprotokollen, die zuverlässige End-to-End-Verbindungen zwischen Anwendungen über miteinander verbundene Netze verschiedenen Typs zur Verfügung stellt. Siehe auch Übertragungsmethode.

Transparenter Rückruf
: Der Prozess, mit dem eine umgelagerte Datei automatisch auf eine Workstation oder einen Dateiserver zurückgerufen wird, wenn auf die Datei zugegriffen wird. Siehe auch Selektiver Rückruf.

Trusted Communications Agent (TCA)
: Ein Programm, das das Anmeldekennwortprotokoll bearbeitet, wenn Clients die Kennwortgenerierung verwenden.

U

Übertragungsmethode
: Die Methode, mit der ein Client und Server Daten austauschen. Siehe auch Transmission Control Protocol/Internet Protocol.

Übertragungsprotokoll
: Eine Gruppe definierter Schnittstellen, über die Computer miteinander kommunizieren können.

UCS-2
: Ein Schema für Codeumsetzung in 2 Byte (16 Bit), das auf der ISO/IEC-Spezifikation 10646-1 basiert. UCS-2 definiert drei Implementierungsebenen: Ebene 1 - Kombination codierter Elemente ist nicht zulässig; Ebene 2 - Kombination codierter Elemente ist nur für die Sprachen Thailändisch, Indoarisch, Hebräisch und Arabisch zulässig; Ebene 3 - Jede Kombination codierter Elemente ist zulässig.

Umgelagerte Datei
: Eine Datei, die aus einem lokalen Dateisystem in den Speicher kopiert wurde. Für HSM-Clients auf UNIX- oder Linux-Systemen wird die Datei durch eine Stubdatei im lokalen Dateisystem ersetzt. Unter Windows ist die Erstellung einer Stubdatei optional. Siehe auch Dateistatus, Vorumgelagerte Datei, Residente Datei, Stubdatei.

Umlagern
: Daten an eine andere Position oder eine Anwendung auf ein anderes Computersystem versetzen.

Umlagerung
: Der Prozess, bei dem Daten von einem Computersystem auf ein anderes Computersystem versetzt werden oder eine Anwendung auf ein anderes Computersystem versetzt wird.

Umlagerungsjob
: Eine Spezifikation der umzulagernden Dateien und der Aktionen, die nach der Umlagerung mit den Originaldateien auszuführen sind. Siehe auch Jobdatei, Schwellenumlagerung.

Umlagerungsschwelle
: Ein hoher und ein niedriger Wert für die Kapazität von Speicherpools oder Dateisystemen, ausgedrückt in Prozentsätzen. Diese Werte legen fest, wann die Umlagerung gestartet und gestoppt wird.

UNC
: Siehe Universal Naming Convention.

Unformatierter logischer Datenträger
: Ein Bereich eines physischen Datenträgers, der aus nicht zugeordneten Blöcken besteht und nicht über eine JFS-Definition (Journaled File System) verfügt. Nur Ein-/Ausgabefunktionen der unteren Ebene haben Lese-/Schreibzugriff auf einen logischen Datenträger.

Unicode
: Ein Standard für die Zeichencodierung, der den Austausch, die Verarbeitung und die Anzeige von Texten in allen Sprachen der Welt sowie von vielen klassischen und historischen Texten ermöglicht.

Unicode-aktivierter Dateibereich
: Ein Dateibereich mit einem Namen, der dem Unicode-Standard entspricht und mit jeder Ländereinstellung auf mehrsprachigen Workstations kompatibel ist.

Universally Unique Identifier (UUID)
: Die aus 128 Bit bestehende numerische Kennung, mit der sichergestellt wird, dass zwei Komponenten nicht über dieselbe Kennung verfügen. Siehe auch Global eindeutige ID.

Universal Naming Convention (UNC)
: Die Kombination aus Servername und Netzname. Diese Namen geben zusammen die Ressource in der Domäne an.

Unternehmenskonfiguration
: Eine Methode der Servereinrichtung, mit der Administratoren die Konfiguration eines der Server mit Hilfe der Server-zu-Server-Übertragung an die anderen Server verteilen kann. Siehe auch Konfigurationsmanager, Verwalteter Server, Profil, Subskription.

Unternehmensprotokollierung
: Der Prozess des Sendens von Ereignissen von einem Server an einen angegebenen Ereignisserver. Der Ereignisserver leitet die Ereignisse an angegebene Empfänger, z. B. an einen Benutzerexit, weiter. Siehe auch Ereignis.

Ursprüngliches Dateisystem
: Das Dateisystem, aus dem eine Datei umgelagert wurde. Wird eine Datei zurückgerufen, wird sie an das ursprüngliche Dateisystem zurückgegeben.

UTF-8
: Unicode Transformation Format, ein 8-Bit-Codierungsformat, das sich für die Verwendung mit vorhandenen ASCII-basierten Systemen eignet. Der CCSID-Wert für Daten im UTF-8-Format lautet 1208.

UUID
: Siehe Universally Unique Identifier.

V

Verfall
: Der Prozess, durch den Dateien, Datensätze oder Objekte für die Löschung gekennzeichnet werden, da ihr Verfallsdatum oder ihr Aufbewahrungszeitraum überschritten wurde.

Verfallende Datei
: Eine umgelagerte oder vorumgelagerte Datei, die für den Verfall und die Entfernung aus dem Speicher markiert wurde. Wird eine Stubdatei oder eine Originalkopie einer vorumgelagerten Datei aus einem lokalen Dateisystem gelöscht oder wird die Originalkopie einer vorumgelagerten Datei aktualisiert, wird die entsprechende umgelagerte oder vorumgelagerte Datei bei Ausführung der nächsten Abstimmung als verfallen markiert.

Version
: Eine Sicherungskopie einer Datei, die im Serverspeicher gespeichert ist. Die letzte Sicherungskopie einer Datei ist die aktive Version. Frühere Kopien derselben Datei sind inaktive Versionen. Die Anzahl der vom Server aufbewahrten Versionen wird durch die Kopiengruppenattribute in der Verwaltungsklasse bestimmt.

Verwalteter Server
: Ein Server, der über eine Subskription für ein oder mehrere Profile Konfigurationsdaten von einem Konfigurationsmanager empfängt. Konfigurationsdaten können Definitionen von Objekten wie Maßnahmen und Zeitpläne umfassen. Siehe auch Konfigurationsmanager, Unternehmenskonfiguration, Profil, Subskription.

Verwaltetes Objekt
: Eine Definition in der Datenbank eines verwalteten Servers, die dem verwalteten Server von einem Konfigurationsmanager zugeteilt wurde. Wenn ein verwalteter Server ein Profil subskribiert, werden alle diesem Profil zugeordneten Objekte zu verwalteten Objekten in der Datenbank des verwalteten Servers.

Verwaltungsberechtigungsklasse
: Siehe Berechtigungsklasse.

Verwaltungsclient
: Ein Programm, das auf einem Dateiserver, einer Workstation oder einem Großrechner ausgeführt wird und von Administratoren für die Steuerung und Überwachung des Servers verwendet wird. Siehe auch Client für Sichern/Archivieren.

Verwaltungsklasse
: Ein Maßnahmenobjekt, das Benutzer an jede Datei binden können, um anzugeben, wie der Server die Datei verwaltet. Die Verwaltungsklasse kann eine Sicherungskopiengruppe, eine Archivierungskopiengruppe und Speicherverwaltungsattribute enthalten. Siehe auch Binden, Kopiengruppe, Client für hierarchische Speicherverwaltung, Maßnahmengruppe, Erneut binden.

Verwaltungssitzung
: Ein Zeitraum, während dessen eine Administrator-ID mit einem Server kommuniziert, um Verwaltungstasks auszuführen. Siehe auch Clientknotensitzung, Sitzung.

Verwendung von Platzhalterzeichen
: Siehe Platzhalterzeichen.

Verzeichniscontainerspeicherpool
: Ein Speicherpool, der von einem Server verwendet wird, um Daten in Containern in Speicherpoolverzeichnissen zu speichern. Daten, die in einem Verzeichniscontainerspeicherpool gespeichert werden, können entweder die Inline-Datendeduplizierung oder die clientseitige Datendeduplizierung verwenden. Siehe auch Cloud-Containerspeicherpool, Containerspeicherpool, Containerkopienspeicherpool, Speicherpool.

Virtueller Dateibereich
: Eine Darstellung eines Verzeichnisses in einem NAS-Dateisystem (NAS = Network-Attached Storage) als Pfad zu diesem Verzeichnis.

Virtueller Datenträger
: Eine Archivierungsdatei auf einem Zielserver, die einen Datenträger mit sequenziellem Zugriff für einen Quellenserver repräsentiert.

Virtueller Mountpunkt
: Eine Verzeichnisverzweigung eines Dateisystems, das als virtuelles Dateisystem definiert ist. Das virtuelle Dateisystem wird in seinem eigenen Dateibereich auf dem Server gesichert. Der Server verarbeitet den virtuellen Mountpunkt als separates Dateisystem, das Clientbetriebssystem jedoch nicht.

Volume Shadow Copy Service (VSS)
: Eine Gruppe von Microsoft-Anwendungsprogrammierschnittstellen (APIs - Application-Programming Interfaces), mit denen Spiegelkopiesicherungen von Datenträgern, exakte Kopien von Dateien einschließlich aller offenen Dateien usw. erstellt werden.

Vorspanndaten
: Datenbytes ab dem Anfang einer umgelagerten Datei, die in der Stubdatei für diese Datei im lokalen Dateisystem gespeichert werden. Der Umfang der Vorspanndaten, die in einer Stubdatei gespeichert werden, ist von der angegebenen Stubgröße abhängig.

Vorumgelagerte Datei
: Eine Datei, die in den Serverspeicher kopiert, jedoch in dem lokalen Dateisystem nicht durch eine Stubdatei ersetzt wurde. Im lokalen Dateisystem und im Serverspeicher sind identische Kopien der Datei vorhanden. Vorumgelagerte Dateien sind in UNIX- und Linux-Dateisystemen vorhanden, denen die Speicherverwaltung hinzugefügt wurde. Siehe auch Dateistatus, Umgelagerte Datei, Residente Datei.

Vorumlagerung
: Der Prozess, bei dem Dateien, die für die Umlagerung auswählbar sind, in den Serverspeicher kopiert werden, wobei jedoch die ursprünglichen Dateien in dem lokalen Dateisystem intakt bleiben.

Vorumlagerungsprozentsatz
: Eine Speicherverwaltungseinstellung, die festlegt, ob die nächsten auswählbaren Kandidaten in einem Dateisystem nach der Schwellen- oder Bedarfsumlagerung vorumgelagert werden.

VSS
: Siehe Volume Shadow Copy Service.

VSS-Schnellzurückschreibung
: Eine Operation, bei der Daten aus einer lokalen Momentaufnahme zurückgeschrieben werden. Die Momentaufnahme ist die VSS-Sicherung, die sich auf einem lokalen Spiegeldatenträger befindet. Die Zurückschreibungsoperation ruft die Daten mithilfe einer Kopiermethode auf Dateiebene ab.

VSS-Sicherung
: Eine Sicherungsoperation, bei der die Microsoft-VSS-Technologie (Volume Shadow Copy Service) verwendet wird. Bei der Sicherungsoperation wird eine Onlinemomentaufnahme (eine konsistente zeitpunktgesteuerte Kopie) erstellt. Diese Kopie kann auf lokalen Spiegeldatenträgern oder im Serverspeicher gespeichert werden.

VSS-Sofortzurückschreibung
: Eine Operation, bei der Daten aus einer lokalen Momentaufnahme zurückgeschrieben werden. Die Momentaufnahme ist die VSS-Sicherung, die sich auf einem lokalen Spiegeldatenträger befindet. Die Zurückschreibungsoperation ruft die Daten mithilfe einer hardwareunterstützten Zurückschreibungsmethode ab (z. B. eine FlashCopy-Operation).

VSS-Zurückschreibung
: Eine Funktion, die einen Microsoft-VSS-Softwareprovider (VSS - Volume Shadow Copy Service) verwendet, um Momentaufnahmen zurückzuschreiben, die sich im Serverspeicher befinden. Die Momentaufnahmen wurden durch eine VSS-Sicherung erstellt und werden an

ihre ursprüngliche Position zurückgeschrieben.

W

Weltweiter Name (WWN)
: Eine nicht signierte 64-Bit-Namenskennung, die eindeutig ist.

Wiederherstellung
: Der Prozess der Konsolidierung der verbleibenden Daten von vielen Datenträgern mit sequenziellem Zugriff auf einer geringeren Anzahl neuer Datenträger mit sequenziellem Zugriff.

Wiederherstellungsplan
: Eine Datei, die vom Disaster Recovery Manager (DRM) erstellt wird. Sie enthält Informationen zur Wiederherstellung von Computersystemen für den Katastrophenfall sowie Scripts, mit denen einige Wiederherstellungstasks ausgeführt werden können. Die Datei umfasst Informationen zu der vom Server verwendeten Software und Hardware sowie zu dem Standort der Wiederherstellungsdatenträger.

Wiederherstellungsprotokoll
: Ein Protokoll mit Aktualisierungen, die in Kürze in die Datenbank geschrieben werden. Das Protokoll kann verwendet werden, um Daten nach System- und Datenträgerfehlern wiederherzustellen. Das Wiederherstellungsprotokoll besteht aus dem aktiven Protokoll (einschließlich der Protokollspiegelung) und den Archivprotokollen.

Wiederherstellungsschwelle
: Der Prozentsatz des Speicherbereichs, über den ein Datenträger mit sequenziellem Zugriff verfügen muss, damit der Server den Datenträger wiederherstellen kann. Speicherbereich kann wiederhergestellt werden, wenn Dateien verfallen oder gelöscht werden.

Wiederherstellungsstandort
: Siehe Sekundärer Standort.

Workloadpartition (WPAR)
: Eine Partition innerhalb einer einzelnen Betriebssysteminstanz.

Workstation
: Eine Datenstation oder ein Personal Computer, an der bzw. dem ein Benutzer Anwendungen ausführen kann und die bzw. der normalerweise mit einem Großrechner oder einem Netz verbunden ist.

WPAR
: Siehe Workloadpartition.

WWN
: Siehe Weltweiter Name.

Z

Zeilengruppe
: Eine Gruppe von Zeilen in einer Datei, die eine gemeinsame Funktion ausführen oder einen Teil des Systems definieren. Zeilengruppen werden normalerweise durch Leerzeilen oder Doppelpunkte getrennt und jede Zeilengruppe hat einen Namen.

Zeitlimitüberschreitung
: Ein Zeitintervall, das einem Ereignis zugeordnet ist. Tritt das Ereignis innerhalb dieses Zeitintervalls nicht auf oder wird das Ereignis innerhalb dieses Zeitintervalls nicht beendet, wird die Operation unterbrochen.

Zeitplan
: Ein Datenbanksatz, der Clientoperationen oder Verwaltungsbefehle beschreibt, die verarbeitet werden sollen. Siehe auch Zeitplan für Verwaltungsbefehle, Clientzeitplan.

Zeitplan für Verwaltungsbefehle
: Ein Datenbanksatz, der die geplante Verarbeitung eines Verwaltungsbefehls während einer bestimmten Zeitspanne beschreibt. Siehe auch Zentrale Zeitplanung, Clientzeitplan, Zeitplan.

Zeitplanung über Clientsendeaufruf
: Eine Betriebsart, bei der der Client den Server nach Arbeit abfragt. Siehe auch Zeitplanung über Serversystemanfrage.

Zeitplanung über Serversystemanfrage
: Ein Client/Server-Kommunikationsverfahren, bei dem der Server den Clientknoten kontaktiert, wenn Tasks ausgeführt werden müssen. Siehe auch Zeitplanung über Clientsendeaufruf.

Zeitspanne für Mount Wait
: Die maximale Anzahl Minuten, die der Server darauf wartet, dass eine Anforderung zum Anhängen eines Datenträgers mit sequenziellem Zugriff ausgeführt wird, bevor die Anforderung abgebrochen wird.

Zentrale Zeitplanung
: Eine Funktion, die es einem Administrator erlaubt, Clientoperationen und Verwaltungsbefehle zu planen. Die Operationen können so geplant werden, dass sie in regelmäßigen Abständen oder an einem bestimmten Datum ausgeführt werden. Siehe auch Zeitplan für Verwaltungsbefehle, Clientzeitplan.

Ziel
: Kopiengruppen- oder Verwaltungsklassenattribut, das den primären Speicherpool angibt, in dem eine Clientdatei gesichert, archiviert oder umgelagert wird. Siehe auch Kopienspeicherpool.

Zielknoten
: Ein Clientknoten, für den anderen Clientknoten (die Agentenknoten genannt werden) Proxyberechtigung erteilt wurde. Mit der Proxyberechtigung können Agentenknoten Operationen wie Sicherung und Zurückschreibung für den Zielknoten ausführen, der Eigner der Daten ist.

Zufallsverarbeitung

Der Prozess, bei dem Zeitplanstartzeiten für unterschiedliche Clients innerhalb eines angegebenen Prozentsatzes des Startfensters des Zeitplans verteilt werden.

Zugriffsmodus
: Ein Attribut eines Speicherpools oder eines Speicherdatenträgers, das angibt, ob der Server in den Speicherpool oder Speicherdatenträger schreiben oder aus diesen lesen kann.

Zugriffssteuerungsliste (ACL)
: In der Computersicherheit eine Liste, die einem Objekt zugeordnet ist und die alle Subjekte, die auf das Objekt zugreifen können, und deren Zugriffsberechtigungen identifiziert.

Zuordnung
: Die definierte Beziehung zwischen einem Clientknoten und einem Clientzeitplan. Eine Zuordnung kennzeichnet den Namen eines Zeitplans, den Namen der Maßnahmendomäne, zu der der Zeitplan gehört, sowie den Namen eines Clientknotens, der geplante Operationen ausführt.

Zurückschreiben
: Informationen vom Sicherungsstandort in den aktiven Speicherstandort kopieren, damit sie verwendet werden können. Ein Beispiel ist das Kopieren von Informationen aus dem Serverspeicher auf eine Client-Workstation.

Zurückschreibung einer einzelnen Mailbox
: Siehe Mailboxzurückschreibung.